17. Let p be any prime and let P be a non-abelian group of order p^3 (up to isomorphism there are two choices for P; for odd p these were constructed when the groups of order p^3 were classified in Section 5.5). This exercise determines the character table of P and shows that both isomorphism types have the same character table (the argument includes the $p = 2$ case worked out in this section).

(a) Prove that P has p^2 characters of degree 1.

(b) Prove that P has $p - 1$ irreducible characters of degree p and that these together with the p^2 degree 1 characters are all the irreducible characters of P. [Use Theorem 10(3) and Theorem 12 in Section 18.2.]

(c) Deduce that (regardless of the isomorphism type) the group P has p^2+p-1 conjugacy classes, p of which are of size 1 (i.e., are central classes) and $p^2 - 1$ of which each have size p. Deduce also that the classes of size p are precisely the nonidentity cosets of the center of P (i.e., if $x \in P - Z(P)$ then the conjugacy class of x is the set of p elements in the coset $xZ(P)$).

(d) Prove that if χ is an irreducible character of degree p then the representation affording χ is faithful.

(e) Fix a generator, z, of the center of P and let ϵ be a fixed primitive p^{th} root of 1 in $\mathbb{C}$. Prove that if χ is an irreducible character of degree p then $\chi(z) = p\epsilon^i$ for some $i \in \{1, 2, \ldots, p-1\}$. Prove further that $\chi(x) = 0$ for all $x \in P - Z(P)$. (Note then that the degree p characters are all algebraically conjugate.) [Use the same reasoning as in the construction of the character table of Q_8.]

(f) Prove that for each $i \in \{1, 2, \ldots, p-1\}$ there is a unique irreducible character χ_i of degree p such that $\chi_i(z) = p\epsilon^i$. Deduce that the character table of P is uniquely determined, and describe it. [Recall from Section 6.1 that regardless of the isomorphism type, $P' = Z(P)$ and $P/P' \cong Z_p \times Z_p$. From this one can write out the degree 1 characters. Part (e) describes the degree p characters.]

19.2 THEOREMS OF BURNSIDE AND HALL

In this section we give a "theoretical" application of character theory: Burnside's p^aq^b Theorem. We also prove Philip Hall's characterization of finite solvable groups, which is a group-theoretic proof relying on Burnside's Theorem as the first step in its induction.

Burnside's Theorem

The following result was proved by Burnside in 1904. Although purely group-theoretic proofs of it were discovered recently (see Theorem 2.8 in *Finite Groups III* by B. Huppert and N. Blackburn, Springer-Verlag, 1982) the original proof by Burnside presented here is very accessible, elegant, and quite brief (given our present knowledge of representation theory).

Theorem 1. (Burnside) For p and q primes, every group of order p^aq^b is solvable.

Before undertaking the proof of Burnside's Theorem itself we establish some results of a general nature. An easy consequence of these preliminary propositions is that the degrees of the irreducible characters of any finite group divide its order. The particular results that lead directly to the proof of Burnside's Theorem appear in Lemmas 6 and 7.

It follows quite easily that a counterexample to Burnside's Theorem of minimal order is a non-abelian simple group, and it is these two character-theoretic lemmas that give the contradiction by proving the existence of a normal subgroup.

We first recall from Section 15.3 the definition of algebraic integers.

Definition. An element $\alpha \in \mathbb{C}$ is called an *algebraic integer* if it is a root of a monic polynomial with coefficients from $\mathbb{Z}$.

The basic results needed for the proof of Burnside's Theorem are:

Proposition 2. Let $\alpha \in \mathbb{C}$.

(1) The following are equivalent:

- **(i)** α is an algebraic integer,
- **(ii)** α is algebraic over $\mathbb{Q}$ and the minimal polynomial of α over $\mathbb{Q}$ has integer coefficients, and
- **(iii)** $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module (where $\mathbb{Z}[\alpha]$ is the subring of $\mathbb{C}$ generated by $\mathbb{Z}$ and α, i.e., is the ring of all $\mathbb{Z}$-linear combinations of nonnegative powers of α).

(2) The algebraic integers in $\mathbb{C}$ form a ring and the algebraic integers in $\mathbb{Q}$ are the elements of $\mathbb{Z}$.

Proof: These are established in Section 15.3. (The portion of Section 15.3 consisting of integral extensions and properties of algebraic integers may be read independently from the rest of Chapter 15.)

