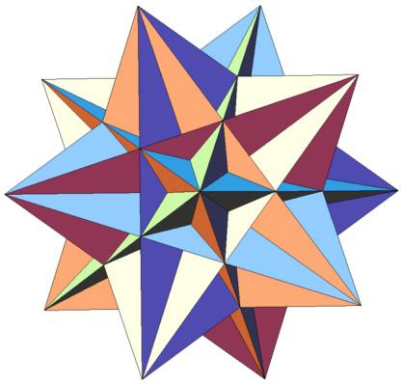
تمارين مقرر ٣٤٣ ريض (نظرية الزمر)

حل تمارين كتاب:
مواضيع في الجبر- تأليف: أي . إن . هيرستين – ط٣
(فصل الزمر)



Rotations and flips form the symmetry group of a great icosahedron

STUDENT'S SOLUTION MANUAL

Abstract Algebra

I.N. Herstein
University of Chicago

Macmillan Publishing Company
New York
Collier Macmillan Publishers
London

CONTENTS

ment, since $a * 1 = a1 = a = 1a = 1 * a$ for every $a \in G$. So we are three-fourths of the way to proving that G is a group. All we need is inverses for the elements of G, relative to $*$, to lie in G. But this just isn't so. Clearly, we cannot find an integer b such that $0 * b = 0b = 1$, since $0b = 0$ for all b. But even other integers fail to have inverses in G. For instance, we *cannot find an integer* b such that $3 * b = 1$ (for this would require that $b = \frac{1}{3}$, and $\frac{1}{3}$ is not an integer).

2. Let G be the set of all nonzero real numbers and define, for $a, b \in G$, $a * b = a^2b$; thus $4 * 5 = 4^2(5) = 80$. Which of the group axioms hold in G under this operation $*$ and which fail to hold? Certainly, G is closed under $*$. Is $*$ associative? If so, $(a * b) * c = a * (b * c)$, that is, $(a * b)^2c = a^2(b * c)$, and so $(a^2b)^2c = a^2(b^2c)$, which boils down to $a^2 = 1$, which holds only for $a = \pm 1$. So, in general, the associative law does *not* hold in G relative to $*$. We similarly can verify that G does not have a unit element. Thus even to discuss inverses relative to $*$ would not make sense.

3. Let G be the set of all *positive* integers, under $*$ where $a * b = ab$, the ordinary product of integers. Then one can easily verify that G fails to be a group *only because it fails* to have inverses for some (in fact, most) of its elements relative to $*$.

We shall find some other nonexamples of groups in the exercises.

PROBLEMS

Easier Problems

1. Determine if the following sets G with the operation indicated form a group. If not, point out which of the group axioms fail.
- **(a)** G = set of all integers, $a * b = a - b$.
- **(b)** G = set of all integers, $a * b = a + b + ab$.
- **(c)** G = set of nonnegative integers, $a * b = a + b$.
- **(d)** G = set of all rational numbers $\neq -1$, $a * b = a + b + ab$.
- **(e)** G = set of all rational numbers with denominator divisible by 5 (written so that numerator and denominator are relatively prime), $a * b = a + b$.
- **(f)** G a set having more than one element, $a * b = a$ for all $a, b \in G$.

2. In the group G defined in Example 6, show that the set $H = \{T_{a,b} \mid a = \pm 1, b \text{ any real}\}$ forms a group under the $*$ of G.

3. Verify that Example 7 is indeed an example of a group.

4. Prove that K defined in Example 8 is an abelian group.
5. In Example 9, prove that $g * f = f * g^{-1}$, and that G is a group, is nonabelian, and is of order 8.
6. Let G and H be as in Examples 6 and 7, respectively. Show that if $T_{a,b} \in G$, then $T_{a,b} * V * T_{a,b}^{-1} \in H$ if $V \in H$.
7. Do Problem 6 with H replaced by the group K of Example 8.
8. If G is an abelian group, prove that $(a * b)^n = a^n * b^n$ for all integers n.
9. If G is a group in which $a^2 = e$ for all $a \in G$, show that G is abelian.
10. If G is the group in Example 6, find all $T_{a,b} \in G$ such that $T_{a,b} * T_{1,x} = T_{1,x} * T_{a,b}$ for *all* real x.
11. In Example 10, for $n = 3$ find a formula that expresses $(f^i h^j) * (f^s h^t)$ as $f^a h^b$. Show that G is a nonabelian group of order 6.
12. Do Problem 11 for $n = 4$.
13. Show that any group of order 4 or less is abelian.
14. If G is any group and $a, b, c \in G$, show that if $a * b = a * c$, then $b = c$, and if $b * a = c * a$, then $b = c$.
15. Express $(a * b)^{-1}$ in terms of a^{-1} and b^{-1}.
16. Using the result of Problem 15, prove that a group G in which $a = a^{-1}$ for every $a \in G$ must be abelian.
17. In any group G, prove that $(a^{-1})^{-1} = a$ for all $a \in G$.
*18. If G is a finite group of *even* order, show that there must be an element $a \neq e$ such that $a = a^{-1}$. (**Hint:** Try to use the result of Problem 17.)
19. In S_3, show that there are four elements x satisfying $x^2 = e$ and three elements y satisfying $y^3 = e$.
20. Find all the elements in S_4 such that $x^4 = e$.

Middle-Level Problems

21. Show that a group of order 5 must be abelian.
22. Show that the set defined in Example 10 is a group, is nonabelian, and has order $2n$. Do this by finding the formula for $(f^i h^j) * (f^s h^t)$ in the form $f^a h^b$.
23. In the group G of Example 6, find all elements $U \in G$ such that $U * T_{a,b} = T_{a,b} * U$ for every $T_{a,b} \in G$.
24. If G is the dihedral group of order $2n$ as defined in Example 10, prove that:
    (a) If n is odd and $a \in G$ is such that $a * b = b * a$ for all $b \in G$, then $a = e$.
    (b) If n is even, show that there is an $a \in G$, $a \neq e$, such that $a * b = b * a$ for all $b \in G$.

(c) If n is even, find all the elements $a \in G$ such that $a * b = b * a$ for all $b \in G$.

25. If G is any group, show that:

(a) e is unique (i.e., if $f \in G$ also acts as a unit element for G, then $f = e$).

(b) Given $a \in G$, then $a^{-1} \in G$ is unique.

***26.** If G is a finite group, prove that, given $a \in G$, there is a positive integer n, depending on a, such that $a^n = e$.

***27.** In Problem 26, show that there is an integer $m > 0$ such that $a^m = e$ for *all* $a \in G$.

Harder Problems

28. Let G be a set with an operation $*$ such that:

1. G is closed under $*$.
2. $*$ is associative.
3. There exists an element $e \in G$ such that $e * x = x$ for all $x \in G$.
4. Given $x \in G$, there exists a $y \in G$ such that $y * x = e$.

Prove that G is a group. (Thus you must show that $x * e = x$ and $x * y = e$ for e, y as above.)

29. Let G be a *finite* nonempty set with an operation $*$ such that:

1. G is closed under $*$.
2. $*$ is associative.
3. Given $a, b, c \in G$ with $a * b = a * c$, then $b = c$.
4. Given $a, b, c, \in G$ with $b * a = c * a$, then $b = c$.

Prove that G must be a group under $*$.

30. Give an example to show that the result of Problem 29 can be false if G is an infinite set.

31. Let G be the group of all nonzero real numbers under the operation $*$ which is the ordinary multiplication of real numbers, and let H be the group of all real numbers under the operation #, which is the addition of real numbers.

(a) Show that there is a mapping $F: G \to H$ of G onto H which satisfies $F(a * b) = F(a)\#F(b)$ for all $a, b \in G$ [i.e., $F(ab) = F(a) + F(b)$].

(b) Show that no such mapping F can be 1-1.

2. SOME SIMPLE REMARKS

In this short section we show that certain formal properties which follow from the group axioms hold in any group. As a matter of fact, most of these results have already occurred as problems at the end of the preceding section.

We promised to list a piece of the argument given above as a separate lemma. We keep this promise and write

Lemma 2.2.2. In any group G and $a, b, c \in G$, we have:

(a) If $ab = ac$, then $b = c$.

(b) If $ba = ca$, then $b = c$.

Before leaving these results, note that if G is the group of real numbers under $+$, then Part (c) of Lemma 2.2.1 translates into the familiar $-(-a) = a$.

There is only a scant bit of mathematics in this section; accordingly, we give only a few problems. No indication is given as to the difficulty of these.

PROBLEMS

1. Suppose that G is a set closed under an associative operation such that
1. given $a, y \in G$, there is an $x \in G$ such that $ax = y$, and
2. given $a, w \in G$, there is a $u \in G$ such that $ua = w$.

Show that G is a group.

***2.** If G is a *finite* set closed under an associative operation such that $ax = ay$ forces $x = y$ and $ua = wa$ forces $u = w$, for every $a, x, y, u, w \in G$, prove that G is a group. (This is a repeat of a problem given earlier. It will be used in the body of the text later.)

3. If G is a group in which $(ab)^i = a^i b^i$ for three consecutive integers i, prove that G is abelian.

4. Show that the result of Problem 3 would not always be true if the word "three" were replaced by "two." In other words, show that there is a group G and consecutive numbers $i, i + 1$ such that G is not abelian but does have the property that $(ab)^i = a^i b^i$ and $(ab)^{i+1} = a^{i+1} b^{i+1}$ for all a, b in G.

5. Let G be a group in which $(ab)^3 = a^3 b^3$ and $(ab)^5 = a^5 b^5$ for all $a, b \in G$. Show that G is abelian.

6. Let G be a group in which $(ab)^n = a^n b^n$ for some fixed integer $n > 1$ for all $a, b \in G$. For all $a, b \in G$, prove that:

(a) $(ab)^{n-1} = b^{n-1} a^{n-1}$.

(b) $a^n b^{n-1} = b^{n-1} a^n$.

(c) $(aba^{-1}b^{-1})^{n(n-1)} = e$.

[**Hint for Part (c):** Note that $(aba^{-1})^r = ab^r a^{-1}$ for all integers r.]

12. Let G be any group and H a subgroup of G. For $a \in G$, let $a^{-1}Ha = \{a^{-1}ha \mid h \in H\}$. We assert that $a^{-1}Ha$ is a subgroup of G. If $x = a^{-1}h_1a$ and $y = a^{-1}h_2a$ where $h_1, h_2 \in H$, then $xy = (a^{-1}h_1a)(a^{-1}h_2a) = a^{-1}(h_1h_2)a$ (associative law), and since H is a subgroup of G, $h_1h_2 \in H$. Therefore, $a^{-1}(h_1h_2)a \in a^{-1}Ha$, which says that $xy \in a^{-1}Ha$. Thus $a^{-1}Ha$ is closed. Also, if $x = a^{-1}ha \in a^{-1}Ha$, then, as is easily verified, $x^{-1} = (a^{-1}ha)^{-1} = a^{-1}h^{-1}a \in a^{-1}Ha$. Therefore, $a^{-1}Ha$ is a subgroup of G.

An even dozen seems to be about the right number of examples, so we go on to other things. Lemma 2.3.1 points out for us what we need in order that a given subset of a group be a subgroup. In an important special case we can make a considerable saving in checking whether a given subset H is a subgroup of G. This is the case in which H is *finite*.

Lemma 2.3.2. Suppose that G is a group and H a nonempty *finite* subset of G closed under the product in G. Then H is a subgroup of G.

Proof. By Lemma 2.3.1 we must show that $a \in H$ implies $a^{-1} \in H$. If $a = e$, then $a^{-1} = e$ and we are done. Suppose then that $a \neq e$; consider the elements $a, a^2, \ldots, a^{n+1}$, where $n = |H|$, the order of H. *Here we have written down $n + 1$ elements, all of them in H since H is closed, and H has only n distinct elements.* How can this be? Only if some two of the elements listed are equal; put another way, only if $a^i = a^j$ for some $1 \leq i < j \leq n + 1$. But then, by the cancellation property in groups, $a^{j-i} = e$. Since $j - i \geq 1$, $a^{j-i} \in H$, hence $e \in H$. However, $j - i - 1 \geq 0$, so $a^{j-i-1} \in H$ and $aa^{j-i-1} = a^{j-i} = e$, whence $a^{-1} = a^{j-i-1} \in H$. This proves the lemma. □

An immediate, but nevertheless important, corollary to Lemma 2.3.2 is the

Corollary. If G is a finite group and H a nonempty subset of G closed under multiplication, then H is a subgroup of G.

PROBLEMS

Easier Problems

1. If A, B are subgroups of G, show that $A \cap B$ is a subgroup of G.
2. What is the cyclic subgroup of $\mathbb{Z}$ generated by -1 under $+$?
3. Let S_3 be the symmetric group of degree 3. Find all the subgroups of S_3.
4. Verify that $Z(G)$, the center of G, is a subgroup of G. (See Example 11.)

5. If $C(a)$ is the centralizer of a in G (Example 10), prove that $Z(G) = \cap_{a \in G} C(a)$.
6. Show that $a \in Z(G)$ if and only if $C(a) = G$.
7. In S_3, find $C(a)$ for each $a \in S_3$.
8. If G is an abelian group and if $H = \{a \in G \mid a^2 = e\}$, show that H is a subgroup of G.
9. Give an example of a nonabelian group for which the H in Problem 8 is *not* a subgroup.
10. If G is an abelian group and $n > 1$ an integer, let $A_n = \{a^n \mid a \in G\}$. Prove that A_n is a subgroup of G.
*11. If G is an abelian group and $H = \{a \in G \mid a^{n(a)} = e$ for some $n(a) > 1$ depending on $a\}$, prove that H is a subgroup of G.

We say that a group G is *cyclic* if there exists an $a \in G$ such that every $x \in G$ is a power of a, that is, $x = a^j$ for some j. In other words, G is cyclic if $G = (a)$ for some $a \in G$, in which case we say that a is a *generator* for G.

*12. Prove that a cyclic group is abelian.
13. If G is cyclic, show that every subgroup of G is cyclic.
14. If G has no proper subgroups, prove that G is cyclic.
15. If G is a group and H a nonempty subset of G such that, given $a, b \in H$, then $ab^{-1} \in H$, prove that H is a subgroup of G.

Middle-Level Problems

*16. If G has no proper subgroups, prove that G is cyclic of order p, where p is a prime number. (This sharpens the result of Problem 14.)
17. If G is a group and $a, x \in G$, prove that $C(x^{-1}ax) = x^{-1}C(a)x$. [See Examples 10 and 12 for the definitions of $C(b)$ and of $x^{-1}C(a)x$.]
18. If S is a nonempty set and $X \subset S$, show that $T(X) = \{f \in A(S) \mid f(X) \subset X\}$ is a subgroup of $A(S)$ *if X is finite.*
19. If A, B are subgroups of an abelian group G, let $AB = \{ab \mid a \in A, b \in B\}$. Prove that AB is a subgroup of G.
20. Give an example of a group G and two subgroups A, B of G such that AB is *not* a subgroup of G.
21. If A, B are subgroups of G such that $b^{-1}Ab \subset A$ for all $b \in B$, show that AB is a subgroup of G.
*22. If A and B are finite subgroups, of orders m and n, respectively, of the abelian group G, prove that AB is a subgroup of order mn *if m and n are relatively prime.*

23. What is the order of AB in Problem 22 if m and n are not relatively prime?

24. If H is a subgroup of G, let $N = \cap_{x \in G} x^{-1}Hx$. Prove that N is a subgroup of G such that $y^{-1}Ny = N$ for every $y \in G$.

Harder Problems

25. Let S, X, $T(X)$ be as in Problem 18 (but X no longer finite). Give an example of a set S and an infinite subset X such that $T(X)$ is *not* a subgroup of $A(S)$.

***26.** Let G be a group, H a subgroup of G. Let $Hx = \{hx \mid h \in H\}$. Show that, given $a, b \in G$, then $Ha = Hb$ or $Ha \cap Hb = \emptyset$.

***27.** If in Problem 26 H is a finite subgroup of G, prove that Ha and Hb have the same number of elements. What is this number?

28. Let M, N be subgroups of G such that $x^{-1}Mx \subset M$ and $x^{-1}Nx \subset N$ for all $x \in G$. Prove that MN is a subgroup of G and that $x^{-1}(MN)x \subset MN$ for all $x \in G$.

***29.** If M is a subgroup of G such that $x^{-1}Mx \subset M$ for all $x \in G$, prove that actually $x^{-1}Mx = M$.

30. If M, N are such that $x^{-1}Mx = M$ and $x^{-1}Nx = N$ for all $x \in G$, and if $M \cap N = (e)$, prove that $mn = nm$ for any $m \in M$, $n \in N$. (**Hint:** Consider the element $m^{-1}n^{-1}mn$.)

4. LAGRANGE'S THEOREM

We are about to derive the first real group-theoretic result of importance. Although its proof is relatively easy, this theorem is like the A-B-C's for finite groups and has interesting implications in number theory.

As a matter of fact, those of you who solved Problems 26 and 27 of Section 3 have all the necessary ingredients to effect a proof of the result. The theorem simply states that in a finite group the order of a subgroup divides the order of the group.

To smooth the argument of this theorem—which is due to Lagrange—and for use many times later, we make a short detour into the realm of set theory.

Just as the concept of "function" runs throughout most phases of mathematics, so also does the concept of "relation." A *relation* is a statement aRb about the elements $a, b \in S$. If S is the set of integers, $a = b$ is a relation on S. Similarly, $a < b$ is a relation on S, as is $a \leq b$.

An immediate consequence of Theorems 2.4.7 and 2.4.5 is a famous result in number theory.

Theorem 2.4.8 (Euler). If a is an integer relatively prime to n, then $a^{\varphi(n)} \equiv 1 \bmod n$.

Proof. U_n forms a group of order $\varphi(n)$, so by Theorem 2.4.5, $a^{\varphi(n)} = e$ for all $a \in U_n$. This translates into $[a^{\varphi(n)}] = [a]^{\varphi(n)} = [1]$, which in turn translates into $n \mid (a^{\varphi(n)} - 1)$ for every integer a relatively prime to p. In other words, $a^{\varphi(n)} \equiv 1 \bmod n$. □

A special case, where $n = p$ is a prime, is due to Fermat.

Corollary (Fermat). If p is a prime and $p \nmid a$, then

$$a^{p-1} \equiv 1 \bmod p.$$

For any integer b, $b^p \equiv b \bmod p$.

Proof. Since $\varphi(p) = p - 1$, if $(a, p) = 1$, we have, by Theorem 2.4.8, that $a^{p-1} \equiv 1(p)$, hence $a^1 \cdot a^{p-1} \equiv a(p)$, so that $a^p \equiv a(p)$. If $p \mid b$, then $b \equiv 0(p)$ and $b^p \equiv 0(p)$, so that $b^p \equiv b(p)$. □

Leonard Euler (1707–1785) was probably the greatest scientist that Switzerland has produced. He was the most prolific of all mathematicians ever.

Pierre Fermat (1601–1665) was a great number theorist. Fermat's Last Theorem—which was in fact first proved in 1994 by Andrew Wiles—states that the equation $a^n + b^n = c^n$ (a, b, c, n being integers) has only the trivial solution where $a = 0$ or $b = 0$ or $c = 0$ if $n > 2$.

One final cautionary word about Lagrange's Theorem. Its *converse* in general is *not* true. That is, if G is a finite group of order n, then it need not be true that for every divisor m of n there is a subgroup of G of order m. A group with this property is very special indeed, and its structure can be spelled out quite well and precisely.

PROBLEMS

Easier Problems

1. Verify that the relation $\sim$ is an equivalence relation on the set S given.

(a) $S = \mathbb{R}$ reals, $a \sim b$ if $a - b$ is rational.

(b) $S = \mathbb{C}$, the complex numbers, $a \sim b$ if $|a| = |b|$.

