EXERCISES

1. Find all subgroups of $Z_{45} = \langle x \rangle$, giving a generator for each. Describe the containments between these subgroups.
2. If x is an element of the finite group G and $|x| = |G|$, prove that $G = \langle x \rangle$. Give an explicit example to show that this result need not be true if G is an infinite group.
3. Find all generators for $\mathbb{Z}/48\mathbb{Z}$.
4. Find all generators for $\mathbb{Z}/202\mathbb{Z}$.
5. Find the number of generators for $\mathbb{Z}/49000\mathbb{Z}$.
6. In $\mathbb{Z}/48\mathbb{Z}$ write out all elements of $\langle \bar{a} \rangle$ for every $\bar{a}$. Find all inclusions between subgroups in $\mathbb{Z}/48\mathbb{Z}$.
7. Let $Z_{48} = \langle x \rangle$ and use the isomorphism $\mathbb{Z}/48\mathbb{Z} \cong Z_{48}$ given by $\bar{1} \mapsto x$ to list all subgroups of Z_{48} as computed in the preceding exercise.
8. Let $Z_{48} = \langle x \rangle$. For which integers a does the map φ_a defined by $\varphi_a : \bar{1} \mapsto x^a$ extend to an *isomorphism* from $\mathbb{Z}/48\mathbb{Z}$ onto Z_{48}.
9. Let $Z_{36} = \langle x \rangle$. For which integers a does the map ψ_a defined by $\psi_a : \bar{1} \mapsto x^a$ extend to a *well defined homomorphism* from $\mathbb{Z}/48\mathbb{Z}$ into Z_{36}. Can ψ_a ever be a surjective homomorphism?
10. What is the order of $\overline{30}$ in $\mathbb{Z}/54\mathbb{Z}$? Write out all of the elements and their orders in $\langle \overline{30} \rangle$.
11. Find all cyclic subgroups of D_8. Find a proper subgroup of D_8 which is not cyclic.
12. Prove that the following groups are *not* cyclic:
    (a) $Z_2 \times Z_2$
    (b) $Z_2 \times \mathbb{Z}$
    (c) $\mathbb{Z} \times \mathbb{Z}$.
13. Prove that the following pairs of groups are *not* isomorphic:
    (a) $\mathbb{Z} \times Z_2$ and $\mathbb{Z}$
    (b) $\mathbb{Q} \times Z_2$ and $\mathbb{Q}$.
14. Let $\sigma = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12)$. For each of the following integers a compute σ^a: $a = 13, 65, 626, 1195, -6, -81, -570$ and -1211.
15. Prove that $\mathbb{Q} \times \mathbb{Q}$ is not cyclic.
16. Assume $|x| = n$ and $|y| = m$. Suppose that x and y *commute*: $xy = yx$. Prove that $|xy|$ divides the least common multiple of m and n. Need this be true if x and y do *not* commute? Give an example of commuting elements x, y such that the order of xy is not equal to the least common multiple of $|x|$ and $|y|$.
17. Find a presentation for Z_n with one generator.
18. Show that if H is any group and h is an element of H with $h^n = 1$, then there is a unique homomorphism from $Z_n = \langle x \rangle$ to H such that $x \mapsto h$.
19. Show that if H is any group and h is an element of H, then there is a unique homomorphism from $\mathbb{Z}$ to H such that $1 \mapsto h$.
20. Let p be a prime and let n be a positive integer. Show that if x is an element of the group G such that $x^{p^n} = 1$ then $|x| = p^m$ for some $m \leq n$.
21. Let p be an odd prime and let n be a positive integer. Use the Binomial Theorem to show that $(1 + p)^{p^{n-1}} \equiv 1 (\text{mod } p^n)$ but $(1 + p)^{p^{n-2}} \not\equiv 1 (\text{mod } p^n)$. Deduce that $1 + p$ is an element of order p^{n-1} in the multiplicative group $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

22. Let n be an integer ≥ 3. Use the Binomial Theorem to show that $(1+2^2)^{2^{n-2}} \equiv 1 (\text{mod } 2^n)$ but $(1+2^2)^{2^{n-3}} \not\equiv 1 (\text{mod } 2^n)$. Deduce that 5 is an element of order 2^{n-2} in the multiplicative group $(\mathbb{Z}/2^n\mathbb{Z})^\times$.

23. Show that $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic for any $n \geq 3$. [Find two distinct subgroups of order 2.]

24. Let G be a finite group and let $x \in G$.

(a) Prove that if $g \in N_G(\langle x \rangle)$ then $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$.

(b) Prove conversely that if $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$ then $g \in N_G(\langle x \rangle)$. [Show first that $gx^kg^{-1} = (gxg^{-1})^k = x^{ak}$ for any integer k, so that $g\langle x \rangle g^{-1} \leq \langle x \rangle$. If x has order n, show the elements gx^ig^{-1}, $i = 0, 1, \ldots, n-1$ are distinct, so that $|g\langle x \rangle g^{-1}| = |\langle x \rangle| = n$ and conclude that $g\langle x \rangle g^{-1} = \langle x \rangle$.]

Note that this cuts down some of the work in computing normalizers of cyclic subgroups since one does not have to check $ghg^{-1} \in \langle x \rangle$ for every $h \in \langle x \rangle$.

25. Let G be a cyclic group of order n and let k be an integer relatively prime to n. Prove that the map $x \mapsto x^k$ is surjective. Use Lagrange's Theorem (Exercise 19, Section 1.7) to prove the same is true for any finite group of order n. (For such k each element has a k^{th} root in G. It follows from Cauchy's Theorem in Section 3.2 that if k is not relatively prime to the order of G then the map $x \mapsto x^k$ is not surjective.)

