Chapter 1. Groups

The Action of a Group on a Set

1.1 Definition: Let G be a group. A **representation** of G is a group homomorphism $\rho : G \to \text{Perm}(X)$ for some set X. A representation $\rho : G \to \text{Perm}(X)$ is called **faithful** when it is injective.

1.2 Remark: Given a faithful representation $\rho : G \to \text{Perm}(X)$, we sometimes identify the group G with its isomorphic image $\rho(G)$, which is a group of permutations of X.

1.3 Definition: Let G be a group and let X be a set. A **group action** of G on X is a map $* : G \times X \to X$, where for $a \in G$ and $x \in X$ we write $*(a,x)$ as $a * x$ or simply as ax, such that

(1) $ex = x$ for all $x \in X$, and
(2) $(ab)x = a(bx)$ for all $a, b \in G$ and all $x \in S$.

1.4 Note: Given a group G and a set X, here is a natural bijective correspondence between representations $\rho : G \to \text{Perm}(X)$ and group actions $* : G \times X \to X$. The representation ρ and its corresponding group action $*$ determine one another by the formula

$$a * x = \rho(a)(x) \text{ for all } a \in G, x \in X\,.$$

As an exercise, verify that given a representation ρ, this formula defines a group action $*$, and conversely that given a group action $*$, the formula defines a representation ρ.

1.5 Definition: Suppose that a group G acts on a set X. The group action is called **faithful** when the corresponding representation is faithful.

1.6 Example: When a group G acts on itself by its own operation, so $a * x = ax = \ell_a(x)$, the corresponding representation $\rho : G \to \text{Perm}(G)$ is given by $\rho(a) = \ell_a$. This map is used in the proof of Cayley's Theorem: the representation is faithful, so it gives an isomorphism from G to its image $\rho(G) \leq \text{Perm}(G)$.

1.7 Example: When a group G acts on itself by conjugation, so $a * x = axa^{-1} = c_a(x)$, the corresponding representation $\rho : G \to \text{Perm}(G)$ is given by $\rho(a) = c_a$. This map is used to show that $G/Z(G) \cong \text{Inn}(G)$: indeed we have $\text{Ker}(\rho) = Z(G)$ and $\text{Image}(\rho) = \text{Inn}(G)$ giving the isomorphism $G/Z(G) \cong \text{Inn}(G)$.

1.8 Example: When F is a field (or a commutative ring with 1) and the group $GL_n(F)$ acts on F^n by matrix multiplication, so that $A * x = Ax = L_A(x)$, the corresponding representation $\rho : GL_n(F) \to \text{Perm}(F^n)$ is given by $\rho(A) = L_A$ (so ρ sends the matrix A to the linear map L_A given by $L_A(x) = Ax$). The representation is faithful, so its gives an isomorphism from $GL_n(F)$ (which is a set of invertible matrices) to its image (which is a set of invertible linear maps).

1.9 Definition: Let G be a group which acts on a set X. For $a \in G$ we define the **fixed set** of a in X to be the set

$$\mathrm{Fix}(a) = \left\{ x \in X \middle| ax = x \right\} \subseteq X\,.$$

For $x \in X$ we define the **orbit** of x under G to be the set

$$\mathrm{Orb}(x) = \left\{ ax \middle| a \in G \right\} \subseteq X\,.$$

Verify that for $x, y \in S$ we have $y \in \mathrm{Orb}(x) \iff \mathrm{Orb}(x) = \mathrm{Orb}(y)$ so, for the equivalence relation on X given by $x \sim y \iff \mathrm{Orb}(x) = \mathrm{Orb}(y)$, the equivalence class of x is equal to the orbit of x, and X is equal to the disjoint union of the orbits.
The set of distinct orbits is denoted by X/G so we have

$$X/G = \left\{ \mathrm{Orb}(x) \middle| x \in X \right\}.$$

For $x \in X$ we define the **stabilizer** of x in G to be the subgroup

$$\mathrm{Stab}(x) = \left\{ a \in G \middle| ax = x \right\} \leq G\,.$$

Note that Stab(x) $\leq G$ because $ex = x$, if $ax = x$ and $bx = x$ then $(ab)x = a(bx) = ax = x$, and if $ax = x$ then $x = ex = (a^{-1}a)x = a^{-1}(ax) = a^{-1}x$.

