

23.7 Group Representations

Sections 01–06 studied an algebra of operators in the abstract. A group is not an algebra — its elements cannot be added — but a group can be made to *act* by operators, and then the operators it produces span an algebra. This section sets up that translation: a representation of a group G over F is the same thing as a representation of the group algebra $F[G]$, so everything proved about algebras applies at once. The section’s main theorem, Maschke’s, says when the resulting algebra is semisimple, and its hypothesis on the field is not decoration: we exhibit a group and a field where the conclusion fails outright.

Throughout, G is a **finite** group, written multiplicatively, with its identity element written 1, and F is a field. All vector spaces are finite-dimensional over F . Where a statement needs F to be $\mathbb{C}$, or needs a condition on $\text{char } F$, the statement says so.

23.7.1 Letting a group act by operators

The book’s groups so far have been groups *of* matrices or *of* permutations: $\text{GL}_n(F)$ (Example (Groups)), the symmetric group S_n , the classical groups of Chapter 14. Such a group arrives with its linear algebra attached. An abstract group does not. If all we know about G is its multiplication table, the only way to bring linear algebra to bear is to manufacture operators out of it.

The manufacture has one requirement. Group multiplication must become composition of operators, since composition is the only product on $\mathcal{L}(V)$, and every group element must become an **invertible** operator, since every group element can be undone. That is exactly the definition of a homomorphism into the group $\text{GL}(V)$ of invertible operators on V , a group under composition by the same argument that makes $\text{GL}_n(F)$ one (Example (Groups)).

A representation is a way of realizing the elements of a group as invertible operators, so that multiplying in the group means composing the operators.

Definition 23.7.1. Representation of a group

Let G be a group, F a field, and V a finite-dimensional vector space over F . A **representation** of G on V over F is a group homomorphism

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

that is, a map assigning to each $g \in G$ an invertible operator $\rho(g)$ on V such that $\rho(gh) = \rho(g)\rho(h)$ **for all** $g, h \in G$. The space V is the **representation space**, and $\dim V$ is the **degree** of ρ . The representation is **faithful** if ρ is injective. When $V = F^n$ we speak of a **matrix representation** and write $\rho(g) \in \text{GL}_n(F)$.

In words: to give a representation is to attach to each $g \in G$ an invertible operator $\rho(g)$ on one fixed space V , in such a way that the operator attached to a product is the composition of the operators attached to the factors. Two conditions that look like extra demands are already implied by Theorem 0.10.3: $\rho(1) = \text{id}_V$, and $\rho(g^{-1}) = \rho(g)^{-1}$ for every g . So we never have to check them.

Note what is **not** required. Nothing says ρ is injective, and nothing says the operators $\rho(g)$ are distinct. The constant map $g \mapsto \text{id}_V$ is a perfectly good representation; it simply carries no information about G .

Examples. Fix a finite group G and a field F .

- **The trivial representation.** $V = F$ and $\rho(g) = \text{id}_F$ for every g . It is a representation because $\text{id}_F \cdot \text{id}_F = \text{id}_F$, matching $\rho(gh) = \rho(g)\rho(h)$. Its degree is 1. This is the degenerate case, and it is not a curiosity: it is one of the basic building blocks, and in Section 08 it is the piece that detects averages.
- **The sign representation of S_n .** $V = F$ and $\rho(\sigma) = \text{sgn}(\sigma) \text{id}_F$, where sgn is the sign of a permutation (Definition 7.3.2). It is a homomorphism because $\text{sgn}(\sigma\tau) = \text{sgn}(\sigma)\text{sgn}(\tau)$ (Theorem 7.3.1). Over a field of characteristic 2 we have $-1 = 1$, so the sign representation coincides with the trivial one; over $\mathbb{C}$ it does not. It is faithful on S_2 , whose two elements have signs 1 and -1 , but not on S_n for $n \geq 3$, where $\text{sgn}((1\ 2\ 3)) = 1 = \text{sgn}(\text{id})$ while $(1\ 2\ 3) \neq \text{id}$.
- **The permutation representation of S_n .** $V = F^n$ and $\rho(\sigma)\mathbf{e}_i = \mathbf{e}_{\sigma(i)}$, extended linearly (Theorem 2.1.6). Then $\rho(\sigma)\rho(\tau)\mathbf{e}_i = \rho(\sigma)\mathbf{e}_{\tau(i)} = \mathbf{e}_{\sigma(\tau(i))} = \rho(\sigma\tau)\mathbf{e}_i$, where the last step uses that $\sigma\tau$ means “first τ , then σ ”. So ρ is a homomorphism, and each $\rho(\sigma)$ is invertible with inverse $\rho(\sigma^{-1})$. The matrix of $\rho(\sigma)$ in the standard basis is the permutation matrix $\mathbf{P}_\sigma$ of Definition 3.4.2. The same recipe works for any subgroup of S_n .
- **The rotation representation of $\mathbb{Z}/n\mathbb{Z}$ over $\mathbb{R}$.** $V = \mathbb{R}^2$ and $\rho([k])$ is rotation by $2\pi k/n$, with matrix $\begin{pmatrix} \cos(2\pi k/n) & -\sin(2\pi k/n) \\ \sin(2\pi k/n) & \cos(2\pi k/n) \end{pmatrix}$. Composing rotations adds angles, so $\rho([k])\rho([l]) = \rho([k+l])$; and rotating by $2\pi n/n = 2\pi$ is the identity, so the recipe does not depend on the representative k . For $n \geq 3$ this representation has no invariant line. A line invariant under $\rho([1])$ would give that matrix a real eigenvalue (Proposition 9.1.2), but with $c = \cos(2\pi/n)$ and $s = \sin(2\pi/n)$ its characteristic polynomial is $x^2 - 2cx + 1$, of discriminant $4c^2 - 4 = -4s^2$, which is negative because $0 < 2\pi/n < \pi$ forces $s \neq 0$ when $n \geq 3$. (The quarter-turn case is Example (A Rotation Has No Invariant Lines).) Section 04 turned this into the standard warning about Schur’s lemma over $\mathbb{R}$.
- **The regular representation.** $V = F[G]$, the group algebra of Definition 23.1.5: the free vector space on the set G (Definition 15.2.3), with basis $\{\delta_g : g \in G\}$ and multiplication determined by $\delta_g\delta_h = \delta_{gh}$. Its dimension is $|G|$. Put $\rho_{\text{reg}}(g)\delta_h = \delta_{gh}$, extended linearly. Then $\rho_{\text{reg}}(g)\rho_{\text{reg}}(g')\delta_h = \delta_{gg'h} = \rho_{\text{reg}}(gg')\delta_h$, so ρ_{reg} is a homomorphism, and $\rho_{\text{reg}}(g)$ is invertible with inverse $\rho_{\text{reg}}(g^{-1})$. It is faithful: if $\rho_{\text{reg}}(g) = \text{id}$ then $\delta_g = \rho_{\text{reg}}(g)\delta_1 = \delta_1$, so $g = 1$ because the δ_h are distinct basis vectors. Its degree is $|G|$.

