Complex representations of finite groups

Adrien Deloro

Şirince '23 Winter School

These are lecture notes with exercises for a two week course of $12 \times 2 = 24$ hours given in 2011, 2012 and 2023 at the Nesin Matematik Köyü in Şirince, Turkey. They should be accessible to a 4th year student in mathematics; syllabus and prerequisites are described below. I wish to thank Yiğithan Tamer for his many questions and suggestions.

If found with flaws or mistakes, this document compiled on 3rd February 2023 should be returned to adrien.deloro@imj-prg.fr. Please mention the date.

Contents

Each section corresponds to a lecture of 2 hours, with the introduction fitting into § 1. The material is very standard. §§ 1–5 is one block; § 2 and § 3 may be exchanged. The exercise session § 6 can be skipped, but at the risk of losing practical understanding of phenomena. The three blocks §§ 7–8, §§ 9–10, and §§ 11–12 may be swapped freely; however § 10 uses some material from § 7. • The optional (and untaught) § 13 is a module-theoretic rephrasing of §§ 1–5. Turkish students tend to be familiar with module terminology early in their curriculum. If I were to teach the course again, I might opt for module language and introduce the group algebra as soon as § 1.

Introduction

Group theory is the natural language for symmetries and was promoted as such. As a matter of fact and contrary to modern-style expositions, groups first emerged as groups of symmetries. Some symmetries (not to be mistaken for reflections) have undisputed geometric origin, as in Klein's *Erlanger Programm*. Some are more combinatorial or algebraic in nature, as in Galois' theory of polynomial equations. In either case, mathematical practice is full of groups of transformations, viz. of group actions. In the XIX$^{\text{th}}$ century, groups were sets of bijections preserving some structure. 'Abstract' groups were introduced later, around Burnside's time, in order to achieve some unification and for intrinsic interest.

The purpose of representation theory is to return to 'concrete' groups, viz. groups acting somewhere. Permutation group theory embeds group theory into combinatorics, thus yielding counting arguments. But (linear) representation theory even embeds group theory into linear algebra. There one conveniently relies on geometric intuition.

Just like a group action of G is simply a morphism $G \to \mathrm{Sym}(X)$ for some set X, a linear representation is simply a morphism from G to $\mathrm{GL}(V)$ for some vector space. What is remarkable is that to some extent, G 'is' the class of its representations. (There is almost some phenomenological lesson here: an abstract object is entirely determined by its concrete manifestations.) Equally importantly, complex representations of finite groups are themselves determined by some number-theoretic functions called *characters*. As a result, the amount of group-theoretic information encoded in characters is beyond first expectations; the strength of Frobenius' character theory is a miracle.

The course will describe this theory, with some of its most classical and celebrated applications to 'pure' finite group theory. All the material here is extremely standard; neither the exposition nor the choice of contents has any claim to originality. (See the *Further reading* section for deeper sources.) Before you start with the notes, let me recommend a lovely survey by a major contributor to the topic.[1]

Prerequisites

The class is for advanced undergraduate or graduate students.

Algebraic number theory: Almost none. The characteristic of a field; algebraically closed fields. It is safe to assume $\mathbb{K} = \mathbb{C}$ everywhere. (See 'Note on fields' below.)

Group theory: Prerequisites corresponding to a full first course in pure group theory. Groups, subgroups, normal subgroups and quotient groups; morphisms and factorisation; cosets and Lagrange's theorem on orders; conjugation and centralisers; group actions, stabilisers, orbits. Advanced topics will occasionally involve semidirect products.

I shall use $x^y = y^{-1}xy$ for conjugacy; a typical conjugacy class will be denoted by γ. I reserve c for left cosets, viz. subsets of the form $c = aH = \{ah : h \in H\}$ whenever $H \leq G$ is a subgroup.

Linear algebra: Finite-dimensional vector spaces; linear maps, eigenvalues and trace of an endomorphism; projectors; linear forms, dual space; bilinear forms, non-degenerate bilinear forms, symmetric forms, Hermite-symmetric forms and complex scalar products. The course tends to avoid bases and matrices but prefers 'intrinsic' arguments, so an abstract course in linear algebra is a prerequisite.

Module theory: Terminology helps, but no knowledge of module theory is required. Familiarity with the tensor product is not required, as it will be briefly discussed.

[1] C. Curtis, *Representation theory of finite groups: From Frobenius to Brauer*. Mathematical Intelligencer 14, No. 4, pp. 48–57, 1992.

Note on fields. Most arguments need assumptions both on the characteristic of $\mathbb{K}$ and its algebraic closedness.

Technically the conjunction (characteristic 0 and algebraically closed) defines the class ACF_0 of algebraically closed fields of characteristic 0. Two examples are the field of complex numbers $\mathbb{C}$ and the field of algebraic numbers, viz. the algebraic closure $\overline{\mathbb{Q}}$ of the rationals inside the complex field. Characteristic 0 theory naturally takes place over number fields, viz. over finite extensions of $\mathbb{Q}$. Now every number field embeds into $\overline{\mathbb{Q}}$, so into $\mathbb{C}$. (Moreover, $\mathbb{C}$-vector spaces bear additional 'Hermite structure', also known as complex scalar products. This is the reason why working over $\mathbb{C}$ is so efficient.)

The beginner can safely assume $\mathbb{K} = \mathbb{C}$ throughout. It is however a good exercise to understand what assumptions are needed in each theorem, so we discuss characteristics a little.

Most of the theory works similarly provided $\operatorname{char}\mathbb{K}$ *is not a prime factor of* $|G|$; we call this $\mathbb{K}$ *has coprime characteristic with respect to* G. One could introduce for each finite G the class $\mathrm{ACF}_{|G|^\perp}$ of algebraically closed fields of characteristic coprime to $|G|$, viz. of good fields. For brevity, a *good field* will be an algebraically closed field of coprime characteristic. Hence 'algebraically closed of characteristic 0' implies good.

Definition. Let G be a finite group and $\mathbb{K}$ be a field.

- $\mathbb{K}$ has *coprime characteristic* with respect to G if ($\operatorname{char}\mathbb{K} = 0$ or $\operatorname{char}\mathbb{K}$ does not divide $|G|$).
- $\mathbb{K}$ is *good* if it is algebraically closed of coprime characteristic.

Remarks.

- Coprimality makes sense only for finite G; so does goodness. Almost nothing remains of the theory for infinite G. *There is no general representation theory of abstract infinite groups.*
- Because the characteristic of a field is 0 or a prime number, this is equivalent to: $\operatorname{char}\mathbb{K}$ is 0 or does not divide the *exponent* $\exp G$, which is the least common multiple of orders of elements of G.
- The fields $\overline{\mathbb{Q}}$, $\mathbb{C}$ are universally good (viz. independently of G).

1 Representations

Abstract. This section is mostly terminology. § 1.1 introduces the main objects: *representations*. These simply consist in an action on some vector space. § 1.2 discusses subrepresentations, and we stress the importance of *irreducible representations*. Finally § 1.3 describes *morphisms of representations*.

1.1 Representations

1.1.1. Definition. Let G be a group and $\mathbb{K}$ be a field.

- A *linear representation of* G *in a* $\mathbb{K}$*-vector space* V is a morphism $\rho\colon G \to \mathrm{GL}(V)$.
- A *linear representation of* G *over* $\mathbb{K}$, or $\mathbb{K}$*-linear representation*, is a pair (V, ρ) as above; one often omits V or ρ from notation.

  (Omitting V is less ambiguous than omitting ρ. Common practice can do either.)

1.1.2. Remarks.

- In the notation above, let $g \in G$ and $v \in V$. Then $\rho(g) \in \mathrm{GL}(V)$, so $\rho(g)(v) \in V$. As alternatives to this clumsy notation, one may write:
  - $\rho(g) \cdot v$ (useful if there are several representations),
  - $g * v$ (useful to distinguish operators from vectors),
  - $g \cdot v$, or simply gv (useful to save time).
- By definition of a morphism, one has $\rho(1) = \mathrm{Id}_V$ and $\rho(gh^{-1}) = \rho(g) \circ \rho(h)^{-1}$.
- Tradition calls *degree* of the representation the cardinal number $\deg \rho = \dim V$.
- A linear representation ρ of G induces an ijective linear representation of $G/\ker\rho$.
- Tradition calls *faithful* an injective representation, viz. one with $\ker\rho = \{1\}$.

1.1.3. Examples.

- The *trivial representation* is:

$$\begin{array}{rccc} \mathrm{triv}\colon & G & \to & \mathrm{GL}(\mathbb{K}) \\ & g & \mapsto & 1, \end{array}$$

  with dimension 1.

- Let V be the $\mathbb{K}$-vector space with dimension $|G|$ and basis $\mathcal{B} = \{e_g : g \in G\}$. For $g \in G$ we define $\mathrm{reg}(g)$ on the basis $\mathcal{B}$ by letting $\mathrm{reg}(g)(e_h) = e_{g \cdot h}$. Then we extend linearly, meaning we let: $\mathrm{reg}(g)(\sum \lambda_h e_h) = \sum \lambda_h e_{gh}$. This defines the *regular representation*:

$$\begin{array}{rccc} \mathrm{reg}\colon & G & \to & \mathrm{GL}(V) \\ & g & \mapsto & \mathrm{reg}(g). \end{array}$$

  (Check that one does have $\mathrm{reg}(g_1 g_2^{-1}) = \mathrm{reg}(g_1) \circ (\mathrm{reg}(g_2))^{-1}$ in $\mathrm{GL}(V)$.)

  From § 13 on, we shall drop unnecessary symbols and simply write g for e_g.

- Technically, the above is the *left*-regular representation. (See exercice 1.4.4.)
- The regular representation is a special case of a more general construction. Let G act on some set X by $g * x$. Let V be the vector space with dimension $\#X$ and basis $\mathcal{B} = \{e_x : x \in X\}$. Now define $\mathrm{perm}(g)$ on the basis $\mathcal{B}$ by: $\mathrm{perm}(g)(e_x) = e_{g*x}$, then extend linearly. This defines the *permutation representation* associated to the *permutation group* (G, X). Its kernel is exactly the kernel of the action.
- The regular representation is thus the permutation representation associated to the left-regular, 'Cayley' group action of G on itself: $g * x = gx$.

  It is injective. Indeed, $\mathrm{reg}(g) = \mathrm{Id}_V$ implies $\mathrm{reg}(g)(e_1) = \mathrm{Id}(e_1) = e_1$ while $\mathrm{reg}(g)(e_1) = e_g$. So $g = 1$ and $\ker \mathrm{reg} = \{1\}$.

- *Not all* representations are permutation representations, so the topic does not reduce to group actions.

1.1.4. Remarks (even more general representations)**.**

- One may represent other algebraic structures; for instance, a representation of an (associative) ring R in a vector space V is simply a ring morphism $R \to \mathrm{End}(V)$.

  Actually, $\mathbb{K}$-linear representations of a group G, correspond to representations of the 'group algebra' $\mathbb{K}[G]$, by taking $\rho: G \to \mathrm{GL}(V)$ to the linear extension $\hat{\rho}: \mathbb{K}[G] \to \mathrm{End}(V)$. (This is discussed in § 13.)

- One may also represent algebraic structures in more general modules than vector spaces. For instance, a representation of a group G in an abelian group A is simply a morphism $G \to \mathrm{Aut}(A)$. (This can be interesting, and bring new phenomena, if A is for instance the torsion subgroup of the circle group $\mathbb{S}^1 \simeq \mathrm{SO}_2(\mathbb{R})$, which is no vector space.) Likewise, one may represent associative rings, or even Lie rings, dropping linearity.

- Linear algebra gives intuition and tools, and linear representations of a given group G already encode much information about it.

The purpose of this course is to give general notions on *linear* representations of *finite* groups in *finite-dimensional* vector spaces *over good fields*, such as $\mathbb{C}$. This is a well-chartered territory, but it has striking applications. The following basic lemma is used throughout.

1.1.5. Lemma. *Let G be a finite group and $\mathbb{K}$ be a good field. Let $\rho: G \to \mathrm{GL}(V)$ be a $\mathbb{K}$-linear, finite-dimensional representation. Then each $\rho(g)$ is diagonalisable, and its eigenvalues are roots of unity.*

Proof. Each $g \in G$ has finite order $g^k = 1$, so $\rho(g)$ is annihilated by the polynomial $X^k - 1$, which is split with simple roots over $\mathbb{K}$. Moreover, eigenvalues of $\rho(g)$ must satisfy $X^k - 1 = 0$ in $\mathbb{K}$: so they are roots of unity. □

1.1.6. Remark. In general the various $\rho(g)$'s cannot be diagonalised simultaneously.

1.2 Subrepresentations and irreducibility

We discuss subobjects.

1.2.1. Definition. Let G be a group and $\mathbb{K}$ be a field. Let (V, ρ) be a $\mathbb{K}$-linear representation.

- A *subrepresentation* is a $\mathbb{K}$-linear subspace $W \leq V$ which is also *G-invariant*, viz. $(\forall g \in G)(\forall w \in W)(g \cdot w \in W)$.

  (This is the same as a $\mathbb{K}[G]$-submodule; see § 13.2.)

- A nonzero representation V is *irreducible* if the only G-invariant subspaces are $\{0\}$ and V.

  (This is the same as simplicity as a $\mathbb{K}[G]$-module; see § 13.1.)

Notice that by convention, $\{0\}$ is not irreducible (similar to '1 is not a prime').

1.2.2. Examples.

1. If A is an abelian group and $\mathbb{K}$ is an algebraically closed field, then every finite-dimensional, $\mathbb{K}$-linear representation of A is actually 1-dimensional. This is an important fact (exercise 1.4.3).

2. This need not hold over arbitrary $\mathbb{K}$. Let $G = \mathrm{SO}_2(\mathbb{R})$ be the real unit circle, acting by rotations on $V = \mathbb{R}^2$. This representation is irreducible because no vector line is invariant under rotations.

Irreducible representations are the building blocks, the 'atoms' of more elaborate representations (accordingly thought of as molecules). This analogy underlies the entire theory over good fields and is developed in §§ 3–4.

1.2.3. Lemma. *Let G be a finite group and $\mathbb{K}$ be a field.*

(i) Every irreducible linear representation is finite-dimensional.

(ii) Every nonzero linear representation contains an irreducible representation.

Proof.

(i) Let V be irreducible. Let $v \in V \setminus \{0\}$. Now the set $X = \{g \cdot v : g \in G\}$ is finite, hence spans a finite-dimensional subspace $W \leq V$. Any $g \in G$ acts on X, so it leaves W invariant. Hence $W \leq V$ is a subrepresentation. Since $0 \neq v \in W$, irreducibility implies $V = W$, which is finite-dimensional.

(ii) Let $V \neq 0$ be arbitrary. Here again, V contains a finite-dimensional subrepresentation W. Now a finite-dimensional subrepresentation of minimal dimension is irreducible. □

1.2.4. Remarks.

- Some infinite groups do not have a non-trivial, finite-dimensional representation (even reducible). See exercise 1.4.5.
- Some groups, and even some finite groups, do not have a injective irreducible representation. See exercise 1.4.6.
- Still, every group has a injective representation—for instance the regular one.

1.2.5. Remark (quotient representations)**.** If V is a $\mathbb{K}$-linear representation and $W \leq V$ a subrepresentation, then the quotient group V/W naturally bears the structure of a $\mathbb{K}$-linear representation of G, called *quotient representation*.

Due to Maschke's splitting phenomenon discussed in § 3.2, quotient representations turn out to be avoidable in a first course, very much like quotient vector spaces are usually omitted from basic treatments of linear algebra.

1.3 Morphisms and isomorphisms of representations

We discuss arrows.

1.3.1. Definition. Let G be a group and $\mathbb{K}$ be a field. Let (V_1, ρ_1) and (V_2, ρ_2) be two $\mathbb{K}$-linear representations of G.

- A *morphism of representations*, also called a *G-covariant morphism*, is a function $f\colon V_1 \to V_2$ which is both $\mathbb{K}$-linear and compatible with G, viz. in obvious notation:

$$f(\rho_1(g)\cdot v_1) = \rho_2(g)\cdot f(v_1).$$

  In lighter notation, this rewrites as $f(g\cdot v_1) = g\cdot f(v_2)$.

- This is the same as a morphism of $\mathbb{K}[G]$-modules. (See § 13.2.)

- We let $\mathrm{Hom}_{\mathbb{K}[G]}(\rho_1,\rho_2)$ be the set of morphisms of representations.

  More casual notations are $\mathrm{Hom}_{\mathbb{K}[G]}(V_1,V_2)$, or $\mathrm{Hom}_G(\rho_1,\rho_2)$, or $\mathrm{Hom}_G(V_1,V_2)$.

- If $V_1 = V_2 = V$ (implicitly we request $\rho_1=\rho_2=\rho$; see remarks 1.3.3), we simply write $\mathrm{End}_{\mathbb{K}[G]}(\rho)$. (More casual: $\mathrm{End}_G(\rho)$ or $\mathrm{End}_G(V)$.)

  An alternative notation could be $C_{\mathrm{End}_{\mathbb{K}}(V)}(G)$, because it consists of those $\mathbb{K}$-linear maps $f\in\mathrm{End}_{\mathbb{K}}(V)$ which commute with the 'Hom' action of G, in the sense of § 2.4.

- An *isomorphism* is a bijective morphism. Notice that the inverse of an isomorphism is an isomorphism.

- Tradition calls *equivalence* an isomorphism of representations.

1.3.2. Remark. A $\mathbb{K}$-linear map $f\colon V_1\to V_2$ is G-covariant iff for all $g\in G$ the following diagram is *commutative*, viz. the two possible compositions define the same morphism:

$$\begin{tikzcd} V_1 \arrow[r, "f"] \arrow[d, "\rho_1(g)"'] & V_2 \arrow[d, "\rho_2(g)"] \\ V_1 \arrow[r, "f"] & V_2. \end{tikzcd}$$

1.3.3. Remarks.

- $\mathrm{Hom}_{\mathbb{K}[G]}(V_1,V_2)$ is a slightly ambiguous notation: what matters is not V_i, but truly (V_i,ρ_i). Hence $\mathrm{Hom}_{\mathbb{K}[G]}(\rho_1,\rho_2)$ is clearer but one has to accept 'arrows between arrows'.

- In more modern notation, $(\rho_1\to\rho_2)$ would be in order, meaning: those arrows from ρ_1 to ρ_2, being well understood that ρ_1,ρ_2 live in the category of $\mathbb{K}[G]$-modules. Another option is $(\rho_1\to\rho_2\colon\mathbb{K}[G]\text{-}\mathbf{Mod})$, for *those arrows in the category* $\mathbb{K}[G]$-**Mod**.

1.3.4. Remark. Isomorphisms are classically denoted by $\simeq$. Since there will be a constant tension between isomorphisms of underlying vector spaces, and isomorphisms of representations (which are stronger), we prefer explicit notation.

The notion of an isomorphism is relative to a category. For isomorphisms of $\mathbb{K}$-vector spaces, we write $V_1\simeq V_2\quad[\mathbb{K}\text{-}\mathbf{Mod}]$ ('isomorphism of $\mathbb{K}$-modules'). For isomorphims of $\mathbb{K}$-linear representations of G, we write $V_1\simeq V_2\quad[\mathbb{K}[G]\text{-}\mathbf{Mod}]$ ('isomorphism of $\mathbb{K}[G]$-modules'). (See § 13.)

1.3.5. Notation. Let G a group and $\mathbb{K}$ be a field. Let $\mathrm{Irr}_{\mathbb{K}}(G)$ denote the class of the irreducible, $\mathbb{K}$-linear representations of G *up to isomorphism*.

Truly elements of $\mathrm{Irr}_{\mathbb{K}}(G)$ are not representations, more isomorphism classes.

1.3.6. Remarks.

- In general, $\mathrm{Irr}_{\mathbb{K}}(G)$ need not be finite. But *if G is finite then so is* $\mathrm{Irr}_{\mathbb{K}}(G)$. This is proved in exercise 1.4.7.
- Actually *if G is finite and $\mathbb{K}$ is good* then $\#\,\mathrm{Irr}_{\mathbb{K}}(G)$ is the number of conjugacy classes in G, as proved in Theorem 5.1.1. In particular, $\#\,\mathrm{Irr}_{\mathbb{C}}(G) = \#\,\mathrm{Conj}(G)$.
- For algebraically closed $\mathbb{K}$ of characteristic dividing $|G|$, the number $\#\,\mathrm{Irr}_{\mathbb{K}}(G)$ takes another value found by Brauer[2]. For non-algebraically closed $\mathbb{K}$, matters are more involved.

1.4 Exercises

1.4.1. Exercise. *Let $G = \mathrm{Sym}(3)$, which is generated by (12) and (123). Let $V \simeq \mathbb{C}^2$ have basis $\mathcal{B} = (e_1, e_2)$. Now let $\rho((12))$ swap e_1 and e_2, while $\rho((123))$ does the following:*

$$\rho((123))(e_1) = e_2 \qquad \textit{and} \qquad \rho((123))(e_2) = -e_1 - e_2.$$

1. *Prove that it defines a linear representation.*
2. *Write the matrix $\mathrm{Mat}_{\mathcal{B}}\, \rho(g)$ for every $g \in G$.*

1.4.2. Exercise. *Let $G = \mathrm{Sym}(n)$ be the symmetric group over n symbols.*

1. *The* sign representation *of G is:*

$$\begin{array}{rccl} \varepsilon\colon & G & \mapsto & \mathrm{GL}(\mathbb{K}^1) \\ & g & \mapsto & \varepsilon(g), \end{array}$$

   where $\varepsilon(g)$ is the usual signature of g. Show that it is a representation.

2. *Let $\rho\colon G \to \mathrm{GL}(V)$ be a $\mathbb{K}$-linear representation. Show that $\rho'(g) = \varepsilon(g)\cdot\rho(g)$ is another $\mathbb{K}$-linear representation. (More generally see* tensor representations, *§ 2.3.)*

1.4.3. Exercise.

1. *Let A be a finite,* abelian *group and $\rho \in \mathrm{Irr}_{\mathbb{C}}(A)$. Show that* $\dim \rho = 1$. *Hint: eigenvalue. Does this generalise to nilpotent groups?*
2. *Let A be an abelian subgroup of a finite group G. Let $\rho \in \mathrm{Irr}_{\mathbb{C}}(G)$. Show that* $\dim \rho \le [G : A]$.
3. *Characterise which finite groups have a* non-trivial, *complex, 1-dimensional representation $\rho \neq$* triv. *Did you use properties of the field?*

1.4.4. Exercise. *The* right-regular *representation is defined as follows. Let V have basis $\{e_g : g \in G\}$. Now let $\mathrm{reg}^{\mathrm{op}}(g)(e_h) = e_{h\cdot g^{-1}}$, and extend linearly. Prove that* reg *and* $\mathrm{reg}^{\mathrm{op}}$ *are isomorphic.*

1.4.5. Exercise. *Let G be a group.*

1. *Prove that the following are equivalent:*

[2] R. Brauer, *Über die Darstellung von Gruppen in Galoisschen Feldern.* Actualités scientifiques et industrielles 195. Hermann & Cie, Paris, 1935.

(i) if $X \subseteq G$ is any subset, there are finitely many $x_1, \dots, x_n \in X$ such that $C_G(X) = C_G(x_1, \dots, x_n)$;

(ii) every ascending chain of centralisers $C_G(X_1) \leq C_G(X_2) \leq \dots$ is stationary;

(iii) every descending chain of centralisers $C_G(X_1) \geq C_G(X_2) \geq \dots$ is stationary.

Hint: $CCC = C$.

2. *A* linear group *is a subgroup of some $\mathrm{GL}_n(\mathbb{K})$ for some integer n and some field $\mathbb{K}$. Prove that every linear group satisfies the above condition. Hint: use $M_n(\mathbb{K})$.*

(*) 3. *Let $\mathrm{Alt}(\mathbb{N})$ be the set of permutations of $\mathbb{N}$ with finite support and signature 1. Deduce that every finite-dimensional representation of $\mathrm{Alt}(\mathbb{N})$ is trivial.*

1.4.6. Exercise. *Let $N \simeq C_2^4$ be generated by e_1, e_2, e_3, e_4. Now let $\langle \sigma \rangle \simeq C_3$ act on N as follows:*

$$e_1^\sigma = e_2, \quad e_2^\sigma = e_1 e_2, \quad e_3^\sigma = e_4, \quad e_4^\sigma = e_3 e_4.$$

Let $G = N \rtimes \langle \sigma \rangle$. Show that G has no injective irreducible representation over $\mathbb{C}$. Hint: diagonalise N simultaneously.
Note. *Characterisation of finite groups admitting a injective irreducible representation is a classical topic.*[3]

1.4.7. Exercise. *Let G be a finite group, and let $\mathbb{K}[G]$ denote the left-regular representation.*

1. *Prove that every irreducible representation V is isomorphic to some $V' \leq \mathbb{K}[G]$. Hint: fix a non-zero linear form $\varphi \in V^*$ and consider $f(v) = \sum_{g \in G} \varphi(g^{-1}v) e_g$.*

2. *Suppose that $V_1, \dots, V_r \leq \mathbb{K}[G]$ are pairwise non-isomorphic irreducible representations. Prove that $\sum V_i = \bigoplus V_i$ is a direct sum. Hint: if $V_0 \leq \bigoplus V_i$, consider the projectors $\pi_i \colon V_0 \to V_i$ onto the i^{th} coordinate.*

3. *Deduce that G has finitely many irreducible representations up to isomorphism.*

Note. *With more tools (and provided* $\operatorname{char} \mathbb{K} \nmid |G|$*), there are other arguments relying on the Artin-Wedderburn theorem applied to the algebra $\mathbb{K}[G]$.*

2 Algebraic constructions

Abstract. We build new representations from existing ones. Direct sum representations (§ 2.1) are easily understood. *Dual representations* (§ 2.2) offer the opportunity to return to algebraic duality and dual bases in finite-dimensional spaces. *Tensor representations* (§ 2.3) endow the vector tensor product of two spaces with an action of G. Last, Hom-representations (§ 2.4) connect to dual and tensor constructions. In general, irreducibility is lost.

This section contains almost no representation theory except a couple of definitions (dual representation, tensor representation, Hom representation). There are no assumptions on $\mathbb{K}$. Throughout we pay attention to traces as they will underlie character theory.

[3] W. Gaschütz, *Endliche Gruppen mit treuen absolut-irreduziblen Darstellungen*. Math. Nach. 12, pp. 253-255, 1954.

2.1 Direct sum representation

Direct sum space. The notion of a direct sum space is expected to be familiar.

2.1.1. Definition. Let V_1 and V_2 be two vector spaces over the same field. Their (external) *direct sum* is the vector space $V_1 \oplus V_2$ of pairs (v_1, v_2), equiped with componentwise linear structure.

2.1.2. Remarks.

- V_1 and V_2 naturally embed into $V_1 \oplus V_2$. There, their *internal* direct sum equals $V_1 \oplus V_2$.
- In particular if V_1 has basis $\mathcal{B}_1$ and V_2 has basis $\mathcal{B}_2$, then $V_1 \oplus V_2$ has basis $\mathcal{B}_1 \cup \mathcal{B}_2$.
- Not to be mistaken with the direct product space—though isomorphic as long as only finitely many vector spaces are involved.

Direct sum representation. The simplest possible construction is as follows.

2.1.3. Definition. Let (V_1, ρ_1) and (V_2, ρ_2) be two representations of the same group over the same field. The *direct sum representation* is $(V_1 \oplus V_2, \rho_1 \oplus \rho_2)$ given by:

$$(\rho_1 \oplus \rho_2)(g)_{|V_1} = \rho_1(g) \quad \text{and} \quad (\rho_1 \oplus \rho_2)(g)_{|V_2} = \rho_2(g).$$

This means that g acts on $V_1 \oplus V_2$ componentwise; in finite dimension, one may use 'block matrices'. The following is therefore obvious.

2.1.4. Remark. Let V_1 and V_2 be finite-dimensional representations of G. Then for $g \in G$ one has $\operatorname{tr}(\rho_1 \oplus \rho_2)(g) = \operatorname{tr} \rho_1(g) + \operatorname{tr} \rho_2(g)$.

2.2 Dual representation

Dual space. We first review some properties of the dual space of a vector space, with no reference to representation theory.

2.2.1. Definition. Let V be a $\mathbb{K}$-vector space.

- A *linear form* on V is a linear map $V \to \mathbb{K}$.
- The *dual space* of V is the space V^* of all linear forms on V, equiped with the following linear structure in obvious notation:
  - $(\varphi_1 + \varphi_2)(v) = \varphi_1(v) + \varphi_2(v)$,
  - $(\lambda\varphi)(v) = \lambda\varphi(v)$.

2.2.2. Remark (duality pairing)**.** There is a 'pairing' $V^* \times V \to \mathbb{K}$, given by $\langle \varphi | v \rangle = \varphi(v)$.

Now if $f: V \to V$ is a linear endomorphism, it induces $f^*: V^* \to V^*$ defined by:

$$f^*(\varphi) = \varphi \circ f.$$

Notice that $\langle f^*(\varphi) | v \rangle = \varphi \circ f(v) = \langle \varphi | f(v) \rangle$.

2.2.3. Lemma (and definition: dual basis)**.** *Let V be a finite-dimensional vector space.*

(i) $\dim V^* = \dim V$.

(ii) *If $\mathcal{B} = \{e_1, \dots, e_n\}$ is a basis of V, let $e_i^* \in V^*$ be the linear form such that $e_i^*(e_j) = \delta_{ij}$. Then $\mathcal{B}^* = \{e_1^*, \dots, e_n^*\}$ is a basis of V^*, called the* dual basis.

(iii) *Let $f \in \operatorname{End}(V)$. In the notation above,* $\operatorname{Mat}_{\mathcal{B}^*} f^* = (\operatorname{Mat}_{\mathcal{B}} f)^t$.

(iv) *In the notation above,* $\operatorname{tr} f = \operatorname{tr} f^*$.

Proof.

(i) is a consequence of (ii).

(ii) We prove both linear independence and generation. Suppose $\sum_{i=1}^n \lambda_i e_i^* = 0$, in obvious notation. Then evaluating at each e_j gives $\lambda_j = 0$: whence linear independence.

Now let $\varphi \in V^*$. For $i \in \{1, \dots, n\}$, let $\lambda_i = \varphi(e_i)$. Then notice that $\varphi - \sum \lambda_i e_i^*$ vanishes on $\mathcal{B}$, so on V. Thus $\varphi = \sum \lambda_i e_i^*$, which proves generation. Hence $\mathcal{B}^*$ is a basis of V^*.