1.10 Theorem: (*The Orbit-Stabilizer Theorem*) *Let G be a group which acts on a set X. Then for all $x \in X$ we have*

$$|G| = \left|\mathrm{Orb}(x)\right| \left|\mathrm{Stab}(x)\right|.$$

Proof: Let $x \in X$. We shall show that $\Big|\mathrm{Orb}(x)\Big| = \Big|G/\mathrm{Stab}(x)\Big|$. Write $H = \mathrm{Stab}(x)$. Define a map $\Phi : G/H \to \mathrm{Orb}(x)$ by $\Phi(aH) = ax$. Then Φ is well-defined because for $a, b \in G$ we have $aH = bH \implies b^{-1}a \in H \implies b^{-1}a\,x = x \implies ax = bx$, Φ is injective because for $a, b \in G$ we have $ax = bx \implies b^{-1}a\,x = x \implies b^{-1}a \in H \implies aH = bH$, and the map Φ is clearly surjective.

1.11 Exercise: Consider D_6 as a subgroup of S_6. Find Orb(1) and Stab(1).

1.12 Exercise: Let G be the rotation group of a cube Q. Label the vertices of the cube by elements of $S = \{1, 2, \cdots, 6\}$, think of the elements of G as permutations of S and hence identify G with a subgroup of S_6. Find $\left|\mathrm{Orb}(1)\right|$ and $\left|\mathrm{Stab}(1)\right|$ and hence find $|G|$.

1.13 Theorem: (*The Class Equation*) *Let G be a finite group. Choose $a_1, a_2, \cdots, a_n \in G$ with one element a_i selected from each conjugacy class containing more than one element. Then*

$$|G| = \left|Z(G)\right| + \sum_{i=1}^{n} \left|G/C(a_i)\right|.$$

Proof: For $a \in G$ we have $\left|\mathrm{Cl}(a)\right| = 1 \iff bab^{-1} = a$ for all $b \in G \iff a \in Z(G)$. Say $Z(G) = \left\{a_{n+1}, a_{n+2}, \cdots, a_m\right\}$ so that G has exactly m distinct conjugacy classes and the elements $a_1, \cdots, a_n, a_{n+1}, \cdots, a_m$ make up exactly one element from each class. Let G act on itself by conjugation, so that $b * a = bab^{-1}$. Note that for $a \in G$, we have $\mathrm{Orb}(a) = \left\{xax^{-1} \middle| x \in G\right\} = \mathrm{Cl}(a)$ (the conjugacy class of a in G) and we have $\mathrm{Stab}(a) = \left\{x \in G \middle| xax^{-1} = a\right\} = C(a)$ (the centralizer of a in G). Also, by the Orbit-Stabilizer Theorem, we have $\left|\mathrm{Orb}(a_i)\right| = \frac{|G|}{|C(a_i)|} = \left|G/C(a_i)\right|$. Since G is the disjoint union of the orbits,

$$|G| = \sum_{i=1}^{m} \left|\mathrm{Orb}(a_i)\right| = \sum_{i=1}^{n} \left|G/C(a_i)\right| + \sum_{i=n+1}^{m} 1 = \sum_{i=1}^{n} |G/C(a_i)| + |Z(G)|.$$

1.14 Example: Let X be the set of all subgroups of a group G. Let G act on X by conjugation, so $a * H = c_a(H) = aHa^{-1}$, where $a \in G$ and $H \leq G$. For $H \in X$, that is $H \leq G$, we have

$$\begin{aligned} \text{Stab}(H) &= \big\{a \in G \big| aHa^{-1} = H\big\} = \big\{a \in G \big| aH = Ha\big\} = N_G(H), \\ \text{Orb}(H) &= \big\{aHa^{-1} \big| a \in G\big\} = \text{Cl}(H), \end{aligned}$$

where $N_G(H)$ is the normalizer of H in G and $\text{Cl}(H)$ is the conjugacy class of H in G, that is the set of all subgroups conjugate to H in G.

