

4 Classifications & Constructions

Copyright © 2025 by Gregory G. Smith
Last updated: 2025-09-22

There are several distinct strategies for understanding all groups up to isomorphism. For instance, one can enumerate all possibilities, tabulate the basic building blocks of group theory, or define groups using generators and relations.

4.0 Groups of Small Order

It is possible to completely classify finite groups of small order up to isomorphism. We illustrate some of the rudimentary ideas by classifying the groups of order 12.

4.0.1 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 subgroup of order p , all $p - 1$ nonidentity elements have order p . The Lagrange Theorem implies that distinct subgroups of order p must intersect trivially. Thus, the total number of elements of order p is $k(p - 1)$. $\square$

4.0.2 Definition. Let n be a nonnegative integer. The *alternating group* A_n is the subgroup of $\mathfrak{S}_n$ consisting of all even permutations.

Since A_n is the kernel of the group homomorphism $\text{sgn}: \mathfrak{S}_n \rightarrow \mu_2$, it is a normal subgroup of $\mathfrak{S}_n$.

4.0.3 Proposition. *Groups of order 12 have five isomorphism classes:*

(cyclic) $\mathbb{Z}/\langle 12 \rangle \cong \mathbb{Z}/\langle 3 \rangle \times \mathbb{Z}/\langle 4 \rangle$

(product) $\mathbb{Z}/\langle 2 \rangle \times \mathbb{Z}/\langle 2 \rangle \times \mathbb{Z}/\langle 3 \rangle$

(alternating) A_4

(dihedral) D_6

(dicyclic) *the group generated by two elements f and g satisfying the relations $f^4 = e$, $g^3 = e$, and $fg = g^2f$.*

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 2.2.12 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. It follows that K has four conjugate subgroups $K_1 := K, K_2, K_3, K_4$. Lemma 4.0.1 implies that there are $4 \cdot 2 = 8$ elements of order 3. We deduce that the subgroup H contains the 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 can be expressed uniquely as a product hk where $h \in H$ and $k \in K$. As $|G| = 12$, it follows that $G = HK$. If the subgroup H is normal, then the subgroup K

acts on H by conjugation. We claim that this action, together with the structure of H and K , determines the structure of the group 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 H is normal, but K is not. Proposition 2.1.6 implies that the conjugation action of the group G on the set $\{K_1, K_2, K_3, K_4\}$ defines a group homomorphism $\varphi: G \rightarrow \mathfrak{S}_4$. We claim that the map φ is an isomorphism from G to $A_4 \subset \mathfrak{S}_4$.

The stabilizer of each subgroup K_i under conjugation is the normalizer $N(K_i)$ which contains K_i . Example 3.1.11 shows that $|N(K_i)| = 3$, so $N(K_i) = K_i$. As the unique element common to all K_i , only the identity stabilizes all of these subgroups. Therefore, the map φ is injective and 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 G . If the element g in G has order 3, then its image $\varphi(g)$ is a permutation of order 3 in $\mathfrak{S}_4$. The permutations of order 3 are even, so we deduce that $\text{Im}(\varphi) \subseteq A_4$. Since $|G| = |A_4|$, the two groups are equal.

Case 3: Suppose that K is normal, but H is not. The subgroup H acts on 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 H is cyclic. Let f in G be a generator for H , so $f^4 = e$. 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 final possibility is that the subgroup 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 $h(fg)h^{-1} = fg^2 = g^2f = (fg)^{-1}$. Lastly, the relations $(fg)^6 = e$, $h^2 = e$, and $h(fg)h^{-1} = (fg)^{-1}$ define the dihedral group D_6 . $\square$

4.0.4 Remark. 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 groups of order 1024.

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 .

Figure 4.1: Number of groups of order less than 100

	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9
0+	0	1	1	1	2	1	2	1	5	2
10+	2	1	5	1	2	1	14	1	5	1
20+	5	2	2	1	15	2	2	5	4	1
30+	4	1	51	1	2	1	14	1	2	2
40+	14	1	6	1	4	2	2	1	52	2
50+	5	1	5	1	15	2	13	2	2	1
60+	13	1	2	4	267	1	4	1	5	1
70+	4	1	50	1	2	3	4	1	6	1
80+	52	15	2	1	15	1	2	1	12	1
90+	10	1	4	2	2	1	231	1	5	2

4.1 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

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

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

Proof. Suppose that G is a simple group. Let $\varphi: G \rightarrow H$ be a nontrivial group homomorphism. There exists an element 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.