(iii) Say $\operatorname{Mat}_{\mathcal{B}} f = M = (m_{i,j})$, so that $\operatorname{Col}_j \operatorname{Mat}_{\mathcal{B}} f = \operatorname{Coord}_{\mathcal{B}} f(e_j)$, viz. $f(e_j) = \sum_i m_{i,j} e_i$. Let $v = \sum_i \lambda_i e_i$. Compute as follows:

$$\begin{aligned}
f^*(e_j^*)(v) &= e_j^*(f(v)) \\
&= (e_j^* \circ f)(\sum_i \lambda_i e_i) \\
&= e_j^*(\sum_i \lambda_i f(e_i)) \\
&= e_j^*(\sum_i \lambda_i \sum_k m_{k,i} e_k) \\
&= \sum_{i,k} \lambda_i m_{k,i} e_j^*(e_k) \\
&= \sum_i \lambda_i m_{j,i} \\
&= \sum_i (M^t)_{i,j} e_i^*(v),
\end{aligned}$$

whence $f^*(e_j^*) = \sum_i (M^t)_{i,j} e_i^*$. This is our claim.

(iv) Obvious from (iii). $\square$

2.2.4. Remark. This no longer holds if $\dim V$ is infinite. One can still define linear forms e_i^*, which remain linearly independent, but they no longer generate V^*.

Dual representation. We now put a G-structure on the dual vector space of a representation of G, in the most natural way.

2.2.5. Definition. Let (V, ρ) be a $\mathbb{K}$-linear representation of G. Its *dual representation* is (V^*, ρ^*), where:

$$\rho^*(g)(\varphi) = \varphi \circ \rho(g)^{-1}.$$

In alternate notation, this rewrites $(g \cdot \varphi)(v) = \varphi(g^{-1}v)$.

2.2.6. Remarks.

- Notice that $\langle \rho^*(g)(\varphi) | \rho(g)(v) \rangle = \varphi \circ \rho(g)^{-1}(\rho(g)v)) = \varphi(v)$, viz. :
$$\langle g \cdot \varphi | g \cdot v \rangle = \langle \varphi | v \rangle .$$
The dual representation is defined precisely in order to preserve the duality pairing.

- Suppose V is finite-dimensional with basis $\mathcal{B}$; let $\mathcal{B}^*$ be the dual basis. Then:
$$\mathrm{Mat}_{\mathcal{B}^*} \rho^*(g) = (\mathrm{Mat}_{\mathcal{B}} \rho(g))^{-t},$$
where $M^{-t} = (M^t)^{-1} = (M^{-1})^t$ is the *inverse-transpose matrix*.

- In the notation above, $\operatorname{tr} \rho^*(g) = \operatorname{tr} \rho(g^{-1})$.

- Important fact: V is irreducible iff V^* is. A general proof is in exercise 2.5.5, but faster proofs in special cases are given in Remarks 3.3.8 and 5.3.2.

2.3 Tensor representation

In this course we only tensor over $\mathbb{K}$, never over $\mathbb{K}[G]$.

Tensor product of vector spaces. Informally speaking, the tensor product converts bilinear maps to linear maps.

2.3.1. Proposition. *Let V_1, V_2 be $\mathbb{K}$-vector spaces over the same field $\mathbb{K}$. Then there is a (unique)* initial *pair (W, β) where W is a $\mathbb{K}$-vector space and $\beta \colon V_1 \times V_2 \to W$ is bilinear.*

This means that there is a unique pair (W, β) as above such that for any other pair (W', β'), one may uniquely factorise $\beta' = h \circ \beta$.

$$\begin{tikzcd} V_1 \times V_2 \arrow[dr, "\beta"] \arrow[dd, "\beta'"'] & \\ & W \arrow[dl, dotted, "\exists! h"] \\ W' & \end{tikzcd}$$

Proof. Say V_i has basis $\mathcal{B}_i$. Let $\mathcal{C} = \mathcal{B}_1 \times \mathcal{B}_2$; let W have basis indexed by $\mathcal{C}$. Map $(b_1, b_2) \in \mathcal{C}$ to the corresponding vector in W and extend bilinearly. This defines β.

We have to check that (W, β) meets the requirements. So let (W', β') be another pair. On $\beta(b_1, b_2)$ we let $h(\beta(b_1, b_2)) = \beta'(b_1, b_2)$. This is well-defined. Then we extend h linearly. So β' factor through β. Moreover we had no other choice.

We now check that (W, β) is unique up to isomorphism. Indeed, if (W', β') is another initial pair, then there are unique h, h' such that $\beta = h' \circ h \circ \beta$. But $\beta = \mathrm{Id}_W \circ \beta$ would have worked as well, so $h' \circ h = \mathrm{Id}_W$. Likewise, $h \circ h' = \mathrm{Id}_{W'}$. So h and h' are linear isomorphism and we are done. $\square$

2.3.2. Definition. In the notation above, one writes $W = V_1 \otimes_{\mathbb{K}} V_2$ and $\beta(v_1, v_2) = v_1 \otimes v_2$. This is called the *tensor product of V_1 and V_2 over $\mathbb{K}$*.

Of course the tensor product is more an isomorphism type than a given realisation; in particular one may always pick bases $\mathcal{B}_1$ and $\mathcal{B}_2$ more adapted to specific problems.

2.3.3. Remarks.

- Write $\mathcal{B}_1 \otimes \mathcal{B}_2 = \mathcal{B}_1 \times \mathcal{B}_2$. This is a basis of $V_1 \otimes V_2$. In particular, $\dim(V_1 \otimes V_2) = \dim V_1 \cdot \dim V_2$.

- Every element of $V_1 \otimes V_2$ is therefore a unique linear combination of basic elements $b_1 \otimes b_2$. However, it is useful to forget about bases. Thus every element is a linear combination of 'elementary tensors' $v_1 \otimes v_2$, but not every element of $V_1 \otimes V_2$ is an elementary tensor. (Physicists call this phenomenon 'intrication'.)

- A remark on the construction. The general notion of a tensor product over a ring R is more involved and requires some factorisation. Since vector spaces are free modules, our construction is (fortunately) much simpler than the general module-theoretic one.

Tensor representation. We now equip the *vector tensor product* of representations with the structure of a representation (viz. a G-action).

2.3.4. Definition. Let G be a group and $\mathbb{K}$ be a field. Let $(V_1, \rho_1), (V_2, \rho_2)$ be two $\mathbb{K}$-linear representations. The *tensor representation* is $(V_1 \otimes_{\mathbb{K}} V_2, \rho_1 \otimes \rho_2)$ where:

$$(\rho_1 \otimes \rho_2)(g)(v_1 \otimes v_2) = (gv_1 \otimes gv_2).$$

2.3.5. Lemma. $\operatorname{tr}(\rho_1 \otimes \rho_2)(g) = (\operatorname{tr} \rho_1(g)) \cdot (\operatorname{tr} \rho_2(g))$.

Proof. Let $\mathcal{B}_1 = \{e_1, \dots, e_p\}$ be a basis of V_1 and $\mathcal{B}_2 = \{f_1, \dots, f_q\}$ be one of V_2; then $\{e_i \otimes f_k\}$ is one of $V_1 \otimes V_2$. By definition there are matrices $M = (m_{i,j})$ and $N = (n_{k,\ell})$ such that:

$$\rho_1(g) \cdot e_j = \sum_i m_{i,j} e_i \quad \text{and} \quad \rho_2(g) \cdot f_\ell = \sum_k n_{k,\ell} f_k.$$

Thus:

$$(\rho_1 \otimes \rho_2)(g) \cdot (e_j \otimes f_\ell) = \sum_{i,k} m_{i,j} n_{k,\ell} (e_i \otimes f_k).$$

Summing diagonal terms, we find:

$$\operatorname{tr}(\rho_1 \otimes \rho_2)(g) = \sum_{j,\ell} m_{j,j} n_{\ell,\ell} = (\sum_j m_{j,j})(\sum_\ell n_{\ell,\ell}) = (\operatorname{tr} \rho_1(g))(\operatorname{tr} \rho_2(g)). \qquad \square$$

2.4 Hom-representation

The definition.

2.4.1. Definition. Let V_1, V_2 be $\mathbb{K}$-vector spaces. Let $\operatorname{Hom}_{\mathbb{K}}(V_1, V_2)$ be the space of linear maps $V_1 \to V_2$, equiped with the following linear structure in obvious notation:

- $(f + g)(v_1) = f(v_1) + g(v_1)$,
- $(\lambda f)(v_1) = \lambda f(v_1)$.

Thus $V^* = \operatorname{Hom}_{\mathbb{K}}(V, \mathbb{K})$.

2.4.2. Definition. Let (V_1, ρ_1), (V_2, ρ_2) be two $\mathbb{K}$-linear representations of G. The *Hom-representation* is $(\mathrm{Hom}_{\mathbb{K}}(V_1, V_2), \rho_{\mathrm{Hom}})$ where:

$$\rho_{\mathrm{Hom}}(g)(f) = \rho_2(g) \circ f \circ \rho_1(g)^{-1} = g \cdot f \cdot g^{-1}.$$

2.4.3. Remark. A $\mathbb{K}$-linear homomorphism $f\colon V_1 \to V_2$ is fixed under the Hom-action of G if and only if $(\forall g)(f \circ \rho_1(g) = \rho_2(g) \circ f)$ if and only if f is a $\mathbb{K}[G]$-morphism. In symbols,

$$C_{\mathrm{Hom}_{\mathbb{K}}(V_1,V_2)}(G) = \mathrm{Hom}_{\mathbb{K}[G]}(V_1, V_2).$$

This simple observation is crucial in character theory (§ 5.2).

Hom and tensors. Let $f\colon V_1 \to V_2$ be linear between finite-dimensional spaces. Suppose V_1 has basis $\mathcal{B} = \{e_1, \ldots, e_n\}$. Then for $x \in V$, one may write $x = \sum \lambda_j e_j$. Now $e_i^*(x) = \lambda_i$, so $x = \sum_j e_j^*(x) e_j$. Notice that this amounts to writing, as functions:

$$\mathrm{Id} = \sum_j e_j^* e_j.$$

Furthermore $f(x) = f\left(\sum_j e_j^*(x) e_j\right) = \sum e_j^*(x) f(e_j)$. Thus as functions from V_1 to V_2 we have:

$$f = \sum_j e_j^* f(e_j).$$

The proper place to deal with the right-hand is the tensor space $V_1^* \otimes V_2$. This motivates the following.

2.4.4. Proposition. *Let V_1, V_2 be two finite-dimensional $\mathbb{K}$-vector spaces.*

(i) There is a natural $\mathbb{K}$-linear isomorphism:

$$\mathrm{Hom}_{\mathbb{K}}(V_1, V_2) \simeq V_1^* \otimes_{\mathbb{K}} V_2 \quad [\mathbb{K}\text{-}\mathbf{Mod}].$$

(ii) If in addition V_1, V_2 are representations of G, then the above is even an isomorphism of representations, viz.:

$$\mathrm{Hom}_{\mathbb{K}}(V_1, V_2) \simeq V_1^* \otimes_{\mathbb{K}} V_2 \quad [\mathbb{K}[G]\text{-}\mathbf{Mod}].$$

In (ii) one has a $\mathbb{K}[G]$-isomorphism, but one still tensors over $\mathbb{K}$.

Proof.

(i) First notice that dimensions agree, so it is enough to find a linear injection. Let $\mathcal{B} = \{e_1, \ldots, e_n\}$ be a basis of V_1 and $\mathcal{B}^* = \{e_1^*, \ldots, e_n^*\}$ be the dual basis.

To $f \in \mathrm{Hom}_{\mathbb{K}}(V_1, V_2)$, associate the element:

$$T(f) = \sum_{i=1}^{n} e_i^* \otimes f(e_i) \in V_1^* \otimes_{\mathbb{K}} V_2.$$

This is well-defined. Moreover, $T\colon \mathrm{Hom}_{\mathbb{K}}(V_1, V_2) \to V_1^* \otimes_{\mathbb{K}} V_2$ is clearly linear.

Now suppose $T(f) = 0$. Expressing $f(e_i)$ over any basis of V_2, we see that the non-zero $e_i^* \otimes f(e_i)$ are linearly independent in $V_1^* \otimes V_2$. So all are zero, meaning $f(e_i) = 0$ on $\mathcal{B}$. This implies $f = 0$, and T is injective. The dimensional argument gives the conclusion.

(ii) Let $f\colon V_1 \to V_2$ and $g \in G$. We shall compute and compare $T(g \cdot f)$ with $g \cdot T(f)$. Consider the linear map:

$$u = (g^{-1})^*\colon \begin{array}{ccc} V^* & \to & V^* \\ \varphi & \mapsto & \varphi \circ g^{-1}. \end{array}$$

Let $M = \mathrm{Mat}_{\mathcal{B}}(g^{-1})$ have coefficients $(m_{i,j})$, so that $g^{-1}(e_j) = \sum_i m_{i,j} e_i$. Then by Lemma 2.2.3, we know that $\mathrm{Mat}_{\mathcal{B}^*} u = M^t$. This means that $u(e_j^*) = \sum_i m_{j,i} e_i^*$. We are ready for computation.

$$\begin{aligned}
T(g \cdot f) &= T[x \mapsto g f(g^{-1}x)] \\
&= \sum_i e_i^* \otimes g f(g^{-1} e_i) \\
&= \sum_{i,k} e_i^* \otimes g f(m_{k,i} e_k) \\
&= \sum_{i,k} (m_{k,i} e_i^*) \otimes (g \cdot f(e_k)) \\
&= \sum_k u(e_k^*) \otimes (g f(e_k)) \\
&= \sum_k (e_k^* \circ g^{-1}) \otimes (g \cdot f(e_k)) \\
&= \sum_k (g \cdot e_k^*) \otimes (g \cdot f(e_k)) \\
&= g \cdot \left(\sum_k e_k^* \otimes f(e_k) \right) \\
&= g \cdot T(f).
\end{aligned}$$

We are done. □

2.4.5. Remark. This does not hold if $\dim V_1$ is infinite; see exercise 2.5.2. It is however enough to have $\dim V_1 < \infty$; see exercise 2.5.3.

2.5 Exercises

2.5.1. Exercise. *Let V_1, V_2, V_3 be $\mathbb{K}$-vector spaces.*

1. *Show that there are natural linear isomorphisms:* • $V_2 \oplus V_1 \simeq V_1 \oplus V_2$, • $V_1 \oplus (V_2 \oplus V_3) \simeq (V_1 \oplus V_2) \oplus V_3$, • $V_1 \otimes (V_2 \otimes V_3) \simeq (V_1 \otimes V_2) \otimes V_3$, • $V_2 \otimes V_1 \simeq V_1 \otimes V_2$, • $V_1^{**} \simeq V_1$, • $V_1^* \oplus V_2^* \simeq (V_1 \oplus V_2)^*$, • $V_1^* \otimes V_2^* \simeq (V_1 \otimes V_2)^*$.
2. *Show that if V_1, V_2 are $\mathbb{K}$-linear representation of G, the above is an isomorphism of representations.*

2.5.2. Exercise. *Let V, W be $\mathbb{K}$-vector spaces. Show that in general, $V^* \otimes_{\mathbb{K}} W \simeq \{\varphi \in$* $\mathrm{Hom}_{\mathbb{K}}(V, W) : \dim \operatorname{im} \varphi < \infty\}$.

2.5.3. Exercise. *Show that Proposition 2.4.4 still holds if V_1 is finite-dimensional, regardless of V_2. Hint: explicitly give the converse isomorphism.*

2.5.4. Exercise. *Let V_1, V_2 be two $\mathbb{K}$-vector spaces and $\beta: V_1 \times V_2 \to \mathbb{K}$ be a bilinear form. Suppose β is non-degenerate, viz.:*

- $(\forall v_1 \in V_1)[(\forall v_2 \in V_2)(\beta(v_1, v_2) = 0) \to v_1 = 0]$;
- $(\forall v_2 \in V_2)[(\forall v_1 \in V_1)(\beta(v_1, v_2) = 0) \to v_2 = 0]/$

1. *Find natural linear embeddings $V_1 \hookrightarrow V_2^*$ and $V_1^* \hookrightarrow V_2$.*
2. *Deduce that if V_1 or V_2 is finite-dimensional, then both are and $V_1 \simeq V_2^*$.*

2.5.5. Exercise. For this exercise it is preferable to know about quotient vector spaces. *Let V be a finite-dimensional vector space.*

1. *For $W \leq V$ a subspace, let $W^\perp = \{\varphi \in V^* : (\forall w \in W)(\varphi(w) = 0)\}$. Prove that* $\dim W^\perp = \dim V - \dim W$.
2. *Suppose in addition that V is a representation of G. Prove that V is irreducible iff V^* is.*

(*) **2.5.6. Exercise.** *Return to Proposition 2.4.4. Prove that $T(f)$ does* not *depend on the choice of the basis. Deduce another proof that T is G-covariant.*

3 Around reducibility

Abstract. *Schur's Lemma* (§ 3.1) describes arrows between irreducible representations; there are extra claims if $\mathbb{K}$ is algebraically closed but the general part is worth remembering. *Maschke's Theorem* (§ 3.2) provides nice direct sum decompositions and eliminates the need for quotient objects, but has assumptions on $\operatorname{char} \mathbb{K}$. We then introduce *isotypical components* (§ 3.3).

From this section on, it is important to distinguish assumptions on algebraic closedness ('à la Schur+') from assumptions on the characteristic ('à la Maschke').

3.1 Schur's Lemma

The phrase 'Schur's Lemma' refers to various statements about morphisms between irreducible representations. Some are extremely general; some hold in finite-dimensional spaces; some require, in addition, the base field to be algebraically closed. But there are no assumptions on the characteristic.

3.1.1. Lemma (Schur's Lemma)**.** *Let G be a group and $\mathbb{K}$ be a field. Let $(V_1, \rho_1), (V_2, \rho_2)$ be irreducible $\mathbb{K}$-linear representations.*

(i) If $f: \rho_1 \to \rho_2$ is a morphism of representations, then either $f = 0$ or f is an isomorphism.

(ii) In particular, if (V, ρ) is an irreducible representation, then $\operatorname{End}_{\mathbb{K}[G]}(V)$ is a skew-field.

(iii) *Suppose that $\mathbb{K}$ is algebraically closed. If (V,ρ) is a finite-dimensional, irreducible representation over $\mathbb{K}$, then* $\operatorname{End}_{\mathbb{K}[G]}(V) = \mathbb{K}\operatorname{Id}_V \simeq \mathbb{K}$.

Proof.

(i) Suppose $f \neq 0$. Then $W_1 = \ker f < V_1$. However, W_1 is G-invariant since for $x \in W_1$ and $g \in G$ one has $f(gx) = gf(x) = g \cdot 0 = 0$. By irreducibility of V, one has $W_1 = \{0\}$ and f is injective. Similarly, $W_2 = \operatorname{im} f > 0$ is G-invariant, hence by irreducibility $W_2 = V_2$ and f is surjective. It is thus a G-covariant linear isomorphism, hence an isomorphism of representations.

(ii) A special case. Recall that the inverse of a $\mathbb{K}$-linear, G-covariant isomorphism, is again $\mathbb{K}$-linear and G-covariant.

(iii) Of course every scalar map $\lambda\operatorname{Id}_V$ is G-covariant, so $\mathbb{K}\operatorname{Id}_V \leq \operatorname{End}_{\mathbb{K}[G]}(V)$. We prove the converse. Let $\sigma \in \operatorname{End}_{\mathbb{K}[G]}(V)$. By assumption, V is finite-dimensional over $\mathbb{K}$ and $\mathbb{K}$ is algebraically closed. So any linear endomorphism of V has an eigenvalue. Say $\lambda \in \mathbb{K}$ has a non-zero eigenspace $E_\lambda(\sigma) \neq \{0\}$. Then $\tau = \sigma - \lambda\operatorname{Id}_V \in \operatorname{End}_{\mathbb{K}[G]}(V)$ has a non-zero kernel. But $\operatorname{End}_{\mathbb{K}[G]}(V)$ is a skew-field by (ii), so $\sigma = \lambda\operatorname{Id}_V$. Hence $\operatorname{End}_{\mathbb{K}[G]}(V) = \mathbb{K}\operatorname{Id}_V \simeq \mathbb{K}$. □

A useful consequence is that over an algebraically closed field, if both ρ_1 and ρ_2 are irreducible, then $\dim \operatorname{Hom}_{\mathbb{K}[G]}(\rho_1, \rho_2)$ is 0 or 1.

3.1.2. Remarks.

- Even starting with a commutative $\mathbb{K}$, one can construct irreducible representations where $\operatorname{End}_{\mathbb{K}[G]}(V)$ is a *non-commutative* skew-field. We return to the topic in § 11; meanwhile see exercise 3.4.1.
- The argument makes crucial use of commutativity of $\mathbb{K}$. For vector spaces over skew-fields, the maps $\lambda\operatorname{Id}_V$ are no longer $\mathbb{K}$-linear. I am however not aware of a developed representation theory over skew-fields.

3.2 Maschke's Theorem

The phrase 'Maschke's Theorem' refers to various statements about expressing arbitrary representations as direct sums of irreducible ones. All require the characteristic to be coprime to the order of the finite group, hence always work in characteristic 0. (Generalisations to infinite groups would require higher-level structure.) But there are no assumptions on algebraic closedness.

3.2.1. Theorem (Maschke's Theorem)**.** *Let G be a finite group and $\mathbb{K}$ be a field. Suppose that $\mathbb{K}$ has coprime characteristic. Let (V,ρ) be a $\mathbb{K}$-linear representation. Then:*

(i) Every G-invariant subspace $W \leq V$ admits a G-invariant direct complement.

(ii) V is a direct sum of irreducible representations.

(iii) In particular, if V is finite-dimensional, then it is a direct sum of finitely many *irreducible representations.*

3.2.2. Remarks.

- (i) expresses *complete reducibility*, also known as *semisimplicity* of the group algebra $\mathbb{K}[G]$. (See § 13.2.)
- While (ii) does not require finite-dimensionality (it does require finiteness of G though), it is the kind of claim that often disturbs beginners.

Proof.

(i) Let $W \leq V$ be as in the statement. Because direct complements exist in the category of vector spaces, we may take a linear subspace $S \leq V$ such that $V = W \oplus S$. The problem is that S need not be G-invariant. We shall 'average it' as follows.

Let $\pi \colon V \to W$ be the linear projector onto W parallel to S. Now let:

$$\hat{\pi} = \frac{1}{|G|} \sum_{g \in G} \rho(g^{-1}) \circ \pi \circ \rho(g) = \frac{1}{|G|} \sum_{g \in G} g^{-1} \pi g.$$

(The second formula is in implicit notation, which we now use.) We claim the following.

- $\hat{\pi}$ is a linear, G-covariant map. Linearity is obvious since $\hat{\pi}$ is a sum of linear maps. Now for fixed $h \in G$, the map $g \mapsto gh$ is a bijection of the indexing set G so:

$$\begin{aligned}\hat{\pi} h &= \frac{1}{|G|} \sum_{g \in G} g^{-1} \pi g \cdot h \\ &= \frac{1}{|G|} \sum_{g \in G} h \cdot h^{-1} g^{-1} \cdot \pi \cdot gh \\ &= \frac{1}{|G|} \sum_{g' \in G} h \cdot g' \pi g' \\ &= h \hat{\pi}.\end{aligned}$$

- $\hat{\pi}$ is a linear projector onto W. Recall that W is G-invariant. So for any $g \in G$ and $v \in V$, one has $gv \in V$, then $\pi(gv) \in W$, and $g^{-1}\pi(gv) \in W$. Hence $\hat{\pi}(g) \in W$ and $\operatorname{im} \hat{\pi} \leq W$. Now π is the identity on W. So for $w \in W$, one has $gw \in W$, then $\pi(gw) = gw$, and $g^{-1}\pi(gw) = w$. Hence $\hat{\pi}(w) = w$.

  Summing up, $\operatorname{im} \hat{\pi} \leq W$ and $\hat{\pi}_{|W} = \mathrm{Id}_W$. This is the definition of a linear projector with image W.

Let $\hat{S} = \ker \hat{\pi}$. Being the kernel of the projector $\hat{\pi}$, it is a direct complement of $W = \operatorname{im} \hat{\pi}$. Moreover it is G-invariant, because $\hat{\pi}$ is G-covariant. We are done.

(ii) This requires some maximality argument à la Zorn (and the proof may be omitted by the unexperienced).

Let $\mathcal{F}$ be a family of irreducible subrepresentations of V whose sum is direct, and maximal as such. (This exists by Zorn's lemma, or the axiom of choice and ordinal induction.) Let $S = \sum_{W \in \mathcal{F}} W = \bigoplus_{W \in \mathcal{F}} W$.

If $S < V$, then by (i), there is a G-invariant complement T. Now T contains an irreducible representation W' by Lemma 1.2.3. So $\mathcal{F} = \mathcal{F} \cup \{W'\}$ is a family of irreducible representations whose sum is direct. By maximality of $\mathcal{F}$ as such, one has $W' \in \mathcal{F}$. So $W' \leq S$, a contradiction. This proves $S = V$, as wanted.

(iii) A direct consequence of (ii), but it can also be proved directly by induction on $\dim V$. See exercise 3.4.4. □

3.2.3. Remarks.

- If $\operatorname{char} \mathbb{K}$ divides $|G|$, then Maschke's theorem no longer holds (exercise 3.4.6), so the theory of *modular representations* is more complicated.
- Maschke's principle fails for infinite groups, even over $\mathbb{C}$. *However*, it can be salvaged for certain infinite groups bearing extra structure (typically, a Haar measure as used in Lie theory).

3.3 Isotypical components

We proceed to analysing *reducible* representations in terms of 'atoms' (viz. irreducible representations).

3.3.1. Definition. Let G be a group and $\mathbb{K}$ be a field. Let V be a $\mathbb{K}$-linear representation of G. Also let $T \in \operatorname{Irr}_{\mathbb{K}}(G)$.

- Let $\operatorname{Cp}_V(T) = \{W \leq V : W \text{ is a subrepresentation and } W \simeq T\}$ be the set of isomorphic copies of T inside V.
- Let $\operatorname{Iso}_V(T) = \sum_{W \in \operatorname{Cp}_V(T)} W$ be their sum, called the *isotypical component* of V of type T.

These notions behave extremely well in presence of both Schur's and Maschke's phenomena. The following can be read following the analogy with p-primary components of abelian groups.

3.3.2. Theorem. *Let G be a finite group and $\mathbb{K}$ be a field of coprime characteristic. Let V be a $\mathbb{K}$-linear representation. Then:*

(i) Every irreducible subrepresentation of $\operatorname{Iso}_V(T)$ is isomorphic to T.

(ii) $V = \bigoplus_{T \in \operatorname{Irr}_{\mathbb{K}}(G)} \operatorname{Iso}_V(T)$.

(iii) If V_1, V_2 are two $\mathbb{K}$-linear representations, and $f: V_1 \to V_2$ is a morphism of representations, then $f(\operatorname{Iso}_{V_1}(T)) \leq \operatorname{Iso}_{V_2}(T)$.

(iv) For every $T \in \operatorname{Irr}_{\mathbb{K}}(G)$, there is a subfamily $\mathcal{F}_T \subseteq \operatorname{Cp}_V(T)$ such that $\operatorname{Iso}_V(T) = \bigoplus_{W \in \mathcal{F}_T} W$.

3.3.3. Remarks.

- Subrepresentations $\operatorname{Iso}_V(T)$ are completely canonical, which is confirmed by (iii).
- However a family $\mathcal{F}_T$ as in (iv) is highly non-canonical. The simplest example is a 2-dimensional vector space V as a representation of $\{1\}$. Certainly V is a direct sum of two vector lines, but these are not uniquely determined.

- The theorem does not require algebraic closedness, but fails badly in characteristic dividing $|G|$.

Proof. We use quick lemmas.

3.3.4. Lemma. *Suppose $V', W \leq V$ are subrepresentations with W irreducible. Then $W \cap V' = \{0\}$ or $W \leq V'$.*

Proof. Let $R = W \cap V'$, which is a subrepresentations of W. If $R = \{0\}$ we are done. Otherwise, by irreducibility, $W = R \leq V'$. □

3.3.5. Lemma. *Every sum $\sum_I W_i$ of irreducible subrepresentations $W_i \leq V$ is the* direct *sum of a subfamily $J \subseteq I$.*

Proof. Let $S = \sum_I W_i$ be a sum of irreducible subrepresentations. Let $J \subseteq I$ be a subfamily whose sum is direct, and maximal with respect to this property. (This exists by maximality principles à la Zorn.) Now let $S' = \sum_J W_j = \bigoplus_J W_j$. We claim that $S' = S$.

If it is not the case, there is $i \in I$ with $W_i \nleq S'$. By Lemma 3.3.4, $W_i \cap S' = \{0\}$. So $J \cup \{i\}$ is a family properly containing J, whose sum is direct: a contradiction. So $S = S' = \bigoplus_J W_j$ is the direct sum of a subfamily. □

3.3.6. Lemma. *Suppose that all W_i for $i \in I$ and W are irreducible subrepresentations of V, with $W \leq \sum_I W_i$. Then W is isomorphic to one of the W_i.*

Proof. By Lemma 3.3.5, up to taking a subfamily we may assume $\sum_I W_i = \bigoplus_I W_i$. So we may consider the projectors π_i onto W_i parallel to the other summands. Since $W \neq \{0\}$, there is $i \in I$ such that $\pi_i(W) \neq 0$. We fix one such and let f be the restriction $\pi_{i|W}\colon W \to W_i$. Then $f \neq 0$. Now both W and W_i are irreducible, so by Schur's Lemma f is an isomorphism $W \simeq W_i$. □

(i) Immediate from Lemma 3.3.6.

(ii) By Maschke's theorem, V is a sum of irreducible representations. Each lies in some $\mathrm{Iso}_V(T)$, whence $V = \sum_{T\in\mathrm{Irr}_{\mathbb{K}}(G)}$.

