Algebra I, Fall 2003: Section 7. Universal Objects: Free Groups, Generators, and Relations.

7.1 Universal Objects.

We begin with a somewhat cryptic definition, whose meaning will soon become clear.

> A *free object* is the mother of all objects of that type, in the sense that every object of that type is a quotient of the free object.

As a simple example, consider the set $\mathcal{V}_n$ of all vector spaces over $\mathbb{R}$ that have dimension $\dim_{\mathbb{R}} V \leq n$, which is the same as saying V has "n generators":

$$\text{(1)} \qquad \text{There exist } \mathbf{v}_1, \ldots, \mathbf{v}_n \in V \text{ such that } V = \left\{ \sum_{i=1}^{n} c_i \mathbf{v}_i : c_i \in \mathbb{R} \right\}$$

These "generators" are not required to be independent, so the $\mathbf{v}_i$ need not be a basis and in fact some generators could be the zero vector; therefore the coefficients c_i need not be unique.

7.1.1 Example. A free object for the class of vector spaces $\mathcal{V}_n$ is the familiar Euclidean vector space of n-tuples $\mathbb{R}^n = \{\mathbf{x} = (x_1, \ldots, x_n) : x_i \in \mathbb{R}\}$. Let $\mathcal{X} = \{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ be the standard basis vectors $\mathbf{e}_i = (0, \ldots, 0, 1, 0, \ldots, 0)$; then we have a unique decomposition $\mathbf{x} = x_1\mathbf{e}_1 + \ldots + x_n\mathbf{e}_n$ for every $\mathbf{x} = (x_1, \ldots, x_n)$ in $\mathbb{R}^n$. Given any $V \in \mathcal{V}_n$ and any set of generators $\mathbf{v}_1, \ldots, \mathbf{v}_n$, there is a uniquely defined map $\phi : \mathbb{R}^n \to V$ such that $\phi(\mathbf{e}_i) = \mathbf{v}_i$, namely

$$\text{(2)} \qquad \phi(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i \mathbf{v}_i \qquad \text{for all } \mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n$$

This is a well-defined $\mathbb{R}$-*linear map* (a homomorphism of vector spaces) and it is surjective since the $\mathbf{v}_i$ span V. This already shows that every $V \in \mathcal{V}_n$ is a homomorphic image of the particular vector space $\mathbb{R}^n$, but we can say more. $W = \ker \phi = \{\mathbf{x} \in \mathbb{R}_n : \phi(\mathbf{x}) = \mathbf{0}\}$ is a vector subspace in $\mathbb{R}^n$ and we may form the quotient vector space $\mathbb{R}^n/W = (\text{all additive cosets } \mathbf{x}+W)$, in which

$$\begin{aligned} (\mathbf{x} + W) + (\mathbf{y} + W) &= (\mathbf{x} + \mathbf{y}) + W \qquad \text{for all } \mathbf{x}, \mathbf{y} \in \mathbb{R}^n \\ \lambda \cdot (\mathbf{x} + W) &= (\lambda \mathbf{x}) + W \qquad \text{for all } \lambda \in \mathbb{R},\ \mathbf{x} \in \mathbb{R}^n \end{aligned}$$

The quotient map $\pi : \mathbb{R}^n \to \mathbb{R}^n/W$, defined via $\pi(\mathbf{x}) = \mathbf{x} + W$, is $\mathbb{R}$-linear and surjective. By definition $\ker \pi = \ker \phi = W$, so we may adapt the proof of the First Isomorphism Theorem for groups 3.3.13 to show that ϕ induces a unique map $\tilde{\phi} : \mathbb{R}^n/W \to V$ that makes the diagram shown in Figure 7.1 commute: simply define $\tilde{\phi}(\mathbf{x} + W) = \phi(\mathbf{x})$. It is easy to check that $\tilde{\phi}$ is well-defined, $\mathbb{R}$-linear, and bijective, and hence an isomorphism of vector spaces over $\mathbb{R}$.

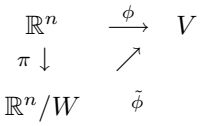

Figure 7.1. The induced map $\tilde{\phi}(\mathbf{x} + W) = \phi(x)$ satisfies $\tilde{\phi} \circ \pi = \phi$.

> *Conclusion:* Every vector space $V \in \mathcal{V}_n$ is isomorphic to a quotient $\mathbb{R}^n/W$ of the "universal" vector space on n generators $\mathbb{R}^n$. □

7.1.2 Exercise. Verify that the map $\tilde{\phi} : \mathbb{R}^n/W \to V$ is well-defined, $\mathbb{R}$-linear, and bijective as claimed. □

7.1.3 Example (Free abelian group on n generators). The group $(\mathbb{Z}^n, +)$ is a universal object for the set $\mathcal{A}_n$ of all *abelian* groups with n generators. If $G = \langle x_1, \ldots, x_n \rangle$ is such a group then

(a) There is a surjective homomorphism $\phi : \mathbb{Z}^n \to G$

(b) There is a subgroup $W \subseteq \mathbb{Z}^n$ such that $\mathbb{Z}^n/W \cong G$.

The map ϕ in (a) can be chosen so it maps the standard unit vectors $\mathbf{e}_1, \ldots, \mathbf{e}_n$ in $\mathbb{Z}^n$ to the generators of G, and then ϕ is uniquely determined.

DISCUSSION: Every element $\mathbf{m} \in \mathbb{Z}^n$ is uniquely a sum $\mathbf{m} = m_1\mathbf{e}_1 + \ldots + m_n\mathbf{e}_n$ with integer coefficients. Now define $\phi : \mathbb{Z}^n \to G$ so that

$$\phi(\mathbf{m}) = \phi(m_1\mathbf{e}_1 + \ldots + m_n\mathbf{e}_n) = x_1^{m_1} \cdot \ldots \cdot x_n^{m_n} \qquad \text{for all } \mathbf{m} \in \mathbb{Z}^n \tag{3}$$

Since G is abelian we have $\phi(\mathbf{0}) = e$ and $\phi(\mathbf{m} + \mathbf{m}') = \phi(\mathbf{m}) \cdot \phi(\mathbf{m}')$. This homomorphism is surjective since the x_i generate G, and its kernel $W = \{\mathbf{m} : \prod_{i=1}^n x_i^{m_i} = e\}$ is a subgroup in $\mathbb{Z}^n$. By the First Isomorphism Theorem for groups 3.3.13, the quotient group $(\mathbb{Z}^n/W, +)$ is isomorphic to G via the induced bijection $\tilde{\phi}(\mathbf{m} + W) = \phi(\mathbf{m})$. □

We note for future reference that the nature of the additive subgroups W in $\mathbb{Z}^n$ is not obvious. When $n = 1$ the group $\mathbb{Z}$ is infinite cyclic, with 1 as its generator. By 3.1.30 any subgroup W is also cyclic, so there exists some $k \geq 0$ such that $W = k\mathbb{Z} = \{mk : m \in \mathbb{Z}\} = \langle k \rangle$. If $k = 0$ we get the trivial subgroup, and for $k \neq 0$ the subgroup is isomorphic to $\mathbb{Z}$ (though not *equal to* $\mathbb{Z}$). When $n > 1$ the situation gets more complicated. Not all subgroups are singly generated, nor are they isomorphic to $\mathbb{Z}^n$ – just consider the subgroup $W = \{\mathbf{m} \in \mathbb{Z}^3 : m_3 = 0,\ m_1, m_2 \in \mathbb{Z}\}$, which is isomorphic to $\mathbb{Z}^2$ and is generated by the basis vectors $\mathbf{e}_1, \mathbf{e}_2$. The following result, which we will not prove here, is important in geometry.