Nonexample by minimal change. Keep $V = F^2$ and $G = \mathbb{Z}/4\mathbb{Z}$, and try $\rho([k]) = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$

over $\mathbb{Q}$. Each matrix is invertible, and $\rho([k])\rho([l]) = \begin{pmatrix} 1 & k+l \\ 0 & 1 \end{pmatrix}$, so multiplicativity holds on representatives. But the recipe is not **well defined** on $\mathbb{Z}/4\mathbb{Z}$: the class $[0]$ is also $[4]$, and $\begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix} \neq \mathbf{I}_2$. The clause that fails is that ρ must be a function on G . Over $\mathbb{F}_2$ the same recipe on $\mathbb{Z}/2\mathbb{Z}$ is well defined, because $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \mathbf{I}_2$ there; we return to that example when Maschke’s theorem breaks.

Warning. A representation need not remember the group. The trivial representation of any group is a representation, and it forgets everything. Conversely, a noninjective ρ can still be useful: the sign representation of S_n has a huge kernel yet separates even from odd permutations. When a statement needs ρ to see all of G , it must say **faithful**; none of the theorems below does.

Quick check. Is $\rho: \mathbb{Z}/3\mathbb{Z} \rightarrow \text{GL}_1(\mathbb{R}) = \mathbb{R} \setminus \{0\}$, $\rho([k]) = (-1)^k$, a representation?

Solution. No: it is not well defined. We have $[0] = [3]$ in $\mathbb{Z}/3\mathbb{Z}$, but $(-1)^0 = 1$ while $(-1)^3 = -1$. Equivalently, a representation of degree 1 is a homomorphism $\mathbb{Z}/3\mathbb{Z} \rightarrow \mathbb{R} \setminus \{0\}$, and $\rho([1])^3 = \rho([0]) = 1$ forces $\rho([1]) = 1$, since 1 is the only real cube root of 1. So the only degree-1 real representation of $\mathbb{Z}/3\mathbb{Z}$ is the trivial one.

23.7.2 Subrepresentations, equivalence, and irreducibility

Having made operators, we ask the question this book always asks of a family of operators: can the space be broken into smaller pieces that the family preserves? Chapter 9 called such a piece an invariant subspace (Definition 9.1.1). Here the family is $\{\rho(g) : g \in G\}$.

Definition 23.7.2. Subrepresentation

Let ρ be a representation of G on V . A subspace $U \subseteq V$ is **G -invariant** if $\rho(g)u \in U$ for every $g \in G$ and every $u \in U$. In that case the restrictions $\rho(g)|_U$ define a representation $\rho|_U$ of G on U , the **subrepresentation** of ρ on U .

Two checks make this legitimate. First, $\rho(g)|_U$ really is an operator **on** U , by invariance. Second, it is invertible on U : applying invariance to g^{-1} gives $\rho(g)^{-1}U = \rho(g^{-1})U \subseteq U$, so $\rho(g)|_U$ has a two-sided inverse on U , namely $\rho(g^{-1})|_U$. Multiplicativity is inherited. The subspaces $\{0\}$ and V are always G -invariant; we call them the **trivial** invariant subspaces.

Definition 23.7.3. Equivalence of representations

Let ρ and ρ' be representations of G on V and V' , over the same field. A linear map $S: V \rightarrow V'$ **intertwines** ρ and ρ' if

$$S \rho(g) = \rho'(g) S \quad \text{for every } g \in G.$$

The representations are **equivalent**, written $\rho \cong \rho'$, if some intertwining S is an isomorphism; equivalently, if $\rho'(g) = S \rho(g) S^{-1}$ for all g .

Equivalence is what “the same representation written in another basis” means. Indeed, if $V = V' = F^n$ and S is an invertible matrix, then $\rho'(g) = S \rho(g) S^{-1}$ is simultaneous similarity of the whole family $\{\rho(g)\}$ by one matrix. It is an equivalence relation: id_V intertwines ρ with itself; if S intertwines ρ with ρ' and is invertible then S^{-1} intertwines ρ' with ρ , since $S \rho(g) = \rho'(g) S$ gives $\rho(g) S^{-1} = S^{-1} \rho'(g)$; and a composition of intertwining isomorphisms intertwines.

Definition 23.7.4. Irreducible representation

A representation ρ of G on V is **irreducible** if $V \neq \{0\}$ and the only G -invariant subspaces of V are $\{0\}$ and V . A representation with $V \neq \{0\}$ that is not irreducible is **reducible**.

Read the two clauses separately. The zero space is excluded by decree, exactly as 1 is excluded from the primes: keeping it would break every statement of the form “every representation is built from irreducible ones”. The second clause is the real content.

Examples and a nonexample.

- Every representation of degree 1 is irreducible: a one-dimensional space has no subspaces but $\{0\}$ and itself.
- The permutation representation of S_3 on F^3 is **reducible** for every F . The line $L = \text{span}(\mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3)$ is S_3 -invariant, since $\rho(\sigma)(\mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3) = \mathbf{e}_{\sigma(1)} + \mathbf{e}_{\sigma(2)} + \mathbf{e}_{\sigma(3)} = \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3$, the same three basis vectors in another order. And $L \neq \{0\}$, $L \neq F^3$.
- So is the **sum-zero** subspace $W = \{\mathbf{x} \in F^3 : x_1 + x_2 + x_3 = 0\}$, of dimension 2: permuting the coordinates of $\mathbf{x}$ does not change their sum. We will see below that over $\mathbb{C}$ the subrepresentation on W is irreducible; this is the **standard representation** of S_3 .
- **Nonexample by minimal change.** Replace S_3 by the subgroup $H = \{\text{id}, (1\ 2)\} \subseteq S_3$ and keep $V = F^3$. Then $\text{span}(\mathbf{e}_3)$ is H -invariant, though it is not S_3 -invariant. Invariance depends on the whole group, not on one element of it.

Finally, the operation that puts representations together. If ρ_1, ρ_2 are representations of G on V_1, V_2 , their **direct sum** is the representation $\rho_1 \oplus \rho_2$ on $V_1 \oplus V_2$ given by $(\rho_1 \oplus \rho_2)(g)(v_1, v_2) = (\rho_1(g)v_1, \rho_2(g)v_2)$. In a basis adapted to the decomposition its matrix is block diagonal, $\rho_1(g) \oplus \rho_2(g)$. Conversely, if $V = U \oplus W$ with both summands G -invariant, then the map $U \oplus W \rightarrow V$, $(u, w) \mapsto u + w$, is an isomorphism intertwining $\rho|_U \oplus \rho|_W$ with ρ , so $\rho \cong \rho|_U \oplus \rho|_W$. So “decomposing a representation” and “finding an invariant complement” are the same task.