We prove that the latter sum is direct; suppose not. Then there are distinct types $T_0, T_1, \dots, T_n$ with $n \geq 1$ such that $\mathrm{Iso}_V(T_0) \cap (\sum_{i=1}^n \mathrm{Iso}_V(T_i)) \neq \{0\}$. So there is $W \in \mathrm{Cp}_V(T_0)$ contained in $\sum_{i=1}^n \mathrm{Iso}_V(T_i)$. By Lemma 3.3.6, T_0 is isomorphic to one summand of some $\mathrm{Iso}_V(T_i)$, viz. $T_0 \simeq T_i$, a contradiction.

(iii) Let $W_1 \in \mathrm{Cp}_{V_1}(T)$. Then $f(W_1) \leq V_2$ is G-invariant, hence a subrepresentation. By Schur's Lemma, either $f(W_1) = \{0\}$ or $f(W_1) \simeq W_1 \simeq T$. So in either case, $f(W_1) \leq \mathrm{Iso}_{V_2}(T)$.

(iv) Immediate from Lemma 3.3.5. □

3.3.7. Corollary (and definition)**.** *Let G be a finite group and $\mathbb{K}$ be a field of coprime characteristic. Let V be a $\mathbb{K}$-linear, finite-dimensional representation. Then there are well-*

defined integers $n_T = n_T(V)$ for $T \in \mathrm{Irr}_{\mathbb{K}}(G)$ such that:

$$V \simeq \bigoplus_{T \in \mathrm{Irr}_{\mathbb{K}}(G)} T^{n_T} \quad [\mathbb{K}[G]\text{-}\mathbf{Mod}].$$

The integer $n_T(V)$ is called the multiplicity of T in V.

Proof. The existence is a reformulation of Theorem 3.2.1 (iii). Write V as a direct sum of irreducible representations; now sort them according to their isomorphism types.

It remains to show that the integers do not depend on the decomposition. Suppose there is an isomorphism of representations $f\colon \bigoplus T^{n_T} \simeq \bigoplus T^{m_T}$. By Theorem 3.3.2 (iii), it restricts to isomorphisms $f_T\colon T^{n_T} \simeq T^{m_T}$ for each $T \in \mathrm{Irr}_{\mathbb{K}}(G)$. But then, $n_T \dim T = m_T \dim T$, so $n_T = m_T$, as wanted. □

Hence a finite-dimensional, $\mathbb{K}$-linear representation of a finite group over a field of coprime characteristic is entirely determined by the number of 'atoms' (viz. irreducible representations) of each type in it.

3.3.8. Remark. Corollary 3.3.7 can be used to give a proof in coprime characteristic that a representation V is irreducible iff V^* is. (This holds with no assumptions on the characteristic: see exercise 2.5.5.)

Suppose V is irreducible and write $V^* \simeq \bigoplus_T T^{n_T}$ $[\mathbb{K}[G]\text{-}\mathbf{Mod}]$. Then $V \simeq V^{**} \simeq \bigoplus_T (T^*)^{n_T}$ $[\mathbb{K}[G]\text{-}\mathbf{Mod}]$. But V is irreducible, so there is only one term, and it has multiplicity 1. Hence V^* is irreducible. The converse also uses $V^{**} \simeq V$ $[\mathbb{K}[G]\text{-}\mathbf{Mod}]$.

In § 5, exercise 5.6.6 will give an explicit formula for the projector π_T onto $\mathrm{Iso}_V(T)$ parallel to the sum of the other isotypical components.

3.4 Exercises

3.4.1. Exercise. *Let $\mathbb{H}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ be the group of basic quaternions, satisfying:*

$$i^2 = j^2 = k^2 = -1, \quad , ij = k = -ji, \quad jk = i = -kj, \quad ki = j = -ik.$$

Let $V \simeq \mathbb{R}^4$ have basis $1, i, j, k$, and extend linearly to define an $\mathbb{R}$-representation of $\mathbb{H}_8$ in V. Prove that it is irreducible, and determine $\mathrm{End}_{\mathbb{R}[G]}(V)$.

3.4.2. Exercise. *Let G be a finite group and $\rho \in \mathrm{Irr}_{\mathbb{C}}(G)$. Show that if ρ is injective, then $Z(G)$ is cyclic.*

3.4.3. Exercise. *Let ρ be the permutation representation of $G = \mathrm{Sym}(3)$, viz. the permutation action on $V = \mathbb{C}e_1 \oplus \mathbb{C}e_2 \oplus \mathbb{C}e_3$. Check that $L = \langle e_1 + e_2 + e_3 \rangle$ is G-invariant. Give a G-invariant complement. (Exercise 3.4.5 gives an instant method.)*

3.4.4. Exercise. *Return to Theorem 3.2.1. Suppose $\mathrm{char}\, \mathbb{K} = 0$ and $\dim V < \infty$. Prove (iii) by induction on $\dim V$ without using (ii).*

3.4.5. Exercise (an alternative proof of Maschke's theorem over $\mathbb{C}$)**.** *Let G be a group and V be a finite-dimensional, complex, linear representation of G. Let $[\cdot|\cdot]$ be a complex scalar product, viz. a sesquilinear, Hermite-symmetric, positive definite form $V \times V \to \mathbb{C}$.*

1. *Let* $[\![x|y]\!] = \frac{1}{|G|}\sum_{g\in G}[gx|gy]$. *Prove that this is a complex scalar product.*
2. *Prove that for* $x, y \in V$ *and* $g \in G$ *one has* $[\![gx|gy]\!] = [\![x|y]\!]$.
3. *Deduce a proof of Maschke's theorem* over $\mathbb{C}$.
4. *Extra question: if V is irreducible, show that* all *G-invariant complex scalar products are multiples of* $[\![\cdot|\cdot]\!]$.

3.4.6. Exercise (failure of Maschke in native characteristic)**.** *Let* $G = C_2$ *be the cyclic group with two elements. Let it act on* $V \simeq \mathbb{F}_2^2$ *by taking the generator to:*

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Prove that $\mathbb{F}_2 e_2$ *is G-invariant, but has no G-invariant complement.*

3.4.7. Exercise. *Let G be finite. Show that if all irreducible, linear complex representations are* 1*-dimensional, then G is abelian.*

3.4.8. Exercise. *Determine which lemmas and which ads of Theorem 3.3.2 remain true* • *if* char $\mathbb{K}$ *divides* $|G|$, • *if G is infinite.*

4 Characters

Abstract. The definition of a *character* (§ 4.1) first looks 'too simple to be useful', and yet is extremely powerful. *Character tables* encode the values of the irreducible characters. Characters are typical examples of *class functions* (§ 4.2). We then describe characters of representations obtained by the usual algebraic constructions (§ 4.3).

4.1 Characters and character tables

4.1.1. Definition. Let G be a group and $\mathbb{K}$ be a field. Let $\rho\colon G \to \mathrm{GL}(V)$ be a finite-dimensional, $\mathbb{K}$-linear representation. Its *character* is the map

$$\begin{array}{cccc} \chi_\rho\colon & G & \to & \mathbb{K} \\ & g & \mapsto & \operatorname{tr}\rho(g), \end{array}$$

where tr denotes the trace. (When there is no ambiguity on ρ, one simply writes χ.)

4.1.2. Remarks.

- A character need not be a morphism!
- Since the trace is invariant under conjugation, so is any character, viz. one has $\chi(g^{-1}hg) = \chi(h)$. In particular, one really computes $\chi(\gamma)$ for γ a *conjugacy class* of G.
- Characters are especially useful if $\mathbb{K}$ is algebraically closed (so we have eigenvalues) and has coprime characteristic 0 (so we have complete reducibility). *One cannot imagine at first the strength of character theory over* $\mathbb{C}$.

- It follows immediately from Corollary 3.3.7 that in coprime characteristic, for every character χ_V there are integers n_T for $T \in \mathrm{Irr}_{\mathbb{K}}(G)$ such that:

$$\chi_V = \sum_{T \in \mathrm{Irr}_{\mathbb{K}}(G)} n_T \chi_T.$$

- Interestingly enough, the n_T's above are integers *of* $\mathbb{K}$, meaning that in positive characteristic p they are to be considered modulo p. Thus characters can, at best, detect multiplicity *modulo the characteristic.*

  For instance, the character of $\mathrm{triv} \oplus T^p$ is $\chi_{\mathrm{triv}} + p\chi_T = \chi_{\mathrm{triv}}$. But as *representations*, $\mathrm{triv} \not\simeq (\mathrm{triv} \oplus T^p)$. So parts of character theory even require $\mathrm{char}\,\mathbb{K} = 0$.

4.1.3. Lemma. *Suppose $\mathbb{K} \leq \mathbb{C}$. Let G be a finite group and $\rho\colon G \to \mathrm{GL}(V)$ be a $\mathbb{K}$-linear representation of G with character χ. Then for all $g \in G$:*

$$\chi(g^{-1}) = \overline{\chi(g)}.$$

Proof. We know that $\rho(g)$ can be brought to diagonal form, say one of its matrices is $\mathrm{diag}(\lambda_1, \dots, \lambda_n)$. Hence $\rho(g^{-1}) = \rho(g)^{-1}$ is diagonalisable to $\mathrm{diag}(\lambda_1^{-1}, \dots, \lambda_n^{-1})$. But each λ_i is a complex root of unity, so $\lambda_i^{-1} = \overline{\lambda_i}$. Therefore one of the matrices of g^{-1} is $\mathrm{diag}(\overline{\lambda_1}, \dots, \overline{\lambda_n})$, with trace:

$$\chi(g^{-1}) = \mathrm{tr}\,\rho(g^{-1}) = \mathrm{tr}\,\mathrm{diag}(\overline{\lambda_1}, \dots, \overline{\lambda_n}) = \sum_i \overline{\lambda_i} = \overline{\sum_i \lambda_i} = \overline{\mathrm{tr}\,\rho(g)} = \overline{\chi(g)}. \qquad \square$$

4.1.4. Definition.

- An *irreducible character* is the character of an irreducible representation.

  We let $\mathrm{Irr}_{\mathbb{K}}(G)$ be the set of irreducible characters. Because characters will determine representations (at least in the irreducible case over good fields), this does *not* conflict with the same notation for the set of irreducible representations.

- The *character table* of a finite group G over $\mathbb{K}$ is the table constructed as follows:
  - list all conjugacy classes $\gamma_1, \dots, \gamma_r$ of G, with respective number of elements say $d_1, \dots, d_r$.
  - list all irreducible characters $\chi_1, \dots, \chi_r$ of G over $\mathbb{K}$. *For good* $\mathbb{K}$, it is the same number r (Theorem 5.1.1).
  - Now tabulate values as follows:

G	$\gamma_1\ [\times d_1]$	$\dots$	$\gamma_r\ [\times d_r]$
χ_1	$\chi_1(\gamma_1)$	$\dots$	$\chi_1(\gamma_r)$
$\vdots$			
χ_r	$\chi_r(\gamma_1)$	$\dots$	$\chi_r(\gamma_r)$

When not otherwise specified, character tables are usually given over $\mathbb{C}$ (or $\overline{\mathbb{Q}}$).

4.1.5. Example. Here is the character table of $\mathrm{Sym}(3)$.

	$1\ [\times 1]$	$(12)\ [\times 3]$	$(123)\ [\times 2]$
χ_{triv}	1	1	1
χ_ε	1	-1	1
χ_2	2	0	-1

4.1.6. Remarks.

- Such a table does not really give the representations themselves, nor the group structure.

  For instance, the dihedral group $D_{2\cdot 4}$ and the basic quaternion group $\mathbb{H}_8$ have the same character table over $\mathbb{C}$, although they are non-isomorphic.

- This cannot happen with finite *simple* groups, but we know this because we have the full list of them. Actually the finite simple groups are determined by much less information than their character tables—again because we have the list.

- However character tables encode much information on finite groups. Actually some properties can be 'read off' character tables; see exercise 7.4.2.

4.2 Class functions

Invariance under conjugation begs for a definition.

4.2.1. Definition. A *class function* (also: *central function*) is a function $\alpha\colon G \to \mathbb{K}$ satisfying: $(\forall g)(\forall h)(\alpha(g^{-1}hg) = \alpha(g))$.

More algebraically, these are functions which factor through the conjugation relation. For a class function α and a conjugacy class γ, it makes sense to write $\alpha(\gamma)$.

4.2.2. Lemma (and notation)**.** *Let G be a finite group and $\mathbb{K}$ be a field of coprime characteristic.*

(i) Class functions form a $\mathbb{K}$-vector subspace of the space $\mathbb{K}^G$ of all maps $G \to \mathbb{K}$.

We denote it by $\mathcal{C}_{\mathbb{K}}(G)$ (or simply $\mathcal{C}$ if there is no ambiguity on $\mathbb{K}$ or G).

(ii) $\dim_{\mathbb{K}} \mathcal{C}_{\mathbb{K}}(G)$ *is the number of conjugacy classes of G.*

(iii) $\mathcal{C}_{\mathbb{K}}$ bears a bilinear, symmetric, non-degenerate form given by:

$$(\alpha|\beta) = \frac{1}{|G|}\sum_{g\in G}\alpha(g^{-1})\beta(g).$$

(iv) If $\mathbb{K} = \mathbb{C}$, then $\mathcal{C}_{\mathbb{C}}$ also *bears a complex scalar product, given by:*

$$[\alpha|\beta] = \frac{1}{|G|}\sum_{g\in G}\overline{\alpha(g)}\beta(g).$$

(v) When $\mathbb{K} \leq \mathbb{C}$ and χ_1, χ_2 are characters*, both coincide: $(\chi_1|\chi_2) = [\chi_1|\chi_2]$.*

Actually (i) and (ii) do *not* require coprimality of the characteristic (as seen from the proof). But dividing by $|G|$ certainly does.

Proof.

(i) is clear.

(ii) For $\gamma \subseteq G$ a conjugacy class, let $\mathbf{1}_\gamma$ be the indicator function, viz. the function which is 1 on γ and 0 elsewhere. This map is in $\mathcal{C}$. Let $\mathcal{B} = \{\mathbf{1}_\gamma : \gamma \text{ a conjugacy class}\}$. We claim that it is a basis of $\mathcal{C}_{\mathbb{K}}(G)$. Indeed, suppose $\sum \lambda_\gamma \mathbf{1}_\gamma = 0$ in obvious notation. Let δ be a conjugacy class and let $g \in \delta$; then $\sum \lambda_\gamma \mathbf{1}_\gamma(g) = \lambda_\delta = 0$, which applies to every class. Now if $\alpha \in \mathcal{C}$, then for every class γ let $\lambda_\gamma = \alpha(\gamma)$. Then α and $\sum \lambda_\gamma \mathbf{1}_\gamma$ agree everywhere.

(iii) Bilinearity is clear. Symmetry follows from reindexing:

$$(\beta|\alpha) = \frac{1}{|G|}\sum_{g\in G}\beta(g^{-1})\alpha(g) = \frac{1}{|G|}\sum_{g'\in G}\beta(g')\alpha(g'^{-1}) = (\alpha|\beta)\,.$$

We prove non-degeneracy. Let $\alpha \in \mathcal{C}_\mathbb{K}$ be $(\cdot|\cdot)$-orthogonal to all class functions. Let γ be a conjugacy class; then so is $\gamma^{-1} = \{g^{-1} : g \in \gamma\}$. Let $f = \mathbf{1}_{\gamma^{-1}}$ be the indicator function of γ^{-1}. Then since α is a class function:

$$0 = |G|\cdot(f|\alpha) = \sum_{g\in G} f(g^{-1})\alpha(g) = \sum_{g\in G}\mathbf{1}_{\gamma^{-1}}(g^{-1})\alpha(g) = \#\gamma\cdot\alpha(\gamma).$$

Now $\#\gamma = [G : C_G(g)]$ for any $g \in \gamma$, and therefore $\#\gamma$ divides $|G|$. In particular, $\#\gamma$ is coprime to the characteristic (if positive), and it follows $\alpha(\gamma) = 0$. This holds for any conjugacy class: so α is zero globally.

(iv) Actually the formula defines a complex vector space on all of $\mathbb{C}^G$, as easily seen. Since $\mathcal{C}_\mathbb{C}$ is a vector subspace, the claim follows.

(v) Clear since by Lemma 4.1.3, $\chi(g^{-1}) = \overline{\chi(g)}$ *for a character*. □

4.2.3. Remarks.

- There are other conventions (inverse on the right, complex-conjugation on the right). What matters is the resulting theory, viz. side-invariant phenomena.
- Over $\mathbb{C}$ there are two natural pairings of class functions: $(\cdot|\cdot)$ and $[\cdot|\cdot]$. They return the same values on characters but need not agree on all class functions. Only the former is symmetric; the latter is merely Hermite-symmetric.
- In particular they give rise to *distinct* notions of orthonormality, which however agree on characters.
- Analysts will favour working with $[\cdot|\cdot]$, and algebraists will prefer $(\cdot|\cdot)$.

4.3 Characters and algebraic constructions

§ 2 gave methods how to obtain new representations from existing ones. The proposition below will describe the consequent behaviour of characters. It builds on the principle that *isomorphic representations have equal character*.

4.3.1. Lemma. *Let G be a finite group and $\mathbb{K}$ be a field. If $\rho_1 \simeq \rho_2$ are isomorphic finite-dimensional representations, then $\chi_1 = \chi_2$.*

Proof. By definition, there is an isomorphism $f\colon \rho_1 \simeq \rho_2$, viz. a linear isomorphism

$V_1 \simeq V_2$ such that for all $g \in G$:

$$\begin{tikzcd} V_1 \arrow[r, "f"] \arrow[d, "\rho_1(g)"'] & V_2 \arrow[d, "\rho_2(g)"] \\ V_1 \arrow[r, "f"] & V_2. \end{tikzcd}$$

Another way to write it is $\rho_2(g) = f^{-1}\rho_1(g)f$. Taking matrices if necessary, one sees $\operatorname{tr}\rho_2(g) = \operatorname{tr}\rho_1(g)$ for all $g \in G$, that is, $\chi_2 = \chi_1$. ☐

4.3.2. Remark. A converse will be seen: in good cases, representations with equal characters are actually isomorphic (Theorem 5.1.1).

We return to the constructions of § 2 and determine their characters.

4.3.3. Proposition. *Let G be a group and $\mathbb{K}$ be a field. Let $(V,\rho), (V_1,\rho_1), (V_2,\rho_2)$ be $\mathbb{K}$-linear, finite-dimensional representations with characters χ, χ_1, χ_2.*

(i) The character of $\rho_1 \oplus \rho_2$ is $\chi_1 + \chi_2$.

(ii) The character of ρ^* is $\chi^*(g) = \chi(g^{-1})$. In case $\mathbb{K} \leq \mathbb{C}$, this also equals $\overline{\chi(g)}$.

(iii) The character of $\rho_1 \otimes_{\mathbb{K}} \rho_2$ is $\chi_1\chi_2$.

(iv) The character of $\operatorname{Hom}_{\mathbb{K}}(\rho_1, \rho_2)$ is $\chi_1^*\chi_2$. In case $\mathbb{K} \leq \mathbb{C}$, this also equals $\overline{\chi_1} \cdot \chi_2$.

Proof.

(i) By definition, $\rho_1 \oplus \rho_2$ is the natural action of G on $V_1 \oplus V_2$, viz. G acts on V_1 via ρ_1 and on V_2 via ρ_2. So:

$$\chi_{\rho_1+\rho_2}(g) = \operatorname{tr}(\rho_1 \oplus \rho_2)(g) = \operatorname{tr}\rho_1(g) + \operatorname{tr}\rho_2(g) = \chi_1(g) + \chi_2(g).$$

(ii) By definition, $\rho^*(g)\colon V^* \to V^*$ takes a linear form φ to the linear form $v \mapsto \varphi(g^{-1} \cdot v)$. Working in coordinates if necessary, if $\mathcal{B}$ is a basis of V then:

$$\operatorname{Mat}_{\mathcal{B}^*} \rho^*(g) = \left(\operatorname{Mat}_{\mathcal{B}} \rho(g^{-1})\right)^t,$$

so $\chi^*(g) = \chi(g^{-1})$. In case $\mathbb{K} \leq \mathbb{C}$, this also equals $\overline{\chi(g)}$ by Lemma 4.1.3.

(iii) By definition, $\rho_1 \otimes \rho_2$ is the tensor action of G on $V_1 \otimes V_2$, viz. G acts on $v_1 \otimes v_2$ by $(\rho_1 \otimes \rho_2)(g)(v_1 \otimes v_2) = \rho_1(g)(v_1) \otimes \rho_2(g)(v_2)$. Working in coordinates if necessary,

$$\chi_{\rho_1\otimes\rho_2}(g) = \operatorname{tr}(\rho_1 \otimes \rho_2)(g) = \operatorname{tr}\rho_1(g) \cdot \operatorname{tr}\rho_2(g) = (\rho_1\rho_2)(g).$$

(iv) Recall from Proposition 2.4.4 (ii) that there is an isomorphism of representations (viz. a $\mathbb{K}[G]$-isomorphism):

$$\operatorname{Hom}_{\mathbb{K}[G]}(V_1, V_2) \simeq V_1^* \otimes_{\mathbb{K}} V_2 \quad [\mathbb{K}[G]\text{-}\mathbf{Mod}].$$

By Lemma 4.3.1 it is enough to give the character of the right-hand, and the claim follows from (ii) and (iii). ☐

4.3.4. Remark. Thus the character of T^n is $n\chi_T$. If $\mathbb{K}$ has positive characteristic dividing n, this is the zero map. Similarly, triv $\oplus$ T^n has character χ_{triv}. This simply tells us that the expected function:

$$\{\text{finite-dimensional } \mathbb{K}\text{-linear representations}\} \to \{\text{characters}\}$$

cannot be injective. This is as deep as saying that in positive characteristic, the base field does *not* have infinitely many integers.

4.4 Exercises

4.4.1. Exercise.

1. *Compute* χ_{reg} *for any finite group* G.
2. *Generalise to* χ_{perm}*: prove that* $\chi_{\text{perm}}(g) = \#\{x \in X : gx = x\}$.
3. *Let* $G = \text{Sym}(3)$. *Inside* perm, *consider the line* $L = \langle e_1 + \cdots + e_3 \rangle$. *Let* V *be a* G*-invariant complement of* L *inside* perm. *Give* χ_V.
4. *Same question when* $n = 4$.

4.4.2. Exercise. *Give the character table of the cyclic group* C_n *over* $\mathbb{C}$.

For the next exercises, admit that the number of complex, irreducible representations of a finite group equals the number of conjugacy classes (Theorem 5.1.1).

4.4.3. Exercise. *Give the character table of* $\text{Sym}(3)$ *over* $\mathbb{C}$.

4.4.4. Exercise. *Give the character table of* $\text{Alt}(4)$ *over* $\mathbb{C}$. *Hint: act on a regular tetrahedron in the usual* 3*-dimensional space.*

5 Orthogonality relations

Abstract. The main Theorem (§ 5.1) says that irreducible complex characters of a finite group form an orthonormal basis of the space of class functions. There are numerous consequences, such as: every finite-dimensional, complex representation is determined by its character, or: every irreducible, complex representation occurs in the regular representation with multiplicity equal to its dimension. The proof builds on a simple lemma giving the dimension of the subspace of fixed points of a representation (§ 5.2). Orthonormality is then proved in § 5.3 and generation in § 5.4.

5.1 The main theorem

We fix a finite group G and a good field $\mathbb{K}$. Recall from § 4.2 that a $\mathbb{K}$-valued *class function* on a group G is a map $\alpha\colon G \to \mathbb{K}$ such that $(\forall x)(\forall y)(\alpha(x^y) = \alpha(x))$.

- Class functions form a $\mathbb{K}$-vector space $\mathcal{C}_{\mathbb{K}}(G)$, and $\dim_{\mathbb{K}} \mathcal{C}_{\mathbb{K}}(G) = \#\,\text{Conj}(G)$, the number of conjugacy classes of G.
- Characters are class functions.

- $\mathcal{C}_{\mathbb{K}}(G)$ bears a natural bilinear, symmetric, non-degenerate form:

$$(\alpha|\beta) = \frac{1}{|G|}\sum_{g\in G}\alpha(g^{-1})\beta(g).$$

- If $\mathbb{K} = \mathbb{C}$, then $\mathcal{C}_{\mathbb{C}}(G)$ *also* bears a natural complex scalar product:

$$[\alpha|\beta] = \frac{1}{|G|}\sum_{g\in G}\overline{\alpha(g)}\beta(g).$$

- These agree on characters, so for that matter one may work with either.

5.1.1. Theorem. *Let G be a finite group and $\mathbb{K}$ be a good field.*

(i) $\mathrm{Irr}_{\mathbb{K}}(G)$ *forms an orthonormal basis of the space of class functions on G. In particular,* $\#\,\mathrm{Irr}_{\mathbb{K}}(G) = \dim_{\mathbb{K}}\mathcal{C}_{\mathbb{K}}(G) = \#\,\mathrm{Conj}(G)$.

In case $\mathbb{K} \leq \mathbb{C}$, the same holds with respect to $[\cdot|\cdot]$-orthonormality.

(ii) Let V be a $\mathbb{K}$-linear, finite-dimensional representation. Then, as functions from G to $\mathbb{K}$, one has $\chi_V = \sum_{\chi\in\mathrm{Irr}_{\mathbb{K}}(G)}(\chi_V|\chi_T)\,\chi_T$.

(iii) Every irreducible *representation is determined by its character. If* char $\mathbb{K} = 0$, *then every* finite-dimensional *representation is determined by its character.*

(iv) Let reg *be the regular representation of G over $\mathbb{K}$. Then* $\mathrm{reg} \simeq \bigoplus_{T\in\mathrm{Irr}_{\mathbb{K}}(G)} T^{\dim T}$.

5.1.2. Remarks.

- As a consequence of (iii), it is safe to let $\mathrm{Irr}_{\mathbb{K}}(G)$ be the set of irreducible *characters*. Likewise, it is safe to write $\mathrm{Iso}_V(\chi)$ instead of $\mathrm{Iso}_V(T)$.

- The general case in (iii) fails in characteristic $p > 0$ (even over good fields).

  Indeed, for any representation W, letting $V = \mathrm{triv}\oplus W^p$ one gets $\chi_V = \mathrm{triv}$. But $V \not\simeq \mathrm{triv}\ [\mathbb{K}[G]\text{-}\mathbf{Mod}]$.

- Another way to write (iv) is:

$$\chi_{\mathrm{reg}} = \sum_{\chi\in\mathrm{Irr}_{\mathbb{K}}(G)}\chi(1)\cdot\chi.$$

  This immediately implies:

$$|G| = \dim\mathrm{reg} = \chi_{\mathrm{reg}}(1) = \sum_{\chi\in\mathrm{Irr}_{\mathbb{K}}(G)}\chi(1)^2,$$

  so $|G|$ *is a sum of* $\#\,\mathrm{Conj}(G)$*-many squares.*

5.1.3. Remark. Although $\mathrm{Conj}(G)$ and $\mathrm{Irr}_{\mathbb{K}}(G)$ have the same number of elements (so they are equipotent), there is in general no *distinguished* bijection between them.

An interesting exception is the symmetric group $\mathrm{Sym}(n)$ where one can attach to each conjugacy class an irreducible character, in a systematic way. This is the theory of *Young tableaux*.[4]

[4] For example, see § 28 in the Curtis-Reiner book ('Further reading').

5.2 Trivial spaces

5.2.1. Definition. Let V be a $\mathbb{K}$-linear representation of a group G. The *space of fixed vectors*, or the *G-trivial subspace of V*, is the subspace:

$$C_V(G) = \{v \in V : (\forall g \in G)(gv = v)\}.$$

It should be obvious that $C_V(G)$ is indeed a linear subspace. An alternative notation is V^G; we avoid it.

5.2.2. Lemma. *Let G be a finite group and $\mathbb{K}$ be a field of coprime characteristic. Let V, V_1, V_2 be $\mathbb{K}$-linear, finite-dimensional representations with character χ, χ_1, χ_2.*

(i) $\dim_{\mathbb{K}} C_V(G) = \frac{1}{|G|}\sum_{g\in G}\chi(g)$.

(ii) $\dim \mathrm{Hom}_{\mathbb{K}[G]}(V_1, V_2) = (\chi_1|\chi_2)$.

One should be careful that these are formulas in $\mathbb{K}$. The right-hand could be 0 for a bad reason; typically if the left-hand is divisible by the characteristic.

Proof.

(i) Consider the following linear endomorphism of V:

$$\pi = \frac{1}{|G|}\sum_{g\in G} g.$$

For $h \in G$ one has:

$$h \circ \pi = \frac{1}{|G|}\sum_{g\in G} hg = \frac{1}{|G|}\sum_{hg\in G} hg = \pi.$$

It follows that $\pi^2 = \frac{1}{|G|}\sum_{h\in G} h\pi = \frac{1}{|G|}\sum_{h\in G}\pi = \pi$. So π is a linear projector. Let us determine its image. If $v \in C_V(G)$ then $\pi(v) = v$. Conversely, if $v \in V$, then for any $h \in G$ one has $h\pi(v) = \pi(v)$, so $\pi(v) \in C_V(G)$.

Thus π is a projector with image $C_V(G)$ (we do not care for its kernel). Now for any projector, $\operatorname{tr}\pi = \dim \operatorname{im}\pi$; here this gives:

$$\dim C_V(G) = \dim \operatorname{im}\pi = \operatorname{tr}\pi = \frac{1}{|G|}\sum_{g\in G}\operatorname{tr} g = \frac{1}{|G|}\sum_{g\in G}\chi(g).$$

(ii) Consider the $\mathbb{K}$-linear representation of G:

$$\mathrm{Hom}_{\mathbb{K}}(V_1, V_2),$$

whose character is $\chi_1^*\chi_2$ by Proposition 4.3.3 (iv). We investigate the G-trivial space.

A $\mathbb{K}$-linear map $f\colon V_1 \to V_2$ is invariant under the action of G iff $g \cdot f = f$ iff $\rho_2(g)\circ f \circ \rho_1(g^{-1}) = f$ iff $\rho_2(g)\circ f = f \circ \rho_1(g)$ iff f is G-covariant. Hence:

$$C_{\mathrm{Hom}_{\mathbb{K}}(V_1,V_2)}(G) = \mathrm{Hom}_{\mathbb{K}[G]}(V_1, V_2).$$

The dimension of the above is given by (i):

$$\dim \mathrm{Hom}_{\mathbb{K}[G]}(V_1, V_2) = \frac{1}{|G|} \sum_{g \in G} \chi_1^*(g)\chi_2(g) = (\chi_1|\chi_2)\,. \qquad \square$$

5.3 Orthonormality

5.3.1. Lemma. *Let G be a finite group and $\mathbb{K}$ be a good field. Let V_1, V_2 be two $\mathbb{K}$-linear, finite-dimensional representations with characters χ_1, χ_2.*

(i) If V_1 and V_2 are irreducible, then $(\chi_1|\chi_2) = \begin{cases} 1 & \text{if } V_1 \simeq V_2 \\ 0 & \text{otherwise.} \end{cases}$

(ii) Every irreducible representation is determined by its character. If $\operatorname{char} \mathbb{K} = 0$, this extends to every finite-dimensional representation.

