Chapter 8. The Classification of Groups of Small Order

8.1 Theorem: (*Some Classification Theorems*) *Let G be a finite group and let p and q be prime numbers with $p > q$.*
(1) If $|G| = p$ then $G \cong \mathbb{Z}_p$.
(2) If $|G| = p^2$ then either $G \cong \mathbb{Z}_{p^2}$ or $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.
(3) If $|G| = 2p$ then either $G \cong \mathbb{Z}_{2p}$ or $G \cong D_p$.
(4) If $|G| = pq$ and $q \nmid p-1$ then $G \cong \mathbb{Z}_{pq}$. If $|G| = pq$ and $q \big| p-1$ then $G \cong \mathbb{Z}_{pq}$ or $G \cong T$ where T is a group whose elements are uniquely of the form $\alpha^i \beta^j$ with $i \in \mathbb{Z}_p$ and $j \in \mathbb{Z}_q$, with $|\alpha| = p$, $|\beta| = q$ and $\beta\alpha\beta^{-1} = \alpha^s$, where $s \neq 1$ and $s^q = 1 \mod p$.

Proof: To prove Part 1, suppose that $|G| = p$ and choose $a \in G$ with $a \neq e$. By Lagrange's Theorem, we have $|a| = p$, so that $G = \langle a \rangle \cong \mathbb{Z}_p$.

To prove Part 2, suppose that $|G| = p^2$. Consider the action of G on itself given by conjugation, that is by $x * a = xax^{-1}$. Note that G is the disjoint union of the orbits, and the size of each orbit divides $|G| = p^2$. Some of the orbits have size 1 and the size of each of the other orbits is a multiple of p. It follows that $|G|$ is equal to the number of orbits of size 1, modulo p. For $a \in G$ we have $\big|\text{Orb}(a)\big| = 1 \iff xax^{-1} = a$ for all $x \in G \iff a \in Z(G)$, and hence $|Z(G)| \equiv |G| = p^2 \equiv 0 \mod p$. Thus $|Z(G)| \neq 1$ so, by Lagrange's Theorem, either $|Z(G)| = p$ or $|Z(G)| = p^2$. If we had $|Z(G)| = p$ then we could choose $a \in G$ with $a \notin Z(G)$, but then we would have proper subgroups $Z(G) < C(a)$ and $C(a) < G$ which is not possible by Lagrange's Theorem, since $|Z(G)| = p$ and $|G| = p^2$. Thus we must have $|Z(G)| = p^2$, and hence $Z(G) = G$ so that G is abelian. By the classification of finite abelian groups, either $G \cong \mathbb{Z}_{p^2}$ or $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$, as required.

Part 3 follows as a special case of Part 4, but we provide a proof anyway. If $p = 2$ and $|G| = 2p = 4$ then, by Part 2, either $G \cong \mathbb{Z}_4$ or $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \cong D_2$. Suppose that $p > 2$ and $|G| = 2p$, and suppose that $G \not\cong \mathbb{Z}_{2p}$. Each non-identity element of G has order 2 or p. By Cauchy's Theorem, we can choose $a \in G$ with $|a| = p$, then we choose $b \notin \langle a \rangle$, so that G is the disjoint union of two cosets $G = \langle a \rangle \cup b\langle a \rangle$. Note that $b^2\langle a \rangle \neq b\langle a \rangle$ since $b = b^{-1}b^2 \notin \langle a \rangle$, and so we must have $b^2\langle a \rangle = \langle a \rangle$ and hence $b^2 \in \langle a \rangle$. Note that $|b| \neq p$, since if we had $b^p = e$ then (since $p+1$ is even) we would have $b = b^{p+1} \in \langle b^2 \rangle \subseteq \langle a \rangle$, and so $|b| = 2$. The same argument shows that $|x| = 2$ for every $x \notin \langle a \rangle$. Consider the element ab. Note that $ab \notin \langle a \rangle = a\langle a \rangle$ since $b = a^{-1}ab \notin \langle a \rangle$, and so we have $|ab| = 2$. Thus $abab = e$ and so $ab = (ab)^{-1} = b^{-1}a^{-1} = ba^{p-1}$ Since G is the disjoint union $G = \langle a \rangle \cup b\langle a \rangle$, we have $G = \big\{e, a, a^2, \cdots, a^{p-1}, b, ba, ba^2, \cdots, ba^{p-1}\big\}$ with the listed elements distinct. Since $ab = ba^{-1}$, we have $a^2b = aba^{-1} = ba^{-2}$ and $a^3b = aba^{-2} = ba^{-3}$ and so on so that $a^kb = ba^{-k}$. This determines the operation on G completely: indeed we have $a^k \cdot a^l = a^{k+l}$, $a^k \cdot ba^l = ba^{l-k}$, $ba^k \cdot a^l = ba^{k+l}$ and $ba^k \cdot ba^l = a^{l-k}$, and hence $G \cong D_p$, as required.