7.1.4 Theorem. *Let W be any subgroup of $(\mathbb{Z}^n, +)$. Then there is an integer $0 \leq r \leq n$, called the* **rank** *of W, and a set of "integral basis vectors" $\{\mathbf{w}_1, \ldots, \mathbf{w}_r\} \subseteq W$, such that every $\mathbf{w} \in W$ is uniquely a sum $\mathbf{w} = m_1\mathbf{w}_1 + \ldots + m_r\mathbf{w}_r$ with integer coefficients. In particular, every subgroup of $\mathbb{Z}^n$ is isomorphic to $(\mathbb{Z}^r, +)$ for some $0 \leq r \leq n$.*

7.1.5 Exercise. Verify that the subset $W = \{\mathbf{m} : m_1 + m_2 - 2m_3 = 0\}$ is an additive subgroup of $\mathbb{Z}^3$.

(a) For which $r \geq 0$ is $W \cong \mathbb{Z}^r$?

(b) Find a set of vectors $\mathbf{w}_1, \ldots, \mathbf{w}_r$ such that every $\mathbf{w} \in W$ is a unique integer linear combination $\mathbf{w} = m_1\mathbf{w}_1 + \ldots + m_r\mathbf{w}_r$. □

We now show that there are similar universal objects for *all* groups, commutative or not. We shall construct the **free group on n generators**.

The Free Group F(n). Let S be any set of n distinct objects. This will become our alphabet for constructing "words" based on S, but first we double the number of elements in our alphabet by attaching exponents ± 1 to each letter. We obtain the enlarged alphabet $S \cup S^{-1} = \{a^{+1}, a^{-1} : a \in S\}$. A **word** is then any symbol string of finite length

$$w = a_1 a_2 \ldots a_r \qquad \text{with} \quad r < \infty \quad \text{and} \quad a_i \in S \cup S^{-1} \tag{4}$$

We allow the "empty word" e (the list with no entries) as the lone word of length zero.

7.1.6 Definition. *The* **free semigroup on n letters** *is the set $W(S)$ of all words of finite length based on an alphabet S with n letters. In $W(S)$ we define a multiplication operation by adjoining one word to another*

$$w_1 \cdot w_2 = a_1 \ldots a_r b_1 \ldots b_s \qquad \textit{if} \qquad w_1 = a_1 \ldots a_r \quad \textit{and} \quad w_2 = b_1 \ldots b_s \tag{5}$$

For products involving the empty word we define $we = w = ew$. Note that $w_1w_2 \neq w_2w_1$.

It is easily verified that this product operation is associative, so $w_1(w_2w_3) = (w_1w_2)w_3$, and that the empty word is an identity element, with $ew = w = we$ for all w. What $W(S)$ lacks to become a group is the existence of inverses. Note that words such as aa^{-1} or $a^{-1}a$ are *not* equal to the empty word e in the system $W(S)$. The best we can do is define the "reflection map" $J : W(S) \to W(S)$, which will become the inversion map when we define the free group based on S. Let

$$J(e) = e \quad \text{for the empty word} \qquad J(a_1 \dots a_r) = a_r^{-1} \dots a_1^{-1} \tag{6}$$

where we interpret $(s^{-1})^{-1} = s$ for any letter $s^{-1} \in S^{-1}$.

There are natural elementary operations on words $w = a_1 \dots a_r$

(i) *Insertions:* Insert the symbols ss^{-1} or $s^{-1}s$ (with $s \in S$) into a word w. The insertion can be made at the ends or in the middle of w.

(ii) *Cancellations:* If the original symbol string w contains adjacent symbols ss^{-1} or $s^{-1}s$ we may strike these out. The length of the word is reduced by 2, and we may end up with the empty word.

It is fairly obvious that if we wish to make a group out of $W(S)$ we should identify words that can be transformed into each other by a finite sequence of elementary operations.

7.1.7 Definition. *Two words in the free semigroup $W(S)$ are* **equivalent**, *written $w \sim_R w'$, if we can transform w into w' by a finite sequence of elementary operations. It is easily verified that this is an equivalence relation* (RST *relation*), *so we can form the space $W(S)/R$ of equivalence classes and the projection map $\pi : W(S) \to W(S)/R$ such that $\pi(x) = [x]$. Equipped with a suitably defined product operation, the quotient space $F(S) = W(S)/R$ will become the* **free group on n generators**.

7.1.8 Definition. *A word $w \in W(S)$ is a* **reduced word** *if no cancellations are possible – i.e. w contains no symbol strings of the form ss^{-1} or $s^{-1}s$. The empty word is regarded as reduced. The set of reduced words is denoted $W_0(S)$.*

$W_0(S)$ is not closed under multiplication. We now show that reduced words provide a complete set of representatives for the equivalence classes in $W(S)/R$.

7.1.9 Proposition. *Each equivalence class in $W(S)$ contains a unique reduced word. If $w \in W(S)$ all sequences of cancellations only (no insertions) that begin with w and terminate in a reduced word yield the same outcome w_0, which is the unique reduced representative in $[w]$.*

PROOF: Repeated cancellations applied to a word w must terminate in a reduced word. Generally, the sequence of cancellation operations is not unique – consider the possible transformations $s^{-1}ssss^{-1}s \to \dots \to ss \in W_0(S)$. Our first step is to show that the outcome is always the same.

7.1.10 Lemma. *Let $C_1, \dots, C_r$ be any sequence of cancellations that transforms a word w to a reduced word w_0. All such sequences yield the same result.*

PROOF: We use induction on the length of $w = a_1 \dots a_r$. If w is reduced, there is nothing to prove. If not, there is some pair of letters $a_ia_{i+1} = ss^{-1}$ or $s^{-1}s$ that can be cancelled. We now show that every reduced form w_0 can be obtained by cancelling this pair *first*. Then we may apply induction to the shorter word that remains, to show that all sequences of cancellations yield w_0.

We know that the reduced form w_0 is obtained by some sequence of cancellations. *Case 1: at some stage the pair a_ia_{i+1} is cancelled* (and neither a_i nor a_{i+1} is involved in any previous cancellations). Then we might as well rearrange the cancellation operations and cancel a_ia_{i+1} first. That settles this case.

Case 2: The first cancellation involving these elements cancels just one, say a_i, and not the other. Then we must have $a_{i-1} = a_i^{-1}$ and the cancelled pair is $a_{i-1}a_i$. Since $a_{i+1} = a_i^{-1}$ by definition, the word remaining after this cancellation,

$$\dots a_{i-2}(a_{i-1}a_i)a_{i+1}a_{i+2}\dots = \dots a_{i-2}(a_{i-1}a_i)a_i^{-1}a_{i+2} \to \dots a_{i-2}a_i^{-1}a_{i+2}\dots = \dots a_{i-2}a_{i-1}a_{i+2}\dots$$

is the same as the word obtained by cancelling the original pair a_ia_{i+1}

$$\dots a_{i-2}a_{i-1}a_ia_{i+1}a_{i+2}\dots = \dots a_{i-2}a_{i-1}(a_ia_i^{-1})a_{i+2}\dots \to \dots a_{i-2}a_{i-1}a_{i+2}\dots$$

This puts us back in Case 1, which has already been resolved. The lemma is proved. □

Resuming the main proof, we consider an elementary operation $w \xrightarrow{T} w'$ between two equivalent words. Let $C_1, \dots, C_r$ and $C'_1, \dots, C'_q$ be sequences of cancellations that transform w, w' to reduced words w_0, w'_0. If T is a cancellation, then the sequence of cancellations $T, C'_1, \dots, C'_q$ applied to w must yield w_0 by Lemma 7.1.8 and hence $w'_0 = w_0$. If T is an insertion we may write $w = w_1w_2$ and we have $w' = w_1ss^{-1}w_2$ (or same with $s^{-1}s$). Applying the obvious cancellation C to w' we get $C(w') = w$. By Lemma 7.1.8 the sequence $C, C_1, \dots, C_r$ transforms w' to w_0, but by the same lemma it must also transform w' to w'_0, so that $w_0 = w'_0$.

