subgroup in the quotient. The image of the subgroup H of G under the natural projection homomorphism from G to G/N is the same as the image of the subgroup HN of G, and the subgroup HN of G contains N. Conversely, the preimage of a subgroup $\overline{H}$ of G/N contains N and is the unique subgroup of G containing N whose image in G/N is $\overline{H}$. It is the subgroups of G containing N which appear explicitly in the lattice for G/N.

The two lattices of groups of order 8 above emphasize the fact that the isomorphism type of a group cannot in general be determined from the knowledge of the isomorphism types of G/N and N, since $Q_8/\langle -1 \rangle \cong D_8/\langle r^2 \rangle$ and $\langle -1 \rangle \cong \langle r^2 \rangle$ yet Q_8 and D_8 are not isomorphic. We shall discuss this question further in the next section.

We shall often indicate the index of one subgroup in another in the lattice of subgroups, as follows:

$$\begin{tikzcd} A \arrow[d, dash, "n"] \\ B \end{tikzcd}$$

where the integer n equals $|A : B|$. For example, all the unbroken edges in the lattices of Q_8 and D_8 would be labelled with 2. Thus the order of any subgroup, A, is the product of all integers which label any path upward from the identity to A. Also, by Theorem 20(2) these indices remain unchanged in quotients of G by normal subgroups of G contained in B, i.e., the portion of the lattice for G corresponding to the lattice of the quotient group has the correct indices for the quotient as well.

Finally we include a remark concerning the definition of homomorphisms on quotient groups. We have, in the course of the proof of the isomorphism theorems, encountered situations where a homomorphism φ on the quotient group G/N is specified by giving the value of φ on the coset gN in terms of the representative g alone. In each instance we then had to prove φ was well defined, i.e., was independent of the choice of g. In effect we are defining a homomorphism, Φ, on G itself by specifying the value of φ at g. Then independence of g is equivalent to requiring that Φ be trivial on N, so that

$$\textit{φ is well defined on G/N if and only if $N \leq$} \ker \Phi.$$

This gives a simple criterion for defining homomorphisms on quotients (namely, define a homomorphism on G and check that N is contained in its kernel). In this situation we shall say the homomorphism Φ *factors through N* and φ is the *induced* homomorphism on G/N. This can be denoted pictorially as in Figure 7, where the diagram indicates that $\Phi = \varphi \circ \pi$, i.e., the image in H of an element in G does not depend on which path one takes in the diagram. If this is the case, then the diagram is said to *commute*.

$$\begin{tikzcd} G \arrow[r, "\pi"] \arrow[dr, "\Phi"'] & G/N \arrow[d, "\varphi"] \\ & H \end{tikzcd}$$

Fig. 7

At this point we have developed all the background material so that Section 6.3 on free groups and presentations may now be read.

EXERCISES

Let G be a group.

1. Let F be a finite field of order q and let $n \in \mathbb{Z}^+$. Prove that $|GL_n(F) : SL_n(F)| = q - 1$. [See Exercise 35, Section 1.]
2. Prove all parts of the Lattice Isomorphism Theorem.
3. Prove that if H is a normal subgroup of G of prime index p then for all $K \leq G$ either
   (i) $K \leq H$ or
   (ii) $G = HK$ and $|K : K \cap H| = p$.
4. Let C be a normal subgroup of the group A and let D be a normal subgroup of the group B. Prove that $(C \times D) \trianglelefteq (A \times B)$ and $(A \times B)/(C \times D) \cong (A/C) \times (B/D)$.
5. Let $QD_{16} = \langle \sigma, \tau \rangle$ be the quasidihedral group described in Exercise 11 of Section 2.5. Prove that $\langle \sigma^4 \rangle$ is normal in QD_{16} and use the Lattice Isomorphism Theorem to draw the lattice of subgroups of $QD_{16}/\langle \sigma^4 \rangle$. Which group of order 8 has the same lattice as this quotient? Use generators and relations for $QD_{16}/\langle \sigma^4 \rangle$ to decide the isomorphism type of this group.
6. Let $M = \langle v, u \rangle$ be the modular group of order 16 described in Exercise 14 of Section 2.5. Prove that $\langle v^4 \rangle$ is normal in M and use the Lattice Isomorphism Theorem to draw the lattice of subgroups of $M/\langle v^4 \rangle$. Which group of order 8 has the same lattice as this quotient? Use generators and relations for $M/\langle v^4 \rangle$ to decide the isomorphism type of this group.
7. Let M and N be normal subgroups of G such that $G = MN$. Prove that $G/(M \cap N) \cong (G/M) \times (G/N)$. [Draw the lattice.]
8. Let p be a prime and let G be the group of p-power roots of 1 in $\mathbb{C}$ (cf. Exercise 18, Section 2.4). Prove that the map $z \mapsto z^p$ is a surjective homomorphism. Deduce that G is isomorphic to a proper quotient of itself.
9. Let p be a prime and let G be a group of order $p^a m$, where p does not divide m. Assume P is a subgroup of G of order p^a and N is a normal subgroup of G of order $p^b n$, where p does not divide n. Prove that $|P \cap N| = p^b$ and $|PN/N| = p^{a-b}$. (The subgroup P of G is called a *Sylow p-subgroup* of G. This exercise shows that the intersection of any Sylow p-subgroup of G with a normal subgroup N is a Sylow p-subgroup of N.)
10. Generalize the preceding exercise as follows. A subgroup H of a finite group G is called a *Hall subgroup* of G if its index in G is relatively prime to its order: $(|G : H|, |H|) = 1$. Prove that if H is a Hall subgroup of G and $N \trianglelefteq G$, then $H \cap N$ is a Hall subgroup of N and HN/N is a Hall subgroup of G/N.