(c) $S =$ straight lines in the plane, $a \sim b$ if a, b are parallel.

(d) $S =$ set of all people, $a \sim b$ if they have the same color eyes.

2. The relation $\sim$ on the real numbers $\mathbb{R}$ defined by $a \sim b$ if both $a > b$ and $b > a$ is *not* an equivalence relation. Why not? What properties of an equivalence relation does it satisfy?

3. Let $\sim$ be a relation on a set S that satisfies (1) $a \sim b$ implies that $b \sim a$ and (2) $a \sim b$ and $b \sim c$ implies that $a \sim c$. These seem to imply that $a \sim a$. For if $a \sim b$, then by (1), $b \sim a$, so $a \sim b$, $b \sim a$, so by (2), $a \sim a$. If this argument is correct, then the relation $\sim$ must be an equivalence relation. Problem 2 shows that this is not so. What is wrong with the argument we have given?

4. Let S be a set, $\{S_\alpha\}$ nonempty subsets such that $S = \cup_\alpha S_\alpha$ and $S_\alpha \cap S_\beta = \emptyset$ if $\alpha \neq \beta$. Define an equivalence relation on S in such a way that the S_α are precisely all the equivalence classes.

*** 5.** Let G be a group and H a subgroup of G. Define, for $a, b \in G$, $a \sim b$ if $a^{-1}b \in H$. Prove that this defines an equivalence relation on G, and show that $[a] = aH = \{ah \mid h \in H\}$. The sets aH are called *left cosets* of H in G.

6. If G is S_3 and $H = \{i, f\}$, where $f: S \to S$ is defined by $f(x_1) = x_2, f(x_2) = x_1, f(x_3) = x_3$, list all the right cosets of H in G and list all the left cosets of H in G.

7. In Problem 6, is every right coset of H in G also a left coset of H in G?

8. If every right coset of H in G is a left coset of H in G, prove that $aHa^{-1} = H$ for all $a \in G$.

9. In $\mathbb{Z}_{16}$, write down all the cosets of the subgroup $H = \{[0], [4], [8], [12]\}$. (Since the operation in $\mathbb{Z}_n$ is $+$, write your coset as $[a] + H$. We don't need to distinguish between right cosets and left cosets, since $\mathbb{Z}_n$ is abelian under $+$.)

10. In Problem 9, what is the index of H in $\mathbb{Z}_{16}$? (Recall that we defined the index $i_G(H)$ as the number of right cosets in G.)

11. For any finite group G, show that there are as many distinct left cosets of H in G as there are right cosets of H in G.

12. If aH and bH are distinct left cosets of H in G, are Ha and Hb distinct right cosets of H in G? Prove that this is true or give a counterexample.

13. Find the orders of all the elements of U_{18}. Is U_{18} cyclic?

14. Find the orders of all the elements of U_{20}. Is U_{20} cyclic?

***15.** If p is a prime, show that the only solutions of $x^2 \equiv 1 \bmod p$ are $x \equiv 1 \bmod p$ or $x \equiv -1 \bmod p$.

***16.** If G is a finite abelian group and $a_1, \ldots, a_n$ are all its elements, show that $x = a_1 a_2 \cdots a_n$ must satisfy $x^2 = e$.

17. If G is of odd order, what can you say about the x in Problem 16?

18. Using the results of Problems 15 and 16, prove that if p is an odd prime number, then $(p-1)! \equiv -1 \bmod p$. (This is known as *Wilson's Theorem.*) It is, of course, also true if $p = 2$.

19. Find all the distinct conjugacy classes of S_3.

20. In the group G of Example 6 of Section 1, find the conjugacy class of the element $T_{a,b}$. Describe it in terms of a and b.

21. Let G be the dihedral group of order 8 (see Example 9, Section 1). Find the conjugacy classes in G.

22. Verify Euler's Theorem for $n = 14$ and $a = 3$, and for $n = 14$ and $a = 5$.

23. In U_{41}, show that there is an element a such that $[a]^2 = [-1]$, that is, an integer a such that $a^2 \equiv -1 \bmod 41$.

24. If p is a prime number of the form $4n + 3$, show that we *cannot* solve

$$x^2 \equiv -1 \bmod p$$

[**Hint:** Use Fermat's Theorem that $a^{p-1} \equiv 1 \bmod p$ if $p \nmid a$.]

25. Show that the nonzero elements in $\mathbb{Z}_n$ form a group under the product $[a][b] = [ab]$ if and only if n is a prime.

Middle-Level Problems

26. Let G be a group, H a subgroup of G, and let S be the set of all distinct right cosets of H in G, T the set of all left cosets of H in G. Prove that there is a 1-1 mapping of S onto T. (**Note:** The obvious map that comes to mind, which sends Ha into aH, is not the right one. See Problems 5 and 12.)

27. If $aH = bH$ forces $Ha = Hb$ in G, show that $aHa^{-1} = H$ for every $a \in G$.

28. If G is a cyclic group of order n, show that there are $\varphi(n)$ generators for G. Give their form explicitly.

29. If in a group G, $aba^{-1} = b^i$, show that $a^r ba^{-r} = b^{i^r}$ for all positive integers r.

30. If in G $a^5 = e$ and $aba^{-1} = b^2$, find $o(b)$ if $b \neq e$.

***31.** If $o(a) = m$ and $a^s = e$, prove that $m \mid s$.

32. Let G be a finite group, H a subgroup of G. Let $f(a)$ be the least positive m such that $a^m \in H$. Prove that $f(a) \mid o(a)$.

33. If $i \neq f \in A(S)$ is such that $f^p = i$, p a prime, and if for some $s \in S$, $f^j(s) = s$ for some $1 \leq j < p$, show that $f(s) = s$.

34. If $f \in A(S)$ has order p, p a prime, show that for every $s \in S$ the orbit of s under f has one or p elements. [**Recall:** The orbit of s under f is $\{f^j(s) \mid j \text{ any integer}\}$.]

35. If $f \in A(S)$ has order p, p a prime, and S is a finite set having n elements, where $(n, p) = 1$, show that for some $s \in S$, $f(s) = s$.

Harder Problems

36. If $a > 1$ is an integer, show that $n \mid \varphi(a^n - 1)$, where φ is the Euler φ-function. [**Hint:** Consider the integers mod$(a^n - 1)$.]

37. In a cyclic group of order n, show that for each positive integer m that divides n (including $m = 1$ and $m = n$) there are $\varphi(m)$ elements of order m.

38. Using the result of Problem 37, show that $n = \Sigma_{m \mid n} \varphi(m)$.

39. Let G be a finite abelian group of order n for which the number of solutions of $x^m = e$ is at most m for any m dividing n. Prove that G must be cyclic. [**Hint:** Let $\psi(m)$ be the number of elements in G of *order* m. Show that $\psi(m) \leq \varphi(m)$ and use Problem 38.]

40. Using the result of Problem 39, show that U_p, if p is a prime, is cyclic. (This is a famous result in number theory; it asserts the existence of a *primitive root* mod p.)

41. Using the result of Problem 40, show that if p is a prime of the form $p = 4n + 1$, then we can solve $x^2 \equiv -1 \bmod p$ (with x an integer).

42. Using Wilson's Theorem (see Problem 28), show that if p is a prime of the form $p = 4n + 1$ and if

$$y = 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} = \left(\frac{p-1}{2}\right)!,$$

then $y^2 \equiv -1 \bmod p$. (This gives another proof of the result in Problem 41.)

43. Let G be an abelian group of order n, and $a_1, \ldots, a_n$ its elements. Let $x = a_1 a_2 \cdots a_n$. Show that:

(a) If G has exactly one element $b \neq e$ such that $b^2 = e$, then $x = b$.

(b) If G has more than one element $b \neq e$ such that $b^2 = e$, then $x = e$.

(c) If n is odd, then $x = e$ (see Problem 16).

5. HOMOMORPHISMS AND NORMAL SUBGROUPS

In a certain sense the subject of group theory is built up out of three basic concepts: that of a homomorphism, that of a normal subgroup, and that of the factor or quotient group of a group by a normal subgroup. We discuss the first two of these in this section, and the third in Section 6.

Without further ado we introduce the first of these.

4. If G is any group, $Z(G)$, the *center* of G, is a normal subgroup of G (see Example 11 of Section 3).
5. If $G = S_3$, G has the elements i, f, g, g^2, fg, and gf, where $f(x_1) = x_2$, $f(x_2) = x_1$, $f(x_3) = x_3$ and $g(x_1) = x_2$, $g(x_2) = x_3$, $g(x_3) = x_1$. We claim that the subgroup $N = \{i, g, g^2\} \lhd S_3$. As we saw earlier (or can compute now), $fgf^{-1} = g^{-1} = g^2$, $fg^2f^{-1} = g$. $(fg)\, g(fg)^{-1} = fggg^{-1}f^{-1} = fgf^{-1} = g^2$, and so on. So $N \lhd S_3$ follows.

The material in this section has been a rather rich diet. It may not seem so, but the ideas presented, although simple, are quite subtle. We recommend that the reader digest the concepts and results thoroughly before going on. One way of seeing how complete this digestion is, is to take a stab at many of the almost infinite list of problems that follow. The material of the next section is even a richer diet, and even harder to digest. Avoid a mathematical stomachache later by assimilating this section well.

PROBLEMS

Easier Problems

1. Determine in each of the parts if the given mapping is a homomorphism. If so, identify its kernel and whether or not the mapping is 1-1 or onto.
- **(a)** $G = \mathbb{Z}$ under $+$, $G' = \mathbb{Z}_n$, $\varphi(a) = [a]$ for $a \in \mathbb{Z}$.
- **(b)** G group, $\varphi: G \to G$ defined by $\varphi(a) = a^{-1}$ for $a \in G$.
- **(c)** G abelian group, $\varphi: G \to G$ defined by $\varphi(a) = a^{-1}$ for $a \in G$.
- **(d)** G group of all nonzero real numbers under multiplication, $G' = \{1, -1\}$, $\varphi(r) = 1$ if r is positive, $\varphi(r) = -1$ if r is negative.
- **(e)** G an abelian group, $n > 1$ a fixed integer, and $\varphi: G \to G$ defined by $\varphi(a) = a^n$ for $a \in G$.

2. Recall that $G \simeq G'$ means that G is isomorphic to G'. Prove that for all groups G_1, G_2, G_3:
- **(a)** $G_1 \simeq G_1$.
- **(b)** $G_1 \simeq G_2$ implies that $G_2 \simeq G_1$.
- **(c)** $G_1 \simeq G_2$, $G_2 \simeq G_3$ implies that $G_1 \simeq G_3$.

3. Let G be any group and $A(G)$ the set of all 1-1 mappings of G, as a set, onto itself. Define $L_a: G \to G$ by $L_a(x) = xa^{-1}$. Prove that:
- **(a)** $L_a \in A(G)$.
- **(b)** $L_a L_b = L_{ab}$.
- **(c)** The mapping $\psi: G \to A(G)$ defined by $\psi(a) = L_a$ is a monomorphism of G into $A(G)$.

4. In Problem 3 prove that for all $a, b \in G$, $T_a L_b = L_b T_a$, where T_a is defined as in Example 8.
5. In Problem 4, show that if $V \in A(G)$ is such that $T_a V = V T_a$ for all $a \in G$, then $V = L_b$ for some $b \in G$. (**Hint:** Acting on $e \in G$, find out what b should be.)
6. Prove that if $\varphi : G \to G'$ is a homomorphism, then $\varphi(G)$, the image of G, is a subgroup of G'.
7. Show that $\varphi : G \to G'$, where φ is a homomorphism, is a monomorphism if and only if $\text{Ker}\, \varphi = (e)$.
8. Find an isomorphism of G, the group of all real numbers under $+$, *onto* G', the group of all positive real numbers under multiplication.
9. Verify that if G is the group in Example 6 of Section 1, and $H = \{T_{a,b} \in G \mid a \text{ rational}\}$, then $H \lhd G$, the dihedral group of order 8.
10. Verify that in Example 9 of Section 1, the set $H = \{i, g, g^2, g^3\}$ is a normal subgroup of G, the dihedral group of order 8.
11. Verify that in Example 10 of Section 1, the subgroup

$$H = \{i, h, h^2, \ldots, h^{n-1}\}$$

is normal in G.

12. Prove that if $Z(G)$ is the center of G, then $Z(G) \lhd G$.
13. If G is a finite abelian group of order n and $\varphi : G \to G$ is defined by $\varphi(a) = a^m$ for all $a \in G$, find the necessary and sufficient condition that φ be an isomorphism of G onto itself.
14. If G is abelian and $\varphi : G \to G'$ is a homomorphism of G *onto* G', prove that G' is abelian.
15. If G is any group, $N \lhd G$, and $\varphi : G \to G'$ a homomorphism of G *onto* G', prove that the image, $\varphi(N)$, of N is a normal subgroup of G'.
16. If $N \lhd G$ and $M \lhd G$ and $MN = \{mn \mid m \in M, n \in N\}$, prove that MN is a subgroup of G and that $MN \lhd G$.
17. If $M \lhd G$, $N \lhd G$, prove that $M \cap N \lhd G$.
18. If H is any subgroup of G and $N = \cap_{a \in G} a^{-1} H a$, prove that $N \lhd G$.
19. If H is a subgroup of G, let $N(H)$ be defined by the relation $N(H) = \{a \in G \mid a^{-1} H a = H\}$. Prove that:
    (a) $N(H)$ is a subgroup of G and $N(H) \supset H$.
    (b) $H \lhd N(H)$.
    (c) If K is a subgroup of G such that $H \lhd K$, then $K \subset N(H)$. [So $N(H)$ is the largest subgroup of G in which H is normal.]
20. If $M \lhd G$, $N \lhd G$, and $M \cap N = (e)$, show that for $m \in M, n \in N$, $mn = nm$.

21. Let S be any set having more than two elements and $A(S)$ the set of all 1-1 mappings of S onto itself. If $s \in S$, we define $H(s) = \{f \in A(S) \mid f(s) = s\}$. Prove that $H(s)$ *cannot* be a normal subgroup of $A(S)$.

22. Let $G = S_3$, the symmetric group of degree 3 and let $H = \{i, f\}$, where $f(x_1) = x_2, f(x_2) = x_1, f(x_3) = x_3$.

(a) Write down all the left cosets of H in G.

(b) Write down all the right cosets of H in G.

(c) Is every left coset of H a right coset of H?

23. Let G be a group such that all subgroups of G are normal in G. If $a, b \in G$, prove that $ba = a^j b$ for some j.

24. If G_1, G_2 are two groups, let $G = G_1 \times G_2$, the Cartesian product of G_1, G_2 [i.e., G is the set of all ordered pairs (a, b) where $a \in G_1$, $b \in G_2$]. Define a product in G by $(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2)$.

(a) Prove that G is a group.

(b) Show that there is a monomorphism φ_1 of G_1 into G such that $\varphi_1(G_1) \lhd G$, given by $\varphi_1(a_1) = (a_1, e_2)$, where e_2 is the identity element of G_2.

(c) Find the similar monomorphism φ_2 of G_2 into G.

(d) Using the mappings φ_1, φ_2 of Parts (b) and (c), prove that $\varphi_1(G_1)\varphi_2(G_2) = G$ and $\varphi_1(G_1) \cap \varphi_2(G_2)$ is the identity element of G.

(e) Prove that $G_1 \times G_2 \simeq G_2 \times G_1$.

25. Let G be a group and let $W = G \times G$ as defined in Problem 24. Prove that:

(a) The mapping $\varphi: G \to W$ defined by $\varphi(a) = (a, a)$ is a monomorphism of G into W.

(b) The image $\varphi(G)$ in W [i.e., $\{(a, a) \mid a \in G\}$] is normal in W if and only if G is abelian.

Middle-Level Problems

***26.** If G is a group and $a \in G$, define $\sigma_a: G \to G$ by $\sigma_a(g) = aga^{-1}$. We saw in Example 9 of this section that σ_a is an isomorphism of G onto itself, so $\sigma_a \in A(G)$, the group of all 1-1 mappings of G (as a set) onto itself. Define $\psi: G \to A(G)$ by $\psi(a) = \sigma_a$ for all $a \in G$. Prove that:

(a) ψ is a homomorphism of G into $A(G)$.

(b) Ker $\psi = Z(G)$, the center of G.

27. If θ is an automorphism of G and $N \lhd G$, prove that $\theta(N) \lhd G$.

28. Let θ, ψ be automorphisms of G, and let $\theta\psi$ be the product of θ and ψ as mappings on G. Prove that $\theta\psi$ is an automorphism of G, and that θ^{-1} is an automorphism of G, so that the set of all automorphisms of G is itself a group.

*29. A subgroup T of a group W is called *characteristic* if $\varphi(T) \subset T$ for all automorphisms, φ, of W. Prove that:
   (a) M characteristic in G implies that $M \triangleleft G$.
   (b) M, N characteristic in G implies that MN is characteristic in G.
   (c) A normal subgroup of a group *need not* be characteristic. (This is quite hard; you must find an example of a group G and a noncharacteristic normal subgroup.)

30. Suppose that $|G| = pm$, where $p \nmid m$ and p is a prime. If H is a normal subgroup of order p in G, prove that H is characteristic.

31. Suppose that G is an abelian group of order $p^n m$ where $p \nmid m$ is a prime. If H is a subgroup of G of order p^n, prove that H is a characteristic subgroup of G.

32. Do Problem 31 even if G is not abelian if you happen to know that for some reason or other $H \triangleleft G$.

33. Suppose that $N \triangleleft G$ and $M \subset N$ is a characteristic subgroup of N. Prove that $M \triangleleft G$. (It is *not* true that if $M \triangleleft N$ and $N \triangleleft G$, then M must be normal in G. See Problem 50.)

34. Let G be a group, $\mathcal{A}(G)$ the group of all automorphisms of G. (See Problem 28.) Let $I(G) = \{\sigma_a \mid a \in G\}$, where σ_a is as defined in Problem 26. Prove that $I(G) \triangleleft \mathcal{A}(G)$.

35. Show that $Z(G)$, the center of G, is a characteristic subgroup of G.

36. If $N \triangleleft G$ and H is a subgroup of G, show that $H \cap N \triangleleft H$.

Harder Problems

37. If G is a nonabelian group of order 6, prove that $G \simeq S_3$.

38. Let G be a group and H a subgroup of G. Let $S = \{Ha \mid a \in G\}$ be the set of all right cosets of H in G. Define, for $b \in G$, $T_b : S \to S$ by $T_b(Ha) = Hab^{-1}$.
   (a) Prove that $T_b T_c = T_{bc}$ for all $b, c \in G$ [therefore the mapping $\psi : G \to A(S)$ defined by $\psi(b) = T_b$ is a homomorphism].
   (b) Describe Ker ψ, the kernel of $\psi : G \to A(S)$.
   (c) Show that Ker ψ is the largest normal subgroup of G lying in H [largest in the sense that if $N \triangleleft G$ and $N \subset H$, then $N \subset$ Ker ψ].

39. Use the result of Problem 38 to redo Problem 37.

Recall that if H is a subgroup of G, then the *index* of H in G, $i_G(H)$, is the number of distinct right cosets of H and G (if this number is finite).

40. If G is a finite group, H a subgroup of G such that $n \nmid i_G(H)!$ where $n = |G|$, prove that there is a normal subgroup $N \neq (e)$ of G contained in H.

41. Suppose that you know that a group G of order 21 contains an element a of order 7. Prove that $A = (a)$, the subgroup generated by a, is normal in G. (**Hint:** Use the result of Problem 40.)

42. Suppose that you know that a group G of order 36 has a subgroup H or order 9. Prove that either $H \lhd G$ or there exists a subgroup $N \lhd G$, $N \subset H$, and $|N| = 3$.

