even well defined. For example, consider the product of the two left cosets $1H$ and $(1\ 3)H$. The elements 1 and $(1\ 2)$ are both representatives for the coset $1H$, yet $1 \cdot (1\ 3) = (1\ 3)$ and $(1\ 2) \cdot (1\ 3) = (1\ 3\ 2)$ are not both elements of the same left coset as they should be if the product of these cosets were independent of the particular representatives chosen. This is an example of Theorem 6 which states that the cosets of a subgroup form a group *only* when the subgroup is a normal subgroup.

(2) Let $G = S_n$ for some $n \in \mathbb{Z}^+$ and fix some $i \in \{1, 2, \dots, n\}$. As in Section 2.2 let

$$G_i = \{\sigma \in G \mid \sigma(i) = i\}$$

be the stabilizer of the point i. Suppose $\tau \in G$ and $\tau(i) = j$. It follows directly from the definition of G_i that for all $\sigma \in G_i$, $\tau\sigma(i) = j$. Furthermore, if $\mu \in G$ and $\mu(i) = j$, then $\tau^{-1}\mu(i) = i$, that is, $\tau^{-1}\mu \in G_i$, so $\mu \in \tau G_i$. This proves that

$$\tau G_i = \{\mu \in G \mid \mu(i) = j\},$$

i.e., the left coset τG_i consists of the permutations in S_n which take i to j. We can clearly see that distinct left cosets have empty intersection and that the number of distinct left cosets equals the number of distinct images of the integer i under the action of G, namely there are n distinct left cosets. Thus $|G : G_i| = n$. Using the same notation let $k = \tau^{-1}(i)$, so that $\tau(k) = i$. By similar reasoning we see that

$$G_i\tau = \{\lambda \in G \mid \lambda(k) = i\},$$

i.e., the right coset $G_i\tau$ consists of the permutations in S_n which take k to i. If $n > 2$, for some nonidentity element τ we have $\tau G_i \neq G_i\tau$ since there are certainly permutations which take i to j but do not take k to i. Thus G_i is not a normal subgroup. In fact $N_G(G_i) = G_i$ by Exercise 30 of Section 1, so G_i is in some sense far from being normal in S_n. This example generalizes the preceding one.

(3) In D_8 the only subgroup of order 2 which is normal is the center $\langle r^2 \rangle$.

We shall see many more examples of non-normal subgroups as we develop the theory.

The *full converse* to Lagrange's Theorem is *not* true: namely, if G is a finite group and n divides $|G|$, then G need not have a subgroup of order n. For example, let A be the group of symmetries of a regular tetrahedron. By Exercise 9 of Section 1.2, $|A| = 12$. Suppose A had a subgroup H of order 6. Since $\dfrac{|A|}{|H|} = 2$, H would be of index 2 in A, hence $H \trianglelefteq A$ and $A/H \cong Z_2$. Since the quotient group has order 2, the square of every element in the quotient is the identity, so for all $g \in A$, $(gH)^2 = 1H$, that is, for all $g \in A$, $g^2 \in H$. If g is an element of A of order 3, we obtain $g = (g^2)^2 \in H$, that is, H must contain all elements of A of order 3. This is a contradiction since $|H| = 6$ but one can easily exhibit 8 rotations of a tetrahedron of order 3.

There are some partial converses to Lagrange's Theorem. For finite *abelian* groups the full converse of Lagrange is true, namely an abelian group has a subgroup of order n for each divisor n of $|G|$ (in fact, this holds under weaker assumptions than "abelian"; we shall see this in Chapter 6). A partial converse which holds for arbitrary finite groups is the following result:

Theorem 11. *(Cauchy's Theorem)* If G is a finite group and p is a prime dividing $|G|$, then G has an element of order p.

Proof: We shall give a proof of this in the next chapter and another elegant proof is outlined in Exercise 9.

