Representation theory of algebras

Leandro Vendramin

Abstract. 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.

Contents

Part 1.

Introduction 2
1. Lecture: Week 1 3
2. Lecture: Week 2 11
3. Lecture: Week 3 18
4. Lecture: Week 4 22
5. Lecture: Week 5 32
6. Lecture: Week 6 38
7. Lecture: Week 7 46
8. Lecture: Week 8 55
9. Lecture: Week 9 63
10. Lecture: Week 10 65
11. Lecture: Week 11 67
12. Lecture: Week 12 72

Part 2.

13. Project: Irreducible characters of dihedral groups 80
14. Project: Hurwitz' theorem 83
15. Project: Gallagher's theorem 88

Part 3.

Some other topics for final projects 90
References 92
Index 94

Department of Mathematics and Data Science, Vrije Universiteit Brussel, Pleinlaan 2, 1050 Brussel

E-mail address: `Leandro.Vendramin@vub.be`.

Introduction

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

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

The notes include Magma code, which we use to verify examples and offer alternative solutions to certain exercises. Magma [**5**] is a powerful software tool designed for working with algebraic structures. There is a free online version of Magma available.

Thanks go to Luca Descheemaeker, Wannes Malfait, Silvia Properzi, Lukas Simons.

This version was compiled on April 4, 2025 at 23:25.

1. Lecture: Week 1

§ 1.1. The Artin–Wedderburn theorem. We first review the basic definitions concerning finite-dimensional semisimple algebras. Proofs can be found in the notes to the course **Associative Algebras** (see Lectures 1, 2 and 3).

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

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

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

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

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

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

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

1.2. Theorem (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 $n_1, \dots, n_k \in \mathbb{Z}_{>0}$.

The unique simple module of the algebra $M_{n_j}(\mathbb{C})$ is the column space $\mathbb{C}^{n_j}$. This means that the simple component of dimension n_j^2 has a simple module of dimension n_j.

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

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

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

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

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

§ 1.2. 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 $\mathbb{C}[G]$.

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

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

1.4. Exercise. Prove that $\mathbb{C}[C_n] \simeq \mathbb{C}[X]/(X^n - 1)$.

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

$$\operatorname{Fun}(G, \mathbb{C}) = \{\alpha \colon G \to \mathbb{C}\}$$

is a complex vector space with the operations

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

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

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

Let

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

Prove the following statements:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

where r is the number of isomorphism classes of simple modules of $\mathbb{C}[G]$. Moreover,

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

and the integers $n_1, n_2, \dots, n_r$ are the dimensions of the non-isomorphic simple modules of the complex group algebra $\mathbb{C}[G]$.

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

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

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

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

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

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

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

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

If G is a finite group, then

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

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

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

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

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

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

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

1.12. Bonus exercise. 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. Prove that if the map $U \to U$, $u \mapsto u^m$, is bijective, there exists a normal K-invariant subgroup N of V such that $V = U \times N$.

1.13. Bonus exercise. 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. Prove that if U be a K-invariant subgroup of V, there exists a K-invariant subgroup N of V such that $V = U \times N$.

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

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

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

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

where $n = \dim V$.

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

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

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

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

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

is a representation of G.

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

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

is a representation of G.

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

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

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

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

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

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

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

is a representation.

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

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

is a representation of degree $|X|$.

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

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

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

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

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

This bijection between representations of groups and modules over group algebras allows us to construct a dictionary between concepts in the language of representations and that of modules. Both languages are useful, so depending on our convenience, we will use one or the other.

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

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

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

$$\psi_g T = T\phi_g$$

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

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

1.25. Example. The representation

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

is equivalent to the representation

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

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

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

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

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

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

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

1.29. Example. Degree-one representations are irreducible.

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

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

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

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

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

The set

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

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

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

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

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

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

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

1.34. Example. 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 1.33 shows that ϕ is irreducible.

2. Lecture: Week 2

We now describe some crucial examples of representations.

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

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

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

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

such that $\{v_i\otimes w_j : 1\leq i\leq k,\ 1\leq j\leq l\}$ 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

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

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

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

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

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

where

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

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

2.3. Exercise. Let G be a finite group and V be a $\mathbb{C}[G]$-module. Prove that the dual V^* is a $\mathbb{C}[G]$-module with

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

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

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

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

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

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

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

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

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

2.6. Definition. A representation $\rho\colon G \to \mathbf{GL}(V)$ 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.

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

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

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

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

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

2.9. Example. We can compute the character of the representation

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

of Example 1.34. Since

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

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

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

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

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

PROOF. The first statement is trivial.

To prove 2) note that

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

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

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

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

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

If two representations are equivalent, their characters are equal.

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

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

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

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

2.12. EXERCISE. Let G be a finite group. For a conjugacy class K of G let

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

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

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

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

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

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

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

PROOF. For each $g \in G$, the map ρ_g is diagonalizable. Let $\{v_1, \dots, v_n\}$ 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 $(\rho \otimes \psi)_g$ with eigenvalue $\lambda_i\mu_j$, as

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

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

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

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

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

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

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

and the claim follows.

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

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

We can then form linear combinations of characters. These functions, of course, are not necesarilly characters.

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

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

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

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

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

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

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

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

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

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

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

PROOF. The first part is left as an exercise.

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

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

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

2.17. EXERCISE. 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:

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

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

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

2.19. EXERCISE. Let G be a finite group. Prove that the set $\mathrm{Irr}(G)$ is a basis of $\mathrm{ClassFun}(G)$.

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

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

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

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

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

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

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

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

Thus

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

for all $u \in U$. This implies that α has eigenvalues 0 and 1. In fact, if $u \in U$ is an eigenvector of α of eigenvalue $\lambda \in \mathbb{C}$, then

$$\lambda u = \alpha(u) = \alpha(\alpha(u)) = \alpha(\lambda u) = \lambda\alpha(u) = \lambda^2 u.$$

Thus $\lambda(\lambda - 1) = 0$.

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

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

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

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

Thus

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

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.

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

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

Proof. We claim that

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

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

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

for all $u \in U$. Now we prove that $\operatorname{Hom}_G(U,V) \supseteq \operatorname{Hom}(U,V)^G$. Let $f \in \operatorname{Hom}(U,V)^G$. Then $f\colon U \to V$ 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 2.18,

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

Since $\dim \operatorname{Hom}_G(U,V) \in \mathbb{R}$, one has

$$\langle \chi_U, \chi_V \rangle = \overline{\langle \chi_V, \chi_U \rangle} = \langle \chi_V, \chi_U \rangle$$

and the claim follows. □

Let G be a finite group and $\operatorname{Irr}(G) = \{\chi_1, \dots, \chi_k\}$. Note that k is 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 $i, j \in \{1, \dots, k\}$.

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

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

Two entries of the character table of Example 2.22 are still unknown. As we further develop the theory of characters, we will discover several tricks that can be used to find these missing entries.

3. Lecture: Week 3

§ 3.1. Schur's orthogonality relations. We start with a crucial exercise. It is known as Schur's lemma.

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

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

3.2. Definition. Let G be a group. A representation $\rho\colon G \to \mathbf{GL}(V)$ is said to be **faithful** if ρ is injective.

3.3. Exercise. Let G be a finite group that admits a faithful irreducible representation. Prove that $Z(G)$ is cyclic.

To solve Exercise 3.3 one needs to use the following elementary fact: A finite subgroup of $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ is cyclic.

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

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

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

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

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

With the theorem, one can construct the character table of $\mathbb{S}_3$. For example, this can be done using that $\langle \chi_3, \chi_3 \rangle = 1$ and that $\langle \chi_1, \chi_3 \rangle = 0$. As an exercise, verify that the character table of $\mathbb{S}_3$ is given in Table 3.1.

Table 1. The character table of $\mathbb{S}_3$.

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

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

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

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

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

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

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

for some integers $a_1,\dots,a_k\geq 0$. Let $L\colon G\to\mathbb{S}_G$, $g\mapsto L_g$, 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

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

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

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

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

We now prove Schur's second orthogonality relation.

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

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

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

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

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

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

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

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

3.9. Exercise. Let G be a finite group and $g_1, \dots, g_r$ be the representatives of the conjugacy classes of G. Assume that $\mathrm{Irr}(G) = \{\chi_1, \dots, \chi_r\}$. Compute the determinant of the matrix $X = (\chi_j(g_i))_{1 \leq i,j \leq r}$.

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

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

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

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

Then

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

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

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

3.11. Exercise (Solomon). Let G be a finite group and $g_1, \dots, g_r$ be the representatives of the conjugacy classes of G. Assume that $\mathrm{Irr}(G) = \{\chi_1, \dots, \chi_r\}$. Prove that

$$|G| \geq \sum_{i=1}^{r} \sum_{j=1}^{r} \chi_i(C_j) \in \mathbb{Z}_{\geq 1}.$$

Moreover, if $|G| = \sum_{i=1}^{r} \sum_{j=1}^{r} \chi_i(C_j)$, then $G/Z(G)$ is abelian.

§ 3.2. Algebraic integers and characters.

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

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

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

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

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

$$f = X^k + a_{k-1}X^{k-1} + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$$

of degree $k \geq 1$, then

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

This implies that

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4. Lecture: Week 4

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 $g \in C$.

4.1. Theorem. *Let G be a finite group, $\chi \in \mathrm{Irr}(G)$ and K be a conjugacy class of G. Then*

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

We need a lemma.

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

Proof. Let us first prove $\implies$. Let $f = X^k + a_{k-1}X^{k-1} + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$ 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, $xz_k = x^k = -a_0 - a_1x - \cdots - a_{k-1}x^{k-1}$.

We now prove $\impliedby$. Let $A = (a_{ij}) \in \mathbb{Z}^{k\times k}$ and Z be the column vector $Z = \begin{pmatrix} z_1 \\ \vdots \\ z_k \end{pmatrix}$. Note that Z is non-zero. Moreover, $AZ = xZ$, as

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

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

The previous lemma could be used to give an alternative proof of the fact that the algebraic integers form a ring.

Proof of Theorem 4.1. Let φ be a representation of G and χ be its character. Note that φ is irreducible. Let $C_1, \dots, C_r$ be the conjugacy classes of G and for every $i \in \{1, \dots, r\}$ let

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

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

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

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

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

We now prove that

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

To prove this we compute λ:

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

Then the claim follows.

Now we claim that

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

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

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

where a_{ijg} is the number of elements $(x,y)\in C_i\times C_j$ such that $g=xy$.

Claim. Once i and j are fixed, a_{ijg} depends only on the conjugacy class of g.

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

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

is well-defined. It is bijective with inverse

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

Hence $|X_g| = |X_h|$.

Let a_{ijk} be the number of elements $(x,y)\in C_i\times C_j$ such that $xy = g$ for some $g\in C_k$. Then

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

Therefore

$$\left(\frac{|C_i|}{\chi(1)}\chi(C_i)\right)\left(\frac{|C_j|}{\chi(1)}\chi(C_j)\right) = \sum_{k=1}^{r} a_{ijk}\left(\frac{|C_k|}{\chi(1)}\chi(C_k)\right). \tag{4.1}$$

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

§ 4.1. Frobenius' theorem.

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

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

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

Note that this is a rational number. Let $C_1,\dots,C_r$ be the conjugacy classes of G. Then

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

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

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

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

Another application:

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

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

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

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

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

for some $\lambda, \mu \in \{-1, 1\}$. Since $1 = \det \rho_x = \lambda\mu$ and ρ_x is not the identity matrix, $\lambda = \mu = -1$. 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. $\square$

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

Let G and G_1 be groups. If V is a $\mathbb{C}[G]$-module and V_1 is a $\mathbb{C}[G_1]$-module, then $V \otimes V_1$ is a $\mathbb{C}[G \times G_1]$-module with

$$(g, g_1) \cdot v \otimes v_1 = (g \cdot v) \otimes (g_1 \cdot v_1)$$

for $(g, g_1) \in G \times G_1$, $v \in V$ and $v_1 \in V_1$.

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

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

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

□

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

We now prove Schur's theorem. The proof goes back to Tate; it uses the **tensor power trick**. See Tao's blog for other applications of this powerful trick.

Proof of Theorem 4.6. Let $\rho\colon G \to \mathbf{GL}(V)$ be an irreducible representation with character χ. Let $z \in Z(G)$. Then ρ_z commutes with ρ_g for all $g \in G$. By Schur's lemma, $\rho_z(v) = \lambda(z)v$ for all $v \in V$. Note that $\lambda\colon Z(G) \to \mathbb{C}^\times$, $z \mapsto \lambda(z)$, is a well-defined group homomorphism, as

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

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

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

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

Then σ is a representation. The character of σ is χ^n. By the previous lemma, σ is irreducible. For $z_1, \dots, z_n \in Z(G)$, we compute

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

Let

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

Then H is a central subgroup of G^n. Moreover, H acts trivially on $V^{\otimes n}$, so there exists a group homomorphism σ that makes the diagram

$$\begin{tikzcd} G^n \arrow[r, "\sigma"] \arrow[d] & \mathbf{GL}(V^{\otimes n}) \\ G^n/H \arrow[ur, dashed, "\tau"'] & \end{tikzcd}$$

commutative. Thus

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

is a representation of degree $\chi(1)^n$: 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

$$|G| = \chi(1)s \quad \text{and} \quad |G|(G:Z(G))^{n-1} = \chi(1)^n r$$

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). □

§ 4.2. Examples of character tables. Let G be a finite group and $\chi_1, \dots, \chi_r$ be the irreducible characters of G. Without loss of generality, we may assume that χ_1 is the trivial character, i.e., $\chi_1(g) = 1$ for all $g \in G$. Recall that r is the number of conjugacy classes of G. Each χ_j is constant on conjugacy classes. The **character table** of G is presented as follows, arranging group elements and character values in a tabular format:

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

Here, the numbers n_j represent the degrees of the irreducible representations of G, and each k_j denotes the size of the conjugacy class of the element g_j. By convention, the character table contains only the values of the irreducible characters of the group.

4.9. Example. For $n \geq 2$, let $G = \langle g \rangle$ be the cyclic group of order n. Let λ be a primitive n-th root of one. For each i, let V_i be a (complex) one-dimensional vector space with basis $\{v\}$. Each V_i is a $\mathbb{C}[G]$-module with

$$g \cdot v = \lambda^{i-1} v.$$

Moreover, each V_i is simple, as $\dim V_i = 1$. The character χ_i associated with V_i is given by $\chi_i(g^m) = \lambda^{m(i-1)}$ for all $m \in \{1, \dots, n\}$. Since the $\chi_1, \dots, \chi_n$ are all different and G admits n irreducible representations, it follows that $\mathrm{Irr}(G) = \{\chi_1, \dots, \chi_n\}$. The character table of G is shown in Table 2.

Table 2. The character table of the cyclic group C_n of order n.

	1	1	1	$\cdots$	1
	1	g	g^2	$\cdots$	g^{n-1}
χ_1	1	1	1	$\cdots$	1
χ_2	1	λ	λ^2	$\cdots$	λ^{n-1}
χ_3	1	λ^2	λ^4	$\cdots$	λ^{n-2}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
χ_n	1	λ^{n-1}	λ^{n-2}	$\cdots$	λ

4.10. Example. Let $G = \langle g : g^4 = 1\rangle$ be the cyclic group of order four. The character table of G is given by Table 3. Let us see how to see this calculation on the computer:

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


Character Table of Group C4
---------------------------


--------------------
Class |   1  2  3  4
Size  |   1  1  1  1
Order |   1  2  4  4
--------------------
p  =  2   1  1  2  2
--------------------
X.1   +   1  1  1  1
X.2   +   1  1 -1 -1
X.3   0   1 -1  I -I
X.4   0   1 -1 -I  I


Explanation of Character Value Symbols
--------------------------------------

I = RootOfUnity(4)
```

Table 3. The character table of the cyclic group C_4 of order four.

	1	1	1	1
	1	g	g^2	g^3
χ_1	1	1	1	1
χ_2	1	1	-1	-1
χ_3	1	-1	i	$-i$
χ_4	1	-1	$-i$	i

Some remarks:

1) The symbol `I` denotes a primitive fourth root of 1.

2) The function `CharacterTable` computes more than just the character table of the group; it also provides additional information.

```
> T[1];
( 1, 1, 1, 1 )
> Degree(T[1]);
1
```

```
> Degree(T[2]);
1
> Degree(T[3]);
1
> Degree(T[4]);
1
```

4.11. Example. The character table of the group $C_2 \times C_2 = \{1, a, b, ab\}$ is shown in Table 4.

Table 4. The character table of $C_2 \times C_2$.

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

Let us do this by computer:

```
> C2xC2 := AbelianGroup([2,2]);
> T := CharacterTable(C2xC2);
> T;


Character Table of Group C2xC2
------------------------------


--------------------
Class |   1  2  3  4
Size  |   1  1  1  1
Order |   1  2  2  2
--------------------
p  =  2   1  1  1  1
--------------------
X.1    +   1  1  1  1
X.2    +   1 -1  1 -1
X.3    +   1  1 -1 -1
X.4    +   1 -1 -1  1
```

4.12. Example. The character table of $\mathbb{S}_3$ was computed on Table 3.1; see page 18. Let us recall briefly one possible way to compute this table. Degree-one characters were easy to compute. To compute the third row of the table, one possible approach is to use the irreducible representation

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

Then

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

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

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

```
> S3 := Sym(3);
> T := CharacterTable(S3);
> T;