23.7.3 Representations of G and representations of $F[G]$

Here is the bridge that puts Sections 01–06 to work. The group algebra $F[G]$ was built in Definition 23.1.5 precisely so that the next theorem is true.

Theorem 23.7.1. Representations of G are representations of $F[G]$

Let G be a finite group, F a field, and V a finite-dimensional vector space over F . The assignment

$$\rho \longmapsto \tilde{\rho}, \quad \tilde{\rho}\left(\sum_{g \in G} a_g \delta_g\right) := \sum_{g \in G} a_g \rho(g),$$

is a bijection from the set of representations $\rho: G \rightarrow \text{GL}(V)$ onto the set of algebra homomorphisms $F[G] \rightarrow \text{End}(V)$ (Definition 23.1.2) — that is, onto the ways of making V an $F[G]$ -space in the sense of Definition 23.3.2. Moreover a subspace $U \subseteq V$ is G -invariant for ρ if and only if $\tilde{\rho}(a)U \subseteq U$ for every $a \in F[G]$.

Idea. An element of $F[G]$ is a formal linear combination of group elements, so a linear map out of $F[G]$ is determined by, and may be prescribed freely on, the basis $\{\delta_g\}$. The only thing to check is that “multiplicative on the basis” upgrades to “multiplicative everywhere”, and that is bilinearity of both products. The inverse map recovers ρ by restricting to the basis; the one point needing care is why $\tilde{\rho}(\delta_g)$ is automatically **invertible**, which is where $\delta_g \delta_{g^{-1}} = \delta_1$ earns its keep.

Proof. Let $\rho: G \rightarrow \text{GL}(V)$ be a representation. The formula defines a linear map $\tilde{\rho}: F[G] \rightarrow \text{End}(V)$, because $\{\delta_g\}$ is a basis of $F[G]$ and a linear map may be prescribed on a basis (Theorem 2.1.6). It sends δ_1 to $\rho(1) = \text{id}_V$ (Theorem 0.10.3). For multiplicativity, take $a = \sum_g a_g \delta_g$ and $b = \sum_h b_h \delta_h$. Multiplication in $F[G]$ and composition in $\text{End}(V)$ are both bilinear, so

$$\begin{aligned} \tilde{\rho}(ab) &= \tilde{\rho}\left(\sum_{g,h} a_g b_h \delta_{gh}\right) = \sum_{g,h} a_g b_h \rho(gh) \\ &= \sum_{g,h} a_g b_h \rho(g)\rho(h) = \left(\sum_g a_g \rho(g)\right)\left(\sum_h b_h \rho(h)\right) = \tilde{\rho}(a)\tilde{\rho}(b), \end{aligned}$$

where the third equality is the homomorphism property of ρ . Hence $\tilde{\rho}$ is an algebra homomorphism.

Conversely, let $\varphi: F[G] \rightarrow \text{End}(V)$ be an algebra homomorphism, and set $\rho(g) := \varphi(\delta_g)$. Since δ_1 is the identity of $F[G]$ (Definition 23.1.5) and id_V is the identity of $\text{End}(V)$, the unital clause of Definition 23.1.2 gives $\varphi(\delta_1) = \text{id}_V$. Then $\rho(g)\rho(h) = \varphi(\delta_g \delta_h) = \varphi(\delta_{gh}) = \rho(gh)$. In particular $\rho(g)\rho(g^{-1}) = \varphi(\delta_1) = \text{id}_V$ and likewise in the other order, so each $\rho(g)$ is invertible and ρ maps into $\text{GL}(V)$. Thus ρ is a representation, and $\tilde{\rho} = \varphi$ because the two agree on the basis $\{\delta_g\}$ and both are linear. Since also $\tilde{\rho}(\delta_g) = \rho(g)$, the two constructions are mutually inverse, and the assignment is a bijection.

For the last sentence, suppose U is G -invariant. For $a = \sum_g a_g \delta_g$ and $u \in U$, each $\rho(g)u$ lies in U , and U is a subspace, so $\tilde{\rho}(a)u = \sum_g a_g \rho(g)u \in U$. Conversely, if $\tilde{\rho}(a)U \subseteq U$ for all a , take $a = \delta_g$. This proves the theorem. ■

So the two languages are interchangeable, and we use whichever is shorter. A G -invariant subspace is an $F[G]$ -invariant subspace; an irreducible representation of G on V is exactly a simple $F[G]$ -space in the sense of Definition 23.3.3; and a map intertwining two representations of G is exactly an $F[G]$ -map in the sense of Definition 23.4.1, since the condition $S\rho(g) = \rho'(g)S$ for all g extends by linearity to all of $F[G]$. In particular Schur's lemma (Theorem 23.4.1) applies verbatim to irreducible representations of groups, and we use it that way in Section 08.

Remark. Working with $F[G]$ rather than with G buys one thing that matters: the ability to **add** group elements. Every averaging argument below lives in $F[G]$, not in G . Chapter 10 §07 made the same move for a single operator, replacing T by the algebra $F[T]$ and the space by an $F[x]$ -module.

23.7.4 Maschke's theorem

We now know that a reducible representation has a proper nonzero invariant subspace U . To break V into pieces we need more: an invariant **complement**, a G -invariant W with $V = U \oplus W$. An ordinary complement always exists (Theorem 1.7.6), but it has no reason to be invariant.

The idea for repairing it is the one move this chapter uses over and over. Start with an object that is not invariant, and average its G -translates. The average is invariant because translating it permutes the terms of the sum. Averaging divides by $|G|$, and that is the whole hypothesis.

Lemma 23.7.2. When the group order is invertible

Let F be a field and m a positive integer. Then $m \cdot 1_F \neq 0$ in F if and only if $\text{char } F$ does not divide m .

Proof. If $\text{char } F = 0$, then $m \cdot 1_F \neq 0$ for every positive integer m (Definition 0.7.2), and 0 divides no positive integer, so both sides of the equivalence hold. Assume from now on that $p := \text{char } F > 0$, so p is the **smallest** positive integer with $p \cdot 1_F = 0$.

($\Rightarrow$) We prove the contrapositive: if $p \mid m$, then $m \cdot 1_F = 0$. Write $m = qp$ with $q \geq 1$. By Lemma 0.7.4, $m \cdot 1_F = (qp) \cdot 1_F = (q \cdot 1_F)(p \cdot 1_F) = (q \cdot 1_F) \cdot 0 = 0$.

