More on characters

1 One dimensional representations

In this section, we give a systematic description of all one dimensional representations of a finite group G. Recall that a one dimensional representation of G is the same thing as a homomorphism $\lambda\colon G \to \mathbb{C}^*$, and is always irreducible.

Definition 1.1. Let G be a group, not necessarily finite. A *commutator* in G is an expression of the form

$$[x, y] = xyx^{-1}y^{-1}.$$

Example 1.2. (i) The group G is abelian $\iff$ $[x, y] = 1$ for all $x, y \in G$. More generally, $[x, y] = 1 \iff x$ and y commute, i.e. $xy = yx$. For example, $[x, x] = 1$ for all $x \in G$, and $[1, x] = 1$ as well. In particular, 1 is always a commutator.
(ii) The group D_n is generated by two elements ρ and τ with $\rho^n = 1$, $\tau^2 = 1$ (thus $\tau = \tau^{-1}$), and $\tau\rho\tau^{-1} = \tau\rho\tau = \rho^{-1}$. Thus

$$[\tau, \rho] = \tau\rho\tau^{-1}\rho^{-1} = \rho^{-2}.$$

We have the following properties of commutators:

Lemma 1.3. *For all $x, y, g \in G$,*

(i) $[x, y]^{-1} = [y, x]$.

(ii) $g[x, y]g^{-1} = [gxg^{-1}, gyg^{-1}]$.

Proof. These follow from:

$$[x, y]^{-1} = (xyx^{-1}y^{-1})^{-1} = (y^{-1})^{-1}(x^{-1})^{-1}y^{-1}x^{-1} = yxy^{-1}x^{-1} = [y, x].$$
$$\begin{aligned} g[x, y]g^{-1} &= gxyx^{-1}y^{-1}g^{-1} = gxg^{-1}gyg^{-1}gx^{-1}g^{-1}gy^{-1}g^{-1} \\ &= [gxg^{-1}, gyg^{-1}], \end{aligned}$$

since $(gxg^{-1})^{-1} = gx^{-1}g^{-1}$ and similarly for y. □

Thus, the set of commutators is closed under taking inverses and conjugation (but **not** in general under products). The following is a straightforward generalization of (ii) in Lemma 1.3, whose proof is left as an exercise:

Lemma 1.4. *If $f\colon G \to H$ is a homomorphism, then for all $x, y \in G$,*

$$f([x,y]) = [f(x), f(y)]. \quad \square$$

Here, the the lemma implies (ii) in Lemma 1.3 since $gxg^{-1} = i_g(x)$ is a homomorphism (in fact an isomorphism) from G to G.

Definition 1.5. The *commutator subgroup* or *derived subgroup* G' of G is the subgroup generated by all commutators.

Since $1 \in G'$ and the inverse of a commutator is a commutator, it is easy to see that G' is equal to the set of all products of commutators:

$$G' = \{[x_1, y_1] \cdots [x_k.y_k] : x_i, y_i \in G\}.$$

It is the smallest subgroup of G containing all commutators. Also, since the conjugate of a commutator is again a commutator, it is easy to see that G' is a **normal** subgroup of G, i.e. $G' \lhd G$.

Definition 1.6. We set $G^{\mathrm{ab}} = G/G'$. (Sometimes G^{ab} is called the *abelianization* of G.)

Proposition 1.7. *With G' and G^{ab} defined as above,*

(i) *G^{ab} is abelian.*

(ii) *If $f\colon G \to H$ is a homomorphism from G to a group H, then $\operatorname{Im} f$ is abelian $\iff$ $\operatorname{Ker} f$ contains G'.*

(iii) *Let H be an abelian group. There is a bijection between homomorphisms $f\colon G \to H$ and homomorphisms $\tilde{f}\colon G^{\mathrm{ab}} \to H$. In fact, if $\pi\colon G \to G^{\mathrm{ab}}$ is the quotient homomorphism and $\tilde{f}\colon G^{\mathrm{ab}}$ is a homomorphism, then $\tilde{f} \circ \pi\colon G \to H$ is a homomorphism from G to H and every homomorphism from G to H arises in this way for a unique $\tilde{f}$.*

Proof. (i) With $\pi\colon G \to G^{\mathrm{ab}}$ the natural quotient homomorphism as above (i.e. $\pi(x) = xG'$), $[\pi(x), \pi(y)] = \pi[x,y] = 1$ (where here $1 = G'$ is the identity coset in $G^{\mathrm{ab}} = G/G'$), since $[x,y] \in G'$. Since every element of G^{ab} is of the form $\pi(x)$ for some $x \in G$, this shows that every pair of elements in G^{ab} commutes, hence G^{ab} is abelian.

(ii) Let $f\colon G \to H$ be a homomorphism from G to a group H. Then $\operatorname{Im} f$ is abelian $\iff$ for all $x, y \in G$, $1 = [f(x), f(y)] = f([x, y]) \iff$ for all $x, y \in G$, $[x, y] \in \operatorname{Ker} f \iff G' \subseteq \operatorname{Ker} f$.

(iii) Let H be an abelian group. Clearly, if $\tilde{f}\colon G^{\mathrm{ab}}$ is a homomorphism, then $f = \tilde{f} \circ \pi\colon G \to H$ is a homomorphism from G to H and it is easy to see that f determines and is determined by $\tilde{f}$. Conversely, suppose that $f\colon G \to H$ is a homomorphism. Since H is abelian, $\operatorname{Im} f$ is abelian and hence, by (ii), $G' \subseteq \operatorname{Ker} f$. In particular, there is a well-defined homomorphism $\nu\colon G/G' = G^{\mathrm{ab}} \to G/\operatorname{Ker} f$, defined by

$$\nu(xG') = x \operatorname{Ker} f.$$

By the Fundamental Homomorphism Theorem, there is a homomorphism $\hat{f}\colon G/\operatorname{Ker} f \to \operatorname{Im} f \subseteq H$, such that $f(x) = \hat{f}(x \operatorname{Ker} f)$. Define $\tilde{f}\colon G^{\mathrm{ab}} \to H$ via: $\tilde{f} = \hat{f} \circ \nu$. In other words,

$$\tilde{f} \circ \pi(x) = \tilde{f}(xG') = \hat{f}(x \operatorname{Ker} f) = f(x).$$

This produces a $\tilde{f}\colon G^{\mathrm{ab}} \to H$ with the property that $f = \tilde{f} \circ \pi$. This gives the required bijection in (iii). □

Corollary 1.8. *Let G be a finite group. Then there is a bijection from the set of one dimensional representations of G up to isomorphism to the group $\widehat{G^{\mathrm{ab}}}$, the dual group to the abelian group G^{ab}. In particular, the number of one dimensional representations of G up to isomorphism is $\#(G^{\mathrm{ab}}) = \#(G)/\#(G')$, and hence divides $\#(G)$.*

Proof. By (iii) of Proposition 1.7, there is a bijection from the set of homomorphisms from G to $\mathbb{C}^*$ to the set of homomorphisms from G^{ab} to $\mathbb{C}^*$. By definition, this last set is the dual group $\widehat{G^{\mathrm{ab}}}$ of G^{ab}. As we have seen, the order of the dual group to a finite abelian group is the same as the order of the original group, and this proves the remaining statements of the corollary. □

The definition of G' as the subgroup generated by all commutators is a little hard to apply directly in practice. The following lemma gives a somewhat easier way to find G' and G^{ab}:

Lemma 1.9. *Let N be a normal subgroup of G such that N is generated by commutators and G/N is abelian. Then $N = G'$.*

Proof. Since N is generated by commutators, $N \subseteq G'$. Since G/N is abelian, the kernel of the surjective homomorphism $G \to G/N$ contains G', by (ii) of Proposition 1.7. But the kernel of the projection $G \to G/N$ is N. Thus $G' \subseteq N$. As $N \subseteq G'$, $N = G'$. □

Example 1.10. For $G = D_n$, let $N = \langle \rho^2 \rangle$, in the notation of Example 1.2.