Corollary 3. For every character ψ of the finite group G, $\psi(x)$ is an algebraic integer for all $x \in G$.

Proof: By Proposition 14 in Section 18.3, $\psi(x)$ is a sum of roots of 1. Each root of 1 is an algebraic integer, so the result follows immediately from Proposition 2(2).

We shall also need some preliminary character-theoretic lemmas before beginning the main proof. Adopt the following notation for the arbitrary finite group G: $\chi_1, \ldots, \chi_r$ are the distinct irreducible (complex) characters of G, $\mathcal{K}_1, \ldots, \mathcal{K}_r$ are the conjugacy classes of G and φ_i is an irreducible matrix representation whose character is χ_i for each i.

Proposition 4. Define the complex valued function ω_i on $\{\mathcal{K}_1, \ldots, \mathcal{K}_r\}$ for each i by

$$\omega_i(\mathcal{K}_j) = \frac{|\mathcal{K}_j|\chi_i(g)}{\chi_i(1)}$$

where g is any element of $\mathcal{K}_j$. Then $\omega_i(\mathcal{K}_j)$ is an algebraic integer for all i and j.

Proof: We first prove that if I is the identity matrix, then

$$\sum_{g \in \mathcal{K}_j} \varphi_i(g) = \omega_i(\mathcal{K}_j) I. \tag{19.1}$$

To see this let X be the left hand side of (1). As we saw in Section 18.2, each $x \in G$ acting by conjugation permutes the elements of $\mathcal{K}_j$ and so X commutes with $\varphi_i(g)$ for all g. By Schur's Lemma (Exercise 18 in Section 18.1) X is a scalar matrix:

$$X = \alpha I \qquad \text{for some } \alpha \in \mathbb{C}.$$

It remains to show that $\alpha = \omega_i(\mathcal{K}_j)$. But

$$\operatorname{tr} X = \sum_{g \in \mathcal{K}_j} \operatorname{tr} \varphi_i(g) = \sum_{g \in \mathcal{K}_j} \chi_i(g) = |\mathcal{K}_j| \chi_i(g).$$

Thus $\alpha \chi_i(1) = \operatorname{tr} X = |\mathcal{K}_j| \chi_i(g)$, as needed to establish (1).

Now let g be a fixed element of $\mathcal{K}_s$ and define a_{ijs} to be the number of ordered pairs g_i, g_j with $g_i \in \mathcal{K}_i$, $g_j \in \mathcal{K}_j$ and $g_i g_j = g$. Notice that a_{ijs} is an integer. It is independent of the choice of g in $\mathcal{K}_s$ because if $x^{-1}gx$ is a conjugate of g, every ordered pair g_i, g_j whose product is g gives rise to an ordered pair $x^{-1}g_i x$, $x^{-1}g_j x$ whose product is $x^{-1}gx$ (and vice versa).

Next we prove that for all $i, j, t \in \{1, \ldots, r\}$

$$\omega_t(\mathcal{K}_i)\omega_t(\mathcal{K}_j) = \sum_{s=1}^{r} a_{ijs}\omega_t(\mathcal{K}_s). \tag{19.2}$$

To see this note that by (1), the left hand side of (2) is the diagonal entry of the scalar matrix on the left of the following equation:

$$\begin{aligned}
\Big(\sum_{g \in \mathcal{K}_i} \varphi_t(g)\Big)\Big(\sum_{g \in \mathcal{K}_j} \varphi_t(g)\Big) &= \sum_{g_i \in \mathcal{K}_i} \sum_{g_j \in \mathcal{K}_j} \varphi_t(g_i g_j) \\
&= \sum_{s=1}^{r} \sum_{g \in \mathcal{K}_s} a_{ijs}\varphi_t(g) \\
&= \sum_{s=1}^{r} a_{ijs} \sum_{g \in \mathcal{K}_s} \varphi_t(g) \qquad \text{(since } a_{ijs} \text{ is independent of } g \in \mathcal{K}_s\text{)} \\
&= \sum_{s=1}^{r} a_{ijs}\omega_t(\mathcal{K}_s) I \qquad \text{(by (1)).}
\end{aligned}$$

Comparing entries of these scalar matrices gives (2).