1.15 Theorem: *(Cauchy's Theorem) Let G be a finite group. Let p be a prime divisor of $|G|$. Then G contains an element of order p. Indeed*

$$\Big|\big\{a \in G \big| |a| = p\big\}\Big| = p - 1 \bmod p(p-1)\,.$$

Proof: Let n be the number of elements of order p in G, that is $n = \big|\{a \in G\big||a| = p\}\big|$. Recall that $n = 0 \mod (p-1)$ (indeed n is equal to $(p-1)$ times the number of cyclic subgroups of order p in G because each of these subgroups has $\phi(p) = p - 1$ generators). Let $X = \big\{(x_1, x_2, \cdots, x_p) \in G^p \big| x_1 x_2 \cdots x_p = e\big\}$. Note that $|X| = |G|^{p-1}$ since to get $(x_1, x_2, \cdots, x_p) \in X$ we can choose $x_1, x_2, \cdots, x_{p-1}$ arbitrarily and then x_p must be given by $x_p = (x_1 x_2 \cdots x_{p-1})^{-1}$. Note that $\mathbb{Z}_p$ acts on X by cyclic permutation, that is by

$$k * (x_1, x_2, \cdots, x_p) = (x_{1+k}, x_{2+k}, \cdots, x_p, x_1, \cdots, x_k)$$

since if $x_1 x_2 \cdots x_p = e$ then $x_1 x_2 \cdots x_k = (x_{k+1} \cdots x_p)^{-1}$ so $x_{1+k} x_{2+k} \cdots x_p x_1 \cdots x_k = e$. For $x = (x_1, x_2, \cdots, x_p) \in S$, by the Orbit/Stabilizer Theorem $\big|\text{Orb}(x)\big|$ divides $|\mathbb{Z}_p| = p$ so that $\big|\text{Orb}(x)\big| \in \{1, p\}$, so we have

$$\Big|\text{Orb}(x)\Big| = \begin{cases} 1 \text{ , if } x = (a, a, \cdots, a) \text{ for some } a \in G, \text{ and} \\ p \text{ , otherwise.} \end{cases}$$

Since X is the disjoint union of the orbits, we have $|X| = k + pl$ where k is the number of orbits of size 1 and l is the number of orbits of size p. Note that k is equal to the number of elements $a \in G$ with $a^p = 1$, and so $k = 1 + n$. Since $|X| = |G|^{p-1} = 0 \mod p$ we have $n = k - 1 = |S| - pl - 1 = -1 \mod p$. Since $n = -1 = p - 1 \bmod p$ and $n = 0 = p - 1 \bmod (p-1)$, we have $n = p - 1 \mod p(p-1)$ by the Chinese Remainder Theorem.

1.16 Theorem: *Let G be a finite group and let $H \leq G$. Suppose that $|G/H| = p$, where p is the smallest prime divisor of $|G|$. Then $H \trianglelefteq G$.*

Proof: Let $X = G/H = \big\{aH \big| a \in G\big\}$. Since $|X| = p$ we have $\text{Perm}(X) \cong S_p$. Let G act on X by left multiplication, so we have $a * (bH) = abH$ for $a, b \in G$. Let $\rho : G \to \text{Perm}(X)$ be the associated representation, so $\rho(a)(bH) = abH$. Let

$$K = \text{Ker}(\rho) = \big\{a \in G \big| abH = bH \text{ for all } b \in G\big\} \trianglelefteq G\,.$$

Note that $K \leq H$ because $a \in K \implies aeH = eH \implies a \in H$. Since $K \trianglelefteq G$ (it is the kernel of a homomorphism) and $K \leq H$, we also have $K \trianglelefteq H$. By the First Isomorphism Theorem, we have $G/K \cong \rho(G) \leq \text{Perm}(X) \cong S_p$. By Lagrange's Theorem $|G/K|$ divides $|S_p| = p!$. By another application of Lagrange's Theorem, $|G/K|$ also divides $|G|$. Since $|G/K| \,\big|\, |G|$ and p is the smallest prime factor of $|G|$, $|G/K|$ has no prime factors less than p. Since $|G/K| \,\big|\, p!$, we must have $|G/K| = 1$ or p. Since $|G/K| = |G/H|\,|H/K| = p|H/K|$ we have $|G/K| = p$ and $|H/K| = 1$. Thus in fact $H = K \trianglelefteq G$.