3.4 COMPOSITION SERIES AND THE HÖLDER PROGRAM

The remarks in the preceding section on lattices leave us with the intuitive picture that a quotient group G/N is the group whose structure (e.g., lattice) describes the structure of G "above" the normal subgroup N. Although this is somewhat vague, it gives at least some notion of the driving force behind one of the most powerful techniques in finite group theory (and even some branches of infinite group theory): the use of induction. In many instances the application of an inductive procedure follows a pattern similar to the following proof of a special case of Cauchy's Theorem. Although Cauchy's Theorem is valid for arbitrary groups (cf. Exercise 9 of Section 2), the following is a good example of the use of information on a normal subgroup N and on the quotient G/N to determine information about G, and we shall need this particular result in Chapter 4.

Proposition 21. If G is a finite abelian group and p is a prime dividing $|G|$, then G contains an element of order p.

Proof: The proof proceeds by induction on $|G|$, namely, we assume the result is valid for every group whose order is strictly smaller than the order of G and then prove the result valid for G (this is sometimes referred to as *complete* induction). Since $|G| > 1$, there is an element $x \in G$ with $x \neq 1$. If $|G| = p$ then x has order p by Lagrange's Theorem and we are done. We may therefore assume $|G| > p$.

Suppose p divides $|x|$ and write $|x| = pn$. By Proposition 2.5(3), $|x^n| = p$, and again we have an element of order p. We may therefore assume p does not divide $|x|$.

Let $N = \langle x \rangle$. Since G is abelian, $N \trianglelefteq G$. By Lagrange's Theorem, $|G/N| = \dfrac{|G|}{|N|}$ and since $N \neq 1$, $|G/N| < |G|$. Since p does not divide $|N|$, we must have $p \mid |G/N|$. We can now apply the induction assumption to the smaller group G/N to conclude it contains an element, $\bar{y} = yN$, of order p. Since $y \notin N$ ($\bar{y} \neq \bar{1}$) but $y^p \in N$ ($\bar{y}^p = \bar{1}$), we must have $\langle y^p \rangle \neq \langle y \rangle$, that is, $|y^p| < |y|$. Proposition 2.5(2) implies $p \mid |y|$. We are now in the situation described in the preceding paragraph, so that argument again produces an element of order p. The induction is complete.

The philosophy behind this method of proof is that if we have a sufficient amount of information about some normal subgroup, N, of a group G and sufficient information on G/N, then somehow we can piece this information together to force G itself to have some desired property. The induction comes into play because both N and G/N have smaller order than G. In general, just how much data are required is a delicate matter since, as we have already seen, the full isomorphism type of G cannot be determined from the isomorphism types of N and G/N alone.

Clearly a basic obstruction to this approach is the necessity of producing a normal subgroup, N, of G with $N \neq 1$ or G. In the preceding argument this was easy since G was abelian. Groups with no nontrivial proper normal subgroups are fundamental obstructions to this method of proof.

Definition. A (finite or infinite) group G is called *simple* if $|G| > 1$ and the only normal subgroups of G are 1 and G.

By Lagrange's Theorem if $|G|$ is a prime, its only subgroups (let alone normal ones) are 1 and G, so G is simple. In fact, every abelian simple group is isomorphic to Z_p, for some prime p (cf. Exercise 1). There are non-abelian simple groups (of both finite and infinite order), the smallest of which has order 60 (we shall introduce this group as a member of an infinite family of simple groups in the next section).

Simple groups, by definition, cannot be "factored" into pieces like N and G/N and as a result they play a role analogous to that of the primes in the arithmetic of $\mathbb{Z}$. This analogy is supported by a "unique factorization theorem" (for finite groups) which we now describe.