(5) In the multiplicative group $(\mathbb{Z}/7\mathbb{Z})^\times$, the powers of the element $\bar{2}$ are $\bar{2}, \bar{4}, \bar{8} = \bar{1}$, the identity in this group, so $\bar{2}$ has order 3. Similarly, the element $\bar{3}$ has order 6, since 3^6 is the smallest positive power of 3 that is congruent to 1 modulo 7.

Definition. Let $G = \{g_1, g_2, \ldots, g_n\}$ be a finite group with $g_1 = 1$. The *multiplication table* or *group table* of G is the $n \times n$ matrix whose i, j entry is the group element $g_i g_j$.

For a finite group the multiplication table contains, in some sense, all the information about the group. Computationally, however, it is an unwieldly object (being of size the square of the group order) and visually it is not a very useful object for determining properties of the group. One might think of a group table as the analogue of having a table of all the distances between pairs of cities in the country. Such a table is useful and, in essence, captures all the distance relationships, yet a map (better yet, a map with all the distances labelled on it) is a much easier tool to work with. Part of our initial development of the theory of groups (finite groups in particular) is directed towards a more conceptual way of visualizing the internal structure of groups.

EXERCISES

Let G be a group.

1. Determine which of the following binary operations are associative:
   (a) the operation $\star$ on $\mathbb{Z}$ defined by $a \star b = a - b$
   (b) the operation $\star$ on $\mathbb{R}$ defined by $a \star b = a + b + ab$
   (c) the operation $\star$ on $\mathbb{Q}$ defined by $a \star b = \dfrac{a+b}{5}$
   (d) the operation $\star$ on $\mathbb{Z} \times \mathbb{Z}$ defined by $(a, b) \star (c, d) = (ad + bc, bd)$
   (e) the operation $\star$ on $\mathbb{Q} - \{0\}$ defined by $a \star b = \dfrac{a}{b}$.
2. Decide which of the binary operations in the preceding exercise are commutative.
3. Prove that addition of residue classes in $\mathbb{Z}/n\mathbb{Z}$ is associative (you may assume it is well defined).
4. Prove that multiplication of residue classes in $\mathbb{Z}/n\mathbb{Z}$ is associative (you may assume it is well defined).
5. Prove for all $n > 1$ that $\mathbb{Z}/n\mathbb{Z}$ is not a group under multiplication of residue classes.
6. Determine which of the following sets are groups under addition:
   (a) the set of rational numbers (including $0 = 0/1$) in lowest terms whose denominators are odd
   (b) the set of rational numbers (including $0 = 0/1$) in lowest terms whose denominators are even
   (c) the set of rational numbers of absolute value < 1
   (d) the set of rational numbers of absolute value ≥ 1 together with 0
   (e) the set of rational numbers with denominators equal to 1 or 2
   (f) the set of rational numbers with denominators equal to 1, 2 or 3.
7. Let $G = \{x \in \mathbb{R} \mid 0 \leq x < 1\}$ and for $x, y \in G$ let $x \star y$ be the fractional part of $x + y$ (i.e., $x \star y = x + y - [x + y]$ where $[a]$ is the greatest integer less than or equal to a). Prove that $\star$ is a well defined binary operation on G and that G is an abelian group under $\star$ (called the *real numbers mod 1*).

8. Let $G = \{z \in \mathbb{C} \mid z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}$.
(a) Prove that G is a group under multiplication (called the group of *roots of unity* in $\mathbb{C}$).
(b) Prove that G is not a group under addition.

9. Let $G = \{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$.
(a) Prove that G is a group under addition.
(b) Prove that the nonzero elements of G are a group under multiplication. ["Rationalize the denominators" to find multiplicative inverses.]

10. Prove that a finite group is abelian if and only if its group table is a symmetric matrix.

11. Find the orders of each element of the additive group $\mathbb{Z}/12\mathbb{Z}$.

12. Find the orders of the following elements of the multiplicative group $(\mathbb{Z}/12\mathbb{Z})^\times$: $\overline{1}$, $\overline{-1}$, $\overline{5}$, $\overline{7}$, $\overline{-7}$, $\overline{13}$.