To prove Part 4, suppose that $|G| = pq$. By Cauchy's Theorem, we can choose $a, b \in G$ with $|a| = p$ and $|b| = q$. Let $H = \langle a \rangle$ and $K = \langle b \rangle$. Since $|G/H| = q$, which is the smallest prime divisor of $|G|$, if follows from Theorem 1.16 that $H \trianglelefteq G$. Since $|G/H| = q$, which is prime, G/H is cyclic, and G is the disjoint union of the cosets $b^jH = Hb^j$. Thus each element in G can be written uniquely in the form a^ib^j with $0 \leq i < p$ and $0 \leq j < q$. In particular, we have $G = \langle a, b \rangle = HK$ and $H \cap K = \{e\}$.

Note that K is a Sylow q-subgroup of G. By the third Sylow Theorem, the number of Sylow q-subgroups divides $|G|$, so it must be equal to 1, p, q or pq, and it is also equal to 1 modulo q (so it cannot be equal to q or pq). Thus if $q\not|\,p-1$ (so that $p \neq 1 \mod q$) then K is the only Sylow p-subgroup, while if $q|p-1$ (so that $p = 1 \mod q$) then either K is the only Sylow q-subgroup or there are exactly p distinct Sylow q-subgroups.

If K is the only Sylow q-subgroup, then by the second Sylow Theorem we must have $bKb^{-1} = K$ for all $b \in G$, so that $K \trianglelefteq G$. Recall (or verify) that since $H \trianglelefteq G$, $K \trianglelefteq G$, $G = HK$ and $H \cap K = \{e\}$, it follows that $G \cong H \times K \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$.

Suppose that K is not the only Sylow q-subgroup. Note that G cannot be abelian (if G was abelian we would have $G \cong Z_{pq}$ which has a unique Sylow q-subgroup). Since $H \trianglelefteq G$ we have $bab^{-1} = a^r$ for some $r \in \mathbb{Z}_p$. Note that $r \neq 0$ since $a \neq e$ and $r \neq 1$ since G is not abelian. The fact that $bab^{-1} = a^r$ determines the operation on G completely: We have $b^2ab^{-2} = b(bab^{-1})b^{-1} = ba^rb^{-1} = (bab^{-1})^r = (a^r)^r = a^{r^2}$ and similarly we have $b^3ab^{-3} = ba^{r^2}b^{-1} = (bab^{-1})^{r^2} = a^{r^3}$ and so on, so that by induction $b^jab^{-j} = a^{r^j}$, that is $b^ja = a^{r^j}b^j$, for all $j \in \mathbb{Z}^+$. Also, we have $b^ja^2 = a^{r^j}b^ja = a^{r^j}a^{r^j}b^j = a^{2r^j}b^j$ and similarly $b^ja^3 = a^{2r^j}b^ja = a^{3r^j}b^j$ and so on, so that in general $b^ja^k = a^{kr^j}b^j$ for all $j,k \in \mathbb{Z}^+$. Thus the elements in G are of the form a^ib^j with $i \in \mathbb{Z}_p$ and $j \in \mathbb{Z}_q$, and the operation is given by

$$(a^ib^j)(a^kb^\ell) = a^i(b^ja^k)b^\ell = a^i\big(a^{kr^j}b^j\big)b^\ell = a^{i+kr^j}b^{j+\ell}.$$

The same calculation shows that in the group T, the fact that $\beta\alpha\beta^{-1} = \alpha^s$ determines the operation, and it is given by

$$(\alpha^i\beta^j)(\alpha^k\beta^\ell) = \alpha^{i+ks^j}\beta^{j+\ell}.$$

We claim that $G \cong T$. Since $b^q = e$ we have $a = b^qab^{-q} = a^{r^q}$. Since $|a| = p$ and $a^{r^q} = a$ we have $r^q = 1 \mod p$. Recall (or verify) that the group of units $U_p = (\mathbb{Z}_p)^*$ is a cyclic group of order $p-1$. Since $r \neq 1$ and $r^q = 1 \mod p$, we see that r is a generator of the (unique) q-element subgroup of U_p. Likewise, since $s \neq 1$ and $s^q = 1 \mod p$, we have $\langle s\rangle = \langle r\rangle = \big\{1, r, r^2, \cdots, r^{q-1}\big\} \leq U_p$ and so we can choose $t \in \mathbb{Z}_{q-1}$ so that $r^t = s \mod p$. Verify that the map $\phi : T \to G$ given by $\phi(\alpha^i\beta^j) = a^ib^{tj}$ is a group isomorphism.

