1.12 Groups of Small Order

1.12.1 Lemma. *Let p be a prime number. Any group with k subgroups of order p has $k(p-1)$ elements of order p.*

Proof. In a group of order p, all non-identity elements have order p. The Lagrange Theorem implies that distinct subgroups of order p must intersect trivially. Each subgroup of order p has a distinct set of $p-1$ elements of order p, so the total number of elements of order p is $k(p-1)$. □

1.12.2 Definition. For any $n \in \mathbb{N}$, the ***alternating group*** A_n is the group of even permutations of the finite set $[n] := \{1, 2, \dots, n\}$.

Since A_n is the kernel of the group homomorphism $\operatorname{sgn} : \mathfrak{S}_n \to \mu_n$, it is a normal subgroup of $\mathfrak{S}_n$.

1.12.3 Proposition. *Groups of order 12 have five isomorphism classes:*
- *the product of cyclic groups $\mathbb{Z}/\langle 3\rangle \times \mathbb{Z}/\langle 4\rangle \cong \mathbb{Z}/\langle 12\rangle$,*
- *the product of cyclic groups $\mathbb{Z}/\langle 2\rangle \times \mathbb{Z}/\langle 2\rangle \times \mathbb{Z}/\langle 3\rangle$,*
- *the alternating group A_4,*
- *the dihedral group D_6,*
- *the group generated by two elements f, g with relations $f^4 = 1$, $g^3 = 1$ and $fg = g^2 f$.*

Proof. Let G be a group of order $12 = 2^2 \cdot 3$. Consider a Sylow 2-subgroup H and a Sylow 3-subgroup K. Since $|H| = 4$ and $|K| = 3$, Example 1.6.12 establishes that $H \cong \mathbb{Z}/\langle 4\rangle$ or $H \cong \mathbb{Z}/\langle 2\rangle \times \mathbb{Z}/\langle 2\rangle$, and $K \cong \mathbb{Z}/\langle 3\rangle$. The Third Sylow Theorem shows that the number of Sylow 2-subgroups is either 1 or 3, and that the number of Sylow 3-subgroups is either 1 or 4.

We first claim that at least one of H or K is normal. Suppose that K is not normal. Hence, the subgroup K has four conjugate subgroups $K_1 := K$, K_2, K_3, K_4. Lemma 1.12.1 implies that there are $4 \cdot 2 = 8$ elements of order 3. We deduce that H consists of remaining $12 - 8 = 4$ elements. This shows that there is only one Sylow 2-subgroup, so the subgroup H is normal.

Since $H \cap K = \{e\}$, each element in HK has a unique expression as a product hk where $h \in H$ and $k \in K$. As $|G| = 12$, it follows that $G = HK$. If H is normal, then the group K acts on H by conjugation. We claim that this action, together with the structure of H and K, determine the structure of G. Similarly, when K is normal, the group H acts on K and this action determines G.

Case 1: Suppose that both subgroups H and K are normal. It follows that $G \cong H \times K$ so $G \cong \mathbb{Z}/\langle 3\rangle \times \mathbb{Z}/\langle 4\rangle$ or $G \cong \mathbb{Z}/\langle 2\rangle \times \mathbb{Z}/\langle 2\rangle \times \mathbb{Z}/\langle 3\rangle$.

Case 2: Suppose that the subgroup H is normal but the subgroup K is not. Conjugation action of the group G on the set $\{K_1, K_2, \dots, K_4\}$ determines a group homomorphism $\varphi : G \to \mathfrak{S}_4$. We claim that the map φ defines an isomorphism from G to the alternating group $A_4 \subset \mathfrak{S}_4$.

When H is normal and K is not, the subgroup H is the Klein 4-group, as it is the Sylow 2-subgroup of A_4.

The stabilizer of the subgroup K_i under the conjugation action is the normalizer $N(K_i)$ which contains K_i. Example 1.9.13 shows that $|N(K_i)| = 3$, so $N(K_i) = K_i$. Since the only element common to all K_i is the identity, only the identity stabilizes all of these subgroups. Thus, the map φ is injective and the group G is isomorphic to its image in $\mathfrak{S}_4$.

Since G has four subgroups of order 3, it contains 8 elements of order 3 and these elements certainly generate the group. If $g \in G$ has order 3, then $\varphi(g)$ is a permutation of order 3 in $\mathfrak{S}_4$. The permutations of order 3 are even. Therefore, we have $\mathrm{Im}(\varphi) \subseteq A_4$. Since $|G| = |A_4|$, the two groups are equal.