Character Table of Group S3
---------------------------


-----------------
Class |   1  2  3
Size  |   1  3  2
Order |   1  2  3
-----------------
p  =  2   1  1  3
p  =  3   1  2  1
-----------------
X.1   +   1  1  1
X.2   +   1 -1  1
X.3   +   2  0 -1
```

4.13. Example. Let us compute the character table of $\mathbb{S}_4$. We know that $|\mathbb{S}_4| = 24$ and that $\mathbb{S}_4$ has five conjugacy classes:

Representative	id	(12)	(12)(34)	(123)	(1234)
Size	1	6	3	8	6

Thus $\operatorname{Irr}(\mathbb{S}_4) = \{\chi_1, \chi_2, \dots, \chi_5\}$. We may assume that χ_1 is the trivial character and that χ_2 is the sign. Since $[\mathbb{S}_4, \mathbb{S}_4] \simeq \mathbb{A}_4$, the quotient $\mathbb{S}_4/[\mathbb{S}_4, \mathbb{S}_4]$ has order two and hence $\mathbb{S}_4$ admits exactly two degree-one irreducible representations. Hence we know two rows of the character table of $\mathbb{S}_4$:

	id	(12)	(12)(34)	(123)	(1234)
χ_1	1	1	1	1	1
χ_2	1	-1	1	1	-1

There exist $n_3, n_4, n_5 \in \{2, 3, 4\}$ such that $24 = 1 + 1 + n_3^2 + n_4^2 + n_5^2$. A direct calculation shows that $(n_3, n_4, n_5) = (2, 3, 3)$ is the only solution with $n_3 \leq n_4 \leq n_5$.

To find the other characters, it is useful to use the action of $\mathbb{S}_4$ on the vector space

$$V = \{(x_1, x_2, x_3, x_4) \in \mathbb{R}^4 : x_1 + x_2 + x_3 + x_4 = 0\},$$

given by

$$g \cdot (x_1, x_2, x_3, x_4) = (x_{g^{-1}(1)}, x_{g^{-1}(2)}, x_{g^{-1}(3)}, x_{g^{-1}(4)}).$$

Let

$$v_1 = (1,0,0,-1), \quad v_2 = (0,1,0,-1), \quad v_3 = (0,0,1,-1).$$

Then $\{v_1, v_2, v_3\}$ is a basis of V and

$$\begin{aligned} &(12)\cdot v_1 = v_2, && (12)\cdot v_2 = v_1, && (12)\cdot v_3 = v_3,\\ &(1432)\cdot v_1 = -v_3, && (1432)\cdot v_2 = v_1 - v_3, && (1432)\cdot v_3 = v_2 - v_3. \end{aligned}$$

Since $\mathbb{S}_4 = \langle (12), (1432)\rangle$, this is enough to know how any element $g \in \mathbb{S}_4$ acts on any $v \in V$. This action yields a representation $\rho \colon \mathbb{S}_4 \to \mathbf{GL}(V)$:

$$\rho_{(12)} = \begin{pmatrix} 0 & 1 & 0\\ 1 & 0 & 0\\ 0 & 0 & 1 \end{pmatrix}, \quad \rho_{(1432)} = \begin{pmatrix} 0 & 1 & 0\\ 0 & 0 & 1\\ -1 & -1 & -1 \end{pmatrix}.$$

Let χ be the character of ρ. Then $\chi(\mathrm{id}) = 3$, $\chi\left((12)\right) = 1$, $\chi\left((1234)\right) = -1$. How to compute the value of χ on 3-cycles? Here is the trick:

$$\chi\left((234)\right) = \chi\left((12)(1234)\right) = \operatorname{trace}(\rho_{(12)}\rho_{(1234)}) = \operatorname{trace}\begin{pmatrix} 0 & 0 & 1\\ 0 & 1 & 0\\ 1 & -1 & -1 \end{pmatrix} = 0.$$

Similarly, to compute χ on products of two transpositions, we note that

$$\chi\left((13)(24)\right) = \chi\left((1234)(1234)\right) = \operatorname{trace}(\rho^2_{(1234)}) = \operatorname{trace}\begin{pmatrix} 0 & 0 & 1\\ 1 & -1 & -1\\ -1 & 2 & 0 \end{pmatrix} = -1.$$

Now is an easy exercise to check that this χ is irreducible:

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

Moreover, $\operatorname{sign}\otimes\chi$ is also an irreducible representation:

$$\langle \operatorname{sign}\otimes\chi, \operatorname{sign}\otimes\chi\rangle = \frac{1}{24}(3^2 + (-1)^2 6 + (-1)^2 3 + 6) = 1.$$

With the trivial representation χ_1, the sign representation χ_2 and these two new characters, namely $\chi_3 = \chi$ and $\chi_4 = \operatorname{sign}\otimes\chi$, we are almost done. Only one irreducible character is missing. Let us call this character χ_5. This character can be determined using the left regular representation L:

$$\begin{aligned} 0 &= \chi_L\left((12)\right) = 1 + (-1) + 3 + 3(-1) + 2\chi_5\left((12)\right),\\ 0 &= \chi_L\left((12)(34)\right) = 1 + 1 + 3(-1) + 3(-1) + 2\chi_5\left((12)(34)\right),\\ 0 &= \chi_L\left((123)\right) = 1 + 1 + 0 + 0 + 2\chi_5\left((123)\right),\\ 0 &= \chi_L\left((1234)\right) = 1 + (-1) + 3(-1) + 3 + 2\chi_5\left((1234)\right) = 0, \end{aligned}$$

Now we are ready to compute the character table of $\mathbb{S}_4$:

TABLE 5. The character table of $\mathbb{S}_4$.

	1 id	6 (12)	3 (12)(34)	8 (123)	6 (1234)
χ_1	1	1	1	1	1
sign	1	-1	1	1	-1
χ	3	1	-1	0	-1
sign $\otimes\chi$	3	-1	-1	0	1
χ_5	2	0	2	-1	0

4.14. EXERCISE. Compute the character table of $\mathbb{A}_4$.

4.15. EXERCISE. Compute the character table of a non-abelian group of order eight.

There are two non-isomorphic non-abelian groups of order eight: the dihedral group $\mathbb{D}_4$ and the quaternion group Q_8. One does not need to use this information to solve Exercise 4.15.

5. Lecture: Week 5

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

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

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

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

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

Isaacs proved the conjecture for solvable groups; see [20, 23]. Using [24] and the classification of finite simple groups, Malle and Späth proved the conjecture for p = 2 in [31].

In full generality, McKay's conjecture was proved in 2024.

5.2. Theorem (Cabanes–Späth). *If G is finite, p a prime number and $P \in \mathrm{Syl}_p(G)$, then*

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

We cannot prove Theorem 5.2 here. However, we can use the computer to prove some particular cases with the following function:

```
> McKay := function(G, p)
function> local N, n, m;
function> N := Normalizer(G, SylowSubgroup(G, p));
function> degG := CharacterDegrees(G);
function> degN := CharacterDegrees(N);
function> n := &+[ d[2] : d in degG | d[1] mod p ne 0 ];
function> m := &+[ d[2] : d in degN | d[1] mod p ne 0 ];
function> return n eq m;
function> end function;
```

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