Case I: $n = 2k+1$ is odd. Then, as $\gcd(2,n) = 1$, ρ^2 is a generator of $\langle \rho \rangle$. Hence $N = \langle \rho^2 \rangle$ has order n, and thus index two in D_n, so is automatically normal. Moreover, D_n/N is a group of order 2, thus automatically abelian. So $N = G'$ and $G^{\mathrm{ab}} \cong \mathbb{Z}/2\mathbb{Z}$. Hence D_n has exactly 2 one dimensional representations in case n is odd.

Case II: $n = 2k$ is even. Then $N = \langle \rho^2 \rangle$ has order $n/2 = k$. Conjugating ρ^2 by the two generators of D_n, we see that

$$\begin{aligned} \rho \cdot \rho^2 \cdot \rho^{-1} &= \rho^2 \in \langle \rho^2 \rangle; \\ \tau \cdot \rho^2 \cdot \tau^{-1} &= \rho^{-2} \in \langle \rho^2 \rangle. \end{aligned}$$

Thus $N \lhd D_n$. The index of N in D_n is $2n/k = 4$, hence D_n/N is a group of order 4 and thus automatically abelian. In fact, D_n/N contains two different elements of order 2, since $(\tau N)^2 = \tau^2 N = N$, and $(\rho N)^2 = \rho^2 N = N$. Thus $G^{\mathrm{ab}} = D_n/N \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and D_n has exactly 4 one dimensional representations in case n is even.

It is a nice exercise to describe the homomorphisms $\lambda\colon D_n \to \mathbb{C}^*$ explicitly.

We have seen in a HW problem that every irreducible representation of D_n has dimension at most 2. If a is the number of 2-dimensional irreducible representations of D_n, then (by the usual formula that $\sum_{i=1}^h d_i^2 = \#(G)$),

$$2n = \#(D_n) = \begin{cases} 2 + 4a, & \text{if } n = 2k+1 \text{ is odd;} \\ 4 + 4a, & \text{if } n = 2k \text{ is even.} \end{cases}$$

Solving for a, we see that the number a of 2-dimensional irreducible representations of D_n is given by

$$a = \begin{cases} k, & \text{if } n = 2k+1 \text{ is odd;} \\ k-1, & \text{if } n = 2k \text{ is even.} \end{cases}$$

Of course, we know of one such 2-dimensional representation ρ_V, and considering representation $\rho_V \otimes \lambda$, where $\lambda\colon D_n \to \mathbb{C}^*$ is a homomorphism, allows us to potentially construct 2 or 4 2-dimensional representations (potentially, because it is in fact possible that $\rho_V \otimes \lambda_1$ and $\rho_V \otimes \lambda_2$ are isomorphic, for $\lambda_1 \neq \lambda_2$). But we need a new method to find all of them, which we shall describe when we discuss induced representations.

2 Cartesian products

Our goal in this section is to describe all of the irreducible representations for a product $G_1 \times G_2$ of two finite groups. If V_1 is a representation of G_1, then it becomes a representation of $G_1 \times G_2$ via the surjective homomorphism $\pi_1 \colon G_1 \times G_2 \to G_1$. In other words, is we are given a homomorphism $\rho_{V_1} \colon G_1 \to \operatorname{Aut} V_1$, then we have the composed homomorphism

$$\rho_{V_1} \circ \pi_1 \colon G_1 \times G_2 \to \operatorname{Aut} V_1.$$

We sometimes denote $\rho_{V_1} \circ \pi_1$ by $\pi_1^*\rho_{V_1}$ and V_1, considered as a $G_1 \times G_2$-representation, by $\pi_1^*V_1$. Explicitly,

$$\pi_1^*\rho_{V_1}(g_1, g_2) = \rho_{V_1}(g_1).$$

Clearly, the character $\chi_{\pi_1^*V_1}$ is equal to $\chi_{V_1} \circ \pi_1$, i.e.

$$\chi_{\pi_1^*V_1}(g_1, g_2) = \chi_{V_1}(g_1).$$

Note that, as π_1 is surjective, if ρ_{V_1} is irreducible, then $\pi_1^*\rho_{V_1}$ is also irreducible. Similarly, if V_2 is a representation of V_2, we can form $\pi_2^*\rho_{V_2}$ or $\pi_2^*V_2$. Finally, we can take the tensor product $\pi_1^*V_1 \otimes \pi_2^*V_2$. This is sometimes called the *external tensor product* and is written as $V_1 \boxtimes V_2$ or $V_1 \widehat{\otimes} V_2$. (Note that the tensor product $V_1 \otimes V_2$ does not make sense as a representation, since V_1 and V_2 are representations of **different** groups.)

Theorem 2.1. *Let G_1 and G_2 be two finite groups.*

(i) *If V_1 is an irreducible representation of G_1 and V_2 is an irreducible representation of G_2, then $\pi_1^*V_1 \otimes \pi_2^*V_2$ is an irreducible representation of $G_1 \times G_2$. Moreover, the $G_1 \times G_2$-representation $\pi_1^*V_1 \otimes \pi_2^*V_2$ determines the representations V_1 and V_2.*

(ii) *Every irreducible representation of $G_1 \times G_2$ is of the form $\pi_1^*V_1 \otimes \pi_2^*V_2$, where V_1 is an irreducible representation of G_1 and V_2 is an irreducible representation of G_2.*

Proof. (i) To show that $\pi_1^*V_1 \otimes \pi_2^*V_2$ is irreducible, it suffices to show that $\langle \chi_{\pi_1^*V_1\otimes\pi_2^*V_2}, \chi_{\pi_1^*V_1\otimes\pi_2^*V_2}\rangle = 1$. By our results about tensor products and the remarks above, we know that

$$\chi_{\pi_1^*V_1\otimes\pi_2^*V_2}(g_1,g_2) = \chi_{\pi_1^*V_1}(g_1,g_2)\chi_{\pi_2^*V_2}(g_1,g_2) = \chi_{V_1}(g_1)\chi_{V_2}(g_2).$$