43. Prove that a group of order 9 must be abelian.

44. Prove that a group of order p^2, p a prime, has a normal subgroup of order p.

45. Using the result of Problem 44, prove that a group of order p^2, p a prime, must be abelian.

46. Let G be a group of order 15; show that there is an element $a \neq e$ in G such that $a^3 = e$ and an element $b \neq e$ such that $b^5 = e$.

47. In Problem 46, show that both subgroups $A = \{e, a, a^2\}$ and $B = \{e, b, b^2, b^3, b^4\}$ are normal in G.

48. From the result of Problem 47, show that any group of order 15 is cyclic.

Very Hard Problems

49. Let G be a group, H a subgroup of G such that $i_G(H)$ is finite. Prove that there is a subgroup $N \subset H$, $N \lhd G$ such that $i_G(N)$ is finite.

50. Construct a group G such that G has a normal subgroup N, and N has a normal subgroup M (i.e., $N \lhd G$, $M \lhd N$), yet M is not normal in G.

51. Let G be a finite group, φ an automorphism of G such that φ^2 is the identity automorphism of G. Suppose that $\varphi(x) = x$ implies that $x = e$. Prove that G is abelian and $\varphi(a) = a^{-1}$ for all $a \in G$.

52. Let G be a finite group and φ an automorphism of G such that $\varphi(x) = x^{-1}$ for *more than three-fourths* of the elements of G. Prove that $\varphi(y) = y^{-1}$ for *all* $y \in G$, and so G is abelian.

6. FACTOR GROUPS

Let G be a group and N a normal subgroup of G. In proving Lagrange's Theorem we used, for an arbitrary subgroup H, the equivalence relation $a \sim b$ if $ab^{-1} \in H$. Let's try this out when N is normal and see if we can say a little more than one could say for just any old subgroup.

So, let $a \sim b$ if $ab^{-1} \in N$ and let $[a] = \{x \in G \mid x \sim a\}$. As we saw earlier, $[a] = Na$, the right coset of N in G containing a. Recall that in looking at $\mathbb{Z}_n$ we defined for it an operation $+$ via $[a] + [b] = [a + b]$. Why

1. Let $G = \{T_{a,b} \mid a \neq 0,\ b \text{ real}\}$ (Example 6 of Section 1). Let $N = \{T_{1,b} \mid b \text{ real}\} \subset G$; we saw that $N \lhd G$, so it makes sense to talk about G/N. Now $T_{a,b}$ and $T_{a,0}$ are in the same left coset of N in G, so in G/N we are getting an element by identifying $T_{a,b}$ with $T_{a,0}$. The latter element just depends on a. Moreover, the $T_{a,b}$ multiply according to $T_{a,b}T_{c,d} = T_{ac,ad+b}$ and if we identify $T_{a,b}$ with $T_{a,0}$, $T_{c,d}$ with $T_{c,0}$, then their product, which is $T_{ac,ad+b}$, is identified with $T_{ac,0}$. So in G/N multiplication is like that of the group of nonzero real numbers under multiplication, and in some sense (which will be made more precise in the next section) G/N can be identified with this group of real numbers.

2. Let G be the group of real numbers under $+$ and let $\mathbb{Z}$ be the group of integers under $+$. Since G is abelian, $\mathbb{Z} \lhd G$, and so we can talk about $G/\mathbb{Z}$. What does $G/\mathbb{Z}$ really look like? *In forming $G/\mathbb{Z}$, we are identifying any two real numbers that differ by an integer.* So 0 is identified with $-1, -2, -3, \ldots$ and $1, 2, 3, \ldots$; $\frac{3}{2}$ is identified with $\frac{1}{2}, \frac{5}{2}, -\frac{1}{2}, -\frac{3}{2}, \ldots$. Every real number a thus has a mate, $\tilde{a}$, where $0 \leq \tilde{a} < 1$. So, in $G/\mathbb{Z}$, the whole real line has been compressed into the unit interval $[0, 1]$. But a little more is true, for we have also identified the end points of this unit interval. So we are bending the unit interval around so that its two end points touch and become one. What do we get this way? A circle, of course! So $G/\mathbb{Z}$ is like a circle, in a sense that can be made precise, and this circle is a group with an appropriate product.

3. Let G be the group of nonzero complex numbers and let $N = \{a \in G \mid |a| = 1\}$ which is the unit circle in the complex plane. Then N is a subgroup of G and is normal since G is abelian. In going to G/N we are declaring that any complex number of absolute value 1 will be identified with the real number 1. Now any $a \in G$, in its polar form, can be written as $a = r(\cos\theta + i \sin\theta)$, where $r = |a|$, and $|\cos\theta + i \sin\theta| = 1$. In identifying $\cos\theta + i \sin\theta$ with 1, we are identifying a with r. So in passing to G/N every element is being identified with a positive real number, and this identification jibes with the products in G and in the group of positive real numbers, since $|ab| = |a||b|$. So G/N is in a very real sense (no pun intended) the group of positive real numbers under multiplication.

PROBLEMS

1. If G is the group of all nonzero real numbers under multiplication and N is the subgroup of all positive real numbers, write out G/N by exhibiting the cosets of N in G, and construct the multiplication in G/N.

2. If G is the group of nonzero real numbers under multiplication and

$N = \{1, -1\}$, show how you can "identify" G/N as the group of all positive real numbers under multiplication. What are the cosets of N in G?

3. If G is a group and $N \triangleleft G$, show that if $\overline{M}$ is a subgroup of G/N and $M = \{a \in G \mid Na \in \overline{M}\}$, then M is a subgroup of G, and $M \supset N$.
4. If $\overline{M}$ in Problem 3 is normal in G/N, show that the M defined is normal in G.
5. In Problem 3, show that M/N must equal $\overline{M}$.
6. Arguing as in the Example 2, where we identified $G/\mathbb{Z}$ as a circle, where G is the group of reals under $+$ and $\mathbb{Z}$ integers, consider the following: let $G = \{(a, b) \mid a, b \text{ real}\}$, where $+$ in G is defined by $(a, b) + (c, d) = (a + c, b + d)$ (so G is the plane), and let $N = \{(a, b) \in G \mid a, b \text{ are integers}\}$. Show that G/N can be identified as a torus (donut), and so we can define a product on the donut so that it becomes a group. Here, you may think of a torus as the Cartesian product of two circles.
7. If G is a cyclic group and N is a subgroup of G, show that G/N is a cyclic group.
8. If G is an abelian group and N is a subgroup of G, show that G/N is an abelian group.
9. Do Problems 7 and 8 by observing that G/N is a homomorphic image of G.
10. Let G be an abelian group of order $p_1^{a_1}p_2^{a_2} \cdots p_k^{a_k}$, where $p_1, p_2, \ldots, p_k$ are distinct prime numbers. Show that G has subgroups $S_1, S_2, \ldots, S_k$ of orders $p_1^{a_1}, p_2^{a_2}, \ldots, p_k^{a_k}$, respectively. (**Hint:** Use Cauchy's Theorem and pass to a factor group.) This result, which actually holds for all finite groups, is a famous result in group theory known as *Sylow's Theorem*. We prove it in Section 11.
11. If G is a group and $Z(G)$ the center of G, show that if $G/Z(G)$ is cyclic, then G is abelian.
12. If G is a group and $N \triangleleft G$ is such that G/N is abelian, prove that $aba^{-1}b^{-1} \in N$ for all $a, b \in G$.
13. If G is a group and $N \triangleleft G$ is such that

$$aba^{-1}b^{-1} \in N$$

for all $a, b \in G$, prove that G/N is abelian.

14. If G is an abelian group of order $p_1 p_2 \cdots p_k$, where $p_1, p_2, \ldots, p_k$ are distinct primes, prove that G is cyclic. (See Problem 15.)

1. Let $G = \{T_{a,b} \mid a \neq 0,\ b \text{ real}\}$ (Example 6 of Section 1). Let $N = \{T_{1,b} \mid b \text{ real}\} \subset G$; we saw that $N \lhd G$, so it makes sense to talk about G/N. Now $T_{a,b}$ and $T_{a,0}$ are in the same left coset of N in G, so in G/N we are getting an element by identifying $T_{a,b}$ with $T_{a,0}$. The latter element just depends on a. Moreover, the $T_{a,b}$ multiply according to $T_{a,b}T_{c,d} = T_{ac,ad+b}$ and if we identify $T_{a,b}$ with $T_{a,0}$, $T_{c,d}$ with $T_{c,0}$, then their product, which is $T_{ac,ad+b}$, is identified with $T_{ac,0}$. So in G/N multiplication is like that of the group of nonzero real numbers under multiplication, and in some sense (which will be made more precise in the next section) G/N can be identified with this group of real numbers.

2. Let G be the group of real numbers under $+$ and let $\mathbb{Z}$ be the group of integers under $+$. Since G is abelian, $\mathbb{Z} \lhd G$, and so we can talk about $G/\mathbb{Z}$. What does $G/\mathbb{Z}$ really look like? *In forming $G/\mathbb{Z}$, we are identifying any two real numbers that differ by an integer.* So 0 is identified with $-1, -2, -3, \ldots$ and $1, 2, 3, \ldots$; $\frac{3}{2}$ is identified with $\frac{1}{2}, \frac{5}{2}, -\frac{1}{2}, -\frac{3}{2}, \ldots$. Every real number a thus has a mate, $\tilde{a}$, where $0 \leq \tilde{a} < 1$. So, in $G/\mathbb{Z}$, the whole real line has been compressed into the unit interval $[0, 1]$. But a little more is true, for we have also identified the end points of this unit interval. So we are bending the unit interval around so that its two end points touch and become one. What do we get this way? A circle, of course! So $G/\mathbb{Z}$ is like a circle, in a sense that can be made precise, and this circle is a group with an appropriate product.

3. Let G be the group of nonzero complex numbers and let $N = \{a \in G \mid |a| = 1\}$ which is the unit circle in the complex plane. Then N is a subgroup of G and is normal since G is abelian. In going to G/N we are declaring that any complex number of absolute value 1 will be identified with the real number 1. Now any $a \in G$, in its polar form, can be written as $a = r(\cos\theta + i \sin\theta)$, where $r = |a|$, and $|\cos\theta + i \sin\theta| = 1$. In identifying $\cos\theta + i \sin\theta$ with 1, we are identifying a with r. So in passing to G/N every element is being identified with a positive real number, and this identification jibes with the products in G and in the group of positive real numbers, since $|ab| = |a||b|$. So G/N is in a very real sense (no pun intended) the group of positive real numbers under multiplication.

PROBLEMS

1. If G is the group of all nonzero real numbers under multiplication and N is the subgroup of all positive real numbers, write out G/N by exhibiting the cosets of N in G, and construct the multiplication in G/N.

2. If G is the group of nonzero real numbers under multiplication and

$N = \{1, -1\}$, show how you can "identify" G/N as the group of all positive real numbers under multiplication. What are the cosets of N in G?

3. If G is a group and $N \triangleleft G$, show that if $\overline{M}$ is a subgroup of G/N and $M = \{a \in G \mid Na \in \overline{M}\}$, then M is a subgroup of G, and $M \supset N$.
4. If $\overline{M}$ in Problem 3 is normal in G/N, show that the M defined is normal in G.
5. In Problem 3, show that M/N must equal $\overline{M}$.
6. Arguing as in the Example 2, where we identified $G/\mathbb{Z}$ as a circle, where G is the group of reals under $+$ and $\mathbb{Z}$ integers, consider the following: let $G = \{(a, b) \mid a, b \text{ real}\}$, where $+$ in G is defined by $(a, b) + (c, d) = (a + c, b + d)$ (so G is the plane), and let $N = \{(a, b) \in G \mid a, b \text{ are integers}\}$. Show that G/N can be identified as a torus (donut), and so we can define a product on the donut so that it becomes a group. Here, you may think of a torus as the Cartesian product of two circles.
7. If G is a cyclic group and N is a subgroup of G, show that G/N is a cyclic group.
8. If G is an abelian group and N is a subgroup of G, show that G/N is an abelian group.
9. Do Problems 7 and 8 by observing that G/N is a homomorphic image of G.
10. Let G be an abelian group of order $p_1^{a_1}p_2^{a_2} \cdots p_k^{a_k}$, where $p_1, p_2, \ldots, p_k$ are distinct prime numbers. Show that G has subgroups $S_1, S_2, \ldots, S_k$ of orders $p_1^{a_1}, p_2^{a_2}, \ldots, p_k^{a_k}$, respectively. (**Hint:** Use Cauchy's Theorem and pass to a factor group.) This result, which actually holds for all finite groups, is a famous result in group theory known as *Sylow's Theorem*. We prove it in Section 11.
11. If G is a group and $Z(G)$ the center of G, show that if $G/Z(G)$ is cyclic, then G is abelian.
12. If G is a group and $N \triangleleft G$ is such that G/N is abelian, prove that $aba^{-1}b^{-1} \in N$ for all $a, b \in G$.
13. If G is a group and $N \triangleleft G$ is such that

$$aba^{-1}b^{-1} \in N$$

for all $a, b \in G$, prove that G/N is abelian.

14. If G is an abelian group of order $p_1 p_2 \cdots p_k$, where $p_1, p_2, \ldots, p_k$ are distinct primes, prove that G is cyclic. (See Problem 15.)

Finally, we go on to the *Third Homomorphism Theorem*, which tells us a little more about the relationship between N and N' when $N' \lhd G'$.

Theorem 2.7.4 (Third Homomorphism Theorem). If the map $\varphi: G \to G'$ is a homomorphism of G onto G' with kernel K then, if $N' \lhd G'$ and $N = \{a \in G \mid \varphi(a) \in N'\}$, we conclude that $G/N \simeq G'/N'$. Equivalently, $G/N \simeq (G/K)/(N/K)$.

Proof. Define the mapping $\psi: G \to G'/N'$ by $\psi(a) = N'\varphi(a)$ for every $a \in G$. Since φ is onto G' and every element of G'/N' is a coset of the form $N'x'$, and $x' = \varphi(x)$ for some $x \in G$, we see that ψ maps G onto G'/N'.

Furthermore, ψ is a homomorphism of G onto G'/N', for $\psi(ab) = N'\varphi(ab) = N'\varphi(a)\varphi(b) = (N'\varphi(a))(N'\varphi(b)) = \psi(a)\psi(b)$, since $N' \lhd G'$. What is the kernel, M, of ψ? If $a \in M$, then $\psi(a)$ is the unit element of G'/N', that is, $\psi(a) = N'$. On the other hand, by the definition of ψ, $\psi(a) = N'\varphi(a)$. Because $N'\varphi(a) = N'$ we must have $\varphi(a) \in N'$; but this puts a in N, by the very definition of N. Thus $M \subset N$. That $N \subset M$ is easy and is left to the reader. Therefore, $M = N$, so ψ is a homomorphism of G onto G'/N' with kernel N, whence, by the First Homomorphism Theorem, $G/N \simeq G'/N'$.

Finally, again by Theorems 2.7.1 and 2.7.2, $G' \simeq G/K$, $N' \simeq N/K$, which leads us to $G/N \simeq G'/N' \simeq (G/K)/(N/K)$. □

This last equality is highly suggestive; we are sort of "canceling out" the K in the numerator and denominator.

PROBLEMS

1. Show that $M \supset N$ in the proof of Theorem 2.7.3.
2. Let G be the group of all real-valued functions on the unit interval $[0, 1]$, where we define, for $f, g \in G$, addition by $(f + g)(x) = f(x) + g(x)$ for every $x \in [0, 1]$. If $N = \{f \in G \mid f(\frac{1}{4}) = 0\}$, prove that $G/N \simeq$ real numbers under $+$.
3. Let G be the group of nonzero real numbers under multiplication and let $N = \{1, -1\}$. Prove that $G/N \simeq$ positive real numbers under multiplication.
4. If G_1, G_2 are two groups and $G = G_1 \times G_2 = \{(a, b) \mid a \in G_1, b \in G_2\}$, where we define $(a, b)(c, d) = (ac, bd)$, show that:
   (a) $N = \{(a, e_2) \mid a \in G_1\}$, where e_2 is the unit element of G_2, is a normal subgroup of G.
   (b) $N \simeq G_1$.
   (c) $G/N \simeq G_2$.

5. Let G be a group, H a subgroup of G, and $N \triangleleft G$. Let the set $HN = \{hn \mid h \in H, n \in N\}$. Prove that:
   (a) $H \cap N \triangleleft H$.
   (b) HN is a subgroup of G.
   (c) $N \subset HN$ and $N \triangleleft HN$.
   (d) $(HN)/N \simeq H/(H \cap N)$.

*6. If G is a group and $N \triangleleft G$, show that if $a \in G$ has finite order $o(a)$, then Na in G/N has finite order m, where $m \mid o(a)$. (Prove this by using the homomorphism of G onto G/N.)

7. If φ is a homomorphism of G onto G' and $N \triangleleft G$, show that $\varphi(N) \triangleleft G'$.

8. CAUCHY'S THEOREM

In Theorem 2.6.4—Cauchy's Theorem—we proved that if a prime p divides the order of a finite *abelian* group G, then G contains an element of order p. We did point out there that Cauchy's Theorem is true even if the group is not abelian. We shall give a very neat proof of this here; this proof is due to McKay.

We return for a moment to set theory, doing something that we mentioned in the problems in Section 4.

Let S be a set, $f \in A(S)$, and define a relation on S as follows: $s \sim t$ if $t = f^i(s)$ for some integer i (i can be positive, negative, or zero). We leave it to the reader as a problem that this does indeed define an equivalence relation on S. The equivalence class of s, $[s]$, is called the *orbit* of s under f. So S is the disjoint union of the orbits of its elements.

When f is of order p, p a prime, we can say something about the size of the orbits under f; those of the readers who solved Problem 34 of Section 4 already know the result. We prove it here to put it on the record officially.

[If $f^k(s) = s$, of course $f^{tk}(s) = s$ for every integer t. (Prove!)]

Lemma 2.8.1. If $f \in A(S)$ is of order p, p a prime, then the orbit of any element of S under f has 1 or p elements.

Proof. Let $s \in S$; if $f(s) = s$, then the orbit of s under f consists merely of s itself, so has one element. Suppose then that $f(s) \neq s$. Consider the elements $s, f(s), f^2(s), \ldots, f^{p-1}(s)$; we claim that these p elements are distinct and constitute the orbit of s under f. If not, then $f^i(s) = f^j(s)$ for some $0 \leq i < j \leq p - 1$, which gives us that $f^{j-i}(s) = s$. Let $m = j - i$; then $0 < m \leq p - 1$ and $f^m(s) = s$. But $f^p(s) = s$ and since $p \nmid m$, $ap + bm = 1$ for some integers a and b. Thus $f^1(s) = f^{ap+bm}(s) = f^{ap}(f^{bm}(s)) = f^{ap}(s) = s$,

Before considering the more general case of groups of order pq, let's look at a special case, namely, a group G of order 15. By Cauchy's Theorem, G has elements b of order 3 and a of order 5. By the Corollary to Lemma 2.8.3, $b^{-1}ab = a^i$, where $0 < i < 5$. Thus

$$b^{-2}ab^2 = b^{-1}(b^{-1}ab)b = b^{-1}a^ib = (b^{-1}ab)^i = (a^i)^i = a^{i^2}$$

and similarly, $b^{-3}ab^3 = a^{i^3}$. But $b^3 = e$, so we get $a^{i^3} = a$, whence $a^{i^3-1} = e$. Since a is of order 5, 5 must divide $i^3 - 1$, that is, $i^3 \equiv 1(5)$. However, by Fermat's Theorem (Corollary to Theorem 2.4.8), $i^4 \equiv 1(5)$. These two equations for i tell us that $i \equiv 1(5)$, so, since $0 < i < 5$, $i = 1$. In short, $b^{-1}ab = a^i = a$, which means that $ab = ba$. Since a is of order 5 and b of order 3, by Lemma 2.8.4, $c = ab$ is of order 15. This means that the 15 powers $e = c^0, c, c^2, \ldots, c^{14}$ are distinct, so must sweep out all of G. In a word, *G must be cyclic.*

The argument given for 15 could have been made shorter, but the form in which we did it is the exact prototype for the proof of the more general

Theorem 2.8.5. Let G be a group of order pq, where p, q are primes and $p > q$. If $q \nmid p - 1$, then G must be cyclic.

