Definitions 2.1.12. We write $M_n(\mathbf{R})$ for the set of $n \times n$ matrices over the real numbers, $\mathbf{R}$. We shall make use of the binary operation of matrix multiplication, which is defined as follows. If

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ & \vdots & \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} b_{11} & \dots & b_{1n} \\ & \vdots & \\ b_{n1} & \dots & b_{nn} \end{pmatrix},$$

then the product AB is the matrix whose ij-th coordinate is

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj} = a_{i1} b_{1j} + \cdots + a_{in} b_{nj}.$$

We write $I = I_n$ for the $n \times n$ identity matrix: the matrix whose diagonal entries are all equal to 1 and whose off-diagonal entries are all equal to 0.

Thus, $I_2 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $I_3 = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$, etc.

The properties we need here regarding matrix multiplication are few. We shall discuss matrices in greater detail in Section 7.10 and Chapter 10.

Lemma 2.1.13. *Multiplication of $n \times n$ matrices gives an associative binary operation on $M_n(\mathbf{R})$. Moreover, I_n is an identity element for this operation. Thus, $M_n(\mathbf{R})$ is a monoid under matrix multiplication.* □

The invertible elements in this monoid structure on $M_n(\mathbf{R})$ are precisely the invertible matrices in the usual sense. As such, they merit a name.

Definition 2.1.14. We write $\mathrm{Gl}_n(\mathbf{R})$ for $\mathrm{Inv}(M_n(\mathbf{R}))$, the group of invertible elements of $M_n(\mathbf{R})$. We call it the n-th general linear group of $\mathbf{R}$.

Later in this chapter, we shall construct two infinite families of finite nonabelian groups, the dihedral groups and the quaternionic groups, as explicit subgroups of $\mathrm{Gl}_n(\mathbf{R})$ for $n = 2$ and 4, respectively. We shall show in Chapter 10 that every finite group is a subgroup of $\mathrm{Gl}_n(\mathbf{R})$ for some value of n.

It is sometimes useful to study partial inverses in a monoid.

Definitions 2.1.15. Let X be a monoid with identity element e. If $x, y \in X$ with $xy = e$, then we say that x is a left inverse for y and that y is a right inverse for x.

Exercises 2.1.16.

1. Let M be the set of all nonzero integers. Then M is a monoid under multiplication. What is $\mathrm{Inv}(M)$?

† 2. Let G be a group and let $x, y \in G$. Show that x and y commute if and only if $x^2y^2 = (xy)^2$.

† 3. Let G be a group such that $x^2 = e$ for all $x \in G$. Show that G is abelian.

4. Let G be a group and let $x_1, \dots, x_k \in G$. Show that $(x_1 \dots x_k)^{-1} = x_k^{-1} \dots x_1^{-1}$.

5. Let G be a group and let $x, y \in G$. Show that x and y commute if and only if $(xy)^{-1} = x^{-1}y^{-1}$.

6. Let G be a group and let $x, y \in G$. Suppose there are three consecutive integers n such that $x^n y^n = (xy)^n$. Show that x and y commute.

7. Let G be an abelian group and let $x, y \in G$. Show that $x^n y^n = (xy)^n$ for all $n \in \mathbf{Z}$.

8. Verify that multiplication of $n \times n$ matrices is associative.

9. Show that $\mathrm{Gl}_1(\mathbf{R})$ is isomorphic to $\mathbf{R}^\times$, the group of non-zero real numbers under multiplication.

10. Show that $\mathrm{Gl}_n(\mathbf{R})$ is nonabelian for $n \geq 2$.

11. Let
$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \;\middle|\; b \in \mathbf{R},\ a, c \in \mathbf{Q} \text{ and } ac \neq 0 \right\}.$$
Show that G is a group under matrix multiplication. Is G abelian?

12. Let X be a monoid. Suppose that $x \in X$ has a left inverse, y, and a right inverse, z. Show that $y = z$, and that x is invertible with inverse y.

† 13. Let X be a monoid with the property that every element of X has a left inverse. Show that X is a group.