Conversely, suppose that all nontrivial group homomorphisms from G are injective. Given a proper normal subgroup K of G , the canonical group homomorphism $\pi: G \rightarrow G/K$ has kernel K . Since π is injective, the kernel of π must be trivial, so G is simple. $\square$

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

Proof. Suppose that p is prime number and G is a group such that $|G| = p$. By the Lagrange Theorem, any subgroup has order dividing p . Hence, the only subgroups are $\langle e_G \rangle$ and G .

Conversely, suppose that the abelian group G is simple. Every subgroup of G is normal, because G is abelian. Choose an element $g \neq e$ 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 , contradicting the simplicity hypothesis. Hence, the element g has finite order m . Were m to have a nontrivial factorization $m = k\ell$, the subgroup $\langle g^k \rangle$ would be proper, again contradicting the simplicity hypothesis. We conclude that G has prime order. $\square$

4.1.4 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 $\varphi: G \rightarrow \mathfrak{S}_{G/H} \cong \mathfrak{S}_5$. The kernel of the map φ is a normal subgroup of G . Since G is simple, this kernel is either $\{e\}$ or G . For any element g in $\text{Ker}(\varphi)$, we have $gH = H$ or $g \in H$, so $\text{Ker}(\varphi) = \{e\}$. 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 $\text{sgn}|_{\varphi(G)}: \varphi(G) \rightarrow \mu_2$ is

The complete classification of finite simple groups consists of tens of thousands of pages in several hundred journal articles written by about 100 authors, published mostly between 1955 and 2004.

There are no nonabelian simple groups of order less than 60.

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 $\varphi' : G \rightarrow \mathfrak{S}_{G/H'} \cong \mathfrak{S}_r$. Since the Lagrange Theorem implies that $|G| = 60$ divides $r! = |\mathfrak{S}_r|$, we see that $r \geq 5$.

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 3.1.11 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. As $n_3 = 10$ and $n_5 = 6$, we need to consider the two cases $n_2 \in \{5, 15\}$.

($n_5 = 5$) Example 3.1.11 already proves that there exists a subgroup of G with index 5.

($n_5 = 15$) Lemma 4.0.1 establishes that 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 for 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 which is absurd. Choose two distinct Sylow 2-subgroups P and Q that 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 $[G : I] = 5$. $\square$

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

4.1.5 Remark. 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”, 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 $2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^2 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \approx 8 \cdot 10^{53}$.

4.2 Free Groups

Roughly speaking, a free group over a set X is the largest possible group generated by X ; the only relations are the ones required by the group axioms.

4.2.1 Definition. A group F is *free* over a set $X \subseteq F$ if, for any group G and any map $\xi: X \rightarrow G$, there is a unique group homomorphism $\varphi: F \rightarrow G$ such that $\varphi(x) = \xi(x)$ for all $x \in X$.

4.2.2 Proposition. Free groups over the sets X and Y are isomorphic if and only if we have $|X| = |Y|$.

Proof. Let F and G be free groups over X and Y and let $\zeta: X \rightarrow F$ and $\eta: Y \rightarrow G$ be the canonical inclusion maps. Since $|X| = |Y|$, there is a bijection $\beta: X \rightarrow Y$. Applying the definition of a free group to the maps $\eta \circ \beta: X \rightarrow G$ and $\zeta \circ \beta^{-1}: Y \rightarrow F$, we obtain group homomorphisms $\varphi: F \rightarrow G$ and $\theta: G \rightarrow F$ that restrict to $\zeta \circ \beta$ and $\eta \circ \beta^{-1}$ respectively. Hence, the map $\theta \circ \varphi: F \rightarrow F$ restricts to the identity on X and the map $\varphi \circ \theta: G \rightarrow G$ restricts to the identity on Y . Therefore, the uniqueness part of the definition implies that $\theta \circ \varphi = \text{id}_F$ and $\varphi \circ \theta = \text{id}_G$, so the group homomorphisms φ and θ are mutually inverse and $F \cong G$. $\square$

4.2.3 Definition. The *rank* of the free group over a set is just the cardinality of the set.

Nothing in their definition ensures that free groups actually exist.