The Sylow Theorems

1.17 Definition: Let G be a group with $|G| = p^m \ell$ where p is prime and $\gcd(p, \ell) = 1$. A **p-subgroup** of G is a subgroup of order p^k for some k, and a **Sylow p-subgroup** of G is a subgroup of order p^m.

1.18 Exercise: Find the Sylow p-subgroups of S_3 and A_4 for $p = 2, 3$.

1.19 Theorem: *(The Sylow Theorems) Let G be a group with $|G| = p^m \ell$ where p is prime and $\gcd(p, \ell) = 1$.*

(1) For every $0 \leq k \leq m$, G has a subgroup of order p^k, and when $k < n$, each subgroup of order p^k is normal in a subgroup of order p^{k+1}. In particular, G has a Sylow p-subgroup, and every p-subgroup of G is contained in a Sylow p-subgroup.
(2) If P is a p-subgroup of G and S is a Sylow p-subgroup of G, then there exists $a \in G$ such that $aPa^{-1} \leq S$. In particular, any two Sylow p-subgroups of G are conjugate.
(3) The number of distinct Sylow p-subgroups of G divides $|G|$ and is equal to 1 mod p.

Proof: To prove Part 1, note that the trivial subgroup of G is a p-subgroup of order p^0. By induction, it suffices to show that for every p-subgroup $P \leq G$ with $|P| = p^k$ for $0 \leq k < m$ we have $P \trianglelefteq H$ for some $H \leq G$ with $|H| = p^{k+1}$. Let $0 \leq k < m$ and let $P \leq G$ with $|P| = p^k$. Consider the action of P on the set of left cosets G/P given by $x * (aP) = xaP$. Note that G/P is the disjoint union of the orbits, and the size of each orbit divides $|P| = p^k$. Some of the orbits have size 1 and the size of all other orbits is a multiple of p, and so $|G/P|$ is equal to the number of orbits of size 1, modulo p. For $a \in G$,

$$\begin{aligned}|\mathrm{Orb}(aP)| = 1 &\iff xaP = aP \text{ for all } x \in P \iff a^{-1}xa \in P \text{ for all } x \in P \\ &\iff a^{-1}Pa = P \iff Pa = aP \iff a \in N(P) = N_G(P),\end{aligned}$$

so the number of orbits of size 1 is equal to the number of cosets aP with $a \in N(P)$, which is equal to $N(P)/P$. Thus we have $|N(P)/P| \equiv |G/P| \equiv 0 \mod p$. By Cauchy's Theorem, since p divides $|N(P)/P|$ it follows that the group $N(P)/P$ contains an element of order p, hence a subgroup of order p. This subgroup is of the form H/P where $P \leq H \leq N(P) \leq G$. Since $P \trianglelefteq N(P)$ we also have $P \trianglelefteq H$. Since $|H/P| = p$ and $|P| = p^k$ we have $|H| = p^{k+1}$.

To prove Part 2, let P be a p-subgroup of G with $|P| = p^k$, and let S be a Sylow p-subgroup of G. Consider the action of P on the G/S given by $x(aS) = xaS$. Since G/S is equal to the disjoint union of the orbits, and the size of each orbit divides $|P| = p^k$, it follows that $|G/S|$ is equal to the number of orbits of size 1, modulo p. Since $|G/S| \neq 0 \mod p$, there is at least one orbit of size 1, so we can choose $a \in G$ such that $xaS = aS$ for all $x \in P$. Then we have $a^{-1}xa \in S$ for all $x \in P$, so that $a^{-1}Pa \leq S$, and hence $P \leq aSa^{-1}$. Finally, note that aSa^{-1} is a Sylow p-subgroup of G.