14. Let X be a finite monoid with the left cancellation property: if $xy = xz$, then $y = z$. Show that X is a group.

15. Let X be a finite set with an associative binary operation. Suppose this operation has both the left and the right cancellation properties. Show that X is a group.

2.2 Subgroups

One can tell quite a bit about about a group by knowing its subgroups.

Definitions 2.2.1. A subset S of a group G is said to be closed under multiplication if for x and y in S, the product xy is also in S.

A subset H of G is said to be a subgroup if it is nonempty and closed under multiplication, and if for each $x \in H$, the inverse element x^{-1} is also in H.

Examples 2.2.2.

1. The groups $\mathbf{Z}$ and $\mathbf{Q}$ are subgroups of $\mathbf{R}$.

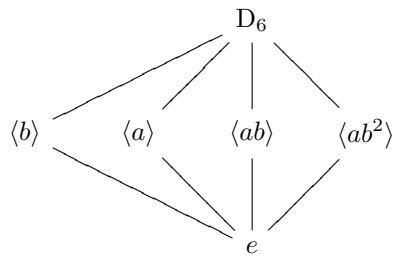
2. The inclusions below are all inclusions of subgroups.
$$\begin{array}{ccc} \mathbf{Q}_+^\times & \subset & \mathbf{Q}^\times \\ \cap & & \cap \\ \mathbf{R}_+^\times & \subset & \mathbf{R}^\times \end{array}$$

3. $\mathbf{Z}_+ \subset \mathbf{R}_+^\times$ is closed under multiplication, but is not a subgroup, because the inverses in $\mathbf{R}_+^\times$ of the non-identity elements of $\mathbf{Z}_+$ do not lie in $\mathbf{Z}_+$.

4. Any group G is a subgroup of itself.

5. For any group G, consider the subset $\{e\} \subset G$, consisting of the identity element alone. Because $e \cdot e = e$ and $e^{-1} = e$, $\{e\}$ is a subgroup of G, called the trivial subgroup, or identity subgroup. By abuse of notation (i.e., for convenience), we shall generally write e in place of $\{e\}$ for this subgroup. (When the identity element is called 1 or 0, we shall write 1 or 0 for the trivial subgroup as well.)

Example 2.2.16. We write D_6 for the dihedral group of order 6. As will become clear later, the following is the lattice of subgroups of D_6.



Here, $\langle b \rangle$ has order 3, while $\langle a \rangle$, $\langle ab \rangle$, and $\langle ab^2 \rangle$ have order 2. The upward-slanted lines represent the inclusions of subgroups.

Because the elements of monoids don't necessarily have inverses, the definition of a submonoid will have to be different from that of a subgroup.

Definition 2.2.17. A submonoid of a monoid M is a subset which is closed under multiplication and contains the identity element.

Exercises 2.2.18.

1. Show that in the real numbers $\mathbf{R}$, the cyclic subgroup generated by 1 is the integers. In particular, $\mathbf{Z}$ is cyclic.

2. In $\mathbf{Z}$, show that $\langle n \rangle = \mathbf{Z}$ if and only if $n = \pm 1$.

3. Consider the group, $\mathbf{Q}_+^\times$, of positive rational numbers under multiplication. What are the elements of $\langle 2 \rangle \subset \mathbf{Q}_+^\times$?

4. Consider the group $\mathbf{Q}^\times$ of nonzero rational numbers under multiplication. What are the elements of $\langle -1 \rangle \subset \mathbf{Q}^\times$? What are the elements of $\langle -2 \rangle$?

† 5. Let M be a monoid. We can define the positive powers of the elements in M in exactly the same way that positive powers in a group are defined. We have $m^1 = m$ for all $m \in M$, and the higher powers are defined by induction: $m^k = m^{k-1}m$. Show that for $m \in M$ and for $i, j \geq 1$, we have

   (a) $m^i \cdot m^j = m^{i+j}$, and

   (b) $(m^i)^j = m^{ij}$.