This idea can be applied repeatedly to any sequence of elementary operations

$$w \xrightarrow{T_1} w_1 \xrightarrow{T_2} w_2 \xrightarrow{T_3} \dots \xrightarrow{T_m} w'$$

to show that they have the common reduced form described in 7.1.8. In particular, if these operations transform w into a reduced word w' we must have $w' = w_0$. □

To construct the free group on n generators we observe that the product in $W(S)$ passes down to the quotient space $W(S)/R$, and the induced operation is automatically associative. In fact, suppose $w_1 \sim w'_1$ and $w_2 \sim w'_2$. We can perform elementary transformations on w_1w_2, first transforming w_1 to w'_1 and then w_2 to w'_2, to obtain $w'_1w'_2$. Hence $w_1w_2 \sim w'_1w'_2$, and the following operation on equivalence classes is well defined

$$[w_1] \cdot [w_2] = [w_1w_2] \qquad \text{for all } w_1, w_2 \in W(S) \tag{7}$$

It is easy to check that this operation is associative, and that the class e of the empty word is an identity element for $W(S)/R$. But now every element $[w]$ has a multiplicative inverse. In fact, the reflection operation $J(a_1 \dots a_r) = a_r^{-1} \dots a_1^{-1}$ in $W(S)$ passes down to $W(S)/R$ to become the desired inversion operation: since $w \sim w' \Rightarrow Jw \sim Jw'$ the class $[J(w)]$ is well defined and

$$[J(w)][w] = [a_r^{-1} \dots a_1^{-1}a_1 \dots a_r] = e = [w][J(w)] \qquad \text{for all } w \in W(S)$$

Thus $F(S) = W(S)/R$ is a group, generated by the set of n element $[s]$ with $s \in S$.

By Proposition 7.1.7 there is a natural bijection $F(S) = W(S)/R \leftrightarrow W_0(S)$, which means we can transfer the group operation (7) over to a group operation $(*)$ defined on the set of representatives $W_0(S)$. In this model the product operation in the free group is given by

$$w_1^0, w_2^0 \in W_0(S) \;\longrightarrow\; \text{product } w_1^0w_2^0 \in W(S) \xrightarrow{\text{reduce}} \text{unique element } w_1^0 * w_2^0 \text{ in } W_0(S)$$

because $[w_1^0][w_2^0] = [w_1^0w_2^0] = [w_1^0 * w_2^0]$.

7.1.11 Exercise. Verify that the free group on n generators is abelian $\Leftrightarrow n = 1$. □

7.1.12 Exercise. Verify that the free group on one generator is isomorphic to $(\mathbb{Z}, +)$. □

We now show that $F(S) = W(S)/R$ has the desired universal mapping properties. To begin, we define the map $j : S \to F(S)$ that identifies letters $s \in S$ with group elements $j(s) = [s]$.

Obviously $F(S) = \langle j(S) \rangle$, so in this sense $F(S)$ is "generated by the elements of S."

7.1.13 Theorem. *Let $S = \{s_1, \ldots, s_n\}$ be a set of n distinct objects and let $F(S) = W(S)/R$ be the free group on n generators defined above. Let $\mathcal{G}_n$ be the class of groups with n generators and let $G = \langle x_1, \ldots, x_n \rangle$ be such a group. Then*

(a) *If $\phi : S \to G$ is any mapping, then there exists a unique homomorphism $\tilde{\phi} : F(S) \to G$ such that the diagram shown in Figure 2 commutes – i.e. $\tilde{\phi} \circ j = \phi$.*

The map ϕ specifies where we wish to send the generators of $F(S)$. In (a) *the map $\tilde{\phi}$ need not be surjective; its range is the subgroup $H = \langle \phi(S) \rangle$.*

(b) *There is a unique surjective homomorphism $\tilde{\phi} : F(S) \to G$ such that $\tilde{\phi}(s_i) = x_i$ for $1 \le i \le n$.*

(c) *There is a normal subgroup $N \subseteq F(S)$ such that $F(S)/N \cong G$.*

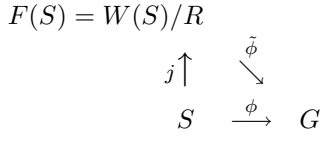

Figure 7.2. Universal mapping property of $F(S)$. Here $j(s) = [s]$.

PROOF: Obviously (b) follows from (a) by taking $\phi(s_i) = x_i$; surjectivity holds because the x_i generate G. Then (b) $\Rightarrow$ (c) by the applying the First Isomorphism Theorem 3.1.13 to the map $\tilde{\phi}$ in (b); writing $N = \ker \tilde{\phi}$ we get $F(S)/N \cong G$. So, everything follows from the "universal mapping property" (a).

To prove (a) we construct an intermediate map $\phi_0 : W(S) \to G$, setting

$$\begin{aligned} \phi_0(\text{ empty word }) &= e \\ \phi_0(s_{i_1}^{\pm 1} \ldots s_{i_r}^{\pm 1}) &= x_{i_1}^{\pm 1} \cdot \ldots \cdot x_{i_r}^{\pm 1} \qquad \text{where } 1 \le i_1, \ldots, i_r \le n \end{aligned}$$

It is clear that $\phi_0(w_1 w_2) = \phi_0(w_1) \cdot \phi_0(w_2)$ in G, so that ϕ_0 is a homomorphism of *semigroups*; furthermore, $\phi_0(s_i) = x_i$. Next we show that

(8) $\qquad \phi_0$ respects equivalences: $\quad w \sim w' \implies \phi_0(w) = \phi_0(w')$

Once (8) is proved we get a well-defined map $\tilde{\phi} : W(S)/R \to G$ by setting $\tilde{\phi}([w]) = \phi_0(w)$. This map is obviously surjective, and it is a homomorphism of groups because

$$\tilde{\phi}([w_1][w_2]) = \tilde{\phi}([w_1 w_2]) = \phi_0(w_1 w_2) = \phi_0(w_1)\phi_0(w_2) = \tilde{\phi}([w_1]) \cdot \tilde{\phi}([w_2])$$

To prove (8), suppose $w' = C(w)$ where C is a cancellation, say $w = w_1 s s^{-1} w_2$ and $w' = w_1 w_2$. Then $\phi_0(w) = \phi_0(w_1)\phi_0(s)\phi_0(s)^{-1}\phi_0(w_2) = \phi_0(w')$. On the other hand, if T is an insertion, say $w = w_1 w_2$ and $w' = w_1 s s^{-1} w_2$, then we again have $\phi_0(w') = \phi_0(w)$. The same invariance-of-image remains true for any sequence of elementary operations. That proves (8), and finishes the proof of the theorem. $\square$

Uniqueness of the Universal Object F(S). It is natural to wonder whether there might be other objects quite different from $F(S)$ that have the universal mapping property 7.1.13(a). That property actually forces uniqueness of the universal object.