Case 3: Suppose that the subgroup K is normal, but the subgroup H is not. The subgroup H acts on subgroup K by conjugation and conjugation by an element of H is an automorphism of K. Let $g \in G$ be a generator for K, so we have $g^3 = e$. There are precisely two automorphisms of subgroup K: the identity and the automorphism that interchanges g and g^2.

Suppose that the subgroup H is cyclic. Let $f \in G$ be a generator for H, so we have $f^4 = e$. Since G is not abelian, $fg \neq gf$ and so conjugation by f is not the trivial automorphism of K. It follows that $fgf^{-1} = g^2$. One verifies that these relations define a group of order 12.

The last possibility is that H is isomorphic to the Klein 4-group. Since there are only two automorphisms of the group K, there is a nonidentity element $f \in H$ that acts trivially: $fgf^{-1} = g$. Since G is not abelian, there is also an element $h \in H$ which operates nontrivially: $hgh^{-1} = g^2$. The elements of H are $\{1, f, h, fh\}$ and the relations $f^2 = h^2 = e$ and $fh = hf$ hold. The element fg has order 6 and $h(fg)h^{-1} = fg^2 = g^2 f = (fg)^{-1}$. Finally, the three relations $(fg)^6 = e$, $h^2 = e$, and $h(fg)h^{-1} = (fg)^{-1}$ define the dihedral group D_6. □

1.12.4 Remark. It is possible to completely classify finite groups of small order up to isomorphism. For example, the SmallGrp package in the GAP software system gives access to the 423 164 062 groups of order at most 2000 (except groups of order 1024).

There are 49 487 365 422 of order 1024.

Table 1.1: Number of groups of given order

	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9	+10	+11	+12	+13	+14	+15	+16	+17	+18	+19
0+	0	1	1	1	2	1	2	1	5	2	2	1	5	1	2	1	14	1	5	1
20+	5	2	2	1	15	2	2	5	4	1	4	1	51	1	2	1	14	1	2	2
40+	14	1	6	1	4	2	2	1	52	2	5	1	5	1	15	2	13	2	2	1
60+	13	1	2	4	267	1	4	1	5	1	4	1	50	1	2	3	4	1	6	1
80+	52	15	2	1	15	1	2	1	12	1	10	1	4	2	2	1	231	1	5	2

1.13 Simple Groups

A group that contains a proper normal subgroup can be broken into smaller groups. From this perspective, the basic building blocks of all finite groups are those groups without a proper normal subgroup

1.13.1 Definition. A group is ***simple*** when it is nontrivial and its only normal subgroups are the trivial subgroup and the whole group.

The classification of finite simple groups proves that every finite simple group is either cyclic, alternating, belongs to a infinite class called the groups of Lie type (essentially matrix groups over finite fields), or else it is one of twenty-six sporadic groups. The smallest sporadic group has order $2^4 \cdot 3^2 \cdot 4 \cdot 11 = 7920$ and the largest, known as the Monster group, has order $2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^2 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \approx 8 \cdot 10^{53}$.

1.13.2 Proposition. *A nontrivial group G is simple if and only if every nontrivial group homomorphism from G is injective.*

Proof.
($\Rightarrow$) Suppose that G is a simple group. Let $\varphi : G \to H$ is a nontrivial group homomorphism. There exists $g \in G$ such that $\varphi(g) \neq e_H$, so the kernel of φ is a proper subgroup of G. Since G is simple, the kernel of φ is trivial which means that φ is injective.
($\Leftarrow$) Suppose that all nontrivial group homomorphisms from G are injective. Given a proper normal subgroup K of G, the canonical group homomorphism $\pi : G \to G/K$ has kernel K. Since π is injective, the kernel of π must be trivial, so G is simple. □

1.13.3 Proposition. *An abelian group is simple if and only if its order is a prime number.*

Proof.
($\Rightarrow$) Suppose that p is prime number and G is a group of order p. By the Lagrange Theorem, any subgroup has order dividing p. Hence, the only subgroups are $\{e_G\}$ and G.
($\Leftarrow$) Suppose that the abelian group G is simple. Every subgroup of G is normal, because G is abelian. Choose $e \neq g \in G$. Since G is simple, it follows that $G = \langle g \rangle$ as otherwise $\langle g \rangle$ is a proper subgroup. Were g to have infinite order, all powers of g would be distinct and $\langle g^2 \rangle$ would be a proper subgroup of G which contradicts the simplicity hypothesis. Hence, g has finite order m. Were m to have a nontrivial factorization $m = k\ell$, the subgroup $\langle g^k \rangle$ would be proper which again contradicts the simplicity hypothesis. We conclude that G has prime order. □