($\Leftarrow$) Suppose, for a contradiction, that some positive integer m has $m \cdot 1_F = 0$ and $p \nmid m$. Choose such an m as small as possible. Now $m \neq p$, since $p \mid p$, and $m > p$, since p is the smallest positive integer killing 1_F . So $m - p$ is a positive integer, and by Lemma 0.7.4

$$(m - p) \cdot 1_F + p \cdot 1_F = m \cdot 1_F = 0,$$

whence $(m - p) \cdot 1_F = 0$. Also $p \nmid m - p$, for otherwise p would divide $(m - p) + p = m$. This contradicts the minimality of m . This proves the lemma. ■

Theorem 23.7.3. Maschke's Theorem

Let G be a **finite** group and F a field whose characteristic does **not** divide $|G|$. Let ρ be a representation of G on a finite-dimensional space V over F , and let $U \subseteq V$ be a G -invariant subspace. Then there is a G -invariant subspace $W \subseteq V$ with

$$V = U \oplus W.$$

Idea. Pick **any** projection P of V onto U ; its kernel is a complement, but the wrong one, because P need not commute with the $\rho(g)$. Repair it by averaging the conjugates $\rho(g)P\rho(g)^{-1}$ over $g \in G$. ① Each conjugate is again a projection onto U , because U is invariant. ② Their average P_0 is therefore again a projection onto U — here we divide by $|G|$. ③ Conjugating P_0 by $\rho(h)$ only permutes the terms of the sum, so P_0 commutes with every $\rho(h)$, and then its kernel is invariant.

Proof. Write $n = |G|$. By hypothesis and Lemma 23.7.2, $n \cdot 1_F \neq 0$, so the scalar $\frac{1}{n} := (n \cdot 1_F)^{-1}$ exists in F . By Theorem 1.7.6 there is a subspace W_0 with $V = U \oplus W_0$; let $P \in \mathcal{L}(V)$ be the projection onto U along W_0 (Theorem 4.5.1 (b)), so $\text{im } P = U$ and $Pu = u$ for all $u \in U$. Define

$$P_0 := \frac{1}{n} \sum_{g \in G} \rho(g) P \rho(g)^{-1} \in \mathcal{L}(V).$$

Step 1: $\text{im } P_0 \subseteq U$. Let $v \in V$ and $g \in G$. Then $P\rho(g)^{-1}v \in \text{im } P = U$, and U is G -invariant, so $\rho(g)P\rho(g)^{-1}v \in U$. A subspace is closed under sums and scalar multiples, so $P_0v \in U$.

Step 2: $P_0 u = u$ for $u \in U$. Let $u \in U$ and $g \in G$. Since U is G -invariant and $\rho(g)^{-1} = \rho(g^{-1})$, we have $\rho(g)^{-1}u \in U$, so $P\rho(g)^{-1}u = \rho(g)^{-1}u$ and hence $\rho(g)P\rho(g)^{-1}u = u$. Summing over the n elements of G gives $\sum_g \rho(g)P\rho(g)^{-1}u = (n \cdot 1_F)u$, and multiplying by $\frac{1}{n}$ gives $P_0 u = u$.

By Steps 1 and 2, $P_0 v \in U$ for every v , and P_0 fixes U pointwise; therefore $P_0^2 v = P_0(P_0 v) = P_0 v$, so P_0 is a projection (Definition 4.5.1) with $\text{im } P_0 = U$.

Step 3: P_0 commutes with every $\rho(h)$. Fix $h \in G$. Then

$$\rho(h)P_0\rho(h)^{-1} = \frac{1}{n} \sum_{g \in G} \rho(hg) P \rho(hg)^{-1},$$

using $\rho(h)\rho(g) = \rho(hg)$ and $\rho(g)^{-1}\rho(h)^{-1} = (\rho(h)\rho(g))^{-1} = \rho(hg)^{-1}$. The map $g \mapsto hg$ is a bijection $G \rightarrow G$, with inverse $g \mapsto h^{-1}g$ by Theorem 0.10.1, so as g runs over G so does hg , and the sum is unchanged: $\rho(h)P_0\rho(h)^{-1} = P_0$. Multiplying on the right by $\rho(h)$ gives $\rho(h)P_0 = P_0\rho(h)$.

Step 4: conclusion. Put $W := \ker P_0$. By Theorem 4.5.1 (a), $V = \text{im } P_0 \oplus \ker P_0 = U \oplus W$. And W is G -invariant: if $P_0 w = 0$ and $h \in G$, then by Step 3, $P_0 \rho(h)w = \rho(h)P_0 w = 0$, so $\rho(h)w \in W$. This proves the theorem. ■

Two hypotheses did real work, and it is worth naming where. **Finiteness** of G is what makes the sum $\sum_g$ a finite sum, hence an operator at all. The condition on the **characteristic** is what makes $\frac{1}{n}$ exist, and Step 2 is where it is spent: without the division, the computation in Step 2 gives $\sum_g \rho(g)P\rho(g)^{-1}u = (n \cdot 1_F)u$, which is 0 for every $u \in U$ when $\text{char } F$ divides n . The unnormalized sum then **annihilates** U instead of fixing it, and there is nothing to rescue. Both failures are real, not artifacts of the proof.

Example. Maschke fails when the characteristic divides the order

Let p be a prime, $F = \mathbb{F}_p$, $G = \mathbb{Z}/p\mathbb{Z}$, and $V = \mathbb{F}_p^2$. Define

$$\rho([k]) := \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \in \text{GL}_2(\mathbb{F}_p).$$

Show that ρ is a well-defined representation, that $U = \text{span}(\mathbf{e}_1)$ is G -invariant, and that U has **no** G -invariant complement.

Solution. Well defined. The entry k is read in $\mathbb{F}_p$, so the matrix depends only on k modulo p ; and $\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & l \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & k+l \\ 0 & 1 \end{pmatrix}$, so $\rho([k])\rho([l]) = \rho([k] + [l])$. Each matrix is invertible, with inverse $\rho([-k])$. So ρ is a representation of the additive group $\mathbb{Z}/p\mathbb{Z}$. Here $|G| = p = \text{char } \mathbb{F}_p$, so the characteristic **does** divide the order and the hypothesis of Theorem 23.7.3 fails.

The invariant line. $\rho([k])\mathbf{e}_1 = \mathbf{e}_1$ for every k , so $U = \text{span}(\mathbf{e}_1)$ is G -invariant, and $U \neq \{\mathbf{0}\}, V$.

No invariant complement. If $V = U \oplus W$, then $\dim W = 2 - 1 = 1$ by Theorem 1.7.3, so $W = \text{span}(\mathbf{v})$ for some $\mathbf{v} = (a, b) \neq \mathbf{0}$; and $b \neq 0$, since $b = 0$ would force $a \neq 0$ and $W = \text{span}(\mathbf{e}_1) = U$, which is not a complement of itself. Suppose W is G -invariant. Then $\rho([1])\mathbf{v} = (a + b, b)$ must be a scalar multiple $\lambda\mathbf{v} = (\lambda a, \lambda b)$. Comparing second coordinates

and dividing by $b \neq 0$ gives $\lambda = 1$; comparing first coordinates then gives $a + b = a$, so $b = 0$, a contradiction. Hence U has no G -invariant complement. In fact U is the **only** nontrivial invariant subspace, so V is neither irreducible nor a direct sum of irreducibles.