6. In $\mathbf{Z}$, show that $\langle 2, 3 \rangle = \mathbf{Z}$.

7. In $\mathbf{Z}$, show that $\langle 3n, 5n \rangle = \langle n \rangle$ for any $n \in \mathbf{Z}$.

8. In the group, $\mathbf{Q}_+^\times$, of positive rational numbers under multiplication, show that $\langle 2, 3 \rangle$ is not a cyclic subgroup. In other words, there is no rational number q such that $\langle 2, 3 \rangle = \langle q \rangle$.

9. Show that $\mathbf{Q}_+^\times$ is generated by the set of all prime numbers.

10. Show that the group $\mathbf{Q}^\times$ of nonzero rational numbers is generated by the set consisting of -1 and all of the prime numbers.

11. Let G be a group and let $a, b \in G$ such that $aba^{-1} \in \langle b \rangle$. Show that $H = \{a^i b^j \mid i, j \in \mathbf{Z}\}$ is a subgroup of G. Deduce that $H = \langle a, b \rangle$.

12. In $\mathbf{Z}$, show that $\langle 2 \rangle \cap \langle 3 \rangle = \langle 6 \rangle$.

13. In $\mathbf{Z}$, show that $\langle m \rangle \cap \langle n \rangle = \langle k \rangle$, where k is the least common multiple of m and n.

14. In the group $\mathbf{Q}_+^\times$ of positive rational numbers under multiplication, show that $\langle 2 \rangle \cap \langle 3 \rangle = 1$. Here, 1 is the trivial subgroup of $\mathbf{Q}_+^\times$.

15. Let M be a monoid. Show that the group of invertible elements $\mathrm{Inv}(M)$ is a submonoid of M.

16. Show that not every submonoid of a group is a group.

17. Show that every submonoid of a finite group is a group.

2.3 The Subgroups of the Integers

One of the simplest yet most powerful results in mathematics is the Euclidean Algorithm. We shall use it here to identify all subgroups of $\mathbf{Z}$ and to derive the properties of prime decomposition in $\mathbf{Z}$.

Theorem 2.3.1. (The Euclidean Algorithm[2]) *Let m and n be integers, with $n > 0$. Then there are integers q and r, with $0 \leq r < n$, such that $m = qn + r$.*

Proof First, we assume that $m \geq 0$, and argue by induction on m. If $m < n$, we may take $q = 0$ and $r = m$. If $m = n$, we take $q = 1$ and $r = 0$. Thus, we may assume that $m > n$ and that the result holds for all non-negative integers less than m.

In particular, the induction hypothesis gives

$$m - 1 = q'n + r',$$

for integers q' and r' with $0 \leq r' < n$. If $r' < n - 1$, we may take $q = q'$ and $r = r' + 1$ for the desired result. Otherwise, $m = (q' + 1)n$, and the proof for $m \geq 0$ is complete.

If $m < 0$, then $-m$ is positive, and hence $-m = q'n + r'$ with $0 \leq r' < n$. If $r' = 0$, this gives $m = -q'n$. Otherwise, we have $m = -q'n - r'$. Subtracting and adding a copy of n on the right of the equation gives $m = (-q' - 1)n + (n - r')$, and since $0 < r' < n$, we have $0 < n - r' < n$ as well. □

We shall use this to characterize the subgroups of $\mathbf{Z}$. The subgroups we already know are the cyclic ones:

$$\langle n \rangle = \{qn \mid q \in \mathbf{Z}\}.$$

We shall next show that these are all the subgroups of $\mathbf{Z}$. First, note that if H is a nonzero subgroup of $\mathbf{Z}$, then there must be a nonzero element in it, and hence, by closure under inverses, a positive element. Since the set of positive integers less than or equal to a given one is finite, there is a unique smallest positive element in it.

[2]The terminology that we've chosen here is not universal. There are some mathematicians who refer to Theorem 2.3.1 as the Division Algorithm, and use the term Euclidean Algorithm for the procedure for calculating greatest common divisors, outlined in Problem 3 of Exercises 2.3.18.