We compute $\langle \chi_{\pi_1^*V_1\otimes\pi_2^*V_2}, \chi_{\pi_1^*V_1\otimes\pi_2^*V_2}\rangle$, using $\#(G_1\times G_2) = \#(G_1)\#(G_2)$:

$$\begin{aligned}
\langle \chi_{\pi_1^*V_1\otimes\pi_2^*V_2}, \chi_{\pi_1^*V_1\otimes\pi_2^*V_2}\rangle &= \frac{1}{\#(G_1\times G_2)}\sum_{(g_1,g_2)\in G_1\times G_2} |\chi_{\pi_1^*V_1\otimes\pi_2^*V_2}(g_1,g_2)|^2 \\
&= \frac{1}{\#(G_1)\#(G_2)}\sum_{g_1\in G_1, g_2\in G_2} |\chi_{V_1}(g_1)\chi_{V_2}(g_2)|^2 \\
&= \frac{1}{\#(G_1)}\frac{1}{\#(G_2)}\sum_{g_1\in G_1, g_2\in G_2} |\chi_{V_1}(g_1)|^2|\chi_{V_2}(g_2)|^2 \\
&= \left(\frac{1}{\#(G_1)}\sum_{g_1\in G_1}|\chi_{V_1}(g_1)|^2\right)\left(\frac{1}{\#(G_2)}\sum_{g_2\in G_2}|\chi_{V_2}(g_2)|^2\right) \\
&= \langle \chi_{V_1}, \chi_{V_1}\rangle\langle \chi_{V_2}, \chi_{V_2}\rangle,
\end{aligned}$$

where in the last line the first inner product is of functions on G_1 and the second is of functions on G_2. Under the assumption that V_1 and V_2 are irreducible, $\langle \chi_{V_1}, \chi_{V_1}\rangle = \langle \chi_{V_2}, \chi_{V_2}\rangle = 1$, and so $\langle \chi_{\pi_1^*V_1\otimes\pi_2^*V_2}, \chi_{\pi_1^*V_1\otimes\pi_2^*V_2}\rangle = 1$ as well. Thus $\pi_1^*V_1 \otimes \pi_2^*V_2$ is irreducible.

Next, let us show that $\pi_1^*V_1 \otimes \pi_2^*V_2$ determines the representations V_1 and V_2, more precisely that $\pi_1^*V_1 \otimes \pi_2^*V_2 \cong \pi_1^*V_1' \otimes \pi_2^*V_2' \iff V_1 \cong V_1'$ and $V_2 \cong V_2'$ (assuming that V_i and V_i' are irreducible for simplicity). To do so, consider the restriction $\mathrm{Res}^{G_1\times G_2}_{G_1\times\{1\}}(\pi_1^*V_1 \otimes \pi_2^*V_2)$ to the subgroup $G_1\times\{1\} \cong G_1$. Viewed as a representation of G_1, the value of its character at an element g_1 is

$$\chi_{\pi_1^*V_1\otimes\pi_2^*V_2}(g_1,1) = \chi_{V_1}(g_1)\chi_{V_2}(1) = d_2\chi_{V_1}(g_1),$$

where $d_2 = \dim V_2$, in other words its character is $d_2\chi_{V_1}$. This says that

$$\mathrm{Res}^{G_1\times G_2}_{G_1\times\{1\}}(\pi_1^*V_1 \otimes \pi_2^*V_2) \cong V_1^{d_2},$$

so every irreducible summand is isomorphic to V_1. By the same argument, every irreducible summand is isomorphic to $(V_1')^{d_2'}$, where $d_2' = \dim V_2'$. By the uniqueness of the irreducible summands of a G-representation up to isomorphism, $V_1 \cong V_1'$. Applying the same argument to the restriction $\mathrm{Res}^{G_1\times G_2}_{\{1\}\times G_2}(\pi_1^*V_1 \otimes \pi_2^*V_2)$, we see that $V_2 \cong V_2'$ as well.

(ii) Enumerate the irreducible representations of G_1 up to isomorphism as $V_1^{(1)}, \ldots, V_{h_1}^{(1)}$, where $\dim V_i^{(1)} = d_i^{(1)}$, and similarly let the irreducible representations of G_2 up to isomorphism be denoted $V_1^{(2)}, \ldots, V_{h_2}^{(2)}$, with $\dim V_j^{(2)} = d_j^{(2)}$. Then we have seen that $\sum_{i=1}^{h_1}(d_i^{(1)})^2 = \#(G_1)$ and that $\sum_{j=1}^{h_2}(d_j^{(2)})^2 = \#(G_2)$.

By Part (i), for each i, $1 \leq i \leq h_1$, and for each j, $1 \leq j \leq h_2$, the representation $\pi_1^* V_i^{(1)} \otimes \pi_2^* V_j^{(2)}$ is an irreducible representation of dimension $d_i^{(1)} d_j^{(2)}$, and the representations $\pi_1^* V_i^{(1)} \otimes \pi_2^* V_j^{(2)}$ and $\pi_1^* V_k^{(1)} \otimes \pi_2^* V_\ell^{(2)}$ are isomorphic $\iff$ $i = k$ and $j = \ell$. Computing, we see that

$$\begin{aligned}
\sum_{\substack{1 \leq i \leq h_1 \\ 1 \leq j \leq h_2}} \dim(\pi_1^* V_i^{(1)} \otimes \pi_2^* V_j^{(2)})^2 &= \sum_{\substack{1 \leq i \leq h_1 \\ 1 \leq j \leq h_2}} (d_i^{(1)} d_j^{(2)})^2 \\
&= \sum_{\substack{1 \leq i \leq h_1 \\ 1 \leq j \leq h_2}} (d_i^{(1)})^2 (d_j^{(2)})^2 \\
&= \left(\sum_{1 \leq i \leq h_1} (d_i^{(1)})^2 \right) \left(\sum_{1 \leq j \leq h_2} (d_j^{(2)})^2 \right) \\
&= \#(G_1)\#(G_1) = \#(G_1 \times G_2).
\end{aligned}$$

On the other hand, the sums of the squares of **all** of the irreducible representations of $G_1 \times G_2$ add up to $\#(G_1 \times G_2)$. So if we have found a collection of irreducible representations of $G_1 \times G_2$, such that no two distinct ones are isomorphic, and such that the sum of the squares of their dimensions is $\#(G_1 \times G_2)$, then this collection must be exactly the set of irreducible representations of $\#(G_1 \times G_2)$ up to isomorphism. This is the statement of (ii). □

3 Theorems of Frobenius and Burnside

In this section, we state the theorems of Frobenius and Burnside. The following three sections will be devoted to the proofs.

Theorem 3.1 (Frobenius)**.** *Let G be a finite group, let V be an irreducible representation of G, and let $d = \dim V$. Then d divides G.*

We give some easy applications of the theorem. Most of these can be easily proved by Modern Algebra I methods as well.

Proposition 3.2. *Let G be a finite group of order p^2, where p is a prime number. Then G is abelian.*

Proof. If G is not abelian, then there exists an irreducible representation of G of dimension d greater than 1 and dividing p^2. Hence, as p is prime, either $d = p$ or $d = p^2$, and in any case $d^2 \geq p^2$. But then the sum $\sum_{i=1}^{h} d_i^2$ of the squares of the dimensions of all irreducible representations contains a summand $d^2 \geq p^2$ and a summand equal to 1 (coming from the trivial representation). Thus $\sum_{i=1}^{h} d_i^2 \geq p^2 + 1 > p^2 = \#(G)$. This contradicts $\sum_{i=1}^{h} d_i^2 = p^2$. □

Remark 3.3. To give a proof of the proposition that does not use representation theory, one first shows that, for a group G with $\#(G) = p^a$, $a \geq 1$, the center $Z(G) \neq \{1\}$. We want to show that, in case $a = 2$, $Z(G) = G$. Otherwise, necessarily $\#(Z(G)) = p$, and the quotient group $G/Z(G)$ has order p, hence is cyclic. But an easy argument shows that, if G is any group such that $G/Z(G)$ is cyclic, then G is abelian (and thus $Z(G) = G$).