(iii) The multiplicity of an irreducible representation T in reg *is exactly $\dim T$, viz.:*

$$\mathrm{reg} \simeq \bigoplus_{T \in \mathrm{Irr}_{\mathbb{K}}(G)} T^{\dim T}.$$

Proof.

(i) Recall from Lemma 5.2.2 (ii) that $\dim \mathrm{Hom}_{\mathbb{K}[G]}(V_1, V_2) = (\chi_1|\chi_2)$.

- If V_1 and V_2 are two non-isomorphic, irreducible representations, then $\mathrm{Hom}_{\mathbb{K}[G]}(V_1, V_2) = \{0\}$ by Schur's Lemma, so $(\chi_1|\chi_2) = 0$.
- If V_1 and V_2 are irreducible and isomorphic, then on the one hand $\chi_2 = \chi_1$, and on the other hand, always by Schur's Lemma, $\mathrm{Hom}_{\mathbb{K}[G]}(V_1, V_2) \simeq \mathbb{K}$ is 1-dimensional. So $(\chi_1|\chi_2) = \frac{|G|}{|G|} = 1$.

(ii) The irreducible case is trivial from (i). Now suppose $\operatorname{char} \mathbb{K} = 0$. Let V be a finite-dimensional representation V; then by Corollary 3.3.7, there are integers n_T such that:

$$V \simeq \bigoplus_{T \in \mathrm{Irr}_{\mathbb{K}}(G)} T^{n_T}.$$

Then $\chi_V = \sum n_T \chi_T$ where χ_T is the character of T. By linear independence of the orthonormal family, χ_V completely determines the elements $n_T \in \mathbb{K}$.

Now the ring morphism $\mathbb{Z} \to \mathbb{K}$ is injective in characteristic 0, so χ_V even determines the *integers* $n_T \in \mathbb{Z}$. It therefore determines the isomorphism type.

(iii) A priori $\mathrm{reg} = \sum n_\chi \chi$ where the sum ranges over irreducible characters. We now determine the integers n_χ. By orthonormality, for any irreducible ψ one has:

$$(\mathrm{reg}|\psi) = \sum_{\chi \in \mathrm{Irr}_{\mathbb{K}}(G)} (n_\chi \chi|\psi) = \sum_{\chi \in \mathrm{Irr}_{\mathbb{K}}(G)} n_\chi \delta_{\chi,\psi} = n_\psi\, (\psi|\psi) = n_\psi.$$

Now reg is the permutation character attached to the regular representation: if $g \neq 1$, then $g \cdot e_h = e_{gh}$. So the matrix coding the action of g is a permutation matrix avoiding the diagonal, meaning $\mathrm{reg}(g) = 0$. In particular, for *any* character ψ one has:

$$(\mathrm{reg}|\psi) = \frac{1}{|G|}\sum_{g\in G}\mathrm{reg}(g^{-1})\psi(g) = \frac{1}{|G|}\mathrm{reg}(1)\psi(1) = \psi(1).$$

Applying to irreducible χ, we get $n_\chi = \chi(1) = \dim\chi$, as wanted. $\square$

Notice that the above also holds of $[\cdot|\cdot]$ when working over (a subfield of) $\mathbb{C}$.

5.3.2. Remarks.

- Lemma 5.3.1 can be used to give a quick proof *in characteristic* 0 that a finite-dimensional representation V is irreducible iff V^* is. (This is true in any characteristic, but the general argument is more geometric: see exercise 2.5.5. Also see Remark 3.3.8.)

  Indeed, V is irreducible iff $(\chi_V|\chi_V) = 1$. This is because a priori, $V \simeq \bigoplus_T T^{n_T}$; now $(\chi_V|\chi_V) = \sum n_T^2$ in $\mathbb{K}$. But in characteristic 0, this can equal 1 iff there is a unique non-zero n_T, which equals 1. This proves the claim.

  Finally notice that $(\chi_V^*|\chi_V^*) = (\chi_V|\chi_V)$.

- The above proof does *not* work in positive characteristic $p > 0$ (even over a good field). Indeed, for $V = \mathrm{triv} \oplus T^p$ one gets $(\chi_V|\chi_V) = 1$ but V is certainly *not* irreducible. The reason is that here, $(\chi_V|\chi_V)$ is not an absolute integer $\in \mathbb{Z}$, but an element of the prime field of $\mathbb{K}$.

5.4 The space of class functions

We need one last fact to prove Theorem 5.1.1.

5.4.1. Proposition. *Let G be a finite group and $\mathbb{K}$ be a good field. Then* $\mathrm{Irr}_{\mathbb{K}}(G)$ *spans* $\mathcal{C}_{\mathbb{K}}(G)$.

Proof. Let $\alpha\colon G \to \mathbb{K}$ be a class function. We shall prove that $\alpha = \sum_{\chi\in\mathrm{Irr}\,\mathbb{K}(G)} (\chi|\alpha)\,\chi$. Considering the difference $\alpha - \sum_{\chi\in\mathrm{Irr}\,\mathbb{K}(G)} (\chi|\alpha)\,\chi$, it suffices to prove that a class function orthogonal to all irreducible characters is trivial.

So let α be such. Let $V = \mathrm{reg}$ be the regular representation and

$$f = \frac{1}{|G|}\sum_{g\in G}\alpha(g)g \in \mathrm{End}_{\mathbb{K}}(V).$$

Since α is a class function, one can easily show that f is G-covariant (see exercise 5.6.4), hence $f \in \mathrm{End}_{\mathbb{K}[G]}(\mathrm{reg})$.

Let $W \leq \mathrm{reg}$ be any *irreducible* subrepresentation, with character χ. By construction, W is f-invariant; moreover f remains an endomorphism of W. So by Schur's Lemma there is $\lambda \in \mathbb{K}$ such that $f_{|W} = \lambda\,\mathrm{Id}_W$. Then:

$$\lambda \dim W = \mathrm{tr}\, f_{|W} = \frac{1}{|G|}\sum_{g\in G}\alpha(g)\,\underbrace{\mathrm{tr}\, g_{|W}}_{=\chi(g)} = (\chi^*|\alpha)\,.$$

Now χ^* is an irreducible character, so by assumption the above is 0; hence $\lambda = 0$ and

$f_{|W} = 0$.

So f vanishes on all irreducible subrepresentations of reg. The latter is a direct sum of irreducible representations by Maschke's Theorem, so $f = 0$ globally. Finally $f(e_1) = \frac{1}{|G|} \sum_{g \in G} \alpha(g) e_g = 0$, meaning that α is identically 0. We are done. $\square$

5.5 Column orthogonality

Orthogonality has uncountable consequences. A useful tool is provided by the following lemma.

5.5.1. Lemma (column orthogonality). *Let G be a finite group and $\mathbb{K}$ be a good field. Then for any two conjugacy classes γ_1, γ_2, one has:*

$$\sum_{\chi \in \mathrm{Irr}_{\mathbb{K}}(G)} \chi(\gamma_1^{-1}) \chi(\gamma_2) = \begin{cases} \frac{|G|}{\#\gamma_1} & \text{if } \gamma_1 = \gamma_2 \\ 0 & \text{otherwise.} \end{cases}$$

Proof. We use matrix theory. Let $A = (\chi(\gamma))_{\chi,\gamma}$ be the character table. We also need the version with inverses: $B = (\chi(\gamma^{-1}))_{\chi,\gamma}$. Last, let J be the *diagonal* matrix:

$$J = \begin{pmatrix} \frac{\#\gamma_1}{|G|} & & \\ & \ddots & \\ & & \frac{\#\gamma_r}{|G|} \end{pmatrix}.$$

By orthogonality, the (χ_1, χ_2)-entry of the product BJA^t is:

$$(BJA^t)_{\chi_1,\chi_2} = \sum_{\gamma \in \mathrm{Conj}(G)} \chi_1(\gamma^{-1}) \frac{\#\gamma}{|G|} \chi_2(\gamma) = \frac{1}{|G|} \sum_{g \in G} \chi_1(g^{-1}) \chi_2(g) = \delta_{\chi_1,\chi_2}.$$

Hence $BJA^t = I$ is the identity matrix. This implies $AJB^t = I$, and $B^t A = J^{-1}$. The latter gives, at (γ_1, γ_2):

$$\sum_{\chi \in \mathrm{Irr}_{\mathbb{K}}(G)} \chi(\gamma_1^{-1}) \chi(\gamma_2) = (B^t A)_{\gamma_1,\gamma_2} = (J^{-1})_{\gamma_1,\gamma_2} = \delta_{\gamma_1,\gamma_2} \frac{|G|}{\#\gamma_1}.$$ $\square$

5.6 Exercises

5.6.1. Exercise. *Let V be an irreducible representation and L be a 1-dimensional representation. Prove that $V \otimes L$ is irreducible.*

5.6.2. Exercise (column orthogonality). *Let G be a finite group and $\mathbb{K}$ be a good field.*

1. *Prove that x, y are conjugate iff $(\forall \chi \in \mathrm{Irr}_{\mathbb{C}}(G))(\chi(g) = \chi(h))$.*
2. *If $\mathbb{K} \leq \mathbb{C}$, prove that the square matrix $\left(\chi(\gamma) \cdot \sqrt{\frac{\#\gamma}{|G|}}\right)$ is unitary.*

5.6.3. Exercise. *Let G be finite and V be a linear, complex, irreducible representation. Prove that* $(\dim V)^2 \leq [G : Z(G)]$.

5.6.4. Exercise. *Let $\alpha\colon G \to \mathbb{K}$ be any map. For V a $\mathbb{K}$-linear representation of G, let:*

$$f_{\alpha,V} = \frac{1}{|G|}\sum_{g\in G}\alpha(g)g\colon V \to V.$$

Prove that the following are equivalent:

(i) α *is a class function;*

(ii) *for every representation V, $f_{\alpha,V}$ is a G-covariant endomorphism of V;*

(iii) *$f_{\alpha,\mathrm{reg}}$ is a G-covariant endomorphism of* reg.

5.6.5. Exercise. *Let G be a finite group and $\mathbb{K}$ be a good field of positive characteristic. Let V, V' be finite-dimensional representations with the same character. Prove that there are natural integers n_T and n'_T with $T \in \mathrm{Irr}_{\mathbb{K}}(G)$ such that:*

- *for each T, at least one of n_T or n'_T is* 0*,*
- *for each T, both n_T and n'_T are divisible by* $\mathrm{char}\,\mathbb{K}$*,*
- *one has:*

$$V \oplus \bigoplus_T T^{n_T} \simeq V' \oplus \bigoplus_T T^{n'_T} \quad [\mathbb{K}[G]\text{-}\mathbf{Mod}].$$

(*) **5.6.6. Exercise.** *Let $\mathbb{K}$ be a good field. Let V be a $\mathbb{K}$-linear, finite-dimensional representation and $T \in \mathrm{Irr}_{\mathbb{K}}(G)$. Prove that the projector onto $\mathrm{Iso}_T(V)$ parallel to the other terms $\bigoplus_{T'\neq T}\mathrm{Iso}_{T'}(V)$ is given by:*

$$\pi_T = \frac{\dim T}{|G|}\sum_{g\in G}\chi_T(g^{-1})g.$$

6 Computing character tables

Abstract. A problem session.

We give a couple of character tables over $\mathbb{C}$. For each, I try to give a flow of natural arguments to determine it, and then a flow of natural comments on it. But there are many approaches to the same problem, so some of the remarks could be used in the determination process. *The only way to read the notes for this section is by actually trying to construct the tables yourself.*

Sym(1)=Alt(2)

- There is nothing to say before or after.

Sym(1)	1 [×1]
triv	1

Alt(3)

- Alt(3) is abelian.
- By abelianity, conjugacy classes have one element, so there are three of them.
- By abelianity again, the irreducible representations have dimension 1, hence are simply morphisms $\mathrm{Alt}(3) \to \mathbb{C}^\times$. We need three of them (including triv).
- For a non-trivial morphism $\mathrm{Alt}(3) \to \mathbb{C}^\times$, the image of (123) in $\mathbb{C}^\times$ must have order 3. Let $j = e^{\frac{2i\pi}{3}}$.

Alt(3)	1 [×1]	(123) [×1]	(132) [×1]
triv	1	1	1
χ_1	1	j	j^2
ψ_1	1	j^2	j

- Here the orthogonality relations essentially reduce to: $1+1+1 = 3$, and $1+j+j^2 = 0$.
- Observe how $\chi_1^* = \psi_1 = \chi_1 \otimes \chi_1$.

Sym(3)

- There are three conjugacy classes and we easily find their cardinalities.
- Therefore there are three irreducible representations.
- In addition to triv, there is the signature representation sign. We miss one more.
- Let d be its dimension. Since $(\dim \mathrm{triv})^2 + (\dim \mathrm{sign})^2 + d^2 = |\mathrm{Sym}(3)| = 6$, the last irreducible representation is 2-dimensional. Call it χ_2.
- One can predict that χ_2 is real-valued, and vanishes on (12). Indeed:
  - By exercise 2.5.5 or Remark 5.3.2, χ_2^* is an irreducible, 2-dimensional representation. But only χ_2 is irreducible and 2-dimensional, so $\chi_2^* = \chi_2$, which means it is real-valued.
  - $\chi_2 \otimes \mathrm{sign}$ is an irreducible, 2-dimensional representation (exercise 5.6.1), so $\chi_2 \otimes \mathrm{sign} = \chi_2$. But $\mathrm{sign}((12)) = -1$, so $\chi_2((12)) = 0$.

  One could use orthogonality to find $\chi_2((123))$, but geometry is more natural.
- Let perm_3 be the permutation representation, which is 3-dimensional. Clearly $\mathrm{perm}_3(1) = 3$, $\mathrm{perm}_3((12)) = 1$, and $\mathrm{perm}_3((123)) = 0$. Thus, $\left(\mathrm{perm}_3 | \mathrm{perm}_3\right) = \frac{1}{6}(9 \times 1 + 1 \times 3 + 0 \times 2) = 2$. So perm_3 is the sum of *two* irreducible representations. One of them must have dimension 2: thus χ_2 is a subrepresentation of perm_3.
- Of course $e_1 + e_2 + e_3 \in \mathrm{perm}_3$ is fixed by $\mathrm{Sym}(3)$, so perm_3 contains a copy of triv.
- By the above, $\chi_2 = \mathrm{perm}_3 - \mathrm{triv}$, and we get the table.

Sym(3)	1 [×1]	(12) [×3]	(123) [×2]
triv	1	1	1
sign	1	−1	1
χ_2	2	0	−1

- Let us check orthogonality: • $1^2 \times 1 + 1^2 \times 3 + 1^2 \times 2 = 6$ expresses $(\mathrm{triv}|\mathrm{triv}) = 1$; • $1^2 \times 1 + (-1)^2 \times 3 + 1^2 \times 2 = 6$ expresses $(\mathrm{sign}\,|\,\mathrm{sign}) = 1$; • $1 \times 1 + (-1) \times 3 + 1 \times 2 = 0$ expresses $(\mathrm{triv}|\,\mathrm{sign}) = 0$; • and so on.

- As predicted, $\chi_2 = \chi_2^* = \chi_2 \cdot \mathrm{sign}$.

Alt(4)

- One should be careful with conjugacy classes. Although (123) and (132) are conjugate in Sym(4), the Sym(4)-conjugacy class 'breaks' into two when going down to Alt(4). This produces *two* Alt(4)-classes of the same size. With this in mind, or just remembering $\mathrm{Alt}(4) \simeq C_2^2 \rtimes C_3$, we find 4 conjugacy classes and count their elements.

- There are 4 irreducible representations and triv is one of them. (For $\mathrm{Alt}(n)$, by definition sign = triv.) We need three more.

- Let $K = \{1, (12)(34), (13)(24), (14)(23)\} \leq \mathrm{Alt}(4)$, the (very important) subgroup of bitranspositions. It is normal and $\mathrm{Alt}(4)/K$ has order 3, hence is abelian. Now each representation of $\mathrm{Alt}(4)/K$ gives one of Alt(4) (by letting K act trivially).

- This way we gain two 1-dimensional representations of Sym(4): just 'lifting' those of $\mathrm{Sym}(4)/K \simeq \mathrm{Sym}(3)$. Call them χ_1 and ψ_1.

- We need one more. Its dimension satisfies $3 + d^2 = 12$, so the dimension is 3.

- Of course it is $\mathrm{perm}_4 - \mathrm{triv}$, which is indeed irreducible by computation.

Alt(4)	1 [×1]	(123) [×4]	(132) [×4]	(12)(34) [×3]
triv	1	1	1	1
χ_1	1	j	j^2	1
$\psi_1 = \chi_1^*$	1	j^2	j	1
χ_3	3	0	0	-1

- Orthogonality can be checked, or simply deduced. Indeed, since $\chi_3 = \mathrm{perm}_4 - \mathrm{triv}$ is irreducible, it *must* be the missing irreducible character. By orthogonality, we know it is orthogonal to the others.

- Here is the geometric realisation of χ_3.

  Consider the tetrahedron centered at the origin, whose vertices are:

  $$v_1 = (1,1,1), \quad v_2 = (1,-1,-1), \quad v_3 = (-1,1,-1), \quad v_4 = (-1,-1,1).$$

  Alt(4) acts on this tetrahedron. It is a good exercise to explicitly write the matrices in $\{e_1, e_2, e_3\}$, but we simply determine the character—in the basis $\{v_1, v_2, v_3\}$, where computations are easy.

  - (123) is a circular permutation of the same basis; the trace is 0. The same applies to its inverse.
  - Now $(12)(34)$ swaps v_1 and v_2, but takes v_3 to $v_4 = -v_1 - v_2 - v_3$. So the trace is -1.

  And we retrieve χ_3. This geometric argument gives it directly, and not as a quotient of perm_4.

Sym(4)

- There are 5 conjugacy classes.
- We already know two irreducible representations: triv and sign.
- Now perm_4 – triv is again irreducible, and we can compute its character χ_3.
- Then $\chi_3^* = \chi_3$, but χ_3 sign $\neq \chi_3$, so we just produced a fourth irreducible representation.
- Computation reveals that the missing one has dimension 2. One can predict $\chi_2^* = \chi_2$ (real values) and χ_2 sign $= \chi_2$ (so it vanishes where sign $= -1$). One could then use orthogonality to compute the missing values.
- Now $K = \{1, (12)(34), (13)(24), (14)(23)\}$ remains normal in Sym(4). This is most remarkable as normality is not transitive in general. Here, $K = \mathrm{Alt}(4)'$ and $\mathrm{Alt}(4) = \mathrm{Sym}(4)'$ are so-called *characteristic subgroups*, and being characteristic is transitive.
- Then $\mathrm{Sym}(4)/K \simeq \mathrm{Sym}(3)$. It suffices to extend the irreducible 2-dimensional representation of Sym(3) by letting K act trivially. Now in any isomorphism $\mathrm{Sym}(4)/K \simeq \mathrm{Sym}(3)$, the image of a 4-cycle becomes a transposition, while a bitransposition becomes the identity: this gives the values of χ_2.

Sym(4)	1 [×1]	(12) [×6]	(123) [×8]	(1234) [×6]	(12)(34) [×3]
triv	1	1	1	1	1
sign	1	−1	1	−1	1
χ_2	2	0	−1	0	2
χ_3	3	1	0	−1	−1
$\psi_3 = \chi_3 \otimes$ sign	3	−1	0	1	−1

- Here again, the geometric interpretation of χ_3 is by acting on the tetrahedron. In the notation above, (12) swaps v_1 and v_2, but fixes v_3 (and v_4). So $\chi_3((12)) = 1$. Likewise, (1234) takes v_1 to v_2, v_2 to v_3, and v_3 to $v_4 = -v_1 - v_2 - v_3$; thus $\chi_3((1234)) = -1$.
- The geometric interpretation of χ_2 is different. Since $K \trianglelefteq \mathrm{Sym}(4)$, there is a conjugation action on the set $X = K \smallsetminus \{1\}$. It is transitive. This gives us a 3-dimensional permutation representation.

  Whenever one has a permutation representation, the vector $\sum_X e_x$ is fixed by G, so here perm_X contains (at least) a copy of triv.

  One checks that $\chi_2 = \mathrm{perm}_X - \mathrm{triv}$.

Alt(5)

- Since Alt(5) is simple, the situation is completely different now (and interesting at last).
- In Alt(5), (123) is conjugate to its inverse (132). One may *not* use $(23) \notin \mathrm{Alt}(5)$ to perform this conjugation, but $(23)(45) \in \mathrm{Alt}(5)$ does as well.

- However, (12345) is *not* $\mathrm{Alt}(5)$-conjugate to its inverse (15432): the $\mathrm{Sym}(5)$-class of 5-cycles breaks into two $\mathrm{Alt}(5)$-classes of equal size.
- In addition to triv, one easily finds the irreducible character perm − triv; it has dimension 4. We need *three* more, and number theory gives dimensions $3, 3, 5$.
- There are no subgroups of index 3 or 4, so actions on coset spaces are limited. Also, the action on cosets of $\mathrm{Alt}(4) \leq \mathrm{Alt}(5)$ is equivalent to perm: this gives nothing new.
- An educated guess and 5-dimensionality suggest to look for a permutation representation on 6 elements, and Sylow theory provides one.
- $\mathrm{Alt}(5)$ has exactly 6 Sylow 5-subgroups, all of order 5.
- Let $P = \langle(12345)\rangle$; this is a Sylow 5-subgroup. Then $[G : N_G(P)] = 6$ so $N_G(P)$ has order 10.
- This implies that in the conjugation action, an element of order 3 fixes *no* Sylow 5-subgroup.
- $|N_G(P)| = 10$ also implies that P is acted on by (the group generated by) a bitransposition; in abstract terms, $N_G(P) \simeq C_5 \rtimes C_2$.
- The bi-transposition $(12)(34)$ fixes exactly *two* Sylow 5-subgroups: the one generated by (12354), and the one generated by (12453). (This can be seen because it inverts said generators.) But it fixes no other Sylow 5-subgroup and this remains to be seen.
- A good approach is by Burnside's classical 'fixed point formula'. For any finite group action $G \curvearrowright X$, one has:

$$\sum_G \# \operatorname{Fix} g = \sum_{(G,X)} \mathbf{1}_{g\cdot x = x} = \sum_X |\operatorname{Stab}_G(x)|.$$

  Here, the identity fixes 6 elements, a 3-cycle fixes 0, a 5-cycle fixes 1 (because if a 5 element normalises a Sylow 5-subgroup, it is already inside). There remains $15 \cdot \# \operatorname{Fix}(12)(34) = 60 - 6 - 12 - 12 = 30$, and therefore $\# \operatorname{Fix}(12)(34) = 2$.
- This gives us $\mathrm{perm}_{\mathrm{Syl}}$, and we can check that $\chi_5 = \mathrm{perm}_{\mathrm{Syl}} - \mathrm{triv}$ is irreducible and 5-dimensional.
- We miss two more irreducible characters, say φ_3 and φ_3'. We do not know whether they will be complex-conjugate, or if each will be sel-dual (real-valued). We then use brute force: orthogonality relations.
- Let $a = \varphi_3((123))$, $b = \varphi_3((12)(34))$, $c = \varphi_3((12345))$ and $d = \varphi_3((15432))$. Define a', b', c', d' similarly.
- By orthogonality:

$$\begin{aligned} 0 &= |G|\,(\mathrm{triv}|\varphi_3) = 3 + 20a + 15b + 12c + 12d \\ 0 &= |G|\,(\chi_4|\varphi_3) = 12 + 20a - 12c - 12d \\ 0 &= |G|\,(\chi_5|\varphi_3) = 15 - 20a + 15b. \end{aligned}$$

  This immediately yields $a = 0$, then $b = -1$, and $c + d = 1$.

- We also have:
$$60 = |G|\,(\varphi_3|\varphi_3) = 9 + 15 + 12c^2 + 12d^2,$$
which gives $c^2 + d^2 = 3$.

- Together with $c + d = 1$, this solves into:
$$\{c, d\} = \left\{\frac{1-\sqrt{5}}{2}, \frac{1+\sqrt{5}}{2}\right\} = \{c', d'\},$$
and we finally get the character table.

Alt(5)	1 [×1]	(123) [×20]	(12)(34) [×15]	(12345) [×12]	(15432) [×12]
triv	1	1	1	1	1
φ_3	3	0	−1	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
φ_3'	3	0	−1	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$
χ_4	4	1	0	−1	−1
χ_5	5	−1	1	0	0

- Although φ_3 and φ_3' are self-dual, they are indeed related by a Galois action (but *not* that of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$, which is generated by complex conjugation).

- Representations φ_3 and φ_3' arise in nature, as embeddings $\mathrm{Alt}(5) \hookrightarrow \mathrm{SO}_3(\mathbb{R})$. They are the symmetry groups of the regular icosahedron/dodecahedron.[5]

6.1 Exercises

6.1.1. Exercise. *Give the character tables of the group of isometries of the square (viz. $D_{2\cdot 4}$). Same question with the group of basic quaternions (viz. $\mathbb{H}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$).*
Note. *Thus, two non-isomorphic groups can have the* same *character table.* [6]

6.1.2. Exercise. *Let G be the group of isometries of the Euclidean cube. Give its character table.*

6.1.3. Exercise. *Let $D_{2\cdot n}$ be the dihedral group of order $2n$, viz. the group of transformations of a regular n-gon in the usual plane. Give its character table.*

6.1.4. Exercise. *Compute the character table of* Sym(5). *You should find:*

Sym(5)	1 [×1]	(12) [×10]	(123) [×20]	(1234) [×30]	(12)(34) [×15]	(12345) [×24]	(12)(345) [×20]
triv	1	1	1	1	1	1	1
sign	1	−1	1	−1	1	1	−1
χ_4	4	2	1	0	0	−1	−1
$\chi_4 \cdot$ sign	4	−2	1	0	0	−1	1
χ_5	5	1	−1	−1	1	0	1
$\chi_5 \cdot$ sign	5	−1	−1	1	1	0	−1
χ_6	6	0	0	0	−2	1	0

[5] I have to teach this in the Village someday.

[6] Quite interestingly, the same cannot happen with the earlier, rival theory of *group determinants*. See E. Formanek and D. Sibley, *The group determinant determines the group*, Proc. Amer. Math. Soc. 112(3), pp. 649–656, 1991.
Thanks to Baran Çetin for pointing this out.

6.1.5. Exercise. *Read something about* Young tableaux *and representations of the symmetric group.*

7 Number-theoretic aspects

Abstract. From here on we shall be working in characteristic 0. The kernel of a representation is often called the *character kernel* (§ 7.1); every normal subgroup is an intersection of irreducible character kernels. We then move to using algebraic number theory in character theory (§ 7.2). A first application is a theorem by Burnside: the dimension of an irreducible complex representation divides $|G|$ (§ 7.3).

7.1 Character kernels and their intersections

7.1.1. Definition. Let G be a group and $\mathbb{K}$ be a field. Let (V, ρ) be a finite-dimensional, $\mathbb{K}$-linear representation with character χ. We let $\ker \chi = \ker \rho$ and call it the *kernel* of χ.

This is a slight abuse of terminology since χ itself is not a morphism.

7.1.2. Lemma. *Let G be a finite group and $\mathbb{K}$ be a field. Let (V, ρ) be a finite-dimensional, $\mathbb{K}$-linear, representation with character χ.*

(i) $\ker \chi$ *is a normal subgroup of G.*

(ii) Suppose that $\mathbb{K}$ has characteristic 0. Then $\ker \chi = \{g \in G : \chi(g) = \chi(1)\}$.

Proof. (i) is completely obvious since $\ker \chi = \ker \rho$, a kernel in the usual sense. So we prove (ii). If $g \in \ker \chi$, then $\rho(g) = \mathrm{Id}_V$ so $\chi(g) = \operatorname{tr} \mathrm{Id}_V = \chi(1)$. Conversely suppose $\chi(g) = \chi(1)$; we must prove $\rho(g) = \mathrm{Id}_V$.

As above, $\chi(1) = \operatorname{tr} \mathrm{Id}_V = \dim V$. Also, g has finite order, so there is an integer k with $g^k = 1$, and $\rho(g)^k = \mathrm{Id}_V$. Therefore all eigenvalues of g, even in an algebraic closure, must satisfy this equation.

We finish the proof with $\mathbb{K} = \mathbb{C}$ (see Remark 7.1.3). Then $\rho(g) \in \mathrm{GL}(V)$ is an element of finite order say k. Since the polynomial $X^k - 1$ is split with simple roots, $\rho(g)$ is diagonalisable. Moreover, all its eigenvalues $\lambda_1, \dots, \lambda_{\dim V}$ satisfy $\lambda_i^k = 1$, so they lie on the unit circle. By assumption, their sum is $\dim V$. This is possible only if each $\lambda_i = 1$. So $\rho(g)$ diagonalises to the identity, implying $\rho(g) = \mathrm{Id}_V$, as wanted. □

7.1.3. Remark. It is enough to have $\operatorname{char} \mathbb{K} = 0$. Indeed, all coefficients and eigenvalues of $\rho(g)$ will live in an algebraic extension of $\mathbb{Q}$, so all in $\overline{\mathbb{Q}} \leq \mathbb{C}$, and we safely conduct the argument there.

However (ii) no longer holds in non-zero characteristic. *As opposed to many results, this one already fails in good fields of positive characteristic.*

7.1.4. Theorem. *Let G be a finite group and $\mathbb{K}$ be an algebraically closed field of characteristic 0.*

(i) $\bigcap_{\chi \in \mathrm{Irr}_{\mathbb{K}}(G)} \ker \chi = \{1\}$.

(ii) Let $N \leq G$ be a subgroup. Then $N \trianglelefteq G$ iff there is $J \subseteq \mathrm{Irr}_{\mathbb{K}}(G)$ such that $N = \bigcap_{\chi \in J} \ker \chi$.

Proof.