There is one last subtle detail which remains, and that is to prove that the group T actually exists, that is to show that there exists $s \in \mathbb{Z}_p$ with $s \neq 1$ and $s^q = 1 \mod p$, and there exists a group T whose elements are uniquely of the form $\alpha^i\beta^j$ with $i \in \mathbb{Z}_p$ and $j \in \mathbb{Z}_q$ such that $|\alpha| = p$, $|\beta| = q$ and $\beta\alpha\beta^{-1} = \alpha^s$. We leave this part of the proof as an exercise.

8.2 Remark: The above theorem fully classifies, up to isomorphism, all groups of order $n \leq 20$ except for $n \in \{8, 12, 16, 18, 20\}$.

8.3 Exercise: Show that every group of order 8 is isomorphic to one of the groups $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_8$, D_4 or Q_8, where Q_8 is the quaternionic group.

8.4 Exercise: Show that every group of order 12 is isomorphic to one of the groups $\mathbb{Z}_2 \times \mathbb{Z}_6$, $\mathbb{Z}_{12}$, D_6, A_4 or T, where $T = \langle\alpha, \beta\rangle$ with $|\alpha| = 6$, $|\beta| = 4$, $\beta^2 = \alpha^3$ and $\alpha\beta\alpha = \beta$.

8.5 Exercise: Classify (up to isomorphism) all groups of order 18 and 20.

Simple Groups and Composition Series

8.6 Definition: A group G is called **simple** when it has no nontrivial proper normal subgroup.

8.7 Definition: Let G be a group. A **subnormal series** for G is a sequence of subgroups

$$\{e\} = N_0 \leq N_1 \leq \cdots \leq N_\ell = G$$

with $N_{k-1} \lhd N_k$ for $1 \leq k \leq \ell$. A **composition series** for G is a subnormal series $\{e\} = N_0 \leq N_1 \leq \cdots N_\ell = G$ such that $N_{k-1} \lhd N_k$ with N_k/N_{k-1} simple for $1 \leq k \leq \ell$.

8.8 Example: In the group $D_4 = \langle \sigma, \tau \rangle$ with $|\sigma| = 4$, $|\tau| = 2$ and $\sigma\tau\sigma = \tau$, we have the two composition series

$$\{e\} \leq \langle r^2 \rangle \leq \langle r \rangle \leq D_4 \quad \text{and} \quad \{e\} \leq \langle \tau \rangle \leq \langle \sigma^2, \tau \rangle \leq D_4 .$$

8.9 Theorem: *(The Jordan-Hölder Theorem) Let G be a finite group. Then*
(1) G has a composition series and
(2) the composition factors are unique in the sense that if $\{e\} = N_0 \leq N_1 \leq \cdots \leq N_n = G$ and $\{e\} = M_0 \leq M_1 \leq \cdots \leq M_m = G$ are two composition series for G, then $n = m$ and there is a permutation $\sigma \in S_n$ such that $M_{\sigma(k)}/M_{\sigma(k)-1} \cong N_k/N_{k-1}$ for $1 \leq k \leq n$.

Proof: The proof is left as a (fairly long) exercise.

8.10 Remark: The above theorem suggests a two-part program, known as the **Hölder program**, for classifying all finite groups, up to isomorphism. The first part of the program is to classify all finite simple groups, and the second part is two determine, given a list of simple groups, all the ways to form a group G with the given simple groups as the composition factors. The first part of this program is considered to have been completed: the simple groups include the cyclic groups of prime order, the alternating groups A_n with $n \geq 5$, 16 additional infinite families of finite simple groups which are said to be **of Lee type**, along with 27 specific finite simple groups, called the **sporadic groups**. The second part of the program is known as the **extension problem**, and it is considered to be an extremely difficult problem.

8.11 Example: Show that for $n \geq 3$, A_n is generated by the set of all 3-cycles, and for any $a \neq b \in \{1, 2, \cdots, n\}$, A_n is generated by the 3-cycles of the form (abk) with $k \neq a, b$.