Proposition 3.4. *Let G be a finite group of order pq, where p and q are prime numbers and $p < q$. Then G is abelian unless $q \equiv 1 \bmod p$. Moreover, in this last case, there exists a normal subgroup of G of order q.*

Proof. If V is an irreducible representation of G of dimension d, then d divides pq and hence $d \in \{1, p, q, pq\}$. If $d = q$ or $d = pq$, then $d^2 > pq = \#(G)$, contradicting $\sum_{i=1}^{h} d_i^2 = \#(G)$. Hence every irreducible representation of G has dimension 1 or p. Suppose that there are a irreducible representations of G (up to isomorphism) of dimension 1 and b irreducible representations of G (up to isomorphism) of dimension p. If G is not abelian, then $b > 0$. Then, from $\sum_{i=1}^{h} d_i^2 = pq$, we see that $a + bp^2 = pq$. Thus $p|a$, say $a = cp$. But also $a|\#(G) = pq$, by Corollary 1.8. Thus $a = p$ or $a = pq$. Since $b > 0$, $a < pq$ and hence $a = p$. Then

$$pq = p + bp^2 = p(1 + bp).$$

Hence $q = 1 + bp$, i.e. $q \equiv 1 \bmod p$. Moreover, in this case $\#(G/G') = p$, so that G' is a normal subgroup of G and $\#(G') = q$. □

Remark 3.5. This proposition can be proved via the Sylow theorem: the number of q-Sylow subgroups is $\equiv 1 \bmod q$ and divides pq. Since pq has no proper divisor greater than q, there must be exactly one q-Sylow subgroup H, which is then automatically normal. Likewise, the number of p-Sylow subgroups is $\equiv 1 \bmod p$ and divides pq. If there is a p-Sylow subgroup which is not normal, then the number of p-Sylow subgroups is $\equiv 1 \bmod p$, is greater than 1, and divides pq. Hence this number is a proper divisor of pq, $\neq 1, p, pq$, hence equal to q. This says that $q \equiv 1 \bmod p$. Conversely, if $q \not\equiv 1 \bmod p$, there is exactly one p-Sylow subgroup H' and it is normal. An straightforward group theory argument then shows that $G \cong H \times H'$, and in particular G is abelian and $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$.

We turn next to the statement of Burnside's theorem. Although it contains no mention of representation theory, the proof will draw heavily on it, and in particular on the methods used to prove Frobenius' theorem.

Theorem 3.6 (Burnside)**.** *Let G be a finite group, with $\#(G) = p^a q^b$, where p and q are distinct primes and a and b are positive integers. Then G is not simple, i.e. there exists a normal subgroup $N \lhd G$ with $N \neq \{1\}$, $N \neq G$.*

Remark 3.7. (1) If $\#(G) = p^a$ with $a \geq 2$, then it is much easier to show that G is not simple. One argument uses the fact that the center $Z(G) \neq \{1\}$ (noted above in Remark 3.3). Another argument uses Frobenius' theorem.

(2) The case $a = b = 1$, i.e. $\#(G) = pq$, has been discussed in Proposition 3.4 and the following remark.

(3) It follows easily from Burnside's theorem and induction that every group of order $p^a q^b$ is *solvable*: There exists a sequence of subgroups

$$G_0 = \{1\} \subseteq G_1 \subseteq \cdots \subseteq G_n = G$$

such that, for every i, $1 \leq i \leq n$, $G_{i-1} \lhd G_i$ and G_i/G_{i-1} is abelian (one can even assume that G_i/G_{i-1} is cyclic of prime order).

(4) Burnside's theorem, proved in 1904, was the first major application of representation theory to the study of finite groups. The first purely group-theoretic proofs were given around 1970.

(5) By Burnside's theorem, if G is a finite simple group which is not cyclic of prime order, then $\#(G)$ is divisible by at least 3 primes. It is elementary to see that a group whose order is twice an odd number is not simple. Thus the smallest possible order of a noncyclic finite simple group is $2^2 \cdot 3 \cdot 5 = 60$, and in fact every simple group of order 60 is isomorphic to A_5.

(6) Feit and Thompson proved in 1963 that every noncyclic finite simple group has even order; this was conjectured by Burnside.

4 Algebraic integers

Before we can prove the theorems of Frobenius and Burnside, we need to make a digression to discuss algebraic integers. We start with some standard terminology:

Definition 4.1. Let k be a field. Then $k[x]$ is the set of all polynomials with coefficients in k. More generally, if R is a (commutative) ring, then $R[x]$ is the set of all polynomials with coefficients in R. We shall just be interested in $\mathbb{Z}[x] \subseteq \mathbb{Q}[x] \subseteq \mathbb{R}[x] \subseteq \mathbb{C}[x]$, the set of all polynomials with coefficients in (respectively) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. As usual, if $f(x) \in \mathbb{C}[x]$, then $f(x)$ can be viewed as a function from $\mathbb{C}$ to $\mathbb{C}$.

If $\alpha \in \mathbb{C}$, then α is *algebraic* or an *algebraic number* if there exists a polynomial $f(x) \in \mathbb{Q}[x]$, with $f(x)$ not the zero polynomial, such that $f(\alpha) = 0$, i.e. α is a root of some polynomial with rational coefficients. For example, $\sqrt{2}$ and i are algebraic but e and π are not (although it is not easy to prove this). We can always assume that, if α is algebraic, then there exists a nonzero polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$, by starting with a nonzero polynomial $f_0(x) \in \mathbb{Q}[x]$ and then replacing $f_0(x)$ by $Nf_0(x)$, where $N \in \mathbb{Z}$ is a multiple of all of the denominators of the nonzero coefficients of $f_0(x)$.

Finally, although we shall not need this, if α and β are algebraic, then so are $\alpha \pm \beta$, $\alpha \cdot \beta$, and α/β (if $\beta \neq 0$). This is a standard fact proved in Modern Algebra II.

We want an algebraic analogue of the integers, viewed as a subring of $\mathbb{Q}$. That is the point of the next definition:

Definition 4.2. Let $\alpha \in \mathbb{C}$. Then α is an *algebraic integer* if there exists a polynomial $f(x) \in \mathbb{Z}[x]$ with leading coefficient 1 (also called a *monic* polynomial) such that $f(\alpha) = 0$.

Since a polynomial with leading coefficient 1 is necessarily nonzero, an algebraic integer is in particular an algebraic number. But the converse does not hold. For example, $\sqrt{2}$ is an algebraic integer because it is a root of the monic polynomial $x^2 - 2$. Likewise i is a root of $x^2 + 1$ and hence is an algebraic integer. But, if $d \in \mathbb{Z}$ and $d > 1$, then it is not hard to show that $\sqrt{2}/d$ and i/d are not algebraic integers. For example, $\sqrt{2}/d$ is algebraic because it is a root of the polynomial $d^2x^2 - 2 \in \mathbb{Z}[x]$. But $d^2x^2 - 2$ is not monic, and a homework exercise shows that $\sqrt{2}/d$ is not a root of a monic polynomial with integer coefficients.