To prove Part 3, let X be the set of all Sylow p-subgroups of G, and choose $S \in X$. By Part 2, G acts on X by conjugation, that is by $a * T = aTa^{-1}$ where $a \in G$, $T \in X$, and the number of Sylow p-subgroups is $|X| = \big|\mathrm{Orb}(S)\big|$, which divides G. Likewise, we can consider the action of S on X by conjugation. Since X is the disjoint union of the orbits, and the size of each orbit divides $|S| = p^m$, it follows that $|X|$ is equal to the number of orbits of size 1, modulo p. For $T \in X$, we have

$$|\mathrm{Orb}(T)| = 1 \iff aTa^{-1} = T \text{ for all } a \in S \iff S \leq N(T) = N_G(T).$$

Since S and T are Sylow p-subgroups of G, they are also Sylow p-subgroups of $N(T)$, and so they are conjugate in $N(T)$ by Part 2, and since $T \trianglelefteq N(T)$ it follows that $S = T$. Thus there is only one orbit of size 1, namely $\{S\}$, so we have $|X| \equiv 1 \mod p$, as required.

The Classification of Groups of Small Order

1.20 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 $q \not| \, p-1$ 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 $q \big| p-1$ (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.

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

1.22 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.

1.23 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 $\alpha\beta\alpha = \beta$.

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

Composition Series and Simple Groups

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

1.26 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 $1 \leq k \leq \ell$.

1.27 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

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

1.28 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.

1.29 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.

1.30 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

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

1.31 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 $\alpha = (a_1a_2a_3 \cdots a_r)\beta \in H$. Then $(a_1a_3a_r) = \alpha^{-1}(a_1a_2a_3)\alpha(a_1a_2a_3)^{-1} \in H$ 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 $\alpha = (a_1a_2a_3)(a_4a_5a_6)\beta \in H$. Then we have $(a_1a_4a_2a_6a_3) = \alpha^{-1}(a_1a_2a_4)\alpha(a_1a_2a_4)^{-1} \in H$ 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 $\alpha = (a_1a_2a_3)\beta \in H$ where β is a product of disjoint 2-cycles so that $\beta^2 = e$. Then $(a_1a_3a_2) = \alpha^2 \in H$ 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 $\alpha = (a_1a_2)(a_3a_4)\beta \in H$. Then $(a_1a_3)(a_2a_4) = \alpha^{-1}(a_1a_2a_3)\alpha(a_1a_2a_3)^{-1} \in H$. Let $\gamma = (a_1a_3)(a_2a_4)$ and choose b distinct from a_1, a_2, a_3, a_4. Then $(a_1a_3b) = \gamma(a_1a_2b)\gamma(a_1a_3b)^{-1} \in H$ and so $H = A_n$ by Case 1.

1.32 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.

1.33 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

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

1.34 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).

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

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

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

Solution: We know that every abelian group of order 8 is isomorphic to one of the groups $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Let G be a non-abelian group with $|G| = 8$. The elements in G can have order equal to 1, 2, 4 or 8. If there was an element of order 8 the G would be cyclic. If every non-identity element had order 2 then G would be abelian (since we would have $a^2 = b^2 = (ab)^2 = e$ hence $ab = a(ab)^2 b = a^2 bab^2 = ba$ for all a, b). Thus G must have an element of order 4. Choose $a \in G$ with $|a| = 4$.

