When A is the finite set $\{a_1, a_2, \ldots, a_n\}$ we write $\langle a_1, a_2, \ldots, a_n \rangle$ for the group generated by $a_1, a_2, \ldots, a_n$ instead of $\langle \{a_1, a_2, \ldots, a_n\} \rangle$. If A and B are two subsets of G we shall write $\langle A, B \rangle$ in place of $\langle A \cup B \rangle$.

This "top down" approach to defining $\langle A \rangle$ proves existence and uniqueness of the smallest subgroup of G containing A but is not too enlightening as to how to construct the elements in it. As the word "generates" suggests we now define the set which is the closure of A under the group operation (and the process of taking inverses) and prove this set equals $\langle A \rangle$. Let

$$\overline{A} = \{a_1^{\epsilon_1} a_2^{\epsilon_2} \ldots a_n^{\epsilon_n} \mid n \in \mathbb{Z},\ n \geq 0 \text{ and } a_i \in A, \epsilon_i = \pm 1 \text{ for each } i\}$$

where $\overline{A} = \{1\}$ if $A = \emptyset$, so that $\overline{A}$ is the set of all finite products (called *words*) of elements of A and inverses of elements of A. Note that the a_i's need not be distinct, so a^2 is written aa in the notation defining $\overline{A}$. Note also that A is not assumed to be a finite (or even countable) set.

Proposition 9. $\overline{A} = \langle A \rangle$.

Proof: We first prove $\overline{A}$ is a subgroup. Note that $\overline{A} \neq \emptyset$ (even if $A = \emptyset$). If $a, b \in \overline{A}$ with $a = a_1^{\epsilon_1} a_2^{\epsilon_2} \ldots a_n^{\epsilon_n}$ and $b = b_1^{\delta_1} b_2^{\delta_2} \ldots b_m^{\delta_m}$, then

$$ab^{-1} = a_1^{\epsilon_1} a_2^{\epsilon_2} \ldots a_n^{\epsilon_n} \cdot b_m^{-\delta_m} b_{m-1}^{-\delta_{m-1}} \ldots b_1^{-\delta_1}$$

(where we used Exercise 15 of Section 1.1 to compute b^{-1}). Thus ab^{-1} is a product of elements of A raised to powers ± 1, hence $ab^{-1} \in \overline{A}$. Proposition 1 implies $\overline{A}$ is a subgroup of G.

Since each $a \in A$ may be written a^1, it follows that $A \subseteq \overline{A}$, hence $\langle A \rangle \subseteq \overline{A}$. But $\langle A \rangle$ is a group containing A and, since it is closed under the group operation and the process of taking inverses, $\langle A \rangle$ contains each element of the form $a_1^{\epsilon_1} a_2^{\epsilon_2} \ldots a_n^{\epsilon_n}$, that is, $\overline{A} \subseteq \langle A \rangle$. This completes the proof of the proposition.

We now use $\langle A \rangle$ in place of $\overline{A}$ and may take the definition of $\overline{A}$ as an equivalent definition of $\langle A \rangle$. As noted above, in this equivalent definition of $\langle A \rangle$, products of the form $a \cdot a$, $a \cdot a \cdot a$, $a \cdot a^{-1}$, etc. could have been simplified to $a^2, a^3, 1$, etc. respectively, so another way of writing $\langle A \rangle$ is

$$\langle A \rangle = \{a_1^{\alpha_1} a_2^{\alpha_2} \ldots a_n^{\alpha_n} \mid \text{for each } i, \quad a_i \in A, \alpha_i \in \mathbb{Z}, a_i \neq a_{i+1} \text{ and } n \in \mathbb{Z}^+\}.$$

In fact, when $A = \{x\}$ this was our definition of $\langle A \rangle$.

If G is *abelian*, we could commute the a_i's and so collect all powers of a given generator together. For instance, if A were the finite subset $\{a_1, a_2, \ldots, a_k\}$ of the abelian group G, one easily checks that

$$\langle A \rangle = \{a_1^{\alpha_1} a_2^{\alpha_2} \ldots a_k^{\alpha_k} \mid \alpha_i \in \mathbb{Z} \text{ for each } i\}.$$

If in this situation we further assume that each a_i has finite order d_i, for all i, then since there are exactly d_i distinct powers of a_i, the total number of distinct products of the form $a_1^{\alpha_1} a_2^{\alpha_2} \ldots a_k^{\alpha_k}$ is at most $d_1 d_2 \ldots d_k$, that is,

$$|\langle A \rangle| \leq d_1 d_2 \ldots d_k.$$

It may happen that $a^\alpha b^\beta = a^\gamma b^\delta$ even though $a^\alpha \neq a^\gamma$ and $b^\beta \neq b^\delta$. We shall explore exactly when this happens when we study direct products in Chapter 5.

When G is *non-abelian* the situation is much more complicated. For example, let $G = D_8$ and let r and s be the usual generators of D_8 (note that the notation $D_8 = \langle r, s \rangle$ is consistent with the notation introduced in Section 1.2). Let $a = s$, let $b = rs$ and let $A = \{a, b\}$. Since both s and r ($= rs \cdot s$) belong to $\langle a, b \rangle$, $G = \langle a, b \rangle$, i.e., G is also generated by a and b. Both a and b have order 2, however D_8 has order 8. This means that it is *not* possible to write every element of D_8 in the form $a^\alpha b^\beta$, $\alpha, \beta \in \mathbb{Z}$. More specifically, the product aba cannot be simplified to a product of the form $a^\alpha b^\beta$. In fact, if $G = D_{2n}$ for any $n > 2$, and r, s, a, b are defined in the same way as above, it is still true that

$$|a| = |b| = 2, \quad D_{2n} = \langle a, b \rangle \quad \text{and} \quad |D_{2n}| = 2n.$$

This means that for large n, long products of the form $abab \dots ab$ cannot be further simplified. In particular, this illustrates that, unlike the abelian (or, better yet, cyclic) group case, the order of a (finite) group cannot even be bounded once we know the orders of the elements in some generating set.