4.2.4 Proposition. There exists a free group over any nonempty set.

Proof. Let X be a nonempty set and let $X^{-1} := \{x^{-1} \mid x \in X\}$ be a set disjoint from X with the same cardinality. A *word* in $X \sqcup X^{-1}$ is a finite sequence of symbols $w := x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_r^{\epsilon_r}$ where $x_i \in X$, $\epsilon_i = \pm 1$, and r is a nonnegative integer. When $r = 0$, the sequence is empty and the *empty word* is denoted by 1. By definition, the *product* of the words $w := x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_r^{\epsilon_r}$ and $v := y_1^{\delta_1} y_2^{\delta_2} \cdots y_s^{\delta_s}$ is given by concatenation $wv := x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_r^{\epsilon_r} y_1^{\delta_1} y_2^{\delta_2} \cdots y_s^{\delta_s}$. The *inverse* of the word w is defined to $w^{-1} := x_r^{-\epsilon_r} \cdots x_2^{-\epsilon_2} x_1^{-\epsilon_1}$.

Let W be the set of all words in $X \sqcup X^{-1}$. Two words w and v are equivalent $w \sim v$ if it is possible to pass from one word to the other by a finite sequence of two basic operations: the insertion of an xx^{-1} or $x^{-1}x$ as consecutive elements, or the deletion of consecutive elements of the form xx^{-1} or $x^{-1}x$. It follows immediately that this relation is reflexive, symmetric, and transitive. The equivalence class containing w is denoted $[w]$.

Let $F := W/\sim$ be the set of all equivalence classes. Given $w \sim w'$ and $v \sim v'$, we see that $wv \sim w'v'$, so the product $[w][v] = [wv]$

This definition mimics the construction of a linear map from a vector space with basis to another vector space. Specifically, if $\{v_1, v_2, \dots, v_n\}$ is a basis of a vector space V and W is a vector space with $w_1, w_2, \dots, w_n \in W$, then there is a unique linear map $T: V \rightarrow W$ such that $T(v_i) = w_i$ for all $1 \leq i \leq n$.

Proposition 4.2.2 proves that any two free groups over the same set are isomorphic.

The number r is the *length* of the word and we set $|w| := r$.

By definition, we have $w1 = w = 1w$.

is well-defined. Since we have $(wv)u = wvu = w(vu)$, it follows that $([w][v])[u] = [(wv)u] = [w(vu)] = [w]([v][u])$. We also have $[w][1] = [w] = [1][w]$ and $[w][w^{-1}] = [ww^{-1}] = [1]$. Therefore, F is a group and the inclusion map $X \rightarrow F$ is given by $x \mapsto [x]$.

To show that F is free over X , let G be an arbitrary group and let $\xi: X \rightarrow G$ be any map. Consider the map $\tilde{\varphi}: W \rightarrow G$ defined by $\tilde{\varphi}(x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_r^{\varepsilon_r}) := \xi(x_1)^{\varepsilon_1} \xi(x_2)^{\varepsilon_2} \cdots \xi(x_r)^{\varepsilon_r}$. When $w \sim w'$, we see that $\tilde{\varphi}(w) = \tilde{\varphi}(w')$ because products like gg^{-1} and $g^{-1}g$ equal e_G in the group G . Hence, we obtain a well-defined map $\varphi: F \rightarrow G$. Moreover, we have

$$\varphi([w][v]) = \varphi([wv]) = \tilde{\varphi}(wv) = \tilde{\varphi}(w)\tilde{\varphi}(v) = \varphi([w])\varphi([v])$$

so φ is a group homomorphism extending ξ . It is clearly unique.

To see that the map $x \mapsto [x]$ defines a bijection from X to $[X]$, let G be any group with $|G| \geq |X|$ and let $\xi: X \rightarrow G$ be an injection. Since $\varphi([x]) = \xi(x)$ for all $x \in X$, we deduce that $x \mapsto [x]$ must define a bijection. $\square$

The equivalence classes of words arising in the construction of $F := W/\sim$ have distinguished representatives.

4.2.5 Definition. A word is *reduced* if it contains neither xx^{-1} nor $x^{-1}x$ as a subsequence.

4.2.6 Proposition. *Each equivalence class of words contains a unique reduced word.*

Proof. We have $x^\varepsilon x^{-\varepsilon} \sim 1$ for all $x \in X \sqcup X^{-1}$. Since deleting such a pair reduces the length, each equivalence class contains a reduced word, namely one of minimal length.