13. Find the orders of the following elements of the additive group $\mathbb{Z}/36\mathbb{Z}$: $\overline{1}$, $\overline{2}$, $\overline{6}$, $\overline{9}$, $\overline{10}$, $\overline{12}$, $\overline{-1}$, $\overline{-10}$, $\overline{-18}$.

14. Find the orders of the following elements of the multiplicative group $(\mathbb{Z}/36\mathbb{Z})^\times$: $\overline{1}$, $\overline{-1}$, $\overline{5}$, $\overline{13}$, $\overline{-13}$, $\overline{17}$.

15. Prove that $(a_1 a_2 \ldots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \ldots a_1^{-1}$ for all $a_1, a_2, \ldots, a_n \in G$.

16. Let x be an element of G. Prove that $x^2 = 1$ if and only if $|x|$ is either 1 or 2.

17. Let x be an element of G. Prove that if $|x| = n$ for some positive integer n then $x^{-1} = x^{n-1}$.

18. Let x and y be elements of G. Prove that $xy = yx$ if and only if $y^{-1}xy = x$ if and only if $x^{-1}y^{-1}xy = 1$.

19. Let $x \in G$ and let $a, b \in \mathbb{Z}^+$.
(a) Prove that $x^{a+b} = x^a x^b$ and $(x^a)^b = x^{ab}$.
(b) Prove that $(x^a)^{-1} = x^{-a}$.
(c) Establish part (a) for arbitrary integers a and b (positive, negative or zero).

20. For x an element in G show that x and x^{-1} have the same order.

21. Let G be a finite group and let x be an element of G of order n. Prove that if n is odd, then $x = (x^2)^k$ for some k.

22. If x and g are elements of the group G, prove that $|x| = |g^{-1}xg|$. Deduce that $|ab| = |ba|$ for all $a, b \in G$.

23. Suppose $x \in G$ and $|x| = n < \infty$. If $n = st$ for some positive integers s and t, prove that $|x^s| = t$.

24. If a and b are *commuting* elements of G, prove that $(ab)^n = a^n b^n$ for all $n \in \mathbb{Z}$. [Do this by induction for positive n first.]

25. Prove that if $x^2 = 1$ for all $x \in G$ then G is abelian.

26. Assume H is a nonempty subset of $(G, \star)$ which is closed under the binary operation on G and is closed under inverses, i.e., for all h and $k \in H$, hk and $h^{-1} \in H$. Prove that H is a group under the operation $\star$ restricted to H (such a subset H is called a *subgroup* of G).

27. Prove that if x is an element of the group G then $\{x^n \mid n \in \mathbb{Z}\}$ is a subgroup (cf. the preceding exercise) of G (called the *cyclic subgroup* of G generated by x).

28. Let $(A, \star)$ and $(B, \diamond)$ be groups and let $A \times B$ be their direct product (as defined in Example 6). Verify all the group axioms for $A \times B$:
(a) prove that the associative law holds: for all $(a_i, b_i) \in A \times B$, $i = 1, 2, 3$
$(a_1, b_1)[(a_2, b_2)(a_3, b_3)] = [(a_1, b_1)(a_2, b_2)](a_3, b_3)$,

(b) prove that $(1, 1)$ is the identity of $A \times B$, and
(c) prove that the inverse of (a, b) is (a^{-1}, b^{-1}).

29. Prove that $A \times B$ is an abelian group if and only if both A and B are abelian.

30. Prove that the elements $(a, 1)$ and $(1, b)$ of $A \times B$ commute and deduce that the order of (a, b) is the least common multiple of $|a|$ and $|b|$.

31. Prove that any finite group G of even order contains an element of order 2. [Let $t(G)$ be the set $\{g \in G \mid g \neq g^{-1}\}$. Show that $t(G)$ has an even number of elements and every nonidentity element of $G - t(G)$ has order 2.]

32. If x is an element of finite order n in G, prove that the elements $1, x, x^2, \ldots, x^{n-1}$ are all distinct. Deduce that $|x| \leq |G|$.

33. Let x be an element of finite order n in G.
(a) Prove that if n is odd then $x^i \neq x^{-i}$ for all $i = 1, 2, \ldots, n - 1$.
(b) Prove that if $n = 2k$ and $1 \leq i < n$ then $x^i = x^{-i}$ if and only if $i = k$.