The strongest converse to Lagrange's Theorem which applies to *arbitrary* finite groups is the following:

Theorem 12. (Sylow) If G is a finite group of order $p^\alpha m$, where p is a prime and p does not divide m, then G has a subgroup of order p^α.

We shall prove this theorem in the next chapter and derive more information on the number of subgroups of order p^α.

We conclude this section with some useful results involving cosets.

Definition. Let H and K be subgroups of a group and define

$$HK = \{hk \mid h \in H,\ k \in K\}.$$

Proposition 13. If H and K are finite subgroups of a group then

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Proof: Notice that HK is a union of left cosets of K, namely,

$$HK = \bigcup_{h \in H} hK.$$

Since each coset of K has $|K|$ elements it suffices to find the number of *distinct* left cosets of the form hK, $h \in H$. But $h_1K = h_2K$ for $h_1, h_2 \in H$ if and only if $h_2^{-1}h_1 \in K$. Thus

$$h_1K = h_2K \quad \Leftrightarrow \quad h_2^{-1}h_1 \in H \cap K \quad \Leftrightarrow \quad h_1(H \cap K) = h_2(H \cap K).$$

Thus the number of distinct cosets of the form hK, for $h \in H$ is the number of distinct cosets $h(H \cap K)$, for $h \in H$. The latter number, by Lagrange's Theorem, equals $\frac{|H|}{|H \cap K|}$. Thus HK consists of $\frac{|H|}{|H \cap K|}$ distinct cosets of K (each of which has $|K|$ elements) which gives the formula above.

Notice that there was no assumption that HK be a subgroup in Proposition 13. For example, if $G = S_3$, $H = \langle (1\,2) \rangle$ and $K = \langle (2\,3) \rangle$, then $|H| = |K| = 2$ and $|H \cap K| = 1$, so $|HK| = 4$. By Lagrange's Theorem HK cannot be a subgroup. As a consequence, we must have $S_3 = \langle (1\,2), (2\,3) \rangle$.

Proposition 14. If H and K are subgroups of a group, HK is a subgroup if and only if $HK = KH$.

Proof: Assume first that $HK = KH$ and let $a, b \in HK$. We prove $ab^{-1} \in HK$ so HK is a subgroup by the subgroup criterion. Let

$$a = h_1k_1 \qquad \text{and} \qquad b = h_2k_2,$$

for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Thus $b^{-1} = k_2^{-1}h_2^{-1}$, so $ab^{-1} = h_1k_1k_2^{-1}h_2^{-1}$. Let $k_3 = k_1k_2^{-1} \in K$ and $h_3 = h_2^{-1}$. Thus $ab^{-1} = h_1k_3h_3$. Since $HK = KH$,

$$k_3h_3 = h_4k_4, \qquad \text{for some } h_4 \in H, \quad k_4 \in K.$$

Thus $ab^{-1} = h_1h_4k_4$, and since $h_1h_4 \in H, k_4 \in K$, we obtain $ab^{-1} \in HK$, as desired.

Conversely, assume that HK is a subgroup of G. Since $K \leq HK$ and $H \leq HK$, by the closure property of subgroups, $KH \subseteq HK$. To show the reverse containment let $hk \in HK$. Since HK is assumed to be a subgroup, write $hk = a^{-1}$, for some $a \in HK$. If $a = h_1k_1$, then

$$hk = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH,$$

completing the proof.

Note that $HK = KH$ does *not* imply that the elements of H commute with those of K (contrary to what the notation may suggest) but rather that every product hk is of the form $k'h'$ (h need not be h' nor k be k') and conversely. For example, if $G = D_{2n}$, $H = \langle r \rangle$ and $K = \langle s \rangle$, then $G = HK = KH$ so that HK is a subgroup and $rs = sr^{-1}$ so the elements of H do not commute with the elements of K. This is an example of the following sufficient condition for HK to be a subgroup:

Corollary 15. If H and K are subgroups of G and $H \leq N_G(K)$, then HK is a subgroup of G. In particular, if $K \trianglelefteq G$ then $HK \leq G$ for any $H \leq G$.