7.1.14 Proposition. *Let S be a set of n distinct objects and let (S, j, F), (S, j', F') be two systems that have the universal mapping property* 7.1.13(a). *Then there is an isomorphism of groups $\psi : F \to F'$ such that $\psi \circ j = j'$ (the diagram in Figure* 7.3(a) *commutes).*

PROOF: The universal mapping property tells us that corresponding to the map $j' : S \to F'$ there is a homomorphism $\tilde{j'}$ from F to F' that makes the top part of the diagram in Figure 7.3(b) commute; $\tilde{j'}$ is surjective because $\tilde{j'}(j(S)) = j'(S)$ is a set of generators for F'. Now reverse roles of j and j' to get the map $\tilde{j}$ in the lower part of the diagram. We have $\tilde{j} \circ \tilde{j'} = \mathrm{id}$ on $j(S)$ because $\tilde{j}\tilde{j'}(js) = \tilde{j}(j's) = j(s)$ for all $s \in S$. Thus $\tilde{j} \circ \tilde{j'} = \mathrm{id}_F$ since $j(S)$ generates F. The map $\psi = \tilde{j'}$ is the desired isomorphism and its inverse is $\psi^{-1} = \tilde{j}$. $\square$

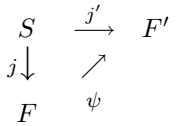

Figure 7.3(a)

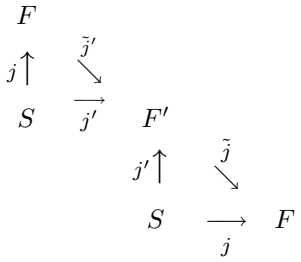

Figure 7.3(b)

7.2 Generators and Relations.

The dihedral group D_n is generated by two elements ρ, σ that satisfy the relations

$$\rho^n = e \qquad \sigma^2 = e \qquad \sigma\rho\sigma = \rho^{-1} \tag{9}$$

Actually, we know somewhat more about the generators, namely that

$$\begin{aligned} o(\rho) &= n \quad \text{– i.e. the powers } e, \rho, \dots \rho^{n-1} \text{ are distinct and } \rho^n = e \\ o(\sigma) &= 2 \quad \text{– i.e. } \sigma \neq e \text{ and } \sigma^2 = e \end{aligned}$$

You might be tempted to believe that the relations (9), together with the fact that ρ and σ generate D_n, suffice to identify the dihedral group. This is not so. For example the relations (9) are also satisfied by the following groups

- The trivial group $G = (e)$, which can be expressed as $G = \langle \rho, \sigma \rangle$ if we take $\rho = \sigma = e$.
- The $G = \mathbb{Z}_2$, which can be expressed as $G = \langle \rho, \sigma \rangle$ if we take $\rho = e$ and σ the other element in $\mathbb{Z}_2$.

What distinguishes D_n from these examples is that the others are all quotients D_n/N of the dihedral group – taking $N = D_n$ in the first case and $N = \langle \rho \rangle$ in the second. The dihedral group itself is not a quotient of any larger group $G = \langle x_1, x_2 \rangle$ whose generators satisfy the relations $x_1^n = x_2^2 = x_1 x_2 x_1 x_2 = e$, and in this sense D_n is the *largest* group of this type.

Here's another example. Suppose we wish to construct a group $G = \langle x, y, z \rangle$ with three generators that satisfy the relations

$$x^2 = e \qquad y^2 = e \qquad xyz = e \tag{10}$$

Is there such a group? How many (up to isomorphism)? Are there any *nontrivial* groups of this type? Is there a maximal group that is the mother of all such groups by taking quotients? Is this group some more familiar group in disguise? These questions are not easy to answer. In particular it is seldom obvious whether a group satisfying a set of relations is nontrivial!

The purpose of this section is to clarify the connection between a finitely generated group $G = \langle x_1, \dots, x_n \rangle$ and the relations satisfied by its generators. In particular we will show that if a finite set of relations are imposed on the generators, there is an essentially unique "maximal" group with the same number of generators satisfying those relations, from which every group of this type is obtained by taking suitable quotients.

Let $G = \langle x_1, \dots, x_n \rangle$ be any finitely generated group. Given any nonempty word $w = w(s_1, \dots, s_n)$ built upon the generators of the free group $F(S)$ with n generators, we can form a corresponding word $w(x_1, \dots, x_n)$ in G by substituting $s_i \mapsto x_i$.

7.2.1 Definition. *A* **relation** *between the generators of G is any equality of the form*

$$w(x_1, \ldots, x_n) = e \qquad \textit{where } w \textit{ is a nonempty word in } F(S) \tag{11}$$

Obviously a word $w \in F(S)$ and the corresponding reduced word w_0 determine the same element in G, so we need only consider reduced words in discussing relations. There is also no need to consider relations of the form $w_1 = w_2$ since these can be rewritten as $w_1 w_2^{-1} = e$; for instance the relation $\sigma\rho\sigma = \rho^{-1}$ in (9) can be recast as $\rho\sigma\rho\sigma = e$.

Notice that a statement such as $o(\rho) = n$ *cannot* be expressed by setting a finite number of words $w_k(\rho, \sigma) = e$; the statement $o(\rho) = n$ incorporates a number of *inequality* statements such as

$$\rho^i \rho^{-j} \neq e \text{ for } 0 \leq j < i \leq n-1, \quad \text{or equivalently} \quad \rho^k \neq e \text{ for } 0 < k < n \ ,$$

in addition to the equality $\rho^n = e$ which is a true relation among the generators of D_n. Notice too, that our original definition of the dihedral group was based on the properties $o(\rho) = n$ and $o(\sigma) = 2$ rather than the relations $\rho^n = \sigma^2 = e$. The latter are satisfied by various quotients of D_n, while the former are not.

Suppose nonempty (reduced) words $w_1, \ldots, w_r$ have been specified in the free group on generators $S = \{s_1, \ldots, s_n\}$. We want to create a group $G = \langle x_1, \ldots, x_n \rangle$ whose generators x_i satisfy the relations

$$w_i(x_1, \ldots, x_r) = e \qquad \text{for } 1 \leq i \leq r$$

and we would like G to be as large as possible. We will obtain G by taking a suitable quotient $F(S)/N$, keeping in mind that the smaller the normal subgroup we factor out, the larger the quotient. The idea is to define N so the quotient map $\pi : F(S) \to F(S)/N$ kills the words w_i. That means N should contain the w_i, and products thereof, and in fact it must contain the entire subgroup $H = \langle w_1, \ldots, w_r \rangle$ in $F(S)$ generated by the w_i. But N is also normal, so N must contain all conjugates gxg^{-1} where $g \in F(S)$, $x \in H$. Therefore the smallest *normal* subgroup we can factor out to kill the words $w_1, \ldots, w_r$ is

$$N = \bigcap \{M : M \text{ is a normal subgroup in } F(S) \text{ and contains } w_1, \ldots, w_r \ \} \tag{12}$$

We denote this group by $N = \langle\langle w_1, \ldots, w_r \rangle\rangle$.

7.2.2 Exercise. If $\{w_1, \ldots, w_r\}$ is a set of words in the free group $F(S)$ prove that

(a) The intersection of all normal subgroups containing these words is a normal subgroup in $F(S)$.