```
> M11 := sub<Sym(11) | (1,10)(2,8)(3,11)(5,7), (1,4,7,6)(2,11,10,9)>;
> McKay(M11,2);
true
> McKay(M11,3);
true
> McKay(M11,5);
true
> McKay(M11,11);
true
```

5.3. Bonus exercise. Verify the McKay's conjecture for all sporadic simple groups.

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

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

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

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

5.5. BONUS EXERCISE. Verify the Isaacs–Navarro conjecture in some small groups, such as the Mathieu simple group M_{11}.

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

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

In the proof of Theorem 4.1, Equality (4.1), we obtained that

$$\omega_\chi(C_i)\omega_\chi(C_j) = \sum_{k=1}^{s} a_{ijk}\omega_\chi(C_k), \tag{5.1}$$

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

5.6. THEOREM (Burnside). *Let G be a finite group with conjugacy classes $C_1, \dots, C_s$. Then*

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

PROOF. By (5.1),

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

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

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

because

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

$\square$

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

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

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

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

We first prove $\Longleftarrow$. Since $a_{ijk} > 0$, there exist $u \in C_i$ and $v \in C_j$ such that $g = uv$ (since $zgz^{-1} = u_1v_1$ 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 $z_2x^{-1}z_2^{-1} = v$. If $y = z^{-1}z_2$, then g and $[x, y]$ are conjugate, as

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

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

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

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

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

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

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

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

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

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

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

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

solutions. If (x,u) is a solution of $xu^{-1}=g$, then there are exactly $|C_G(x)|$ elements y such that $yxy^{-1}=u$. In fact, since x and u are conjugate, there exists y such that $yxy^{-1}=u$. And if $u=y_1xy_1^{-1}$ for some y_1, then $y_1^{-1}y\in C_G(x)$ which implies that $y_1=y\xi$ for some $\xi\in C_G(x)$. Now $[x,y]=x(yx^{-1}y^{-1})=g$ 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 C of G:

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

From this, the formula follows. □

Application:

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

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

§ 5.3. Ore's conjecture. In 1951 Ore and independently Itô 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".

5.11. Conjecture (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:

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

The proof appears in [**29**]. It needs about 70 pages and uses the classification of finite simple groups (CFSG) and character theory. See [**30**] for more information on Ore's conjecture and its proof.

Although 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:

5.13. Bonus exercise. Verify Ore's conjecture for sporadic simple groups.

See [28] for other applications of character theory.

§ 5.4. The Cauchy–Frobenius–Burnside theorem. The result we will now see is often called Burnside's lemma. Burnside proved this lemma in his book on finite groups, attributing it to Frobenius. However, the formula was already known to Cauchy in 1845. Because of this, the result is sometimes referred to as the lemma that is not Burnside's; see [32].

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

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

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

Proof. Let $X = \{x_1,\dots,x_n\}$ and V be the complex vector space with basis $\{x_1,\dots,x_n\}$. Let $\rho\colon G \to \mathbf{GL}_n(\mathbb{C})$, $g \mapsto \rho_g$, be the representation

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

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

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

Recall that

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

and that

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

where χ_1 is the trivial character of G (see Lemma 2.20).

We can assume that, after a possible re-enumeration, $x_1,\dots,x_m$ are 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

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

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

$$\sum_{g\in G} |\operatorname{Fix}(g)| = \sum_{g\in G} \sum_{\substack{x\in X\\ g\cdot x = x}} 1 = \sum_{x\in X} \sum_{\substack{g\in G\\ g\cdot x = x}} 1 = \sum_{x\in X} |G_x| = |G_{x_0}||X| = |G|,$$

where $x_0 \in X$ is any fixed element of X. I learned about this analytic number theory-style proof in Serre's paper [**34**].

5.15. Exercise. Use the previous idea to prove Theorem 5.14.

A probabilistic proof of Theorem 5.14 is presented in [**42**].

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

$$g \cdot (x, y) = (g \cdot x, g \cdot y). \tag{5.2}$$

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

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

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

Proof. The action (5.2) has $\operatorname{Fix}(g) \times \operatorname{Fix}(g)$ as fixed points, as

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

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

5.17. Definition. Let G act 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 $g \cdot x = x_1$ and $g \cdot y = y_1$.

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

5.18. Proposition. *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 $g \cdot x = x_1$ and $g \cdot y = y_1$, so $g \cdot (x, y) = (x_1, y_1)$. $\square$

6. Lecture: Week 6

The Cauchy–Frobenius–Burnside theorem is helpful to find characters.

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

Proof. By assumption, G is 2-transitive on X. In particular, G is transitive on X. Let $\operatorname{Irr}(G) = \{\chi_1, \dots, \chi_k\}$, where χ_1 is the trivial character. Since χ_1 is irreducible, $\langle \chi_1, \chi_1 \rangle = 1$. By the Cauchy–Frobenius–Burnside theorem, the rank of G on X is

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

Moreover, again by the Cauchy–Frobenius–Burnside theorem,

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

since the action of G on X is, in particular, transitive. Thus

$$\langle \chi - \chi_1, \chi - \chi_1 \rangle = \langle \chi, \chi \rangle - \langle \chi, \chi_1 \rangle - \langle \chi_1, \chi \rangle + \langle \chi_1, \chi_1 \rangle = 2 - \frac{2}{|G|} \sum_{g \in G} \chi(g) + 1 = 1.$$

Now write $\chi - \chi_1 = \sum_{i=1}^{k} a_i \chi_i$ for some integers $a_1, \dots, a_k \in \mathbb{Z}$. Since $a_1 = \langle \chi, \chi_1 \rangle$, it follows that

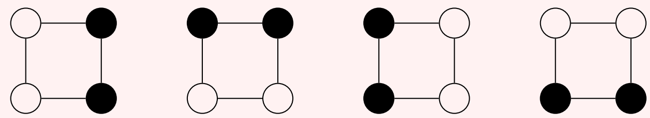
$$1 = \left\langle \sum_{i=1} a_i \chi_i, \sum_{j=1} a_j \chi_j \right\rangle = \sum_{i=2}^{k} a_i^2.$$

Since χ is a character, $\chi - \chi_1$ is an integer linear combination of the irreducible characters of G. Then there exists a unique $i \in \{2, \dots, k\}$ such that $a_i \in \{-1, 1\}$ and $a_j = 0$ for all $j \neq i$. Hence $\chi - \chi_1 = \pm \chi_i$. Since $(\chi - \chi_1)(1) = |X| - 1 \geq 0$, it follows that $\chi - \chi_1 = \chi_i$. □

6.2. Example. 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 $\chi(g) = |\operatorname{Fix}(g)| - 1$.

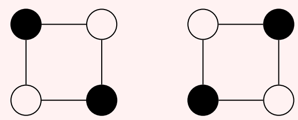
6.3. Example. Let p be a prime number and let $q = p^m$. Let V be the vector space of dimension 2 over the finite field of q elements. The group $G = \mathbf{GL}_2(q)$ acts 2-transitively on the set X of one-dimensional subspaces of V. In fact, if $\langle v \rangle \neq \langle v_1 \rangle$ and $\langle w \rangle \neq \langle w_1 \rangle$, 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 $\chi(g) = |\operatorname{Fix}(g)| - 1$.

6.4. Example. 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

(6.1) 

will be considered 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 act on X by anti-clockwise rotations of 90°. All the colorings of (6.1) belong to the same orbit. Another orbit of X is

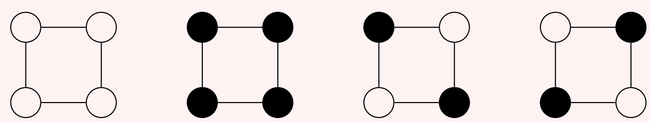


Cauchy–Frobenius–Burnside theorem states that there are

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

orbits.

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



Thus X is the union of

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

orbits.

6.5. Bonus exercise. 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.

There are 5282 ways (up to symmetry) to arrange eight non-attacking rooks on a chessboard.

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

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

We claim that

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

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

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

as $\operatorname{Fix}(g)=\{x\in G:gxg^{-1}=x\}=C_G(g)$ and $\sum_{g\in G}|C_G(g)|=|C|$. Alternatively, using Theorem 5.9 with $g=1$,

$$\operatorname{cp}(G)=\frac{\tau(1)}{|G|^2}=\frac{1}{|G|}\sum_{\chi\in\operatorname{Irr}(G)}1=\frac{k}{|G|},$$

as $k=|\operatorname{Irr}(G)|$.

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

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

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

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 $k/|G|\leq 5/8$. $\square$

6.7. Exercise.

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

6.8. Exercise. Let G be a finite non-abelian group and p be the smallest prime number dividing $|G|$. Prove that $\operatorname{cp}(G)\leq(p^2+p-1)/p^3$.

6.9. Bonus exercise. Let G be a finite group and H be a subgroup of G.

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

For the next proposition, which provides a lower bound for the commuting probability, we will use the **Cauchy–Schwarz inequality**:

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

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

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

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

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

From this, the claim follows. □

Using basic facts about irreducible characters, we derive a generalization of Theorem 6.6.

6.11. Theorem. *Let G be a finite group. Then*

$$\operatorname{cp}(G) \leq \frac{1}{4} \left(1 + \frac{3}{|[G,G]|} \right) .$$

Proof. For $n \in \mathbb{Z}_{>0}$, let ρ_n be the number of irreducible characters of degree n. Then the number of conjugacy classes of G is $k = \sum_{i \geq 1} \rho_i$ and $|G| = \sum_{i \geq 1} i^2 \rho_i$. It follows that

$$|G| - \rho_1 = \sum_{i \geq 2} i^2 \rho_i \geq 4 \sum_{i \geq 2} \rho_i = 4(k - \rho_1) = 4(|G| \operatorname{cp}(G) - \rho_1).$$

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

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

□

6.12. Exercise. Use Theorem 6.11 to prove Theorem 6.6.

Theorem 6.11 can also be used to prove similar statements.

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

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

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

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

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

is well-defined.

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

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

$$\begin{tikzcd} G/Z(G) \times G/Z(G) \arrow[r, "\sigma\times\sigma"] \arrow[d, "c_G"'] & H/Z(H) \times H/Z(H) \arrow[d, "c_H"] \\ {[G,G]} \arrow[r, "\tau"'] & {[H,H]} \end{tikzcd} \tag{6.2}$$

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

Prove the following statements:

1) If $G \simeq H$, then $G \sim H$.
2) If G and H are finite groups such that $G \sim H$, then $\mathrm{cp}(G) = \mathrm{cp}(H)$.

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

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

The following theorem appeared in 1970 as a problem in volume 13 of the *Canadian Math. Bulletin*. The solution appeared in 1973. Iván Sadosfchi Costa found in 2018 the proof we present here.

6.18. Theorem (Dixon). *The commuting probability of every finite non-abelian simple group is at most* $1/12$.

Sketch of the proof. Let G be a finite non-abelian simple group. We claim that $\mathrm{cp}(G) \le 1/12$. We assume that $\mathrm{cp}(G) > 1/12$. Since G is a non-abelian simple group, the identity of G is the only central element of G.

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

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

$$|G| \ge 1 + (k-1)13 = 13k - 12.$$

Since $\mathrm{cp}(G) = k/|G| > 1/12$, $k > |G|/12$. Thus

$$|G| > \frac{13}{12}|G| - 12$$

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

6.19. Bonus exercise. Provide the details of the proof of Theorem 6.18.

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

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

The proof appears in [**15**].

Results on probability of commuting elements generalize in other directions. In [**38, 39, 40, 41**], Thompson proved the following result:

6.21. Theorem (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 [**9**].

There is a probabilistic version of Thompson's theorem:

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

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

2) *If the probability that two random elements of G generate a nilpotent group is $> 1/2$, then G is nilpotent.*

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

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

§ 6.2. Jordan's theorem and applications. We now follow [**34**] to present other applications.

6.23. Theorem (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. The Cauchy–Frobenius–Burnside theorem implies that

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

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

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

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

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

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 $g \notin \bigcup_{x\in G} xHx^{-1}$. □

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

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

Proof. We prove $\Longleftarrow$. Assume that C commutes 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 $G = \bigcup_{g\in G} gHg^{-1}$. 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 $x = y^{-1}hy \in \bigcup_{g\in G} gHg^{-1}$. By Corollary 6.24, $H = G$. Thus c is central and hence $C = \{c\}$.

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

There is a theorem similar to Jordan's.

6.26. Theorem (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 [7] and depends on the CFSG. It is unknown whether a proof of Theorem 6.26 without relying on the CFSG exists.

§ 6.3. Derangements: The Cameron–Cohen theorem. Let G be a finite group that acts faithfully and transitively on a finite set X, say $G \leq \mathbb{S}_n$, where $X = \{1,2,\dots,n\}$. Let G_0 be 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**.

6.27. Example. Let $G = \mathbb{S}_3$. Then $G_0 = \{(123),(132)\}$.

6.28. Example. Let $G = \mathbb{S}_4$. Then

$$G_0 = \{(12)(34),(13)(24),(14)(23),(1234),(1243),(1324),(1342),(1423),(1432)\}.$$

We want to estimate the number of derangements. For this purpose, let $c_0 = |G_0|/|G|$.

6.29. Theorem (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 $\chi(g) = |\operatorname{Fix}(g)|$ 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,

$$\begin{aligned}
&\frac{1}{|G|}\sum_{g\in G}(\chi(g)-1)(\chi(g)-n)\\
&\qquad\qquad = \frac{1}{|G|}\left\{\sum_{g\in G_0}+\sum_{g\in G\setminus G_0}\right\}(\chi(g)-1)(\chi(g)-n)\\
&\qquad\qquad = \frac{1}{|G|}\sum_{g\in G_0}(\chi(g)^2-(n+1)\chi(g)+n)+\underbrace{\frac{1}{|G|}\sum_{g\in G\setminus G_0}(\chi(g)-1)(\chi(g)-n)}_{\leq 0}\\
&\qquad\qquad \leq n\frac{|G_0|}{|G|}=nc_0.
\end{aligned}$$

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

$$\begin{aligned}
\frac{1}{|G|}\sum_{g\in G}(\chi(g)-1)(\chi(g)-n) &= \frac{1}{|G|}\sum_{g\in G}(\chi(g)^2-(n+1)\chi(g)+n)\\
&\geq 2-\frac{n+1}{|G|}\sum_{g\in G}\chi(g)+n
\end{aligned}$$

Since G is transitive on X, the Cauchy–Frobenius–Burnside theorem implies that

$$\sum_{g\in G}\chi(g)=|G|.$$

Thus $2-(n+1)+n\leq nc_0$ and hence $1/n\leq c_0$. □

The Cameron–Cohen theorem contains another claim: If n is not the power of a prime number, then $c_0>1/n$ (see Theorem 9.4). The proof uses Frobenius' theorem.

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

6.30. Theorem (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 [**13**] and uses the classification of finite 2-transitive groups, which depends on the CFSG.

7. Lecture: Week 7

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

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

It is an exercise to check that

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

for all $v, w \in V$. (Thus T does not depend on the basis $\{v_1, \dots, v_n\}$.) Note that T is a homomorphism of $\mathbb{C}[G]$-modules, as

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

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

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

and the **antisymmetric** part

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

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

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

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

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

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

We claim that

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

is a basis of $S(V \otimes V)$, and that

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

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

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

Moreover,

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

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

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

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

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

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

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

it follows that

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

On the other hand, $g^2 \cdot e_i = \lambda_i^2 e_i$ for all i, $\chi(g^2) = \sum_{i=1}^n \lambda_i^2$. Thus

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

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

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

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

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

where χ_1 is the trivial character of G.

Proof. Assume that $\mathrm{Irr}(G) = \{\chi_1, \dots, \chi_k\}$. For $x \in G$ let

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

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

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

For every $\chi \in \mathrm{Irr}(G)$ we compute:

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

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

7.3. Example. We know that $\mathbb{S}_3$ has three involutions, namely (12), (23) and (13). Thus $t = 3$. Let us use Proposition 7.2 to verify this. We have already computed the character table of $\mathbb{S}_3$:

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

A direct calculation shows that

$$(\chi_1)_S = (\chi_2)_S = \chi_1 \quad \text{and} \quad (\chi_1)_A = (\chi_2)_A = 0.$$

Moreover, the values of $(\chi_3)_S$ and $(\chi_3)_A$ are given by the following table:

	1	(12)	(123)
$(\chi_3)_S$	3	1	0
$(\chi_3)_A$	1	-1	1

Let t be the number of elements of order two of $\mathbb{S}_3$. Since

$$\langle \chi_S - \chi_A, \chi_1 \rangle = 1$$

for all $\chi \in \{\chi_1, \chi_2\}$ and

$$\langle (\chi_3)_S - (\chi_3)_A, \chi_1 \rangle = \frac{1}{6}(12 + 6 - 2) = \frac{1}{6}(2 + 6 - 2) = 1,$$

Proposition 7.2 yields

$$\begin{aligned} 1 + t &= \langle (\chi_1)_S - (\chi_1)_A, \chi_1 \rangle \chi_1(1) + \langle (\chi_2)_S - (\chi_2)_A, \chi_1 \rangle \chi_2(1) + \langle (\chi_3)_S - (\chi_3)_A, \chi_1 \rangle \chi_3(1) \\ &= 1 + 1 + 2. \end{aligned}$$

Thus $t = 3$.

Before proving the Brauer–Fowler theorem, we need a lemma.

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

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

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

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

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

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

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

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

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

Now we prove the Brauer–Fowler theorem.

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

Proof. If G is abelian, the claim is trivial. Let G be a finite non-abelian simple group. We first assume the existence of a proper subgroup H of G such that

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

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

Let $m = (|G|-1)/t$, where t is the number of involutions of G. Since $|C_G(x)| = n$, the group G has at least $|G|/n$ involutions (because the conjugacy class of x has size $|G|/n$ and all its elements are involutions), that is $t \geq |G|/n$. Hence

$$m = (|G|-1)/t < n.$$

It is enough to show that G contains a subgroup of index $\leq m^2$.

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

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

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

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

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

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

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

As an exercise, a simple application:

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

§ 7.2. The character table of $\mathbb{S}_5$. Let $G = \mathbb{S}_5$. The conjugacy classes of G are given in the following table:

Representative	id	(12)	(123)	(12)(34)	(1234)	(123)(45)	(12345)
Size	1	10	20	15	30	20	24

Thus there are seven irreducible characters. The trivial character χ_1 and the sign χ_2 are degree-one (hence irreducible) characters.

	id	(12)	(123)	(12)(34)	(1234)	(123)(45)	(12345)
χ_1	1	1	1	1	1	1	1
sign	1	-1	1	1	-1	-1	1

Since $[G,G] = \mathbb{A}_5$ and $|G/[G,G]| = 2$, it follows from Exercise 1.30 that χ_1 and sign are the only degree-one characters.

Since G acts 2-transitively on $\{1,\dots,5\}$, Proposition 6.1 implies that $\varsigma(g) = |\operatorname{Fix}(g)| - 1$ is an irreducible character. A direct calculation yields the values of ς:

	id	(12)	(123)	(12)(34)	(1234)	(123)(45)	(12345)
ς	4	2	1	0	0	-1	-1

The values of the product $\operatorname{sign}\varsigma$ are easily computed:

	id	(12)	(123)	(12)(34)	(1234)	(123)(45)	(12345)
$\operatorname{sign}\varsigma$	4	-2	1	0	0	1	-1

Since

$$\begin{aligned}\langle \operatorname{sign}\varsigma, \operatorname{sign}\varsigma\rangle &= \frac{1}{120}(4^2 + 10(-2)^2 + 20 + 15\cdot 0 + 30\cdot 0 + 20 + 24)\\ &= \frac{1}{120}(16+40+20+20+24) = 1,\end{aligned}$$

it follows that $\operatorname{sign}\varsigma \in \operatorname{Irr}(G)$.

We now consider the characters

$$\psi(g) = \frac{1}{2}(\varsigma^2(g) + \varsigma(g^2)) \quad\text{and}\quad \eta(g) = \frac{1}{2}(\varsigma^2(g) - \varsigma(g^2)),$$

where $\varsigma^2(g) = \varsigma(g)\varsigma(g) = \varsigma(g)^2$ (see Proposition 7.1). A straightforward calculation shows that

	id	(12)	(123)	(12)(34)	(1234)	(123)(45)	(12345)
ψ	10	4	1	2	0	1	0
η	6	0	0	-2	0	0	1

Since

$$\langle \eta, \eta \rangle = \frac{1}{120}(6^2 + 15(-2)^2 + 24) = 1,$$

it follows that $\eta \in \operatorname{Irr}(G)$. On the other hand,

$$\langle \psi, \psi \rangle = \frac{1}{120}(10^2 + 10 \cdot 16 + 20 + 15 \cdot 4 + 20) = 3.$$

Thus ψ is the sum of three irreducible characters (see Exercise 3.7). Since

$$\langle \psi, \chi_1 \rangle = \frac{1}{120}(10 + 10 \cdot 4 + 20 + 15 \cdot 2 + 20) = 1,$$
$$\langle \psi, \varsigma \rangle = \frac{1}{120}(10 \cdot 4 + 10 \cdot 4 \cdot 2 + 20 - 20) = 1,$$

it follows that $\psi = \chi_1 + \varsigma + \chi$ for some $\chi \in \operatorname{Irr}(G)$. Thus we can compute χ:

	id	(12)	(123)	(12)(34)	(1234)	(123)(45)	(12345)
χ	5	1	-1	1	-1	1	0

We are missing one irreducible character. Let n be the degree of this character. Since $120 = 1 + 1 + 16 + 16 + 36 + 25 + n^2$, it follows that $n = 5$. Since we need a degree-five irreducible character, we can try with $\xi = \operatorname{sign} \chi$:

	id	(12)	(123)	(12)(34)	(1234)	(123)(45)	(12345)
ξ	5	-1	-1	1	1	-1	0

Since

$$\langle \xi, \xi \rangle = \frac{1}{120}(25 + 10(-1)^2 + 20(-1)^2 + 15 + 30 + 20(-1)^2) = 1,$$