Clearly, if $n \in \mathbb{Z}$, then n is an algebraic integer because it is a root of the monic polynomial $x - n \in \mathbb{Z}[x]$. The following (a version of the rational roots test) shows that this is the only way that a rational number can be an algebraic integer:

Proposition 4.3. *Let $r \in \mathbb{Q}$. Then r is an algebraic integer $\iff r \in \mathbb{Z}$.*

Proof. We have just seen that $r \in \mathbb{Z} \implies r$ is an algebraic integer. Conversely, suppose that r is an algebraic integer. Write $r = s/t$, where $s, t \in \mathbb{Z}$ and $\gcd(s,t) = 1$. Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial such that $f(r) = 0$, say $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, where the $a_i \in \mathbb{Z}$. Then

$$0 = f(r) = f(s/t) = s^n/t^n + a_{n-1}s^{n-1}/t^{n-1} + \cdots + a_0.$$

Clearing denominators by multiplying by t^n, we have

$$s^n + a_{n-1}s^{n-1}t + \cdots + a_0t^n = 0,$$

and thus

$$-s^n = a_{n-1}s^{n-1}t + \cdots + a_0t^n = t(a_{n-1}s^{n-1} + \cdots + a_0t^{n-1}).$$

This says that t divides s^n. As $\gcd(s,t) = 1$, it follows that $\gcd(s^n, t) = 1$, so that $t = \pm 1$. Hence $r = s/t \in \mathbb{Z}$. □

We collect some other standard examples of algebraic integers:

Example 4.4. (1) If ζ is an n^{th} root of unity, then ζ is an algebraic integer, since it is a root of the monic polynomial $x^n - 1$.

(2) If A is an $n \times n$ matrix with integer coefficients, then the characteristic polynomial $p_A(t) = \det(t\,\mathrm{Id} - A)$ is a polynomial with integer coefficients and leading term t^n, hence it is monic. Thus, the eigenvalues of A are algebraic integers.

(3) Let K be a a subfield of $\mathbb{C}$, which is a finite extension of $\mathbb{Q}$, i.e. K is a finite-dimensional vector space over $\mathbb{Q}$. Then, as we shall see, the set

$$O_K = \{\alpha \in K : \alpha \text{ is an algebraic integer}\}$$

is a subring of K, i.e. it is closed under addition and multiplication.

(4) If $\alpha \in \mathbb{C}$ is an algebraic integer, then so is its complex conjugate $\bar{\alpha}$. In fact, if $f(x) \in \mathbb{Z}[x]$ is a monic polynomial such that $f(\alpha) = 0$, then

$$f(\bar{\alpha}) = \overline{f(\alpha)} = 0.$$

Thus $\bar{\alpha}$ is an algebraic integer.

(5) More generally, let $\alpha \in \mathbb{C}$ is an algebraic integer, and suppose that $\alpha \in K$, where K is a subfield of $\mathbb{C}$. Let $\sigma\colon K \to \mathbb{C}$ be a field homomorphism, i.e. σ preserves addition and multiplication, and by convention $\sigma(1) = 1$. Then $\sigma(n) = n$ for all $n \in \mathbb{Z}$. We claim that $\sigma(\alpha)$ is again an algebraic integer. In fact, it is easy to check that, if $f(x) \in \mathbb{Z}[x]$ is a monic polynomial such that $f(\alpha) = 0$, then

$$f(\sigma(\alpha)) = \sigma(f(\alpha)) = 0.$$

Thus $\sigma(\alpha)$ is an algebraic integer.

The following is the main technical criterion we shall need:

Proposition 4.5. *Let $\alpha \in \mathbb{C}$. Then α is an algebraic integer $\iff$ there exist $z_1, \dots, z_n \in \mathbb{C}$, not all 0, and $b_{ij} \in \mathbb{Z}$, $1 \le i \le n$, such that, for all i,*

$$\alpha z_i = \sum_{j=1}^{n} b_{ij} z_j.$$

Proof. $\implies$: Since α is an algebraic integer, there exist $a_{n-1}, \dots, a_0 \in \mathbb{Z}$ such that $\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_0 = 0$. Define $z_i = \alpha^{i-1}$, $1 \le i \le n$. Then $\alpha z_i = \alpha^i = z_{i+1}$ if $1 \le i \le n-1$, and

$$\begin{aligned} \alpha z_n = \alpha^n &= -a_0 - a_1\alpha - \dots - a_{n-1}\alpha^{n-1} \\ &= (-a_0)z_1 + \dots + (-a_{n-1})z_n. \end{aligned}$$

Thus we have found $z_i \in \mathbb{C}$ with the desired properties.

$\impliedby$: Write the condition that, for all i, $\alpha z_i = \sum_{j=1}^{n} b_{ij} z_j$ as

$$\sum_{j=1}^{n} (\alpha \delta_{ij} - b_{ij}) z_j = 0,$$

where as usual $\delta_{ij} = 1$ if $i = j$ and $\delta_{ij} = 0$ otherwise. This says that, if $B = (b_{ij})$, then

$$(z_1, \dots, z_n) \in \operatorname{Ker}(\alpha \operatorname{Id} - B).$$

Thus, the matrix $\alpha \operatorname{Id} - B$ has a nonzero kernel, so that $\det(\alpha \operatorname{Id} - B) = 0$. But then α is a root of the characteristic polynomial $p_B(t)$. As B has integer coefficients, α is an algebraic integer by (2) of Example 4.4. □

Corollary 4.6. *If α and β are algebraic integers, then so are $\alpha \pm \beta$ and $\alpha \cdot \beta$.*

Proof. Using the previous proposition choose $z_1, \dots, z_n \in \mathbb{C}$, not all 0, and $w_1, \dots, w_m \in \mathbb{C}$, not all 0, such that there exist integers b_{ij} and $c_{k\ell}$ with

$$\alpha z_i = \sum_{j=1}^{n} b_{ij} z_j, \qquad \beta w_k = \sum_{\ell=1}^{m} c_{k\ell} w_\ell.$$

Then

$$(\alpha \pm \beta)(z_i w_k) = \sum_j b_{ij} z_j w_k \pm \sum_\ell c_{k\ell} z_i w_\ell,$$

and

$$(\alpha\beta)(z_i w_k) = \left(\sum_j b_{ij} z_j\right)\left(\sum_\ell c_{k\ell} w_\ell\right) = \sum_{j,\ell} (b_{ij} c_{k\ell}) z_j w_\ell.$$

Since not all of the products $z_i w_k$ are 0, the conditions of Proposition 4.5 are met, hence $\alpha \pm \beta$ and $\alpha \cdot \beta$ are algebraic integers. □

5 Proof of Frobenius' theorem

We begin with the following easy application of the previous section:

Lemma 5.1. *If G is a finite group and ρ_V is a G-representation, then, for all $x \in G$, $\chi_V(x)$ is an algebraic integer.*

Proof. We know that, for all $x \in G$, $\rho_V(x)$ of diagonalizable, i.e. there exists a basis for V consisting of eigenvalues of $\rho_V(x)$. If the eigenvalues are $\lambda_1, \dots, \lambda_d$, then λ_i is a root of unity for every i, hence an algebraic integer by (1) of Example 4.4. Hence

$$\chi_V(x) = \operatorname{Tr} \rho_V(x) = \lambda_1 + \cdots + \lambda_d$$

is also an algebraic integer, by Corollary 4.6. □

There is a much deeper improvement of this result as follows:

Theorem 5.2. *Let V be an irreducible representation of G, of dimension d_V. For $x \in G$, let $c(x) = \#(C(x))$, where as usual $C(x)$ is the conjugacy class containing x. Then $\dfrac{c(x)}{d_V}\chi_V(x)$ is an algebraic integer.*

Proof. We begin by defining a subring R of the ring $L^2(G)$ of functions on G (with the operations of addition and convolution):

$$R = \{f \in L^2(G) : f \text{ is a class function and } f(x) \in \mathbb{Z} \text{ for all } x \in G\}.$$

Clearly the sum of two class functions is a class function, as is the convolution (as follows from our identification of the set of class functions with the center of $L^2(G)$). Similarly, if $f_1(g), f_2(g) \in \mathbb{Z}$ for all $g \in \mathbb{Z}$, then $(f_1 + f_2)(g) = f_1(g) + f_2(g) \in \mathbb{Z}$ and

$$(f_1 * f_2)(g) = \sum_{xy=g} f_1(x)f_2(y) \in \mathbb{Z}.$$

Thus R is closed under addition and convolution. Enumerate the distinct conjugacy classes of G as $C(x_1), \dots, C(x_h)$, and define (as usual) $f_{C(x_i)}$ to the characteristic function of $C(x_i)$ (i.e. $f_{C(x_i)}(x) = 1$ if $x \in C(x_i)$ and $f_{C(x_i)}(x) = 0$ otherwise). Then, given $f \in R$, since f is constant on each $C(x_i)$ and its value for every $x \in C(x_i)$ is an integer n_i, we can write f (uniquely) as

$$f = \sum_{i=1}^{h} n_i f_{C(x_i)}.$$

Note also that $1 = f_{C(x_1)} + \cdots + f_{C(x_h)}$.

Claim 5.3. *Let $\varphi\colon R \to \mathbb{C}$ be a ring homomorphism, i.e. for all $f_1, f_2 \in R$, $\varphi(f_1 + f_2) = \varphi(f_1) + \varphi(f_2)$, $\varphi(f_1 * f_2) = \varphi(f_1)\varphi(f_2)$, and $\varphi(1) = 1$. Then, for all $f \in R$, $\varphi(f)$ is an algebraic integer.*

Proof. We must show that that, with $\alpha = \varphi(f)$, there exist complex numbers z_i as in Proposition 4.5. Define $z_i = \varphi(f_{C(x_i)})$. The z_i are not all 0, because

$$1 = \varphi(1) = \varphi(f_{C(x_1)}+\cdots+f_{C(x_h)}) = \varphi(f_{C(x_1)})+\cdots+\varphi(f_{C(x_h)}) = z_1+\cdots+z_h.$$

Since R is closed under convolution, $f * f_{C(x_i)} \in R$, and hence there exist integers b_{ij} such that

$$f * f_{C(x_i)} = \sum_{j=1}^{h} b_{ij} f_{C(x_j)}.$$

Applying φ to this equality, we see that

$$\begin{aligned}\alpha \cdot z_i = \varphi(f * f_{C(x_i)}) &= \varphi(\sum_{j=1}^{h} b_{ij} f_{C(x_j)}) \\ &= \sum_{j=1}^{h} b_{ij}\varphi(f_{C(x_j)}) = \sum_{j=1}^{h} b_{ij}\varphi(f_{C(x_j)}) = \sum_{j=1}^{h} b_{ij} z_j.\end{aligned}$$

Thus α and the z_i satisfy the hypotheses of Proposition 4.5. Hence α is algebraic. □

Now recall that, given a representation ρ_V, we have defined a homomorphism, also denoted ρ_V, from $L^2(G)$ to $\operatorname{End} V$ via:

$$\rho_V(f) = \sum_{g\in G} f(g)\rho_V(g).$$

Moreover, if V is irreducible and f is a class function, then $\rho_V(f) = \lambda(f)\operatorname{Id}$, where

$$\lambda(f) = \frac{\#(G)}{d_V}\langle f, \overline{\chi_V}\rangle.$$

It is easy to check that, since ρ_V is a homomorphism, $\lambda\colon R \to \mathbb{C}$ is also a homomorphism. Thus, by Claim 5.3, for all $f \in R$, $\lambda(f)$ is an algebraic integer. Taking in particular $f = f_{C(x)}$ for some $x \in G$, we see that $\lambda(f_{C(x)})$ is an algebraic integer. But

$$\begin{aligned}\lambda(f_{C(x)}) &= \frac{\#(G)}{d_V}\langle f_{C(x)}, \overline{\chi_V}\rangle = \frac{\#(G)}{d_V}\cdot\frac{1}{\#(G)}\sum_{g\in G} f_{C(x)}(g)\overline{\chi_V}(g)\\ &= \frac{c(x)}{d_V}\overline{\chi_V}(x),\end{aligned}$$

since $f_{C(x)}(g) = 0$ if $g \notin C(x)$, $f_{C(x)}(g) = 1$ if $g \in C(x)$, and $\overline{\chi_V}(g) = \overline{\chi_V}(x)$ if $g \in C(x)$. Thus $\dfrac{c(x)}{d_V}\overline{\chi_V}(x)$ is an algebraic integer. Taking conjugates and using (4) of Example 4.4, it follows that $\dfrac{c(x)}{d_V}\chi_V(x)$ is an algebraic integer as well. □

We can now prove the theorem of Frobenius, which we restate here:

Theorem 5.4. *Let G be a finite group, let V be an irreducible representation of G, and let $d = d_V = \dim V$. Then d divides G.*

Proof. Since V is irreducible $\langle \chi_V, \chi_V\rangle = 1$, and hence

$$\sum_{x\in G}\chi_V(x)\overline{\chi_V}(x) = \#(G)\langle\chi_V,\chi_V\rangle = \#(G).$$

Enumerate the conjugacy classes of G as usual by $C(x_1), \dots, C(x_h)$, with $\#(C(x_i)) = c(x_i)$. Then G is the disjoint union of the $C(x_i)$. For all $x \in C(x_i)$, $\chi_V(x) = \chi_V(x_i)$. Thus

$$\#(G) = \sum_{x\in G}\chi_V(x)\overline{\chi_V}(x) = \sum_{i=1}^{h} c(x_i)\chi_V(x_i)\overline{\chi_V}(x_i).$$

Hence, after dividing by d_V, we can write

$$\frac{\#(G)}{d_V} = \sum_{i=1}^{h} \left(\frac{c(x_i)\chi_V(x_i)}{d_V} \right) \overline{\chi_V}(x_i).$$

By the previous theorem, $\dfrac{c(x_i)\chi_V(x_i)}{d_V}$ is an algebraic integer, and $\overline{\chi_V}(x_i)$ is an algebraic integer by Lemma 5.1. Thus, as sums of products of algebraic integers are algebraic integers by Corollary 4.6, $\#(G)/d_V$ is an algebraic integer. But $\#(G)/d_V$ is also a rational number, so it is an integer by Proposition 4.3. Hence d_V divides $\#(G)$. □

Remark 5.5. There are various strengthenings of this theorem. For example, Schur has proved that, if as above V is an irreducible representation of G of dimension d_V, then d_V divides $\#(G)/\#(Z(G))$, where $Z(G)$ is the center of G. If G is abelian, then $Z(G) = G$ and this says that d_V divides 1, hence is equal to 1 for every irreducible V. Of course, we have seen this directly. On the other hand, if G is a nonabelian simple group, or more generally if $Z(G) = \{1\}$, this result does not tell us anything more than Frobenius' theorem. Finally, once can replace the subgroup $Z(G)$ is the above statement by any abelian normal subgroup.