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

Solution: Let G be a non-abelian group of order 12. By Cauchy's Theorem, we can choose $c \in G$ with $|c| = 3$. Let $H = \langle c \rangle$ and note that H is a Sylow 3-subgroup. When G acts on G/H by $a * (bH) = abH$, the corresponding representation $\rho : G \to \text{Perm}(G/H)$ is given by $\rho(a)(bH) = abH$. For $K = \text{Ker}(\rho)$, note that $K \trianglelefteq G$ and $K \leq H$ (since when $a \in K$ we have $abH = bH$ for all $b \in G$, hence $aH = H$, hence $a \in H$). Since $K \leq H$ and $|H| = 3$, either $K = \{e\}$ or $K = H$. If $K = \{e\}$ then we have $G \cong \rho(G) \leq \text{Perm}(G/H) \cong S_4$ so that G is isomorphic to a 12-element subgroup of S_4, and the only such subgroup is A_4, so we have $G \cong A_4$.

Suppose that $K = H$ so that $H \trianglelefteq G$. Since H is a Sylow 3-subgroup and $H \trianglelefteq G$, it follows that H is the only Sylow 3-subgroup, and so G has exactly 2 elements of order 3, namely c and c^2. Consider the centralizer $C(c)$. We have $H = \langle c \rangle \leq C(c) \leq G$. Recall that when G acts on itself by conjugation, we have $\text{Orb}(c) = \text{Cl}(c)$ and $\text{Stab}(c) = C(c)$ so that $|G/C(c)| = |\text{Cl}(c)|$. Since c and c^2 are the only two elements in G of order 3, either $\text{Cl}(c) = \{c\}$ or $\text{Cl}(c) = \{c, c^2\}$, so that $|G/C(c)| = |\text{Cl}(c)| = 1$ or 2, and hence $|C(c)| = 6$ or 12. In either case, we can choose an element $d \in C(c)$ with $|d| = 2$. Let $a = cd$ and note that since $|c| = 3$ and $|d| = 2$ and $d \in C(c)$ so that d and c commute, we have $|a| = 6$.

Since $|G/\langle a \rangle| = 2$ we have $\langle a \rangle \trianglelefteq G$. Choose $b \in G$ with $b \notin \langle a \rangle$. Note that G is the disjoint union $G = \langle a \rangle \cup \langle a \rangle b$. Since $\langle a \rangle \trianglelefteq G$ we have $bab^{-1} \in \langle a \rangle$, say $bab^{-1} = a^r$ with $r \in \mathbb{Z}_6$. Note that $b^2 \in \langle a \rangle$ (because if we had $b^2 \in \langle a \rangle b$ with say $b^2 = a^j b$, then we would have $b = a^j \in \langle a \rangle$), say $b^2 = a^s$ with $s \in \mathbb{Z}_6$. Since $b^2 = a^s$ and $bab^{-1} = a^r$ we have

$$a = a^s a\, a^{-s} = b^2 a\, b^{-2} = b(bab^{-1})b^{-1} = ba^r b^{-1} = (bab^{-1})^r = (a^r)^r = a^{r^2}.$$

Since $a^{r^2} = a$ and $|a| = 6$, we must have $r^2 = 1 \in \mathbb{Z}_6$ so that $r = \pm 1$. If we had $r = 1$ so that $bab^{-1} = a$, then we would have $ba = ab$, but then G would be abelian, so we must have $r = -1$. Thus $bab^{-1} = a^{-1}$, or equivalently, $aba = b$. Note that $s \neq \pm 1$ because if we had $b^2 = a$ or $b^2 = a^{-1}$ then we would have $|b| = 12$, but then G would be cyclic, hence abelian. Also $s \neq 2$ since if we had $b^2 = a^2$ then we would have $aba = b$, $abab = b^2 = a^2$, Also $s \neq 4$ since if we had $s = 4$ then we would have Thus either $s = 0$ so that $b^2 = e$ or $s = 3$ so that $b^2 = a^3$.