(i) Let $K = \bigcap_{\chi\in\mathrm{Irr}_{\mathbb{K}}(G)} \ker\chi$, an intersection of normal subgroups. We must show $K = \{1\}$. Let us fix some notation. First, let $\pi_K\colon G \to G/K$ be the canonical projection.

Let $\chi \in \mathrm{Irr}_{\mathbb{K}}(G)$. Then χ is the character of some irreducible, complex, linear representation (V_χ, ρ_χ), viz. we have a morphism $\rho_\chi\colon G \to \mathrm{GL}(V_\chi)$. Since $K \leq \ker\rho_\chi$, one may factor and consider:

$$\check{\rho}_\chi\colon G/K \to \mathrm{GL}(V_\chi).$$

By definition, $\rho_\chi = \check{\rho}_\chi \circ \pi_K$.

We claim that $\check{\rho}_\chi$ is an irreducible representation of G/K. This is obvious since K acts trivially on V_χ, so G-invariant subspaces are the same as G/K-invariant subspaces.

Let $\check{\chi}$ be the character of $\check{\rho}_\chi$. Thus $\check{\chi} \in \mathrm{Irr}_{\mathbb{K}}(G/K)$. Again, $\chi = \check{\chi}\circ\pi$. It follows that if $\chi_1 \neq \chi_2$ in $\mathrm{Irr}_{\mathbb{K}}(G)$, then $\check{\chi}_1 \neq \check{\chi}_2$ in $\mathrm{Irr}_{\mathbb{K}}(G/K)$. So characters $\check{\chi}$ for $\chi \in \mathrm{Irr}_{\mathbb{K}}(G)$ are distinct elements of $\mathrm{Irr}_{\mathbb{K}}(G/K)$, meaning $\{\check{\chi} : \chi \in \mathrm{Irr}_{\mathbb{K}}(G)\} \subseteq \mathrm{Irr}_{\mathbb{K}}(G/K)$.

By the orthogonality relations:

$$|G| = \sum_{\chi\in\mathrm{Irr}_{\mathbb{K}}(G)} \chi(1)^2 = \sum_{\chi\in\mathrm{Irr}_{\mathbb{K}}(G)} \check{\chi}(1)^2 \leq \sum_{\psi\in\mathrm{Irr}_{\mathbb{K}}(G/K)} \psi(1)^2 = |G/K|,$$

which proves $|K| = 1$, as desired.

(ii) The converse implication is obvious, so suppose $N \trianglelefteq G$. Let $\pi_N\colon G \to G/N$ be the canonical projection. We consider $\mathrm{Irr}_{\mathbb{K}}(G/N)$, whose elements are the irreducible characters ψ, attached to morphisms $\sigma_\psi\colon G/N \to \mathrm{GL}(V_\psi)$.

For $\psi \in \mathrm{Irr}_{\mathbb{K}}(G/N)$, let:

$$\rho_\psi = \sigma_\psi \circ \pi_N\colon G \to \mathrm{GL}(V_\psi).$$

We claim that ρ_ψ is an irreducible representation of G. Indeed, a G-invariant subspace of V_ψ is also G/N-invariant, hence $\{0\}$ or V_ψ by irreducibility of σ_ψ.

Let $\hat{\psi}$ be the character of ρ_ψ. Thus $\hat{\psi} \in \mathrm{Irr}_{\mathbb{K}}(G)$. Again, $\hat{\psi} = \psi \circ \pi_N$. It follows that if $\psi_1 \neq \psi_2$ in $\mathrm{Irr}_{\mathbb{K}}(G/N)$, then $\hat{\psi}_1 \neq \hat{\psi}_2$ in $\mathrm{Irr}_{\mathbb{K}}(G)$. (This is because π_N is onto.) So $J = \{\hat{\psi} : \psi \in \mathrm{Irr}_{\mathbb{K}}(G/N)\}$ is a family of irreducible characters of G.

We claim that $N = \bigcap_{\chi\in J} \ker\chi$. Indeed,

$$\bigcap_{\chi\in J} \ker\chi = \bigcap_{\psi\in\mathrm{Irr}_{\mathbb{K}}(G/N)} \ker\rho_\psi = \bigcap_{\mathrm{Irr}_{\mathbb{K}}(G/N)} \ker(\sigma_\psi \circ \pi_N) = \pi_N^{-1}\left(\bigcap_{\mathrm{Irr}_{\mathbb{K}}(G/N)} \ker\sigma_\psi\right).$$

By (i) applied to G/N, the latter intersection is $\{1 \mod N\}$, so $\bigcap_{\chi\in J} \ker\chi = \pi_N^{-1}(1) = N$, as wanted. □

7.2 Algebraic integers

7.2.1. Definition. Let R be a ring with 1. An element $x \in R$ is *integral* (over $\mathbb{Z}$) if there is a polynomial $P \in \mathbb{Z}[X]$ with leading coefficient 1 such that $P(x) = 0$.

One often denotes by $\mathbb{O}_R$ the set of integral elements of R.

7.2.2. Remark. Since $R[x]$ is always commutative, commutativity of R is not required for the general definition. (But one needs $1 \in R$ for the definition.)

If $R = \mathbb{C}$, one calls x an *algebraic integer*; we simply write $\mathbb{O} = \mathbb{O}_{\mathbb{C}}$.

7.2.3. Remark. Algebraic *integers* are not to be mistaken with algebraic *numbers*, where the condition on the leading coefficient is removed. Algebraic numbers exactly form the field $\overline{\mathbb{Q}}$; but $\mathbb{O}$ is a proper subring of $\overline{\mathbb{Q}}$.

7.2.4. Example. $\sqrt{2}$ is an algebraic integer; $\frac{1}{2}$ is not.

7.2.5. Proposition. *If R is a commutative ring with unit, then $\mathbb{O}_R$ is a subring of R.*

Proof. Clearly $0, 1$ are in $\mathbb{O}_R$, and $\mathbb{O}_R$ is closed under $-$; so we need closedness under $+$ and $\cdot$.

7.2.6. Lemma. *Let $x \in R$. Then $x \in \mathbb{O}_R$ iff $\mathbb{Z}[x]$ is finitely generated as an abelian group.*

Commutativity of R is not required in the Lemma, since $R[x]$ always is commutative.

Proof. If x is integral and $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$ vanishes at x, then clearly $\mathbb{Z}[x]$ is generated by $\{1, x, \dots, x^{n-1}\}$ as an abelian group.

We prove the converse. For $n \in \mathbb{N}$, let R_n be the abelian group generated by $\{1, \dots, x^{n-1}\}$. Then (R_n) is an ascending chain of abelian subgroups with union $\mathbb{Z}[x]$. But the latter is finitely generated, so there is n such that R_n contains all generators. Then $R_{n+1} = R_n$. This implies $x^{n+1} \in R_n$, so x is integral. □

If x and y are algebraic integers, then $\mathbb{Z}[x]$ and $\mathbb{Z}[y]$ are finitely generated, and so is their tensor product $\mathbb{Z}[x] \otimes_{\mathbb{Z}} \mathbb{Z}[y]$, which maps onto $\mathbb{Z}[x, y]$. The latter contains $\mathbb{Z}[x + y]$ and $\mathbb{Z}[x \cdot y]$. It is not true in general that subgroups of finitely generated groups are finitely generated, but this holds of abelian groups. □

7.2.7. Remark. Proposition 7.2.5 requires commutativity of R. The reason is that the proof uses that $\mathbb{Z}[x, y]$ is an image of $\mathbb{Z}[x] \times \mathbb{Z}[y]$, which holds only if x and y commute. See Remark 7.3.2.

7.2.8. Lemma. $\mathbb{O} \cap \mathbb{Q} = \mathbb{Z}$.

Proof. The converse inclusion is obvious. Suppose $x = \frac{p}{q} \in \mathbb{O}$ where p and q are coprime. Since $x \in \mathbb{O}$, there is a polynomial $P = X^n + a_{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$ with leading coefficient 1 such that $P(x) = 0$. Multiplying by q^n one has:

$$p^n + a_{n-1}qp^{n-1} + \cdots + a_0 q^n = 0$$

Since p and q are coprime, one has $q = 1$, so $x \in \mathbb{Z}$. □

Characters and algebraic integers.

7.2.9. Proposition. *Let G be a finite group and χ be a complex character. Then χ takes values in $\mathbb{O}$.*

Proof. Write $\rho(g)$ in diagonal form. Diagonal entries are roots of unity, hence algebraic integers. So their sum $\chi(g)$ is an algebraic integer. □

7.3 A Theorem of Burnside

7.3.1. Theorem. *Let V be a complex, irreducible representation of a finite group G. Then* $\dim V$ *divides* $|G|$.

Proof. Let V be an irreducible representation of G and let χ be its character; we wish to prove that $\dim V$ divides $|G|$.

Let γ be a conjugacy class and $f_\gamma = \sum_{g\in\gamma} \rho(g) \colon V \to V$. Then f_γ is G-covariant, so by Schur's Lemma there is $\lambda_\gamma \in \mathbb{C}$ with $f_\gamma = \lambda_\gamma \operatorname{Id}$. Furthermore, taking the trace one has:

$$\lambda_\gamma \dim V = \sum_{g\in\gamma} \chi(g) = \#\gamma \cdot \chi(\gamma).$$

Step 1. $\lambda_\gamma \in \mathbb{O}$.

Verification. While it is now clear that $\chi(\gamma) \in \mathbb{O}$ and $\#\gamma \cdot \chi(\gamma) \in \mathbb{O}$, we even want $\lambda_\gamma = \frac{\#\gamma\cdot\chi(\gamma)}{\dim V} \in \mathbb{O}$. Division is not permitted so there is something to prove.

One could argue as follows in the group ring $\mathbb{Z}[G]$ (§ 13):

> Let $e_\gamma = \sum_{g\in\gamma} g \in \mathbb{Z}[G]$. Then $e_\gamma \in Z(\mathbb{Z}[G])$. The latter is a commutative ring, and finitely generated as a group. So $e_\gamma \in \mathbb{O}_{Z(\mathbb{Z}[G])} \leq \mathbb{O}_{\mathbb{Z}[G]}$. Thus $\rho(e_\gamma) = f_\gamma = \lambda_\gamma \operatorname{Id}_V$ is an algebraic integer of $\operatorname{End}(V)$, and $\lambda_\gamma \in \mathbb{O}$.

But we have *not* introduced the algebraic object $\mathbb{Z}[G]$. (Also, be careful; see Remark 7.3.2.) We therefore give an ad hoc argument which will reappear in Lemma 8.2.1.

Let δ be another conjugacy class. For $x \in G$ let $X_{\gamma,\delta} = \{(g,h) \in \gamma \times \delta : x = gh\}$. Then:

$$f_\gamma f_\delta = \sum_{g\in\gamma}\sum_{h\in\delta} \rho(gh) = \sum_{x\in G}\left(\sum_{(g,h)\in X_{\gamma,\delta}} \rho(x)\right) = \sum_{x\in G} \#X_{\gamma,\delta}\rho(x).$$

Actually $\#X_{\gamma,\delta}$ depends only on the conjugacy class of x. Indeed, if $x' = x^y \in x^G$, then the map $(g,h) \mapsto (g^y, h^y)$ defines a bijection $X_{\gamma,\delta} \simeq X'_{\gamma,\delta}$. So the integer $\#X_{\gamma,\delta}$ is constant on x^G. Therefore there are integers $n_{\gamma,\delta,\varepsilon}$ such that:

$$f_\gamma f_\delta = \sum_{\varepsilon\in\operatorname{Conj}(G)} \sum_{x\in\varepsilon} n_{\gamma,\delta,\varepsilon}\rho(x) = \sum_{\varepsilon\in\operatorname{Conj}(G)} n_{\gamma,\delta,\varepsilon} f_\varepsilon.$$

Returning to the irreducible representation, this implies:

$$\lambda_\gamma\lambda_\delta = \sum_{\varepsilon\in\operatorname{Conj}(G)} n_{\gamma,\delta,\varepsilon}\lambda_\varepsilon.$$

Let Λ be the column vector of the λ_δ for $\delta \in \mathrm{Conj}(G)$. Let A be the matrix with entries $(n_{\gamma,\delta,\varepsilon})$ for $\delta, \varepsilon \in \mathrm{Conj}(G)$. Then varying δ, the equations above rewrite:

$$A \cdot \Lambda = \lambda_\gamma \Lambda.$$

So λ_γ is an eigenvalue of the *integral* matrix A, and therefore a solution of its characteristic polynomial. But the latter is in $\mathbb{Z}[X]$ and has leading coefficient 1. Hence λ_γ is an algebraic integer. $\diamond$

Step 2. A formula for $\frac{|G|}{\dim V}$.

Verification. Since V is irreducible, $(\chi|\chi) = 1$. Therefore:

$$\begin{aligned} |G| &= \sum_{g \in G} \chi(g^{-1})\chi(g) \\ &= \sum_{\gamma \in \mathrm{Conj}(G)} \#\gamma \cdot \chi(\gamma^{-1})\chi(\gamma) \\ &= \sum_{\gamma \in \mathrm{Conj}(G)} \chi(\gamma^{-1})\lambda_\gamma \dim V, \end{aligned}$$

and $\frac{|G|}{\dim V} = \sum_{\gamma \in \mathrm{Conj}(G)} \chi(\gamma^{-1})\lambda_\gamma$. $\diamond$

For each γ, we know that $\chi(\gamma^{-1})$ is an algebraic integer (Proposition 7.2.9). Likewise, λ_γ is an algebraic integer by Step 1. Since $\mathbb{O}$ is a ring, we find $|G|/\dim V \in \mathbb{O}$. But obviously $|G|/\dim V \in \mathbb{Q}$. By Lemma 7.2.8, $|G|/\dim V$ is an integer. $\square$

7.3.2. Remark (if you already know the group algebra)**.** It is the case that every $g \in G$ is an algebraic integer of $\mathbb{Z}[G]$. But it is *not* the case that every sum of g's chosen at random is one. This fails because $\mathbb{Z}[G]$ is not a commutative ring. See exercise 7.4.5.

7.4 Exercises

7.4.1. Exercise. *Let G be a finite group. Prove the following equivalence:*

(i) G is simple;

(ii) for $\chi \in \mathrm{Irr}_{\mathbb{C}}(G)$, *one has* $\ker \chi = G$ *or* $\ker \chi = \{1\}$;

(iii) for $\chi \in \mathrm{Irr}_{\mathbb{C}}(G) \setminus \{\mathrm{triv}\}$ *and* $g \in G \setminus \{1\}$, *one has* $\chi(g) \neq \chi(1)$.

7.4.2. Exercise. *Let G be a finite group.*

1. *Prove that G is simple iff:*

$$(\forall \chi \in \mathrm{Irr}_{\mathbb{C}}(G))(\forall g \in G)[(\chi(g) = \chi(1)) \to (\chi = \mathrm{triv} \vee g = 1)].$$

(*) 2. *Devise a solubility test from the character table.*

7.4.3. Exercise. *Let G be a finite group and* $G \to \mathrm{GL}(V)$ *be a finite-dimensional, linear, complex representation with character* χ.

1. *Prove that* $\ker|\chi| = \{g \in G : |\chi(g)| = \dim V\}$ *is a normal subgroup.*

(*) 2. *Prove that* $\bigcap_{\chi \in \mathrm{Irr}_{\mathbb{C}}(G)} \ker|\chi| = Z(G)$.

7.4.4. Exercise. *Let G be a finite simple group. Prove that no irreducible complex representation has dimension 2. Hint: use Theorem 7.3.1 to prove that G has an involution.*

7.4.5. Exercise. *One needs to know or admit existence of the group ring* $\mathbb{Z}[G]$ *(see § 13). Let* $G = \mathrm{Sym}(3)$ *and* $x = (12) + (23) \in \mathbb{Z}[G]$. *Prove that x is not an algebraic integer of* $\mathbb{Z}[G]$.

8 Burnside's $p^a q^b$ theorem

Abstract. An application of character theory: Burnside's $p^a q^b$ theorem (§ 8.1). The proof uses a little algebraic number theory (§ 8.2) and is given in § 8.3.

8.1 Statement

8.1.1. Theorem. *Let G be a finite group of order* $p^a q^b$ *where* p, q *are prime numbers. Then G is soluble.*

One must recall the definition of a *soluble* group. Actually the proof also relies on *nilpotent* groups, and finite Sylow theory. The following facts will be required:

- every finite group has a p-subgroup of maximal order;
- every finite p-group is nilpotent.

Hence groups of order p^a are nilpotent, and groups of order $p^a q^b$ are soluble. There is nothing to say about groups of order $p^a q^b r^c$; for instance $\mathrm{Alt}(5)$ has order $60 = 2^2 \cdot 3 \cdot 5$ but is simple.

8.1.2. Remark. We shall give a *character-theoretic* proof of the theorem. However, there exist *character-free* proofs; a full one which is not completely elementary, and two partial elementary proofs in the odd and even cases.[7]

8.2 A number-theoretic lemma

8.2.1. Lemma. *Let G be a finite group; work over* $\mathbb{C}$. *Let* $(V, \rho, \chi) \in \mathrm{Irr}_{\mathbb{C}}(G)$ *and* $g \in G$.

(i) The complex number:

$$[G : C_G(g)] \frac{\chi(g)}{\chi(1)}$$

is an algebraic integer.

[7] They are respectively:
H. Bender, *A group theoretic proof of Burnside's* $p^a q^b$*-theorem*. Math. Zeitschrift 126, pp. 327–338, 1972.
D. Goldschmidt, *A group theoretic proof of the* $p^a q^b$ *theorem for odd primes*. Math. Zeitschrift 113, pp. 373–375, 1970.
H. Matsuyama, *Solvability of groups of order* $2^a p^b$. Osaka Math. J. 10, pp. 375–378, 1973.

(ii) If $[G : C_G(g)]$ and $\chi(1)$ are coprime, then $\chi(g) = 0$ or $\rho(g) \in \mathbb{C}\,\mathrm{Id}_V$.

Proof.

(i) Throughout we work in $\mathrm{End}_{\mathbb{C}}(V)$. For γ a G-conjugacy class let:

$$f_\gamma = \sum_{g\in\gamma} g.$$

Clearly $f_\gamma \in \mathrm{End}_{\mathbb{C}[G]}(V)$. By Schur's Lemma, there is $\lambda_\gamma \in \mathbb{K}$ such that $f_\gamma = \lambda_\gamma \mathrm{Id}_V$. Therefore:

$$\lambda_\gamma \chi(1) = \mathrm{tr}\, f_\gamma = \sum_{g\in\gamma} \chi(g) = \#\gamma \cdot \chi(\gamma).$$

For $g \in \gamma$, one has $\#\gamma = [G : C_G(g)]$. Hence:

$$[G : C_G(g)]\frac{\chi(g)}{\chi(1)} = \lambda_\gamma,$$

and it remains to prove that λ_γ is an algebraic integer.

We argue exactly like in the proof of Theorem 7.3.1, Step 1: there are *integers* $n_{\gamma,\delta,\varepsilon}$ such that:

$$f_\gamma f_\delta = \sum_{\varepsilon\in\mathrm{Conj}(G)} n_{\gamma,\delta,\varepsilon} f_\varepsilon.$$

This means $\lambda_\gamma\lambda_\delta = \sum_{\varepsilon\in\mathrm{Conj}(G)} n_{\gamma,\delta,\varepsilon}\lambda_\varepsilon$. Now let $A = (n_{\gamma,\delta,\varepsilon})_{\delta,\varepsilon}$, a square matrix with integer entries, and let $\Lambda = (\lambda_\delta)_\delta$, a column vector with complex entries. Clearly $\Lambda \neq 0$. The above rewrites:

$$\lambda_\gamma \Lambda = A\Lambda.$$

Hence λ_γ is an eigenvalue of A, and λ_γ is an algebraic number by the Cayley-Hamilton theorem.

(ii) By Bézout's theorem, there are $a, b \in \mathbb{Z}$ such that:

$$a[G : C_G(g)] + b\chi(1) = 1,$$

which immediately yields $a[G : C_G(g)]\frac{\chi(g)}{\chi(1)} + b\chi(g) = \frac{\chi(g)}{\chi(1)}$. The terms of the left-hand member are algebraic integers, and therefore so is $\frac{\chi(g)}{\chi(1)}$. Now $\chi(g)$ is a sum of $\chi(1)$-many roots of unity. We finish with an algebraic lemma.

8.2.2. Lemma. *Let $x_1, \dots, x_n$ be complex roots of unity and $m = \frac{x_1+\cdots+x_n}{n}$. If $m \in \mathbb{O}$, then $m = 0$ or $x_1 = \cdots = x_n = m$.*

Sketch of proof. The proof uses a little Galois theory. Say all x_i are k^{th} roots of unity; let $\zeta = e^{\frac{2i\pi}{k}}$. Now let $\mathbb{F} = \mathbb{Q}[\zeta]$ and $\Sigma = \mathrm{Gal}(\mathbb{F} : \mathbb{Q})$. By the fundamental theorem of Galois theory, $C_{\mathbb{F}}(\Sigma) = \mathbb{Q}$.

Let $q = \prod_{\sigma\in\Sigma} \sigma(m)$. Clearly Σ maps $\mathbb{O}$ to $\mathbb{O}$; so $q \in \mathbb{O}$. But $q \in C_{\mathbb{F}}(\Sigma)$, so $q \in \mathbb{O} \cap \mathbb{Q} = \mathbb{Z}$. Now Σ maps roots of unity to roots of unity. In particular for every $\sigma \in \Sigma$, one has $|\sigma(m)| \leq 1$. Thus $|q| \leq 1$, and two cases remain.

- If $|q| = 0$ then $q = 0$, so one $\sigma(m)$ is zero. So is m.
- If $|q| = 1$, then $|m| = 1$ as well. A clear convexity argument gives that all x_i are equal (and equal to m). $\square$

Let $\lambda_1, \dots, \lambda_{\chi(1)}$ be the eigenvalues of $\rho(g)$. By the Lemma, either their sum is 0, meaning $\chi(g) = 0$, or they are all equal, in which case $\rho(g) = \lambda \operatorname{Id}_V$. $\square$

8.3 The main lemma, and proof of Burnside's theorem

8.3.1. Lemma. *Let G be a finite group. Suppose there is a conjugacy class $\gamma \in \operatorname{Conj}(G)$ with $\#\gamma$ a prime power. Then G is not simple.*

Proof. Let $g \in G$ be such that $\gamma = g^G$ has cardinality p^k for some prime p and $k > 0$. Suppose G is simple. Then every non-trivial representation is injective.

Since $g \notin 1^G = \{1\}$, by column orthogonality (Lemma 5.5.1) we have:

$$\sum_{\chi \in \operatorname{Irr}_{\mathbb{C}}(G)} \chi(1)\chi(g) = \sum_{\chi \in \operatorname{Irr}_{\mathbb{C}}(G)} \chi(1^{-1})\chi(g) = 0.$$

Separating triv from the sum and dividing,

$$\sum_{\chi \in \operatorname{Irr}_{\mathbb{C}}(G) \setminus \{\mathrm{triv}\}} \frac{\chi(1)\chi(g)}{p} = -\frac{1}{p}.$$

Now $\frac{1}{p}$ is a proper rational, so it is not an algebraic integer. Since a sum of algebraic integers is again an algebraic integer, there is $\chi \in \operatorname{Irr}_{\mathbb{C}}(G) \setminus \{\mathrm{triv}\}$ such that $\frac{\chi(1)\chi(g)}{p}$ is not an algebraic integer; this certainly implies $\chi(g) \neq 0$.

Now $\chi(g)$ is an algebraic integer, so p does not divide $\chi(1)$. In particular $\chi(1)$ and $\#g^G = [G : C_G(g)] = p^k$ are coprime. Moreover, $\chi(g) \neq 0$. By Lemma 8.2.1 (ii), there is λ with $\rho(g) = \lambda \operatorname{Id}_V$. This implies $\rho(g) \in Z(\rho(G))$. But ρ is injective, so $g \in Z(G)$: a contradiction. $\square$

Proof of Burnside's $p^a q^b$ theorem. Let G be a counterexample of minimal order. If $a = 0$ or $b = 0$, then G has order a prime power, so it is nilpotent: hence not a counterexample, a contradiction. Hence both a and b are non-zero.

If G is not simple, then there is $\{1\} < N \lhd G$. Notice that N and G/N still have order of the form $p^{a'} q^{b'}$. By minimality, both N and G/N are soluble; hence so is G, a contradiction. So G is simple. If $Z(G) \neq \{1\}$ then by simplicity $Z(G) = G$ and G is abelian: a contradiction.

Let $P < G$ be a Sylow p-subgroup; since $a > 0$, one has $P \neq \{1\}$. Since P is a non-trivial, finite p-group, it has a non-trivial centre; let $g \in Z(P) \setminus \{1\}$. Then $P \leq C_G(g)$, so $|g^G|$ divides q^b. On the other hand $g \notin Z(G) = \{1\}$. So $g^G \neq \{g\}$ is a conjugacy class of cardinality a prime power. By Lemma 8.3.1, G is not simple, a contradiction. $\square$

9 Induced representations and Frobenius reciprocity

Abstract. *Induced representations* (§ 9.1) construct representations of supgroups. The *Frobenius formula* (§ 9.2) is an explicit formula for induced characters. Its consequence, *Frobenius reciprocity* (§ 9.3), plays an important role in applied character theory.

Suppose $H \leq G$ are groups. *In this section and the next, c, d will stand for (left-)cosets of G modulo H.*

9.0.1. Notation. If (V, ρ) is a representation of G, then the restriction $\rho_{|H}\colon H \to \mathrm{GL}(V)$ define a representation of H, denoted by $\mathrm{Res}_H^G(\rho)$.

(In general, irreducibility is not preserved.)

The whole section discusses one basic, converse, question. Suppose (W, σ) is a representation of H. Does it come from some representation of G? We start with a basic lemma on 'coset geometry'.

9.0.2. Lemma. *Let $H \leq G$ be groups and $c = aH$ be a (left-)coset of H. Let $g^c = \{g^b : b \in c\}$. Then $(gc = c)$ iff $(g^a \in H)$ iff $(g^c \subseteq H)$.*

Proof.

- If $gc = c$, then $gaH = aH$ and $ga \in aH$, so there is $h \in H$ with $ga = ah$, viz. $g^a = a^{-1}ga = h \in H$.
- If $g^a \in H$ and $b \in c$, then there is $h \in H$ with $b = ah$. Hence $g^b = g^{ah} \in H^h = H$.
- If $g^c \subseteq H$, then for $b \in c$ there is $h \in H$ with $b^{-1}gb = g^b = h$, so $gb = bh$ and $gc = gbH = bhH = bH = c$. □

9.1 Induced representations

Let $H \leq G$ be groups and $\sigma\colon H \to \mathrm{GL}(W)$ be a representation of H. In general there is no $\rho\colon G \to \mathrm{GL}(W)$ extending σ (exercise 9.4.4). But if we allow for a larger vector space, an extension can be found. The present subsection describes this construction.

9.1.1. Definition. Let $H \leq G$ be groups and $\mathbb{K}$ be a field. Let (W, σ) be a $\mathbb{K}$-linear representation of H. Construct a $\mathbb{K}$-linear representation of G as follows.

- Let $\{a_c : c \in G/H\}$ be a *transversal* of H in G, viz. a set of representatives of the left-cosets, so that $G = \bigsqcup_{c \in G/H} a_c H$. *We request $a_H = 1$.*
- Let $V = \bigoplus_{c \in G/H} a_c W$ be a vector space obtained as a direct sum of $[G : H]$ copies of W.
- For $g \in G$ and $v = a_c w \in V$, first write $ga_c = a_d h$, then let:

$$g \cdot v = a_d(h \cdot w).$$

  Extend linearly this action.

The resulting object is called *the induced representation of G*, denoted by $\mathrm{Ind}_H^G W$.

(It is perfectly fine to leave $\mathbb{K}$ implicit in notation.)

9.1.2. Proposition.

(i) *This is well-defined and does define a representation of G in V.*

(ii) $a_H W \leq V$ *is H-invariant and* $W \simeq a_H W \quad [\mathbb{K}[H]\text{-}\mathbf{Mod}]$.

(iii) *The ($\mathbb{K}[G]$-isomorphism type of the) construction does not depend on the transversal chosen, provided $a_H = 1$.*

(iv) *If V' is another representation of G and $f\colon W \to \mathrm{Res}_H^G V'$ is H-covariant, then there is a unique $\hat{f}\colon \mathrm{Ind}_H^G \to V'$ which is G-covariant and extends f.*

Proof.

(i) By definition of a transversal, if $g \in G$ and $c \in G/H$, there is a unique pair (a_d, h) such that $ga_c = a_d h$. So the construction is well-defined. Clearly each g acts linearly. We now check that we have defined a morphism $G \to \mathrm{GL}(V)$. Clearly 1 acts as the identity (this does not require $a_H = 1$ yet). Now let $g, g' \in G$ and $v \in V$. We must check $g(g'v) = (gg'v)$. By linearity, we may suppose $v = a_c w$ for some a_c and $w \in W$.

By construction, $g'a_c = a_d h'$ and $ga_d = a_e h$ for cosets d, e. Altogether, this gives:
$$g'v = a_d(h'w),$$
and then:
$$g(g'v) = a_e(hh'w).$$
On the other hand, $(gg')a_c = g(g'a_c) = g(a_d h') = (ga_d)h' = a_e hh'$, so we also have:
$$(gg')v) = a_e(hh'w).$$
This proves mulitplicativity of the action. We have constructed a representation.

(ii) Let $h \in H$ and $v = a_H W$. Then $ha_H \in H$, so $ha_H = a_H h'$ for some h'. Then $h \cdot v = a_H(h'w) \in a_H W$, which is therefore H-invariant (this does not require $a_H = 1$ yet).

We now construct an isomorphism of H-representations $W \simeq a_H W$, using $a_H = 1$. Map w to $\varphi(w) = a_H w$. Then for $h \in H$ one has $ha_H = a_H h$, so:
$$h \cdot \varphi(w) = h \cdot (a_H w) = a_H(hw) = \varphi(hw),$$
as wanted. (Actually this only requires $a_H \in Z(H)$.)

(iii) Suppose $\{b_c : c \in G/H\}$ is another transversal, also with $b_H = 1$. So our construction now comes in two flavours: V_a and V_b. We must give an isomorphism of representations of G. For $c \in G/H$, one has $a_c H = b_c H$, so $\eta_c = b_c^{-1} a_c \in H$.