it follows that $\xi \in \operatorname{Irr}(G)$. We have found the character table of G.

Table 6. The character table of $\mathbb{S}_5$.

	1 id	10 (12)	20 (123)	15 (12)(34)	30 (1234)	20 (123)(45)	24 (12345)
χ_1	1	1	1	1	1	1	1
sign	1	-1	1	1	-1	-1	1
ς	4	2	1	0	0	-1	-1
$\operatorname{sign} \varsigma$	4	-2	1	0	0	1	-1
η	6	0	0	-2	0	0	1
χ	5	1	-1	1	-1	1	0
ξ	5	-1	-1	1	1	-1	0

§ 7.3. An elementary proof of the Brauer–Fowler theorem. We need to find a subgroup of index $\leq 2n^2$. Let X be the conjugacy class of x. For $g \in G$ let

$$J(g) = \{z \in X : zgz^{-1} = g^{-1}\}.$$

We claim that $|J(g)| \leq |C_G(g)|$. The map $J(g) \to C_G(g)$, $z \mapsto gz$, is well-defined, as

$$(gz)g(gz)^{-1} = g(zgz^{-1})g^{-1} = g^{-1} \in C_G(g).$$

It is injective, as $gz = gz_1$ implies $z = z_1$.

Let $J = \{(g,z) \in G \times X : zgz^{-1} = g^{-1}\}$. Since $X \times X \to J$, $(y,z) \mapsto (yz,z)$, is well-defined (since $z(yz)z^{-1} = zy = (yz)^{-1}$) and it is trivially injective,

$$|X|^2 \leq |J| = \sum_{(g,z)\in J} 1 \leq \sum_{g\in G} |J(g)| \leq \sum_{g \in G} |C_G(g)| = k|G|,$$

where k is the number of conjugacy classes of G, as $(g,z) \in J$ if and only if $z \in J(g)$. Thus $|G| \leq kn^2$, as

$$\left(\frac{|G|}{|C_G(x)|}\right)^2 = |X|^2 = \frac{|G|^2}{n^2} \leq k|G|.$$

Claim. There exists a non-trivial conjugacy class with $\leq 2n^2$ elements.

Assume that the claim is not true. Let $C_1, \dots, C_k$ be the conjugacy classes of G, where $C_1 = \{1\}$ and $|C_i| > 2n^2$ for all $i \in \{2, \dots, k\}$. Then

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

a contradiction.

Claim. There exists a subgroup H of G such that $(G : H) \leq 2n^2$.

Let C be a conjugacy class of G such that $|C| \leq 2n^2$. Let $g \in C$. Then $H = C_G(g)$ is a subgroup of G such that $(G : H) \leq 2n^2$.

§ 7.4. Frobenius's reciprocity. We now present a very quick version of Frobenius' reciprocity theorem. We first define the restriction of class functions.

7.8. Definition. Let G be a finite group and $f\colon G \to \mathbb{C}$ be a map. For a subgroup H of G, the **restriction** of f to H is the map $\mathrm{Res}_H^G = f|_H\colon H \to \mathbb{C}$, $h \mapsto f(h)$.

7.9. Exercise. Let G be a finite group. Prove that the map

$$\mathrm{Res}_H^G\colon \mathrm{ClassFun}(G) \to \mathrm{ClassFun}(H), \quad f \mapsto \mathrm{Res}_H^G(f),$$

is a well-defined linear map.

One important property is the following:

7.10. Exercise. Let G be a finite group, H a subgroup of G and $\chi \in \mathrm{Char}(G)$. Prove that $\mathrm{Res}_H^G(\chi) \in \mathrm{Char}(H)$.

We now define induction. Let G be a finite group and H be a subgroup of G. If $f\colon H\to\mathbb{C}$ is a map, then

$$f^0(x)=\begin{cases}f(x) & \text{if } x\in H,\\ 0 & \text{otherwise.}\end{cases}$$

It is an exercise to prove that the map $f\mapsto f^0$ is linear.

7.11. Definition. Let G be a finite group and H be a subgroup of G. Let $f\colon H\to\mathbb{C}$ be a map. The **induction** of f to G is the map

$$g\mapsto \operatorname{Ind}_H^G f(g)=\frac{1}{|H|}\sum_{x\in G} f^0(x^{-1}gx).$$

7.12. Exercise. Let G be a finite group. Prove that the map

$$\operatorname{Ind}_H^G\colon \operatorname{ClassFun}(H)\to\operatorname{ClassFun}(G),\quad f\mapsto \operatorname{Ind}_H^G(f),$$

is a well-defined linear map.

Before proving that the induction of a character is a character, we mention the following crucial property:

7.13. Theorem (Frobenius' reciprocity). *Let G be a finite group and H be a subgroup of G. If $a\in\operatorname{ClassFun}(H)$ and $b\in\operatorname{ClassFun}(G)$, then*

$$\langle \operatorname{Ind}_H^G a,b\rangle=\langle a,\operatorname{Res}_H^G b\rangle\quad\textit{and}\quad \langle \operatorname{Res}_H^G a,b\rangle=\langle a,\operatorname{Ind}_H^G b\rangle.$$

Proof. We only need to prove the first equality. We compute

$$\langle \operatorname{Ind}_H^G a,b\rangle=\frac{1}{|G|}\sum_{x\in G}\operatorname{Ind}_H^G a(x)\overline{b(x)}=\frac{1}{|G|}\frac{1}{|H|}\sum_{x,y\in G}a^0(y^{-1}xy)\overline{b(x)}. \tag{7.1}$$

Setting $h=y^{-1}xy$, we can write (7.1) as

$$\begin{aligned}\langle \operatorname{Ind}_H^G a,b\rangle&=\frac{1}{|G|}\frac{1}{|H|}\sum_{y\in G}\sum_{h\in H}a(h)\overline{b(yhy^{-1})}\\&=\frac{1}{|G|}\frac{1}{|H|}\sum_{y\in G}\sum_{h\in H}a(h)\overline{b(h)}\\&=\frac{1}{|G|}\sum_{y\in G}\langle a,\operatorname{Res}_H^G b\rangle.\end{aligned}$$

□

7.14. Corollary. *Let G be a finite group and H be a subgroup of G. Let $\chi\in\operatorname{Char}(H)$ be such that $\chi(1)=n$. Then $\operatorname{Ind}_H^G\chi\in\operatorname{Char}(G)$ and has degree $n(G:H)$.*

Proof. It is enough to show that each $m_\psi=\langle\operatorname{Ind}_H^G\chi,\psi\rangle\in\mathbb{Z}_{\geq 0}$ for all $\psi\in\operatorname{Irr}(G)$. Let $\psi\in\operatorname{Irr}(G)$. By Frobenius' reciprocity theorem,

$$m_\psi=\langle\operatorname{Ind}_H^G\chi,\psi\rangle=\langle\chi,\operatorname{Res}_H^G\psi\rangle\in\mathbb{Z}_{\geq 0}$$

because both χ and $\operatorname{Res}_H^G\psi$ are characters of H. In fact, let $\operatorname{Irr}(H)=\{\theta_1,\dots,\theta_k\}$. Since $\chi\in\operatorname{ClassFun}(H)$ and $\operatorname{Res}_H^G\in\operatorname{ClassFun}(H)$, there are non-negative integers $a_1,\dots,a_k$ and

$b_1, \dots, b_k$ such that $\chi = \sum_{i=1}^k a_i\theta_i$ and $\operatorname{Res}_H^G \psi = \sum_{j=1}^k b_j\theta_j$. Then

$$\langle \chi, \operatorname{Res}_H^G \psi\rangle = \sum_{i=1}^k \sum_{j=1}^k a_i b_j \langle \theta_i, \theta_j\rangle = \sum_{i=1}^k a_i b_i \in \mathbb{Z}_{\geq 0}.$$

Therefore

$$\operatorname{Ind}_H^G \chi = \sum_{\psi \in \operatorname{Irr}(G)} m_\psi \psi \in \operatorname{Char}(G).$$

In particular,

$$\left(\operatorname{Ind}_H^G \chi\right)(1) = \frac{1}{|H|}\sum_{x\in G} \chi^0(1) = \frac{1}{|H|}|G|\chi(1) = \chi(1)(G:H). \qquad \square$$

7.15. Exercise. Let G be a finite group and χ_1 be the trivial character. If $H = \{1\}$, compute $\operatorname{Ind}_H^G \chi_1$.

7.16. Exercise. Let $G = \mathbb{S}_3$ and $H = \langle (12)\rangle$. Let $\varphi = \operatorname{sign}|_H$ be the restriction sign homomorphism to the subgroup H. Compute $\operatorname{Ind}_H^G \varphi$.

There are some useful properties that are easy to show.

7.17. Exercise. Let G be a finite group, H be a subgroup of G, $a \in \operatorname{ClassFun}(H)$ and $b \in \operatorname{ClassFun}(G)$. Prove that

$$\operatorname{Ind}_H^G((\operatorname{Res}_H^G b)a) = b(\operatorname{Ind}_H^G a).$$

7.18. Exercise (Transitivity of induction). Let G be a finite group, $H \subseteq K$ be subgroups of G and $a \in \operatorname{ClassFun}(H)$. Prove that

$$\operatorname{Ind}_K^G \operatorname{Ind}_H^K a = \operatorname{Ind}_H^G a.$$

7.19. Exercise. Let G be a finite group, H be a subgroup of G and $t_1, \dots, t_k$ be a transversal of H in G. Prove that

$$(\operatorname{Ind}_H^G \alpha)(g) = \sum_{i=1}^k \alpha^0(t_i^{-1} g t_i)$$

for all $\alpha \in \operatorname{ClassFun}(H)$.

7.20. Exercise. Let G be a finite group, H be a normal subgroup and χ be the trivial character of H. Prove that $\operatorname{Ind}_H^G \chi$ is the character of the representation induced by the action of G on G/H by left multiplication.

8. Lecture: Week 8

§ 8.1. The correspondence theorem. Let N be a normal subgroup of G and

$$\pi\colon G \to G/N,\quad g \mapsto gN,$$

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

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

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

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

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

is a normal subgroup of G.

Proof. Let $\rho\colon G \to \mathbf{GL}_n(\mathbb{C})$ be a representation with character χ. Then $\ker\rho \subseteq \ker\chi$, as $\rho_g = \mathrm{id}$ implies $\chi(g) = \operatorname{trace}(\rho_g) = n = \chi(1)$.

We claim that $\ker\chi \subseteq \ker\rho$. If $g \in G$ is such that $\chi(g) = \chi(1)$, since ρ_g is diagonalizable, there exist eigenvalues $\lambda_1, \dots, \lambda_n \in \mathbb{C}$ such that

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

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

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

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

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

that maps irreducible characters to irreducible characters.

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

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

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

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

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

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

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

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

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

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

Thus

$$\begin{aligned}\chi \text{ is irreducible } &\iff \rho \text{ is irreducible}\\ &\iff \widetilde{\rho} \text{ is irreducible } \iff \widetilde{\chi} \text{ is irreducible .}\end{aligned}$$ □

8.3. Example. Let $G = \mathbb{S}_4$ and $N = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$. We know that N is normal in G and that $G/N = \langle a, b\rangle \simeq \mathbb{S}_3$, where $a = (123)N$ and $b = (12)N$. The character table of G/N is

	N	$(12)N$	$(123)N$
$\widetilde{\chi}_1$	1	1	1
$\widetilde{\chi}_2$	1	-1	1
$\widetilde{\chi}_3$	2	0	-1

For each $i \in \{1, 2, 3\}$ we compute the lifting χ_i to G of the character $\widetilde{\chi}_i$ of G/N. Since $(12)(34) \in N$ and $(13)(1234) = (12)(34) \in N$,

$$\chi((12)(34)) = \widetilde{\chi}(N), \quad \chi((1234)) = \widetilde{\chi}((13)N) = \widetilde{\chi}((12)N).$$

Since the characters $\widetilde{\chi}_i$ are irreducibles, the liftings χ_i are also irreducibles. With this process we obtain the following irreducible characters of G:

	1	(12)	(123)	(12)(34)	(1234)
χ_1	1	1	1	1	1
χ_2	1	-1	1	1	-1
χ_3	2	0	-1	2	0

Theorem 8.2 has some unexpected applications. For example, the following exercise is elementary but tricky. A simpler solution uses the second orthogonality relation and Theorem 8.2.

8.4. Exercise. Let G be a finite group, $g \in G$ and N be a normal subgroup of G. Prove that $|C_{G/N}(gN)| \leq |C_G(g)|$.

The character table of a group can be used to find the lattice of normal subgroups. In particular, the character table detects simple groups.

8.5. Lemma. *Let G be a finite group and let $g, h \in G$. Then g and h are conjugate if and only if $\chi(g) = \chi(h)$ for all $\chi \in \mathrm{Char}(G)$.*

Proof. If g and h are conjugate, then $\chi(g) = \chi(h)$, as characters are class functions of G. Conversely, if $\chi(g) = \chi(h)$ for all $\chi \in \mathrm{Char}(G)$, then $f(g) = f(h)$ for all class function f of G, as characters G generate the space of class functions of G. In particular, $\delta(g) = \delta(h)$, where

$$\delta(x) = \begin{cases} 1 & \text{if } x \text{ and } g \text{ are conjugate,}\\ 0 & \text{otherwise.}\end{cases}$$

This implies that g and h are conjugate. □

As a consequence, we get that

$$\bigcap_{\chi \in \mathrm{Irr}(G)} \ker \chi = \{1\}. \tag{8.1}$$

Indeed, if $g \in \ker \chi$ for all $\chi \in \mathrm{Irr}(G)$, then $g = 1$ since the lemma implies that g and 1 are conjugate because $\chi(g) = \chi(1)$ for all $\chi \in \mathrm{Irr}(G)$.

8.6. Proposition. *Let G be a finite group. If N is a normal subgroup of G, then there exist characters $\chi_1,\dots,\chi_k\in\mathrm{Irr}(G)$ such that*

$$N=\bigcap_{i=1}^{k}\ker\chi_i.$$

Proof. Apply the previous remark to the group G/N to obtain that

$$\bigcap_{\widetilde{\chi}\in\mathrm{Irr}(G/N)}\ker\widetilde{\chi}=\{N\}.$$

Assume that $\mathrm{Irr}(G/N)=\{\widetilde{\chi}_1,\dots,\widetilde{\chi}_k\}$. We lift the irreducible characters of G/N to G to obtain (some) irreducible characters $\chi_1,\dots,\chi_k$ of G such that

$$N\subseteq\ker\chi_1\cap\cdots\cap\ker\chi_k.$$

If $g\in\ker\chi_i$ for all $i\in\{1,\dots,k\}$, then

$$\widetilde{\chi}_i(N)=\chi_i(1)=\chi_i(g)=\widetilde{\chi}_i(gN)$$

for all $i\in\{1,\dots,k\}$. This implies that

$$gN\in\bigcap_{i=1}^{k}\ker\widetilde{\chi}_i=\{N\},$$

that is $g\in N$. □

Recall that a non-trivial group is **simple** if it contains no non-trivial normal proper subgroups. Examples of simple groups are cyclic groups of prime order and the alternating groups $\mathbb{A}_n$ for $n\geq 5$. As a corollary of Proposition 8.6, we can use the character table to detect simple groups.

8.7. Proposition. *Let G be a finite group. Then G is not simple if and only if there exists a non-trivial irreducible character χ such that $\chi(g)=\chi(1)$ for some $g\in G\setminus\{1\}$.*

Proof. If G is not simple, there exists a normal subgroup N of G such that $N\neq G$ and $N\neq\{1\}$. By Proposition 8.6, there exist characters $\chi_1,\dots,\chi_k\in\mathrm{Irr}(G)$ such that $N=\ker\chi_1\cap\cdots\cap\ker\chi_k$. In particular, there exists a non-trivial character χ_i such that $\ker\chi_i\neq\{1\}$. Thus there exists $g\in G\setminus\{1\}$ such that $\chi_i(g)=\chi_i(1)$.

Assume now that there exists a non-trivial irreducible character χ such that $\chi(g)=\chi(1)$ for some $g\in G\setminus\{1\}$. In particular, $g\in\ker\chi$ and hence $\ker\chi\neq\{1\}$. Since χ is non-trivial, $\ker\chi\neq G$. Thus $\ker\chi$ is a proper non-trivial normal subgroup of G. □

8.8. Example. If there exists a group G with a character table of the form

χ_1	1	1	1	1	1	1
χ_2	1	1	1	-1	1	-1
χ_3	1	1	1	1	-1	-1
χ_4	1	1	1	-1	-1	1
χ_5	2	-2	2	0	0	0
χ_6	8	0	-1	0	0	0

then G cannot be simple. Note that such a group G would have order $\sum_{i=1}^{6}\chi_i(1)^2=72$. Mathieu's group M_9 has precisely this character table!

8.9. EXAMPLE. Let $\alpha = \frac{1}{2}(-1+\sqrt{7}i)$. If there exists a group G with a character table of the form

χ_1	1	1	1	1	1	1
χ_2	7	-1	-1	1	0	0
χ_3	8	0	0	-1	1	1
χ_4	3	-1	1	0	α	$\overline{\alpha}$
χ_5	3	-1	1	0	$\overline{\alpha}$	α
χ_6	6	2	0	0	0	0

then G is simple. Note that such a group G would have order $\sum_{i=1}^{6} \chi_i(1)^2 = 168$. The group

$$\mathbf{PSL}_2(7) = \mathbf{SL}_2(7)/Z(\mathbf{SL}_2(7))$$

is a simple group that has precisely this character table!

§ 8.2. Frobenius' groups.

If p is a prime number, then the units $(\mathbb{Z}/p)^\times$ of $\mathbb{Z}/p$ form a multiplicative group. Moreover, $(\mathbb{Z}/p)^\times$ is cyclic of order $p-1$.

Let

$$G = \left\{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} : x \in (\mathbb{Z}/p)^\times,\ y \in \mathbb{Z}/p \right\}.$$

Then G is a group with the usual matrix multiplication and $|G| = p(p-1)$. Let p and q be prime numbers such that q divides $p-1$, $z \in \mathbb{Z}$ be an element of multiplicative order q modulo p and

$$a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} z & 1 \\ 0 & 1 \end{pmatrix}, \quad H = \langle a, b \rangle.$$

A direct calculation shows that

$$a^p = b^q = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad bab^{-1} = \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} = a^z. \tag{8.2}$$

Every element of H is of the form $a^i b^j$ for $i \in \{0, \dots, p-1\}$ and $j \in \{0, \dots, q-1\}$. Thus $|H| = pq$. Using (8.2) we can compute the multiplication table of G.

8.10. EXERCISE. Let p and q be prime numbers such that q divides $p-1$. Let $u, v \in \mathbb{Z}$ be elements of order q modulo p. Prove that

$$\langle a, b : a^p = b^q = 1, bab^{-1} = a^u \rangle \simeq \langle a, b : a^p = b^q = 1, bab^{-1} = a^v \rangle.$$

The group

$$\langle a, b : a^p = b^q = 1, bab^{-1} = a^u \rangle,$$

where $u \in \mathbb{Z}$ has order q modulo p, is a particular case of a **Frobenius group**.

8.11. EXERCISE. Let p and q be prime numbers such that $p > q$. Let G be a group of order pq. Then either G is abelian or q divides $p-1$ and

$$G \simeq \langle a, b : a^p = b^q = 1, bab^{-1} = a^u \rangle$$

for some $u \in \mathbb{Z}$ of order q modulo p.

Using Exercise 8.11, we can prove, for example, that every group of order 15 is abelian.

8.12. Definition. We say that a finite group G is a **Frobenius group** if G has a non-trivial proper subgroup H such that $H \cap xHx^{-1} = \{1\}$ for all $x \in G \setminus H$. In this case, the subgroup H is called a **Frobenius complement**.

A subgroup H such that $gHg^{-1} \cap H = \{1\}$ for all $g \notin H$ is called a **malnormal** subgroup. Note that if H is malnormal, then $N_G(H) = H$.

8.13. Exercise. Let G be a group and H be a subgroup of G. Prove that the following statements are equivalent:

1) H is malnormal.
2) The action of H on $G/H \setminus \{H\}$ by left multiplication is free.
3) Any $g \in G \setminus \{1\}$ has zero or one fixed point on G/H.

For any group G, the subgroups $\{1\}$ and G are malnormal in G. Moreover, they are the only subgroups of G that are both normal and malnormal

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

1) If H is malnormal in G, then gHg^{-1} is malnormal in G for all $g \in G$.
2) If H is malnormal in G and K is malnormal in H, then K is malnormal in G.
3) The intersection of malnormal subgroups is malnormal.
4) If H is malnormal in G and S is a subgroup of G, then $H \cap S$ is malnormal in S.

8.15. Example. Let

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in \mathbb{R}^\times, b \in \mathbb{R} \right\} \quad \text{and} \quad H = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} : a \in \mathbb{R}^\times \right\} \subseteq G.$$

Let $g = \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \in G \setminus H$. Then $y \neq 0$. Since

$$g \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} g^{-1} = \begin{pmatrix} a & -ay+y \\ 0 & 1 \end{pmatrix},$$

it follows that the subgroup H is malnormal in G.

8.16. Exercise. Let G be a group and H be a non-trivial subgroup of G. Prove that if $Z(G) \neq \{1\}$, then H is not malnormal in G.

8.17. Bonus exercise. Let G be a group with no 2-torsion that contains a normal infinite cyclic group. Prove that G cannot contain a non-trivial proper malnormal subgroup.

8.18. Example. Let G be a finite group and $P \in \mathrm{Syl}_p(G)$ be such that $|P| = p$ and $N_G(P) = P$. Then G is a Frobenius group with complement P.

The previous example shows that $\mathbb{A}_4$ is a Frobenius group with complement $\langle (123) \rangle$. Another situation where the example applies is the dihedral group

$$\mathbb{D}_{2n+1} = \langle r, s : r^{2n+1} = s^2 = 1, srs = r^{-1} \rangle$$

of order $2(2n+1)$. It follows that $\mathbb{D}_{2n+1}$ is a Frobenius group with complement $\langle s \rangle$.

8.19. THEOREM (Frobenius). *Let G be a Frobenius group with complement H. Then*

$$N = \left(G \setminus \bigcup_{x \in G} xHx^{-1} \right) \cup \{1\}$$

is a normal subgroup of G.

PROOF. Let 1_H and 1_G be the trivial characters of H and G, respectively. For each $\chi \in \mathrm{Irr}(H)$, $\chi \neq 1_H$, let $\alpha = \chi - \chi(1)1_H \in \mathrm{ClassFun}(H)$, where 1_H denotes the trivial character of H.

We claim that $\mathrm{Res}_H^G \mathrm{Ind}_H^G \alpha = \alpha$. First, $\mathrm{Ind}_H^G \alpha(1) = \alpha(1) = 0$. If $h \in H \setminus \{1\}$, then

$$\mathrm{Ind}_H^G \alpha(h) = \frac{1}{|H|} \sum_{\substack{x \in G \\ x^{-1}hx \in H}} \alpha(x^{-1}hx) = \frac{1}{|H|} \sum_{x \in H} \alpha(h) = \alpha(h),$$

since, if $x \notin H$, then $x^{-1}hx \in H$ implies that $h \in H \cap xHx^{-1} = \{1\}$.

By Frobenius' reciprocity and the definition of α,

$$\langle \mathrm{Ind}_H^G \alpha, \mathrm{Ind}_H^G \alpha \rangle = \langle \alpha, \mathrm{Res}_H^G \mathrm{Ind}_H^G \alpha \rangle = \langle \alpha, \alpha \rangle = 1 + \chi(1)^2. \tag{8.3}$$

Again, by Frobenius' reciprocity,

$$\langle \mathrm{Ind}_H^G \alpha, 1_G \rangle = \langle \alpha, \mathrm{Res}_H^G 1_G \rangle = \langle \alpha, 1_H \rangle = \langle \chi - \chi(1)1_H, 1_H \rangle = -\chi(1),$$

where 1_G is the trivial character of G. If we write

$$\mathrm{Ind}_H^G \alpha = \sum_{\eta \in \mathrm{Irr}(G)} \langle \mathrm{Ind}_H^G \alpha, \eta \rangle \eta = \langle \mathrm{Ind}_H^G \alpha, 1_G \rangle 1_G + \underbrace{\sum_{\substack{1_G \neq \eta \\ \eta \in \mathrm{Irr}(G)}} \langle \mathrm{Ind}_H^G \alpha, \eta \rangle \eta}_{\phi},$$

then $\mathrm{Ind}_H^G \alpha = -\chi(1)1_G + \phi$, where ϕ is a linear combination of non-trivial irreducible characters of G. We compute

$$1 + \chi(1)^2 = \langle \mathrm{Ind}_H^G \alpha, \mathrm{Ind}_H^G \alpha \rangle = \langle \phi - \chi(1)1_G, \phi - \chi(1)1_G \rangle = \langle \phi, \phi \rangle + \chi(1)^2$$

and hence $\langle \phi, \phi \rangle = 1$.

CLAIM. If $\eta \in \mathrm{Irr}(G)$ is such that $\eta \neq 1_G$, then $\langle \mathrm{Ind}_H^G \alpha, \eta \rangle \in \mathbb{Z}$.

By Frobenius' reciprocity, $\langle \mathrm{Ind}_H^G \alpha, \eta \rangle = \langle \alpha, \mathrm{Res}_H^G \eta \rangle$. If we decompose $\mathrm{Res}_H^G \eta$ into irreducibles of H, say

$$\mathrm{Res}_H^G \eta = m_1 1_H + m_2 \chi + m_3 \theta_3 + \cdots + m_t \theta_t$$

for some $m_1, m_2, \dots, m_t \geq 0$, then, since

$$\langle \alpha, 1_H \rangle = \langle \chi - \chi(1)1_H, 1_H \rangle = -\chi(1), \qquad \langle \alpha, \chi \rangle = \langle \chi - \chi(1)1_H, \chi \rangle = 1,$$

and

$$\langle \alpha, \theta_j \rangle = \langle \chi - \chi(1)1_H, \theta_j \rangle = 0$$

for all $j \in \{3, \dots, t\}$, we conclude that

$$\langle \mathrm{Ind}_H^G \alpha, \eta \rangle = -m_1 \chi(1) + m_2 \in \mathbb{Z}.$$

CLAIM. $\phi \in \mathrm{Irr}(G)$.

Since $\langle \operatorname{Ind}_H^G \alpha, \eta\rangle \in \mathbb{Z}$ for all $\eta \in \operatorname{Irr}(G)$ such that $\eta \neq 1_G$ and

$$1 = \langle \phi, \phi\rangle = \sum_{\substack{\eta,\theta\in\operatorname{Irr}(G)\\ \eta,\theta\neq 1_G}} \langle \operatorname{Ind}_H^G \alpha, \eta\rangle\langle \operatorname{Ind}_H^G \alpha, \theta\rangle\langle \eta, \theta\rangle = \sum_{\substack{\eta\neq 1_G\\ \eta\in\operatorname{Irr}(G)}} \langle \operatorname{Ind}_H^G \alpha, \eta\rangle^2,$$

there is a unique $\eta \in \operatorname{Irr}(G)$ such that $\langle \operatorname{Ind}_H^G \alpha, \eta\rangle^2 = 1$ and all the other products are zero, that is $\phi = \pm\eta$ for some $\eta \in \operatorname{Irr}(G)$. Since

$$\chi - \chi(1)1_H = \alpha = \operatorname{Res}_H^G \operatorname{Ind}_H^G \alpha = \operatorname{Res}_H^G(\phi - \chi(1)1_G) = \operatorname{Res}_H^G \phi - \chi(1)1_H,$$

it follows that $\phi(1) = \operatorname{Res}_H^G \phi(1) = \chi(1) \in \mathbb{Z}_{\geq 1}$. Thus $\phi \in \operatorname{Irr}(G)$.

We have proved that if $\chi \in \operatorname{Irr}(H)$ is such that $\chi \neq 1_H$, then there exists $\phi_\chi \in \operatorname{Irr}(G)$ such that $\operatorname{Res}_H^G(\phi_\chi) = \chi$.

We prove that N is equal to

$$M = \bigcap_{\substack{\chi\in\operatorname{Irr}(H)\\ \chi\neq 1_H}} \ker \phi_\chi.$$

We first prove that $N \subseteq M$. Let $n \in N \setminus \{1\}$ and $\chi \in \operatorname{Irr}(H) \setminus \{1_H\}$. Since n does not belong to a conjugate of H,

$$\operatorname{Ind}_H^G \alpha(n) = \frac{1}{|H|} \sum_{\substack{x\in G\\ x^{-1}nx\in H}} \alpha(x^{-1}nx) = 0,$$

as $n \in N$ implies that the set $\{x \in G : x^{-1}nx \in H\}$ is empty. Since

$$0 = \operatorname{Ind}_H^G \alpha(n) = \phi_\chi(n) - \chi(1) = \phi_\chi(n) - \phi_\chi(1),$$

we conclude that $n \in \ker \phi_\chi$.

We now prove that $M \subseteq N$. Let $h \in M \cap H$ and $\chi \in \operatorname{Irr}(H) \setminus \{1_H\}$. Then

$$\phi_\chi(h) - \chi(1) = \operatorname{Ind}_H^G \alpha(h) = \alpha(h) = \chi(h) - \chi(1),$$

and $h \in \ker \chi$, as

$$\chi(h) = \phi_\chi(h) = \phi_\chi(1) = \chi(1).$$

Therefore

$$h \in \bigcap_{\chi\in\operatorname{Irr}(H)} \ker \chi = \{1\}.$$

By (8.1), the kernels of irreducible characters have trivial intersection. We now prove that $M \cap xHx^{-1} = \{1\}$ for all $x \in G$. Let $x \in G$ and $m \in M \cap xHx^{-1}$. Since $m = xhx^{-1}$ for some $h \in H$, $x^{-1}mx \in H \cap M = \{1\}$. This implies that $m = 1$. □

There is no proof of Frobenius' theorem that is independent of character theory. Purely group-theoretic proofs exist in cases where the Frobenius complement has even order or is solvable; see [**19**, Remark 16.2]. The Feit–Thompson theorem (which relies heavily on character theory and is significantly more difficult than Frobenius' theorem) implies that these two cases cover all possibilities.

In 2013, Terence Tao discovered an alternative Fourier-analytic proof of Frobenius' theorem, though it resembles the original character-theoretic approach.

8.20. Definition. Let G be a Frobenius group. The normal subgroup N of Frobenius' theorem is called the **Frobenius kernel**.

8.21. Corollary. *Let G be a Frobenius group with complement H. Then there exists a normal subgroup N of G such that $G = HN$ and $H \cap N = \{1\}$.*

Proof. Frobenius' theorem yields the subgroup N. Since $H \cap gHg^{-1} = \{1\}$ for all $g \in G \setminus H$, it follows that $N_G(H) = H$. It follows that H has $(G : H)$ conjugates. Let

$$N = \left(G \setminus \bigcup_{x \in G} xHx^{-1} \right) \cup \{1\}.$$

Then $|N| = |G| - (G : H)(|H| - 1) = (G : H)$. Since, moreover, $N \cap H = \{1\}$, we conclude that

$$|HN| = |N||H|/|H \cap N| = |N||H| = |G|.$$

Therefore $G = NH$. □

In his doctoral thesis Thompson proved the following result, conjectured by Frobenius.

8.22. Theorem (Thompson). *Let G be a Frobenius group. If N is the Frobenius kernel, then N is nilpotent.*