This subgroup $N = \langle\langle w_1, \ldots, w_r \rangle\rangle$, is obviously the *smallest* normal subgroup containing this set of words.

(b) Prove that this subgroup can also be described as the subgroup $\langle gsg^{-1} : s \in S \rangle$ generated by all conjugates of elements $s \in S$. □

7.2.3 Theorem. *Let $w_1, \ldots, w_r$ be a set of words in the free group $F(S)$ on the generators $S = \{s_1, \ldots, s_n\}$. Define the normal subgroup*

$$N = \langle\langle w_1, \ldots, w_r \rangle\rangle = \bigcap \{M : M \textit{ is a normal subgroup in } F(S) \textit{ and contains } w_1, \ldots, w_r \ \}$$

as above. The quotient $\overline{G} = F(S)/N$ is generated by the elements $\overline{x}_i = \pi(s_i)$, $1 \leq i \leq n$, which satisfy the relations

$$w_i(\overline{x}_1, \ldots, \overline{x}_n) = e \qquad \textit{for } 1 \leq i \leq r \tag{13}$$

If $G = \langle y_1, \ldots, y_n \rangle$ is any other finitely generated group whose generators satisfy these relations, there is a unique surjective homomorphism $\phi : F(S)/N \to G$ such that $\phi(\overline{x}_i)$ is equal to y_i. In particular, G is isomorphic to a quotient of $F(S)/N$.

PROOF: The last statement follows by the First Isomorphism Theorem. The first follows because the quotient map $\pi : F(S) \to \overline{G}$ is surjective and a homomorphism. Now let $G = \langle y_1, \ldots, y_n \rangle$. By the universal mapping property 7.1.13 there is a unique surjective homomorphism $f : F(S) \to G$ such that $f(s_i) = y_i$; let $K = \ker f$. Since f is a homomorphism we get

$$\begin{array}{rcl} f(w_i(s_1, \ldots, s_n)) & = & w_i(f(s_1), \ldots, f(s_n)) \\ & = & w_i(y_1, \ldots, y_n) = e \end{array}$$

$$\begin{array}{ccc} F(S) & \xrightarrow{f} & G \\ \pi \downarrow & \nearrow & \\ F(S)/N & \tilde{f} & \end{array}$$

Figure 7.4.

Thus $w_i \in K$ for all i, hence $H = \langle w_1, \ldots, w_r \rangle$ is contained in K, and because K is normal we actually have $N = \langle\langle w_1, \ldots, w_r \rangle\rangle \subseteq K$. In Figure 7.4 there is a natural induced map $\tilde{f}$ that makes the diagram commute. Just set

$$\tilde{f}(xN) = f(x) \qquad \text{for all } x \in F(S)$$

This is well defined since $N \subseteq K$; in fact, if $x'N = xN$ then $x'x^{-1} \in N \subseteq K$ and hence $f(x') = f(x)$. Commutativity of the diagram is built into the definition of $\tilde{f}$. Finally, $\tilde{f}$ is a homomorphism because

$$\tilde{f}(xN \cdot yN) = \tilde{f}(xyN) = f(xy) = f(x)f(y) = \tilde{f}(xN)\tilde{f}(yN)$$

and it is surjective because $g \in G \Rightarrow g = f(x)$ for some $x \in F(S) \Rightarrow \tilde{f}(\pi(x)) = f(x) = g$. $\square$

Returning to our earlier comments about the dihedral group, we now show that D_n is the maximal group on two generators satisfying the relations (9).

7.2.4 Example. In the free group $F(S)$ on two generators consider the normal subgroup

$$N = \langle\langle\, s_1^n,\, s_2^2,\, s_1 s_2 s_1 s_2 \,\rangle\rangle$$

determined by the words $w_1 = s_1^n$, $w_2 = s_2^2$, $w_3 = s_1 s_2 s_1 s_2$. We claim that there is an isomorphism from $F(S)/N$ to the dihedral group D_n that sends $\overline{x} = \pi(s_1)$, $\overline{y} = \pi(s_2)$ to ρ, σ respectively.

DISCUSSION: By 7.1.3 there is a surjective homomorphism $f : F(S) \to D_n = \langle \rho, \sigma \rangle$ such that $f(s_1) = \rho$, $f(s_2) = \sigma$. The elements $\overline{x}, \overline{y}$ generate $\overline{G} = F(S)/N$, and they satisfy the same relations (9) as ρ and σ because

$$w_1 \in N \Rightarrow \overline{x}^n = \overline{e} \qquad w_2 \in N \Rightarrow \overline{y}^2 = \overline{e} \qquad w_3 \in N \Rightarrow \overline{xyxy} = \overline{e}$$

Then $o(\overline{x})$ is a divisor of n, but in fact it is equal to n because

$$\begin{array}{rcl} \tilde{f}(\overline{x}) & = & \tilde{f}(\pi(s_1)) = f(s_1) = \rho \\ & \Rightarrow & \text{the images } \tilde{f}(\overline{x}^i) = (\tilde{f}(\overline{x}))^i = \rho^i \text{ are distinct in } D_n \text{ for } 1 \le i \le n-1 \\ & \Rightarrow & \text{the elements } \overline{x}^i \text{ are distinct in } F(S)/N \text{ for } 1 \le i \le n-1 \\ & \Rightarrow & o(\overline{x}) = n \end{array}$$

Likewise, $\tilde{f}(\overline{y}) = \sigma$ and $o(\overline{y}) = 2$.

Hence $H_1 = \langle \overline{x} \rangle$ and $H_2 = \langle \overline{y} \rangle$ are cyclic subgroups of $\overline{G}$ and $H_1 \cap H_2 = (\overline{e})$ because $\overline{x}^i = \overline{y}^j \Rightarrow \rho^i = \sigma^j \Rightarrow \rho^i = e$ and $\sigma^j = e \Rightarrow i \equiv 0 \pmod{n}$ and $j \equiv 0 \pmod{2} \Rightarrow \overline{x}^i = \overline{y}^j = \overline{e}$.

Furthermore H_1 is normal in $\overline{G}$ because $\overline{y}(\overline{x}^k)\overline{y}^{-1} = (\overline{x})^{-k}$ for all $k \in \mathbb{Z}_n$. Thus H_1H_2 is a subgroup, which must equal $\overline{G}$ since H_1H_2 contains the generators.

But $|H_1H_2| = 2n$ and the same is true of the surjective image $D_n = \tilde{f}(\overline{G})$. Therefore $\tilde{f}$ is bijective, and is an isomorphism. $\square$

Theorem 7.2.3 also provides an alternative approach to the free abelian group introduced in Example 7.1.2. If we wish the quotient $\overline{G} = F(S)/N$ to be abelian we must, at the very least, factor out the subgroup

$$N = \langle\langle\, [s_i, s_j] = s_i s_j s_i^{-1} s_j^{-1} : 1 \le i \ne j \le n \,\rangle\rangle \tag{14}$$

determined by commutators of the generators of $F(S)$. You might think it necessary to factor out *arbitrary* commutators $[w_1, w_2] = w_1 w_2 w_1^{-1} w_2^{-1}$ of words $w_1, w_2 \in F(S)$ – an infinite set of relations – but the following observation shows that these commutators are already included in N.