Proof: We prove $HK = KH$. Let $h \in H$, $k \in K$. By assumption, $hkh^{-1} \in K$, hence

$$hk = (hkh^{-1})h \in KH.$$

This proves $HK \subseteq KH$. Similarly, $kh = h(h^{-1}kh) \in HK$, proving the reverse containment. The corollary follows now from the preceding proposition.

Definition. If A is any subset of $N_G(K)$ (or $C_G(K)$), we shall say A *normalizes* K (*centralizes* K, respectively).

With this terminology, Corollary 15 states that HK *is a subgroup if* H *normalizes* K (similarly, HK *is a subgroup if* K *normalizes* H).

In some instances one can prove that a finite group is a product of two of its subgroups by simply using the order formula in Proposition 13. For example, let $G = S_4$, $H = D_8$ and let $K = \langle (1\,2\,3) \rangle$, where we consider D_8 as a subgroup of S_4 by identifying each symmetry with its permutation on the 4 vertices of a square (under some fixed labelling). By Lagrange's Theorem, $H \cap K = 1$ (see Exercise 8). Proposition 13 then shows $|HK| = 24$ hence we must have $HK = S_4$. Since HK is a group, $HK = KH$. We leave as an exercise the verification that neither H nor K normalizes the other (so Corollary 15 could not have been used to give $HK = KH$).

Finally, throughout this chapter we have worked with left cosets of a subgroup. The same combinatorial results could equally well have been proved using right cosets. For normal subgroups this is trivial since left and right cosets are the same, but for non-normal subgroups some left cosets are not right cosets (for any choice of representative) so some (simple) verifications are necessary. For example, Lagrange's Theorem gives that in a finite group G

$$\textit{the number of right cosets of the subgroup } H \textit{ is } \frac{|G|}{|H|}.$$

Thus in a finite group the *number* of left cosets of H in G equals the *number* of right cosets even though the left cosets are not right cosets in general. This is also true for infinite groups as Exercise 12 below shows. Thus for purely combinatorial purposes one may use either left or right cosets (but not a mixture when a partition of G is needed). Our consistent use of left cosets is somewhat arbitrary although it will have some benefits when we discuss actions on cosets in the next chapter. Readers may encounter in some works the notation $H \backslash G$ to denote the set of right cosets of H in G.

In some papers one may also see the notation G/H used to denote the set of left cosets of H in G even when H is not normal in G (in which case G/H is called the *coset space* of left cosets of H in G). We shall not use this notation.

EXERCISES

Let G be a group.

1. Which of the following are permissible orders for subgroups of a group of order 120: 1, 2, 5, 7, 9, 15, 60, 240? For each permissible order give the corresponding index.

2. Prove that the lattice of subgroups of S_3 in Section 2.5 is correct (i.e., prove that it contains all subgroups of S_3 and that their pairwise joins and intersections are correctly drawn).

3. Prove that the lattice of subgroups of Q_8 in Section 2.5 is correct.

4. Show that if $|G| = pq$ for some primes p and q (not necessarily distinct) then either G is abelian or $Z(G) = 1$. [See Exercise 36 in Section 1.]

5. Let H be a subgroup of G and fix some element $g \in G$.

(a) Prove that gHg^{-1} is a subgroup of G of the same order as H.

(b) Deduce that if $n \in \mathbb{Z}^+$ and H is the unique subgroup of G of order n then $H \trianglelefteq G$.

6. Let $H \leq G$ and let $g \in G$. Prove that if the right coset Hg equals *some* left coset of H in G then it equals the left coset gH and g must be in $N_G(H)$.

7. Let $H \leq G$ and define a relation $\sim$ on G by $a \sim b$ if and only if $b^{-1}a \in H$. Prove that $\sim$ is an equivalence relation and describe the equivalence class of each $a \in G$. Use this to prove Proposition 4.

8. Prove that if H and K are finite subgroups of G whose orders are relatively prime then $H \cap K = 1$.