Proof. By Cauchy's Theorem, G has an element a of order p and an element b of order q. By the Corollary to Lemma 2.8.3, $b^{-1}ab = a^i$ for some i with $0 < i < p$. Thus $b^{-r}ab^r = a^{i^r}$ for all $r \geq 0$ (Prove!), and so $b^{-q}ab^q = a^{i^q}$. But $b^q = e$; therefore, $a^{i^q} = a$ and so $a^{i^q-1} = e$. Because a is of order p, we conclude that $p \mid i^q - 1$, which is to say, $i^q \equiv 1(p)$. However, by Fermat's Theorem, $i^{p-1} \equiv 1(p)$. Since $q \nmid p - 1$, we conclude that $i \equiv 1(p)$, and since $0 < i < p$, $i = 1$ follows. Therefore, $b^{-1}ab = a^i = a$, hence $ab = ba$. By Lemma 2.8.4, $c = ab$ has order pq, so the powers of c sweep out all of G. Thus G is cyclic, and the theorem is proved. □

PROBLEMS

Middle-Level Problems

1. In the proof of Theorem 2.8.2, show that if some two entries in $s = (a_1, a_2, \ldots, a_p)$ are different, then $f(s) \neq s$, and the orbit of s under f has p elements.
2. Prove that a group of order 35 is cyclic.
3. Using the result of Problem 40 of Section 5, give another proof of Lemma 2.8.3. (**Hint:** Use for H a subgroup of order p.)
4. Construct a nonabelian group of order 21. (**Hint:** Assume that $a^3 = e$,

$b^7 = e$ and find some i such that $a^{-1}ba = a^i \neq a$, which is consistent with the relations $a^3 = b^7 = e$.)

5. Let G be a group of order $p^n m$, where p is prime and $p \nmid m$. Suppose that G has a normal subgroup P of order p^n. Prove that $\theta(P) = P$ for every automorphism θ of G.
6. Let G be a finite group with subgroups A, B such that $|A| > \sqrt{|G|}$ and $|B| > \sqrt{|G|}$. Prove that $A \cap B \neq (e)$.
7. If G is a group with subgroups A, B of orders m, n, respectively, where m and n are relatively prime, prove that the subset of G, $AB = \{ab \mid a \in A, b \in B\}$, has mn distinct elements.
8. Prove that a group of order 99 has a nontrivial normal subgroup.
9. Prove that a group of order 42 has a nontrivial normal subgroup.
10. From the result of Problem 9, prove that a group of order 42 has a normal subgroup of order 21.

Harder Problems

11. If G is a group and A, B finite subgroups of G, prove that the set $AB = \{ab \mid a \in A, b \in B\}$ has $(|A|\ |B|)/|A \cap B|$ distinct elements.
12. Prove that any two nonabelian groups of order 21 are isomorphic. (See Problem 4.)

Very Hard Problems

13. Using the fact that any group of order 9 is abelian, prove that any group of order 99 is abelian.
14. Let $p > q$ be two primes such that $q \mid p - 1$. Prove that there exists a nonabelian group of order pq. (**Hint:** Use the result of Problem 40 of Section 4, namely that U_p is cyclic if p is a prime, and the idea needed to do Problem 4 above.)
15. Prove that if $p > q$ are two primes such that $q \mid p - 1$, then any two nonabelian groups of order pq are isomorphic.

9. DIRECT PRODUCTS

In several of the problems and examples that appeared earlier, we went through the following construction: If G_1, G_2 are two groups, then $G = G_1 \times G_2$ is the set of all ordered pairs (a, b), where $a \in G_1$ and $b \in G_2$ and

Proof. This follows easily from the fact that $\psi: N_1 \times N_2 \to G$, which is given by $\psi(a_1, a_2) = a_1 a_2$, is an isomorphism if and only if $N_1 N_2 = G$ and $N_1 \cap N_2 = (e)$. □

In view of the result of Theorem 2.9.4 and its corollary, we drop the adjectives "internal" and "external" and merely speak about the "direct product." When notation $G = N_1 \times N_2$ is used it should be clear from context whether it stands for the internal or external direct product.

The objective is often to show that a given group is the direct product of certain normal subgroups. If one can do this, the structure of the group can be completely determined if we happen to know those of the normal subgroups.

PROBLEMS

1. If G_1 and G_2 are groups, prove that $G_1 \times G_2 \simeq G_2 \times G_1$.

2. If G_1 and G_2 are cyclic groups of orders m and n, respectively, prove that $G_1 \times G_2$ is cyclic if and only if m and n are relatively prime.

3. Let G be a group, $A = G \times G$. In A let $T = \{(g, g) \mid g \in G\}$.
(a) Prove that $T \simeq G$.
(b) Prove that $T \lhd A$ if and only if G is abelian.

4. Let G be an abelian group of order $p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$, where $p_1, p_2, \ldots, p_k$ are distinct primes and $m_1 > 0, m_2 > 0, \ldots, m_k > 0$. By Problem 10 of Section 6, for each i, G has a subgroup P_i of order $p_i^{m_i}$. Show that $G \simeq P_1 \times P_2 \times \cdots \times P_k$.

5. Let G be a finite group, $N_1, N_2, \ldots, N_k$ normal subgroups of G such that $G = N_1 N_2 \cdots N_k$ and $|G| = |N_1|\,|N_2| \cdots |N_k|$. Prove that G is the direct product of $N_1, N_2, \ldots, N_k$.

6. Let G be a group, $N_1, N_2, \ldots, N_k$ normal subgroups of G such that:
1. $G = N_1 N_2 \cdots N_k$.
2. For each i, $N_i \cap (N_1 N_2 \cdots N_{i-1} N_{i+1} \cdots N_k) = (e)$.

Prove that G is the direct product of $N_1, N_2, \ldots, N_k$.

10. FINITE ABELIAN GROUPS (OPTIONAL)

We have just finished discussing the idea of the direct product of groups. If we were to leave that topic at the point where we ended, it might seem like a nice little construction, but so what? To give some more substance to it,

For $n = 4$ we see the partitions are $4 = 4$, $4 = 3 + 1$, $4 = 2 + 2$, $4 = 2 + 1 + 1$, $4 = 1 + 1 + 1 + 1$, which are five in number. Thus there are five nonisomorphic groups of order p^4. Can you describe them via the partitions of 4?

Given an abelian group of order $n = p_1^{a_1}p_2^{a_2} \cdots p_k^{a_k}$, where the p_i are distinct primes and the a_i are all positive, then G is the direct product of its so-called p_i– Sylow subgroups (see, e.g., the Corollary to Lemma 2.10.1). For each prime p_i there are as many groups of order $p_i^{a_i}$ as there are partitions of a_i. So the number of nonisomorphic abelian groups of order $n = p_1^{a_1} \cdots p_k^{a_k}$ is $f(a_1)f(a_2) \cdots f(a_k)$, where $f(m)$ denotes the number of partitions of m. Thus we know how many nonisomorphic finite abelian groups there are for any given order.

For instance, how many nonisomorphic abelian groups are there of order 144? Since $144 = 2^4 3^2$, and there are five partitions of 4, two partitions of 2, there are 10 nonisomorphic abelian groups of order 144.

The material treated in this section has been hard, the path somewhat tortuous, and the effort to understand quite intense. To spare the reader too much further agony, we assign only three problems to this section.

PROBLEMS

1. Let A be a normal subgroup of a group G, and suppose that $b \in G$ is an element of prime order p, and that $b \notin A$. Show that $A \cap (b) = (e)$.

2. Let G be an abelian group of order p^n, p a prime, and let $a \in G$ have maximal order. Show that $x^{o(a)} = e$ for all $x \in G$.

3. Let G be a finite group, with $N \lhd G$ and $a \in G$. Prove that:

(a) The order of aN in G/N divides the order of a in G, that is, $o(aN) \mid o(a)$.

(b) If $(a) \cap N = (e)$, then $o(aN) = o(a)$.

11. CONJUGACY AND SYLOW'S THEOREM (OPTIONAL)

In discussing equivalence relations in Section 4 we mentioned, as an example of such a relation in a group G, the notion of *conjugacy*. Recall that the element b in G is said to be *conjugate* to $a \in G$ (or merely, a conjugate of a) if there exists an $x \in G$ such that $b = x^{-1}ax$. We showed in Section 4 that this defines an equivalence relation on G. The equivalence class of a, which we denote by $\mathrm{cl}(a)$, is called the *conjugacy class* of a.

PROBLEMS

Easier Problems

1. In S_3, the symmetric group of degree 3, find all the conjugacy classes, and check the validity of the class equation by determining the orders of the centralizers of the elements of S_3.
2. Do Problem 1 for G the dihedral group of order 8.
3. If $a \in G$, show that $C(x^{-1}ax) = x^{-1}C(a)x$.
4. If φ is an automorphism of G, show that $C(\varphi(a)) = \varphi(C(a))$ for $a \in G$.
5. If $|G| = p^3$ and $|Z(G)| \geq p^2$, prove that G is abelian.
6. If P is a p-Sylow subgroup of G and $P \lhd G$, prove that P is the only p-Sylow subgroup of G.
7. If $P \lhd G$, P a p-Sylow subgroup of G, prove that $\varphi(P) = P$ for every automorphism φ of G.
8. Use the class equation to give a proof of Cauchy's Theorem.

   If H is a subgroup of G, let $N(H) = \{x \in G \mid x^{-1}Hx = H\}$. This *does not mean* that $xa = ax$ whenever $x \in N(H)$, $a \in H$. For instance, if $H \lhd G$, then $N(H) = G$, yet H need not be in the center of G.
9. Prove that $N(H)$ is a subgroup of G, $H \subset N(H)$ and in fact $H \lhd N(H)$.
10. Prove that $N(x^{-1}Hx) = x^{-1}N(H)x$.
11. If P is a p-Sylow subgroup of G, prove that P is a p-Sylow subgroup of $N(P)$ and is the only p-Sylow subgroup of $N(P)$.
12. If P is a p-Sylow subgroup and $a \in G$ is of order p^m for some m, show that if $a^{-1}Pa = P$ then $a \in P$.
13. Prove that if G is a finite group and H is a subgroup of G, then the number of distinct subgroups $x^{-1}Hx$ of G equals $i_G(N(H))$.
14. If P is a p-Sylow subgroup of G, show that the number of distinct $x^{-1}Px$ *cannot* be a multiple of p.
15. If $N \lhd G$, let $B(N) = \{x \in G \mid xa = ax \text{ for all } a \in N\}$. Prove that $B(N) \lhd G$.

Middle-Level Problems

16. Show that a group of order 36 has a normal subgroup of order 3 or 9. (**Hint:** See Problem 40 of Section 5.)
17. Show that a group of order 108 has a normal subgroup of order 9 or 27.
18. If P is a p-Sylow subgroup of G, show that $N(N(P)) = N(P)$.
19. If $|G| = p^n$, show that G has a subgroup of order p^m for all $1 \leq m \leq n$.

20. If p^m divides $|G|$, show that G has a subgroup of order p^m.

21. If $|G| = p^n$ and $H \neq G$ is a subgroup of G, show that $N(H) \supsetneq H$.

22. Show that any subgroup of order p^{n-1} in a group G of order p^n is normal in G.

Harder Problems

23. Let G be a group, H a subgroup of G. Define for $a, b \in G$, $a \sim b$ if $b = h^{-1}ah$ for some $h \in H$. Prove that

(a) this defines an equivalence relation on G.

(b) If $[a]$ is the equivalence class of a, show that if G is a finite group, then $[a]$ has m elements where m is the index of $H \cap C(a)$ in H.

24. If G is a group, H a subgroup of G, define a relation $B \sim A$ for subgroups A, B of G by the condition that $B = h^{-1}Ah$ for some $h \in H$.

(a) Prove that this defines an equivalence relation on the set of subgroups of G.

(b) If G is finite, show that the number of distinct subgroups equivalent to A equals the index of $N(A) \cap H$ in H.

25. If P is a p-Sylow subgroup of G, let S be the set of all p-Sylow subgroups of G. For $Q_1, Q_2 \in S$ define $Q_1 \sim Q_2$ if $Q_2 = a^{-1}Q_1a$ with $a \in P$. Prove, using this relation, that if $Q \neq P$, then the number of distinct $a^{-1}Qa$, with $a \in P$, is a multiple of p.

26. Using the result of Problem 25, show that the number of p-Sylow subgroups of G is of the form $1 + kp$. (This is the third part of Sylow's Theorem.)

27. Let P be a p-Sylow subgroup of G, and Q another one. Suppose that $Q \neq x^{-1}Px$ for any $x \in G$. Let S be the set of all $y^{-1}Qy$, as y runs over G. For $Q_1, Q_2 \in S$ define $Q_1 \sim Q_2$ if $Q_2 = a^{-1}Q_1a$, where $a \in P$.

(a) Show that this implies that the number of distinct $y^{-1}Qy$ is a multiple of p.

(b) Using the result of Problem 14, show that the result of Part (a) cannot hold.

(c) Prove from this that given any two p-Sylow subgroups P and Q of G, then $Q = x^{-1}Px$ for some $x \in G$.
(This is the second part of Sylow's Theorem.)

28. If H is a subgroup of G of order p^m show that H is contained in some p-Sylow subgroup of G.

29. If P is a p-Sylow subgroup of G and $a, b \in Z(P)$ are conjugate in G, prove that they are already conjugate in $N(P)$.

2
Groups

SECTION 1.

Easier Problems.

1. (a). G is not a group. The associative law fails to hold in G. Also G has no identity element; although $a*0 = a$ for a in G, $0*a = -a \neq a$ if $a \neq 0$.

(b). G is not a group only because -1 fails to have an inverse with regards to *. G is clearly closed under *, and 0 acts as the identity element since $a*0 = a + 0 + a\cdot 0 = a$ and $0*a = 0 + a + 0\cdot a = a$. The operation * is associative for $a*(b*c) = a + b*c + a(b*c) = a + (b + c + bc) + a(b + c + bc) = a + b + c + ab + ac + abc$, while $(a*b)*c = a*b + c + (a*b)c = a + b + ab + c + (a + b + ab)c = a + b + c + ac + bc + abc$. If $a \neq -1$ then, as is easily verified, $a*b = 0$ where $b = -a(1 + a)^{-1}$. However there is no b such that $(-1)*b = 0$, since $(-1)*b = -1 + b + (-1)b = -1 \neq 0$ for every b in G. So G comes close to being a group but doesn't quite make it.

(c). Using the information obtained in Part (b) we see that G is not a group for, not only does -1 fail to have an inverse relative to *, but this is true for every nonzero element of G, since the inverse of $a \neq -1$ is $-a(1 + a)^{-1}$ which is negative and not an integer so is not in G.

(d). G is a group under *. From what we have seen in Part (b) all we really have to show to verify this is that G is closed under *, that is, if $a \neq -1$ and $b \neq -1$ then $a*b \neq -1$. But, if $-1 = a*b = a + b + ab$, we get that $(1 + a)(1 + b) = 0$ which is not possible if $a \neq -1$ and $b \neq -1$.

(e). G is not a group for 1/5 and 4/5 are in G and $(1/5)*(4/5) = 1/5 + 4/5 = 1$ which is not in G. So G is not closed under *.

(f). G is not a group, although * is an associative operation relative to which G is closed. However G has no identity element, for if e were such then for $b \neq e$, $e*b = e \neq b$.

2. As we saw in the text, the rule for combining T's is given by $T_{a,b}T_{c,d} = T_{ac,ad+b}$. Thus, if $a = \pm 1$ and $c = \pm 1$, then $ac = \pm 1$; therefore G is closed under the product. Moreover H is a subset of the group in Example 6 so we know that the product in H is associative. The identity element $T_{1,0}$ is in H and since $T_{a,b}^{-1} = T_{a^{-1},-a^{-1}b}$ and $a^{-1} = \pm 1$ if $a = \pm 1$ we see that every element in H has its inverse in H. Thus H is a group.

5. Where does g*f map the point (x,y) ? By definition $(g*f)((x,y)) = g(f((x,y))) = g((-x,y) = (-y,-x)$; as is verified by a computation, $g^{-1}((x,y)) = (y,-x)$ therefore $(f*g^{-1})((x,y) = f(g^{-1}((x,y))) = f((y,-x) = (-y,-x)$. Thus $g*f = f*g^{-1}$.

6. Since $H = \{T_{c,d} \in G \mid c \text{ rational, } d \text{ any real}\}$, if $T_{c,d} \in H$ and $T_{a,b} \in G$ then $T_{a,b}T_{c,d}T_{a,b}^{-1} = T_{ac,ad+b}T_{a^{-1},-a^{-1}b} = T_{a,ad-bc+d}$, so is in H.

8. If $n > 0$ we proceed by induction on n. If $n = 1$ then certainly $(a*b)^1 = a*b$. Suppose that for some m we know that $(a*b)m = a^m*b^m$; then $(a*b)^{m+i} = (a*b)*(a*b)^m = (a*b)*(a^m*b^m) = a*(b*(a^m*b^m))$ $=a*((b*a^m)*b^m) = a*((a^m*b)*b^m) = a*(a^m*(b*b^m)) = (a*a^m)*(b*b^m) = a^{m+1}*b^{m+1}$, having made use of the fact that G is abelian and * is associative. This completes the induction and proves the result for all positive integers n. By definition $a^0 = e$ for all a in G so that $(a*b)^0 = e = e*e = a^0*b^0$. Finally, if $n < 0$ then $n = -m$ where $m > 0$ and $a^n = (a^{-1})^m$; since G is abelian, $(a*b)^{-1} = a^{-1}*b^{-1}$ so $(a*b)^n = ((a*b)^{-1})^m = (a^{-1}*b^{-1})^m = (a^{-1})^m*(b^{-i})^m$ (by the result we proved for $m > 0$) $= a^n*b^n$.

In future calculations we shall not be as formal as above and will use the associative law freely, and avoid these long chains of equalities.

9. Suppose $a^2 = e$ for every a in the group G. If a,b are in G then $(a*b)^2 = e$, thus $a*b*a*b = e$; multiply both sides of this relation by a to obtain $a^2*b*a*b = a$, and since $a^2 = e$, $b*a*b = a$. Multiply both sides of this relation on the left by b to obtain $b^2*a*b = b*a$, and since $b^2 = e$, we end up with $a*b = b*a$. Thus G is abelian.

11. Since the * in the example is just the composition of mappings, for ease of notation we drop it and write the product a*b simply as ab.

We are considering the elements f^ih^j where $f^2 = h^3 = e$ and $fh = h^{-1}f$. Thus $fh^2 = h^{-1}fh = h^{-2}f$; so $fh^t = h^{-t}f$ for all integers t, and $h^tf = fh^{-t}$. Thus $(f^ih^j)(fh^t) = f^ifh^{-j+t} = f^{i+1}h^{t-j}$ and $(f^ih^j)(f^0h^t) = f^ih^{j+t}$; these two results can be succinctly written as $(f^ih^j)(f^sh^t) = f^ah^b$ where $a = i + j$ and $b = t + (-1)^sj$. Thus G is closed under the product of mappings. Since $e = f^2h^3$, e is in G. Also, $(f^ih^j)^{-1} = h^{-j}f^{-i} = f^{-i}h^j$ so is in G. (Don't forget, the exponent of f is calculated mod 2 and that of h is mod 3.) Finally,since we are talking about the product of mappings, the product is associative. Thus G is a group.