34. If x is an element of infinite order in G, prove that the elements x^n, $n \in \mathbb{Z}$ are all distinct.

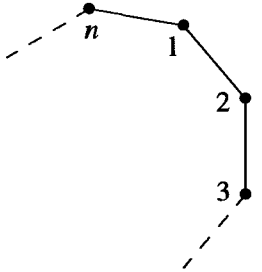
35. If x is an element of finite order n in G, use the Division Algorithm to show that *any* integral power of x equals one of the elements in the set $\{1, x, x^2, \ldots, x^{n-1}\}$ (so these are all the distinct elements of the cyclic subgroup (cf. Exercise 27 above) of G generated by x).

36. Assume $G = \{1, a, b, c\}$ is a group of order 4 with identity 1. Assume also that G has no elements of order 4 (so by Exercise 32, every element has order ≤ 3). Use the cancellation laws to show that there is a unique group table for G. Deduce that G is abelian.

1.2 DIHEDRAL GROUPS

An important family of examples of groups is the class of groups whose elements are symmetries of geometric objects. The simplest subclass is when the geometric objects are regular planar figures.

For each $n \in \mathbb{Z}^+$, $n \geq 3$ let D_{2n} be the set of symmetries of a regular n-gon, where a symmetry is any rigid motion of the n-gon which can be effected by taking a copy of the n-gon, moving this copy in any fashion in 3-space and then placing the copy back on the original n-gon so it exactly covers it. More precisely, we can describe the symmetries by first choosing a labelling of the n vertices, for example as shown in the following figure.



Then each symmetry s can be described uniquely by the corresponding permutation σ of $\{1, 2, 3, \ldots, n\}$ where if the symmetry s puts vertex i in the place where vertex j was originally, then σ is the permutation sending i to j. For instance, if s is a rotation of $2\pi/n$ radians clockwise about the center of the n-gon, then σ is the permutation sending i to $i + 1$, $1 \leq i \leq n - 1$, and $\sigma(n) = 1$. Now make D_{2n} into a group by defining st for $s, t \in D_{2n}$ to be the symmetry obtained by first applying t then s to the n-gon (note that we are viewing symmetries as functions on the n-gon, so st is just function composition — read as usual from right to left). If s, t effect the permutations σ, τ, respectively on the vertices, then st effects $\sigma \circ \tau$. The binary operation on D_{2n} is associative since composition of functions is associative. The identity of D_{2n} is the identity symmetry (which leaves all vertices fixed), denoted by 1, and the inverse of $s \in D_{2n}$ is the symmetry which reverses all rigid motions of s (so if s effects permutation σ on the vertices, s^{-1} effects σ^{-1}). In the next paragraph we show

$$|D_{2n}| = 2n$$

and so D_{2n} is called the *dihedral group of order* $2n$. In some texts this group is written D_n; however, D_{2n} (where the subscript gives the order of the group rather than the number of vertices) is more common in the group theory literature.

To find the order $|D_{2n}|$ observe that given any vertex i, there is a symmetry which sends vertex 1 into position i. Since vertex 2 is adjacent to vertex 1, vertex 2 must end up in position $i + 1$ or $i - 1$ (where $n + 1$ is 1 and $1 - 1$ is n, i.e., the integers labelling the vertices are read mod n). Moreover, by following the first symmetry by a reflection about the line through vertex i and the center of the n-gon one sees that vertex 2 can be sent to either position $i + 1$ or $i - 1$ by some symmetry. Thus there are $n \cdot 2$ positions the ordered pair of vertices 1, 2 may be sent to upon applying symmetries. Since symmetries are rigid motions one sees that once the position of the ordered pair of vertices 1, 2 has been specified, the action of the symmetry on all remaining vertices is completely determined. Thus there are exactly $2n$ symmetries of a regular n-gon. We can, moreover, explicitly exhibit $2n$ symmetries. These symmetries are the n rotations about the center through $2\pi i/n$ radian, $0 \leq i \leq n-1$, and the n reflections through the n lines of symmetry (if n is odd, each symmetry line passes through a vertex and the mid-point of the opposite side; if n is even, there are $n/2$ lines of symmetry which pass through 2 opposite vertices and $n/2$ which perpendicularly bisect two opposite sides). For example, if $n = 4$ and we draw a square at the origin in an x, y plane, the lines of symmetry are