Suppose that an equivalence class contains two distinct reduced words w and w' . There exists a sequence $w = w_0, w_1, \dots, w_\ell = w'$ of words such that w_{i-1} and w_i are related by a basic operation for all $1 \leq i \leq \ell$. Choose such a sequence that minimizes the sum $\sum_{i=0}^{\ell} |w_i|$. Two words related by a basic operation differ in length by 2 and cannot both be reduced, so $\ell > 1$. Choose an index i so that the length of the word w_i is maximal. It follows that $0 < i < \ell$ and $|w_{i-1}| = |w_{i+1}| = |w_i| - 2$. If the two deleted subsequences of w_i are disjoint, then reversing the order of the substitutions produces another sequence with $|w_i| = |w_{i-1}| - 2$ contradicting the minimality of the chosen sequence. If these two subsequences are not disjoint, then either they are equal or they are the subsequences of $x^\varepsilon x^{-\varepsilon}$, $x^{-\varepsilon} x^\varepsilon$ of $x^\varepsilon x^{-\varepsilon} x^\varepsilon$ of w_i . In both cases, we have $w_{i-1} = w_{i+1}$ so we can shorten the sequence again contradicting minimality. $\square$

4.3 Presentation of a Group

Free groups allow one to describe any group in terms of generators and relations. Before formalizing this idea, we collect a few easy consequences of the construction of free groups.

4.3.1 Corollary. *When $|X| \geq 2$, the free group over X is nonabelian.*

Proof. For any two distinct elements $x, y \in X$, the word $x^{-1}y^{-1}xy$ is reduced which means $x^{-1}y^{-1}xy \neq 1$ so $xy \neq yx$. $\square$

4.3.2 Corollary. *Every element, except for the identity, in a free group has infinite order.*

Proof. Let x be an element in X . For any positive integer n , the word $\underbrace{xx \cdots x}_{n\text{-times}}$ is reduced, so not equal to 1 in the free group over X . $\square$

4.3.3 Corollary. *Let F be the free group over the set $\{x, y\}$. The three elements $u := x^2$, $v := y^2$, and $w := xy$ generate a subgroup isomorphic to the free group over the set $\{u, v, w\}$.*

Proof. Let G be the free group on $\{u, v, w\}$. The map defined by $u \mapsto x^2$, $v \mapsto y^2$, and $w \mapsto xy$ determines a group homomorphism $\varphi: G \rightarrow F$. The images of uv, vu, uw, wu, vw and wv are all reduced words in $\{x, y, z\}$, so a reduced word in $\{u, v, w\} \sqcup \{u^{-1}, v^{-1}, w^{-1}\}$ maps to a reduced word in $\{x^2, y^2, xy\} \sqcup \{x^{-1}, y^{-1}, (xy)^{-1}\}$. It follows that the kernel of the map φ is trivial and the map φ is injective. $\square$

4.3.4 Proposition. *Every group is a quotient of a free group.*

Proof. Let X be a set for which there exists a bijection $\xi: X \rightarrow G$ and let F be the free group on X . Hence, there exists a surjective group homomorphism $\varphi: F \rightarrow G$, so $G \cong F / \text{Ker}(\varphi)$. $\square$

4.3.5 Definition. A **presentation** of a group G is given by surjective homomorphism ψ from a free group F over a set X to G . We call the set X the **generators** of G and a set R such that $\langle R \rangle = \text{Ker}(\psi)$ **relations**. One often writes $G = \langle X \mid R \rangle$.

The free group over the singleton $\{x\}$ is an infinite cyclic group and, thereby, isomorphic to $\mathbb{Z}$.

Informally, $\langle X \mid R \rangle$ is the ‘largest’ group that is generated by X in which all of the words $w \in R$ represent the identity element.

4.3.6 Example. The cyclic group of order 6 has at least two different presentations: $\langle x \mid x^6 \rangle$ or $\langle a, b \mid a^3, b^2, a^{-1}b^{-1}ab \rangle$. $\diamond$

4.3.7 Example. The free group has a presentation $\langle X \mid \emptyset \rangle$. $\diamond$

4.3.8 Theorem (Dyck). *Let $G := \langle x_1, x_2, \dots, x_n \mid r_j \text{ for all } j \in J \rangle$. For any group $H := \langle h_1, h_2, \dots, h_n \rangle$ such that $r_j(h_1, h_2, \dots, h_n) = e_H$ for all $j \in J$, there exists a surjective group homomorphism $\varphi: G \rightarrow H$ such that $\varphi(x_i) = h_i$ for all $1 \leq i \leq n$.*

Walther von Dyck (1882) provided the first systematic study of presentations of groups by generators and relations.