1.39 Example: Show that there is no simple group of order 30.

Solution: Suppose, for a contradiction, that G is a simple group of order 30. By the third Sylow theorem, the number of Sylow 5-subgroups of G divides 30 and is equal to 1 modulo 5, so it is equal to 1 or 6. If there was a unique Sylow 5-subgroup then it would be normal and so, since G is simple, there must be 6 Sylow 5-subgroups. Similarly, the number of Sylow 3-subgroups of G divides 60 and is equal to 1 modulo 3, so it is equal to 1 or 10, and there cannot be a unique Sylow 3-subgroup so there must be 10 Sylow 3-subgroups. Each Sylow 5-subgroup H has 5 elements, and the 4 non-identity elements generate H, so the union of the 6 Sylow 5-subgroups consists of the identity along with 24 distinct elements of order 5. Similarly, the union of the 10 Sylow 3-subgroups consists of the identity along with 20 distinct elements of order 3. Thus G has at least 24 elements of order 5 and 20 elements of order 3, which is not possible since G only has 30 elements.

1.40 Example: Classify, up to isomorphism, all groups of order 30.

Solution: We claim that every group of order 30 is isomorphic to one of the groups $\mathbb{Z}_{30}$, D_{15}, $\mathbb{Z}_3 \times D_5$ or $\mathbb{Z}_5 \times D_3$. Let G be a group with $|G| = 30$. As in the above example, we see that it is not possible for G to have both 6 Sylow 5-subgroups and 10 Sylow 3-subgroups, so either G has a unique (hence normal) Sylow 5-subgroup or G has a unique (hence normal) Sylow 3-subgroup. Let H be a Sylow 5-subgroup and let K be a Sylow 3-subgroup. Since either $H \trianglelefteq G$ or $K \trianglelefteq G$, it follows that $HK \leq G$, and since $|HK| = 15$ so that $|G/HK| = 2$, we must have $HK \trianglelefteq G$. Since $|HK| = 15$, it is cyclic (by Part 4 of Theorem 1.20). Let a be a generator of HK, so we have $|a| = 15$. By Cauchy's Theorem, we can choose $b \in G$ with $|b| = 2$. Since $\langle a \rangle = HK \trianglelefteq G$, each element in G can be written uniquely in the form $a^i b^j$ with $i \in \mathbb{Z}_{15}$ and $j \in \mathbb{Z}_2$, and we can choose $r \in \mathbb{Z}_{15}$ such that $bab^{-1} = a^r$. This determines the operation completely. Since $b^2 = e$ we have $a = b^2 a b^{-2} = b(bab^{-1})b^{-1} = ba^r b^{-1} = (bab^{-1})^r = (a^r)^r = a^{r^2}$. Since $|a| = 15$ and $a^{r^2} = a$ we must have $r^2 = 1 \mod 15$ and hence $r \in \{1, 4, 11, 14\} \mod 15$. When $r = 1$ so that $bab^{-1} = a$, that is $ba = ab$, the group G is abelian and we have $G \cong \mathbb{Z}_{30}$. When $r = 14 = -1$ so that $bab^{-1} = a^{-1}$, we have $G \cong D_{15}$ since $D_{15} = \langle \sigma, \tau \rangle$ with $|\sigma| = 15$, $|\tau| = 2$ and $\tau\sigma\tau^{-1} = \sigma^{-1}$. When $r = 4$ so that $bab^{-1} = a^4$ we have $G \cong \mathbb{Z}_3 \times D_5$ because $\mathbb{Z}_3 \times D_5 = \langle \alpha, \beta \rangle$ where $\alpha = (1, \sigma)$ and $\beta = (0, \tau)$ so that $|\alpha| = 15$, $|\beta| = 2$ and $\beta\alpha\beta^{-1} = (0, \tau) * (1, \sigma) * (0, \tau) = (1, \tau\sigma\tau) = (1, \sigma^4) = (1, \sigma)^4 = \alpha^4$. When $\alpha = 11$ we have $G \cong \mathbb{Z}_5 \times D_3$ because $\mathbb{Z}_5 \times D_3 = \langle \alpha, \beta \rangle$ where $\alpha = (1, \sigma)$ and $\beta = (0, \tau)$ so that $|\alpha| = 15$ and $|\beta| = 2$ and $\beta\alpha\beta = (0, \tau) * (1, \sigma) * (0, \tau) = (1, \tau\sigma\tau) = (1, \sigma^2) = (1, \sigma)^{11} = \alpha^{11}$