That G is of order 6 is easy since, in f^ih^j, i has 2 possibilities and j has 3, and these give rise to 6 distinct elements (Check it!) That G is non-abelian is clear since $fh \neq hf$.

13. Suppose that G has 4 elements; let e, a, and b be 3 distinct elements of G. Thus both a*b and b*a are in G; if they are not equal then b*a = e, a, or b. If a*b = e then we quickly get b*a = e and so a*b = b*a. If a*b = a then b = e and if a*b= b then a = e (see the next problem for this), both of which are contradictions. So we get that a*b = b*a and G consists of e, a, b, and a*b. To check that G is abelian one should also check that a(a*b) =(a*b)a and b(a*b) = (a*b)b; we leave these to the reader.

14. See the proof of Lemma 2.2.2.

16. Since $a^2 = e$ for every a in G, by the definition of a^{-1} we have that $a = a^{-1}$. Thus, if a and b are in G then $a*b = (a*b)^{-1} = b^{-1}*a^{-1} = b*a$, hence G is abelian.

18. Suppose that G is a finite group of even order; if $a \neq a^{-1}$ for every a in G other than e, since $a = (a^{-1})^{-1}$ we get an even number of elements which are not e, together with e this would give G an odd number of elements, contrary to our assumption.

Middle-Level Problems.

21. If G is of order 5, then for every element a in G there is a least positive integer k, depending on a, such that $a^k = e$. If $k = 5$ then G must consist merely of e, a, a^2, a^3, and a^4, so is abelian. If $k = 4$ and b in G is not a power of a then $a*b \neq a^i$ any i so e, a, a^2, a^3, and a*b exhaust G; now b*a is in G and is not a power of a, for if $b*a = a^i$ we immediately get that $b = a^{i-1}$, a contradiction. Thus b*a is forced to equal a*b, and so we see that G is abelian. If $k = 3$, then e, a, a^2 are already 3 distinct elements of G. Let b in G not be a power of a; then, as above, $b \neq a*b$, so the elements of G are e, a, a^2, b, and a*b. What can b*a possibly be? As above we quickly arrive at $a*b = b*a$. So we are left with the only possibilty, namely that every a in G satisfies $a^2 = e$. By the result of Problem 9, G must be abelian. In actual fact, as we shall see in Section 4, the first case, $k = 5$, is the only possibility if G has order 5.

24. G is generated by 2 elements f and h satisfying $f^2 = h^n = e$ and $fh = h^{-1}f$, and all the elements of G are of the unique form f^ih^j where $i = 0$ or 1 and j can be any integer $0 \leq j \leq n-1$. Suppose that $a \in G$ satisfies $a*b = b*a$ for all $b \in G$; if $a = f^ih^j$ then, since $f*a = a*f$ we get $f^{i+1}h^j = ff^ih^j = f^ih^jf = f^ifh^{-j}$, by the formula for the product in G derived in Problem 11 (and

Problem 22). Thus $h^{2j} = e$. Also $a*h = h*a$, which gives us that $f^{i}h^{j+1} = f^{i}h^{j}h = hf^{i}h^{j} = fh^{\pm i+j}$ (the + if i = 0 and the - if i = 1) according the the formula obtained in Problem 11. This implies that i = 0; thus $a = h^{j}$ where $h^{2j} = e$, (that is, $a^{2} = e$). Thus if d is the greatest common divisor of n and 2j, $h^{d} = e$.

(a). If n is odd then d = (n,2j) = (n,j); thus d | j, hence $a = h^{j} = h^{kd} = e$.

(b). If n is even then if $a = h^{n/2}$, $fh^{n/2} = h^{-n/2}f = h^{n/2}f$ since $h^{n/2} = h^{-n/2}$, because $h^{n} = e$. From the form of the elements in G we get that $a*b = b*a$ for all b in G.

(c). From the argument above, $a = h^{2j}$ where $h^{2j} = e$; this tells us that 2j = 0 or n and so j = 0 or n/2. Thus the only possibilities for a are a = e or $a = h^{n/2}$.

26. This problem was already done for S_n; the same proof works for any finite group. Let $a \in G$, where G has order k; then a, a^{2} a^{3}, ..., a^{k+1} are k + 1 elements in G, whch only has k elements. Thus 2 of a, a^{2}, ... , a^{k+1} are equal; that is $a^{i} = a^{j}$ for some $1 \le i < j \le k + 1$, and so $a^{j-1} = e$, where $0 < j - i \le k$. Let n = j - i.

Harder Problems.

28. Let $x \in G$ and let y be such that $y*x = e$. Since y is in G there is a z in G such that $z*y = e$. Therefore $z*e = z*(y*x) = (z*y)*x = e*x = x$, which is to say, $z*e = x$. Thus $x*y = (z*e)*y = z*(e*y) = z*y = e$. Also, $x*e = x*(y*x) = (x*y)*x = e*x = x$. Hence, for all x in G, $x*e = e*x$ and there is a y in G such that $x*y = y*x = e$. Since * is associative, G is a group.

29. Let $G = \{a_1, \dots, a_n\}$. If $b \in G$ consider the elements $a_1*b, \dots, a_n*b$; these are all distinct, for $a_i*b = a_j*b$ implies that $a_i = a_j$ by Hypothesis 3.

So these elements must be all the elements of G. Therefore b appears in this list, that is, $b = e*b$ for some e in G. Now consider the elements $b*a_1, \ldots, ba_n$ by Hypothesis 4 these are all distinct so must be all the elements of G in some order. Thus, given x in G, $x = b*a_i$ for some i. Hence $e*x = e*(b*a_i) = (e*b)*a_i = b*a_i = x$. Since e is in G and $a_1*b, \ldots, a_n*b$ give us all the elements of G, $e = y*x$ for some y in G. By the result of Problem 28, G is a group.

31. (a). Let $F(a) = \log_{10}(|ab|)$; then $F(a*b) = \log_{10}(|a*b|) = \log_{10}(|ab|) = \log_{10}(|a||b|) = \log_{10}|a| + \log_{10}|b| = F(a) + F(b) = F(a)*F(b)$

(b). Suppose that F is a mapping from G to H such that $F(a*b) = F(a)*F(b)$. Thus $F(a) = F(1*a)) = F(1)*F(a) = F(1) + F(a)$, therefore $F(1) = 0$. But $0 = F(i) = F((-1)^2) = F(-1)*F(-1) = F(-1) + F(-1) = 2F(-1)$, hence $F(-1) = 0 = F(1)$, therefore F is not 1-1.

SECTION 2.

1. Given $a \in G$, by Hypothesis (a) there is an element $e \in G$ such that $ae = a$. Furthermore, given $w \in G$, by Hypothesis (b) there is an element u in G such that $w = ua$. Thus $we = (ua)e = u(ae) = ua = w$. Also, by (a) there is an x in G such that $ax = e$. By Problem 28 of Section 2 (with things on the right instead of the left) G is a group.

3. This is a tricky problem. Suppose that $(ab)^i = a^ib^i$, $(ab)^{i+1} = a^{i+1}b^{i+1}$, and $(ab)^{i+2} = a^{i+2}b^{i+2}$. Therefore $ab(ab)^i = (ab)^{i+1} = a^{i+1}b^{i+1}$; since we are in a group we can cancel a on the left and b on the right to obtain that $(ba)^i = a^ib^i = (ab)^i$. Since $(ab)^{i+1} = a^{i+1}b^{i+1}$ and $(ab)^{i+2} = a^{i+2}b^{i+2}$, the

argument just used gives us $(ba)^{l+1} = (ab)^{l+1}$. Therefore $ba(ba)^l = a^{l+1}b^{l+1} = (ab)^{l+1} = ab(ab)^l = ab(ba)^l$; cancelling the $(ba)^l$ from this we obtain that $ba = ab$. Thus G is abelian.

5. By assumption $(ab)^3 = a^3b^3$, so, as in Problem 3, $(ba)^2 = a^2b^2$ and $(ab)^5 = a^5b^5$, so $(ba)^4 = a^4b^4$. Thus $a^4b^4 = (ba)^4 = ((ba)^2)^2 = a^2b^2a^2b^2$ which gives us $a^2b^2 = b^2a^2$. Hence $(ab)^2 = b^2a^2 = a^2b^2$; cancelling an a from the left and a b from the right yields $ab = ba$. Thus G is abelian.

6. (a). From $(ba)^n = b^na^n$, cancelling b from the left and a from the right gives us $(ab)^{n-1} = b^{n-1}a^{n-1}$.

(b). $a^nb^n = (ab)^n = ab(ab)^{n-1} = abb^{n-1}a^{n-1}$ from Part (a); cancelling a from the left and b from the right gives $a^{n-1}b^n = b^na^{n-1}$.

SECTION 3.

Easier Problems.

2. The cyclic subgroup generated in Z by -1 is all of Z.

3. S_3 has the 6 elements e, f, g, g^2, fg, gf where $f^2 = g^3 = e$ and $fg = g^{-1}f$. The subgroups of S_3 are : {e}, {e,f}, {e,fg}, {e,gf}, and {e, g, g^2}.

4. If $a,b \in Z(G)$ then $ax = xa$ and $bx = xb$ for all x in G. Thus $(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$. Therefore ab is in Z(G). Also, from $ax = xa$ we obtain that $a^{-1}(ax)a^{-1} = a^{-1}(xa)a^{-1}$ which gives us $a^{-1}x = xa^{-1}$ for all x in G. Thus a^{-1} is in Z(G). Thus Z(G) is a subgroup of G.

7 Using the notation of Problem 3, we see that $C(f) = \{e,f\}$, $C(fg) = \{e,fg\}$, $C(gf) = \{e,gf\}$, $C(g) = \{e,g,g^2\} = C(g^2)$, and $C(e) = S_3$.

9. S_3 is such an example for in it the elements satisfying $x^2 = e$ are e, f, fg, gf (in the notation of Problem 3) and these do <u>not</u> form a subgroup of S_3

11. Suppose that a and b are in H, then $a^m = e$ and $b^n = e$ for some

positive integers m and n. Thus, since G is abelian, $(ab)^{mn} = a^{mn}b^{mn} = e$, which puts ab in H. Also, if a is in H and $a^m = e$ then $(a^{-1})^m = (a^m)^{-1} = e$. thus a^{-1} is in H. So H is a subgroup of G.

13. Let G be a cyclic group and H a subgroup of G. Suppose that a in G is a generator of G. If $H = \{e\}$ then H is certainly cyclic, being generated by the element e. Suppose, then, that $H \neq \{e\}$; if $x \neq e$ is in H then $x = a^i$, where $i \neq 0$. If $i < 0$ then, since H is a subgroup of G, $x^{-1} = a^{-i}$ is in H and $-i > 0$. Therefore a to some positive power falls in H. Thus there is a smallest positive power k such that a^k is in H. Suppose that y is in H; then $y = a^m$ for some m. By the Euclidean Algorithm, $m = qk + r$ where $0 \leq r < k$. Now $y = a^m = a^{qk+r} = a^{qk}a^r$ and so $a^r = a^{-qk}y$ is in H since both y and $a^{-qk} = (a^k)^{-q}$ are in H. Since $r < k$, by the definition of k we cannot have that $r > 0$. Therefore $r = 0$, hence $m = qk$. This shows that $y = (a^k)^q$; thus H is a cyclic group with generator a^k.

14. Suppose that G has no proper subgroups. Let $a \neq e$ be in G and consider $H = \{a^i \mid i \text{ any integer}\}$. As is immediate, if x and y are in H then xy and x^{-1} are in H. Thus H is a subgroup of G, and $H \neq \{e\}$ since $a \neq e$ is in H. Thus, by hypothesis, H = G. Thus G is cyclic with a as generator.

Middle-Level Problems.

16. By the result of Problem 14 <u>any</u> element of G other than e generates G. If a is in G and $a^2 = e$ then the group generated by a has 2 elements, that is, G has 2 elements. If $a^2 \neq e$ then every element of G is a power of a^2; in particular, $a = (a^2)^m = a^{2m}$, hence $a^{2m-1} = e$, for some integer m. Since $2m - 1 \neq 0$ one of $2m - 1 > 0$ or $1 - 2m > 0$. At any rate we get that $a^p = e$ for some smallest positive integer p. Thus G consists of the p distinct elements $e, a, a^2, \ldots, a^{p-1}$. We claim that p is a prime. If $p = uv$ where both $u > 1$ and $v > 1$ then if $b = a^u \neq e$ the subgroup T generated by b consists of

the v elements e, b, b^2, ... ,b^{v-1} since $b^v = a^{uv} = a^p = e$. But T = G, so v = p since v is the order of T, and p is that of G. But then u = 1, contrary to u > 1. Thus p is a prime and |G| = p.

18. Since S is finite A(S) is a finite group. If f and g are in T(X) then $f(X) \subset X$ and $g(X) \subset X$; hence $(fg)(X) = f(g(X) \subset f(X) \subset X$ and so fg is in T(X). Since A(S) is a finite group and T(X) is closed under the product of A(S), T(X) is a subgroup of A(S).

19. Suppose that $x = a_1b_1$ and $y = a_2b_2$ are in AB, where a_1, a_2 are in A and b_1, b_2 are in B. Since G is abelian, $xy = a_1b_1a_2b_2 = a_1a_2b_1b_2 \in AB$, and $x^{-1} = (a_1b_1)^{-1} = b_1^{-1}a_1^{-1} = a_1^{-1}b_1^{-1} \in AB$. Thus AB is a subgroup of G.

22. and 23. We saw in Problem 19 that AB is a subgroup of G. How can $AB = \{ab \mid a \in A, b \in B\}$ fail to have mn distinct elements? Only if there is some collapsing of these elements, that is, if and only if for some distinct pairs (a_1,b_1), (a_2b_2) we have $a_1b_1 = a_2b_2$. But this implies that $a_2^{-1}a_1 = b_2b_1^{-1}$ and since the left side is in A and the right side is in B, the elements on both sides are in $A \cap B$. Thus $a_1 = a_2c$ and $b_1 = c^{-1}b_2$ where c is in $A \cap B$. But, if $c \in A \cap B$ and if $a \in A$, $b \in B$ then $a_1 = ac$ is in A and $b_1 = c^{-1}b$ is in B and $a_1b_1 = (ac)(c^{-1}b) = ab$. Thus there are exactly $|A \cap B|$ pairs giving rise to the same ab. Thus $|AB| = mn/|A \cap B| = |A||B|/|A \cap B|$. This solves Problem 23. However, to solve the present problem, we must show that if |A| and |B| are relatively prime then $A \cap B = \{e\}$ so that $|A \cap B| = 1$. This is most easily done after we learn Lagrange's Theorem. Note that the argument used for |AB| did **not** depend on G being abelian. This will be used many times in the problems in the rest of this chapter.

24. That N is a subgroup follows because the intersection of any number

of subgroups of G is a subgroup of G. (This is a slight generalization of the result in Problem 1; the proof we gave there works in this more general situation). If $x,y \in G$ then $y^{-1}(x^{-1}Hx)y = (xy)^{-1}H(xy)$ and as x runs over G with y fixed then xy runs over all the elements of G. Thus $y^{-1}(n\,(x^{-1}Hx))y = n\,(xy)^{-1}H(xy)$, as x runs over G, $= n\,x^{-1}Hx$, as x runs over G by the remark above. Thus $y^{-1}Ny = N$.

Harder Problems.

25. Let S be the set of all the integers and let X be the set of positive integers. Let f be the 1-1 mapping of S onto itself defined by $f(n) = n + 1$ for every integer n. Then certainly $f(X) \subset X$, hence $f \in T(X)$ but f^{-1} is <u>not</u> in T(X) since $f^{-1}(1) = 0$, which is not in X. Thus T(X) <u>cannot</u> be a subgroup of A(S).

26. See the proof of Lagrange's Theorem (Theorem 2.4.2) in the next section.

28. We first check that MN is a subgroup of G. If mn, m_1n_1 are in MN, where m, m_1 are in M and n, n_1 are in N then $(mn)(m_1n_1) = (mnmn^{-1})nn_1$ and by the hypothesis on M, nmn^{-1} is in M thus $mnmn^{-1}$ is in M, and nn_1 is in N. Therefore $(mn)(m_1n_1)$ is in MN, hence MN is closed under the product in G. Also $(mn)^{-1} = n^{-1}m^{-1} = (n^{-1}m^{-1}n)n^{-1}$ so is in MN since $n^{-1}m^{-1}n$ is in M and n^{-1} is in N. Thus MN is a subgoup of G.

If $x \in G$ then $x^{-1}(MN)x = (x^{-1}Mx)(x^{-1}Nx) \subset MN$ by our hypothesis on M and N.

30. Consider the element $a = mnm^{-1}n^{-1}$; bracketing it one way, $a = (mnm^{-1})n^{-1}$ so is in N since mnm^{-1} and n^{-1} are in N. On the other hand, bracketing it another way, $a = m(nm^{-1}n^{-1})$ so is in M since m and $nm^{-1}n^{-1}$

are in M. Thus $a \in M \cap N = (e)$. This tells us that $e = a = mnm^{-1}n^{-1}$, which implies that $mn = nm$.

SECTION 4.

Easier Problems.

2. The relation $\sim$ defined on $\mathbb{R}$ by $a \sim b$ if both $a > b$ and $b > a$ satisfies the symmetry and transitivity properties but fails to satisfy $a \sim a$.

3. The argument starts with "if $a \sim b$ ... ", however there may be no element b which satisfies this, as is exemplified in Problem 2. However, if we insist that for every a there is some b such that $a \sim b$ then the argument is valid and $\sim$ is then an equivalence relation.

4. Suppose that S is the union of the mutually-disjoint, non-empty subsets S_α. Thus, given s in S there is one and only one S_α such that $s \in S_\alpha$ so if we define $a \sim b$ if a and b lie in the same S_α then we easily see that $\sim$ is an equivalence relation and the equivalence class of s is precisely that S_α in which s lies.

8. Suppose every left coset of H in G is a right coset of H in G. Thus, if a is in G, Ha must be a right coset of H in G, thus $Ha = bH$ for some b in G. But a is in Ha so a must be in bH; because a is in aH and, by Problem 5, the right cosets are equivalence classes, we have that $bH = aH$. Thus $Ha = aH$, hence $H = aHa^{-1}$.

11. Let $\mathbf{M}$ be the set of all left cosets of H in G and $\mathbf{N}$ the set of all right cosets of H in G. Define the mapping F from $\mathbf{M}$ to $\mathbf{N}$ by $F(Ha) = a^{-1}H$. This is clearly a mapping of $\mathbf{M}$ onto $\mathbf{N}$ because, given the right coset xH, then

$xH = F(Hx^{-1})$. Is F 1-1? Yes, because if $F(Ha) = F(Hb)$ then $a^{-1}H = b^{-1}H$, and so $H = ab^{-1}H$; this puts ab^{-1} in H whence $Ha = Hb$. So, even for infinite groups there is a 1-1 correspondence of $\mathbf{M}$ onto $\mathbf{N}$; for finite groups this translates into : $\mathbf{M}$ and $\mathbf{N}$ have the same number of elements. Thus there are the same number of left cosets of H in G as there are right cosets of H in G.

12. The answer is no. For instance if $G = S_3$ and H is the subgroup in Problem 6, then $Hg = \{g, fg\}$ and $Hfg = \{fg, f^2g = g\} = Hg$, while $gH = \{g, gf\}$ and $fgH = \{fg, ffg = g\}$. Because $fg \neq gf$ we see that $fgH \neq gH$ yet $Hfg = Hg$.