Warning. Do not drop finiteness either. Let $G = \mathbb{Z}$ (infinite) act on $\mathbb{Q}^2$ by $\rho(k) = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ — now well defined, since $\mathbb{Z}$ has no relations to respect. The computation just made, with $b \neq 0$ in $\mathbb{Q}$, again shows $\text{span}(\mathbf{e}_1)$ is invariant with no invariant complement, and here the characteristic is 0. Averaging over $\mathbb{Z}$ is not an option: the sum has infinitely many terms.

Once one invariant complement can always be found, the full decomposition follows by induction.

Corollary 23.7.4. Complete Reducibility of Group Representations

Let G be a finite group and F a field with $\text{char } F \nmid |G|$ — for instance $F = \mathbb{C}$. Then every representation ρ of G on a nonzero finite-dimensional space V over F decomposes as

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_r$$

with each V_i a G -invariant subspace on which the subrepresentation is irreducible.

Proof. We argue by strong induction on $\dim V \geq 1$ (Theorem 0.2.10). If ρ is irreducible, take $r = 1$ and $V_1 = V$. Otherwise V has a G -invariant subspace U with $U \neq \{0\}$ and $U \neq V$. By Theorem 23.7.3 there is a G -invariant W with $V = U \oplus W$, and $W \neq \{0\}$ since $U \neq V$. Both $\dim U$ and $\dim W$ are at least 1, and since $U \cap W = \{0\}$ (Theorem 1.7.4) the dimension formula Theorem 1.7.3 gives $\dim U + \dim W = \dim V$; hence both are smaller than $\dim V$. The induction hypothesis decomposes U and W into irreducible invariant subspaces, and concatenating the two lists decomposes V , because a subspace of U invariant under $\rho|_U$ is invariant under ρ . This proves the corollary. ■

In the language of Section 03, the corollary says that $F[G]$ acts semisimply on every representation (Definition 23.3.4, Theorem 23.3.3); applied to the regular representation, it says $F[G]$ is a semisimple algebra. Section 06's structure theorem then applies to $\mathbb{C}[G]$, and Section 08 cashes that in.

Quick check. Where exactly does the proof of Corollary 23.7.4 use that $V \neq \{0\}$?

Solution. In the base of the induction and in the meaning of the conclusion. If $V = \{0\}$ it is not irreducible (Definition 23.7.4 excludes the zero space) and it has no nonzero invariant subspace to split off, so neither branch of the argument applies. The usual convention is that $\{0\}$ is the empty direct sum, $r = 0$; the corollary is stated with $V \neq \{0\}$ so that $r \geq 1$.

23.7.5 Two families worked out

We close with the two examples Section 08 will compute characters for. Both are over $\mathbb{C}$, where [Corollary 23.7.4](#) applies to every finite group.

Example. The irreducible complex representations of a cyclic group

Let $G = \mathbb{Z}/n\mathbb{Z}$ and $F = \mathbb{C}$. Determine all irreducible representations of G up to equivalence.

Solution. Every irreducible is one-dimensional. Let ρ be a representation of G on $V \neq \{0\}$ over $\mathbb{C}$, and set $A = \rho([1])$. By Theorem 9.2.4, A has an eigenvector $v \neq 0$, say $Av = \lambda v$. The line $L = \text{span}(v)$ is invariant under A , hence under every power $A^k = \rho([k])$, so L is G -invariant. If ρ is irreducible then $L = V$, so $\dim V = 1$. (For abelian G the algebra $\mathbb{C}[G]$ is commutative, since $\delta_g \delta_h = \delta_{gh} = \delta_{hg} = \delta_h \delta_g$ and multiplication is bilinear; so this is also [Corollary 23.4.4](#) read through [Theorem 23.7.1](#).)

Listing them. A one-dimensional representation is a homomorphism $\chi: \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{C} \setminus \{0\}$, determined by $z = \chi([1])$, which must satisfy $z^n = \chi([n]) = \chi([0]) = 1$. So z is an n -th root of unity, $z = \omega^k$ with $\omega = e^{2\pi i/n}$ and $0 \leq k \leq n-1$ (Example (Roots of Unity)). Conversely each such z does define a homomorphism $\chi_k([j]) = \omega^{jk}$: the recipe respects representatives because $\omega^n = 1$, and $\omega^{(j+l)k} = \omega^{jk} \omega^{lk}$.

They are pairwise inequivalent. Two one-dimensional representations are equivalent exactly when they are equal, since on a one-dimensional space every operator is λid for a scalar λ , and $S(\lambda \text{id})S^{-1} = \lambda \text{id}$ for every isomorphism S . And $\chi_k \neq \chi_l$ for $0 \leq k < l \leq n-1$, because $\chi_k([1]) = \omega^k \neq \omega^l = \chi_l([1])$, the n -th roots of unity being distinct.

So $\mathbb{Z}/n\mathbb{Z}$ has exactly n irreducible complex representations, all of degree 1, namely $\chi_0, \dots, \chi_{n-1}$. Their degrees satisfy $\sum_k 1^2 = n = |G|$, the count [Corollary 23.6.2](#) gives for the semisimple algebra $\mathbb{C}[G]$.

Example. The irreducible complex representations of the symmetric group on three letters

Write down three pairwise inequivalent irreducible complex representations of S_3 , with explicit matrices for the two-dimensional one.

Solution. Trivial and sign. $\rho_{\text{triv}}(\sigma) = 1$ and $\rho_{\text{sgn}}(\sigma) = \text{sgn}(\sigma)$, both on $\mathbb{C}$, both irreducible because their degree is 1. They are inequivalent: $\rho_{\text{triv}}((1\ 2)) = 1 \neq -1 = \rho_{\text{sgn}}((1\ 2))$.

The standard representation. Take the permutation representation on $\mathbb{C}^3$ and restrict it to the invariant plane $W = \{\mathbf{x} : x_1 + x_2 + x_3 = 0\}$. A basis of W is $\mathcal{B} = (\mathbf{f}_1, \mathbf{f}_2)$ with $\mathbf{f}_1 = \mathbf{e}_1 - \mathbf{e}_2$ and $\mathbf{f}_2 = \mathbf{e}_2 - \mathbf{e}_3$: they lie in W , they are independent, and $\dim W = 2$ because W is the kernel of the surjective functional $\mathbf{x} \mapsto x_1 + x_2 + x_3$ on $\mathbb{C}^3$ ([Theorem 2.3.1](#)). Since S_3 is generated by $(1\ 2)$ and $(1\ 2\ 3)$ — every element of S_3 is a product of transpositions ([Theorem 0.10.4](#)), and $(1\ 3) = (1\ 2\ 3)(1\ 2)$, $(2\ 3) = (1\ 2)(1\ 2\ 3)$ — it is enough to record two matrices. With

$$\rho(\sigma)\mathbf{e}_i = \mathbf{e}_{\sigma(i)}:$$

$$\rho((1\ 2))\mathbf{f}_1 = \mathbf{e}_2 - \mathbf{e}_1 = -\mathbf{f}_1,$$

$$\rho((1\ 2))\mathbf{f}_2 = \mathbf{e}_1 - \mathbf{e}_3 = \mathbf{f}_1 + \mathbf{f}_2,$$

$$\rho((1\ 2\ 3))\mathbf{f}_1 = \mathbf{e}_2 - \mathbf{e}_3 = \mathbf{f}_2,$$

$$\rho((1\ 2\ 3))\mathbf{f}_2 = \mathbf{e}_3 - \mathbf{e}_1 = -\mathbf{f}_1 - \mathbf{f}_2.$$