1.13.4 Theorem. *Every simple group of order* 60 *is isomorphic to* A_5.

Proof. Let G be a simple group of order $60 = 2^2 \cdot 3 \cdot 5$. First, suppose that G has a subgroup H such that $[G : H] = 5$. Left multiplication of the group G on the coset space G/H gives a group homomorphism $\varphi : G \to \mathfrak{S}_{G/H} \cong \mathfrak{S}_5$. The kernel of the map φ is a normal subgroup of G. Since G is simple, this kernel is either $\{e\}$ or G. Given $g \in \operatorname{Ker}(\varphi)$, we have $gH = H$ or $g \in H$, so we deduce that $\operatorname{Ker}(\varphi) = \{e\}$. Thus, the map φ embeds G into $\mathfrak{S}_5$

Next, suppose that $\varphi(G) \not\subseteq A_5$. It follows that the image $\varphi(G)$ contains an odd permutation and the map $\operatorname{sgn}|_{\varphi(G)} : \varphi(G) \to \mu_2$ is surjective. The kernel of this restriction is a normal subgroup of $\varphi(G)$ having index 2. However, the group $G \cong \varphi(G)$ is simple, so such a subgroup cannot exist. Thus, all elements in the image $\varphi(G)$ are even permutations and $\varphi(G) \subseteq A_5$. Since $|G| = 60 = |A_5|$, we conclude that $\varphi(G) = A_5$ and $G \cong A_5$.

We still must show that the subgroup H exists. To that end, we claim that each proper subgroup of G has index at least 5. Suppose that H' is a subgroup of G such that $r := [G : H']$. As above, left multiplication of the group G on the coset space G/H give a injective group homomorphism $\varphi' : G \to \mathfrak{S}_{G/H'} \cong \mathfrak{S}_r$. Since the Lagrange Theorem implies that $|G| = 60$ divides $r! = |\mathfrak{S}_r|$, we see that $r \geqslant 5$.

It remains to show that G has a subgroup of index 5. For any prime number p, let n_p denote the number of Sylow p-subgroups in G. The Lagrange Theorem and Third Sylow Theorem establish that $n_2 \in \{1, 3, 5, 15\}$, $n_3 \in \{1, 4, 10\}$, and $n_5 \in \{1, 6\}$. Since G is simple, the nontrivial Sylow subgroups are not normal, so n_2, n_3, and n_5 are all larger than 1. Example 1.9.13 demonstrates that each n_p is the index of a subgroup of G, so the previous paragraph implies that n_2, n_3, and n_5 are all larger than or equal to 5. Thus, we need to consider the cases $n_2 \in \{5, 15\}$, $n_3 \in \{10\}$, and $n_5 \in \{6\}$.

- Suppose that $n_5 = 5$. Example 1.9.13 already proves that there is a subgroup of G with index 5.
- Suppose that $n_5 = 15$. Lemma 1.12.1 shows that the group G has $n_3 \cdot 2 = 20$ elements of order 3 and $n_5 \cdot 4 = 24$ elements of order 5. This leaves at most $60-(20+24) = 16$ elements that can belong to the Sylow 2-subgroups. The 15 Sylow 2-subgroups are squeezed into this 16-element subset of G. Each Sylow 2-subgroup of G has order 4 and thus is abelian. The Sylow 2-subgroups cannot all have trivial pairwise intersections (otherwise they would contain $3 \cdot 15 = 45$ nonidentity elements). Choose two distinct Sylow 2-subgroups P and Q which have a nontrivial intersection. Set $I := P \cap Q$. Both P and Q are abelian, so I is a normal subgroup in each. It follows that the normalizer of I in G contain both P and Q, so it has size properly divisible by 4. The normalizer of I is not all of G because the group G has no proper nontrivial normal subgroups. Since proper subgroups of G have order 1, 2, 3, 4, 6, or 12, the normalizer of I has order 12 and we have $[G : I] = 5$. □

Since the number of Sylow 2-subgroups in A_5 is 5, we learn a posteriori that $n_5 = 5$.