13. The elements of U_{18} are $\{[1], [5], [7], [11], [13], [17]\}$. The orders of these are: $o([1]) = 1$, $o([5]) = 6$, $o([7]) = 3$, $o([11]) = 6$, $o([13]) = 3$, $o([17]) = 2$. We verify one of them, namely that $o([7]) = 3$; the other verifications are similar. $[7]^1 = [7]$, $[7]^2 = [49] = [13]$, $[7]^3 = [7][13] = [91] = [1]$. Thus the order of [7] is 3 since that is the first positive power of [7] which is the identity element of U_{18}. The group is cyclic since $o([5]) = 6$, so the powers of [5] sweep out all of U_{18}.

15. If $x^2 \equiv 1 \bmod p$ then $p \mid (x^2 - 1) = (x - 1)(x + 1)$. Since p is a prime this tells us that either $p \mid (x - 1)$ or $p \mid (x + 1)$. The first of these yields that $x \equiv 1 \bmod p$ and the second yields $x \equiv -1 \bmod p$.

16. For every a in G there is an inverse a^{-1} in G; if $a \neq a^{-1}$, then in the product $a_1a_2...a_n$, a cancels against a^{-1} since G is abelian. Thus the only terms remaining uncancelled in $a_1...a_n$ are those elements of G which are their own inverses. Since each such element has square equal to e, we get, again using that G is abelian, that $(a_1a_2...a_n)^2 = e$.

20. Recall the basic multiplication rule: $T_{a,b}T_{c,d} = T_{ac,ad+b}$ from which we saw that $T_{c,d}^{-1} = T_{c^{-1},-c^{-1}d}$. Thus $T_{c,d}^{-1}T_{a,b}T_{c,d} = T_{c,d}^{-1}T_{ac,ad+b} = T_{c^{-1},-c^{-1}d}T_{ac,ad+b} = T_{a,c^{-1}(ad+b)-c^{-1}d} = T_{a,x}$ where $x = c^{-1}(d(a-1)+b)$; by choosing appropriate appropriate c and d we can realize <u>any</u> x in the above form <u>provided that</u> not both $a = 1$ and $b \neq 0$. Thus, if $T_{a,b} \neq T_{1,0}$ the identity map, then the conjugacy class of $T_{a,b} = \{T_{a,x} \mid \text{all } x\}$.

21. The dihedral group of order 8 is the group generated by f and h where $f^2 = h^4 = e$ and $fh = h^{-1}f$ ($\neq hf$). A computation shows that there are 4 conjugacy classes, namely $cl(e) = \{e\}$, $cl(h) = \{h,h^{-1}\}$, $cl(h^2) = \{h^2\}$, $cl(f) = \{f,h^2f\}$, and $cl(fh) = \{fh,hf\}$.

24. If p is a prime of the form $4n + 3$ then U_p is a group of order $p - 1 = 4n + 2$ so its order is not divisible by 4. However, if $a^2 \equiv -1 \bmod p$ then [a] has order 4 in U_p, which would force 4 to divide $|U_p|$, a contradiction. So there is no such a.

Middle-Level Problems.

27. Suppose that $aH = bH$ forces $Ha = Hb$; but if h is in H then $aH = ahH$, thus $Ha = Hah$, and so $H = Haha^{-1}$, that is, $aha^{-1} \in H$ for all $h \in H$ and all $a \in G$. Thus $aHa^{-1} \subset H$ for all a in G; by Problem 29 of Section 3 we get that $aHa^{-1} = H$ for all a in G.

28. Let G be a cyclic group of order n and a a generator of G. When is $b = a^i$ also a generator of G, that is, when is b of order n? If $(i,n) = d \neq 1$ then $b^{n/d} = (a^i)^{n/d} = e$ since $d \mid i$. On the other hand, if $(i,n) = 1$ then if $b^k = a^{ik} = e$ then $n \mid ik$ (see Problem 31 below); because $(i,n) = 1$ we must

have that $n \mid k$, hence $k \geq n$, and so $k = n$. Thus a^i has order n if and only if i and n are relatively prime (and $0 < i \leq n$); thus the number of generators of G equals the number of positive integers less than n and relatively prime to n, that is, $\varphi(n)$.

29. Suppose that $aba^{-1} = b^l$. Then $a^2ba^{-2} = a(aba^{-1})a^{-1} = ab^la^{-1} = (aba^{-1})^l = (b^l)^l = b^m$ where $m = l^2$. Continue in this way, or use induction, to prove that $a^rba^{-r} = b^k$ where $k = l^r$.

32. Suppose that $o(a) = qf(a) + r$ where $0 \leq r < f(a)$; then $e = a^{o(a)} = a^{qf(a)+r} = a^{qf(a)}a^r$, hence $a^r = (a^{f(a)})^{-q}$ so is in H since $a^{f(a)}$ is in H. Because $r < f(a)$, by our definition of $f(a)$ we must have $r = 0$. Thus $o(a) = qf(a)$ hence $f(a) \mid o(a)$.

33. Suppose that $H = \{g \in A(S) \mid g(s) = s\}$; H is a subgroup of $A(S)$ and by assumption $f^j(s) = s$, that is, $f^j \in H$. By the result of Problem 32, j must divide $o(f) = p$, since p is a prime and $1 \leq j < p$ we get that $j = 1$, that is, $f \in H$. Thus $f(s) = s$.

35. The orbits of the elements of S under f are the equivalence classes of an equivalence relation so are equal or disjoint. If f has order p and $f(s) \neq s$ for every s in S then each such orbit has p elements by the result of Problem 34. But then $n = kp$ where k is the number of distinct orbits under f. This says that $p \mid n$, contrary to $(n,p) = 1$.

Harder Problems.

36. Let $m = a^n - 1$ and consider U_m, the positive integers less than m and relatively prime to m. Thus $|U_m| = \varphi(m) = \varphi(a^n - 1)$. Since a is relatively prime to $a^n - 1$, $[a]$ is in U_m; moreover, $[a]^n = [1]$ and $[a]^j \neq [1]$ for $0 < j < n$.

Thus $o([a]) = n$ hence $n \mid |U_m| = \varphi(a^n - 1)$.

38. Every element of G has order m, for some divisor m of n, and for every such divisor m of n there are $\varphi(m)$ elements of order m Thus in forming $\Sigma\varphi(m)$ over all the divisors of n we account for each element of G once and only once. Thus $n = \Sigma\varphi(m)$ where m runs over all divisors of n.

39. Let $\psi(d)$ be the number of elements of order d in G, where d is a divisor of $n = |G|$. If G has no elements of order d then $\psi(d) = 0$. If G does have an element a of order d then $e, a^{n/d}, a^{2n/d}, \ldots, a^{(d-1)n/d}$ are d distinct elements in G satisfying $x^d = e$, thus by hypothesis, these are all the elements satisfying $x^d = e$. Of these only $\varphi(d)$ have order d, namely the $a^{kn/d}$ where $(k,d) = 1$. Thus if a has an element of order d it must have $\varphi(d)$ elements of order d, thus $\psi(d) = \varphi(d)$ in this case. Thus for all divisors d of $n = |G|$, $\psi(d) \leq \varphi(d)$. However, every element of G has order d for some divisor d of n thus in forming $\Sigma\psi(d)$, where this sum runs over the divisors of n, accounts for every element of G once and only once. Thus $\Sigma\psi(d) = n$. However $\psi(d) \leq \varphi(d)$ and $n = \Sigma\psi(d) \leq \Sigma\varphi(d) = n$ (by Problem 38) where these sums run over all divisors of n. The upshot of all this is that $\psi(d) = \varphi(d)$ for all d dividing n. Thus $\psi(n) = \varphi(n) \neq 0$. But this says that G has an element of order $n = |G|$. Thus G is cyclic. Note that we did **not** use that G was abelian in the argument, thus the result holds for **all** finite groups.

40. Let p be a prime and consider the group U_p. We will show that for any integer $d \geq 1$ the number of solutions of $x^d = [1]$ in U_p is at most d. The most natural way to go about this is to show that any polynomial of degree d with coefficients in Z_p has at most d roots in Z_p. However these things are officially studied in Chapters 4 and 5, so we do it from scratch here. We prove by induction: the number of $[u]$ in Z_p such that u satisfies the

relation $q(x) = x^d + a_1x^{d-1} + a_2x^{d-1} + \ldots + a_d \equiv 0 \bmod p$, where the a_i are integers, is at most d.

If $d = 1$ then $q(x) = x + a_1$ and the only solution of this in Z_p is $u = [-a_1]$. So the result is correct in this case.

Suppose that for a given k we know that such a congruence has at most k solutions in Z_p. Consider $q(x) = x^{k+1} + a_1x^k + \ldots + a_{k+1}$; if no integer u satisfies $u^{k+1} + a_1u^k + \ldots + a_{k+1} \equiv 0 \bmod p$, then the assertion we are trying to prove is trivially true. Suppose, then, that the integer u satisfies $q(u) = u^{k+1} + a_1u^k + \ldots + a_{k+1} \equiv 0 \bmod p$. However, since $q(x) - q(u) = (x^{k+1} - u^{k+1}) + a_1(x^k - u^k) + \ldots + a_k(x - u)$, and since, for any integer $i \geq 0$, $x^i - u^i = (x - u)(x^{i-1} + x^{i-2}u + x^{i-3}u^2 + \ldots + xu^{i-2} + u^{i-1})$ (check this!) we obtain that $q(x) - q(u) = (x - u)t(x) = (x - u)(x^k + b_1x^{k-1} + \ldots + b_k)$, where the b_i are integers and where $t(x) = x^k + b_1x^{k-1} + \ldots + b_k$. Thus if v is such that $q(v) \equiv 0 \bmod p$ and $[v] \neq [u]$, then $(v - u)t(v) = q(v) \equiv 0 \bmod p$, which tells us that $p \mid (v - u)t(v)$. However $[v] \neq [u]$, thus p does not divide $v - u$; in consequence, $p \mid t(v)$, hence $t(v) \equiv 0 \bmod p$. So the v's that satisfy $q(v) \equiv 0 \bmod p$ and are such that $[v] \neq [u]$ must satisfy $t(v) \equiv 0 \bmod p$. By the form of t(x) and the induction hypothesis there are at most k such [v]. These, together with [u], then give us all the solutions of $q(r) \equiv 0 \bmod p$, thus their number is at most $k + 1$. This completes the induction and thus proves our claim.

The relation $x^d = [1]$ in U_p thus has at most d solutions in Z_p and so, by the result of Problem 39, U_p is a cyclic group.

42. Wilson's Theorem (Problem 28) states that $(p-1)! \equiv -1 \bmod p$. Thus

$1\cdot2\cdots(p-1)/2\cdot(p+1)/2\cdots(p-1) = (p-1)! \equiv -1 \bmod p$. If $y = 1\cdot2\cdots(p-1)/2$ then, since $p-1 \equiv -1 \bmod p$, $p-2 \equiv -2 \bmod p$, ..., $(p+1)/2 \equiv (p-1)/2 \bmod p$ we get $z = (p+1)/2\cdots(p-1) \equiv (-1)^{(p-1)/2}1\cdot2\cdots(p-1)/2 \equiv (-1)^{(p-1)/2}y \bmod p$. Thus $-1 \equiv (p-1)! \equiv yz \equiv (-1)^{(p-1)/2}y^2 \bmod p$. If $p = 4n+1$ then $(p-1)/2 = 2n$ is even, hence $(-1)^{(p-1)/2} = 1$. The net result of this is that $y^2 \equiv -1 \bmod p$.

43. (a). We saw in Problem 16 that $a_1a_2\cdots a_n$ is the product of those elements of G which are their own inverses. Since e and b are the only elements of G with this property, we have that $a_1a_2\cdots a_n = eb = b$.

(b). Let $b \neq e$ and $c \neq e$, $b \neq c$, be such that $b^2 = c^2 = e$; then $(bc)^2 = b^2c^2 = e$. Thus any such pair b, c gives rise to the triple b, c, bc of elements which are their own inverses. Morever, $bc(bc) = b^2c^2 = e$. In the product $a_1a_2\cdots a_n$, which reduces to the product of the elements of G which are their own inverses, every pair b, c with $b^2 = c^2 = e$ gives rise to the triple a, b, bc such that $bc(bc) = e$. Thus $a_1a_2\cdots a_n =$ e

(c). If $n = |G|$ is odd, by Part (a), we have $x = e$, since $x^2 = e$.

SECTION 5.

Easier Problems.

1. (a). The mapping φ is a homomorphism of G onto G' since $\varphi(a + b) = [a + b] = [a] + [b] = \varphi([a]) + \varphi([b])$. It is not 1-1 since, for instance, $\varphi(1) = \varphi(n + 1) = [1]$.

(b). In any group G, $(ab)^{-1} = b^{-1}a^{-1}$ thus $\varphi(a) = a^{-1}$ for a in G satisfies $\varphi(ab) = \varphi(b)\varphi(a)$. Thus φ is not a homomorphism. Such a map is called an anti-homomorphism.

(c). If G is abelian then the mapping in Part (b) is a homomorphism since $\varphi(ab) = \varphi(b)\varphi(a) = \varphi(a)\varphi(b)$. Moreover it is onto, for, given a in G,

then $a = (a^{-1})^{-1} = \varphi(a^{-1})$. It is also 1-1, for if $\varphi(a) = \varphi(b)$ then $a^{-1} = b^{-1}$ so $a = b$.

(d). That φ is a homomorphism is a consequence of: positive times positive is positive, negative times negative is positive, and negative times positive is negative in the real numbers. The mapping φ is onto since $\varphi(1) = 1$ and $\varphi(-1) = -1$. It is not 1-1; for instance $\varphi(2) = \varphi(26.51) = 1$.

(e). Since G is abelian, $(ab)^n = a^n b^n$ for all a, b in G. Thus $\varphi(ab) = \varphi(a)\varphi(b)$. Whether or not it is onto or 1-1 depends on G and n. For instance, if G is a cyclic group of order $n > 1$ then $\varphi(a) = e$ for all a in G, hence in this case φ is neither 1-1 nor onto. If G is a cyclic group of order 3 and $n = 2$ then, as is easily checked, φ is both 1-1 and onto.

$f^{-1}(x)f^{-1}(y)$; therefore f^{-1} is an isomorphism of G_2 onto G_1, thus $G_2 \cong G_1$.

3. (a). Given x in G then $x = (xa)a^{-1}$, so $x = L_a(xa)$, hence L_a is onto. Moreover, if $L_a(x) = L_a(y)$ then $xa^{-1} = ya^{-1}$ so that $x = y$. Thus L_a is 1-1. Therefore $L_a \in A(G)$.

(b). If x is in G then $(L_aL_b)(x) = L_a(L_b(x) = L_a(xb^{-1}) = (xb^{-1})a^{-1} = x(b^{-1}a^{-1}) = x(ab)^{-1} = L_{ab}(x)$; thus $L_{ab} = L_aL_b$.

(c). $\Psi(ab) = L_{ab} = L_aL_b = \Psi(a)\Psi(b)$, by Part(b). If $\Psi(a) = \Psi(b)$ then $L_a = L_b$ hence $a^{-1} = L_a(e) = L_b(e) = b^{-1}$, thus $a = b$. So Ψ is a monomorphism of G into A(G).

5. Suppose that $V \in G$ satisfies $VT_a = T_aV$ for all a in G. Let $c = V(e)$; then $(VT_x)(e) = V(T_x(e)) = V(x)$ for all x in G. Also $(T_xV)(e) = T_x(V(e)) =$

$T_x(c) = xc$. Since $VT_x = T_xV$ for all x in G we get that $V(x) = xc = L_d(x)$ where $d = c^{-1}$. Thus $V = L_d$.

6. Let $\varphi(G)$ be the image of G in G'; if x, y are in $\varphi(G)$ then $x = \varphi(a)$ and $y = \varphi(b)$ for some a, b in G, hence $xy = \varphi(a)\varphi(b) = \varphi(ab)$ so is in $\varphi(G)$, as is $\varphi(a)^{-1} = \varphi(a^{-1})$ in $\varphi(G)$. Thus $\varphi(G)$ is a subgroup of G'.

8. Define f from G to G' by $f(a) = 2^a$; then $f(a + b) = 2^{a+b} = 2^a2^b = f(a)f(b)$ so that f is a homomorphism of G into G'. It is 1-1 because $2^a = 2^b$ implies that a = b. Finally, if $c = \log_2(a)$ then $f(c) = 2^c = a$; therefore f is onto G'.

10. Computing, $fgf^{-1} = fgf = g^{-1}ff = g^{-1} = g^3$, $(fg^i)g(fg^i)^{-1} = fg^igg^{-i}f^{-1} = fgf^{-1} = g^3$, and $g^jgg^{-j} = g$ are all in H. So aga^{-1} is in H for all a in G; thus $(aga^{-1}) = ag^ia^{-1}$ is also in H for every i. Hence H is a normal subgroup of G.

13. We already know that φ is a homomorphism of G into itself by (e) of Problem 1. The kernel of φ is the set of all the elements a in G such that $a^m = e$. Thus this kernel consists of e alone only if $a^m = e$ forces a = e. This happens if and only if m and n are relatively prime.

16. This problem occurred as Problem 28 in Section 3; see the solution there.

21. Let s, t, and v be 3 distinct elements of S. There exists an f in A(S) such that f(s) = s and f(t) = v; also there exists a g in A(S) such that g(s) = t. Thus $(g^{-1}fg)(s) = g^{-1}(f(g(s))) = g^{-1}(f(t)) = g^{-1}(v) \neq s$ because $g^{-1}(t) = s$. Thus, although f is in H(S), $g^{-1}fg$ is not in H(S); thus H(S) cannot be normal in G.

24. (a). G is clearly closed under the product. Also (e_1,e_2), where e_1 is the unit element of G_1 and e_2 that of G_2 is the unit element of G since $(g_1,g_2)(e_1,e_2) = (g_1e_1,g_2e_2) = (g_1,g_2)$, and, similarly $(e_1,e_2)(g_1g_2) =$

(g_1,g_2). A similar verification shows that (g_1^{-1},g_2^{-1}) acts as the inverse of (g_1,g_2). The associative law easily checks out as a consequence of the fact that the associative law holdsin G_1 and G_2. Thus G is a group.

(b). The mapping φ_1 defined by $\varphi_1(a_1) = (a_1,e_2)$ is 1-1. Also $\varphi_1(a_1a_2)$ $= (a_1a_2,e_2) = (a_1,e_2)(a_2,e_2) = \varphi_1(a_1)\varphi_1(a_2)$, hence φ_1 is a homomorphism, thus is a monomorphism.

(c). Trivially the similar argument works for G_2.

(d). Given (a_1,a_2) in G then $(a_1,a_2) = (a_1,e_2)(e_1,a_2)$, and (a_1,e_2) is in $\varphi_1(G_1)$ and (e_1,a_2) is in $\varphi_2(G_2)$. If (a_1,a_2) is in $\varphi_1(G_1) \cap \varphi_2(G_2)$ then $a_1 = e_1$ and $a_2 = e_2$, so this intersection consists of the identity element of G.

Middle-Level Problems.

26. (a). If a, b are in G then, for all g in G, $(\sigma_a\sigma_b)(g) = \sigma_a(bgb^{-1})$ $=a(bgb^{-1})a^{-1} = (ab)g(ab)^{-1} = \sigma_{ab}(g)$. Therefore $\sigma_{ab} = \sigma_a\sigma_b$, whence $\psi(ab) = \sigma_{ab} = \sigma_a\sigma_b = \psi(a)\psi(b)$, so ψ is a homomorphism of G into A(G).