Writing $R_\sigma := \rho(\sigma)|_W$, the two matrices in the basis $\mathcal{B}$ are

$$[R_{(1\ 2)}]_{\mathcal{B}}^{\mathcal{B}} = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \quad [R_{(1\ 2\ 3)}]_{\mathcal{B}}^{\mathcal{B}} = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

The remaining four matrices follow by multiplying: $\mathbf{I}_2$ for id, $\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$ for $(1\ 3)$, $\begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}$ for $(2\ 3)$, and $\begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$ for $(1\ 3\ 2)$.

Irreducibility. A proper nonzero invariant subspace of the plane W would be a line $\text{span}(\mathbf{v})$, and $\mathbf{v}$ would be an eigenvector of **both** displayed matrices. The first has eigenvalues -1 and 1 , with eigenvectors spanned by $(1, 0)$ and $(1, 2)$ respectively. The second has characteristic polynomial $x^2 + x + 1$, whose roots are the two primitive cube roots of unity; neither $(1, 0)$ nor $(1, 2)$ is an eigenvector of it, since $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}(1, 0) = (0, 1)$ and $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}(1, 2) = (-2, -1)$ are not multiples of $(1, 0)$, $(1, 2)$. So there is no common eigenvector, and the standard representation is irreducible.

Inequivalent. It has degree 2, the others degree 1, and equivalent representations act on spaces of the same dimension.

The degrees satisfy $1^2 + 1^2 + 2^2 = 6 = |S_3|$, which is the count Corollary 23.6.2 gives for the semisimple algebra $\mathbb{C}[S_3]$. That count runs over **all** isomorphism classes of irreducible $\mathbb{C}[S_3]$ -spaces (Theorem 23.6.1), and a further class would add at least 1 to a total already equal to 6; so these three are all of the irreducible complex representations of S_3 . Section 08 reaches the same conclusion by counting conjugacy classes, which does not require the list to be found first.

23.7.6 Exercises

23.7.6.1 A. Check your understanding

Exercise. A1

- State the definition of a representation of a group G on a vector space V , and say which two properties of ρ come for free.
- State Maschke's theorem with all of its hypotheses.
- Determine whether the following is true: "every representation of degree 1 is irreducible." Justify your answer.
- Give an example of a reducible representation of S_3 over $\mathbb{C}$, and name an invariant subspace.
- Explain why $\rho: \mathbb{Z}/2\mathbb{Z} \rightarrow \text{GL}_1(\mathbb{Q})$, $\rho([k]) = 2^k$, is **not** a representation.

Solution.

- (a) A representation is a group homomorphism $\rho: G \rightarrow \text{GL}(V)$ with V finite-dimensional over F , that is, $\rho(gh) = \rho(g)\rho(h)$ for all $g, h \in G$ with each $\rho(g)$ invertible (Definition 23.7.1). Free: $\rho(1) = \text{id}_V$ and $\rho(g^{-1}) = \rho(g)^{-1}$, by Theorem 0.10.3.
- (b) If G is finite, F is a field with $\text{char } F \nmid |G|$, V is finite-dimensional over F , and $U \subseteq V$ is G -invariant, then U has a G -invariant complement W , so $V = U \oplus W$ (Theorem 23.7.3).
- (c) True. If $\dim V = 1$ then $V \neq \{0\}$ and the only subspaces of V are $\{0\}$ and V , so in particular the only invariant ones are the trivial ones.
- (d) The permutation representation of S_3 on $\mathbb{C}^3$; the line $\text{span}(\mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3)$ is invariant, as is the sum-zero plane.
- (e) It is not well defined: $[0] = [2]$ in $\mathbb{Z}/2\mathbb{Z}$, but $2^0 = 1 \neq 4 = 2^2$. (Equivalently, a degree-1 representation of $\mathbb{Z}/2\mathbb{Z}$ needs $\rho([1])^2 = 1$, and the only rational solutions of $z^2 = 1$ are $z = \pm 1$.)

23.7.6.2 B. Practice

Exercise. B1: Which of these are representations?

Determine which of the following are representations. Justify your answer in each case.

- (a) $G = \mathbb{Z}/6\mathbb{Z}$, $F = \mathbb{C}$, $\rho([k]) = \begin{pmatrix} \omega^k & 0 \\ 0 & \omega^{-k} \end{pmatrix}$ with $\omega = e^{\pi i/3}$.
- (b) $G = S_3$, $F = \mathbb{R}$, $\rho(\sigma) = \text{sgn}(\sigma) \mathbf{P}_\sigma$, where $\mathbf{P}_\sigma$ is the permutation matrix with $\mathbf{P}_\sigma \mathbf{e}_i = \mathbf{e}_{\sigma(i)}$ (Definition 3.4.2).
- (c) $G = S_3$, $F = \mathbb{R}$, $\rho(\sigma) = \mathbf{P}_\sigma^\top$ with $\mathbf{P}_\sigma$ as in (b).
- (d) $G = \mathbb{Z}/4\mathbb{Z}$, $F = \mathbb{R}$, $\rho([k]) = \begin{pmatrix} 1 & 0 \\ 0 & k+1 \end{pmatrix}$.

Solution.

- (a) Yes. Here $\omega^6 = e^{2\pi i} = 1$, so the matrix depends only on k modulo 6 and the map is well defined; it is diagonal, hence invertible since $\omega^{\pm k} \neq 0$; and $\rho([k])\rho([l]) = \text{diag}(\omega^{k+l}, \omega^{-k-l}) = \rho([k] + [l])$.
- (b) Yes. Both factors are multiplicative: $\text{sgn}(\sigma\tau) = \text{sgn}(\sigma)\text{sgn}(\tau)$ (Theorem 7.3.1) and $\mathbf{P}_\sigma \mathbf{P}_\tau = \mathbf{P}_{\sigma\tau}$ (Lemma 3.4.7 (a)). Scalars commute with matrices, so $\rho(\sigma)\rho(\tau) = \text{sgn}(\sigma\tau)\mathbf{P}_{\sigma\tau} = \rho(\sigma\tau)$, and $\rho(\sigma)$ is invertible because $\mathbf{P}_\sigma$ is and $\text{sgn}(\sigma) \neq 0$.
- (c) No. Taking transposes reverses products: $\rho(\sigma)\rho(\tau) = \mathbf{P}_\sigma^\top \mathbf{P}_\tau^\top = (\mathbf{P}_\tau \mathbf{P}_\sigma)^\top = \mathbf{P}_{\tau\sigma}^\top = \rho(\tau\sigma)$. Since S_3 is not abelian this differs from $\rho(\sigma\tau)$: with $\sigma = (1\ 2)$, $\tau = (1\ 3)$ we get $\tau\sigma = (1\ 2\ 3) \neq (1\ 3\ 2) = \sigma\tau$ (Example (Computing with cycles)), and distinct permutations have distinct permutation matrices. (The repair is $\sigma \mapsto \mathbf{P}_{\sigma^{-1}}^\top$, or equivalently $\mathbf{P}_\sigma$ itself.)
- (d) No, on two counts. It is not well defined: $[0] = [4]$ but $\text{diag}(1, 1) \neq \text{diag}(1, 5)$. And it is not multiplicative even on representatives: $\rho([1])\rho([1]) = \text{diag}(1, 4)$ while $\rho([2]) = \text{diag}(1, 3)$.