Proof. Let F be the free group over the set $\{x_1, x_2, \dots, x_n\}$. There is a group homomorphism $\varphi: F \rightarrow H$ with $\varphi(x_i) = h_i$. Since we have $r_j(h_1, h_2, \dots, h_n) = e_H$ for all $j \in J$, it follows that $r_j \in \text{Ker}(\varphi)$. By the First Isomorphism Theorem, the map φ induces a surjective group homomorphism $G = F/\text{Ker}(\varphi) \rightarrow H$. $\square$

4.3.9 Example. For all integers n greater than 1, we claim that the dihedral group D_n has a presentation $\langle x, y \mid x^n, y^2, yxyx \rangle$. Let G be the group defined by this presentation. Sending x to a rotation by $2\pi/n$ and y to a reflection, Theorem 4.3.8 gives a surjective group homomorphism $\varphi: G \rightarrow D_n$. We see that $|G| \geq 2n$. The subgroup $\langle x \rangle$ has order at most n , because $x^n = e_G$. The relation $yxy^{-1} = x^{-1}$ implies that $\langle x \rangle$ is a normal subgroup of G . It follows that $G/\langle x \rangle$ is generated by the image of y . Finally, the equation $y^2 = e_G$ shows that $|G/\langle x \rangle| \leq 2$. We conclude that $|G| = |\langle x \rangle| |G/\langle x \rangle| \leq 2n$. Since $|G| = 2n$, the map φ is bijective and, thereby, an isomorphism. $\diamond$

4.3.10 Remark. Given integer ℓ, m , and n such that $1 < \ell \leq m \leq n$, the group $G := \langle x, y, z \mid x^\ell, y^m, z^n, xyz \rangle$ is finite if and only if

$$\frac{1}{|G|} = \frac{1}{\ell} + \frac{1}{m} + \frac{1}{n} - 1 > 0.$$

This condition is satisfied only when $\ell = m = 2$ and $n \geq 2$, or $\ell = 2$, $m = 3$, and $3 \leq n \leq 5$.

4.3.11 Remark. We now are at the beginning of combinatorial group theory which explores how much can be said about a group given a presentation.

A group G has a solvable word problem if it has a presentation $G = \langle X \mid R \rangle$ such that there exists an algorithm to determine whether an arbitrary word is equal to the identity. Novikov (1955) showed that there is a finitely presented group for which the word problem is undecidable.

Presentations play an important role in algebraic topology. The Van Kampen Theorem yields presentations for fundamental groups. Moreover, topological techniques provide a “natural” prove of the Nielsen–Schreier Theorem: every subgroup of a free group is free.

One can introduce a metric: the word metric measures the length of the shortest path in the Cayley graph.

4.4 Exercises

4.4.1 Problem. Determine which of the following statements are true. If a statement is false, then provide a counterexample.

- i. When P is a Sylow p -subgroup of a group G , it follows that P is the only Sylow p -subgroup of its normalizer $N_G(P)$.
- ii. The permutation group $\mathfrak{S}_4$ has no normal subgroups of size 6 or 8.
- iii. The free group over a singleton is isomorphic to $\mathbb{Z}$.
- iv. Every group of order 35 is cyclic.
- v. No group of order p^r where p is prime and the integer r is greater than 1 is simple.
- vi. There are at most 5 isomorphism classes of groups of order 20.
- vii. The free group over a set of two elements is isomorphic to the product of two infinite cyclic groups.
- viii. Two elements f and g of a group generate the same subgroup as fgf^2 and fgf^3 .
- ix. The element g^2f^2 is in the normal subgroup generated by fg and its conjugates.
- x. The group generated by f , g , and h with the single relation $gfgh^{-2} = e$ is actually a free group.

Can the false statements be salvaged in some way? In other words, can one find a closely related nontrivial true statement.

4.4.2 Problem. Let p be a prime number. Prove that a group of order $2p$ is either cyclic or dihedral.

4.4.3 Problem. Prove that there are no simple groups of order 80, 96, or 1000.

4.4.4 Problem. Let $\hat{\mathbb{C}} := \mathbb{C} \sqcup \{\infty\}$ be the extended complex plane. Consider the two functions $f: \hat{\mathbb{C}} \rightarrow \hat{\mathbb{C}}$ and $g: \hat{\mathbb{C}} \rightarrow \hat{\mathbb{C}}$ defined, for all z in $\hat{\mathbb{C}}$, by $f(z) := z + 2$ and $g(z) := z/(2z + 1)$ respectively.

- i. Prove that f and g are bijections and, thereby, elements of the symmetric group on the set $\hat{\mathbb{C}}$.
- ii. Show that any nonzero power of f maps the interior of the unit circle $|z| = 1$ to the exterior. Similarly, show that any nonzero power of g maps the exterior of the unit circle to the punctured interior (a point is removed from the interior).
- iii. Prove that the subgroup of the symmetric group on $\hat{\mathbb{C}}$ generated by functions f and g is free.

The Riemann sphere is a geometric model of the extended complex plane. Topologically, it is the one-point compactification of the complex plane.