Another example of this phenomenon is S_n:

$$S_n = \langle (1\,2), (1\,2\,3 \dots n) \rangle.$$

Thus S_n is generated by an element of order 2 together with one of order n, yet $|S_n| = n!$ (we shall prove these statements later after developing some more techniques).

One final example emphasizes the fact that if G is non-abelian, subgroups of G generated by more than one element of G may be quite complicated. Let

$$G = GL_2(\mathbb{R}), \quad a = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 2 \\ 1/2 & 0 \end{pmatrix}$$

so $a^2 = b^2 = 1$ but $ab = \begin{pmatrix} 1/2 & 0 \\ 0 & 2 \end{pmatrix}$. It is easy to see that ab has infinite order, so $\langle a, b \rangle$ is an *infinite* subgroup of $GL_2(\mathbb{R})$ which is generated by two elements of order 2.

These examples illustrate that when $|A| \geq 2$ it is difficult, in general, to compute even the order of the subgroup generated by A, let alone any other structural properties. It is therefore impractical to gather much information about subgroups of a non-abelian group created by taking random subsets A and trying to write out the elements of (or other information about) $\langle A \rangle$. For certain "well chosen" subsets A, even of a non-abelian group G, we shall be able to make both theoretical and computational use of the subgroup generated by A. One example of this might be when we want to find a subgroup of G which contains $\langle x \rangle$ properly; we might search for some element y which commutes with x (i.e., $y \in C_G(x)$) and form $\langle x, y \rangle$. It is easy to check that the latter group is abelian, so its order is bounded by $|x||y|$. Alternatively, we might instead take y in $N_G(\langle x \rangle)$ — in this case the same order bound holds and the structure of $\langle x, y \rangle$ is again not too complicated (as we shall see in the next chapter).

The complications which arise for non-abelian groups are generally not quite as serious when we study other basic algebraic systems because of the additional algebraic structure imposed.

EXERCISES

1. Prove that if H is a subgroup of G then $\langle H \rangle = H$.
2. Prove that if A is a subset of B then $\langle A \rangle \leq \langle B \rangle$. Give an example where $A \subseteq B$ with $A \neq B$ but $\langle A \rangle = \langle B \rangle$.
3. Prove that if H is an abelian subgroup of a group G then $\langle H, Z(G) \rangle$ is abelian. Give an explicit example of an abelian subgroup H of a group G such that $\langle H, C_G(H) \rangle$ is not abelian.
4. Prove that if H is a subgroup of G then H is generated by the set $H - \{1\}$.
5. Prove that the subgroup generated by any two distinct elements of order 2 in S_3 is all of S_3.
6. Prove that the subgroup of S_4 generated by $(1\ 2)$ and $(1\ 2)(3\ 4)$ is a noncyclic group of order 4.
7. Prove that the subgroup of S_4 generated by $(1\ 2)$ and $(1\ 3)(2\ 4)$ is isomorphic to the dihedral group of order 8.
8. Prove that $S_4 = \langle (1\ 2\ 3\ 4),\ (1\ 2\ 4\ 3) \rangle$.
9. Prove that $SL_2(\mathbb{F}_3)$ is the subgroup of $GL_2(\mathbb{F}_3)$ generated by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. [Recall from Exercise 9 of Section 1 that $SL_2(\mathbb{F}_3)$ is the subgroup of matrices of determinant 1. You may assume this subgroup has order 24 — this will be an exercise in Section 3.2.]
10. Prove that the subgroup of $SL_2(\mathbb{F}_3)$ generated by $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is isomorphic to the quaternion group of order 8. [Use a presentation for Q_8.]
11. Show that $SL_2(\mathbb{F}_3)$ and S_4 are two nonisomorphic groups of order 24.
12. Prove that the subgroup of upper triangular matrices in $GL_3(\mathbb{F}_2)$ is isomorphic to the dihedral group of order 8 (cf. Exercise 16, Section 1). [First find the order of this subgroup.]
13. Prove that the multiplicative group of positive rational numbers is generated by the set $\{\frac{1}{p} \mid p \text{ is a prime}\}$.
14. A group H is called *finitely generated* if there is a finite set A such that $H = \langle A \rangle$.
    (a) Prove that every finite group is finitely generated.
    (b) Prove that $\mathbb{Z}$ is finitely generated.
    (c) Prove that every finitely generated subgroup of the additive group $\mathbb{Q}$ is cyclic. [If H is a finitely generated subgroup of $\mathbb{Q}$, show that $H \leq \langle \frac{1}{k} \rangle$, where k is the product of all the denominators which appear in a set of generators for H.]
    (d) Prove that $\mathbb{Q}$ is not finitely generated.
15. Exhibit a proper subgroup of $\mathbb{Q}$ which is not cyclic.
16. A subgroup M of a group G is called a *maximal subgroup* if $M \neq G$ and the only subgroups of G which contain M are M and G.
    (a) Prove that if H is a proper subgroup of the finite group G then there is a maximal subgroup of G containing H.
    (b) Show that the subgroup of all rotations in a dihedral group is a maximal subgroup.
    (c) Show that if $G = \langle x \rangle$ is a cyclic group of order $n \geq 1$ then a subgroup H is maximal if and only $H = \langle x^p \rangle$ for some prime p dividing n.
17. This is an exercise involving Zorn's Lemma (see Appendix I) to prove that every nontrivial finitely generated group possesses maximal subgroups. Let G be a finitely generated