See [**22**, Theorem 6.24] for the proof.

9. Lecture: Week 9

§ 9.1. The Cameron–Cohen theorem (again). In this section, we use Frobenius' theorem to strengthen the Cameron–Cohen theorem on derangements (Theorem 6.29). To do so, we first require an alternative version of Frobenius' theorem.

9.1. Corollary (Frobenius). *Let G be a group acting transitively on a finite set X. Assume that each $g \in G \setminus \{1\}$ fixes at most one element of X. The set N formed by the identity and the derangements of G is a normal subgroup of G.*

Proof. Let $x \in X$ and $H = G_x$. We claim that if $g \in G \setminus H$, then $H \cap gHg^{-1} = \{1\}$. If $h \in H \cap gHg^{-1}$, then $h \cdot x = x$ and $(g^{-1}hg) \cdot x = x$. Since $g \cdot x \neq x$, h fixes two elements of X. Thus $h = 1$, as every non-trivial element fixes at most one element of X.

By Theorem 8.19,

$$N = \left(G \setminus \bigcup_{g \in G} gHg^{-1} \right) \cup \{1\}$$

is a subgroup of G. Let us compute the elements of N. If $h \in \bigcup_{g \in G} gHg^{-1}$, then there exists $g \in G$ such that $g^{-1}hg \in H$, that is $(g^{-1}hg) \cdot x = x$; equivalently, $h \in G_{g \cdot x}$. Therefore, the non-identity elements of N are the elements of G moving every element of X. $\square$

9.2. Example. Let F be a finite field and G be the group of maps $f \colon F \to F$ of the form $f(x) = ax + b$, $a, b \in F$ with $a \neq 0$. The group G acts on F and every $f \neq \mathrm{id}$ fixes at most one element of F, as

$$x = f(x) = ax + b \implies a \neq 1 \text{ and } x = b/(1-a).$$

In this case, $N = \{f : f(x) = x + b\,, b \in F\}$ is a subgroup of G.

9.3. Exercise. Prove that Theorem 8.19 can be obtained from Corollary 9.1.

Using Frobenius' theorem (Corollary 9.1), we can present a refinement of the Cameron–Cohen theorem.

9.4. Theorem (Cameron–Cohen). *Let $G \leq \mathbb{S}_n$ be a transitive subgroup. If n is not the power of a prime number, then $c_0 > \frac{1}{n}$.*

Proof. Let us go back to the proof of Theorem 6.29. Assume that $c_0 = 1/n$. Then

$$\frac{1}{|G|} \sum_{g \in G} (\chi(g)^2 - (n+1)\chi(g) + n) = 1$$

and hence $\frac{1}{|G|} \sum_{g \in G} \chi(g)^2 = 2$. Moreover, since

$$\frac{1}{|G|} \sum_{g \in G_0} (\chi(g) - 1)(\chi(n) - n) + \frac{1}{|G|} \sum_{g \in G \setminus G_0} (\chi(g) - 1)(\chi(g) - n) = 1,$$

it follows that

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

Hence $(\chi(g) - 1)(\chi(g) - n) = 0$ for all $g \in G \setminus G_0$.

By Corollary 9.1, the subset $N = G_0 \cup \{\mathrm{id}\}$ is a normal subgroup of G. Moreover, $G = N \rtimes H$ for some subgroup H of G of order n. Since $n = |H| = |N| - 1$, H acts freely and transitively on $N \setminus \{1\}$.

We claim that N is a p-group for some prime number p. Let $n, m \in N \setminus \{1\}$. Since H is transitive on $N \setminus \{1\}$, there exists $h \in H$ such that $h \cdot n = m$. Then

$$|n| = |h \cdot n| = |m|,$$

since for each $h \in H$, the map $x \mapsto h \cdot x$ is an automorphism of N. Thus every two elements of $N \setminus \{1\}$ have the same order. Let p be a prime divisor of $|N|$. By Cauchy's theorem, there exists $n \in N$ such that $|n| = p$. Since all non-trivial elements of N have the same order, N is a p-group. Therefore $n = |N|$ is a power of a prime. $\square$

9.5. Exercise. Let G be the group of matrices of the form $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ where $a, b \in \mathbb{Z}/5$ and $a \neq 0$. Then $|G| = 20$. Let

$$h = \begin{pmatrix} 2 & \\ & 1 \end{pmatrix}, \quad k = \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}.$$

A direct calculation shows that $h^4 = 1$, $k^5 = 1$ and $hkh^{-1} = k^2$. Let $H = \langle h \rangle$ and $K = \langle k \rangle$. Prove the following statements:

1) Prove that $G = K \rtimes H$.

2) Find the conjugacy classes of G:

Size	1	4	5	5	5
Representative	1	k	h	h^2	h^3

3) Prove that G/K is cyclic of order four.

4) Prove that $[G, G] = K$.

5) Use Theorem 8.2 on G/K to find the degree-one characters of G.

6) Let $\chi \in \mathrm{Irr}(K)$ be such that $\chi(k) = \exp(2\pi i/5)$. Prove that $\mathrm{Ind}_K^G \chi \in \mathrm{Irr}(G)$.

10. Lecture: Week 10

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

$$(\rho_\sigma)_{ij} = \begin{cases} 1 & \text{if } i = \sigma(j), \\ 0 & \text{otherwise.} \end{cases} \tag{10.1}$$

10.1. Lemma. *For $n \geq 1$ let $\rho\colon \mathbb{S}_n \to \mathbf{GL}_n(C)$ be the natural representation of the symmetric group. If $A \in \mathbb{C}^{n\times n}$ and $\sigma \in \mathbb{S}_n$, then*

$$A_{ij} = (\rho_\sigma A)_{\sigma(i)j} = (A\rho_\sigma)_{i\sigma^{-1}(j)}$$

for all $i, j \in \{1, \dots, n\}$.

Proof. With (10.1) we compute:

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

10.2. Definition. Let G be a finite group. A character χ of G is said to be **real** if $\chi = \overline{\chi}$, that is $\chi(g) \in \mathbb{R}$ for all $g \in G$.

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

10.4. Definition. Let G be a group. A conjugacy class C of G is said to be **real** if for every $g \in C$ one has $g^{-1} \in C$.

We use the following notation: if G is a group and $C = \{xgx^{-1} : x \in G\}$ is a conjugacy class of G, then $C^{-1} = \{xg^{-1}x^{-1} : x \in G\}$.

10.5. Theorem (Burnside). *Let G be a finite group. The number of real conjugacy classes equals the number of real irreducible characters.*

Proof. Let $C_1, \dots, C_r$ be the conjugacy classes of G and let $\chi_1, \dots, \chi_r$ be the irreducible characters of G. Let $\alpha, \beta \in \mathbb{S}_r$ be such that $\overline{\chi_i} = \chi_{\alpha(i)}$ and $C_i^{-1} = C_{\beta(i)}$ for all $i \in \{1, \dots, r\}$. Note that χ_i is real if and only if $\alpha(i) = i$ and that C_i is real if and only if $\beta(i) = i$. The number n of fixed points of α is equal to the number of real irreducible characters of G, and the number m of fixed points of β is equal to the number of real classes. Let $\rho\colon \mathbb{S}_r \to \mathbf{GL}_r(\mathbb{C})$ be the natural representation of $\mathbb{S}_r$, with character χ_ρ. Then $\chi_\rho(\alpha) = n$ and $\chi_\rho(\beta) = m$. We claim that $\operatorname{trace} \rho_\alpha = \operatorname{trace} \rho_\beta$. Let $X \in \mathbf{GL}(r, \mathbb{C})$ be the character matrix of G. By Lemma 10.1 and the fact that $\overline{\chi(g)} = \chi(g^{-1})$ for all $g \in G$,

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

Since X is invertible, $\rho_\alpha = X\rho_\beta X^{-1}$. Thus

$$n = \chi_\rho(\alpha) = \operatorname{trace} \rho_\alpha = \operatorname{trace} \rho_\beta = \chi_\rho(\beta) = m. \qquad \square$$

10.6. Corollary. *Let G be a finite group. Then $|G|$ is odd if and only if the only real $\chi \in \mathrm{Irr}(G)$ is the trivial character.*

PROOF. We first prove $\Longleftarrow$. If $|G|$ is even, there exists $g \in G$ of order two (Cauchy's theorem). The conjugacy class of g is real.

We now prove $\Longrightarrow$. Assume that G has a non-trivial real conjugacy class C. Let $g \in C$. We claim that G has an element of even order. Let $h \in G$ be such that $hgh^{-1} = g^{-1}$. Then $h^2 \in C_G(g)$, as $h^2gh^{-2} = g$. If $h \in \langle h^2 \rangle \subseteq C_G(g)$, then g has even order, as $g^{-1} = g$. If $h \notin \langle h^2 \rangle$, then h^2 does not generate $\langle h \rangle$. Hence h has even order, as $|h| \neq |h^2| = |h|/\gcd(|h|, 2)$, so $\gcd(|h|, 2) \neq 1$. $\square$

10.7. THEOREM (Burnside). *Let G be a finite group of odd order with r conjugacy classes. Then $r \equiv |G| \bmod 16$.*

PROOF. Since $|G|$ is odd, every non-trivial $\chi \in \mathrm{Irr}(G)$ is not real by the previous corollary. The irreducible characters of G are

$$\chi_1, \chi_2, \overline{\chi_2}, \dots, \chi_k, \overline{\chi_k}, \quad r = 1 + 2(k-1),$$

where χ_1 denotes the trivial character. For every $j \in \{2, \dots, k\}$ let $d_j = \chi_j(1)$. Since each d_j divides $|G|$ by Frobenius' theorem and $|G|$ is odd, every d_j is an odd number, say $d_j = 1 + 2m_j$. Thus

$$\begin{aligned} |G| &= 1 + \sum_{j=2}^{k} 2d_j^2 = 1 + \sum_{j=2}^{k} 2(2m_j+1)^2 \\ &= 1 + \sum_{j=2}^{k} 2(4m_j^2 + 4m_j + 1) = 1 + 2(k-1) + 8\sum_{j=2}^{k} m_j(m_j+1). \end{aligned}$$

Hence $|G| \equiv r \bmod 16$, as $r = 1 + 2k$ and every $m_j(m_j+1)$ is even. $\square$

10.8. EXERCISE. Prove that every group of order 15 is abelian.

11. Lecture: Week 11

§ 11.1. Clifford theory. We begin with a routine exercise.

11.1. Exercise. Let G be a finite group and N be a normal subgroup of G. Prove that G acts on $\mathrm{Irr}(N)$ via

$$(g\cdot\theta)(n)=\theta(g^{-1}ng),\quad g\in G,\theta\in\mathrm{Irr}(N),n\in N.$$

11.2. Exercise. Let G be a finite group and N be a normal subgroup of G. Let $\chi\in\mathrm{ClassFun}(G)$, $\theta\in\mathrm{ClassFun}(N)$ and $g\in G$. Prove that

$$\langle\mathrm{Res}_N^G\chi,g\cdot\theta\rangle=\langle\mathrm{Res}_N^G\chi,\theta\rangle.$$

Recall that every character χ of a finite group is uniquely a sum of irreducible characters. These are called the **irreducible constituents** of χ. The set of irreducible constituents of χ is the set

$$\{\eta\in\mathrm{Irr}(G):\langle\chi,\eta\rangle>0\}.$$

11.3. Theorem (Clifford). *Let G be a finite group and N be a normal subgroup of G. Let $\chi\in\mathrm{Irr}(G)$ and $\theta\in\mathrm{Irr}(N)$ be an irreducible constituent of $\mathrm{Res}_N^G\chi$. Then*

$$\mathrm{Res}_N^G\chi=e(\theta_1+\cdots+\theta_t),$$

where $\theta=\theta_1,\dots,\theta_t$ are the conjugates of θ in G, and e is a positive integer. In particular, all the constituents of $\mathrm{Res}_N^G\chi$ have the same degree.

Proof. Let $G\cdot\theta=\{\theta_1,\dots,\theta_t\}$ be the orbit of θ. For each $i\in\{1,\dots,t\}$,

$$\langle\mathrm{Res}_N^G\chi,\theta_i\rangle=\langle g_i\cdot\mathrm{Res}_H^G\chi,g_i\cdot\theta\rangle=\langle\mathrm{Res}_H^G\chi,\theta\rangle>0$$

since by assumption θ is an irreducible constituent of $\mathrm{Res}_N^G\chi$. Let $e=\langle\mathrm{Res}_N^G\chi,\theta\rangle$. Then

$$\mathrm{Res}_N^G\chi=e(\theta_1+\cdots+\theta_t)+\eta$$

for some $\eta=0$ or $\eta\in\mathrm{Char}(N)$. Since

$$e=\langle\mathrm{Res}_H^G\chi,\theta\rangle=\langle e(\theta_1+\cdots+\theta_t)+\eta,\theta\rangle=e\sum_{i=1}^t\langle\theta_i,\theta\rangle+\langle\eta,\theta\rangle=e+\langle\eta,\theta\rangle,$$

it follows that $\langle\eta,\theta\rangle=0$. By Frobenius' reciprocity, $\langle\chi,\mathrm{Ind}_N^G\theta\rangle=\langle\mathrm{Res}_N^G\chi,\theta\rangle=e$. Thus

$$\mathrm{Ind}_N^G\theta=e\chi+\lambda$$

for some $\lambda=0$ or $\lambda\in\mathrm{Char}(G)$. Since

$$e=\langle\chi,\mathrm{Ind}_N^G\theta\rangle=\langle\chi,e\chi+\lambda\rangle=e\langle\chi,\chi\rangle+\langle\chi,\lambda\rangle=e+\langle\chi,\lambda\rangle,$$

it follows that $\langle\chi,\lambda\rangle=0$.

Claim. $\mathrm{Res}_N^G\mathrm{Ind}_N^G\theta=t\frac{1}{|N|}\sum_{i=1}^t\theta_i$.

Let $n \in N$. For $i \in \{1, \dots, t\}$ let $x_i \in G$ be such that $x_i \cdot \theta = \theta_i$. Then

$$\begin{aligned}(\operatorname{Ind}_N^G \theta)(n) &= \frac{1}{|N|}\sum_{x\in G}\theta^0(x^{-1}nx)\\ &= \frac{1}{|N|}\sum_{x\in G}(x\cdot\theta)(n)\\ &= \frac{1}{|N|}\sum_{1=1}^{t} t(x_i\cdot\theta)(n)\\ &= \frac{t}{|N|}\sum_{1=1}^{t}\theta_i(n),\end{aligned}$$

where we have used that $n \in N$ and N is normal in G (because $x^{-1}nx \in N$ if and only if $n \in xNx^{-1} = N$).

Therefore

$$\begin{aligned}\frac{t}{|N|}(\theta_1 + \cdots + \theta_t) &= \operatorname{Res}_N^G \operatorname{Ind}_N^G \theta\\ &= \operatorname{Res}_N^G(e\chi + \lambda)\\ &= e \operatorname{Res}_N^G \chi + \operatorname{Res}_N^G \lambda\\ &= e^2(\theta_1 + \cdots + \theta_t) + e\eta + \operatorname{Res}_N^G \lambda.\end{aligned}$$

Taking inner product against η,

$$\frac{t}{|N|}\sum_{i=1}^{t}\langle\theta_i, \eta\rangle = e^2\sum_{i=1}^{t}\langle\theta_i,\eta\rangle + e\langle\eta,\eta\rangle + \langle\operatorname{Res}_N^G \lambda, \eta\rangle.$$

Since $\langle\theta_i, \eta\rangle = 0$ for all $i \in \{1, \dots, t\}$,

$$0 = e\langle\eta,\eta\rangle + \langle\operatorname{Res}_N^G \lambda, \eta\rangle. \tag{11.1}$$

We know that $e > 0$. Moreover, since $\eta \in \operatorname{Char}(N)$ and $\operatorname{Res}_N^G \lambda \in \operatorname{Char}(N)$, each term of the right hand side of (11.1) is non-negative, that is $\langle\eta,\eta\rangle \geq 0$ and $\langle\operatorname{Res}_N^G \lambda, \eta\rangle \geq 0$. Therefore $\langle\eta,\eta\rangle = 0$ and hence $\eta = 0$. □

The integer e in Theorem 11.3 is known as the **ramification index** of χ on N. In general, the number e is not easy to control.

11.4. Exercise. Let G be a finite group and N be a normal subgroup of G. Let $\chi \in \operatorname{Irr}(G)$ and θ be an irreducible constituent of $\operatorname{Res}_N^G \chi$. Prove that $\theta(1)$ divides $\chi(1)$.

Let G be a group and $\theta \in \operatorname{Irr}(G)$. The set

$$I_G(\theta) = \{g \in G : g \cdot \theta = \theta\}$$

is a subgroup of G and is called **inertia subgroup** of θ in G. Note that the inertia subgroup is the stabilizer of the action of G on characters by conjugation (see of Exercise 11.1). In particular, θ has $(G : I_G(\theta))$ conjugates.

11.5. Theorem (Clifford correspondence). *Let G be a finite group and N be a normal subgroup of G. Let $\theta \in \operatorname{Irr}(N)$ and $I = I_G(\theta)$. Then the map*

$$\{\psi \in \operatorname{Irr}(I) : \langle \operatorname{Res}_N^I \psi, \theta\rangle > 0\} \to \{\chi \in \operatorname{Irr}(G) : \langle \operatorname{Res}_N^G \chi, \theta\rangle > 0\}, \quad \psi \mapsto \operatorname{Ind}_I^G \psi,$$

is bijective. Moreover, if ψ is a constituent of $\operatorname{Res}_N^I \theta$, then $\langle \operatorname{Res}_N^I \psi, \theta\rangle = \langle \operatorname{Res}_N^G \chi, \theta\rangle$.

Proof. There are several things to prove.

Claim. The map is $\psi \mapsto \operatorname{Ind}_I^G \psi$ well-defined.

Let $\psi \in \operatorname{Irr}(I)$ be such that $e = \langle \operatorname{Res}_N^I \psi, \theta\rangle > 0$ and let $\chi \in \operatorname{Irr}(G)$ be a constituent of $\operatorname{Ind}_I^G \psi$. By Frobenius' reciprocity,

$$\langle \psi, \operatorname{Res}_I^G \chi\rangle = \langle \operatorname{Ind}_I^G \psi, \chi\rangle > 0.$$

Thus ψ is a constituent of $\operatorname{Res}_I^G \chi$, that is

$$\operatorname{Res}_I^G \chi = \psi + \lambda$$

for some $\lambda = 0$ or $\lambda \in \operatorname{Char}(I)$. Thus

$$\operatorname{Res}_N^G \chi = \operatorname{Res}_N^I \operatorname{Res}_I^G \chi = \operatorname{Res}_N^I(\psi + \lambda) = \operatorname{Res}_N^I \psi + \operatorname{Res}_N^I \lambda,$$

that is $\operatorname{Res}_N^I \psi$ is a constituent of $\operatorname{Res}_N^I \operatorname{Res}_I^G \chi$. Moreover,

$$\chi(1) \leq (\operatorname{Ind}_I^G \psi)(1) = (G : I)\psi(1).$$

Let $f = \langle \operatorname{Res}_N^G \chi, \theta\rangle$. Then

$$f = \langle \operatorname{Res}_N^G \chi, \theta\rangle = \langle \operatorname{Res}_N^I \operatorname{Res}_I^G \chi, \theta\rangle \geq \langle \operatorname{Res}_N^I \psi, \theta\rangle = e > 0.$$

Since $\operatorname{Res}_N^G \chi = f(\theta_1 + \cdots + \theta_t)$, where $G \cdot \theta = \{\theta_1, \dots, \theta_t\}$ is the orbit of θ under the action of G and $t = (G : I)$,

$$ft\theta(1) = \chi(1) = (\operatorname{Res}_N^G \chi)(1) \leq (\operatorname{Ind}_I^G \psi)(1) = t\psi(1) = et\theta(1) \leq ft\theta(1),$$

where the last equality follows since $\operatorname{Res}_N^I \psi = e\theta$ by Clifford's theorem. Therefore $e = f$ and $\operatorname{Ind}_I^G \psi = \chi$.

Claim. The map is $\psi \mapsto \operatorname{Ind}_I^G \psi$ is injective.

Let $\psi_1 \in \operatorname{Irr}(I)$ and $\psi_2 \in \operatorname{Irr}(I)$ be such that $\langle \operatorname{Res}_N^I \psi_i, \theta\rangle > 0$ for all $i \in \{1, 2\}$ and $\chi = \operatorname{Ind}_I^G \psi_1 = \operatorname{Ind}_I^G \psi_2$. In the first claim, we proved that $\chi \in \operatorname{Irr}(G)$. We want to prove that $\psi_1 = \psi_2$.

Suppose $\psi_1 \neq \psi_2$. We know that ψ_1 and ψ_2 from the first claim that are constituents of $\operatorname{Res}_I^G \chi$, that is

$$\operatorname{Res}_I^G \chi = \psi_1 + \psi_2 + \xi$$

for some map $\xi\colon I \to \mathbb{C}$. (The map ξ is either zero or a character of I.) Then both $\operatorname{Res}_N^I \psi_1$ and $\operatorname{Res}_N^I \psi_2$ are constituents of $\operatorname{Res}_N^G \chi$, as

$$\begin{aligned}\operatorname{Res}_N^G \chi &= \operatorname{Res}_N^I \operatorname{Res}_I^G \chi\\ &= \operatorname{Res}_N^I(\psi_1 + \psi_2 + \xi)\\ &= \operatorname{Res}_N^I \psi_1 + \operatorname{Res}_N^I \psi_2 + \operatorname{Res}_N^I \xi.\end{aligned}$$

Moreover,

$$\begin{aligned}\langle \operatorname{Res}_N^G \chi, \theta\rangle &= \langle \operatorname{Res}_N^I \psi_1 + \operatorname{Res}_N^I \psi_2 + \operatorname{Res}_N^I \xi, \theta\rangle\\ &= \langle \operatorname{Res}_N^I \psi_1, \theta\rangle + \langle \operatorname{Res}_N^I \psi_2, \theta\rangle + \langle \operatorname{Res}_N^I \xi, \theta\rangle\\ &\geq \langle \operatorname{Res}_N^I \psi_1, \theta\rangle + \langle \operatorname{Res}_N^I \psi_2, \theta\rangle\\ &= \langle \operatorname{Res}_N^G \chi, \theta\rangle + \langle \operatorname{Res}_N^G \chi, \theta\rangle,\end{aligned}$$

where the last equality holds because we proved in the previous claim that

$$\langle \operatorname{Res}_N^I \psi_i, \theta\rangle = \langle \operatorname{Res}_N^G \chi, \theta\rangle$$

for all $i \in \{1,2\}$. This implies that $\langle \operatorname{Res}_N^G \chi, \theta\rangle = 0$, a contradiction.

Claim. The map is $\psi \mapsto \operatorname{Ind}_I^G \psi$ is surjective.

Let $\chi \in \operatorname{Irr}(G)$ be such that $e = \langle \operatorname{Res}_N^G \chi, \theta\rangle > 0$. Since

$$\operatorname{Res}_I^G \chi = \sum_{\psi \in \operatorname{Irr}(I)} \langle \operatorname{Res}_I^G, \psi\rangle \psi,$$

it follows that

$$\operatorname{Res}_N^G \chi = \operatorname{Res}_N^I \operatorname{Res}_I^G \chi = \sum_{\psi \in \operatorname{Irr}(I)} \langle \operatorname{Res}_I^G \chi, \psi\rangle \operatorname{Res}_N^I \psi.$$

Since

$$e = \langle \operatorname{Res}_N^G \chi, \theta\rangle = \sum_{\psi \in \operatorname{Irr}(I)} \langle \operatorname{Res}_I^G \chi, \psi\rangle \langle \operatorname{Res}_N^I \psi, \theta\rangle$$

is a positive number, there exists some $\psi \in \operatorname{Irr}(I)$ such that $\langle \operatorname{Res}_I^G \chi, \psi\rangle \langle \operatorname{Res}_N^I \psi, \theta\rangle > 0$. In particular, $\langle \operatorname{Res}_N^I \psi, \theta\rangle$ and

$$\langle \chi, \operatorname{Ind}_I^G \psi\rangle = \langle \operatorname{Res}_I^G \chi, \psi\rangle > 0$$

Hence $\chi = \operatorname{Ind}_I^G \psi$. □

§ 11.2. Itô's theorem. We now present a result that is stronger than Schur's Theorem 4.6. To that end, we introduce some exercises on basic properties of the center of characters.

11.6. Definition. Let G be a finite group and $\chi \in \operatorname{Char}(G)$. The **center** of χ is

$$Z(\chi) = \{g \in G : |\chi(g)| = \chi(1)\}.$$

11.7. Exercise. Let G be a finite group and $\rho \colon G \to \mathbf{GL}_n(\mathbb{C})$ be a representation with character χ. Prove the following statements:

1) $Z(\chi) = \{g \in G : \rho_g \text{ is a scalar matrix}\}$.
2) $Z(\chi)$ is a normal subgroup of G.
3) $Z(\chi)/\ker\chi$ is cyclic.

11.8. Exercise. Let G be a finite group and $\chi \in \operatorname{Irr}(G)$. Prove that

$$Z(\chi)/\ker\chi = Z(G/\ker\chi).$$

11.9. Exercise. Let G be a finite group. Prove that

$$Z(G)=\bigcap\{Z(\chi):\chi\in\mathrm{Irr}(G)\}.$$

The previous exercise shows that the center of a finite group can be determined from its character table. It follows that the character table detects nilpotency. To do this, one computes $Z(G)$ from the character table of G, then the character table of $G/Z(G)$, and by iterating this process, one obtains the upper central series of the group G.

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

Proof. Let $Q=G/\ker\chi$. By Theorem 8.2, χ corresponds to $\eta\in\mathrm{Char}(Q)$. By Schur's theorem 4.6, $\chi(1)=\eta(1)$ divides $(Q:Z(Q))$. By Exercise 11.8, $(Q:Z(Q))=(G:Z(\chi))$. □

11.11. Theorem (Itô). *Let G be a finite group and $\chi\in\mathrm{Irr}(G)$. Then $\chi(1)$ divides $(G:A)$ for all normal abelian subgroup A of G.*

Proof. Let A be a normal abelian subgroup of G and $\theta\in\mathrm{Irr}(A)$ be an irreducible constituent of $\mathrm{Res}_A^G\chi$, that is $\langle\mathrm{Res}_A^G\chi,\theta\rangle>0$. Let $I=I_G(\theta)$. By Clifford correspondence (Theorem 11.5), $\chi=\mathrm{Ind}_I^G(\psi)$ for some $\psi\in\mathrm{Irr}(I)$ such that $\langle\mathrm{Res}_A^I\psi,\theta\rangle>0$. By Clifford's theorem, since I acts trivially on θ, $\mathrm{Res}_A^I\psi=e\theta$, where $e=\langle\mathrm{Res}_A^I\psi,\theta\rangle>0$. Since A is abelian and $\theta\in\mathrm{Irr}(A)$, $\theta(1)=1$.

We claim that $A\subseteq Z(\psi)$. In fact, if $a\in A$, then

$$|\psi(a)|=|\mathrm{Res}_A^I\psi(a)|=|e\theta(a)|=e|\theta(a)|=e1=e=\psi(1).$$

By Lagrange's theorem, $|A|$ divides $|Z(\psi)|$. Thus $(I:Z(\psi))$ divides $(I:A)$.

By Lemma 11.10, $e\theta(1)=\psi(1)$ divides $(I:Z(\psi))$. Then $\psi(1)$ divides $(I:A)$. Now

$$\chi(1)=(\mathrm{Ind}_I^G\psi)(1)=(G:I)\psi(1)$$

divides $(G:I)(I:A)=(G:A)$. □

11.12. Bonus exercise. Prove that Itô's theorem remains valid under the assumption that A is subnormal in G.

12. Lecture: Week 12

§ 12.1. Kronecker's theorem. We begin with a classical theorem of Kronecker on algebraic integers. Recall that $\alpha \in \mathbb{C}$ is an **algebraic integer** if there is a monic polynomial $f \in \mathbb{Z}[X]$ such that $f(\alpha) = 0$ (see Definition 3.12). Let $\mathbb{A}$ be the set of algebraic integers.

12.1. Exercise. Let $\alpha \in \mathbb{A}$. Prove that there exists a monic polynomial $f \in \mathbb{Z}[X]$, irreducible $f \in \mathbb{Q}[X]$ such that $f(\alpha) = 0$.

The polynomial of Exercise 12.1 is called the **minimal polynomial** of α.

12.2. Exercise. Let $\alpha \in \mathbb{A}$. Prove that the roots of the minimal polynomial of α are pairwise distinct.

The **conjugates** of α are the roots of the minimal polynomial of α.

Recall that for an $n \times n$ matrix $A = (a_{ij})$, its **norm** (more precisely, **infinity-norm**) is defined as the maximum absolute row sum of the matrix, that is

$$\|A\| = \max_{1 \leq i \leq n} \sum_{j=1}^{n} |a_{ij}|.$$

For $A, B \in \mathbb{C}^{n \times n}$ and $\lambda \in \mathbb{C}$, the following properties hold:

1) $\|A\| \geq 0$.
2) $\|A\| = 0$ if and only if A is the $n \times n$ zero matrix.
3) $\lambda\|A\| = |\lambda|\|A\|$.
4) $\|A + B\| \leq \|A\| + \|B\|$.
5) $\|AB\| \leq \|A\|\|B\|$.

For our purposes, the choice of norm is not important at all (and any other norm could have been chosen). Nevertheless, we provide an example. Let

$$A = \begin{pmatrix} 1 & 2 & -3 \\ 0 & -5 & -7 \\ 11 & 2 & -3 \end{pmatrix}.$$

Then $\|A\| = \max\{6, 12, 16\} = 16$.

12.3. Theorem (Kronecker). *Let $\alpha \in \mathbb{A}$. Assume that all the conjugates of α have absolute value at most one. Then either $\alpha = 0$ or α is a root of one.*

Proof. Assume that $\alpha \neq 0$. Let $f \in \mathbb{Z}[X]$ be the minimal polynomial of α, say

$$f = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$$

for integers $a_0, a_1, \dots, a_{n-1} \in \mathbb{Z}$. Then $f(0) \neq 0$ because f is irreducible in $\mathbb{Q}[X]$ (see Exercise 12.1). Let

$$F = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix} \in \mathbb{Z}^{n \times n}$$

be the **companion matrix** of f. The characteristic polynomial and the minimal polynomial of the matrix F are equal to f. Moreover, the roots of f are the eigenvalues of F. Since all the roots of f are distinct, all the eigenvalues of F are different. Thus F is diagonalizable, so there exists $P \in \mathbf{GL}_n(\mathbb{C})$ such that $F = PDP^{-1}$, where D is the $n \times n$ diagonal matrix with diagonal entries $\alpha = \alpha_1, \alpha_2, \dots, \alpha_n$, the roots of f (i.e., the conjugates of α), so all with absolute value at most one. Thus $\|D\| \leq 1$. Since $0 \notin \{\alpha_1, \dots, \alpha_n\}$, the matrix F is invertible. Moreover,

$$F^k = (PDP^{-1})^k = PD^kP^{-1}$$

for all $k \geq 1$. Note that the set $X = \{F^k : k \geq 1\} \subseteq M_n(\mathbb{Z})$ is bounded in $M_n(\mathbb{C})$, as

$$\|F^k\| = \|PD^kP^{-1}\| \leq \|P\|\|D\|^k\|P^{-1}\| \leq \underbrace{\|P\|\|P^{-1}\|}_{\text{This is independent of } k}.$$

Thus X is finite. In particular, there are integers $i < j$ such that $F^i = F^j$. Since F is invertible, F^{j-i} is the $n \times n$ identity matrix. Since α is an eigenvalue of F, it follows that $\alpha^{j-i} = 1$. □

The proof of the theorem presented here goes back to Greiter [12]. Kronecker's original proof is somewhat similar, relying on Vieta's formulas and estimates involving binomial coefficients; see [6].

§ 12.2. Solvable groups and Burnside's theorem. For a group G let $G^{(0)} = G$ and $G^{(i+1)} = [G^{(i)}, G^{(i)}]$ for $i \geq 0$. The **derived series** of G is the sequence

$$G = G^{(0)} \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \cdots$$

Each $G^{(i)}$ is a characteristic subgroup of G. We say that G is **solvable** if $G^{(n)} = \{1\}$ for some n.

12.4. Example. Abelian groups are solvable.

12.5. Example. The group $\mathbf{SL}_2(3)$ is solvable. Let us see what the computer says:

```
> G := SL(2,3);;
> IsSolvable(G);
true
> [GroupName(x) : x in DerivedSeries(G)];
[ SL(2,3), Q8, C2, C1 ]
```

12.6. Example. Non-abelian simple groups cannot be solvable.

For $n \geq 5$, the group $\mathbb{A}_n$ is not solvable.

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

1) A subgroup H of G is solvable, when G is solvable.
2) Let K be a normal subgroup of G. Then G is solvable if and only if K and G/K are solvable.

For $n \geq 5$, the group $\mathbb{S}_5$ is not solvable.

12.8. Exercise. Let p be a prime number. Prove that finite p-groups are solvable.

Exercises 12.7 and 12.8 may be omitted if the reader is already familiar with solvable groups.

12.9. Theorem (Burnside). *Let G be a finite group. If $\phi\colon G\to \mathbf{GL}_n(\mathbb{C})$ is a representation with character χ and C is a conjugacy class of G such that $\gcd(|C|,n)=1$, then for every $g\in C$ either $\chi(g)=0$ or ϕ_g is a scalar matrix.*

Now we prove the theorem.

Proof of Theorem 12.9. Let $\epsilon_1,\dots,\epsilon_n$ be the eigenvalues of ϕ_g. Then $\epsilon_1,\dots,\epsilon_n$ are roots of one. By assumption, $\gcd(|C|,n)=1$, there exist $a,b\in\mathbb{Z}$ such that $a|C|+bn=1$. Since $|C|\chi(g)/n\in\mathbb{A}$, after multiplying by $\chi(g)/n$ we obtain that

$$a|C|\frac{\chi(g)}{n}+b\chi(g)=\frac{\chi(g)}{n}=\frac{1}{n}(\epsilon_1+\cdots+\epsilon_n)\in\mathbb{A}.$$

Let $\alpha_1=\chi(g)/n\in\mathbb{A}$ and $\alpha_2,\dots,\alpha_n$ be its conjugates. Since $|\alpha_1|\leq 1$ and $\alpha_2,\dots,\alpha_n$ are conjugates of α_1, it follows that $|\alpha_j|\leq 1$ for all $j\in\{1,\dots,n\}$. By Kronecker's theorem, either $\alpha_1=0$ or α_1 is a root of one. If $\alpha_1=0$, then $\chi(g)=0$. If α_1 is a root of one, then

$$1=|\alpha_1|=\frac{|\chi(g)|}{n}=\frac{1}{n}.$$

Thus $|\chi(g)|=n=\chi(1)$. This means that $g\in\mathbb{Z}(\chi)$. By Exercise 11.7, ϕ_g is a scalar matrix. □

12.10. Theorem (Burnside). *Let p be a prime number. If G is a finite group and C is a conjugacy class of G with $p^k>1$ elements, then G is not simple.*

Proof. Let $g\in C\setminus\{1\}$. Column orthogonality implies that

$$\begin{aligned} 0&=\sum_{\chi\in\mathrm{Irr}(G)}\chi(1)\chi(g)\\ &=\sum_{p\mid\chi(1)}\chi(1)\chi(g)+\sum_{p\nmid\chi(1):\chi\neq\chi_1}\chi(1)\chi(g)+1,\end{aligned}\tag{12.1}$$

where the one corresponds to the trivial representation of G.

Look at this equation modulo p. If $\chi(g)=0$ for all $\chi\in\mathrm{Irr}(G)$ such that $\chi\neq\chi_1$ and $p\nmid\chi(1)$, then

$$-\frac{1}{p}=\sum\frac{\chi(1)}{p}\chi(g)\in\mathbb{A}\cap\mathbb{Q}=\mathbb{Z},$$

where the sum is taken over all non-trivial irreducibles of G of degree divisible by p, a contradiction. Hence there exists an irreducible non-trivial representation ϕ with character χ such that p does not divide $\chi(1)$ and $\chi(g)\neq 0$. By the previous theorem, ϕ_g is a scalar matrix. If ϕ is faithful, then g is a non-trivial central element, a contradiction since $|C|>1$. If ϕ is not faithful, then G is not simple (because $\ker\phi$ is a non-trivial proper normal subgroup of G). □

12.11. Theorem (Burnside). *Let p and q be prime numbers. If G has order p^aq^b, then G is solvable.*

Proof. If G is abelian, then it is solvable. Suppose now G is non-abelian. Let us assume that the theorem is not true. Let G be a group of minimal order $p^a q^b$ that is not solvable. Since $|G|$ is minimal, G is a non-abelian simple group. By the previous theorem, G has no conjugacy classes of size p^k nor conjugacy classes of size q^l with $k, l \geq 1$. The size of every conjugacy class of G is one or divisible by pq. Note that, since G is a non-abelian simple group, the center of G is trivial. Thus there is only one conjugacy class of size one. By the class equation,

$$|G| = 1 + \sum_{C:|C|>1} |C| \equiv 1 \bmod pq,$$

where the sum is taken over all conjugacy classes of G with more than one element, a contradiction. $\square$

There are several interesting theorems that generalize Burnside's theorem. We briefly mention two of them.

12.12. Theorem (Kegel–Wielandt). *If G is a finite group and there are nilpotent subgroups A and B of G such that $G = AB$, then G is solvable.*

See [3, Theorem 2.4.3] for the proof.

12.13. Exercise. Prove that Theorem 12.12 implies Theorem 12.11.

Another generalization of Burnside's theorem is based on **word maps**. A word map of a group G is a map

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

for some word $w(x_1, \dots, x_k)$ of the free group F_k of rank k. Some word maps are surjective in certain families of groups. For example, Ore's conjecture is precisely the surjectivity of the word map $(x, y) \mapsto [x, y] = xyx^{-1}y^{-1}$ in every finite non-abelian simple group.

12.14. Theorem (Guralnick–Liebeck–O'Brien–Shalev–Tiep). *Let $a, b \geq 0$, p and q be prime numbers and $N = p^a q^b$. The map $(x, y) \mapsto x^N y^N$ is surjective in every finite simple group.*

The proof appears in [14].

The theorem implies Burnside's theorem. Let G be a group of order $N = p^a q^b$. Assume that G is not solvable. Fix a composition series of G. There is a non-abelian factor S of order that divides N. Since S is simple non-abelian and $s^N = 1$, it follows that the word map $(x, y) \mapsto x^N y^N$ has trivial image in S, a contradiction to the theorem.

§ 12.3. The Feit–Thompson theorem.

12.15. Theorem (Feit–Thompson). *Groups of odd order are solvable.*

The proof of Feit–Thompson theorem is extremely hard. It occupies a full volume of the **Pacific Journal of Mathematics** [8]. A formal verification of the proof (based on the computer software Coq) was announced in [11].

Back in the day it was believed that if a certain divisibility conjecture is true, the proof of Feit–Thompson theorem could be simplified.

12.16. Conjecture (Feit–Thompson). There are no prime numbers p and q such that $\frac{p^q-1}{p-1}$ divides $\frac{q^p-1}{q-1}$.

The conjecture remains open. However, now we know that proving the conjecture will not simplify further the proof of Feit–Thompson theorem.

In 2012 Le proved that the conjecture is true for $q=3$, see [27].

In [36] Stephens proved that a certain stronger version of the conjecture does not hold, as the integers $\frac{p^q-1}{p-1}$ and $\frac{q^p-1}{q-1}$ could have common factors. In fact, if $p=17$ and $q=3313$, then

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

Nowadays we can check this easily in almost every desktop computer:

```
> p := 17;
> q := 3313;
> bool, a := IsCoercible(Integers(), (p^q-1)/(p-1));
> bool, b := IsCoercible(Integers(), (q^p-1)/(q-1));
> Gcd(a,b);
112643
```

No other counterexamples have been found of Stephen's stronger version of the conjecture.

§ 12.4. The character table of $\mathbb{A}_5$. Let $G=\mathbb{A}_5$. The group G is a non-abelian simple group of order 60. It has five conjugacy classes, namely

Representative	id	(12)(34)	(123)	(12345)	(12354)
Size	1	15	20	12	12

One can easily get the conjugacy classes of $\mathbb{A}_5$ with Magma:

```
> A5 := Alt(5);
> ConjugacyClasses(A5);
Conjugacy Classes of group A5
-----------------------------
[1]     Order 1       Length 1
        Id(A5)

[2]     Order 2       Length 15
        (1, 2)(3, 4)

[3]     Order 3       Length 20
        (1, 2, 3)

[4]     Order 5       Length 12
        (1, 2, 3, 4, 5)

```

```
[5]      Order 5       Length 12
         (1, 3, 4, 5, 2)
```

Let us see how to obtain all conjugacy classes of $\mathbb{A}_5$ without computers. Let $\sigma \in \mathbb{A}_5$ and C be its conjugacy class in $\mathbb{S}_5$. Thus $|C| = (\mathbb{S}_5 : C_{\mathbb{S}_5}(\sigma))$. There are two cases to consider

Assume first that $C_{\mathbb{S}_5}(\sigma) \not\subseteq \mathbb{A}_5$. Since $\mathbb{A}_5$ is a maximal subgroup of $\mathbb{S}_5$, it follows that $\mathbb{A}_5 C_{\mathbb{S}_5}(\sigma) = \mathbb{S}_5$. Using the isomorphism theorems,

$$\mathbb{S}_5/\mathbb{A}_5 = \mathbb{A}_5 C_{\mathbb{S}_5(\sigma)}/\mathbb{A}_5 \simeq C_{\mathbb{S}_5}(\sigma)/(C_{\mathbb{S}_5}(\sigma) \cap \mathbb{A}_5) = C_{\mathbb{S}_5}(\sigma)/C_{\mathbb{A}_5}(\sigma).$$

Hence

$$(\mathbb{A}_5 : C_{\mathbb{A}_5}(\sigma)) = \frac{(\mathbb{S}_5 : C_{\mathbb{A}_5}(\sigma))}{(\mathbb{S}_5 : \mathbb{A}_5)} = \frac{(\mathbb{S}_5 : C_{\mathbb{A}_5}(\sigma))}{(C_{\mathbb{S}_5}(\sigma) : C_{\mathbb{A}_5}(\sigma))} = (\mathbb{S}_5 : C_{\mathbb{S}_5}(\sigma)) = |C|.$$

Therefore C is the class of σ in $\mathbb{A}_5$.

Assume now that $C_{\mathbb{S}_5}(\sigma) \subseteq \mathbb{A}_5$. Then $C_{\mathbb{A}_5}(\sigma) = C_{\mathbb{S}_5}(\sigma) \cap \mathbb{A}_5 = C_{\mathbb{S}_5}(\sigma)$ and therefore

$$(\mathbb{A}_5 : C_{\mathbb{A}_5}(\sigma)) = (\mathbb{A}_5 : C_{\mathbb{S}_5}(\sigma)) = \frac{1}{2}(\mathbb{S}_5 : C_{\mathbb{S}_5}(\sigma)) = \frac{1}{2}|C|.$$

Thus C splits into two conjugacy classes of $\mathbb{A}_5$ of equal size.

The identity permutation is central. The even permutations $(12)(34)$ and (123) both commutes with some odd permutation in $\mathbb{S}_5$ (e.g. $[(12)(34),(34)] = [(123),(45)] = \mathrm{id}$). Thus these classes do not split in $\mathbb{A}_5$. There are twenty-four 5-cycles in $\mathbb{S}_5$. Since 24 does not divide $|\mathbb{A}_5| = 60$, it follows that the class of 5-cycles splits in $\mathbb{A}_5$. As representatives of these classes we can take (12345) and (12354).

Since $\mathbb{A}_5$ has five conjugacy classes, $|\operatorname{Irr}(G)| = 5$. Assume that

$$\operatorname{Irr}(G) = \{\chi_1, \chi_2, \chi_3, \chi_4, \chi_5\},$$

where χ_1 is the trivial character.

Let $H = \mathbb{A}_4$. We compute $\operatorname{Ind}_H^G \chi_1$. By Corollary 7.14,

$$\left(\operatorname{Ind}_H^G \chi_1\right)(\mathrm{id}) = 5.$$

And a direct calculation shows

$$\begin{aligned}
\left(\operatorname{Ind}_H^G \chi_1\right)((12)(34)) &= 1,\\
\left(\operatorname{Ind}_H^G \chi_1\right)((123)) &= 2,\\
\left(\operatorname{Ind}_H^G \chi_1\right)((12345)) &= 0\\
\left(\operatorname{Ind}_H^G \chi_1\right)((12354)) &= 0.
\end{aligned}$$

Now, using Frobenius' reciprocity and the fact that $\operatorname{Res}_H^G \chi_1$ is the trivial character of H,

$$\langle \operatorname{Ind}_H^G \chi_1, \chi_1 \rangle = \langle \chi_1, \operatorname{Res}_H^G \chi_1 \rangle = 1.$$

Let $\chi_2 = \operatorname{Ind}_H^G \chi_1 - \chi_1$. Since

$$\langle \operatorname{Ind}_H^G \chi_1 - \chi_1, \operatorname{Ind}_H^G \chi_1 - \chi_1 \rangle = 1,$$

it follows that $\chi_2 \in \operatorname{Irr}(G)$.

12.17. Exercise. Use Proposition 6.1 to derive (once again) the values of χ_2.

So far we have the following table:

	id	(12)(34)	(123)	(12345)	(12354)
χ_1	1	1	1	1	1
χ_2	4	0	1	-1	-1
χ_3	n_3	·	·	·	·
χ_4	n_4	·	·	·	·
χ_5	n_5	·	·	·	·

As G is simple non-abelian, $|G/[G,G]| = 1$. It follows that χ_1 is the only linear character of G. Moreover, $\chi_j(1) \geq 3$ by Theorem 4.5. Since

$$60 = 1 + 16 + n_3^2 + n_4^2 + n_5^2$$

and each n_j divides $|G| = 60$ (see Theorem 4.3), it follows that $n_j \in \{3,4,5,6\}$. If some $n_j = 6$, say without loss of generality $n_3 = 6$, then

$$7 = 43 - 36 = n_2^2 + n_3^2,$$

a contradiction. Thus $n_j \in \{3,4,5\}$ for all $j \in \{3,4,5\}$. Without loss of generality, we may assume that $n_3 = n_4 = 3$ and $n_5 = 5$.

	id	(12)(34)	(123)	(12345)	(12354)
χ_1	1	1	1	1	1
χ_2	4	0	1	-1	-1
χ_3	3	·	·	·	·
χ_4	3	·	·	·	·
χ_5	5	·	·	·	·

The group $\mathbb{A}_5$ acts on the set Y of subsets of $\{1,2,\dots,5\}$ of two elements, namely

$$g \cdot \{a,b\} = \{g \cdot a, g \cdot b\}.$$

Note that $|Y| = \binom{5}{2} = 10$. Moreover, this action is transitive. Let us compute the character ψ of the corresponding $\mathbb{C}\mathbb{A}_5$-module and the difference $\psi - \chi_1$ (We know ψ counts fixed points.)

	id	(12)(34)	(123)	(12345)	(12354)
ψ	10	2	1	0	0
$\psi - \chi_1$	9	1	0	-1	-1

The identity, of course, fixes all the ten elements of Y. The permutation (12)(34) fixed two two-elements subsets, namely $\{1,2\}$ and $\{3,4\}$. The permutation (123) fixes only one two-elements subset, namely $\{4,5\}$. Finally, (12345) and (12354) fix no two-element subsets.

Now we compute

$$\langle \psi - \chi_1, \psi - \chi_1 \rangle = 2$$

and hence $\psi - \chi_1$ is the sum of two irreducible characters (see Exercise 3.7). Since

$$\langle \psi - \chi_1, \chi_2 \rangle = 1,$$

it follows that $\psi - \chi_1 - \chi_2 \operatorname{Irr}(G)$. Let $\chi_5 = \psi - \chi_1 - \chi_2$. Then

	id	(12)(34)	(123)	(12345)	(12354)
χ_1	1	1	1	1	1
χ_2	4	0	1	-1	-1
χ_3	3	·	·	·	·
χ_4	3	·	·	·	·
χ_5	5	1	-1	0	0

Let $K = \langle (12345) \rangle$ and $\eta \in \mathrm{Irr}(K)$ be such that $\eta((12345)) = \zeta$, where $\zeta = \exp(2\pi i/5)$ is a primitive 5-th root of one. We can then compute Ind_K^G.

	id	(12)(34)	(123)	(12345)	(12354)
$\mathrm{Ind}_K^G \psi$	12	0	0	$\zeta^2+\zeta^3$	$\zeta+\zeta^4$

Since $\langle \mathrm{Ind}_K^G \psi, \chi_2 \rangle = 1 = \langle \mathrm{Ind}_H^G, \chi_5 \rangle$, it follows that

	id	(12)(34)	(123)	(12345)	(12354)
$\mathrm{Ind}_K^G \psi - \chi_2 - \chi_5$	3	-1	0	$-\zeta-\zeta^4$	$-\zeta^2-\zeta^3$

Let $\chi_3 = \mathrm{Ind}_K^G \psi - \chi_2 - \chi_5$. Then $\chi_3 \in \mathrm{Irr}(G)$, because it is not the sum of three copies of the trivial character.

	id	(12)(34)	(123)	(12345)	(12354)
χ_1	1	1	1	1	1
χ_2	4	0	1	-1	-1
χ_3	3	-1	0	$-\zeta-\zeta^4$	$-\zeta^2-\zeta^3$
χ_4	3	·	·	·	·
χ_5	5	1	-1	0	0

12.18. Exercise. Use the orthogonality relations to compute the missing row of the character table of $\mathbb{A}_5$.

The previous exercise finishes the calculation of the character table of $\mathbb{A}_5$; see Table 7.

Table 7. The character table of $\mathbb{A}_5$.

	1 id	15 (12)(34)	20 (123)	12 (12345)	12 (12354)
χ_1	1	1	1	1	1
χ_2	4	0	1	-1	-1
χ_3	3	-1	0	$-\zeta-\zeta^4$	$-\zeta^2-\zeta^3$
χ_4	3	-1	0	$-\zeta^2-\zeta^3$	$-\zeta-\zeta^4$
χ_5	5	1	-1	0	0

One last observation: Since $\zeta = \exp(2\pi i/5)$, it follows that

$$-\zeta-\zeta^4 = \frac{1-\sqrt{5}}{2}, \quad -\zeta^2-\zeta^3 = \frac{1+\sqrt{5}}{2}.$$

13. Project: Irreducible characters of dihedral groups

Let $n \geq 3$. Recall that the **dihedral group** of order $2n$ is the group

$$\mathbb{D}_n = \langle r, s : r^n = s^2 = 1, srs = r^{-1} \rangle.$$

Every element of $\mathbb{D}_n$ is of the form $s^i r^j$ for some $i \in \{0,1\}$ and $j \in \{0,\dots,n-1\}$.

Our goal is the construct the character table of $\mathbb{D}_n$.

13.1. Proposition. *Let $n \geq 3$. If n is odd, then*

$$\{1\}, \{r, r^{-1}\}, \{r^2, r^{-2}\}, \cdots, \{r^{(n-1)/2}, r^{(1-n)/2}\}, \{s, sr, sr^2, \dots, sr^{n-1}\}$$

are the conjugacy classes of $\mathbb{D}_n$. If n is even, then

$$\{1\}, \{r, r^{-1}\}, \{r^2, r^{-2}\}, \cdots, \{r^{n/2-1}, r^{1-n/2}\},$$
$$\{r^{n/2}\}, \{s, sr^2, sr^4, \dots, sr^{n-2}\}, \{sr, sr^3, \dots, sr^{n-1}\}$$

are the conjugacy classes of $\mathbb{D}_n$.

Proof. Recall that $sr^j = r^{-j}s$ for all j. Let $g = s^i r^j \in \mathbb{D}_n$ and $x = s^k r^l \in \mathbb{D}_n$. Let us compute xgx^{-1}. We split the proof into several steps.

Assume first that $i = 0$, that is $g = r^j$. Then

$$xgx^{-1} = (s^k r^l) r^j (r^{-l} s^{-k}) = s^k r^j s^{-k} = \begin{cases} r^j & \text{if } k = 0, \\ r^{-j} & \text{if } k = 1. \end{cases}$$

Hence the conjugacy class of $g = r^j$ is $\{r^j, r^{-j}\}$.

Now assume that $i = 1$, that is $g = sr^j$. Since $k \in \{0,1\}$, a direct calculation using the fact that $r^l s = sr^{-l}$ yields

$$xgx^{-1} = \begin{cases} sr^{-2l+j} & \text{if } k = 0, \\ sr^{2l-j} & \text{if } k = 1. \end{cases}$$

Hence the conjugacy class of $g = sr^j$ is $\{sr^{2l-j}, sr^{-2l+j} : 0 \leq l \leq n-1\}$.

Assume that n is odd. We have determined the conjugacy classes

$$\{1\}, \{b, b^{-1}\}, \{b^2, b^{-2}\}, \dots, \{b^{(n-1)/2}, b^{(1-n)/2}\}$$

which together cover all the elements of the subgroup $\langle b \rangle = \{1, b, b^2, \dots, b^{n-1}\}$. Since n is odd, for every integer m there exists an integer x such that $2x \equiv m \bmod n$. Thus the conjugacy class of s is $\{s, sr, sr^2, \dots, sr^{n-1}\}$. These classes together cover all the elements of $\mathbb{D}_n$.

Now assume that n is even. We have determined the conjugacy classes

$$\{1\}, \{b, b^{-1}\}, \{b^2, b^{-2}\}, \dots, \{b^{n/2-1}, b^{1-n/2}\}, \{b^{n/2}\}$$

which together cover all the elements of the subgroup $\langle b \rangle = \{1, b, b^2, \dots, b^{n-1}\}$. The class of s is $\{s, sr^2, sr^4, \dots, sr^{n-2}\}$ and the class of sr is $\{sr, sr^3, \dots, sr^{n-1}\}$. These classes together cover all the elements of $\mathbb{D}_n$. $\square$

The previous proposition gives the number of conjugacy classes of the dihedral group $\mathbb{D}_n$, namely

$$\frac{2n + 9 + (-1)^n 3}{4} = \begin{cases} \frac{n+6}{2} & \text{if } n \text{ is even}, \\ \frac{n+3}{2} & \text{if } n \text{ is odd}. \end{cases}$$

This number is precisely the number of irreducible representations of $\mathbb{D}_n$.

13.2. Exercise. Compute $Z(\mathbb{D}_n)$.

13.3. Exercise. Prove that $\lim_{n\to\infty} \operatorname{cp}(\mathbb{D}_n) = 1/4$.

To determine the number of degree-one representations of our group, we need the index of the commutator subgroup.

13.4. Exercise. Prove that $[\mathbb{D}_n, \mathbb{D}_n] = \langle r^2 \rangle$. Moreover,

$$(G : [G, G]) = \begin{cases} 2 & \text{if } n \text{ is odd.} \\ 4 & \text{if } n \text{ is even.} \end{cases}$$

§ 13.1. n odd. By Proposition 13.1, the representatives of the conjugacy classes of $\mathbb{D}_n$ are $1, r, r^2, \dots, r^{(n-1)/2}, s$. By Exercise 13.4, there are two degree-one characters, namely the trivial character and the character η such that $r \mapsto 1$ and $s \mapsto -1$.

	1	r	r^2	$\cdots$	$r^{(n-1)/2}$	s
trivial	1	1	1	$\cdots$	1	1
η	1	1	1	$\cdots$	1	-1

Assume that $n = 2k - 1$. We need $\frac{n-1}{2} = k - 1$ additional irreducible characters. For $m \in \{1, \dots, k-1\}$, let $\omega_m = e^{2\pi i m/k}$ and

$$\rho_m \colon \mathbb{D}_n \to \mathbf{GL}_2(\mathbb{C}), \quad r \mapsto \begin{pmatrix} \omega_m & 0 \\ 0 & \omega_m^{-1} \end{pmatrix}, \quad s \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

13.5. Exercise. Prove that each ρ_m is a group homomorphism.

A direct calculation produces the values of the character χ_m of ρ_m.

	1	r	r^2	$\cdots$	$r^{(n-1)/2}$	s
χ_m	1	$\omega_m + \omega_m^{-1}$	$\omega_m^2 + \omega_m^{-2}$	$\cdots$	$\omega_m^{(n-1)/2} + \omega_m^{(1-n)/2}$	0

13.6. Exercise. Let $i, j \in \{1, \dots, k-1\}$. Prove that $\chi_i \neq \chi_j$ whenever $i \neq j$.

13.7. Exercise. Prove that each χ_m is irreducible.

It remains only to note that we have constructed $\frac{n+3}{2}$ irreducible characters of $\mathbb{D}_n$, so the character table of $\mathbb{D}_n$ for odd n is complete!

§ 13.2. n even. In this case, by Exercise 13.4, there are four degree-one representations. These are the group homomorphisms defined as follows: For $j \in \{1,2,3,4\}$, let $\eta_j \colon \mathbb{D}_n \to \mathbb{C}$ be given by

$$\begin{aligned} \eta_1(r) &= 1, & \eta_2(r) &= 1, & \eta_3(r) &= -1, & \eta_4(r) &= -1, \\ \eta_1(s) &= 1, & \eta_2(s) &= -1, & \eta_3(s) &= 1, & \eta_4(s) &= -1. \end{aligned}$$

Of course, η_1 is the trivial character of $\mathbb{D}_n$. By a direct calculation, we compute the values of the other characters:

	1	r	r^2	$\cdots$	$r^{n/2}$	s	sr
η_1	1	1	1	$\cdots$	1	1	1
η_2	1	1	1	$\cdots$	1	-1	-1
η_3	1	-1	1	$\cdots$	$(-1)^{n/2}$	1	$(-1)^{n/2}$
η_4	1	-1	1	$\cdots$	$(-1)^{n/2}$	-1	$(-1)^{n/2+1}$

Assume now that $n = 2k$. We need $\frac{n-1}{2} = k-1$ additional irreducible characters. For $m \in \{1,\dots,k-1\}$, let $\omega_m = e^{2\pi i m/k}$ and

$$\rho_m \colon \mathbb{D}_n \to \mathbf{GL}_2(\mathbb{C}), \quad r \mapsto \begin{pmatrix} \omega_m & 0 \\ 0 & \omega_m^{-1} \end{pmatrix}, \quad s \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Each ρ_m is a group homomorphism (see Exercise 13.5). A direct calculation produces the values of the character χ_m of ρ_m.

	1	r	r^2	$\cdots$	$r^{n/2}$	s	sr
χ_m	1	$\omega_m + \omega_m^{-1}$	$\omega_m^2 + \omega_m^{-2}$	$\cdots$	$\omega_m^{n/2} + \omega_m^{-n/2}$	0	0

In the same way that we constructed the character table when n is odd, we now need to verify that we have constructed $\frac{n+6}{2}$ irreducible characters of $\mathbb{D}_n$.

13.8. Exercise. Prove that we have constructed $\frac{n+6}{2}$ irreducible characters of $\mathbb{D}_n$.

14. Project: Hurwitz' theorem

We know that $x^2y^2=(xy)^2$ holds for all $x,y\in\mathbb{R}$. Fibonacci found the identity

$$(x_1^2+x_2^2)(y_1^2+y_2^2)=(x_1y_1-x_2y_2)^2+(x_1y_2-x_2y_1)^2. \tag{14.1}$$

Euler and Hamilton independently found a similar identity:

$$(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2)=z_1^2+z_2^2+z_3^2+z_4^2,$$

where

$$\begin{aligned} z_1&=x_1y_1-x_2y_2-x_3y_3-x_4y_4,\\ z_2&=x_1y_2+x_2y_1+x_3y_4-x_4y_3,\\ z_3&=x_1y_3-x_2y_4+x_3y_1+x_4y_2,\\ z_4&=x_1y_4+x_2y_3-x_3y_2+x_4y_1. \end{aligned} \tag{14.2}$$

Cayley found a similar identity for sums of eight squares. Are there other identities of this type? Hurwitz proved that this is not the case.

The question can be reformulated as follows. For which n does there exist a bilinear map $\mathbb{R}^n\times\mathbb{R}^n\to\mathbb{R}^n$, $(x,y)\mapsto xy$, such that

$$\|xy\|=\|x\|\|y\|$$

for all $x,y\in\mathbb{R}^n$? Here, of course, we use the standard notation

$$\|(x_1,\dots,x_n)\|=\sqrt{x_1^2+\cdots+x_n^2}.$$

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

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

then the following statements hold:

1) $|G|=2^n$.
2) $[G,G]=\{1,\epsilon\}$. *In particular, G has exactly 2^{n-1} degree-one representations.*
3) *If $g\notin Z(G)$, then the conjugacy class of g is $\{g,\epsilon g\}$.*
4) $Z(G)=\{1,\epsilon,x_1\cdots x_{n-1},\epsilon x_1\cdots x_{n-1}\}$.
5) *G has $2^{n-1}+2$ conjugacy classes.*
6) *G has two irreducible representations of degree $2^{\frac{n-2}{2}}>1$.*

Proof. Let us prove 1) and 2). Note that $\epsilon\in Z(G)$, as $\epsilon=x_i^2$ for all $i\in\{1,\dots,n-1\}$. Since $n-1>2$, $[x_1,x_2]=\epsilon$. Hence $\epsilon\in[G,G]$. Moreover, $G/\langle\epsilon\rangle$ is abelian. Thus $[G,G]=\langle\epsilon\rangle$. Since $G/[G,G]$ is elementary abelian of order 2^{n-1}, it follows that $|G|=2^n$.

We now prove 3). Let $g\in G\setminus Z(G)$ and $x\in G$ be such that $[x,g]\neq 1$. Then $[x,g]=\epsilon$ and $xgx^{-1}=\epsilon g$.

To prove 4) let $g\in G$. Write

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

where $a_j\in\{0,1\}$ for all $j\in\{1,\dots,n-1\}$. If $g\in Z(G)$, then $gx_i=x_ig$ for all i. Hence $g\in Z(G)$ if and only if

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

Since $x_i x_j^{a_j} x_i = \epsilon^{a_j} x_j^{a_j}$ whenever $i \neq j$ and $\epsilon \in Z(G)$, the element g is central if and only if

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

for all $i \in \{1, \dots, n-1\}$. In particular,

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

for all $k \neq i$. Therefore $a_i \equiv a_k \bmod 2$ for all $i, k \in \{1, \dots, n-1\}$. Thus $a_1 = \cdots = a_{n-1}$ and $Z(G) = \{1, x_1 \cdots x_{n-1}, \epsilon, \epsilon x_1 \cdots x_{n-1}\}$.

To prove 5) we use the class equation:

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

It follows that G has $N + 4 = 2^{n-1} + 2$ conjugacy classes.

Finally we prove 6). Since G has exactly 2^{n-1} degree-one representations (because $|G/[G,G]| = 2^{n-1}$) and has $2^{n-1} + 2$ conjugacy classes, it follows from

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

that G has two irreducible representations of degrees $f_1 = f_2 = 2^{\frac{n-2}{2}} > 1$. □

14.2. Example. The formulas (14.2) give a representation for the group G of the previous lemma. Write each z_i as

$$z_i = \sum_{k=1}^{4} a_{1k}(x_1, \dots, x_4) y_k.$$

Let A be a matrix such that $A_{ij} = a_{ij}(x_1, \dots, x_4)$, that is

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

The matrix A can be written as $A = A_1 x_1 + A_2 x_2 + A_3 x_3 + A_4 x_4$, where

$$A_1 = \begin{pmatrix} 1 &&& \\ & 1 && \\ && 1 & \\ &&& 1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} & -1 && \\ 1 &&& \\ &&& -1 \\ && 1 & \end{pmatrix}, \quad A_3 = \begin{pmatrix} && -1 & \\ &&& 1 \\ 1 &&& \\ & -1 && \end{pmatrix}, \quad A_4 = \begin{pmatrix} &&& -1 \\ && -1 & \\ & 1 && \\ 1 &&& \end{pmatrix}.$$

For $i \in \{1, \dots, 4\}$ let $B_i = A_i^T A_4$. Then $B_i = -B_i^T$ and $B_i^2 = -I$ for all $i \in \{1, 2, 3\}$. Moreover, $B_i B_j = -B_j B_i$ for all $i, j \in \{1, 2, 3\}$ and $i \neq j$. The group generated by $\{B_1, B_2, B_3\}$ has 2^3 element, all of them of the form

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

for $k_j \in \{0, 1\}$. This group provides an example of the group G of Lemma 14.1.

14.3. Theorem (Hurwitz). *If there is an identity of the form*

$$(x_1^2 + \cdots + x_n^2)(y_1^2 + \cdots + y_n^2) = z_1^2 + \cdots + z_n^2, \tag{14.3}$$

where the x_j's and the y_j's are real numbers and each z_k is a bilinear function in the x_j's and the y_j's, then $n \in \{1, 2, 4, 8\}$.