6 Proof of Burnside's theorem

We begin with a lemma about roots of unity:

Lemma 6.1. *Let $\lambda_1, \dots, \lambda_d$ be roots of unity.*

(i) $|\lambda_1 + \cdots + \lambda_d| \leq d$*, with equality* $\iff$ $\lambda_1 = \cdots = \lambda_d$.

(ii) *If* $\dfrac{\lambda_1}{d} + \cdots + \dfrac{\lambda_d}{d}$ *is an algebraic integer, then either* $\lambda_1 + \cdots + \lambda_d = 0$ *or* $\lambda_1 = \cdots = \lambda_d$.

Proof. (i) By the triangle inequality,

$$|\lambda_1 + \cdots + \lambda_d| \leq |\lambda_1| + \cdots + |\lambda_d| \leq d.$$

Moreover, equality holds in the triangle inequality $\iff$ there exist positive real numbers t_i such that $\lambda_i = t_i\lambda_1$ for all i (note that $\lambda_1 \neq 0$). But $|\lambda_1| = |\lambda_i| = 1$, so in this case

$$1 = |\lambda_i| = |t_i\lambda_1| = |t_i||\lambda_1| = t_i.$$

Thus there exist positive real numbers t_i such that $\lambda_i = t_i\lambda_1$ for all $i \iff \lambda_i = \lambda_1$ for all i.

(ii) This part requires a little Galois theory. By Part (i), $|\lambda_1 + \cdots + \lambda_d| \leq d$. Thus, if we set $\alpha = \sum_{i=1}^{d} \frac{\lambda_i}{d}$, then $|\alpha| \leq 1$. Since the λ_i are all roots of unity, there is some extension $\mathbb{Q}(\mu_N)$ such that $\lambda_i \in \mathbb{Q}(\mu_N)$ for all i. Here

$$\mu_N = \{z \in \mathbb{C} : z^N = 1\}$$

is the set of N^{th} roots of unity. As $\mathbb{Q}(\mu_N)$ is the splitting field of the polynomial $x^N - 1$, it is a normal, hence Galois extension of $\mathbb{Q}$. If $\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})$, then since $\lambda_i \in \mathbb{Q}(\mu_N)$ is a root of unity, $\sigma(\lambda_i)$ is also a root of unity. It then follows from (i) that

$$|\sigma(\lambda_1) + \cdots + \sigma(\lambda_d)| \leq d,$$

hence that $|\sigma(\alpha)| = \left|\sum_{i=1}^{d} \frac{\sigma(\lambda_i)}{d}\right| \leq 1$. Define

$$\beta = \prod_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})} \sigma(\alpha).$$

Then β is in the fixed field of $\mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})$, i.e. $\tau(\beta) = \beta$ for all $\tau \in \mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})$. By standard Galois theory, $\beta \in \mathbb{Q}$. Moreover, by hypothesis α is an algebraic integer, thus so is $\sigma(\alpha)$ by (5) of Example 4.4, and finally so is $\beta = \prod_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})} \sigma(\alpha)$ by Corollary 4.6. Thus $\beta \in \mathbb{Z}$.

Now consider $|\beta|$:

$$|\beta| = \left|\prod_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})} \sigma(\alpha)\right| = \prod_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})} |\sigma(\alpha)| \leq 1,$$

since $|\sigma(\alpha)| \leq 1$ for every $\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})$. Thus β is an integer with $|\beta| \leq 1$, hence $\beta = 0$ or $|\beta| = 1$. If $\beta = 0$, then $\sigma(\alpha) = 0$ for some $\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})$. Hence $\alpha = 0$ and $\lambda_1 + \cdots + \lambda_d = 0$. Otherwise, $|\beta| = 1$. This is only possible if $|\sigma(\alpha)| = 1$ for every $\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})$. In particular, $|\alpha| = 1$ so that $|\lambda_1 + \cdots + \lambda_d| = d$. By (i), this implies that $\lambda_1 = \cdots = \lambda_d$. □

We now apply this to representations:

Corollary 6.2. *Let G be a finite group and V a G-representation, not necessarily irreducible, with* $\dim V = d_V$*.*

(i) *For all $g \in G$, $|\chi_V(g)| \leq d_V$, with equality* $\iff \rho_V(g) = \dfrac{\chi_V(g)}{d_V}\operatorname{Id}$.

(ii) $\chi_V(g) = d_V \iff \rho_V(g) = \operatorname{Id} \iff g \in \operatorname{Ker} \rho_V$.

Proof. (i) Let $d = d_V$. We know that $\rho_V(g)$ is diagonalizable with eigenvalues $\lambda_1, \dots, \lambda_d$ which are roots of unity, and that $\chi_V(g) = \lambda_1 + \cdots + \lambda_d$. Thus, by (i) of Lemma 6.1,

$$|\chi_V(g)| = |\lambda_1 + \cdots + \lambda_d| \leq d = d_V,$$

with equality $\iff \lambda_1 = \cdots = \lambda_d$. This last case holds $\iff \rho_V(g) = \lambda \operatorname{Id}$, where necessarily $d\lambda = \operatorname{Tr} \rho_V(g) = \chi_V(g)$, hence $\lambda = \chi_V(g)/d_V$.

(ii) By definition, $\rho_V(g) = \operatorname{Id} \iff g \in \operatorname{Ker} \rho_V$. If $\chi_V(g) = d_V$, then $|\chi_V(g)| = d_V$, so by (i) $\rho_V(g) = \dfrac{\chi_V(g)}{d_V}\operatorname{Id} = \operatorname{Id}$. Conversely, if $\rho_V(g) = \operatorname{Id}$, then clearly $\chi_V(g) = \dim V = d_V$. □

Corollary 6.3. *Let G be a finite group. Then G is not simple $\iff$ there exists an irreducible representation V, not the trivial representation, with character χ_V, and a $g \in G$, $g \neq 1$, such that $\chi_V(g) = \chi_V(1) = \dim V$.*

Proof. If G is not simple, let N be a proper normal subgroup of G such that $N \neq \{1\}$. In particular G/N is not the trivial group. Then there exists a nontrivial irreducible representation $\psi_V \colon G/N \to \operatorname{Aut} V$. If $\pi \colon G \to G/N$ is the natural homomorphism, then $\rho_V = \psi_V \circ \pi = \pi^*\psi_V$ is a representation of G. It is clearly nontrivial and it is irreducible by a HW problem. Since $N \neq \{1\}$, there exists a $g \in N$ with $g \neq 1$. For such a g, $\chi_V(g) = \chi_V(1) = \dim V$.