26. Let Z_n be a cyclic group of order n and for each integer a let

$$\sigma_a : Z_n \to Z_n \qquad \text{by} \qquad \sigma_a(x) = x^a \text{ for all } x \in Z_n.$$

(a) Prove that σ_a is an automorphism of Z_n if and only if a and n are relatively prime (automorphisms were introduced in Exercise 20, Section 1.6).

(b) Prove that $\sigma_a = \sigma_b$ if and only if $a \equiv b (\text{mod } n)$.

(c) Prove that *every* automorphism of Z_n is equal to σ_a for some integer a.

(d) Prove that $\sigma_a \circ \sigma_b = \sigma_{ab}$. Deduce that the map $\overline{a} \mapsto \sigma_a$ is an isomorphism of $(\mathbb{Z}/n\mathbb{Z})^\times$ onto the automorphism group of Z_n (so $\text{Aut}(Z_n)$ is an abelian group of order $\varphi(n)$).

2.4 SUBGROUPS GENERATED BY SUBSETS OF A GROUP

The method of forming cyclic subgroups of a given group is a special case of the general technique where one forms the subgroup generated by an arbitrary subset of a group. In the case of cyclic subgroups one takes a singleton subset $\{x\}$ of the group G and forms all integral powers of x, which amounts to closing the set $\{x\}$ under the group operation and the process of taking inverses. The resulting subgroup is the smallest subgroup of G which contains the set $\{x\}$ (smallest in the sense that if H is any subgroup which contains $\{x\}$, then H contains $\langle x \rangle$). Another way of saying this is that $\langle x \rangle$ is the unique minimal element of the set of subgroups of G containing x (ordered under inclusion). In this section we investigate analogues of this when $\{x\}$ is replaced by an arbitrary subset of G.

Throughout mathematics the following theme recurs: given an object G (such as a group, field, vector space, etc.) and a subset A of G, is there a unique minimal subobject of G (subgroup, subfield, subspace, etc.) which contains A and, if so, how are the elements of this subobject computed? Students may already have encountered this question in the study of vector spaces. When G is a vector space (with, say, real number scalars) and $A = \{v_1, v_2, \ldots, v_n\}$, then there is a unique smallest subspace of

G which contains A, namely the (linear) span of $v_1, v_2, \ldots, v_n$ and each vector in this span can be written as $k_1v_1 + k_2v_2 + \cdots + k_nv_n$, for some $k_1, \ldots, k_n \in \mathbb{R}$. When A is a single nonzero vector, v, the span of $\{v\}$ is simply the 1-dimensional subspace or line containing v and every element of this subspace is of the form kv for some $k \in \mathbb{R}$. This is the analogue in the theory of vector spaces of cyclic subgroups of a group. Note that the 1-dimensional subspaces contain kv, where $k \in \mathbb{R}$, not just kv, where $k \in \mathbb{Z}$; the reason being that a subspace must be closed under *all* the vector space operations (e.g., scalar multiplication) not just the group operation of vector addition.

Let G be any group and let A be any subset of G. We now make precise the notion of the subgroup of G generated by A. We prove that because the intersection of any set of subgroups of G is also a subgroup of G, the subgroup generated by A is the unique smallest subgroup of G containing A; it is " smallest" in the sense of being the minimal element of the set of all subgroups containing A. We show that the elements of this subgroup are obtained by closing the given subset under the group operation (and taking inverses). In succeeding parts of the text when we develop the theory of other algebraic objects we shall refer to this section as the paradigm in proving that a given subset is contained in a unique smallest subobject and that the elements of this subobject are obtained by closing the subset under the operations which define the object. Since in the latter chapters the details will be omitted, students should acquire a solid understanding of the process at this point.

In order to proceed we need only the following.

Proposition 8. If $\mathcal{A}$ is any nonempty collection of subgroups of G, then the intersection of all members of $\mathcal{A}$ is also a subgroup of G.

Proof: This is an easy application of the subgroup criterion (see also Exercise 10, Section 1). Let

$$K = \bigcap_{H \in \mathcal{A}} H.$$

Since each $H \in \mathcal{A}$ is a subgroup, $1 \in H$, so $1 \in K$, that is, $K \neq \emptyset$. If $a, b \in K$, then $a, b \in H$, for all $H \in \mathcal{A}$. Since each H is a group, $ab^{-1} \in H$, for all H, hence $ab^{-1} \in K$. Proposition 1 gives that $K \leq G$.

Definition. If A is any subset of the group G define

$$\langle A \rangle = \bigcap_{\substack{A \subseteq H \\ H \leq G}} H.$$

This is called the *subgroup of G generated by A.*

Thus $\langle A \rangle$ is the intersection of all subgroups of G containing A. It is a subgroup of G by Proposition 8 applied to the set $\mathcal{A} = \{H \leq G \mid A \subseteq H\}$ ($\mathcal{A}$ is nonempty since $G \in \mathcal{A}$). Since A lies in each $H \in \mathcal{A}$, A is a subset of their intersection, $\langle A \rangle$. Note that $\langle A \rangle$ is the unique minimal element of $\mathcal{A}$ as follows: $\langle A \rangle$ is a subgroup of G containing A, so $\langle A \rangle \in \mathcal{A}$; and any element of $\mathcal{A}$ contains the intersection of all elements in $\mathcal{A}$, i.e., contains $\langle A \rangle$.