Now (2) implies that the subring of $\mathbb{C}$ generated by $\mathbb{Z}$ and $\omega_t(\mathcal{K}_1), \ldots, \omega_t(\mathcal{K}_r)$ is a finitely generated $\mathbb{Z}$-module for each $t \in \{1, \ldots, r\}$ (it is generated as a $\mathbb{Z}$-module by $1, \omega_t(\mathcal{K}_1), \ldots, \omega_t(\mathcal{K}_r)$). Since $\mathbb{Z}$ is a Principal Ideal Domain the submodule $\mathbb{Z}[\omega_t(\mathcal{K}_i)]$ is also a finitely generated $\mathbb{Z}$-module, hence $\omega_t(\mathcal{K}_i)$ is an algebraic integer by Proposition 2. This completes the proof.

Corollary 5. The degree of each complex irreducible representation of a finite group G divides the order of G, i.e., $\chi_i(1) \mid |G|$ for $i = 1, 2, \ldots, r$.

Proof: Under the notation of Proposition 4 and with $g_j \in \mathcal{K}_j$ we have

$$\begin{aligned}\frac{|G|}{\chi_i(1)} &= \frac{|G|}{\chi_i(1)}(\chi_i, \chi_i) \\ &= \sum_{j=1}^{r} \frac{|\mathcal{K}_j|\chi_i(g_j)\overline{\chi_i(g_j)}}{\chi_i(1)} \\ &= \sum_{j=1}^{r} \omega_i(\mathcal{K}_j)\overline{\chi_i(g_j)}.\end{aligned}$$

The right hand side is an algebraic integer and the left hand side is rational, hence is an integer. This proves the corollary.

The next two lemmas lead directly to Burnside's Theorem.

Lemma 6. If G is any group that has a conjugacy class $\mathcal{K}$ and an irreducible matrix representation φ with character χ such that $(|\mathcal{K}|, \chi(1)) = 1$, then for $g \in \mathcal{K}$ either $\chi(g) = 0$ or $\varphi(g)$ is a scalar matrix.

Proof: By hypothesis there exist $s, t \in \mathbb{Z}$ such that $s|\mathcal{K}| + t\chi(1) = 1$. Thus

$$s|\mathcal{K}|\chi(g) + t\chi(1)\chi(g) = \chi(g).$$

Divide both sides of this by $\chi(1)$ and note that by Corollary 3 and Proposition 4 both $\chi(g)$ and $\dfrac{|\mathcal{K}|\chi(g)}{\chi(1)}$ are algebraic integers, hence so is $\dfrac{\chi(g)}{\chi(1)}$. Let $a_1 = \dfrac{\chi(g)}{\chi(1)}$ and let $a_1, a_2, \ldots, a_n$ be all its algebraic conjugates over $\mathbb{Q}$ (i.e., the roots of the minimal polynomial of a_1 over $\mathbb{Q}$). Since a_1 is a sum of $\chi(1)$ roots of 1 divided by the integer $\chi(1)$, each a_i is also a sum of $\chi(1)$ roots of 1 divided by $\chi(1)$. Thus a_i has complex absolute value ≤ 1 for all i. Now $b = \prod_{i=1}^{n} a_i \in \mathbb{Q}$ and b is an algebraic integer ($\pm b$ is the constant term of the irreducible polynomial of a_1), hence $b \in \mathbb{Z}$. But

$$|b| = \prod_{i=1}^{n} |a_i| \leq 1,$$

so $b = 0, \pm 1$. Since all a_i's are conjugate, $b = 0 \Leftrightarrow a_1 = 0 \Leftrightarrow \chi(g) = 0$. Also, $b = \pm 1 \Leftrightarrow |a_i| = 1$ for all i. Thus either $\chi(g) = 0$ or $|\chi(g)| = \chi(1)$. In the former situation the lemma is established, so assume $|\chi(g)| = \chi(1)$.

Let φ_1 be a matrix representation equivalent to φ in which $\varphi_1(g)$ is a diagonal matrix:

$$\varphi_1(g) = \begin{pmatrix} \epsilon_1 & & & \\ & \epsilon_2 & & \\ & & \ddots & \\ & & & \epsilon_n \end{pmatrix}.$$

Thus $\chi(g) = \epsilon_1 + \cdots + \epsilon_n$. By the triangle inequality if $\epsilon_i \neq \epsilon_j$ for any i, j, then $|\epsilon_1 + \cdots + \epsilon_n| < n = \chi(1)$. Since this is not the case we must have $\varphi_1(g) = \epsilon I$ (where $\epsilon = \epsilon_i$ for all i). Since scalar matrices are similar only to themselves, $\varphi(g) = \epsilon I$ as well. This completes the proof.