Proof. Without loss of generality, we may assume that $n > 2$. For $i \in \{1, \dots, n\}$ let

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

where the a_{ik}'s are linear functions. Then

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

for all $i \in \{1, \dots, n\}$. Using these expressions for each z_i in (14.3) and comparing coefficients,

$$\sum_{i=1}^{n} a_{ik}(x_1, \dots, x_n) a_{il}(x_1, \dots, x_n) = \delta_{k,l}(x_1^2 + \cdots + x_n^2), \tag{14.4}$$

where $\delta_{k,l}$ is the usual Kronecker's map. Let A be the $n \times n$ matrix given by

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

Then

$$AA^T = (x_1^2 + \cdots + x_n^2)I, \tag{14.5}$$

where I denotes the $n \times n$ identity matrix, as

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

by (14.4). Since each $a_{ki}(x_1, \dots, x_n)$ is a linear function, there exist $\alpha_{ij1}, \dots, a_{ijn} \in \mathbb{C}$ such that

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

Write

$$A = A_1 x_1 + \cdots + A_n x_n,$$

where each A_k is the matrix $(A_k)_{ij} = \alpha_{ijk}$. The formula (14.5) becomes

$$\sum_{i=1}^{n} \sum_{j=1}^{n} A_i A_j^T x_i x_j = (x_1^2 + \cdots + x_n^2)I.$$

Thus

$$A_i A_j^T + A_j A_i^T = 0 \quad i \neq j, \quad A_i A_i^T = I. \tag{14.6}$$

We need n complex square matrices of size $n \times n$ satisfying (14.6). For $i \in \{1, \dots, n\}$ let $B_i = A_n^T A_i$. Then (14.6) turn into

$$B_i B_j^T + B_j B_i^T = 0 \quad i \neq j, \quad B_i B_i^T = I, \quad B_n = I.$$

Set $j=n$ in the first family of equations to obtain $B_i=-B_i^T$ for all $i\in\{1,\dots,n-1\}$. It follows that

$$(14.7)\qquad \begin{aligned} B_i^2&=-I && \text{for all } i\in\{1,\dots,n-1\},\\ [B_i,B_j]&=-I && \text{for all } i,j\in\{1,\dots,n-1\}.\end{aligned}$$

Claim. n is even.

Computing the determinant of $B_iB_j=-B_jB_i$ we obtain that

$$1=\det(B_iB_j)=(-1)^n\det(B_jB_i)=(-1)^n.$$

Hence n is even.

Claim. The group G of the lemma admits a faithful representation $\rho\colon G\to \mathbf{GL}_n(\mathbb{C})$.

By (14.7), there is a well-defined injective group homomorphism ρ such that $x_i\mapsto B_i$ for all $i\in\{1,\dots,n-1\}$ and $\epsilon\mapsto -I$.

Claim. $2^{\frac{n-2}{2}}$ divides n.

Since $\epsilon\in[G,G]$ by Lemma 14.1, every one-dimensional representation satisfies $\epsilon\mapsto 1$. This implies that ρ cannot have degree-one sub representations. In fact, if $W=\langle w\rangle$ is G-invariant subspace of $\mathbb{C}^n$, then $\psi=\rho|_W\colon G\to\mathbf{GL}(W)\simeq\mathbb{C}^\times$ is a representation. In particular,

$$-w=-Iw=\psi_\epsilon(w)=\psi_{[x_i,x_j]}(w)=\psi_{x_i}\psi_{x_j}\psi_{x_i}^{-1}\psi_{x_j}^{-1}(w)=w,$$

a contradiction.

This means that the $\mathbb{C}[G]$-module $\mathbb{C}^n$ decomposes as $\mathbb{C}^n\simeq aS\oplus bT$, where a and b are integers and S and T are simple $\mathbb{C}[G]$-modules of dimension $2^{\frac{n-2}{2}}$. In particular,

$$n=\dim V=\dim(aS\oplus bT)=(a+b)2^{\frac{n-2}{2}}.$$

To finish the proof of the theorem, write $n=2^ab$ for $a\geq 1$ and b an odd integer. Since $\frac{n-2}{2}$ divides n,

$$2^{\frac{n}{2}-1}=2^{\frac{n-2}{2}}\leq n=2^ab.$$

Thus $\frac{n}{2}-1\leq a$ and hence $2^a\leq n\leq 2(a+1)$. It follows that $n\in\{4,8\}$. □

We now present an application, see [43] for more information.

14.4. Theorem. *Let V be a real vector space (with an inner product) of dimension $n\geq 3$. If there exists a bilinear function $V\times V\to\mathbb{R}$, $(v,w)\mapsto v\times w$, such that $v\times w$ is orthogonal both to v and w and*

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

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

Proof. Let $W=V\oplus\mathbb{R}$ with the inner product

$$\langle (v_1,r_1),(v_2,r_2)\rangle=\langle v_1,v_2\rangle+r_1r_2.$$

Note that

$$\begin{aligned}\langle v_1\times v_2+r_1v_2+r_2v_1,\, &v_1\times v_2+r_1v_2+r_2v_1\rangle\\ &=\|v_1\times v_2\|^2+r_1^2\|v_2\|^2+2r_1r_2\langle v_1,v_2\rangle+r_2^2\|v_1\|^2.\end{aligned}$$

Thus

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

where the z_k's are bilinear functions in (v_1, r_1) and (v_2, r_2). By Hurwitz's theorem, we conclude that $n + 1 \in \{4, 8\}$. Hence $n \in \{3, 7\}$. □

In the theorem, if $\dim V = 3$, we obtain the usual cross product. If $\dim V = 7$, let

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

with the inner product

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

It is an exercise to show that

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

satisfies the properties of the theorem.

15. Project: Gallagher's theorem

15.1. Lemma. *Let G be a finite group and N be a normal subgroup of G. Let $\psi \in \operatorname{Irr}(N)$ be such that $I_G(\psi) = G$. Then*

$$\operatorname{Ind}_N^G \psi = \sum_{\chi \in \operatorname{Irr}(G)} e_\chi \chi,$$

where $e_\chi = \langle \operatorname{Res}_N^G, \chi \rangle$. In particular,

$$\sum_{\chi \in \operatorname{Irr}(G)} e_\chi^2 = (G : N).$$

Proof. Write $\operatorname{Ind}_N^G \psi$ as

$$\operatorname{Ind}_N^G \psi = \sum_{\chi \in \operatorname{Irr}(G)} e_\chi \chi,$$

where by Frobenius' reciprocity $e_\chi = \langle \chi, \operatorname{Ind}_N^G \psi \rangle = \langle \operatorname{Res}_N^G \chi, \psi \rangle$. On the one hand, by Clifford's theorem, $\operatorname{Res}_N^G \chi = e_\chi \psi$ (because $I_G(\psi) = G$). In particular,

$$\chi(1) = (\operatorname{Res}_N^G \chi)(1) = e_\chi \psi(1).$$

On the other hand,

$$(G : N)\psi(1) = (\operatorname{Ind}_N^G \psi)(1) = \sum_{\chi \in \operatorname{Irr}(G)} \langle \chi, \operatorname{Ind}_N^G \psi \rangle \chi(1) = \sum_{\chi \in \operatorname{Irr}(G)} e_\chi \chi(1) = \sum_{\chi \in \operatorname{Irr}(G)} e_\chi^2 \psi(1).$$

Since $\psi(1) \neq 0$, it follows that $(G : N) = \sum_{\chi \in \operatorname{Irr}(G)} e_\chi^2$. □

15.2. Lemma. *Let G be a finite group and N be a normal subgroup of G. Let... Then*

$$\chi_L \chi = \operatorname{Ind}_N^G \operatorname{Res}_N^G \chi,$$

where χ_L is the character of the regular representation of G/N.

Proof. On the one hand, in the proof of Theorem 3.6 we have seen a formula to compute the values of the character of the regular representation of a group. In our case,

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

On the other hand,

$$(\operatorname{Ind}_N^G \operatorname{Res}_N^G)(g) = \frac{1}{|N|} \sum_{x \in G} (\operatorname{Res}_N^G \chi)^0(x^{-1}gx).$$

Note that $x^{-1}gx \in N$ if and only if $g \in xNx^{-1} = N$. Thus if $g \notin N$, then $(\operatorname{Ind}_N^G \operatorname{Res}_N^G)(g) = 0$ and this coincides with $\chi_L(g)\chi(g)$, since $\chi_L(g) = 0$. Suppose then that $g \in N$. Then

$$(\operatorname{Ind}_N^G \operatorname{Res}_N^G)(g) = \frac{1}{|N|} \sum_{x \in G} \chi(g) = (G : N)\chi(g) = \chi_L(g)\chi(g).$$ □

15.3. Theorem (Gallagher). *Let G be a finite group and N be a normal subgroup of G. Let $\chi \in \operatorname{Irr}(G)$ be such that $\psi = \operatorname{Res}_N^G \chi \in \operatorname{Irr}(N)$. Then*

$$\operatorname{Ind}_N^G \psi = \sum_{\lambda \in \operatorname{Irr}(G/N)} \lambda(1)(\lambda\chi),$$

where the characters $\lambda\chi$ are pairwise different and irreducible.

Proof. $\square$

15.4. Exercise. Let G be a finite group and N be a normal subgroup of G. Let $\chi \in \operatorname{Irr}(G)$ be such that $\theta = \operatorname{Res}_N^G \chi \in \operatorname{Irr}(N)$. Prove that the map $\psi \mapsto \psi\chi$ yields a bijective correspondence

$$\operatorname{Irr}(G/N) \leftrightarrow \{\eta \in \operatorname{Irr}(G) : \langle \operatorname{Res}_N^G \eta, \theta \rangle > 0\}.$$

Some other topics for final projects

We collect here some topics for final presentations. Some topics can also be used as bachelor or master theses.

Kolchin's theorem. If V is a finite-dimensional complex vector space and G is a subgroup of $\mathbf{GL}(V)$ such that every element g of G is unipotent (i.e., $g-1$ is a nilpotent linear transformation), then there exists a basis of V in which all the element of G are represented by upper triangular matrices with ones on the diagonal. See my notes for Associative Algebra) or [**2**, Chapter 2].

Staircase groups. This topic describes a situation similar to that of Kolchin's theorem (see the course Associative Algebra), but more general. See [**2**, Chapter 5].

Solvable and nilpotent groups. The character table of a finite group detects solvability and nilpotency of groups, see [**2**, Chapter 6].

Characters of $\mathbf{GL}_2(q)$ and $\mathbf{SL}_2(q)$. One possible topic is the character table of $\mathbf{GL}_2(q)$, see [**35**, §5.2]. Alternatively, one can present the character table of the group $\mathbf{SL}_2(p)$ following Humphreys's paper [**18**]. The character theory of $\mathbf{SL}_2(q)$ appears in [**35**, §5.2], see [**4**, Chapter 20] for details.

Representations of the symmetric group. See for example [**35**, §10] and [**10**].

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 [**10**, 4] and [**35**, §11].

Fourier analysis on finite groups. See [**35**, §5] for a very elementary approach and some basic applications. Other applications appear in [**37**].

Mackey's irreducibility criterion. It is not at all clear that induction of an irreducible character will produce an irreducible character. In fact, inducing the trivial character of the trivial subgroup to the whole group produces the regular representation, which in general is not irreducible. Mackey found a criterion that describes when an induced character is irreducible. See [**35**, §8.3].

McKay's conjecture. Prove McKay's conjecture 5.1 for all sporadic simple groups. This was first proved by Wilson in [**44**]. Note that for some "small" sporadic simple groups this can be done with the script presented in §5.1. However, for several sporadic simple groups a different approach is needed. One needs to know the structure of normalizers.

Hirsh's theorem. In [**17**] Hirsch found a generalization of Burnside's Theorem 10.7. If G is a finite group and d is the greatest common divisor of all the numbers p^2-1, where the p's are prime divisors of $|G|$ and r the number of conjugate sets in G. Then

$$|G| \equiv \begin{cases} r \bmod 2d & \text{if } |G| \text{ odd},\\ r \bmod 3 & \text{if } |G| \text{ even and } \gcd(|G|,3)=1.\end{cases}$$

The proof is elementary and does not use character theory. Is it possible to prove Hirsch's theorem using characters?

Irreducible characters of groups of order pq. Let G be a non-abelian group of order pq, where p and q are prime numbers with $p > q$. Then $q \mid p-1$ and G is a Frobenius group (see Exercise 8.11). The character table of Frobenius groups of order pq can be found in [**26**, Chapter 25].

Irreducible characters of the simple group of order 168. The smallest non-abelian simple group is $\mathbb{A}_5$, of order 60. The next smallest is a certain group of order 168. The character table of this group can be found in [**26**, Chapter 27].

Irreducible characters of semidirect products. What can be said about irreducible characters of semidirect products? The case of semidirect products by abelian groups is treated in [**33**, Section 8.2].

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] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I: The user language. *J. Symb. Comput.*, 24(3-4):235–265, 1997.

[6] P. A. Damianou. Monic polynomials in $\mathbf{Z}[x]$ with roots in the unit disc. *Amer. Math. Monthly*, 108(3):253–257, 2001.

[7] B. Fein, W. M. Kantor, and M. Schacher. Relative Brauer groups. II. *J. Reine Angew. Math.*, 328:39–57, 1981.

[8] W. Feit and J. G. Thompson. Solvability of groups of odd order. *Pacific J. Math.*, 13:775–1029, 1963.

[9] P. Flavell. Finite groups in which every two elements generate a soluble subgroup. *Invent. Math.*, 121(2):279–285, 1995.

[10] 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.

[11] G. Gonthier, A. Asperti, J. Avigad, and et al. A machine-checked proof of the odd order theorem. In *Interactive theorem proving*, volume 7998 of *Lecture Notes in Comput. Sci.*, pages 163–179. Springer, Heidelberg, 2013.

[12] G. Greiter. A simple proof for a theorem of Kronecker. *Amer. Math. Monthly*, 85(9):756–757, 1978.

[13] R. Guralnick and D. Wan. Bounds for fixed point free elements in a transitive group and applications to curves over finite fields. *Israel J. Math.*, 101:255–287, 1997.

[14] R. M. Guralnick, M. W. Liebeck, E. A. O'Brien, A. Shalev, and P. H. Tiep. Surjective word maps and Burnside's $p^a q^b$ theorem. *Invent. Math.*, 213(2):589–695, 2018.

[15] R. M. Guralnick and G. R. Robinson. On the commuting probability in finite groups. *J. Algebra*, 300(2):509–528, 2006.

[16] R. M. Guralnick and J. S. Wilson. The probability of generating a finite soluble group. *Proc. London Math. Soc. (3)*, 81(2):405–427, 2000.

[17] K. A. Hirsch. On a theorem of Burnside. *Quart. J. Math. Oxford Ser. (2)*, 1:97–99, 1950.

[18] J. E. Humphreys. Representations of $\mathrm{SL}(2, p)$. *Amer. Math. Monthly*, 82:21–39, 1975.

[19] B. Huppert. *Character theory of finite groups*, volume 25 of *De Gruyter Expositions in Mathematics*. Walter de Gruyter & Co., Berlin, 1998.

[20] I. M. Isaacs. Characters of solvable and symplectic groups. *Amer. J. Math.*, 95:594–635, 1973.

[21] I. M. Isaacs. *Character theory of finite groups*. AMS Chelsea Publishing, Providence, RI, 2006. Corrected reprint of the 1976 original [Academic Press, New York; MR0460423].

[22] I. M. Isaacs. *Finite group theory*, volume 92 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2008.

[23] I. M. Isaacs. *Characters of solvable groups*, volume 189 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2018.

[24] I. M. Isaacs, G. Malle, and G. Navarro. A reduction theorem for the McKay conjecture. *Invent. Math.*, 170(1):33–101, 2007.

[25] I. M. Isaacs and G. Navarro. New refinements of the McKay conjecture for arbitrary finite groups. *Ann. of Math. (2)*, 156(1):333–344, 2002.

[26] G. James and M. Liebeck. *Representations and characters of groups*. Cambridge University Press, New York, second edition, 2001.

[27] M. Le. A divisibility problem concerning group theory. *Pure Appl. Math. Q.*, 8(3):689–691, 2012.

[28] 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.

[29] 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.

[30] G. Malle. The proof of Ore's conjecture (after Ellers-Gordeev and Liebeck-O'Brien-Shalev-Tiep). In *Séminaire Bourbaki. Volume 2012/2013. Exposés 1059–1073. Avec table par noms d'auteurs de 1948/49 à 2012/13*, pages 325–348, ex. Paris: Société Mathématique de France (SMF), 2014.

[31] G. Malle and B. Späth. Characters of odd degree. *Ann. of Math. (2)*, 184(3):869–908, 2016.

[32] P. M. Neumann. A lemma that is not Burnside's. *Math. Sci.*, 4(2):133–141, 1979.

[33] 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.

[34] J.-P. Serre. On a theorem of Jordan. *Bull. Amer. Math. Soc. (N.S.)*, 40(4):429–440, 2003.

[35] B. Steinberg. *Representation theory of finite groups.* Universitext. Springer, New York, 2012. An introductory approach.

[36] N. M. Stephens. On the Feit-Thompson conjecture. *Math. Comp.*, 25:625, 1971.

[37] A. Terras. *Fourier analysis on finite groups and applications*, volume 43 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1999.

[38] J. G. Thompson. Nonsolvable finite groups all of whose local subgroups are solvable. *Bull. Amer. Math. Soc.*, 74:383–437, 1968.

[39] J. G. Thompson. Nonsolvable finite groups all of whose local subgroups are solvable. II. *Pacific J. Math.*, 33:451–536, 1970.

[40] J. G. Thompson. Nonsolvable finite groups all of whose local subgroups are solvable. III. *Pacific J. Math.*, 39:483–534, 1971.

[41] J. G. Thompson. Nonsolvable finite groups all of whose local subgroups are solvable. IV, V, VI. *Pacific J. Math.*, 48, 1973.

[42] V. Vatter. A probabilistic proof of a lemma that is not Burnside's. *Amer. Math. Monthly*, 127(1):63, 2020.

[43] B. Walsh. Classroom Notes: The Scarcity of Cross Products on Euclidean Spaces. *Amer. Math. Monthly*, 74(2):188–194, 1967.

[44] R. A. Wilson. The McKay conjecture is true for the sporadic simple groups. *J. Algebra*, 207(1):294–305, 1998.

Index

Algebra, 3
  semisimple, 3
  unitary, 3
Algebraic integer, 21
Antisymmetric, 46
Augmentation ideal, 4

Brauer–Fowler theorem, 49
Burnside
  theorem, 65, 66
Burnside $p^a q^b$-theorem, 74
Burnside theorem, 33, 34, 74

Cabanes–Späth theorem, 32
Cameron–Cohen
  theorem, 44, 63
Cauchy–Frobenius–Burnside theorem, 36
Cauchy–Schwarz inequality, 40
Center of a character, 70
Character, 12
Character table
  of $\mathbb{A}_5$, 76
  of $\mathbb{S}_5$, 50
Clifford
  correspondence theorem, 69
  theorem, 67
Commutator map, 41
Correspondence theorem
  for characters, 55

Derangements, 44
Derived series, 73
Dixon theorem, 42

Equivalent representations, 8
Euler identity, 83

Fein–Kantor–Schacher theorem, 44
Feit–Thompson
  conjecture, 76
  theorem, 75
Fibonacci identity, 83
First orthogonality relation, 18
Frobenius
  complement, 59
  divisibility theorem, 23
  group, 59
  kernel, 59, 62
  reciprocity theorem, 53
  theorem, 60, 63
  theorem on involutions, 34

Gallagher theorem, 88
Group
  simple, 57
Group algebra, 4
Group commutativity, 39
Guralnick–Liebeck–O'Brien–Shalev–Tiep theorem, 75
Guralnick–Robinson theorem, 43
Guralnick–Wan theorem, 45
Guralnick–Wilson theorem, 43

Hamilton identity, 83
Hurwitz theorem, 85

Inertia subgroup, 68
Involution, 47
Irreducible constituent, 67
Isaacs–Navarro conjecture, 33
Isoclinism, 42
Itô theorem, 71

Jordan theorem, 43

Kegel–Wielandt theorem, 75
Kernel
  of a character, 55
  of a representation, 55
Kronecker theorem, 72

Liebeck–O'Brien–Shalev–Tiep theorem, 35

Malnormal subgroup, 59
Maschke
  theorem, 4
  theorem, multiplicative version, 6
Mathieu group M_9, 57
Matrix representation, 7
McKay conjecture, 32
Module, 3
  semisimple, 3, 4
  simple, 3, 9

Orbital, 37
Ore conjecture, 35
Orthogonality relations, 18, 19

Ramification index, 68
Rank, 37
Real
  character, 65
  conjugacy class, 65
Representation, 7
  completely reducible, 11
  decomposable, 12
  indecomposable, 12
  irreducible, 9

Schur
  divisibility theorem, 24
Schur lemma, 18
Second orthogonality relation, 19
Solomon theorem, 20
Submodule, 3
Symmetric, 46

Tensor power trick, 25
Theorem
  5/8, 40
Thompson theorem, 43, 62
Trivial
  module, 8
  representation, 8

Wildon theorem, 44
Word maps, 75