To $v = a_c w$ associate $\varphi(v) = b_c(\eta_c w)$, and extend linearly. It clearly defines a linear isomorphism $V_a \simeq V_b$. We contend it is a G-isomorphism. So let $g \in G$; by linearity, it is enough to prove $g \cdot \varphi(v) = \varphi(g \cdot v)$ for v of the form $a_c w$.

Write $ga_c = a_{d_1}h_1$ and $gb_c = b_{d_2}h_2$ in obvious notation. Then:

$$g \cdot \varphi(v) = g \cdot (b_c(\eta_c w)) = b_{d_2}(h_2\eta_c w),$$

while:

$$\varphi(g \cdot v) = \varphi(a_{d_1}(h_1 w)) = b_{d_1}(\eta_{d_1}h_1 w).$$

We must check equality. Indeed,

$$b_{d_2}h_2\eta_c = gb_c\eta_c = ga_c = a_{d_1}h_1 = b_{d_1}\eta_{d_1}h_1,$$

so by definition of a transversal, $d_2 = d_1$, and $h_2\eta_c = \eta_{d_1}h_1$. So we are done.

(iv) Suppose $\hat{f}\colon \operatorname{Ind}_H^G \to V'$ is G-covariant. Then for $c \in G/H$ and $w \in W$, one has:

$$\hat{f}(a_c \cdot w) = \hat{f}(a_c(a_H w)) = \hat{f}(a_c w) = a_c\hat{f}(w) = a_c f(w),$$

so $\hat{f}(a_c w) = a_c f(w)$. This guarantees uniqueness.

Conversely we let $\hat{f}(a_c w) = a_c f(w)$ and extend linearly. This does define a linear map $\hat{f}\colon \operatorname{Ind}_H^G W \to V'$. We prove G-covariance on basic terms $a_c w$. Indeed, with $ga_c = a_d h$ in obvious notation:

$$\begin{aligned}\hat{f}(g \cdot (a_c w)) &= \hat{f}(a_d hw) = a_d\hat{f}(hw) = a_d f(hw)\\ &= a_d hf(w) = ga_c f(w) = g\hat{f}(a_c w),\end{aligned}$$

proving G-covariance. □

9.1.3. Remarks.

- As a consequence of Proposition 9.1.2 (iii), we may write $\operatorname{Ind}_H^G W = \bigoplus_{c\in G/H} cW$ with no mention of the transversal.
- (iv) is a universal property, conveniently described in terms of *adjoint functors*.
- There is a tensor description of $\operatorname{Ind}_H^G W$, but this course avoids tensoring over general rings.
- Recall that Res_H^G does not change the underlying vector space, but Ind_H^G does ('by a factor $[G : H]$').

9.2 Induced class functions and Frobenius formula

If $\beta \in \mathcal{C}_{\mathbb{K}}(G)$ is a class function on G and $H \le G$ is a subgroup, we denote by $\operatorname{Res}_H^G \beta$ the restriction $\beta_{|H}$. Clearly $\beta_{|H} \in \mathcal{C}_{\mathbb{K}}(H)$; the operator $\operatorname{Res}_H^G\colon \mathcal{C}_{\mathbb{K}}(G) \to \mathcal{C}_{\mathbb{K}}(H)$ is clearly linear. We now define a 'converse' linear operator $\operatorname{Ind}_H^G\colon \mathcal{C}_{\mathbb{K}}(H) \to \mathcal{C}_{\mathbb{K}}(G)$. It is converse in a loose sense since *in general,* $\operatorname{Res}\operatorname{Ind}_\alpha \neq \alpha$. ('Adjoint' would be more adapted.)

9.2.1. Lemma. *Let $H \le G$ be a pair of finite groups and $\mathbb{K}$ be a field.*

(i) For $\alpha \in \mathcal{C}_{\mathbb{K}}(H)$ a class function on H, the following definition makes sense:

$$\operatorname{Ind}_H^G \alpha = \sum_{\substack{c\in G/H:\\ gc=c}} \alpha(g^c).$$

(ii) *If W is a finite-dimensional, $\mathbb{K}$-linear representation of H with character χ_W, then:*

$$\operatorname{Ind}_H^G \chi_W = \chi_{\operatorname{Ind}_H^G W}.$$

'The character of the induced (representation) is the induced (function) of the character.'

Proof.

(i) Suppose $a_c, b_c \in c$; say $a_c = b_c \eta_c$ with $\eta_c \in H$. Then by Lemma 9.0.2:

$$gc = c \quad \text{iff} \quad g^{a_c} \in H \quad \text{iff} \quad g^{b_c} \in H.$$

So if $gc = c$, then $\alpha(g^{a_c})$ and $\alpha(g^{b_c})$ both make sense. Moreover, $g^{b_c \eta_c} = g^{a_c}$ so g^{a_c} and g^{b_c} are H-conjugate.

Therefore always assuming $gc = c$, and since α is a class function on H, we have:

$$\alpha(g^{b_c}) = \alpha(g^{a_c}).$$

Hence $\alpha(g^c)$ is well-defined regardless of the choice of the transversal: the formula makes sense.

(ii) Let $V = \operatorname{Ind}_H^G W$, with character χ_V. We prove $\chi_V = \operatorname{Ind}_H^G \chi_W$.

Let $g \in G$. Recall that $V = \bigoplus_{c \in G/H} a_c W$. Moreover, g maps the space $a_c W$ to the space $a_d W$ for $g a_c = a_d h$. But when computing $\operatorname{tr} g$, only g-invariant subspaces from the direct sum contribute, and:

$$\operatorname{tr} g = \sum_{\substack{c \in G/H: \\ g(a_c W) \le a_c W}} \operatorname{tr}(g_{|a_c W}).$$

Notice that $g a_c W \le a_c W$ iff there is $h \in H$ with $g a_c = a_c h$ iff $g^{a_c} \in H$ iff $gc = c$. So:

- cosets d with $gd \neq d$ do not contribute;
- cosets c with $gc = c$ contribute $\operatorname{tr}(g_{|a_c W})$.

In the latter case, g acts on $a_c W$ like $h = g^{a_c}$. Therefore $\operatorname{tr}(g_{|a_c W}) = \chi_W(g^{a_c}) = \chi_W(g^c)$.

Hence:

$$\chi_V(g) = \operatorname{tr}(g) = \sum_{\substack{c \in G/H: \\ gc = c}} \chi_W(g^c) = \operatorname{Ind}_H^G \chi_W. \qquad \square$$

9.3 Frobenius reciprocity

Since we deal with two groups, it is convenient to denote $(\cdot|\cdot)_K$ the usual bilinear form with respect to $K \in \{H, G\}$.

9.3.1. Theorem (Frobenius reciprocity)**.** *Let $H \le G$ be finite groups and $\mathbb{K}$ be a G-good field (hence H-good as well).*

(i) Let W be a $\mathbb{K}$-linear, finite-dimensional representation of H and V be one of G. Then:

$$(\chi_{\operatorname{Ind} W}|\chi_V)_G = (\chi_W|\chi_{\operatorname{Res} V})_H.$$

(ii) For $\alpha \in \mathcal{C}_{\mathbb{K}}(G)$ a class function on H and $\beta \in \mathcal{C}_{\mathbb{K}}(G)$ one on G, one still has:

$$\left(\operatorname{Ind}_H^G \alpha|\beta\right)_G = \left(\alpha|\operatorname{Res}_H^G \beta\right)_H.$$

Proof.

(i) By Proposition 9.1.2 (iv), there is an isomorphism of underlying vector spaces:

$$\operatorname{Hom}_{\mathbb{K}[H]}(W, \operatorname{Res} V) \simeq \operatorname{Hom}_{\mathbb{K}[G]}(\operatorname{Ind} W, V) \quad [\mathbb{K}\text{-}\mathbf{Mod}].$$

In particular, $\mathbb{K}$-linear dimensions match. Now dimensions of spaces of covariant morphisms were computed in Lemma 5.2.2 (ii) using the bilinear form, and this gives:

$$(\chi_W|\chi_{\operatorname{Res} V})_H = (\chi_{\operatorname{Ind} W}|\chi_V)_G.$$

(ii) Notice that $\operatorname{Res}_H^G: \mathcal{C}_{\mathbb{K}}(G) \to \mathcal{C}_{\mathbb{K}}(H)$ and $\operatorname{Ind}_H^G: \mathcal{C}_{\mathbb{K}}(H) \to \mathcal{C}_{\mathbb{K}}(G)$ are linear maps. For $\mathbb{K}$-valued characters, (i) holds. Since characters of a finite group generate the space of class functions, the formula holds of all class functions. □

9.4 Exercises

9.4.1. Exercise.

1. *Show that* $\operatorname{Ind}_{\{1\}}^G \operatorname{triv} \simeq \operatorname{reg}_G$.
2. *For finite G, deduce from Frobenius reciprocity that* $\operatorname{reg} = \sum_{\chi \in \operatorname{Irr}_{\mathbb{C}}(G)} \dim \chi \cdot \chi$.

9.4.2. Exercise. *Let G be a finite group and $K \leq H \leq G$ be two subgroups. Let W be a representation of K. Prove that* $\operatorname{Ind}_K^G W \simeq \operatorname{Ind}_H^G(\operatorname{Ind}_K^H W) \quad [\mathbb{C}[G]\text{-}\mathbf{Mod}]$.

9.4.3. Exercise. *Let $H \leq G$ be finite groups and $\mathbb{K}$ be a field. Let W be a representation of H and $V = \operatorname{Ind}_H^G W$. Let $\hat{\psi}_W$ coincide with ψ_W on H and equal 0 on $G \setminus H$. Prove that:*

$$\chi_V(g) = \frac{1}{|H|} \sum_{x \in G} \hat{\psi}_W(g^x).$$

(*) **9.4.4. Exercise.** *Let* $\operatorname{perm}: \operatorname{Sym}(4) \to \operatorname{GL}_4(\mathbb{K})$ *be the permutation representation. Now view* $\operatorname{Sym}(4)$ *as a subgroup of* $\operatorname{Sym}(5)$. *Show that* perm *does not extend to* $\operatorname{Sym}(5) \to \operatorname{GL}_4(\mathbb{K})$.

10 Frobenius complement theorem

Abstract. Frobenius' famous *complement theorem* deals with certain finite group-theoretic configurations. There is no known full proof avoiding character theory.

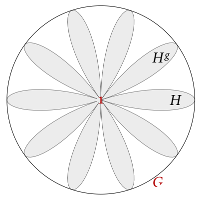
10.1 Frobenius pairs

10.1.1. Definition. A *Frobenius pair* is a pair of groups $(H < G)$ such that:

- H is self-normalising in G, viz. $N_G(H) = H$;
- H has trivial intersections with distinct conjugates, viz. G satisfies:

$$(\forall g)[(H^g = H) \vee (H \cap H^g = \{1\})].$$

A subgroup with trivial intersections looks like this:



(It is harder to draw self-normalisation phenomena.) The conjunction is sometimes called *malnormality* of H in G but we cannot recommend the terminology.

10.1.2. Examples.

- Let $\mathbb{K}$ be a field, $A = (\mathbb{K}; +)$ be its additive group and $M = (\mathbb{K}^\times, \cdot)$ be its multiplicative group. Then:

$$A \rtimes M \simeq \left\{ \begin{pmatrix} m & a \\ 0 & 1 \end{pmatrix} : (a, m) \in A \times M \right\},$$

  with M embedding to $\operatorname{diag}(1, m)$. Then $(M < A \rtimes M)$ is a Frobenius pair.

- While affine configurations are inspirational, they are not typical of Frobenius pairs. For example, there is a Frobenius pair with $H \simeq \mathrm{SL}_2(\mathbb{F}_5)$.

Infinite Frobenius pairs are a desperate topic.[8]

10.1.3. Remarks.

- In the literature, G is sometimes called a *Frobenius group* and H its *Frobenius complement*.

  It can be proved (but it requires tools not available in this class) that if $(H_1 < G)$ and $(H_2 < G)$ are finite Frobenius pairs with the same G, then there is $g \in G$ with $H_2^h = H_1$. So up to isomorphism there is *at most* one way in which a finite group can be the large group of a Frobenius pair, and the phrase 'finite Frobenius group' makes sense.

  This is completely not true with infinite groups.

- The above however supports the following question (Y. Tamer): is there a first-order formula characterising Frobenius groups *among finite groups*?

[8] P. de la Harpe, C. Weber, *Malnormal subgroups and Frobenius groups: basics and examples.* Confluentes Math. 6 (1), pp. 65–76, 2014.

10.2 The geometry of a Frobenius pair

10.2.1. Notation. For $(H < G)$ a Frobenius pair, we let:

$$N = \left(G \setminus \bigcup_{x \in G} H^x\right) \cup \{1\}.$$

Despite suggestive notation, this is just a *subset*. It is normal (viz. closed under G-conjugation) and closed under $^{-1}$. In general, no more can be said; for infinite groups, one could even have $N = \{1\}$.

10.2.2. Lemma. *Let $(H < G)$ be a Frobenius pair and $g \in G$ with $g \neq 1$. Then exactly one of the following two occurs:*

- *$g \in \bigcup_{x \in G} H^x$, there is a unique $c \in G/H$ such that $gc = c$, and $g^G \cap H$ is a single H-conjugacy class;*
- *$g \in N$, there is no $c \in G/H$ such that $gc = c$, and $g^G \cap H = \varnothing$.*

Proof. If $g \in H^x$, then $gx^{-1}H = x^{-1}g^{x^{-1}}H = x^{-1}H$. If also $gaH = aH$, then $ga \in aH$ and $g^a \in H$. So $1 \neq g \in H^x \cap H^{a^{-1}}$, which forces $xa \in N_G(H) = H$. Hence $x^{-1}H = aH$ and the coset solution is unique. Suppose $h_1, h_2 \in g^G \cap H$; they are not 1. There are $x_1, x_2 \in G$ with $h_i = g^{x_i}$. In particular,

$$h_1 = g^{x_1} = h_2^{x_2^{-1}x_1} \in H \cap H^{x_2^{-1}x_1} \setminus \{1\}.$$

So $x_2^{-1}x_1 \in N_G(H) = H$, meaning that h_1 and h_2 are H-conjugate.

If $g \in N$, then $g^G \cap H = \varnothing$. If however $gc = c$ for some coset $c = aH$, then $g \in H^{a^{-1}}$, a contradiction. So the equation $gc = c$ has no solution in G/H. $\square$

10.3 Frobenius' complement theorem

The following remarkable result is due to Frobenius. We repeat that *no fully character-free proof is known.*

10.3.1. Theorem. *Let $(H < G)$ be a finite Frobenius pair. Then there is a normal subgroup $N \trianglelefteq G$ such that $G = N \rtimes H$.*

Proof. There is no conflict with our notation since the only candidate is:

$$N = \left(G \setminus \bigcup_{g \in G} H^g\right) \cup \{1\}.$$

But there is no clear group-theoretic reason why N should be closed under product, and the proof requires a serious detour through character theory. We begin with a simple computation.

Step 1. $\#N = \frac{|G|}{|H|}$.

Verification. Subsets of the form $(H \setminus \{1\})^x = H^x \setminus \{1\}$:

- have $|H| - 1$ elements,
- are disjoint or equal,
- form a family parametrised by $G/N_G(H) = G/H$, with $\frac{|G|}{|H|}$ members.

So:

$$G \smallsetminus N = \bigcup_{x \in G} H^x \smallsetminus \{1\} = \bigcup_{x \in G} (H \smallsetminus \{1\})^x$$

has exactly $\frac{|G|}{|H|}(|H| - 1) = |G| - \frac{|G|}{|H|}$ elements. Hence N has exactly $\frac{|G|}{|H|}$ elements. ◇

The key step will be to use Frobenius' reciprocity formula and prove that *for a Frobenius pair, every irreducible character of H extends to an irreducible character of G.* (This is quite false in general; see exercise 9.4.4.)

The naive guess when trying to extend $\psi \in \mathrm{Irr}_{\mathbb{C}}(H)$ to $\hat{\psi} \in \mathrm{Irr}_{\mathbb{C}}(G)$ would be $\mathrm{Ind}_H^G \psi$. However, recall that 'Ind expands the dimension by a factor $[G : H]$', so $\mathrm{Res}_H^G \mathrm{Ind}_H^G \psi \neq \psi$. Indeed,

$$(\mathrm{Res}_H^G \mathrm{Ind}_H^G \psi)(1) = (\mathrm{Ind}_H^G \psi)(1) = [G : H]\psi(1) \neq \psi(1).$$

The obstacle would disappear 'if $\psi(1)$ were 0'. This suggests to consider the class function $\psi(h) - \psi(1)$, viz. $\psi - \psi(1)\mathrm{triv}_H$.

Step 2. Let $\alpha: H \to \mathbb{C}$ be a class function with $\alpha(1) = 0$. Then $\mathrm{Ind}_H^G \alpha$ is the unique class function on G which • extends α, and • vanishes on N.

Verification. Uniqueness is obvious since $G = N \cup \bigcup_{x \in G} H^x$.

By Lemma 10.2.2, if $g \in G$ is conjugate to *two* elements $h_1, h_2 \in H$, then h_1 and h_2 are already H-conjugate. In particular $\alpha(h_1) = \alpha(h_2)$ and we may define $\mathring{\alpha}(g) = \alpha(h_1)$. On N we let $\mathring{\alpha}(x) = 0$, which is consistent since $N \cap H = \{1\}$ and $\alpha(1) = 0$. So there is an extension of α to a G-class function vanishing on N.

We must prove that $\mathring{\alpha}$ so constructed actually equals:

$$(\mathrm{Ind}_H^G \alpha)(g) = \sum_{\substack{c \in G/H: \\ gc = c}} \alpha(g^c).$$

So let $g \in G$; we may assume $g \neq 1$. We use Lemma 10.2.2. If $g \in N$, the sum giving Ind is empty, so $(\mathrm{Ind}\, \alpha)(g) = 0 = \mathring{\alpha}(g)$. If on the other hand $g \in H^x$, then the sum contains *only* term, namely $\alpha(g^{x^{-1}}) = \mathring{\alpha}(g^{x^{-1}}) = \mathring{\alpha}(g)$. ◇

Step 3. Every irreducible complex character $\psi \in \mathrm{Irr}_{\mathbb{C}}(H)$ extends to some $\hat{\psi} \in \mathrm{Irr}_{\mathbb{C}}(G)$. Moreover we may suppose $N \subseteq \ker \hat{\psi}$.

Verification. The trivial character triv_H certainly extends to triv_G. So consider $\psi \in \mathrm{Irr}_{\mathbb{C}}(H) \smallsetminus \{\mathrm{triv}_H\}$; we seek to extend it to an irreducible character of G. It will be:

$$\hat{\psi} = \mathrm{Ind}_H^G[\psi - \psi(1)\mathrm{triv}_H] + \psi(1)\mathrm{triv}_G.$$

(Keep in mind at all times that although $\mathrm{Ind}_H^G: \mathcal{C}(H) \to \mathcal{C}(G)$ is linear, it does *not* take triv_H to triv_G. So $\hat{\psi}$ does *not* equal $\mathrm{Ind}_H^G \psi$.) Many details are required. Throughout, we write Ind for Ind_H^G and Res for Res_H^G.

First let $d = \psi(1) \in \mathbb{N}$. Now let $\alpha = \psi - d\mathrm{triv}_H$, an H-class function with $\alpha(1) = 0$. By Step 2, $\operatorname{Ind}\alpha$ is a G-class function extending α. Thus $\alpha = \operatorname{Res}\operatorname{Ind}\alpha$. As said, we let:

$$\hat{\psi} = \operatorname{Ind}\alpha + d\mathrm{triv}_G.$$

Then:

$$\operatorname{Res}\hat{\psi} = \operatorname{Res}\operatorname{Ind}\alpha + d\mathrm{triv}_H = \alpha + d\mathrm{triv}_H = \psi.$$

But it remains to prove that $\hat{\psi}$ is a character of G.

First use linearity of Ind, giving:

$$\hat{\psi} = \operatorname{Ind}(\psi - d\mathrm{triv}_H) + d\mathrm{triv}_G = \operatorname{Ind}\psi - d\operatorname{Ind}\mathrm{triv}_H + d\mathrm{triv}_G.$$

Now recall that $\operatorname{Ind}\psi$ and $\operatorname{Ind}\mathrm{triv}_H$ are indeed characters of G by Lemma 9.2.1. So $\hat{\psi}$ is a $\mathbb{Z}$-linear combination of characters of G, hence a $\mathbb{Z}$-linear combination of *irreducible* characters of G. We prove that there is only term by computing $(\hat{\psi}|\hat{\psi})$. This involves Frobenius reciprocity.

By reciprocity (extended to all class functions), bearing in mind $\operatorname{Res}\mathrm{triv}_G = \mathrm{triv}_H$ and $\operatorname{Res}\operatorname{Ind}\alpha = \alpha$, one finds:

$$\begin{aligned}
(\hat{\psi}|\hat{\psi})_G &= (\operatorname{Ind}\alpha + d\mathrm{triv}_G|\operatorname{Ind}\alpha + d\mathrm{triv}_G)_G \\
&= (\operatorname{Ind}\alpha|\operatorname{Ind}\alpha)_G + d\,(\mathrm{triv}_G|\operatorname{Ind}\alpha)_G + d\,(\operatorname{Ind}\alpha|\mathrm{triv}_G)_G + d^2\,(\mathrm{triv}_G|\mathrm{triv}_G)_G \\
&= (\alpha|\operatorname{Res}\operatorname{Ind}\alpha)_H + d\,(\operatorname{Res}\mathrm{triv}_G|\alpha)_H + d\,(\alpha|\operatorname{Res}\mathrm{triv}_H)_H + d^2 \\
&= (\alpha|\alpha)_H + d\,(\mathrm{triv}_H|\alpha)_H + d\,(\alpha|\mathrm{triv}_H)_H + d^2 \\
&= (\alpha + d\mathrm{triv}_H|\alpha + d\mathrm{triv}_H)_H \\
&= (\psi|\psi)_H \\
&= 1.
\end{aligned}$$

Recall that $\hat{\psi}$ is a $\mathbb{Z}$-linear combination of irreducible characters of G, say $\hat{\psi} = \sum n_i\hat{\psi}_i$ in obvious notation. Then by orthonormality, $(\hat{\psi}|\hat{\psi})_G = \sum n_i^2 = 1$. So $\hat{\psi}$ is itself either an irreducible character *or the opposite of one*. However $\hat{\psi}$ extends ψ, so $\hat{\psi}(1) = \psi(1) = d \in \mathbb{N}$ and $\hat{\psi} \in \operatorname{Irr}_{\mathbb{C}}(G)$.

Last, for $g \in N$, the equation $gc = c$ has no solutions by Lemma 10.2.2. So any sum of the form

$$(\operatorname{Ind}\beta)(g) = \sum_{\substack{c \in G/H: \\ gc = c}} \beta(g^c)$$

is actually empty. So there remains only $\hat{\psi}(g) = \psi(1)\mathrm{triv}_G(g) = \psi(1) = \hat{\psi}(1)$, meaning $N \subseteq \ker\hat{\psi}$. ◇

Step 4. N is a normal subgroup of G.

Verification. For $\psi \in \operatorname{Irr}_{\mathbb{C}}(H)$, let $\hat{\psi} \in \operatorname{Irr}_{\mathbb{C}}(G)$ as in Step 3. Recall that $N \subseteq \ker\hat{\psi}$. Now let:

$$K = \bigcap_{\psi \in \operatorname{Irr}_{\mathbb{C}}(H)} \ker\hat{\psi},$$

a normal subgroup of G. We shall prove that $K = N$. The inclusion $N \subseteq K$ is by Step 3.

We now show $K \subseteq N$. This relies on proving $K \cap H = \{1\}$. Indeed let $h \in K \cap H$. Then for $\psi \in \mathrm{Irr}_{\mathbb{C}}(H)$, one has $\psi(h) = \hat{\psi}(h) = \hat{\psi}(1) = \psi(1)$. Hence $h \in \bigcap_{\mathrm{Irr}_{\mathbb{C}}(H)} \ker \psi = \{1\}$ by Theorem 7.1.4 (i). Since K is a normal subgroup, it avoids *all* conjugates of H, viz. $K \subseteq N$. ◇

Hence $N = K$ is a normal subgroup disjoint from H. Now $|N| = \#N = \frac{|G|}{|H|}$ by Step 1, which implies $G = N \rtimes H$. □

10.3.2. Remarks.

- Thompson proved that N must be nilpotent.[9]
- If H has even order, N is even abelian. This is not true in general: see exercise 10.4.2.
- But H can be non-soluble: there is a finite Frobenius group with $H \simeq \mathrm{SL}_2(\mathbb{F}_5)$.

10.3.3. Remark. Frobenius groups have a lovely application to Wedderburn's theorem (finite skew-fields are commutative) going through Desarguesian planes.[10] Good publicity for my other NMK lecture notes!

10.4 Exercises

10.4.1. Exercise. *Let G be a finite group acting transitively on a set X. Suppose that every $g \neq 1$ fixes at most one element of X. Prove that $N = \{$fixed-point free elements$\} \cup \{1\}$ is a normal subgroup.*

10.4.2. Exercise. *Consider the group:*

$$N = \left\{ \begin{pmatrix} 1 & x & z \\ & 1 & y \\ & & 1 \end{pmatrix} : (x, y, z) \in \mathbb{F}_7^3 \right\},$$

and the map:

$$\sigma\left(\begin{pmatrix} 1 & x & z \\ & 1 & y \\ & & 1 \end{pmatrix}\right) = \begin{pmatrix} 1 & 2x & 4z \\ & 1 & 2y \\ & & 1 \end{pmatrix}.$$

Prove that σ is an automorphism of order 3 of N. Now prove that $(\langle\sigma\rangle < N \rtimes \langle\sigma\rangle)$ is a Frobenius pair.

10.4.3. Exercise. *Let $(H < G)$ be a finite Frobenius pair, say $G = N \rtimes H$. Let $\pi\colon G \to G/N \simeq H$ be the quotient map. Let $\chi \in \mathrm{Irr}_{\mathbb{C}}(G)$ be non-trivial. Prove that:*

- *either $\chi = \psi \circ \pi$ for some $\psi \in \mathrm{Irr}_{\mathbb{C}}(G/N) = \mathrm{Irr}_{\mathbb{C}}(H)$,*
- *or $\chi = \mathrm{Ind}_N^G \varphi$ for some $\varphi \in \mathrm{Irr}_{\mathbb{C}}(N)$.*

(**) **10.4.4. Exercise** (Bender's 'even' proof)**.** *This exercise contains no representation theory; on the contrary, it gives a character-free proof of Theorem 10.3.1* under extra assumptions.

Let $(H < G)$ be a finite Frobenius pair. Suppose that H has even order.

[9] J. Thompson, *Finite groups with fixed-point-free automorphisms of prime order*. Proc. Nat. Acad. Sci. U. S. A. 45, pp. 578–581, 1959.

[10] S. Ebey, K. Sitaram, *Frobenius groups and Wedderburn's theorem*. Amer. Math. Monthly 76, pp. 526–528, 1969.

1. *Determine the cardinal of* $N = \left(G \smallsetminus \bigcup_{g\in G} H^g\right) \cup \{1\}$.
2. *Prove that if* i, j *are two involutions (of any group), then* $(ij)^i = (ij)^{-1}$.
3. *Let* $i \in H$ *be an involution. Prove that for* $g \in G \smallsetminus H$*, one has* $1 \neq ig^{-1}ig \in N$.
4. *Determine the cardinal of* $R^* = \{ig^{-1}ig : g \in G \smallsetminus H\} \subseteq N$.
5. *Prove that* $N = R^* \cup \{1\}$
6. *Conclude that* N *is a subgroup of* G.

Notes.

- *The method even proves abelianity of* N under our assumption that H has even order. *This is not true in general; however* N *is nilpotent (see Remarks 10.3.2).*
- *To date, there is no known full character-free proof of Theorem 10.3.1.*[11]

11 Real, purely complex, quaternionic representations

Abstract. § 11.1 gives a correspondence between bilinear forms on V and morphisms $V \simeq V^*$. § 11.2 discusses the irreducible case. Then § 11.3 introduces *real*, *purely complex*, and *quaternionic* representations.

This section discusses only complex representations. The irreducible ones will be classified into *real*, *complex*, and *quaternionic* representations, in a technical sense. To avoid clash in terminology, we make an effort to talk about '$\mathbb{C}$-linear representations', and to refer to the second case as 'purely complex'.

11.1 Bilinear forms and duality

For V a $\mathbb{K}$-vector space, we let $\mathrm{Bil}_{\mathbb{K}}(V \times V, \mathbb{K})$ be the space of $\mathbb{K}$-bilinear forms on V. By definition, one has $\mathrm{Bil}_{\mathbb{K}}(V \times V, \mathbb{K}) \simeq \mathrm{Hom}_{\mathbb{K}}(V \otimes_{\mathbb{K}} V, \mathbb{K})$.

11.1.1. Definition. A bilinear form on a representation V is *preserved by* G if:

$$(\forall g \in G)(\forall x \in V)(\forall y \in V)(\beta(gx, gy) = \beta(x, y)).$$

We shall simply say that β is a *bilinear* G*-form*.

We let $G\text{-}\mathrm{Bil}_{\mathbb{K}}(V \times V, \mathbb{K}) \leq \mathrm{Bil}_{\mathbb{K}}(V \times V, \mathbb{K})$ be the subspace of bilinear G-forms. When no confusion can arise, we simply write $G\text{-}\mathrm{Bil} \leq Bil$.

11.1.2. Remark. We avoid writing '$\mathrm{Bil}_{\mathbb{K}[G]}(V \times V, \mathbb{K})$', because bilinear G-forms are *not* $\mathbb{K}[G]$-bilinear. Likewise, 'G-bilinear' is slightly confusing.

11.1.3. Proposition. *Let* V *be a* finite-dimensional *vector space.*

(i) There is a natural isomorphism $\mathrm{Hom}_{\mathbb{K}}(V, V^*) \to \mathrm{Bil}_{\mathbb{K}}(V \times V, \mathbb{K})$ $[\mathbb{K}\text{-}\mathbf{Mod}]$.