7.2.5 Exercise. Let $G = \langle x_1, \ldots, x_n \rangle$ be a finitely generated group and let

$$N = \langle\langle\, [x_i, x_j] = x_i x_j x_i^{-1} x_j^{-1} : 1 \le i \ne j \le n \,\rangle\rangle$$

Prove that N coincides with the commutator subgroup $[G, G] = \langle\, [x, y] : x, y \in G \,\rangle$.
Hint: By 6.4.3 we have $N \supseteq [G, G] \Leftrightarrow G/N$ is abelian. Start by showing that if all elements in $S = \{x_i\}$ commute, the same is true of all elements in $S \cup S^{-1}$.
Note: The main point here is that *the commutator of the generated group $G = \langle x_1, \ldots, x_r \rangle$ is the normal subgroup generated by commutators of the x_i.* $\square$.

In our present situation 7.2.5 tells us that $F(S)/N = F(S)/[F(S), F(S)]$, and in particular that $F(S)/N$ is abelian.

On the other hand, the generators of any *abelian* group $G = \langle x_1, \ldots, x_n \rangle$ must satisfy the relations $x_i x_j x_i^{-1} x_j^{-1} = e$, so by 7.2.3 we see that G is a quotient of $F(S)/N$. Thus $F(S)/N$, with N defined as in (14), serves as a universal object for all finitely generated abelian groups. The following result reconciles this observation with our previous work in 7.1.2.

7.2.6 Lemma. *If $S = \{s_1, \ldots, s_n\}$ and $N = \langle\langle\, [s_i, s_j] : i \ne j \,\rangle\rangle$, then the quotient $F(S)/N$ is isomorphic to $(\mathbb{Z}^n, +)$.*

Proof: As we have seen, $F(S)/N$ is a finitely generated abelian group with generators $\overline{x}_i = \pi(s_i)$. If $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ is the standard basis vectors in $\mathbb{Z}^n$, then by 7.1.2 there is a unique surjective homomorphism $\phi : \mathbb{Z}^n \to F(S)/N$ such that $\phi(\mathbf{e}_i) = \overline{x}_i$. On the other hand, since $\mathbb{Z}^n = \langle \mathbf{e}_1, \ldots, \mathbf{e}_n \rangle$, we know by 7.2.3 that there is a unique surjective homomorphism $f : F(S)/N \to \mathbb{Z}^n$ such that $f(\overline{x}_i) = \mathbf{e}_i$. Then $f \circ \phi = \phi \circ f = \mathrm{id}$ since this is true on sets of generators. Thus f is an isomorphism and $F(S)/N \cong \mathbb{Z}^n$. $\square$

In the abelian group $F(S)/N = F(S)/[F(S), F(S)]$, the congruence

$$s_i s_j \equiv s_j s_i \pmod{\text{the commutator subgroup}}$$

means that every word $w = a_1 \ldots a_r$ in $F(S)$ can be rewritten (without changing the $[F(S), F(S)]$-coset in which it lies) as

$$w = s_1^{m_1} \ldots s_n^{m_n} \qquad \text{where} \qquad m_i \in \mathbb{Z} \ \text{ and } \ |m_1| + \ldots + |m_n| \le r$$

Cosets in $F(S)/N$ correspond one-to-one with these "abelianized" words in $F(S)$. The rearrangement process might result in some cancellations, so there is no assurance that we will end up with $|m_1| + \ldots + |m_n| = r$ when we abelianize a reduced word of length r.

Presentations of Finitely Generated Groups. Let $G = \langle x_1, \ldots, x_n \rangle$ be a finitely generated group G and $F(S)$ the free group on $S = \{s_1, \ldots, s_n\}$. By 7.1.13 there is a unique surjective homomorphism $f : F(S) \to G$ such that $f(s_i) = x_i$.

7.2.7 Definition. *A* **presentation** *of a group G consists of a pair $(S; R)$ where $S = \{s_1, \ldots, s_n\}$ are generators of a free group $F(S)$, and $R = \{w_1, \ldots, w_r\}$ is a finite set of nonempty words such that $G \cong F(S)/N$, where $N = \langle\langle w_1, \ldots, w_r \rangle\rangle$. We indicate this by writing $G \approx (s_1, \ldots, s_n; w_1, \ldots, w_r)$.*

The subgroup N is referred to as the **relation subgroup** associated with the presentation. Obviously N is the complete set of words that are killed when we pass from $F(S)$ to G.

The images $x_i = \pi(s_i)$ generate G and satisfy the relations $w_i(x_1, \ldots, x_n) = e$ corresponding to the words w_i. However in the other direction, if we write down a set of valid relations $w_i(x_1, \ldots, x_n) = e$ among the generators of a group G, there is no guarantee that we have produced a presentation – i.e. that $G \cong F(S)/\langle\langle w_1, \ldots, w_r \rangle\rangle$.

7.2.8 Example. Take $G = \mathbb{Z}_2$ and write $G = \langle \rho', \sigma' \rangle$ where $\rho' = [0]$ and $\sigma' = [1]$ in $\mathbb{Z}_2$. Let $w_1 = s_1^n, w_2 = s_2^2, w_3 = s_1 s_2 s_1 s_2$ in the free group over $S = \{s_1, s_2\}$. We showed in Example 7.2.4 that $F(S)/N \cong D_n$, so $(\rho', \sigma'; w_1, w_2, w_3)$ is not a presentation of $G = \mathbb{Z}_2$, although it *is* a presentation of D_n. □

The number of generators of a group is not uniquely determined – some might be redundant, as in the last example. It is often not easy to tell whether the mininal number of generators has been achieved. Obviously there *is* a unique minimum number of generators for any finitely generated group, but that might be achieved by taking quite different sets of generators, with quite different relations among them.

7.2.9 Example. Consider the group with the presentation $G \approx (x_1, x_2, x_3; x_1^3, x_2^2, x_3^2, x_1 x_2 x_3)$. Prove that G is isomorphic to D_3, which has the alternative presentation $(\rho, \sigma; \rho^3, \sigma^2, \rho\sigma\rho\sigma)$ involving just two generators.

Discussion: In Figure 7.5, π_2 and π_3 are the quotient maps with respect to the normal subgroups

$$N_2 = \langle\langle s_1^3, s_2^2, s_1 s_2 s_1 s_2 \rangle\rangle \qquad N_3 = \langle\langle x_1^3, x_2^2, x_3^2, x_1 x_2 x_3 \rangle\rangle$$

We have $G = F_3/N_3$ by definition.

Since $x_1 x_2 x_3 = e$, we get $x_3 = x_3^{-1} = x_1 x_2$ so the third generator is redundant. Eliminating x_3 in all relations, we get the familiar defining relations for the dihedral group D_3: $x_1^3 = x_2^2 = e, (x_1 x_2)^2 = x_1 x_2 x_1 x_2 = e$. Thus $G = F_3/N_3$ is equal to $\langle \rho', \sigma' \rangle$ where $\rho' = \pi_3(x_1)$ and $\sigma' = \pi_3(x_2)$, and these generators satisfy the dihedral relations (9). Since D_3 is the maximal group on two generators satisfying these relations (Theorem 7.2.3), F_2/N_2 is isomorphic to D_3 in Figure 7.5, and there is a surjective homomorphism ϕ from F_2/N_2 to $G = F_3/N_3$.

$$\begin{array}{ccc} F_2 = F(s_1, s_2) & \xrightarrow{j} & F_3 = F(x_1, x_2, x_3) \\ \pi_2 \downarrow & & \downarrow \pi_3 \\ D_3 \cong F_2/N_2 & \xrightarrow{\phi} & F_3/N_3 = G \end{array}$$

Figure 7.5. Here $j(s_i) = x_i$ for $i = 1, 2$; $F_2/N_2 = \langle \rho, \sigma \rangle$ where $\rho = \pi_2(s_1)$, $\sigma = \pi_2(s_2)$; $G = F_3/N_3 = \langle \rho', \sigma' \rangle$ where $\rho' = \pi_3(x_1)$, $\sigma' = \pi_3(x_2)$. The diagram is commutative.