Solution: Recall that every permutation in A_n is equal to a product of an even number of 2-cycles. Every product of a pair of 2-cycles is of one of the forms $(ab)(ab)$, $(ab)(ac)$ or $(ab)(cd)$, where a, b, c, d are distinct, and we have

$$(ab)(ab) = (abc)(acb) \ , \ (ab)(ac) = (acb) \ , \ (ab)(cd) = (adc)(abc) \, ,$$

and so A_n is generated by the set of all 3-cycles. Now fix $a, b \in \{1, 2, \cdots, n\}$ with $a \neq b$. Note that every 3-cycle is of one of the forms (abk), (akb), (akl), (bkl) or (klm), where a, b, k, l, m are all distinct, and we have

$$(akb) = (abk)^2 \ , \ (akl) = (abl)(abk)^2 \ , \ (bkl) = (abl)^2(abk) \ , \ (klm) = (abk)^2(abm)(abl)^2(abk) \, .$$

8.12 Theorem: *For $n \geq 5$, the alternating group A_n is simple.*

Proof: Let $H \trianglelefteq A_n$. We shall show that $H = A_n$. We consider 5 cases. Case 1: suppose first that H contains a 3-cycle, say $(abc) \in H$. Then for any $k \neq a, b, c$ we have $(abk) = (ab)(ck)\,(abc)^2(ck)(ab) \in H$ It follows that $A_n = H$ because A_n is generated by the 3-cycles of the form (abk) with $k \neq a, b$ (as shown in Example 1.30). Case 2: suppose that H contains an element α which, when written in cycle notation, has a cycle of length $r \geq 4$, say $\alpha = (a_1 a_2 a_3 \cdots a_r)\beta \in H$. Then $(a_1 a_3 a_r) = \alpha^{-1}(a_1 a_2 a_3)\alpha(a_1 a_2 a_3)^{-1} \in H$ and so $H = A_n$ by Case 1. Case 3: suppose that H contains an element α which, when written in cycle notation, has at least two 3-cycles, say $\alpha = (a_1 a_2 a_3)(a_4 a_5 a_6)\beta \in H$. Then we have $(a_1 a_4 a_2 a_6 a_3) = \alpha^{-1}(a_1 a_2 a_4)\alpha(a_1 a_2 a_4)^{-1} \in H$ and so $H = A_n$ by Case 2. Case 4: suppose that H contains an element α which, when written in cycle notation, is a product of one 3-cycle and some 2-cycles, say $\alpha = (a_1 a_2 a_3)\beta \in H$ where β is a product of disjoint 2-cycles so that $\beta^2 = e$. Then $(a_1 a_3 a_2) = \alpha^2 \in H$ and so $H = A_n$ by Case 1. Case 5: suppose that H contains an element α which, when written in cycle notation, is a product of 2-cycles, say $\alpha = (a_1 a_2)(a_3 a_4)\beta \in H$. Then $(a_1 a_3)(a_2 a_4) = \alpha^{-1}(a_1 a_2 a_3)\alpha(a_1 a_2 a_3)^{-1} \in H$. Let $\gamma = (a_1 a_3)(a_2 a_4)$ and choose b distinct from a_1, a_2, a_3, a_4. Then $(a_1 a_3 b) = \gamma(a_1 a_2 b)\gamma(a_1 a_3 b)^{-1} \in H$ and so $H = A_n$ by Case 1.

8.13 Theorem: *(The Sylow Test for Nonsimplicity) Let G be a finite group with $|G| = n$. Suppose that n is not prime and n has a prime divisor p such that 1 is the only divisor of n which is equal to 1 modulo p. Then G is not simple.*

Proof: If $n = p^k$ with $k \geq 2$ then $Z(G) \neq \{e\}$ by the class equation, so either $Z(G) = G$ so that G is abelian, or $Z(G)$ is a nontrivial proper subgroup of G, and in either case G is not simple. Suppose that n is not a power of p, and let H be a Sylow p-subgroup of G. Since the number of Sylow p-subgroups divides $n = |G|$ and is equal to 1 modulo p, there is only one Sylow p-subgroup, by the hypothesis of the theorem. Since H is the only Sylow p-subgroup, we have $aHa^{-1} = H$ for all $a \in G$ so that H is normal. Thus H is a nontrivial normal subgroup of G so that G is not simple.

8.14 Exercise: Verify that the only composite numbers n with $1 \leq n \leq 100$ for which Theorem 1.32 does *not* rule out the possible existence of a simple group of order n are the numbers

$$n \in \{12, 24, 30, 36, 48, 56, 60, 72, 80, 90, 96\}.$$

8.15 Remark: In fact, the Sylow Theorems can be used to show that the *only* composite number n with $1 \leq n \leq 100$ for which there exists a simple group of order n is the number $n = 60$ (and indeed A_5 is a simple group of order 60).

8.16 Exercise: Show that there is no simple group of order 30.

8.17 Exercise: Classify, up to isomorphism, all groups of order 30.