Conversely, suppose that there exists an irreducible representation V, not the trivial representation, with character χ_V, and a $g \in G$, $G \neq 1$, such that $\chi_V(g) = \chi_V(1) = \dim V$. By (ii) of Corollary 6.2, such a g is in $\operatorname{Ker} \rho_V$, and hence $\operatorname{Ker} \rho_V \neq \{1\}$. Since V is not the trivial representation, $\operatorname{Ker} \rho_V \neq G$. Then $\operatorname{Ker} \rho_V$ is a proper, nontrivial subgroup of G and it is normal as it is the kernel of a homomorphism. Hence G is not simple. □

The following is the main technical result we need:

Proposition 6.4. *Let G be a finite group and let V be an irreducible G-representation with character χ_V and dimension* $\dim V = d_V = d$*. Let $g \in G$ and as usual set $c(g) = \#(C(g))$. Suppose that* $\gcd(c(g), d) = 1$*. Then either $\chi_V(g) = 0$ or there exists a $\lambda \in \mathbb{C}^*$ such that* $\rho_V(g) = \lambda \operatorname{Id}$.

Corollary 6.5. *Let G be a finite, simple and nonabelian group, let V be a nontrivial irreducible G-representation with character χ_V and dimension $\dim V = d_V = d$, and let $g \in G$ with $g \neq 1$. If $\gcd(c(g), d) = 1$, then $\chi_V(g) = 0$.*

Proof of Corollary 6.5. Let G, V and g be as in the statement of the corollary. Since $\operatorname{Ker} \rho_V$ is normal and G is simple, either $\operatorname{Ker} \rho_V = G$ or $\operatorname{Ker} \rho_V = \{1\}$. The first case is impossible since V is not the trivial representation. Hence $\operatorname{Ker} \rho_V = \{1\}$, so that ρ_V is injective. Now assume that $\chi_V(g) \neq 0$. By Proposition 6.4, there exists a $\lambda \in \mathbb{C}^*$ such that $\rho_V(g) = \lambda \operatorname{Id}$. In particular, $\rho_V(g)$ commutes with every element of $\operatorname{Aut} V$, and hence with every element of the form $\rho_V(x)$, $x \in G$. In other words, for all $x \in G$, the commutator $[\rho_V(g), \rho_V(x)]$ is equal to Id. But as $[\rho_V(g), \rho_V(x)] = \rho_V([g, x])$, it follows that $\rho_V([g, x]) = \operatorname{Id}$ for every $x \in G$. As ρ_V is injective, $[g, x] = 1$ for every $x \in G$, so that $g \in Z(G)$. But $Z(G)$ is a normal subgroup of G, and since G is not abelian, $Z(G) \neq G$. Since G is simple, we must have $Z(G) = \{1\}$, hence $g = 1$. This contradicts the hypothesis that $g \neq 1$. □

Proof of Proposition 6.4. Since $\gcd(c(g), d) = 1$, there exist integers A and B such that $Ac(g) + Bd = 1$. Hence

$$\frac{\chi_V(g)}{d} = (Ac(g) + Bd)\frac{\chi_V(g)}{d} = A\frac{c(g)\chi_V(g)}{d} + B\chi_V(g).$$

By Theorem 5.2, $\dfrac{c(g)}{d}\chi_V(g)$ is an algebraic integer. By Lemma 5.1, $\chi_V(g)$ is an algebraic integer. Hence so is $\dfrac{\chi_V(g)}{d}$.

Now $\chi_V(g)$ is of the form $\lambda_1 + \cdots + \lambda_d$, where the λ_i are roots of unity. By Lemma 6.1(i), $\chi_V(g)/d$ is an algebraic integer $\iff$ $\lambda_1 + \cdots + \lambda_d = 0$, i.e. $\chi_V(g) = 0$, or $\lambda_1 = \cdots = \lambda_d$, i.e. $\rho_V(g) = \lambda \operatorname{Id}$ with say $\lambda = \lambda_1$. □

We can now prove the following result, which is a purely group-theoretic statement:

Theorem 6.6. *Let G be a finite, simple and nonabelian group, and let $g \in G$ with $g \neq 1$. Then $c(g) = \#(C(g))$ is not a prime power.*

Proof. Since G is simple and nonabelian, $Z(G) = \{1\}$. Hence, if $g \in G$ and $g \neq 1$, $c(g) = \#(C(g)) \geq 2$. Thus, if $c(g) = p^a$ is a prime power, then $a \geq 1$. Assuming that this is the case, we will derive a contradiction.

If V is any nontrivial G-representation, with character χ_V and dimension d_V, then $\gcd(c(g), d_V) = \gcd(p^a, d_V)$. Hence either $\gcd(c(g), d_V) = 1$ or p divides d_V. By Corollary 6.5, either $\chi_V(g) = 0$ or p divides d_V.

If χ_{reg} is the character of the regular representation, we know that $\chi_{\mathrm{reg}} = \sum_{i=1}^h d_{V_i}\chi_{V_i}$, where $V_1, \ldots, V_h$ are the irreducible representations of G up to isomorphism, and, say, V_1 is the trivial representation. Since $g \neq 1$, $\chi_{\mathrm{reg}}(g) = 0$. Thus

$$0 = \sum_{i=1}^h d_{V_i}\chi_{V_i}(g) = 1 + \sum_{i=2}^h d_{V_i}\chi_{V_i}(g).$$

Hence

$$-\frac{1}{p} = \sum_{i=2}^h \frac{d_{V_i}}{p}\chi_{V_i}(g).$$

We claim that the right hand side is an algebraic integer. In fact, since either $\chi_{V_i}(g) = 0$ or p divides d_{V_i}, every nonzero term in the right hand side is of the form integer times algebraic integer (because $\chi_{V_i}(g)$ is an algebraic integer). Thus $-1/p$ is a sum of algebraic integers, hence an algebraic integer, hence an integer since it is a rational number. This is the desired contradiction. □

We can now prove Burnside's theorem, which we restate:

Theorem 6.7. *Let G be a finite group, with $\#(G) = p^a q^b$, where p and q are distinct primes and a and b are positive integers. Then G is not simple.*

Proof. Suppose to the contrary that G is a simple group of order $p^a q^b$, where p and q are distinct primes and $a, b \geq 1$. Since the only simple abelian groups are cyclic of prime order, G is not abelian. Enumerate the distinct conjugacy classes of G as $C(x_1), \ldots, C(x_h)$, where say $x_1 = 1$. Since $Z(G) = \{1\}$, for all $x \neq 1$, $c(x) = \#(C(x)) > 1$ and $c(x)$ divides $\#(G) = p^a q^b$ since $C(x)$ is an orbit under the conjugation action of G on itself. Since $c(x) = p^r$ is impossible by Theorem 6.6, for all $x \neq 1$, we must have $c(x) = p^r q^s$ with $r, s \geq 1$. In particular, both p and q divide $c(x_i)$ for all $i > 1$. But G is the disjoint union of the $C(x_i)$, $1 \leq i \leq h$, and hence

$$p^a q^b = \sum_{i=1}^h c(x_i) = 1 + \sum_{i>1} c(x_i).$$

The left hand side is divisible by p, say, and all of the terms $c(x_i)$ for $i > 1$ are also divisible by p. This says that 1 is divisible by p, a contradiction. Thus G is not simple. □