On the other hand, G is the maximal group on three generators that satisfy the relations specified in its presentation. The dihedral group can be expressed in this form by writing $D_3 = \langle y_1, y_2, y_3 \rangle$ with generators $y_1 = \rho,\ y_2 = \sigma,\ y_3 = \rho\sigma$, for which $y_1 y_2 y_3 = \rho\sigma\rho\sigma = e$. Therefore there exists a surjective homomorphism from G to D_3, and in particular the quotient F_3/N_3 does not collapse to the trivial group. It follows that $|G| = |D_3| = 6$, the map ϕ in Figure 7.5 is bijective, and $G \cong D_3$. □

The crucial point in the foregoing proof is to show that $G = F_3/N_3$ does not collapse to be the trivial group. The reader might, with some justification, feel that this was resolved by smoke and mirrors, but our discussion is really a case study in the power of the universal mapping property. To understand what has been accomplished, consider what one would have to do to give a *direct* proof that G is nontrivial – i.e. that

$$N_3 = \langle\langle w_1, w_2, w_3, w_4\rangle\rangle \quad \text{with} \quad w_1 = x_1^3,\ w_2 = x_2^2,\ w_3 = x_3^2,\ w_4 = x_1x_2x_3$$

is not the entire free group $F_3 = F(x_1, x_2, x_3)$. For instance, how do you prove that the generator x_1 is not in N_3? According to our comments in Exercise 7.2.2(b), if $x_1 \equiv e \pmod{N_3}$ there would exist a choice of reduced words $u_1, \ldots, u_q$ in $W(x_1, x_2, x_3)$, and indices $1 \le i_1, \ldots, i_q \le 4$, such that

$$x_1^{-1} \cdot u_1 w_{i_1} u_1^{-1} u_2 w_{i_2} u_2^{-1} \ldots u_q w_{i_q} u_q^{-1}$$

collapses to the empty word by a sequence of cancellations. One might procede by induction on q, examining what it means for such a word to collapse (and using the fact that the u_i are already reduced), to show that a contradiction must emerge. But a proof along those lines would be pretty arduous. All of this has been circumvented by appeal to the universal mapping property of 7.2.3.

7.2.10 Exercise. Consider the groups whose presentations are

$$\begin{array}{lcll} G_2 & \approx & (x, y; x^2, y^2) & \text{(with 2 generators)} \\ G_3 & \approx & (x, y, z; x^2, y^2, xyz) & \text{(with 3 generators)} \end{array}$$

Without trying to identify these groups, prove that they are isomorphic. □

In Figure 7.6 we show a regular tetrahedron with vertices labeled **1,2,3,4**. Assume that coordinate axes have been set up so the origin lies at the center of the tetrahedron and the z-axis passes through the vertex labeled **3**; the coordinate axes have not been shown, to keep the diagram from being too cluttered. The set T of orientation-preserving symmetry operations on this figure consist of the following 12 linear operators on $\mathbb{R}^3$.

(i) The identity I

(ii) Eight rotations, by 120° or by 240°, about lines that pass through a vertex and the midpoint of the opposite face.

(iii) Three 180° rotations about lines passing between midpoints of opposite edges.

Figure 7.6. A regular tetrahedron. We show: rotation A_1 by 120° about an axis through vertex 1, and B_{13} by 180° about an axis through midpoints of opposite edges.

The rotation axes are directed line segments and the sense of rotation is to be determined by the usual "right hand rule." Because of the way coordinate axes have been chosen, each of these symmetries is a linear operator τ_A corresponding to some orthogonal matrix $A \in \mathrm{SO}(3)$ that has determinant $+1$. Thus the set T of geometric symmetries can be identified with a set of matrices in the special orthogonal group SO(3). One could study these operators using matrix theory, but there are more direct geometric ways to understand them.

First note that any operator $\tau_A \in T$ must permute the vertices, and hence corresponds to a unique permutation in S_4. For instance the 120° rotation about the vertex **1** corresponds to the 3-cycle $(2, 3, 4)$ in S_4. Furthermore, the vectors $\mathbf{v}_i$ extending from the origin to the vertices

form a spanning set in $\mathbb{R}^3$. Although it is not yet clear whether *every* permutation $\sigma \in S_4$ arises from the action of some linear operator that preserves the tetrahedron, it is evident that distinct operators in T must correspond to different permutations because any operator $\tau_A \in T$ is completely determined once we know how it permutes vertices. Thus we have a natural one-to-one map $\psi : T \to S_4$ that allows us to study T in terms of permutations.

7.2.11 Exercise. Verify that the set of symmetries T is actually a group under composition of operators and that ψ is a (one-to-one) homomorphism.
Hint: First show that $\psi(A \circ B) = \psi(A)\psi(B)$ in S_4. □

7.2.12 Exercise. Show that the symmetry operations T correspond one-to-one with the *even* permutations in S_4. (Thus T is isomorphic to the alternating group A_4.)
Note: It can be shown that the odd permutations also arise from symmetries of the tetrahedron, but they correspond to the orientation-reversing symmetries: reflections across various planes through the origin. □

With these remarks on the tetrahedral group T in mind we can find generators and exhibit a presentation of this group. In Figure 7.6 we labeled a few of the symmetry operations in T. In general, we define

- A_i to be the 120° rotation about the axis extending from the origin through the i^{th} vertex. Its square A_i^2 is rotation by $240° = -120°$ (rotation in the opposite sense).
- B_{ij}, $i \neq j$, to be rotation by 180° about the axis extending from the origin through the center of the edge $[\mathbf{v}_i, \mathbf{v}_j]$. This line also passes through the center of the opposite edge.

These account for all operators in T except for the identity, but there is some redundancy in this notation.

7.2.13 Exercise. Labeling elements of T as above,

(a) Verify that $B_{ij} = B_{ji}$ and that $B_{ij} = B_{k\ell}^{-1}$ $(= B_{k\ell})$ if $\{i, j\} \cap \{k, \ell\} = \emptyset$.

Thus I, A_1, $A_1^2, \ldots, A_4$, A_4^2, B_{12}, B_{13}, B_{23} is a complete list of elements in T.

(b) Determine all twelve products $A_1 \circ B$ with $B \in T$.

(c) Prove that $N = \{I, B_{12}, B_{13}, B_{23}\}$ is an abelian subgroup of T and that $N \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Note: Use 7.2.11 to reduce to calculations involving permutations. □

Armed with the computational background developed in 7.2.13 you should be able to handle the following more abstract problems.

7.2.14 Exercise. Show that T has the following properties.

(a) T is generated by the elements $x = A_1$ and $y = A_3^2$.

(b) These generators have order 3 and satisfy the relations $xyxy = e$.