[11] See however a very interesting entry on Terence Tao's webpage, https://terrytao.wordpress.com/2013/05/24/a-fourier-analytic-proof-of-frobeniuss-theorem/

(ii) The above induces a natural bijection:

$$\begin{aligned} & \{\textit{linear} \text{ isomorphisms } f\colon V \simeq V^* \ [\mathbb{K}\text{-}\mathbf{Mod}]\} \\ \leftrightarrow \quad & \{\text{non-degenerate } \textit{bilinear forms } \beta\colon V \times V \to \mathbb{K}\}. \end{aligned}$$

(iii) If V is also a representation of a group G, then (i) restricts to $\mathrm{Hom}_{\mathbb{K}[G]}(V, V^*) \to G\text{-}\mathrm{Bil}_{\mathbb{K}}(V \times V, \mathbb{K})$, *which like in (ii) induces a natural bijection:*

$$\begin{aligned} & \{\text{isomorphisms } \textit{of representations } f\colon V \simeq V^* \ [\mathbb{K}[G]\text{-}\mathbf{Mod}]\} \\ \leftrightarrow \quad & \{\text{non-degenerate } \textit{bilinear } G\textit{-forms } \beta\colon V \times V \to \mathbb{K}\}. \end{aligned}$$

11.1.4. Remark. In (iii), the isomorphism $\mathrm{Hom}_{\mathbb{K}[G]}(V, V^*) \simeq G\text{-}\mathrm{Bil}$ can be considered in $\mathbb{K}[G]$-**Mod** or in $\mathbb{K}$-**Mod** without loss of information, since the natural action of G on each side is trivial.

Proof.

(i) Truly, in abstract terms, this is because in $\mathbb{K}$-**Mod** one has isomorphisms:

$$\begin{aligned} \mathrm{Bil}_{\mathbb{K}}(V \times V, \mathbb{K}) &\simeq \mathrm{Hom}(V \otimes V, \mathbb{K}) \simeq (V \otimes V)^* \simeq V^* \otimes V^* \\ &\simeq \mathrm{Hom}(V^{**}, V^*) \simeq \mathrm{Hom}(V, V^*) \ [\mathbb{K}\text{-}\mathbf{Mod}]. \end{aligned}$$

One may prefer a casual approach. To $\mathbb{K}$-linear $f\colon V \to V^*$, associate the map $\beta_f(x, y) = f(x)(y) \in \mathbb{K}$. Clearly β_f is bilinear. Moreover $f \mapsto \beta_f$ is linear. Conversely, to bilinear $\beta\colon V \times V \to \mathbb{K}$, associate $f_\beta(x) = \beta(x, \cdot) \in V^*$. Then $f_\beta\colon V \to V^*$ is linear. Moreover $\beta \mapsto f_\beta$ is linear. These constructions are inverses of each other, hence linear isomorphisms.

(ii) Work in the notation above. Suppose $f\colon V \simeq V^*$ is a linear isomorphism. If $x \in V$ is such that $\beta_f(x, \cdot) = 0$, then $f(x) = 0$ and therefore $x = 0$. So β_f is *left*-non-degenerate; by finite-dimensionality, this is enough.

Conversely suppose that $\beta\colon V \times V \to \mathbb{K}$ is a non-degenerate bilinear form. If $f_\beta(x) = 0$, then $x = 0$ by non-degeneracy. So $f_\beta\colon V \simeq V^*$ [$\mathbb{K}$-**Mod**].

(iii) Return to the construction, in the same notation.

Suppose that f is G-covariant. Thus $f(g \cdot x) = g \cdot f(x)$. Let $\varphi = f(x) \in V^*$, so that $f(gx) = g \cdot \varphi$. By definition of the dual representation, for $y \in V$ one has $(g \cdot \varphi)(y) = \varphi(g^{-1}y)$. Therefore $f(gx)(y) = f(x)(g^{-1}y)$ and finally:

$$\beta_f(gx, gy) = f(gx)(gy) = f(x)(g^{-1}gy) = f(x)(y) = \beta_f(x, y),$$

so β_f is preserved by G.

Conversely, if β is preserved by G, then:

$$f_\beta(g \cdot x)(y) = \beta(gx, y) = \beta(x, g^{-1}y) = f(x)(g^{-1}(y)) = (g \cdot f(x))(y),$$

so $f_\beta(g\cdot) = g \cdot f(x)$ inside V^*. □

11.2 Real, purely complex, quaternionic representations

With Proposition 11.1.3, one could expect the theory to divide in two: either $V \simeq V^*$ or not, based on existence or not of non-degenerate bilinear G-forms. But the theory of bilinear forms divides itself into two main subtopics, so there are three cases in total.

11.2.1. Definition. A bilinear form β is:

- *symmetric* if $(\forall x)(\forall y)(\beta(y,x) = \beta(x,y))$;
- *alternating* if $(\forall x)(\forall y)(\beta(y,x) = -\beta(x,y))$.

We write Bil^s, resp. Bil^a for symmetric, resp. alternating bilinear forms. $G\text{-}\mathrm{Bil}^s$ and $G\text{-}\mathrm{Bil}^a$ are defined likewise.

One also says *skew-symmetric* for alternating.

11.2.2. Proposition. *Let G be a finite group; work over $\mathbb{C}$. Let V be an irreducible, $\mathbb{C}$-linear representation. Then:*

(i) every non-zero, bilinear G-form on V is non-degenerate;

(ii) exactly one of the following three case occurs:
- **[real]:** $G\text{-}\mathrm{Bil} = G\text{-}\mathrm{Bil}^s$ *has dimension* 1 *and* $G\text{-}\mathrm{Bil}^a = \{0\}$.
- **[purely complex]:** $G\text{-}\mathrm{Bil} = G\text{-}\mathrm{Bil}^s = G\text{-}\mathrm{Bil}^a = \{0\}$.
- **[quaternionic]:** $G\text{-}\mathrm{Bil} = G\text{-}\mathrm{Bil}^a$ *has dimension* 1 *and* $G\text{-}\mathrm{Bil}^s = \{0\}$.

Proof. The claims follow from two lemmas.

11.2.3. Lemma. *Let V be an irreducible $\mathbb{C}$-linear representation of a finite group G. Then every non-zero, bilinear G-form is non-degenerate. Moreover* $\dim G\text{-}\mathrm{Bil} = 0$ *or* 1.

Proof. Recall from Proposition 11.1.3 that we have a 'dictionary': $G\text{-}\mathrm{Bil}_{\mathbb{C}}(V\times V, \mathbb{C}) \simeq \mathrm{Hom}_{\mathbb{C}[G]}(V, V^*)$. Now V is irreducible, and therefore so is V^*. Thus by Schur's Lemma, $\mathrm{Hom}_{\mathbb{C}[G]}(V, V^*)$ is either trivial or 1-dimensional.

Let $\beta\colon V \times V \to \mathbb{C}$ be a bilinear G-form. Let $f_\beta\colon V \to V^*$ $[\mathbb{C}\text{-}\mathbf{Mod}]$ be given by Proposition 11.1.3; then $f_\beta \neq 0$. By Schur's Lemma again, f_β is an isomorphism. Translating back through Proposition 11.1.3, β_f is non-degenerate. ☐

11.2.4. Lemma. *Let V be any representation over a field of characteristic $\neq 2$. Then* $\mathrm{Bil} = \mathrm{Bil}^s \oplus \mathrm{Bil}^a$, *and* $G\text{-}\mathrm{Bil} = G\text{-}\mathrm{Bil}^s \oplus G\text{-}\mathrm{Bil}^a$.

Proof. Let $\beta\colon V \times V \to \mathbb{C}$ be bilinear. Notice how:

$$\beta^s(x,y) = \frac{\beta(x,y)+\beta(y,x)}{2} \quad \text{and} \quad \beta^a(x,y) = \frac{\beta(x,y)-\beta(y,x)}{2}$$

are two bilinear forms; the first is symmetric and the second is alternating. Moreover $\beta = \beta^s + \beta^a$. Last, if β is a G-form, so are β^s and β^a. ☐

We prove the Proposition. The first lemma implies (i) so we move to (ii). The three cases are mutually exclusive. If there is no non-trivial bilinear G-form, we are in the **purely complex** case. So suppose there is one, $\beta \neq 0$; decompose it as $\beta = \beta^s + \beta^a$. By the first lemma again, $\dim G\text{-}\mathrm{Bil} = 1$, so $G\text{-}\mathrm{Bil} = \langle \beta \rangle$. In particular there is $\lambda \in \mathbb{C}$ with $\beta^s = \lambda\beta$. If $\lambda \neq 0$ then $\beta^s \neq 0$; thus $\langle \beta^s \rangle = G\text{-}\mathrm{Bil}^s = G\text{-}\mathrm{Bil}$ and there remains $G\text{-}\mathrm{Bil}^a = \{0\}$: this is the **real** case. Otherwise $\lambda = 0$, meaning $\beta = \beta^a \neq 0$: we reach the **quaternionic** case. □

11.2.5. Remarks.

- It is enough to have $\mathbb{K}$ a good field of characteristic $\neq 2$.
- Beware of terminology (1). The character χ_V is real-valued iff V is (real or quaternionic). The proof is immediate: χ_V is real-valued iff $\chi_{V^*} = \chi_V^* = \overline{\chi_V} = \chi_V$ iff $V^* \simeq V$ $[\mathbb{C}[G]\text{-}\mathbf{Mod}]$, and we apply Proposition 11.1.3.
- Beware of terminology (2). In all three cases, $\mathrm{End}_{\mathbb{C}[G]}(V) = \mathbb{C}\,\mathrm{Id}_V$ by irreducibility, so quaternions will never emerge as Schur's field. A better name for the third case could have been Weyl's neologism *symplectic*, since a *symplectic form* is a non-degenerate, alternating bilinear form.
- Reason for the terminology is in exercise 11.4.3.

11.3 More on real and quaternionic geometries

We elaborate on the cases delinated by Proposition 11.2.2. Recall that a map $f\colon V_1 \to V_2$ between complex vector spaces is *semi-linear* if it is additive but $f(\lambda v) = \overline{\lambda} f(v)$. (It is then $\mathbb{R}$-linear but 'twists' the action of i.)

11.3.1. Proposition. *Let G be a finite group; work over $\mathbb{C}$. Let V be a $\mathbb{C}$-linear, irreducible representation. Then the following are equivalent:*

(i) there exists a non-degenerate, symmetric, bilinear G-form on V;

(ii) there exists a G-covariant, semi-linear isomorphism $\sigma\colon V \to V$ with $\sigma^2 = \mathrm{Id}_V$;

(iii) there exists a real, *G-invariant vector space $W \subseteq V$ with $V = W \oplus iW$.*

11.3.2. Remarks. Let us rephrase (iii).

- In matrix form: there is a basis $\mathcal{B}$ in which all matrices $\mathrm{Mat}_{\mathcal{B}}\,\rho(g)$ have *real* coefficients.
- In dimension-theoretic form: there is a real, G-invariant vector space $W \subseteq V$ with $\dim_{\mathbb{R}} W = \dim_{\mathbb{C}} V$ and $V = \langle W \rangle_{\mathbb{C}}$.
- In abstract form: there is an $\mathbb{R}$-linear representation W' such that $V \simeq W' \otimes_{\mathbb{R}} \mathbb{C}$, where $\mathbb{C}$ is equipped with the trivial G-action and the usual $\mathbb{R}$-action.

This accounts for the name: a $\mathbb{C}$-linear representation is *real* if it comes from an $\mathbb{R}$-linear representation.

Proof.

(i)⇒(ii). By Proposition 11.1.3, such a bilinear form induces an isomorphism $f_\beta\colon V \simeq V^*$ $[\mathbb{K}[G]\text{-}\mathbf{Mod}]$. (We have not used symmetry of β so far.)

Let $[\cdot|\cdot]$ a complex scalar product on V. It is the same as a semi-linear isomorphism $s\colon V \simeq V^*$. If we average $[\cdot|\cdot]$ using G, we may even take a complex scalar product $[\![\cdot|\cdot]\!]$ *preserved by* G. (This method was already in exercise 3.4.5.) Hence we may suppose that there is a semilinear, G-covariant isomorphism $s\colon V \simeq V^*$. It satisfies $s(x)(y) = [\![x|y]\!]$. In particular, for $\varphi \in V^*$, one has:

$$[\![s^{-1}\varphi|y]\!] = \varphi(y).$$

Finally let $\sigma = s^{-1} \circ f_\beta\colon V \to V$. It is a semi-linear, G-covariant isomorphism. So $\sigma^2\colon V \to V$ is a *linear*, G-covariant isomorphism. By irreducibility and Schur's Lemma, there is $\lambda \in \mathbb{C}$ with $\sigma^2 = \lambda \operatorname{Id}_V$. Now:

$$[\![\sigma x|y]\!] = [\![s^{-1} f_\beta(x)|y]\!] = f_\beta(x)(y) = \beta(x,y),$$

so finally using symmetry of β:

$$[\![\sigma x|y]\!] = \beta(x,y) = \beta(y,x) = [\![\sigma y|x]\!].$$

We apply this to $y = \sigma x$, getting:

$$[\![\sigma x|\sigma x]\!] = [\![\sigma\sigma x|x]\!] = [\![\lambda x|x]\!] = \overline{\lambda}\,[\![x|x]\!].$$

But for $x \neq 0$, both $[\![\sigma x|\sigma x]\!]$ and $[\![x|x]\!]$ are positive real numbers; thus so are $\overline{\lambda}$ and λ. Up to rescaling by $\frac{1}{\sqrt{\lambda}}$, we may thus suppose $\lambda = 1$.

(ii)⇒(iii). Treat V as a *real* vector space. There the *linear* map σ satisfies $\sigma^2 = \operatorname{Id}_V$, so it is diagonalisable with eigenvalues ± 1. Let $W_+ = E_1(\sigma)$ and $W_- = E_{-1}(\sigma)$. Then $V = W_+ \oplus W_-$. Moreover, each is clearly G-invariant.

We claim that $W_- = iW_+$. Indeed, if $w_+ \in W_+$, then $\sigma(iw_+) = -i\sigma(w_+) = -iw_+$, so $iW_+ \leq W_-$. The converse inclusion is proved similarly. It follows that W_+ and W_- have the same real dimension.

Thus $V = W_+ \oplus iW_+$, and in particular, $\langle W\rangle = V$ as a $\mathbb{C}$-vector space. Moreover, $\dim_{\mathbb{C}} V = \frac{1}{2}\dim_{\mathbb{R}} V = \frac{1}{2}(\dim_{\mathbb{R}} W_+ + \dim_{\mathbb{R}}(iW_+)) = \dim_{\mathbb{R}} W_+$.

(iii)⇒(i). Let $W \subseteq V$ be a *real*, G-invariant, subspace such that $V = W \oplus iW$; hence every $v \in V$ writes uniquely as $v = x + iy$ with $x, y \in W$. Take a real scalar product on W. Averaging it, we may take a real scalar product $[\![\cdot|\cdot]\!]$ on W *which is preserved by* G. Now simply put:

$$(x+iy|x'+iy') = ([\![x|x']\!] - [\![y|y']\!]) + ([\![x|y']\!] + [\![y|x']\!])i \in \mathbb{C}.$$

Then $(\cdot|\cdot)$ is $\mathbb{C}$-bilinear and G-covariant. Since it is non-zero, it is non-degenerate by Proposition 11.2.2. □

In a very similar way, one proves the following.

11.3.3. Proposition. *Let G be a finite group and V be a $\mathbb{C}$-linear, irreducible representation. Then the following are equivalent:*

(i) there exists a non-degenerate, alternating, bilinear G-form on V;

(ii) there exists a G-covariant, semi-linear isomorphism $\sigma\colon V \to V$ with $\sigma^2 = -\operatorname{Id}_V$.

11.4 Exercises

11.4.1. Exercise. *Let V be a $\mathbb{K}$-linear representation of G. Define an action of G on* $\mathrm{Bil}_{\mathbb{K}}(V \times V, \mathbb{K})$ *such that the map $\beta \mapsto f_\beta$ of Proposition 11.1.3 is a morphism of representations. Why could you expect inversions?*

11.4.2. Exercise. *Prove Proposition 11.3.3.*

11.4.3. Exercise. *Let $\mathbb{H}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ be the group of basic quaternions.*

1. *Compute the only irreducible, 2-dimensional character over $\mathbb{C}$, say χ_2.*
2. *Prove that χ_2 is* not *real. [Hint: extend the candidate group morphism $\mathbb{H}_8 \to \mathrm{GL}_2(\mathbb{R})$ to the associative algebra of quaternions $\mathbb{H}$.]*
3. *Consider the following realisation of quaternions:*[12]

$$\mathbb{H} = \left\{ \begin{pmatrix} z_1 & -\overline{z_2} \\ z_2 & \overline{z_1} \end{pmatrix} : (z_1, z_2) \in \mathbb{C}^2 \right\} \leq M_2(\mathbb{C}) \quad [\mathbb{R}\text{-}\mathbf{Alg}].$$

   Realise χ_2 by giving explicit $\mathbb{H}_8 \hookrightarrow \mathbb{H}^\times \leq \mathrm{GL}_2(\mathbb{C})$.

11.4.4. Exercise (real-valued characters, and groups of odd order)**.** *Let G be a finite group. We work over $\mathbb{C}$. A (complex) character χ is* real-valued *if $\chi = \overline{\chi}$. A conjugacy class $\gamma \in \mathrm{Conj}(G)$ is* real *if $\gamma^{-1} = \gamma$.*

1. *Prove that γ is real iff $(\forall \chi \in \mathrm{Irr}_{\mathbb{C}}(G))(\chi(\gamma) \in \mathbb{R})$. [Hint: column orthogonality.]*
2. *Let $d = \# \mathrm{Irr}_{\mathbb{C}}(G) = \# \mathrm{Conj}(G)$. Let $\sigma_1, \sigma_2 \in \mathrm{Sym}(d)$ be given by $\overline{\chi_i} = \chi_{\sigma_1(i)}$ and $\gamma_i^{-1} = \gamma_{\sigma_2(i)}$.*

   Also let $\rho = \mathrm{perm}\,\mathrm{Sym}(d) \colon \mathrm{Sym}(d) \to \mathrm{GL}_d(\mathbb{C})$ be the permutation representation. Finally let $M \in M_d(\mathbb{C})$ be the character table.

   What are $\rho(\sigma_1)M$ and $M\rho(\sigma_2)$?
3. *Deduce that the number of real conjugacy classes equals the number of real-valued characters. [Hint: what is $\mathrm{tr}\,\rho(\sigma_1)$?]*
4. *Deduce that $|G|$ is odd iff the only real-valued irreducible character of G is* triv. *[This question contains no representation theory.]*
5. *Deduce that if $|G|$ is odd, then $\# \mathrm{Conj}(G) \equiv |G|\ [16]$.*

12 The Frobenius-Schur formula

Abstract. The *Frobenius-Schur formula* determines whether an irreducible, $\mathbb{C}$-linear representation is real, purely complex, or quaternionic in the sense of § 11.

[12] Good publicity for my other NMK lecture notes!

12.1 Statement

Recall that an irreducible, $\mathbb{C}$-linear representation (V, ρ) is:

- **real** if there exists a non-zero, *symmetric*, bilinear G-form on V;
- **purely complex** if there exists *no* non-zero, bilinear G-form on V;
- **quaternionic** if there exists a non-zero, *alternating*, bilinear G-form on V.

12.1.1. Theorem. *Let G be a finite group and V be a $\mathbb{C}$-linear, irreducible representation with character χ. Then:*

$$\frac{1}{|G|}\sum_{g\in G}\chi(g^2) = \begin{cases} 1 & \text{if } V \text{ is real} \\ 0 & \text{if } V \text{ is purely complex} \\ -1 & \text{if } V \text{ is quaternionic.} \end{cases}$$

There are no other values.

The proof requires a short geometric digression.

12.2 Sym and Alt

Here Sym and Alt do not stand for symmetric and alternating groups, but for certain factors of tensor powers. These construction are natural in geometry.

12.2.1. Definition. Let V be a vector space and k be an integer. Let Σ_k be the symmetric group on $\{1, \ldots, k\}$.

- The k^{th} *symmetric power* of V is:

$$\mathrm{Sym}^k(V) = \left(\bigotimes^k V\right) \Big/ \left\langle \left\{ \begin{array}{r} v_1 \otimes \cdots \otimes v_k = v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(k)} : \\ (v_1, \ldots, v_k) \in V^k, \sigma \in \Sigma_k \end{array} \right\} \right\rangle$$

- The k^{th} *exterior power* of V is:

$$\mathrm{Alt}^k(V) = \left(\bigotimes^k V\right) \Big/ \left\langle \left\{ \begin{array}{r} v_1 \otimes \cdots \otimes v_k = \varepsilon(\sigma) v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(k)} : \\ (v_1, \ldots, v_k) \in V^k, \sigma \in \Sigma_k \end{array} \right\} \right\rangle$$

12.2.2. Notation. In the notation above, we let:

- $v_1 \cdots v_k$ be the image of $v_1 \otimes \cdots \otimes v_k$ in $\mathrm{Sym}^k(V)$;
- $v_1 \wedge \cdots \wedge v_k$ be the image of $v_1 \otimes \cdots \otimes v_k$ in $\mathrm{Alt}^k(V)$.

12.2.3. Lemma. *Let G be a group and $\mathbb{K}$ be a field of characteristic $\neq 2$. Let V be a $\mathbb{K}$-linear, finite-dimensional representation of G. Then:*

(i) $\mathrm{Sym}^2(V)$ *and* $\mathrm{Alt}^2(V)$ *are naturally representations, under* $g \cdot (xy) = (gx)(gy)$ *and* $g \cdot (x \wedge y) = (gx) \wedge (gy)$*, extended linearly.*

(ii) $\mathrm{Sym}^2(V)$ *and* $\mathrm{Alt}^2(V)$ *are isomorphic to subrepresentations of* $V \otimes V$*; moreover*

$$V \otimes V \simeq \mathrm{Sym}^2(V) \oplus \mathrm{Alt}^2(V) \quad [\mathbb{K}[G]\text{-}\mathbf{Mod}];$$

(iii) $\chi_{\mathrm{Sym}^2(V)}(g) = \frac{1}{2}(\chi_V(g)^2 + \chi_V(g^2))$ *and* $\chi_{\mathrm{Alt}^2(V)}(g) = \frac{1}{2}(\chi_V(g)^2 - \chi_V(g^2))$.

Proof.

(i) Clear.

(ii) Let $\mathcal{B} = \{e_1, \dots, e_n\}$ be a basis of V. Then $\{e_i \otimes e_j : 1 \le i, j \le n\}$ is a basis of $V \otimes V$.

- Let $\Sigma_2 = \langle (12) \rangle$ act on $V \otimes V$ by letting $(12)(e_i \otimes e_j) = e_j \otimes e_i$, extended linearly. Let σ be the image of (12) in $\mathrm{End}_{\mathbb{K}}(V \otimes V)$. Thus,

$$\sigma\left(\sum \lambda_{i,j} e_i \otimes e_j\right) = \sum \lambda_{i,j} e_j \otimes e_i = \sum \lambda_{j,i} e_i \otimes e_j.$$

  In particular, $\sigma(v_1 \otimes v_2) = v_2 \otimes v_1$ for all $v_1, v_2 \in V$.
- Notice G-covariance of σ.
- Clearly $\sigma^2 = \mathrm{Id}$ in $\mathrm{End}_{\mathbb{K}}(V \otimes V)$, so $(\sigma - \mathrm{Id})(\sigma + \mathrm{Id}) = 0$. Basic linear algebra implies $\ker(\sigma - \mathrm{Id}) = \mathrm{im}(\sigma + \mathrm{Id})$ while $\ker(\sigma + \mathrm{Id}) = \mathrm{im}(\sigma - \mathrm{Id})$, and also $V \otimes V = \ker(\sigma - \mathrm{Id}) \oplus \ker(\sigma + \mathrm{Id})$.
- Consider the following elements of $V \otimes V$:

$$s_{i,j} = \frac{1}{2}(e_i \otimes e_j + e_j \otimes e_i) \text{ for } i \le j \quad \text{and} \quad a_{i,j} = \frac{1}{2}(e_i \otimes e_j - e_j \otimes e_i) \text{ for } i < j.$$

  Let $\mathcal{B}_s = \{s_{i,j} : i \le j\}$ and $\mathcal{B}_a = \{a_{i,j} : i < j\}$. Since $\#(\mathcal{B}_s \sqcup \mathcal{B}_a) = n^2$ and $e_i \otimes e_j \in \langle \mathcal{B}_s \sqcup \mathcal{B}_a \rangle$, we get that $\mathcal{B}_s \sqcup \mathcal{B}_a$ is a basis.
- Now $\langle \mathcal{B}_s \rangle = \ker(\sigma - 1)$ and $\langle \mathcal{B}_a \rangle = \ker(\sigma + 1)$ follow easily.
- Last, $\mathrm{Sym}^2(V) \simeq (V \otimes V)/\mathrm{im}(\sigma - 1) \simeq \ker(\sigma - 1)$. Moreover, $s_{i,j}$ maps to $e_i e_j$. Similarly, $\mathrm{Alt}^2(V) \simeq (V \otimes V)/\mathrm{im}(\sigma + 1) \simeq \ker(\sigma + 1)$, and $a_{i,j}$ maps to $e_i \wedge e_j$.
- By G-covariance, all the above holds as representations of G.

A byproduct of the proof is that $\{e_i e_j : i \le j\}$ is a basis of $\mathrm{Sym}^2(V)$ and $\{e_i \wedge e_j : i < j\}$ is a basis of $\mathrm{Alt}^2(V)$.

(iii) Let $g \in G$ be fixed. One could have started with an eigenbasis $\mathcal{B} = \{e_1, \dots, e_n\}$ under the action of g, viz. $g e_i = \lambda_i e_i$. Then notice that each $e_i \otimes e_j \in V \otimes V$, each $e_i e_j \in \mathrm{Sym}^2(V)$, each $e_i \wedge e_j \in \mathrm{Alt}^2(V)$ is an eigenvector for g with eigenvalue $\lambda_i \lambda_j$. Since vectors of this type form eigenbases of the corresponding spaces, we conclude that:

$$\chi_{\mathrm{Sym}^2(V)} = \sum_{i \le j} \lambda_i \lambda_j \quad \text{and} \quad \chi_{\mathrm{Sym}^2(V)} = \sum_{i<j} \lambda_i \lambda_j.$$

On the other hand,

$$\chi_V(g)^2 = \left(\sum_i \lambda_i\right)^2 = 2 \sum_{i<j} \lambda_i \lambda_j + \sum_i \lambda_i^2 = 2\chi_{\mathrm{Alt}^2(V)}(g) + \chi_V(g^2).$$

This gives the desired formulas. □

In practice one may want to remember that $\{e_i e_j : i \leq j\}$ is a basis of $\mathrm{Sym}^2(V)$ and $\{e_i \wedge e_j : i < j\}$ one of $\mathrm{Alt}^2(V)$.

12.3 Proof of the Frobenius-Schur formula

Proof. Let V be a $\mathbb{C}$-linear, irreducible representation of G. We study G-covariant bilinear forms on V and the representation $W = \mathrm{Bil}_{\mathbb{K}}(V \times V, \mathbb{K})$. (See exercise 11.4.1.) Also let:

$$W_s = \mathrm{Bil}^s_{\mathbb{K}}(V \times V, \mathbb{K}) = \{\beta \in W : \beta \text{ is symmetric}\},$$

and define W_a likewise. Finally let $d_s = \dim W_s$ and $d_a = \dim W_a$. By Proposition 11.2.2, notice that:

- V is real iff $d_s = 1$ and $d_a = 0$;
- V is purely complex iff $d_s = d_a = 0$;
- V is quaternionic iff $d_s = 0$ and $d_a = 1$.

So the integer $d_s - d_a \in \{1, 0, -1\}$ indicates the geometric type of V. We must therefore prove that the formula computes $d_s - d_a$.

By definition of the tensor product and the dual space,

$$W \simeq \mathrm{Hom}_{\mathbb{K}}(V \otimes V, \mathbb{K}) \simeq (V \otimes V)^* \simeq (V^* \otimes V^*) \quad [\mathbb{K}[G]\text{-}\mathbf{Mod}].$$

It is not hard to see that this induces isomorphisms:

$$W_s \simeq \mathrm{Sym}^2(V^*) \quad [\mathbb{K}[G]\text{-}\mathbf{Mod}] \qquad \text{and} \qquad W_a \simeq \mathrm{Alt}^2(V^*) \quad [\mathbb{K}[G]\text{-}\mathbf{Mod}].$$

By Lemma 12.2.3, their characters are:

$$\chi_{W_s}(g) = \frac{1}{2}(\chi_{V^*}(g)^2 + \chi_{V^*}(g^2)) = \frac{1}{2}(\chi_V^*(g)^2 + \chi_V^*(g^2)),$$

and

$$\chi_{W_a}(g) = \frac{1}{2}(\chi_{V^*}(g)^2 - \chi_{V^*}(g^2)) = \frac{1}{2}(\chi_V^*(g)^2 - \chi_V^*(g^2)).$$

Now the space of symmetric, bilinear G-forms is:

$$G\text{-}\mathrm{Bil}^s_{\mathbb{K}}(V \times V, \mathbb{K}) = C_{W_s}(G) \simeq C_{\mathrm{Sym}^2(V^*)}(G).$$

Lemma 5.2.2 gave a formula for its dimension:

$$d_s = \dim G\text{-}\mathrm{Bil}^s_{\mathbb{K}}(V \times V, \mathbb{K}) = \dim C_{W_s}(G) = \frac{1}{|G|} \sum_G \frac{1}{2}(\chi_V^*(g)^2 + \chi_V^*(g^2)),$$

and likewise:

$$d_a = \dim G\text{-}\mathrm{Bil}^a_{\mathbb{K}}(V \times V, \mathbb{K}) = \dim C_{W_a}(G) = \frac{1}{|G|} \sum_G \frac{1}{2}(\chi_V^*(g)^2 - \chi_V^*(g^2)).$$

Therefore:

$$d_s - d_a = \frac{1}{|G|} \sum_G \chi_V^*(g^2).$$

This looks like the desired formula, but there is a residual *. Fortunately d_s and d_a are integers, so finally:

$$\frac{1}{|G|}\sum_G \chi_V(g^2) = \frac{1}{|G|}\sum_G \overline{\chi_V^*(g^2)} = \overline{d_s - d_a} = d_s - d_a. \qquad \square$$

12.4 Exercises

12.4.1. Exercise. *Return to the decomposition $\beta = \beta^s + \beta^a$ of Lemma 11.2.4. Prove that it is compatible with expressing $V \otimes V \simeq \mathrm{Sym}^2(V) \oplus \mathrm{Alt}^2(V)$ (viz. draw a suitable commutative diagram).*

12.4.2. Exercise.

1. *Show that* $\mathrm{Sym}^k V$ *enjoys the following universal property:*

   > *any k-linear, symmetric map from V^k to another vector space factor uniquely through* $\mathrm{Sym}^k V$.