Exercise. B2: Averaging an inner product

Let G be a finite group and ρ a representation of G on a complex space V carrying an inner product $\langle \cdot, \cdot \rangle$ (Definition 11.1.1). Define

$$\langle u, v \rangle_G := \frac{1}{|G|} \sum_{g \in G} \langle \rho(g)u, \rho(g)v \rangle.$$

Prove that $\langle \cdot, \cdot \rangle_G$ is an inner product on V and that every $\rho(g)$ is an isometry for it. Hence give a second proof of [Theorem 23.7.3](#) over $\mathbb{C}$.

Solution. (IP1). For fixed v , the map $u \mapsto \langle \rho(g)u, \rho(g)v \rangle$ is linear in u , being a composition of the linear map $\rho(g)$ with a slot that is linear by (IP1) for $\langle \cdot, \cdot \rangle$. A sum of linear maps times a scalar is linear.

(IP2). $\langle v, u \rangle_G = \frac{1}{|G|} \sum_g \langle \rho(g)v, \rho(g)u \rangle = \frac{1}{|G|} \sum_g \overline{\langle \rho(g)u, \rho(g)v \rangle} = \overline{\langle u, v \rangle_G}$, since conjugation is additive.

(IP3). For $v \neq 0$, each $\rho(g)v \neq 0$ because $\rho(g)$ is invertible, so each term $\langle \rho(g)v, \rho(g)v \rangle$ is > 0 , and $|G| > 0$ is a positive real. Hence $\langle v, v \rangle_G > 0$.

Isometry. For $h \in G$, $\langle \rho(h)u, \rho(h)v \rangle_G = \frac{1}{|G|} \sum_g \langle \rho(gh)u, \rho(gh)v \rangle = \langle u, v \rangle_G$, because $g \mapsto gh$ is a bijection of G (Theorem 0.10.1).

Second proof of Maschke over $\mathbb{C}$. Let U be G -invariant and let $W = U^\perp$ be its orthogonal complement for $\langle \cdot, \cdot \rangle_G$. Then $V = U \oplus W$ by Theorem 11.3.2. If $w \in W$, $u \in U$, and $h \in G$, then, writing $u = \rho(h)(\rho(h)^{-1}u)$ and using that $\rho(h)$ preserves $\langle \cdot, \cdot \rangle_G$,

$$\langle \rho(h)w, u \rangle_G = \langle \rho(h)w, \rho(h)\rho(h)^{-1}u \rangle_G = \langle w, \rho(h)^{-1}u \rangle_G = 0,$$

the last step because $\rho(h)^{-1}u = \rho(h^{-1})u \in U$ and $w \in U^\perp$. So $\rho(h)w \in W$, and W is G -invariant. Note that this route needs $F = \mathbb{R}$ or $\mathbb{C}$, where inner products live, whereas [Theorem 23.7.3](#) needs only a condition on the characteristic.

Exercise. B3: Decomposing a permutation representation

Number the coordinates of $\mathbb{C}^3$ as $0, 1, 2$, as in Chapter 12 §09, and let $G = \mathbb{Z}/3\mathbb{Z}$ act by $\rho([k]) = \mathbf{S}^k$, where $\mathbf{S}$ is the cyclic shift, $\mathbf{S}\mathbf{x} = (x_1, x_2, x_0)$. Check that ρ is a representation, decompose $\mathbb{C}^3$ into one-dimensional invariant subspaces, and identify each with one of the χ_k of [Example \(The irreducible complex representations of a cyclic group\)](#).

Solution. A representation. Shifting three times restores every entry, so $\mathbf{S}^3 = \mathbf{I}$, and therefore $\mathbf{S}^k$ depends only on k modulo 3: the recipe is well defined on $\mathbb{Z}/3\mathbb{Z}$. It is multiplicative because $\mathbf{S}^k \mathbf{S}^l = \mathbf{S}^{k+l}$, and each $\mathbf{S}^k$ is invertible with inverse $\mathbf{S}^{3-k}$.

Decomposition. Let $\omega = e^{2\pi i/3}$. By Theorem 12.9.2 the vectors $\mathbf{f}_j = \frac{1}{\sqrt{3}}(1, \omega^j, \omega^{2j})$, $j = 0, 1, 2$, satisfy $\mathbf{S}\mathbf{f}_j = \omega^j \mathbf{f}_j$. The three eigenvalues $1, \omega, \omega^2$ are distinct, so the $\mathbf{f}_j$ are independent (Theorem 9.2.2), and three independent vectors in $\mathbb{C}^3$ form a basis (Theorem 1.6.4). Hence

$$\mathbb{C}^3 = \text{span}(\mathbf{f}_0) \oplus \text{span}(\mathbf{f}_1) \oplus \text{span}(\mathbf{f}_2),$$

and each line is invariant under $\mathbf{S}$, hence under every $\rho([k]) = \mathbf{S}^k$.

Identification. On $\text{span}(\mathbf{f}_j)$ the element $[k]$ acts by the scalar ω^{jk} , which is exactly $\chi_j([k])$ in the notation of [Example \(The irreducible complex representations of a cyclic group\)](#). So the three summands realize χ_0, χ_1, χ_2 : every irreducible representation of $\mathbb{Z}/3\mathbb{Z}$ occurs exactly once.

23.7.6.3 C. Going deeper

Exercise. C1: One-dimensional representations and the commutator

Let G be a finite group and F a field.

- Prove that every representation of degree 1 satisfies $\rho(ghg^{-1}h^{-1}) = 1$ for all $g, h \in G$.
- Deduce that the only degree-1 complex representation of $G = S_3$ other than the trivial one is the sign representation. *Hint: write the 3-cycle $(1\ 2\ 3)$ in the form $ghg^{-1}h^{-1}$ with g and h transpositions.*

Solution.