It follows that there is a surjective homomorphism from $\overline{G} \approx (x, y; x^3, y^3, xyxy)$ to T. □

∗**7.2.15 Exercise.** Prove that the maximal group $G = \langle x, y \rangle$ whose generators satisfy the relations

$$x^3 = e \qquad y^3 = e \qquad xyxy = e$$

is isomorphic to the group T of rotational symmetries of the regular tetrahedron. □

7.2.16 Exercise. Given the result in 7.2.15, show that the group whose presentation is $G \approx (x, y, z; x^3, y^2, z^2, xyz)$ is also isomorphic to the tetrahedral group T. □

More can be said about the structure of T by carrying further the analysis in 7.2.13 and 7.2.14.

7.2.17 Exercise. In the tetrahedral group T show that

(a) The elements $N = \{I, B_{12}, B_{13}, B_{23}\}$ form a *normal* subgroup in T such that $N \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

(b) The subgroup $H = \langle A_1 \rangle \cong \mathbb{Z}_3$ cross-sections the cosets in T/N – i.e. $N \cap H = (e)$ and $NH = T$.

It follows that T is a semidirect product $T = N \times_\phi H \cong (\mathbb{Z}_2 \times \mathbb{Z}_2) \times_\phi \mathbb{Z}_3$.

(c) Determine the action of H on N and the associated homomorphism $\Phi : H \to \mathrm{Aut}(N)$.

Then write out the multiplication law obtained when T is modeled on the cartesian product set $N \times H = (\mathbb{Z}_2 \times \mathbb{Z}_2) \times \mathbb{Z}_3$.
Note: As an additive group, $N = \mathbb{Z}_2 \times \mathbb{Z}_2$ is a vector space over the field of scalars $\mathbb{Z}_2$ and $\mathrm{Aut}(N)$ is the set of $\mathbb{Z}_2$-linear operators corresponding to matrices $A \in \mathrm{GL}(2, \mathbb{Z})$ (2×2 matrices with entries in $\mathbb{Z}_2$ and $\det A \neq 0$). □

The following exercises and examples are concerned with other types of finitely presented groups. The relations in the first exercise below look a lot like those for the tetrahedral group, but the outcome is quite different.

7.2.18 Exercise. Prove that the group whose presentation is $G \approx (x, y; x^3, y^3, yxyxy)$ is isomorphic to $(\mathbb{Z}_3, +)$. □

7.2.19 Exercise. Prove that all groups $G = \langle x, y \rangle$ whose generators satisfy the relations $x^4 = e,\ y^3 = e,\ x^2 = yxy$ must be trivial. □

7.2.20 Example. We conclude by examining the group $\overline{G} \approx (x, y;\ x^2, y^2, xyz)$ mentioned earlier in equation (10). As noted in Exercise 7.2.10, the generator z is redundant, so the group we are concerned with has the deceptively simple presentation $\overline{G} \approx (x, y;\ x^2, y^2)$. What can we say about it? Is it nontrivial? Is it finite? Is it isomorphic to any familiar group?

Discussion: One way to obtain information about $\overline{G}$ is to search for concrete groups $G = \langle x, y \rangle$ whose generators satisfy $x^2 = y^2 = e$. By Theorem 7.2.3 every such G is a quotient (surjective homomorphic image) of $\overline{G}$. There are abelian groups $G = \langle x, y \rangle$ whose generators satisfy $x^2 = y^2 = e$, for instance the Klein group $\mathbb{Z}_2 \times \mathbb{Z}_2$, and hence there are natural surjective homomorphisms $\overline{G} \to \mathbb{Z}_2 \times \mathbb{Z}_2$.

7.2.21 Exercise. The group $G_{\mathrm{abel}} = F(s_1, s_2)/N$, where $N = \langle\langle s_1^2, s_2^2, s_1 s_2 s_1^{-1} s_2^{-1} \rangle\rangle$, is the maximal group that is abelian and has generators x, y such that $x^2 = y^2 = e$. Prove that G_{abel} is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. □

That proves $\overline{G} \neq (e)$, but since we hardly expect $\overline{G}$ to be commutative we must search farther afield for concrete models of this group. A larger group with the desired relations is the **infinite dihedral group** $D_\infty = \langle \rho, \sigma \rangle$ whose generators satisfy

$$o(\sigma) = 2 \qquad o(\rho) = \infty \text{ (no relations imposed on } \rho) \qquad \sigma\rho\sigma\rho = e$$

It is easy to see, as we did with D_n, that the elements $\{\rho^i \sigma^j : i \in \mathbb{Z},\ j \in \mathbb{Z}_2\}$ form a group, and that every element in D_∞ has a unique decomposition $g = \rho^i \sigma^j$. To see the connection between D_∞ and $\overline{G}$ we note that $N = \langle \rho \rangle \cong \mathbb{Z}$ is a normal subgroup of index 2 in D_∞, and every element $\rho^i \sigma$ in the other coset has order 2 because $\rho^i \sigma \rho^i \sigma = \rho^i \rho^{-i} = e$. Taking $x' = \rho\sigma$ and $y' = \sigma$ we see that $\rho = x'y',\ \sigma = y'$, so D_∞ has generators x', y' satisfying the relations that define the maximal group $\overline{G}$, and hence there is a surjective homomorphism $\phi : \overline{G} \to D_\infty$ such that $\phi(x) = x', \phi(y) = y'$.

On the other hand, the elements $\rho' = xy$, $\sigma' = y$ in $\overline{G}$ satisfy the same relation $\rho'\sigma'\rho'\sigma' = xyyxyy = e$ as the generators ρ, σ in D_∞, so if we define the map $\psi : D_\infty \to \overline{G}$

$$\psi(\rho^i\sigma^j) = (\rho')^i(\sigma')^j = (xy)^i y^j$$

we get a homomorphism because

$$\begin{aligned}
\psi(\rho^i\sigma^j \cdot \rho^k\sigma^\ell) &= \psi(\rho^{i+(-1)^j k}\,\sigma^{j+\ell}) \\
&= (\rho')^{i+(-1)^j k}\,(\sigma')^{j+\ell} \\
&= (\rho')^i(\sigma')^j \cdot (\rho')^k(\sigma')^\ell = \psi(\rho^i\sigma^j)\cdot\psi(\rho^k\sigma^\ell)
\end{aligned}$$

Obviously $\phi \circ \psi = \psi \circ \phi = \mathrm{id}$ since this is true on sets of generators, so ψ is a bijection and $\overline{G} \cong D_\infty$. $\square$

There is a geometric model of D_∞ but it differs from previous models that described the finite dihedral groups D_n as the rigid-motion symmetries of the regular n-gon. Consider the group $G = \langle r, s\rangle$ of rigid motions generated by

$$\begin{aligned}
r &= \text{(rotation about the origin } \mathbf{0} = (0,0) \text{ by } 180^\circ) \\
s &= \text{(rotation about } \mathbf{p} = (1,0) \text{ by } 180^\circ)
\end{aligned}$$

We denote translation operators by $t_a : v \mapsto v + a$, noting that the set of all translations $T = \{t_a : a \in \mathbb{R}^2\}$ form a group of rigid motions isomorphic to $(\mathbb{R}^2, +)$ since $t_a \circ t_b = t_{a+b}$.

7.2.22 Exercise. Defining G as above

(a) Prove that $s = t_p \circ r \circ t_{-p}$, and that $r \circ t_a \circ r^{-1} = t_{r(a)}$ for all $a \in \mathbb{R}^2$.

(b) The subgroup $T_G = G \cap T$ of translations in G is equal to $\{t_{(2k,0)} : k \in \mathbb{Z}\}$. It is normal in G and isomorphic to $\mathbb{Z}$.

(c) Prove that $G \cong D_\infty$. $\square$