2. *Find a similar universal property describing* $\mathrm{Alt}^k V$.

12.4.3. Exercise.

1. *Suppose $\mathcal{B}$ is a finite basis of V. Give bases of* $\mathrm{Sym}^k(V)$ *and* $\mathrm{Alt}^k(V)$.
2. *Compute characters.*
3. (*) *Suppose that $\mathbb{K}$ has characteristic coprime to $k!$. Find subrepresentations of $\bigotimes^k V$ isomorphic to* $\mathrm{Sym}^k(V)$, *resp.* $\mathrm{Alt}^k(V)$.

12.4.4. Exercise. *The purpose of this exercise is to construct the character table over $\mathbb{C}$ of* $G = \mathrm{Sym}(5)$. *Let* $\chi_4 = \mathrm{perm} - \mathrm{triv}$, *which is irreducible.*

1. *Prove that* $\mathrm{Alt}^2\,\chi_4$ *is irreducible and has dimension* 6.
2. *Prove that* $\mathrm{Sym}^2\,\chi_4$ *is the sum of three irreducible characters.*
3. *Find an irreducible character of dimension* 5.
4. *Complete the character table of* $\mathrm{Sym}(5)$.

12.4.5. Exercise. *Return to the character tables of* $\mathrm{Alt}(4), \mathrm{Sym}(4), \mathrm{Alt}(5), \mathrm{Sym}(5)$. *Find out which representations are real, purely complex, quaternionic.*

13 The group algebra

Abstract. This section recasts representation theory in *module theory* (§ 13.1). The *group algebra* of G over $\mathbb{K}$ (§ 13.2) is precisely the associative $\mathbb{K}$-algebra encoding the representation theory of G. We then translate orthogonality relations in terms of *central idempotents* (§ 13.3).

13.1 Modules, submodules, morphisms

13.1.1. Definition. Let R be a ring. An *R-module* is a abelian group M equipped with an action of R on M such that, for all $r, s \in R$ and $m, n \in M$:

- $(r+s) \cdot m = r \cdot m + s \cdot m$;
- $1 \cdot m = m$;
- $(r \cdot s) \cdot m = r \cdot (s \cdot m)$;
- $r \cdot (m+n) = r \cdot m + r \cdot n$.

(These do imply $0 \cdot m = 0$.) With the notion of a module comes that of a *submodule*.

13.1.2. Examples.

- The $\mathbb{Z}$-modules are the abelian groups. Then $\mathbb{Z}$-submodules are subgroups.
- If $\mathbb{K}$ is a field, the $\mathbb{K}$-modules are the $\mathbb{K}$-vector spaces. Then $\mathbb{K}$-submodules are $\mathbb{K}$-linear subspaces.
- If $\mathbb{K}$ is a field, the $\mathbb{K}[X]$-modules are the $\mathbb{K}$-vector spaces equipped with one distinguished linear endomorphism f. Then $\mathbb{K}[X]$-submodules are f-invariant subspaces.

13.1.3. Definition. Let R be a ring. An R-module M is *simple*, or *irreducible* if the only two R-submodules of M are $\{0\}$ and M.

We now introduce the suitable notion of morphism.

13.1.4. Definition. Let R be a ring and M_1, M_2 two R–modules.

- An *R-morphism* is a map $\varphi\colon M_1 \to M_2$ such that for all $r \in R$ and $m, m' \in M_1$:
$$\varphi(r \cdot m + m') = r \cdot \varphi(m) + \varphi(m').$$
One sometimes says that φ is *R-covariant*.
- Let R be a ring and M_1, M_2 be two R-modules. We let $\mathrm{Hom}_R(M_1, M_2)$ stand for the collection of R-morphisms from M_1 to M_2. (A better notation would be $(M_1 \to M_2 \colon R\text{-}\mathbf{Mod})$.)

  If R is clear from context, one simply writes $\mathrm{Hom}(M_1, M_2)$.
- An *R-isomorphism* is a bijective R-morphism. We write $M_1 \simeq M_2 \quad [R\text{-}\mathbf{Mod}]$ (isomorphism in the category of R-modules).

Notice that $\mathrm{Hom}_R(M_1, M_2)$ itself is an abelian group. However, in general it does not bear a natural R-module structure.

13.1.5. Examples.

- A $\mathbb{Z}$-morphism between $\mathbb{Z}$-modules is a group morphism between abelian groups.
- A $\mathbb{K}$-morphism between $\mathbb{K}$-vector spaces is a $\mathbb{K}$-linear map.
- A $\mathbb{K}[X]$-morphism between $\mathbb{K}[X]$-modules (V_1, f_1) and (V_2, f_2) is a $\mathbb{K}$-linear map $\varphi\colon f_1 \to f_2$ such that $\varphi \circ f_1 = f_2 \circ \varphi$.

We do *not* introduce tensor products over arbitrary rings. This would only create confusion since in this course, we only tensor over $\mathbb{K}$, never over the group algebra.

13.2 The group algebra and representations

13.2.1. Definition. Let $\mathbb{K}$ be a field and G be a group. The *group algebra* of G over $\mathbb{K}$ is the following associative $\mathbb{K}$-algebra:

- let $\mathbb{K}[G]$ be the vector space with basis $\{g : g \in G\}$;
- define multiplication on $\mathbb{K}[G]$ by extending $\mathbb{K}$-linearly multiplication on G.

Thus $\dim_{\mathbb{K}} \mathbb{K}[G] = |G|$. The identity element is 1. The group algebra is associative because G is, but it is commutative *iff* G is.

13.2.2. Remark. Analysts like to think of $\mathbb{K}[G]$ as the algebra of all functions $G \to \mathbb{K}$. It is then equiped with the *convolution product*:

$$(f_1 * f_2)(g) = \sum_{\substack{x,y \in G: \\ xy = g}} f_1(x) f_2(y).$$

One should check at once that $(\mathbb{K}[G]; +, \cdot)$ and $(\mathbb{K}^G; +, *)$ are naturally isomorphic as associative $\mathbb{K}$-algebras: just take $\sum_G \lambda_g g$ to the map $(x \mapsto \lambda_x)$.

13.2.3. Definition. Let $\mathbb{K}$ be a field and G be a group.

- A $\mathbb{K}$-*linear representation of* G is a $\mathbb{K}[G]$-module.
- A representation is *irreducible* if it is a simple $\mathbb{K}[G]$-module.
- A *morphism of representations* is a $\mathbb{K}[G]$-morphism.
- Hence two representations are *isomorphic* if they are, as $\mathbb{K}[G]$-modules.

One should pause and check that definitions do match with their naive forms of § 1. The above relies on a form of universal property: every group morphism $\rho: G \to \mathrm{GL}(V)$ extends to a unique $\mathbb{K}$-algebra morphism $\mathbb{K}[G] \to \mathrm{End}_{\mathbb{K}}(V)$. *We still denote it by* ρ.

13.2.4. Remark. It is possible to tensor $\mathbb{K}[G]$-modules over $\mathbb{K}[G]$, but this does *not* give the tensor representation.

Let $V = \mathrm{reg}$, which is $\mathbb{K}[G]$ as a $\mathbb{K}[G]$-module. Then $V \otimes_{\mathbb{K}[G]} V = \mathbb{K}[G] = V$, while $V \otimes_{\mathbb{K}} V$ has dimension $(\dim V)^2 > \dim V$.

13.2.5. Theorem (Schur's Lemma, revisited)**.** *Let R be any ring and V_1, V_2 be simple R-modules.*

(i) If $f: V_1 \to V_2$ is an R-morphism, then either $f = 0$ or f is an isomorphism.

(ii) In particular, if V is a simple R-module, then $\mathrm{End}_R(V)$ *is a skew-field.*

(iii) Suppose that R is a finite-dimensional associative $\mathbb{K}$-algebra for some algebraically closed field $\mathbb{K}$. If V is a finitely generated, simple R-module, then $\mathrm{End}_R(V) = \mathbb{K}\,\mathrm{Id}_V$.

13.2.6. Definition. Let R be a ring.

- An R-module M is *semisimple* if it a direct sum of simple R-modules.
- R itself is said to be *semisimple* if it is, as a (left) R-module. See exercise 13.5.2.

13.2.7. Theorem. *Let R be a semisimple ring and M be an R-module. Then:*

(i) Every submodule admits a direct complement.

(ii) M is a direct sum of simple submodules.

(iii) If M is finitely generated, then it is a direct sum of finitely many simple submodules.

13.2.8. Theorem (Maschke's Theorem, revisited)**.** *Let G be a finite group and $\mathbb{K}$ be a field of coprime characteristic. Then $\mathbb{K}[G]$ is semisimple.*

Theorem 3.3.2 on isotypical components translates so immediately that we do not reproduce it. We move to the isomorphism type of the group algebra.

13.2.9. Theorem. *Let G be a finite group and $\mathbb{K}$ be a good field. Let $d_\rho = \dim \rho$ be the dimensions of the irreducible representations of G over $\mathbb{K}$. Then as associative $\mathbb{K}$-algebras:*

$$\mathbb{K}[G] \simeq \prod_{\rho \in \mathrm{Irr}_{\mathbb{K}}(G)} M_{d_\rho}(\mathbb{K}) \quad [\mathbb{K}\text{-}\mathbf{Alg}].$$

This is a special instance of the *Artin-Wedderburn theorem*.[13]

Proof. Since $\dim V_\rho = d_\rho$, one has $V_\rho \simeq \mathbb{K}^{d_\rho}$ $[\mathbb{K}\text{-}\mathbf{Mod}]$. Hence $\mathrm{Hom}_{\mathbb{K}}(V_\rho, V_\rho) \simeq \mathrm{End}_{\mathbb{K}}(\mathbb{K}^{d_\rho}) \simeq M_{d_\rho}(\mathbb{K})$ $[\mathbb{K}\text{-}\mathbf{Mod}]$. For each ρ we fix a basis $\mathcal{B}_\rho$ of V_ρ. So we have now fixed an isomorphism:

$$\prod_{\rho \in \mathrm{Irr}_{\mathbb{K}}(G)} \mathrm{End}_{\mathbb{K}}(V_\rho) \simeq \prod_{\rho \in \mathrm{Irr}_{\mathbb{K}}(G)} M_{d_\rho}(\mathbb{K}) \quad [\mathbb{K}\text{-}\mathbf{Alg}].$$

For $g \in G$ and $\rho \in \mathrm{Irr}_{\mathbb{K}}(G)$, let $M_\rho(g) = \mathrm{Mat}_{\mathcal{B}_\rho}(g)$. Each $M_\rho(\cdot)$ is a group morphism from G to $\mathrm{GL}_{d_\rho}(\mathbb{K})$. Now to $g \in G$ associate the family of matrices:

$$(M_\rho(g))_\rho \in \Pi_{\rho \in \mathrm{Irr}_{\mathbb{K}}(G)} M_{d_\rho}(\mathbb{K}).$$

This defines a multiplicative map $G \to \prod_{\rho \in \mathrm{Irr}_{\mathbb{K}}(G)} M_{d_\rho}(\mathbb{K})$, which extends by linearity to a morphism of associative $\mathbb{K}$-algebras $\mathcal{F}\colon \mathbb{K}[G] \to \prod_{\rho \in \mathrm{Irr}_{\mathbb{K}}(G)} M_{d_\rho}(\mathbb{K})$. We claim that $\mathcal{F}$ is an isomorphism in $\mathbb{K}$-**Alg**.

$\mathcal{F}$ is injective: if g acts trivially on every V_ρ, then g acts trivially on any representation, so it acts trivially on the regular representation. But reg is injective, so $g = 1$. Now $\mathcal{F}$ is surjective as well, because $|G| = \sum_{\rho \in \mathrm{Irr}_{\mathbb{K}}(G)} d_\rho^2$. It is an isomorphism. □

An explicit isomorphism is discussed in § 13.4. We first return to orthogonality and class functions.

13.3 Central idempotents

Let us reformulate orthonormality of the irreducible characters in abstract terms.

13.3.1. Definition. Let R be a ring.

- An element x is *central* if $(\forall y)(xy = yx)$.
- An *idempotent* is a nonzero element $0 \neq e \in R$ with $e^2 = e$.
- Two idempotents e_1, e_2 are *orthogonal* if $e_1 e_2 = e_2 e_1 = 0$.

[13] I have to teach this in the Village someday.

- An idempotent e is *primitive* if it cannot be written as $e = f_1 + f_2$ where f_i are idempotents $\neq 0, 1$.
- A *complete set of central primitive idempotents* is a family of central, primitive idempotents summing to 1.

13.3.2. Theorem. *Let G be a finite group and $\mathbb{K}$ be a good field. For $\chi \in \mathrm{Irr}_{\mathbb{K}}(G)$, let $e_\chi = \frac{\chi(1)}{|G|} \sum_{g \in G} \chi(g^{-1}) g$. Then $\{e_\chi : \chi \in \mathrm{Irr}_{\mathbb{K}}(G)\}$ is both:*

(i) a $\mathbb{K}$-linear basis of the centre of $\mathbb{K}[G]$;

(ii) a complete set of central primitive idempotents of $\mathbb{K}[G]$.

Proof. This is essentially repeating the orthogonality relations; here are the main lines.

(i) The space $\mathcal{C}_{\mathbb{K}}(G)$ of class functions is exactly the centre of $\mathbb{K}[G]$. Indeed, $f = \sum_g \lambda_g g \in \mathbb{K}[G]$ is central iff $(\forall h \in G)(fh = hf)$ iff $(\forall g, h \in G)(\lambda_{gh} = \lambda_{hg})$. Since characters are class functions, we do have $e_\chi \in Z(\mathbb{K}[G])$.

They form a family of cardinal $\# \mathrm{Irr}_{\mathbb{K}}(G) = \# \mathrm{Conj}(G) = \dim \mathcal{C}_{\mathbb{K}}(G) = \dim Z(\mathbb{K}[G])$. So it only remains to prove linear independence, which will follow from (ii).

(ii) We analyse reg term by term.

Let (W, σ) be an irreducible representation with character ψ. Since $e_\chi \in Z(\mathbb{K}[G])$, one has $\sigma(e_\chi) \in Z(\sigma(\mathbb{K}[G]))$, so $\sigma(e_\chi)$ is G-covariant. By Schur's Lemma, there is $\lambda_{\chi,\psi} \in \mathbb{K}$ such that $\sigma(e_\chi) = \lambda_{\chi,\psi} \mathrm{Id}_W$. Now:

$$\lambda_{\chi,\psi} \psi(1) = \lambda_{\chi,\psi} \dim W = \operatorname{tr} \sigma(e_\chi) = \frac{\chi(1)}{|G|} \sum_{g \in G} \chi(g^{-1}) \psi(g) = \chi(1) \, (\chi | \psi) \,.$$

By orthogonality, $\lambda_{\chi,\psi} = \delta_{\chi,\psi}$. Thus $\sigma(e_\chi) = \lambda_{\chi,\psi} \mathrm{Id}_W$ is 0 on irreducible representations non-isomorphic to χ, and Id on irreducible representations isomorphic to χ.

Since reg_G is a direct sum of irreducible representations, $e_\chi = \mathrm{reg}(e_\chi)$ is the identity on $\mathrm{Iso}_{\mathrm{reg}}(\chi)$ and the zero map on other isotypical components: thus e_χ is the projector onto $\mathrm{Iso}_{\mathrm{reg}}(\chi)$ parallel to the other terms.

It follows that e_χ is an idempotent, and $e_\chi e_\psi = 0$ whenever $\chi \neq \psi$. Finally, $\sum e_\chi = \mathrm{Id}_{\mathrm{reg}} = 1$. This certainly implies linear independence, and also completes the proof of (i). □

13.3.3. Remark. One sometimes uses the following $\mathbb{Z}$-basis of $\mathbb{Z}[G]$. For $\gamma \in \mathrm{Conj}(G)$ a conjugacy class, let $e_\gamma = \sum_{g \in \gamma} g$. Then $\{e_\gamma : \gamma \in \mathrm{Conj}(G)\}$ is a $\mathbb{Z}$-basis of $\mathbb{Z}[G]$. It can be proved that every e_γ is an algebraic integer of the ring $\mathbb{K}[G]$. (This is what we did in Theorem 7.3.1, Step 1.)

(*) 13.4 Fourier transform

Let G be a finite group and $\mathbb{K}$ be a good field. By the Artin-Wedderburn theorem (Theorem 13.2.9), there are finite-dimensional vector spaces $V_1, \ldots, V_r$ and an isomorphism of associative $\mathbb{K}$-algebras:

$$\mathbb{K}[G] \simeq \prod_{i=1}^{r} \mathrm{End}_{\mathbb{K}}(V_i) \quad [\mathbb{K}\text{-}\mathbf{Alg}].$$

(We do mean $\mathrm{End}_{\mathbb{K}}$ and certainly not $\mathrm{End}_{\mathbb{K}[G]}$.) The present, completely optional, subsection elaborates on this fact and gives an explicit isomorphism: the *Fourier transform* on the group.

Notation. Even though we work over an arbitrary good field, we adopt the *analytic* point of view on the group algebra. So $\mathbb{K}[G]$ is the $\mathbb{K}$-algebra of functions $f: G \to \mathbb{K}$, equiped with the *convolution product*

$$(f_1 * f_2)(g) = \sum_{\substack{x,y:\\ xy=g}} f_1(x) f_2(y).$$

(In algebraic terms, if $f = \sum \lambda_g g$, one simply lets $f(g) = \lambda_g$.)

Thus $f(g)$ makes sense, and is a scalar. Below we shall also consider functions $\varphi: \mathrm{Irr}_{\mathbb{K}}(G) \to S$ for some set S. Then $\varphi(\rho)$ will make sense. (Here, φ will *not* stand for a linear form.)

The Fourier transform takes functions f (viz. functions from G to $\mathbb{K}$) to functions φ (viz. certain functions from $\mathrm{Irr}_{\mathbb{K}}(G)$ to S). The inverse Fourier transform does the converse.

The general case. In physics the Fourier coefficients are not pure numbers. At each *frequency* one has an *energy*; these quantities have very different natures; energies are parametrised by frequencies. In non-abelian group theory, the Fourier 'coefficients' are:

- *linear operators*,
- parametrised by *irreducible representations*.

Hence $\mathrm{Irr}_{\mathbb{K}}(G)$ plays the role of the spectrum, viz. the set indexing the Fourier components, and each component is in $\mathrm{End}_{\mathbb{K}}(\rho)$.

13.4.1. Notation.

- For $\rho: G \to \mathrm{GL}(V)$ a representation of G we still denote by ρ its natural extension $\mathbb{K}[G] \to \mathrm{End}_{\mathbb{K}}(V)$, which is a morphism of $\mathbb{K}[G]$-algebras.

  Hence, always seeing f as a function $G \to \mathbb{K}$:

  $$\rho(f) = \sum_{g \in G} \underbrace{f(g)}_{\in \mathbb{K}} \underbrace{\rho(g)}_{\in \mathrm{End}_{\mathbb{K}}(V)}.$$

  Notice that $\rho(f) \in \mathrm{End}_{\mathbb{K}}(V)$; in general $\rho(f)$ need not be G-covariant.

- For $f \in \mathbb{K}[G]$ we let: $\hat{f}(\rho) = \rho(f) = \sum_{g \in G} f(g)\rho(g)$.

13.4.2. Remark. Technically, $\hat{f}$ is thus a map from $\mathrm{Irr}_{\mathbb{K}}(G)$ to $\bigsqcup_{\rho \in \mathrm{Irr}_{\mathbb{K}}(G)} \mathrm{End}_{\mathbb{K}}(V_\rho)$. However, at each ρ, one has $\hat{f}(\rho) \in \mathrm{End}_{\mathbb{K}}(V_\rho)$, and therefore:

$$\hat{f} \in \prod_{\rho \in \mathrm{Irr}_{\mathbb{K}}(G)} \mathrm{End}_{\mathbb{K}}(V_\rho).$$

(If G is abelian, this will simplify dramatically.)

13.4.3. Theorem. *Let G be a finite group and $\mathbb{K}$ be a good field.*

(i) For $f \in \mathbb{K}[G]$ let $\hat{f}(\rho) = \sum_{g \in G} f(g)\rho(g)$. Then $\mathcal{F}(f) = \hat{f}$ defines an isomorphism of $\mathbb{K}[G]$-algebras:

$$\mathbb{K}[G] \simeq \prod_{\rho \in \mathrm{Irr}_{\mathbb{K}}(G)} \mathrm{End}_{\mathbb{K}}(\rho) \quad [\mathbb{K}\text{-}\mathbf{Alg}].$$

(ii) For $\varphi \in \prod_{\mathrm{Irr}_{\mathbb{K}}(G)} \mathrm{End}_{\mathbb{K}}(\rho)$, let $\check{\varphi} = \mathcal{F}^{-1}(\varphi)$ be the inverse. Then:

$$\check{\varphi}(g) = \sum_{\rho \in \mathrm{Irr}_{\mathbb{K}}(G)} \frac{\dim \rho}{|G|} \operatorname{tr}\left[\rho(g^{-1})\varphi(\rho)\right].$$

13.4.4. Remarks.

- We always consider $\mathrm{End}_{\mathbb{K}}(\rho)$, since $\mathrm{End}_{\mathbb{K}[G]}(\rho)$ is only 1-dimensional by Schur's Lemma. (Cf. abelian case below.)
- $\mathcal{F}$ is a morphism of associative $\mathbb{K}$-algebras, but *not* a morphism of $\mathbb{K}[G]$-modules.

Proof. For brevity we let $\Pi = \prod_{\rho \in \mathrm{Irr}_{\mathbb{K}}(G)} \mathrm{End}_{\mathbb{K}}(G)$.

(i) Clearly $\mathcal{F} \colon \mathbb{K}[G] \to \Pi$ is well-defined, and linear. Recall that $\mathbb{K}[G]$ is equiped with the convolution product (which extends the group law on G), and Π is equiped with its Cartesian product structure, viz. we compose componentwise: $(\varphi_1 \cdot \varphi_2)(\rho) = \varphi_1(\rho) \circ \varphi_2(\rho)$. So $\mathcal{F}$ is multiplicative and takes 1 to $(\mathrm{Id}_\rho : \rho \in \mathrm{Irr}_{\mathbb{K}}(G))$. Hence it is a morphism of $\mathbb{K}$-algebras.

Now dimensions match, so it suffices to prove injectivity. Suppose $\mathcal{F}(f) = 0$. Then in each irreducible representation, (the image of) f acts trivially. But the regular representation is a direct sum of such, so f acts trivially on $\mathrm{reg} \simeq \mathbb{K}[G]$. Since $\mathbb{K}[G]$ has a unit (viz. since reg is injective), this means $f = 0$.

(ii) This may look difficult but the formula is given, so it is a simple matter of checking it. The linear map $\mathcal{F}^{-1}$ is well-defined. Let:

$$\mathcal{G}(\varphi) = \left[g \mapsto \sum_{\rho \in \mathrm{Irr}_{\mathbb{K}}(G)} \frac{\dim \rho}{|G|} \operatorname{tr}\left(\rho(g^{-1})\varphi(\rho)\right) \right],$$

which is clearly linear from Π to $\mathbb{K}[G]$. We want to prove $\mathcal{G} = \mathcal{F}^{-1}$.

Let $h \in G$. When seen in $\mathbb{K}[G]$, viz. when seen as a function $G \to \mathbb{K}$, h is the 'Dirac mass' $\delta_h(x) = \delta_{h,x}$, which equals 1 at h and 0 everywhere else.

Then $\mathcal{F}(\delta_h) = [\rho \mapsto \rho(h)]$, so at any $g \in G$ one has:

$$\begin{aligned}
\mathcal{G}(\mathcal{F}(\delta_h))(g) &= \sum_{\rho \in \mathrm{Irr}_{\mathbb{K}}(G)} \frac{\dim \rho}{|G|} \operatorname{tr}(\rho(g^{-1})\rho(h)) \\
&= \sum_{\rho \in \mathrm{Irr}_{\mathbb{K}}(G)} \frac{1}{|G|} \cdot \dim \rho \cdot \chi_\rho(g^{-1}h) \\
&= \frac{1}{|G|} \mathrm{reg}_G(g^{-1}h) \\
&= \frac{|G|}{|G|} \delta_{g^{-1}h}(1) \\
&= \delta_h(g).
\end{aligned}$$

This also equals $\mathcal{F}^{-1}(\mathcal{F}(\delta_h))(g)$, and equality holds at every g. Thus, as functions, $\mathcal{G}(\mathcal{F}(\delta_h)) = \mathcal{F}^{-1}(\mathcal{F}(\delta_h))$. Therefore $\mathcal{G}$ and $\mathcal{F}^{-1}$ agree on $\{\mathcal{F}(\delta_h) : h \in G\}$, which is a basis of Π. By linearity, they agree everywhere. □

The abelian case. Let A be a finite *abelian* group.

If $\rho \in \mathrm{Irr}_{\mathbb{K}}(A)$ then $\dim \rho = 1$. Although a 1-dimensional vector space V is *non-canonically* isomorphic to $\mathbb{K}$, the ring $\mathrm{End}(V)$ is *canonically* isomorphic to $\mathbb{K}$. Here $\rho: A \to \mathrm{GL}(V)$, so we may assume $\rho: A \to \mathbb{K}^\times$. Thus irreducible representations are elements of the *dual group* $\hat{A}$, viz. the group of all morphisms $A \to \mathbb{K}^\times$. Hence, here, $\mathrm{Irr}_{\mathbb{K}}(A) = \hat{A}$ bears an additional group structure.

Return to $\rho \in \hat{A}$ and to the canonical isomorphism $\mathrm{End}_{\mathbb{K}}(\rho) \simeq \mathbb{K}$. Therefore:

$$\prod_{\rho \in \mathrm{Irr}_{\mathbb{K}}(A)} \mathrm{End}_{\mathbb{K}}(\rho) \simeq \prod_{\hat{A}} \mathbb{K} \simeq \mathbb{K}^{\hat{A}} \quad [\mathbb{K}\text{-}\mathbf{Alg}].$$

The right-hand is no longer formed of operators but of *Fourier coefficients*.

13.4.5. Remark. Be careful that $\mathbb{K}^{\hat{A}}$, as a $\mathbb{K}$-algebra, is still equiped with the *componentwise* product, which is *not* the same as the convolution product. (This simply means $\mathbb{K}^{\hat{A}} \not\simeq \mathbb{K}[\hat{A}]$ $[\mathbb{K}\text{-}\mathbf{Alg}]$.) There is no escaping from the fact that Fourier changes convolution to componentwise, and vice-versa.

The inverse transform rewrites as follows. Since every linear endomorphism u of a 1-dimensional vector space is the scalar action of $\lambda_u = \operatorname{tr} u$, the inverse transform formula simplifies to:

$$\check{\varphi}(a) = \sum_{\rho \in \hat{A}} \frac{1}{|A|} \rho(-a) \varphi(\rho).$$

(**) **13.4.6. Remark.** First notice that the direct transform can rewrite as:

$$\hat{f}(\rho) = \sum_{a \in A} f(a)\rho(a) = |A| \left(f^* | \rho \right)_A,$$

where $(\cdot|\cdot)_A$ is the usual bilinear form on $\mathcal{C}_{\mathbb{K}}(A)$.

With perversity one may move to the bidual group $\hat{\hat{A}}$ and rewrite the inverse transform using it. Let $\mathrm{ev}_a: \hat{A} \to \mathbb{K}^\times$ take ρ to $\mathrm{ev}_a(\rho) = \rho(a)$ ('evaluation map'). It is not hard to see that $\mathrm{ev}: a \mapsto \mathrm{ev}_a$ is a natural isomorphism $A \simeq \hat{\hat{A}}$. The ev_a are the irreducible characters of $\hat{A}$.

Then the inverse formula de-simplifies to:

$$\check{\varphi}(a) = \sum_{\rho\in\hat{A}} \frac{1}{|A|}\rho(-a)\varphi(\rho) = \sum_{\rho\in\hat{A}} \frac{1}{|\hat{A}|}(\mathrm{ev}_a(-\rho))\varphi(\rho) = (\mathrm{ev}_a\,|\varphi)_{\hat{A}},$$

where $(\cdot|\cdot)_{\hat{A}}$ is the usual bilinear form *on* $\mathcal{C}_{\mathbb{K}}(\hat{A})$.

13.5 Exercises

13.5.1. Exercise. *Let $\mathbb{K}$ be a field, G_1, G_2 be two groups, and $\varphi\colon G_1 \to G_2$ be a group morphism.*

(i) Show that φ naturally induces a morphism of $\mathbb{K}$-algebras $\Phi\colon \mathbb{K}[G_1] \to \mathbb{K}[G_2]$.

(ii) Show that φ is an isomorphism iff Φ is an isomorphism.

Note. *It is an open problem in group theory whether one can have $\mathbb{K}[G_1] \simeq \mathbb{K}[G_2]$ as abstract $\mathbb{K}$-algebras without having $G_1 \simeq G_2$ as groups.*

13.5.2. Exercise. *Let R be a ring. Prove that R is semisimple as a left R-module iff it is as a right R-module.*

13.5.3. Exercise. *Let A be a finite abelian group.*

1. *Let $B \leq A$ be a subgroup. Prove that every morphism $B \to \mathbb{C}^*$ extends to A.*

2. *Prove that $\hat{A}$ is isomorphic to A, and that $\hat{\hat{A}}$ is* canonically *isomorphic to A.*

Further reading

- C. Curtis, *Pioneers of representation theory: Frobenius, Burnside, Schur, and Brauer*. History of Mathematics, 15. American Mathematical Society, Providence, RI, 1999.

- C. Curtis and I. Reiner, *Representation theory of finite group and associative algebras*. Reprint of the 1962 original. American Mathematical Society, Providence, RI, 2006.

- M. Isaacs, *Character theory of finite groups*. Pure and applied mathematics, 69. Academic Press, New York–San Francisco–London, 1976.

- J.-P. Serre, *Linear representations of finite groups*. Translated from the French by L. Scott. Graduate Texts in Mathematics, 42. Springer-Verlag, New York, 1977.

- J.-P. Serre, *Finite groups: an introduction*. International Press, Somerville, 2016.