- A degree-1 representation takes values in $F \setminus \{0\}$, which is abelian under multiplication. So $\rho(ghg^{-1}h^{-1}) = \rho(g)\rho(h)\rho(g)^{-1}\rho(h)^{-1} = \rho(g)\rho(g)^{-1}\rho(h)\rho(h)^{-1} = 1$, using Theorem 0.10.3 for the inverses.
- Let ρ have degree 1 over $\mathbb{C}$. Transpositions are self-inverse, so $(1\ 2)(1\ 3)(1\ 2)^{-1}(1\ 3)^{-1} = (1\ 2)(1\ 3)(1\ 2)(1\ 3)$. Applying this product to each point, rightmost factor first: $1 \mapsto 3 \mapsto 3 \mapsto 1 \mapsto 2$, $2 \mapsto 2 \mapsto 1 \mapsto 3 \mapsto 3$, and $3 \mapsto 1 \mapsto 2 \mapsto 2 \mapsto 1$. So the product is $(1\ 2\ 3)$. By (a), $\rho((1\ 2\ 3)) = 1$, and then $\rho((1\ 3\ 2)) = \rho((1\ 2\ 3))^2 = 1$. Let $c = \rho((1\ 2))$. Since $(1\ 2)^2 = \text{id}$, $c^2 = 1$, so $c = \pm 1$. Finally $(1\ 3) = (1\ 2\ 3)(1\ 2)$ and $(2\ 3) = (1\ 2)(1\ 2\ 3)$, so $\rho((1\ 3)) = \rho((2\ 3)) = c$ as well. Thus ρ is determined by c : for $c = 1$ it is trivial, and for $c = -1$ it agrees with sgn on every element. Both values do occur, so there are exactly two.

Exercise. C2: Maschke over a field of the right characteristic

Let $G = \mathbb{Z}/2\mathbb{Z}$ and $V = F^2$, with $\rho([1]) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

- For $F = \mathbb{Q}$, find two G -invariant lines whose direct sum is V .
- For $F = \mathbb{F}_2$, prove that V has exactly one nontrivial G -invariant subspace, and conclude that [Theorem 23.7.3](#) fails here. Which hypothesis is violated?
- For $F = \mathbb{F}_3$, decompose V into irreducible subrepresentations.

Solution.

- $\rho([1])$ swaps the coordinates, so $\mathbf{u} = (1, 1)$ and $\mathbf{w} = (1, -1)$ satisfy $\rho([1])\mathbf{u} = \mathbf{u}$ and $\rho([1])\mathbf{w} = -\mathbf{w}$. Both lines are invariant, since $\rho([0]) = \mathbf{I}_2$ as well. The two vectors are independent, because the matrix with columns $\mathbf{u}, \mathbf{w}$ has determinant $-2 \neq 0$ in $\mathbb{Q}$; hence $\text{span}(\mathbf{u}) \cap \text{span}(\mathbf{w}) = \{\mathbf{0}\}$ and the sum is direct (Theorem 1.7.4). Its dimension

is $2 = \dim V$, so $V = \text{span}(\mathbf{u}) \oplus \text{span}(\mathbf{w})$.

- (b) Over $\mathbb{F}_2$ we have $-1 = 1$, so $\mathbf{w} = \mathbf{u} = (1, 1)$ and the two lines coincide. A nontrivial invariant subspace is a line $\text{span}((a, b))$ with $(a, b) \neq (0, 0)$, and invariance requires $(b, a) = \lambda(a, b)$. Over $\mathbb{F}_2$ the only nonzero scalar is $\lambda = 1$, forcing $a = b$, so $(a, b) = (1, 1)$ and the only nontrivial invariant subspace is $\text{span}((1, 1))$. A complement of a line in the plane V is again a line, and the only invariant line is $\text{span}((1, 1))$ itself, which is not a complement of itself. So this invariant subspace has no invariant complement, and V is not a direct sum of irreducibles. The violated hypothesis is on the characteristic: $\text{char } \mathbb{F}_2 = 2 = |G|$.
- (c) Over $\mathbb{F}_3$, $-1 = 2 \neq 1$, so $\mathbf{u} = (1, 1)$ and $\mathbf{w} = (1, 2)$ are again independent, with $\rho([1])\mathbf{u} = \mathbf{u}$ and $\rho([1])\mathbf{w} = 2\mathbf{w} = -\mathbf{w}$. Hence $V = \text{span}(\mathbf{u}) \oplus \text{span}(\mathbf{w})$, each summand of dimension 1 and so irreducible. Here $\text{char } \mathbb{F}_3 = 3 \nmid 2 = |G|$, and [Theorem 23.7.3](#) applies.

Exercise. C3: The contragredient representation

Let G be a finite group and ρ a representation of G on V over F . For $g \in G$ define $\tau(g) := (\rho(g)^{-1})' \in \mathcal{L}(V^*)$, where T' denotes the dual map (Definition 5.4.1).

- (a) Prove that τ is a representation of G on V^* , the **contragredient** of ρ .
- (b) Prove that if $U \subseteq V$ is G -invariant for ρ , then its annihilator $U^0 \subseteq V^*$ (Definition 5.2.1) is G -invariant for τ .
- (c) Hence deduce that if τ is irreducible, so is ρ .

Solution.

- (a) Each $\rho(g)^{-1}$ is invertible, so $\tau(g)$ is invertible by Theorem 5.4.1 (d). For multiplicativity, put $S = \rho(h)^{-1}$ and $T = \rho(g)^{-1}$. By Theorem 5.4.1 (b),

$$\begin{aligned} \tau(g)\tau(h) &= T'S' = (ST)' = (\rho(h)^{-1}\rho(g)^{-1})' \\ &= ((\rho(g)\rho(h))^{-1})' = (\rho(gh)^{-1})' = \tau(gh), \end{aligned}$$

where the fourth equality is Theorem 0.10.1 (3) applied in $\text{GL}(V)$. So τ is a homomorphism into $\text{GL}(V^*)$.

- (b) Let $\varphi \in U^0$, $g \in G$, and $u \in U$. By Definition 5.4.1, $(\tau(g)\varphi)(u) = \varphi(\rho(g)^{-1}u)$. Since $\rho(g)^{-1} = \rho(g^{-1})$ and U is G -invariant, $\rho(g)^{-1}u \in U$, so the value is 0. Hence $\tau(g)\varphi$ annihilates U , that is, $\tau(g)\varphi \in U^0$.
- (c) Suppose τ is irreducible. Then $V^* \neq \{0\}$, so $V \neq \{0\}$ by Corollary 5.1.4. Let U be a G -invariant subspace of V with $U \neq \{0\}$ and $U \neq V$. By (b), U^0 is G -invariant, and by Theorem 5.2.2, $\dim U^0 = \dim V - \dim U$. From $0 < \dim U < \dim V$ we get $0 < \dim U^0 < \dim V = \dim V^*$, so U^0 is a nontrivial invariant subspace of V^* , contradicting irreducibility. Hence ρ has no such U , and ρ is irreducible.