(b). If $z \in Z(G)$ then $\sigma_z(g) = zgz^{-1} = g$ for all g in G; thus σ_z is the identity mapping on G, hence z is in Ker ψ. Therefore $Z(G) \subset$ Ker ψ. For the other direction note that if $a \in$ Ker ψ then $\sigma_a = \psi(a)$ = identity mapping on G, hence $g = \sigma_a(g) = aga^{-1}$, from which we get that $ga = ag$ for all g in G. This puts a in Z(G). Therefore Ker $\psi \subset Z(G)$. Thus we get that $Z(G) =$ Ker ψ.

27. If g is in G the, since θ is onto, $g = \theta(a)$ for some a in G. Thus $g^{-1}\theta(N)g$ $= \theta(a)^{-1}\theta(N)\theta(a) = \theta(a^{-1})\theta(N)\theta(a) = \theta(a^{-1}Na) \subset \theta(N)$, since N is normal in G.

Thus $\theta(N)$ is normal in G. (the result is also a consequence of the result in Problem 15).

29. (a). The mapping σ_a defined by $\sigma_a(x) = a^{-1}xa$ is an automorphism of G, thus if M is a characteristic subgroup of G then $a^{-1}Ma = \sigma_a(M) \subset M$ for all a in G. Thus M is normal in G.

(b). Since M and N are normal in G we already know that MN is a (normal) subgroup of G. If φ is an automorphism of G then, since $\varphi(M) \subset M$ and $\varphi(N) \subset N$, we get that $\varphi(MN) = \varphi(M)\varphi(N) \subset MN$. Thus MN is a characteristic subgroup of G.

(c). Let G be the group of order 4 having the elements e, a, b, ab where $a^2 = b^2 = e$, and where ab = ba. Since the group G is abelian, every subgroup of G is normal in G; thus A = {e,a} is a normal subgroup of G. The mapping φ defined on G by $\varphi(e) = e$, $\varphi(a) = b$, $\varphi(b) = a$, and $\varphi(ab) = ab$ can be seen to be an automorphism of G. But $\varphi(A) = \{e,b\}$ is not contained in A. Thus A is not a characteristic subgroup of G.

30. Since H is of order p and is normal in G, if φ is an automorphism of G and if $\varphi(H) \neq H$ then $H\varphi(H)$ is a subgroup of G and is of order p^2. (See Problem 16 to see that $H\varphi(H)$ is a subgroup of G; to see why it has order p^2 see the argument given in Problem 22 of Section 3). Thus $p^2 = |H\varphi(H)|$ must divide $|G| = pm$, by Lagrange's Theorem. Thus $p^2 \mid pm$, and so $p \mid m$, contrary to assumption. Thus H is a characteristic subgroup of G.

33. If N is normal in G then, for a in G, σ_a defined by $\sigma_a(x) = a^{-1}xa$ is an automorphism of G and $\sigma_a(N) \subset N$ since N is normal in G. Thus σ_a induces (gives rise to) an automorphism of N, hence takes M into itself because M is a characteristic subgroup of N. Which is to say $\sigma_a(M) = a^{-1}Ma \subset M$ for all a in G. Thus M is normal in G.

34. Let θ be an automorphism of G and consider σ_a, the automorphism of G defined by $\sigma_a(x) = a^{-1}xa$ for all x in G. Then $(\theta\sigma_a\theta^{-1})(x) = \theta(\sigma_a(\theta^{-1}(x)) = \theta(a^{-1}\theta^{-1}(x)a) = \theta(a)^{-1}x\theta(a) = \sigma_{\theta(a)}(x)$, hence $\theta\sigma\theta^{-1} = \sigma_{\theta(a)}$ so is in I(G). Thus I(G) is normal in $\mathcal{A}(G)$.

Harder Problems.

37. Let G be a non-abelian group of order 6. If every element were of order 2 then, by Problem 9 of Section 1, G would be abelian. Also, if there were an element of order 6 in G then G would be cyclic. Since G is of even order it has an element $a \neq e$ such that $a^2 = e$. If $b \neq e$ in G is of not of order 2, by what we said above and Lagrange's Theorem, b has order 3. By the result of Problem 30 the subgroup $B = (e, b, b^2)$ is normal in G. Now, since G is non-abelian, $ab \neq ba$, yet aba^{-1} is in B since B is normal in G. Thus $aba^{-1} = b^{-1}$. Since $a^2 = b^3 = e$ and $ab = b^{-1}a$ the mapping of G onto S_3 which sends a to f and b to g, where $f^2 = g^3 = e$ and $fg = g^{-1}f$ gives an isomorphism of G onto S_3.

38. (a). $(T_bT_c)(Ha) = T_b(T_c(Ha)) = T_b(Hac^{-1}) = Hac^{-1}b^{-1} = Ha(bc)^{-1} = T_{bc}(Ha)$ for every a in G. Thus $T_{bc} = T_bT_c$.

(b). Suppose u is in $K(\psi)$; thus $T_u = \psi(u) = i_S$. Thus, for every a in G, $Hau = T_u(Ha) = Ha$, and so $Haua^{-1} = Ha$. Therefore aua^{-1} is in H for every a in G. Conversely, if aua^{-1} is in H for every a in G the argument reverses to show that $T_u = \psi(u) = i_S$. Thus $K(\psi) = \{u \in G \mid aua^{-1} \in H \text{ for every a in G}\}$. This tells us that if u is in $K(\psi)$ then u is in every $a^{-1}Ha$; from this we get that $K(\psi)$ is the intersection of all $a^{-1}Ha$ as a runs over G.

(c). $K(\psi)$ is a normal subgroup of G, being the kernel of a homomorphism of G, and lies in H since aua^{-1} is in H for every a in G, so in particular, for $a = e$. Thus $K(\psi) \subset H$. Suppose that $N \subset H$ is a normal subgroup of G; then $aNa^{-1} \subset N \subset H$, hence $N \subset K(\psi)$.

40. Suppose that H is a subgroup of G, $|G| = n$, and that n does not divide $i_G(H)!$. If S is as in Problem 38, A(S) has elements has $i_G(H)!$ elements, so, by Lagrange's Theorem, has no subgroup of order n. Thus the mapping ψ of Problem 38 cannot be an isomorphism. Therefore $K(\psi) \neq (e)$ is a normal subgroup of G contained in H.

41. If $|G| = 21$ and H is a subgroup of order 7, then $i_G(H) = 3$, and since 7 does not divide $3! = 6$, H contains a normal subgroup $N \neq (e)$ of G. But, since the only subgroup of H which is different from (e) is H itself, we conclude that $N = H$. Hence H is normal in G.

43., 44., and 45. Let G be a group of order p^2 where p is a prime. If G is cyclic then we are done, for then G is abelian. So if $a \neq e$ is in G then $o(a) = p$, and the subgroup $A = (a)$ is of order p. Thus $i_G(A) = p^2/p = p$, and p^2 doe not divide p!, G has a normal subgroup $T \neq (e)$ contained in A. Hence $T = A$ and A is normal in G. So if b is in G then $bab^{-1} = a^i$ since A is normal and generated by a. From this, since $b^p = e$, we get that $a = b^p ab^{-p} = a^m$ where $m = i^p$. (See Problem 29 of Section 4 for the kind of argument needed for this last step). Since $a^{m-1} = e$ and a is of order p, p must divide $m - 1 = i^p - 1$; however by Fermat's theorem, $i^p \equiv i \bmod p$. The outcome of all this is that $i \equiv 1 \bmod p$. Hence $a^i = a$ and so $bab^{-1} = a$, that is $ab = ba$ for all b in G. This argument held for any $a \neq e$ in G. Thus all elements of G are in Z(G). So G is abelian. Note, for Problem 44, that if G is cyclic and generated by a then a^p generates a subgroup of order p; if G is not cyclic

then every $a \neq e$ in G is of order p, so generates a subgroup of order p. At any rate, G must have a subgroup of order p, and it is normal since G is abelian. If G is of order 9 then $p = 3$, and G is abelian.

46. If G is cyclic with a as generator then a^3 has order 5 and a^5 has order 3, and we would be done. So suppose that G is not cyclic. Every non-identity element has order a divisor of 15, so has order 3 or 5. Suppose that there aren't elements of both orders 3 and 5. So every element has order 5 or every element has order 3. If a and b are of order 5 and b is not a^i for any i, then the elements $a^j b^k$, where j, k take on all values between 0 and 4 give us 25 distinct elements-- far too many for G which only has 15 elements.

Suppose then that every element in G other than e has order 3. If $a \neq e$ is in G and $ba = ab$ we claim that $b = a^i$ for some i. If not, since the subgroups $B = (b)$ and $A = (a)$ satisfy $AB = BA$, AB is a subgroup of G of order 9, and since 9 does not divide 15 this is not possible. Suppose that c is not in A; thus the 3 elements c, aca^{-1}, $a^2ca^{-2} = a^{-1}ca$ are distinct, so c gives rise to a triple of distinct elements in this way. If d is not e nor any of c, aca^{-1}, $a^{-1}ca$ then d, ada^{-1}, $a^{-1}da$ give us 3 <u>new</u> elements. For, if ada^{-1}, say, is one of these earlier elements then $ada^{-1} = a^lca^{-1}$, leading to the contradiction that $d = a^{l-1}ca^{-(l-1)}$. Continue this way to get k distinct triples. These together with e exhaust G so the number of elements in G is $3k + 1 = 15$, which implies that $3 \mid 14$ which is false. So not every element of G can have order 3.

Very Hard Problems.

49. We first show that if $i_G(A)$ and $i_G(B)$ are finite for the subgroups A and B of G then $i_G(A \cap B)$ is also finite. Let $Au_1, Au_2, \ldots, Au_m$ be all the

distinct left cosets of A in G, and $Bv_1, Bv_2, \ldots, Bv_n$ those of B in G. Since $A \cap B$ is a subgroup of B, B is the (possibly infinite) union of left cosets $(A \cap B)w_r$ where the w_r are in B. We claim that there are at most m distinct left cosets of $A \cap B$ in B. For suppose $w_1, \ldots, w_{m+1}$ give us m+1 such distinct cosets. Since G is the union of the Au_i each $w_k = a_k u_i$ where the a_k are in A. Since the number of u_i is m, we must have that for two different k, q the same i appears for w_k and w_q; that is $w_k = a_k u_i$ and $w_q = a_q u_i$. But these imply that $w_k w_q^{-1} = a_k a_q^{-1}$ so is in A; but $w_k w_q^{-1}$ is in B since each of w_k and w_q is. Thus $w_k w_q^{-1}$ is in $A \cap B$, contrary to the fact that they give distinct left cosets of $A \cap B$ in B. Thus B is the union of at most m left cosets $(A \cap B)w_r$, hence Bv_j is the union of $(A \cap B)w_r v_j$, and so G is the union of the $(A \cap B)w_r v_j$, which are at most mn in number. Thus $i_G(A \cap B)$ is finite.

By induction we easily then get that if $G_1, G_2, \ldots, G_s$ are of finite index in G then $A_1 \cap A_2 \cap \ldots \cap A_s$ is of finite index in G. If H is of finite index in G we claim that there are only a finite number of distinct $a^{-1}Ha$ in G. By the result of Problem 19, $N(H) = \{a \in G \mid a^{-1}Ha = H\}$ is a subgroup of G and contains H, so is of of finite index in G; in fact $i_G(N(H)) \leq i_G(H)$. Also the number of distinct $a^{-1}Ha$ equals $i_G(N(H))$ (Prove!). Hence there are only a finite number of distinct $a^{-1}Ha$ in G. Each of these is of finite index in G (Prove!), so their intersection N is of finite in G. By Problem 18, N is normal in G.

50. Let a and b be such that $a^2 = b^2 = e$ and $a \neq e \neq b$, and $a \neq b$, and

ab = ba. The group, N, they generate {e, a, b, ab} is abelian, hence all its subgroups are normal. Let G be generated by a, b, and g where $g^2 = e$, ga = bg, gb = ag, and gab = abg. Then N is normal in G but M = {e,a} which is normal in N is not normal in G, for $gag^{-1} = b$ is not in M.

51. Let f be the mapping defined by $f(x) = \varphi(x)x^{-1}$; if f(x) = f(y) then $\varphi(x)x^{-1} = \varphi(y)y^{-1}$, so $x^{-1}y = \varphi(x)^{-1}\varphi(y) = \varphi(x^{-1}y)$. By our hypothesis on φ we must have $x^{-1}y = e$ and so x = y. Thus f is 1-1, hence maps G onto itself. Therefore, given a in G, then $a = \varphi(x)x^{-1}$ for some x in G; thus $\varphi(a) = \varphi^2(x)\varphi(x^{-1}) = x\varphi(x)^{-1} = a^{-1}$, since φ^2 is the identity automorphim of G. Thus $b^{-1}a^{-1} = (ab)^{-1} = \varphi(ab) = \varphi(a)\varphi(b) = a^{-1}b^{-1}$, whence G is abelian.

52. Let $A = \{a \in G \mid \varphi(a) = a^{-1}\}$, and suppose that $b \notin A$. Thus both A and Ab have more than 3/4 of the elements of G, hence $A \cap Ab$ has more than half the elements of G. If x is in $A \cap Ab$ then x = ab, where a is also in A, and $\varphi(x) = x^{-1} = b^{-1}a^{-1}$ But $\varphi(x) = \varphi(a)\varphi(b) = a^{-1}b^{-1}$; consequently ab = ba follows. So whenever ab is in A we must have that ab = ba. The number of such a is more than half the elements in G, so the subgroup $C(b) = \{x \in B \mid xb = bx\}$ has order greater than |G|/2 yet divides |G| by Lagrange's Theorem. Hence C(b) = G. So $b \in Z(G)$; thus $A \subset Z(G)$. Therefore Z(G) has order larger than 3|G|/4, so must be all of G. Therefore G is abelian. Because G is abelian, A becomes a subgroup of G, and since its order is larger than 3|G|/4, A = G. Thus $\varphi(x) = x^{-1}$ for all x in G.

SECTION 6.

2. If a is a real number identify Na with |a|; since the cosets of N in G multiply via NaNb = Nab which jibes with the fact that |ab| = |a||b|.

4. If g is in G then, since M is normal in G/N, if X = Ng then $X^{-1}MX \subset M$; this gives us that $Ng^{-1}Mg \subset M$, and so $g^{-1}Mg \subset M$. Thus M is normal in G.

6. Every point in the plane has a mate in the unit square where $0 \leq x \leq 1$ and $0 \leq y \leq 1$. So G/Z is the set of points in this unit square where the left hand edge and the right hand edge of this square are identified, and the top edge and bottom edge are identified. Identifying the side edges means folding this square around so that these edges become identical; this gives us a cylinder. Identifying the top edge with the bottom one identifies the top surface of this cylinder with its bottom surface. So we are bending this cylinder around to glue the bottom surface to the top one. Thus we get a torus.

7. If G is cyclic and generated by a then every element x in G is of the form a^l. Every element Nx in G/N is then of the form $Nx = Na^l = (Na)^l$. Thus G/N is cyclic with Na as generator.

10. By Cauchy's Theorem there exists an element $a \neq e$ of order $p = p_i$; let P_i be the set of elements of G of order some power of p. By Problem 11 of Section 3, P_i is a subgroup of G. By Cauchy's Theorem $|P_i| = p^m$ for some m. We claim that $m = a_i$; certainly $m \leq a_i$ since p^m, as the order of P_i, must divide $|G| = p_1^{a_1} \ldots p_k^{a_k}$. Suppose that $m < a_i$; then $|G/P_i| = |G|/|P_i|$ is divisible by p, so, by Cauchy's Theorem has an element $P_i g \neq P_i$ satisfying $(P_i g)^p = P_i$, hence $P_i g^p = P_i$, and thus g^p is in P_i and g is not in P_i. Therefore $(g^p)^{|P_i|} = e$, and since $|P_i| = p^m$ we have that $g^k = e$ where $k = p^{m+1}$. But this puts g in P_i, contrary to assumption. Thus $m = a_i$ and P_i is the sought-after subgroup S_i of order $p_i^{a_i}$.

11. If G/Z(G) is cyclic, suppose that Z(G)a is a cyclic generator of G/Z(G). Thus, for any g in G, $Z(G)g = (Z(G)a)^i = Z(G)a^i$ for some i. This tells us that

$g = za^i$ for some z in $Z(G)$. If h is in G then $h = z'a^j$ for some integer j and some z' in $Z(G)$. Thus $gh = za^iz'a^j = a^{i+j}zz' = z'a^jza^i = hg$ because both z and z' are in $Z(G)$. Thus $G/Z(G)$ is abelian.

13. If $aba^{-1}b^{-1}$ is in N for all a, b in G then $Naba^{-1}b^{-1} = N$, from which we get that $Nab = Nba$. But $NaNb = Nab = Nba = NbNa$; thus G/N is abelian.

14. By the result of Problem 15, if a of order m and b of order n are in the abelian group G then ab is of order mn. By induction this easily extends to : if a_i is of order m_i, for $1 \leq i \leq r$ and for all $i \neq j$ we know that m_i and m_j are relatively prime, then $c = a_1a_2...a_r$ is of order $m_1m_2...m_r$. By Cauchy's theorem, the group G of order $p_1...p_k$, where the p_i are distinct primes, has elements a_i of order p_i for each $1 \leq i \leq k$. By the remark above, $c = a_1...a_k$ is of order $p_1...p_k = |G|$. Thus G is cyclic.

15. Let $A = (a)$ and $B = (b)$ where a is of order m and b is of order n, where m and n are relatively prime. $|A \cap B|$, as a subgroup of both A and B, must divide both $m = |A|$ and $n = |B|$; because m and n are relatively prime we get that $|A \cap B| = 1$, hence $A \cap B = (e)$. If $c = ab$ and $a^sb^s = (ab)^s = c^s = e$ then $a^s = b^{-s}$ is in $A \cap B = (e)$, hence $a^s = e$ and $b^{-s} = e$ (so $b^s = e$). Therefore $m = o(a) \mid s$ and $n = o(b) \mid n$, and since m and n are relatively prime, $mn \mid s$, hence $s \geq mn$. But $(ab)^{mn} = a^{mn}b^{mn} = e$. Thus mn is the smallest positive integer k such that $a^k = e$, whence $o(ab) = mn$.

17. (a). By Problem 11 of Section 3, M is a subgroup of G.

(b). Suppose that $(Mx)^m = M$ in G/M; thus x^m is in M. On the other hand, since $x^n = x^{|G|} = e$, $(Mx)^n = Me = M$, hence x^n is in M. Since m and n are relatively prime, $um + vn = 1$ for some integers u and v. Thus $x = x^{um+vn} = x^{um}x^{vn}$ is in M since both x^m and x^n are in M. Hence $Mx = M$, the identity element of G/M.

SECTION 7.

1. If a is in N then $\psi(a) = N'\varphi(a) = N'$ since $\varphi(a) \in N'$ by the definition of N. Hence $a \in \text{Ker } \psi = M$. Therefore $N \subset M$.

2 Let ψ be defined from G to the real numbers $\mathbf{R}$ under + by the rule $\psi(f(x)) = f(1/4)$. The mapping ψ is a homomorphism of G into $\mathbf{R}$ because $\psi(f(x) + g(x)) = f(1/4) + g(1/4) = \psi(f(x)) + \psi(g(x))$ for f and g in G. Since the function $h(x) = r$ is in G for any real number r, and $\psi(h(x)) = h(1/4) = r$, we get that ψ is onto $\mathbf{R}$. Finally, what is Ker ψ ? We know that $\psi(f(x)) = 0$ if and only if $f(1/4) = 0$; thus Ker $\psi = N$. By the First Homomorphism Theorem we get that $\mathbf{R} \cong G/N$.

3. Define the mapping f of G onto the positive reals by $f(r) = |r|$ for every non-zero real number. Clearly f is a homomorphism since $f(rs) = |r||s| = f(r)f(s)$. Also Ker $f = \{r \mid |r| = 1\}$ so Ker $f = \{1, -1\} = N$. Thus by the First Homomorphism Theorem $G/N \cong$ positive reals under multiplication.

5. (a). If $h \in H$ then $h^{-1}(H \cap N)h \subset h^{-1}Hh \subset H$ and $h^{-1}(H \cap N)h \subset h^{-1}Nh \subset N$ so $h^{-1}(H \cap N)h \subset H \cap N$; thus $H \cap N$ is normal in H.

(b). Since N is normal in G, $HN = NH$; but this is the criterion that HN be a subgroup of G.

(c). $N = eN \subset HN$, and since $g^{-1}Ng \subset N$ for all g in G, it is certainly true if g is in HN. Thus N is normal in HN.

(d). Define the mapping $f : G \to G/N$ by $f(g) = Ng$; since f is a homomorphism of G onto G/N with kernel N, if we look at $g : H \to HN/N$ defined by $g(h) = Nh$ for h in H then Ker $g = H \cap \text{Ker } f = H \cap N$, so the image of H under g is isomorphic to $H/(H \cap N)$. The image of H under g, g(H), is the normal in G'.

SECTION 8.

Middle-Level Problems.

2. If G is of order 35 then, by Cauchy's Theorem it has an element a of order 5 and an element b of order 7. If $B = (b)$ then B is a subgroup of order 7 and, for g in G, $C = gBg^{-1}$ is also a subgroup of order 7. If $B \neq C$ then BC has 49 distinct elements (Prove!), which is impossible since $|G| = 35$. Thus $gBg^{-1} = B$ for all g in G. Thus B is normal in G. Therefore, since aba^{-1} is in B, $aba^{-1} = b^i$. Therefore $b = a^5ba^{-5} = b^k$ where $k = i^5$, and so $b^{k-1} = e$. This implies that $7 \mid (i^5 - 1)$, and since, by Fermat's Theorem, $7 \mid (i^6 - 1)$ we get that $7 \mid (i - 1)$. But this says that $b^i = b$, and so $ab = ba$. But then $c = ab$ is of order $5 \cdot 7 = 35$; hence G is cyclic.

4. Let G be generated by a and b where $a^3 = b^7 = e$ and $aba^{-1} = b^2$. The 21 distinct elements b^ia^j, where $0 \leq j < 3$ and $0 \leq i < 7$, form a group for, as can be verified from the relations between a and b, $(b^ia^m)(b^ja^n) = b^ra^s$ where $r = i + 2^mj$ and $s = m + n$.

5. Suppose that $|G| = p^nm$ where p does not divide m, and suppose that P is a normal subgroup of order p^n. If θ is an automorphism of G then $Q = \theta(P)$ is a subgroup of order p^n and PQ has $|P||Q|/|P \cap Q| = p^{2n}/|P \cap Q|$ elements. Thus, if $P \neq Q$, then $|PQ| = p^s$, where $s \geq n + 1$ But p^s does not divide p^nm since p does not divide m. With this contradiction we get that $\theta(P) = P$, hence P is a characteristic subgroup of G.

6. Since $|AB| = |A||B|/|A \cap B| \leq |G|$, $|A \cap B| \geq |A||B|/|G| \geq \sqrt{|G|}\sqrt{|G|}/|G| > 1$. Thus $A \cap B \neq (e)$.

$|A \cap B| = 1$, hence AB has $|A||B| = mn$ distinct elements.

8. By Cauchy's Theorem G has an element a of order 11. Thus for the subgroup $A = (a)$ of order 11, $i_G(A) = 9$ and 11 does not divide 9!, hence, by Problem 40 of Section 5, A is a normal subgroup of G.

10. By Problem 9, G has a normal subgroup of N of order 7; thus $G_1 = G/N$ is a group of order 6. As such, G_1 has a normal subgroup T_1 of order 3. By the Second Homomorphism Theorem (Theorem 2.7.2) the subgroup $T = \{a \in G \mid Na \in T_1\}$ is a normal subgroup of G and $T/N = T_1$. Since $T_1 = |T/N| = |T|/|N|$, we get that $|T| = |T_1||N| = 3 \cdot 7 = 21$.

Harder Problems.

12. Since G is a group of order 21 it has an element a of order 7 and an element b of order 3. The subgroup $A = (a)$ of order 7 is normal in G since 7 does not divide $i_G(A)! = 3! = 6$. Therefore $bab^{-1} = a^i$. Since G is non-abelian, $i \neq 1$. But since $b^3 = e$ we get that $a = a^k$ where $k = i^3$; thus $i^3 - 1$ is divisible by 7. This gives us that $i = 2$ or 4. If $i = 2$ then $b^2ab^{-2} = a^4$, so in all circumstances G has an element c such that $cac^{-1} = a^4$. If G_1 is another non-abelian group of order 21, the same argument shows that G_1 has elements u and v such that $u^7 = v^3 = e$ and $vuv^{-1} = u^4$. Define the mapping f of G to G_1 by $f(a) = u$ and $f(c) = v$ and $f(a^ic^j) = u^iv^j$. This mapping is an isomorphism of G onto G_1.

Very Hard Problems.

13. By Cauchy's Theorem G has an element a of order 11, and since $A = (a)$ is a subgroup of order 11, $i_G(A) = 9$; because 11 does not divide 9! we have that A is a normal subgroup of G. We claim that $A \subset Z(G)$; for if g is in G then $gag^{-1} = a^i$ since it is in A, hence $g^{11}ag^{-11} = a^m$ where $m = i^{11}$. By Fermat's Theorem, $i^{11} \equiv i \bmod 11$; thus $a^m = a^i$. The net result of all this

is that $g^{11}ag^{-11} = a^i = gag^{-1}$, from which we get that $g^{10}a = ag^{10}$. Since 10 does not divide 99 = |G|, we easily get from this that ga = ag. Thus $a \in Z(G)$, hence $A = (a) \subset Z(G)$.

Also G/A is of order 9, hence is abelian. Thus if u and v are in G then $uvu^{-1}v^{-1}$ is in A (see Problem 12 in Section 6). Hence uv = zvu where z is in A, thus in Z(G), and $z^{11} = e$. Thus $u^2v = u(uv) = uzvu = zuvu = zvu^2$, since z is in Z(G). Continuing this way we get that $u^iv = z^ivu^i$. In particular, if $i = 11$, since $z^{11} = e$, we get $u^{11}v = vu^{11}$. Thus if u is of order 3 we get that $u^{11} = u^2 = u^{-1}$, so $u^{-1}v = vu^{-1}$ for all v in G. In short, u must be in Z(G). Thus Z(G) has order at least 33 since it contains an element of order 11, namely a, and an element of order 3, namely u. Thus the order of G/Z(G) is 1 or 3; at any rate, G/Z(G) is cyclic. By Problem 11 of Section 6, G must be abelian.

14. Consider the group generated by the two elements a and b where we impose the conditions that $a^p = b^q = e$ and $bab^{-1} = a^i$. What value should we assign to i in order to get consistency with the relations $a^p = b^q = e$ and to insure that the group so obtained is a non-abelian group of order pq? As we have done many times, this implies that $b^rab^{-r} = a^m$ where $m = i^r$. Thus if $r = q$, since $b^q = e$ we get $a = a^m$, and so $a^{m-1} = e$. This would require that $q \mid (m - 1) = (i^q - 1)$ and (since we want G non-abelian) q does not divide i - 1. Can we find such an r ? Yes, since U_p is a cyclic group and $q \mid (p - 1)$ there is an element $[i] \neq [1]$ in U_p such that $[i]^q = [1]$, that is, an integer i, where $1 < i < p$ such that $p \mid (i^q - 1)$ and p does not divide i - 1. Pick such an i and let G consist of the distinct elements a^ub^v where $0 \leq u \leq p-1$, and $0 \leq v \leq q-1$, which are pq in number. Motivated by the desired relations $a^p = b^q = e$ and $bab^{-1} = a^i$, we find that these elements a^ub^v multiply according to the rule $(a^ub^v)(a^rb^s) = a^tb^w$ where $w = v + s$ and

$t = u + ri^v$. Using this rule, G is clearly closed under this product, $e = a^0b^0$, and, as we can check, $(a^ub^v)^{-1} = a^rb^s$ where $s = p - v$ and $r = (p - u)i^{q-v}$ which is in G. We leave the checking of the associative law to the reader. So G is a non-abelian group of order pq.

15. Let G and G_1 be two non-abelian groups of order pq. As we saw in Problem 14, G is generated by a and b where $a^p = b^q = e$ and $bab^{-1} = a^i$ where $i^q \equiv 1 \bmod p$ and $i \not\equiv 1 \bmod p$. Similarly, G_1 is generated by two elements c and d such that $c^p = d^q = e$ and $dcd^{-1} = c^j$, where $j^q \equiv 1 \bmod p$ and $j \not\equiv 1 \bmod p$. Since [i] and [j] are of order q in U_p, $[j] = [i]^t$ for some positive integer t such that $0 < t < q$. Thus $j \equiv i^t \bmod p$, hence $b^tab^{-t} = a^m$ where $m = i^t$, and since $i^t \equiv j \bmod p$, $a^m = a^j$. If we let $h = b^t$ then $h^q = e$ and $hah^{-1} = a^j$; the mapping $f : G \to G_1$ defined by $f(a^uh^v) = c^ud^v$ is then an isomorphism of G onto G_1.

SECTION 9.

2. If m and n are relatively prime and G_1 and G_2 cyclic groups of orders m and n respectively, if a generates G_1 and b generates G_2 then the elements (a,e_2) and (e_1,b) in $G_1 \times G_2$ are of orders m and n respectively. Thus, because m and n are relatively prime, $(a,b) = (a,e_2)(e_1,b)$ is of order mn. On the other hand, if $d \neq 1$ is the greatest common divisor of m and n then the elements $(a^{mi/d}, b^{nj/d})$, where $0 \leq i,j \leq d-1$ give us d^2 solutions of the equation $x^d = (e_1,e_2)$ in $G_1 \times G_2$. But in a finite cyclic group the number of solutions of $x^d = e$ is at most d, and since $d^2 > d$, we get that (G_1,G_2) cannot be cyclic.

4. Since P_1 and P_2 are of relatively prime orders, the subgroup P_1P_2 is of order $p_1^{m}1p_2^{m}2$. Continuing by induction we get that $P_1P_2...P_k$ is of order $p_1^{m}1p_2^{m}2...p_k^{m}k = |G|$. Thus $G = P_1P_2...P_k$. Moreover every element g in G has a unique representation in the form $g = a_1a_2...a_k$ where each a_i is in P_i, because, if $a_1a_2...a_k = b_1b_2...b_k$ are two such representations of g then $b_1a_1^{-1} = b_2...b_ka_1^{-1}...a_k^{-1} = (b_2a_2^{-1})...(b_ka_k^{-1})$, so $b_1a_1^{-1}$ is in $P_2...P_k$. But, since $b_1a_1^{-1}$ is in P_1 its order is a power of p_1; the subgroup $P_2...P_k$ is of order $p_2^{m}2...p_k^{m}k$ and since p_1 does not divide $p_2^{m}2...p_k^{m}k$ we get that $b_1a_1^{-1} = e$, hence $a_1 = b_1$. Similarly we get that $a_i = b_i$ for all the i's. Thus g has a unique representation in the form $g = a_1...a_k$. By the definition of internal direct product, G is the internal direct product of $P_1, \ldots, P_k$; thus by Theorem 2.9.4, $G \cong P_1 \times P_2 \times \ldots \times P_k$

5. The order of $N_1N_2...N_k$ is at most $|N_1||N_2|...|N_k| = |G|$; if for any two different products $n_1n_2...n_k = m_1m_2...m_k$ where each of m_i and n_i are in N_i, for every i, then we cannot achieve this maximum for the number of elements in $N_1...N_k$. Thus every element of $G = N_1N_2...N_k$ has a unique representation in the form $n_1n_2...n_k$. By the definition of internal direct product and Theorem 2.9.4 we get G is the direct product of $N_1, N_2, \ldots, N_k$.

6. To show that G is the direct product of $N_1, N_2, \ldots, N_k$, given (a) and (b) we merely must show that each g in G has a unique representation in the form $g = n_1...n_k$ where each n_i is in N_i. From the hypothesis (b) we have that $N_i \cap N_j = (e)$ if $i \neq j$ since $N_j \subset N_1...N_{i-1}N_{i+1}...N_k$ and, since the N_i are

normal in G, we get that $n_i n_j = n_j n_i$ and $n_i m_j = m_j n_i$. In consequence, if $g = n_i...n_k = m_1...m_k$ where each m_i is also in N_i then we obtain that $n_i m_i^{-1} = m_1...m_{i-1}m_{i+1}...m_k n_k^{-1}...n_{i-1}^{-1}n_{i+1}^{-1}...n_1^{-1} = (m_1 n_1)...(m_k n_k^{-1})$ so $n_i m_i^{-1}$ is in $N_i \cap (N_1...N_{i-1}N_{i+1}...N_k) = (e)$. Thus $n_i = m_i$ for each i, whence g has a unique representation in the form $g = n_1...n_k$. Therefore G is the direct product of $N_1, N_2, ..., N_k$.

SECTION 11.

Earier Problems.

1. The conjugacy classes in S_3 are (e), (f,fg, gf), and (g,g^2), where f and g generate S_3, and $f^2 = g^3 = e$ and $fg = g^{-1}f$ (See Problem 19 in Section 4). Also $C(e) = S_3$, $C(f) = \{e,f\}$ and $C(g) = \{e,g,g^2\}$ so $|C(f)| = 2$ and $|C(g)| = 3$, and $|S_3|/|C(e)| = 1$, $|S_3|/|C(f)| = 2$ and $|S_3|/|C(g)| = 2$, and $1 + 2 + 3 = 6$ is the check on the class equation.

2. The dihedral goup of order 8 is generated by a and b where $a^2 = b^4 = e$ and $ab = b^{-1}a$. The conjugate classes are {e}, $\{b^2\}$, $\{b,b^3\}$, $\{a,ab^2\}$, $\{ab,ab^3\}$ and $C(e) = G$, $C(b^2) = G$, $C(b) = \{e,b,b^2,b^3\}$, $C(a) = \{e,a,ab^2,b^2\}$. Therefore $|G|/|C(e)| = 1$, $|G|/|C(b^2)| = 1$, $|G|/|C(b)| = 2$, $|G|/|C(a)| = 2$, and $|G|/|C(ab)| = 2$; thus the class equation checks out as $1 + 1 + 2 + 2 + 2 = 8$.

6. If P is normal in G and $Q \neq P$ is a p-Sylow subgroup of G of order p^n then $PQ = QP$, so PQ is a subgroup of G and $|PQ| = |P||Q|/|P \cap Q| = p^{2n}/|P \cap Q| \geq p^{n+1}$ must divide $|G|$. Since $|G| = p^n m$ whe $(m,p) = 1$, this is not possible. Thus $P = Q$ and P is the only p-Sylow subgroup of G.

8. We proceed by induction on $|G|$ to prove that if the prime p divides $|G|$ then G has an element of order p.

If $|G| = p$ the result is trivially true since every $a \neq e$ in G is of order p. Suppose that the theorem is true for all groups H such that $|H| < |G|$. Let $Z(G)$ be the center of G with $|Z(G)| = z \geq 1$. If $p \mid |H|$ for any subgroup $H \neq G$ of G then, by our induction hypothesis, H has an element of order p, and so the result is correct in this instance. So we may assume that p does not divide the order of any proper subgroup of G. Thus, if a is not in $Z(G)$ then $C(a) \neq G$ is a proper subgroup, hence p does not divide $|C(a)|$. But then p does divide $|G|/|C(a)|$. The class equation tells us that $|G| = z + \Sigma|G|/|C(a)|$ where the sum Σ runs over one element from each conjugacy class of the elements of G which are not in $Z(G)$. For each $|G|/|C(a)|$ which appears in the sum Σ we know that $p \mid |G|/|C(a)|$, hence $p \mid \Sigma|G|/|C(a)|$. Since p also divides $|G|$ we get that $p \mid z$. But we already have proved Cauchy's Theorem for abelian groups in Theorem 2.6.4. Since $Z(G)$ is an abelian group and $p \mid Z(G)|$, $Z(G)$ has an element of order p. This completes the induction and proves the theorem.

11. Since P is a p-Sylow subgroup of G and $P \subset N(P)$, P is also a p-Sylow subgroup of $N(P)$. But P is normal in $N(P)$, thus, by the result of Problem 6, P is the only p-Sylow subgroup of $N(P)$.

12. Let $|P| = p^n$. If a is of order p^m and if $a^{-1}Pa = P$ then, if $A = (a)$ we have A is of order p^m and that $AP = PA$ is a subgroup of G. But $|AP| = |A||P|/|A \cap P| = p^m|p^n/|A \cap P| = p^{m+n}/|A \cap B|$. If a is not in P then $A \cap P \neq A$, so $|A \cap P| = p^r$ where $r < m$. Thus $|AP| = p^{m+n-r}$, and since $m - r \geq 1$, the integer $m + n - r \geq n + 1$, so p^{m+n-r} does not divide $|G|$. But since AP is a subgroup of G, $|AP| = p^{m+n-r}$ must divide $|G|$. With this contradiction we obtain that a is in P.

14. Since $P \subset N(P)$, we know that $p^n = |P|$ must divide $|N(P)|$, thus $|N(P)| = p^n k$ and so $i_G(N(P)) = |G|/|N(P)| = p^n m/p^n k = m/k$, an integer; since p does not divide m we get that p does not divide $i_G(N(P))$. Since the number of distinct $x^{-1}Hx$ equals $i_G(N(P))$ we have established the result.

Middle-Level Problems.

16. Let S be the 3-Sylow subgroup of G of order 9. Thus $i_G(S) = 4$ and since 9 does not divide $4! = 24$, by the result of Problem 40 of Section 5, S contains a normal subgroup $N \neq (e)$. Since N is a subgroup of S, $|N| = 3$ or 9.

17. $|G| = 108 = 3^3 2^2$. Since the 3-Sylow T subgroup of G has order 27, $i_G(T) = 4$. By the argument used in solving Problem 40 of Section 5 there is a homomorphism ψ of G into S_4, which is of order 24, such that Ker ψ is contained in T. Thus $108/|\text{Ker } \psi| = |G|/|\text{Ker } \psi| = |G/\text{Ker } \psi| \leq 24$, hence $|\text{Ker } \psi| \geq 108/24 > 4$. Since it is a subgroup of T and $|T| = 27$, $|\text{Ker } \psi|$ is a subgroup of T, its order must divide 27. We thus have that $|\text{Ker } \psi| = 9$ or 27.

18. Let a be in N(N(P)); thus $a^{-1}N(P)a \subset N(P)$, and since $P \subset N(P)$, $a^{-1}Pa$ is contained in N(P). But then $a^{-1}Pa$ is a p-Sylow subroup of N(P). By the result of Problem 6 we know that P is the only p-Sylow subgroup in N(P). Thus $a^{-1}Pa = P$, whence $a \in N(P)$; therefore $N(N(P)) \subset N(P)$. Since $N(P) \subset N(N(P))$ (since $H \subset N(H)$ for any sugroup H of G), $N(N(P)) = N(P)$.

19. We go by induction on n. For any $n = 1$ a group of order p has an element of order p, thus a subgroup of order p. Thus the result is correct for $n = 1$.

Suppose that any group G of order p^n has a subgroup of order p^m for all $0 \leq m \leq n$. Let G be a group of order p^{n+1}. Since $|G| = p^{n+1}$, then by

uPu^{-1}, from which we get that $(u^{-1}x)P(u^{-1}x)^{-1} = P$. Thus $v = u^{-1}x$ is in N(P). However $vav^{-1} = u^{-1}xax^{-1}u = u^{-1}bu = b$ since $ub = bu$. Thus a and b are conjugate in N(P).