STUDENT'S SOLUTION MANUAL

Abstract Algebra

I.N. Herstein
University of Chicago

Macmillan Publishing Company
New York
Collier Macmillan Publishers
London

Preface

As I stressed in the book *Abstract Algebra*, it is very important that you try to solve many of the problems. It's nice to solve a given problem, but it is more important to make an attempt to solve it. There is no better way for you to test how much control you have over the material. It is too much to expect that you will try, or solve, all, or most, of the large number of problems appearing in the book. The chief thing is that you take a stab at a good cross-section of them.

In this addendum to the book you will find solutions to many of the problems. Roughly one-half of the so-called Easier Problems are solved here; a slightly higher fraction of the Middle-Level Problems also have their solution given. The solution is given for a rather large fraction of the Harder Problems or Very Hard Problems. There is no systematic way—for instance, every second one—in which I chose those exercises for which I give solutions. The choice was made on the basis of how instructive or useful a given solution would be for the student who attempted a given problem and did not succeed in solving it. Even if you do solve a particular one, it might be of interst to you to compare your approach and mine to that exercise.

There is a great temptation to peek at the solution after an initial attempt at a problem fails. Don't give in to this temptation. Only after you have thought about a problem and approached it from a variety of angles, and still didn't get it, should you look up the solution in this booklet. To give in and peek prematurely is self-defeating for it takes away from both the challenge and learning experience that you could have in thinking through the matter on your own.

What I have written above applies particularly to those problems designated as Harder Problems or Very Hard Problems. These problems, in general, were designed to challenge the would-be solver to the utmost. So don't be discouraged if you fail to solve a great many of them. The fun you derive should be in the attempt, and not necessarily in the success, of grappling with something difficult.

The problems are occasionally not rated as to difficulty. This is deliberate on my part. The ability to guess or to judge the difficulty of a situation can be an essential part of the learning process.

Solutions to some problems depend on those of other ones. There is often some cross-reference indicated in the statement of the problem. Some problems come a little before the required material needed to handle them has been discussed. This serves two purposes. First, it gives you a chance to develop some of the needed notions on your own. Second, it tends to show you that this material has some bite to it, and that it allows you to do things which you were unable to do without it.

At any rate, I hope you have lots of fun with the problems, that they challenge you enough, and that they don't frustrate you too often.

I.N.H.

Contents

1

Things Familiar and Less Familiar

SECTION 2.

Easier Problems.

3. $A \cap B \cap C$ is the set of all women residents of the United States who are Canadian citizens, $A - B$ is the set of all non-Canadian residents of the United States, $A - C$ is the set of all male residents of the United States, and $C - A$ is the set of all the women in the world not residing in the United States.

4. $a = 9$.

6. If $A \subset B$ and if $u \in A \cup C$ then $u \in A$ or $u \in C$; if $u \in A$ then $u \in B$ since $A \subset B$, hence u is certainly in $B \cup C$. On the other hand, if $u \in C$ then $u \in B \cup C$. Thus, in either case, $u \in B \cup C$, whence $A \cup C \subset B \cup C$.

8. If u is in $(A - B) \cup (B - A)$ then u is certainly in $A \cup B$; if u is in $A - B$ then u is <u>not</u> in B so is not in $A \cap B$ hence u is in $(A \cup B) - (A \cap B)$. Similarly, if u is in $B - A$ then u is in $(A \cup B) - (A \cap B)$. Therefore $(A - B) \cup (B - A) \subset (A \cup B) - (A \cap B)$. On the other hand, if $u \in (A \cup B) - (A \cap B)$ then $u \in A \cup B$ and u is not in <u>both</u> A and B ; thus if u is in A then u is <u>not</u> in B hence u is in $A - B$. Similarly, if u is in B then u is not in $B - A$. Thus in all cases u is in $(A - B) \cup (B - A)$, whence $(A \cup B) - (A \cap B) \subset (A - B) \cup (B - A)$. We thus get the required equality of these two sets.

10. Since $A \cup (B \cap C)$ is contained in both $A \cup B$ and $A \cup C$ we get that $(A \cup B) \cap (A \cup C) \supset A \cup (B \cap C)$. For the other way, if $u \in (A \cup B) \cap (A \cup C)$, then u is in both $A \cup B$ and $A \cup C$ and, if u is not in A, then $u \in B$ and $u \in C$ so

that $u \in B \cap C$, and so $u \in A \cup (B \cap C)$. If u should happen to be in A then certainly u is in $A \cup (B \cap C)$. So we get that if u is in $(A \cup B) \cap (A \cup C)$ then u is in $A \cup (B \cap C)$, hence $(A \cup B) \cap (A \cup C) \subset A \cup (B \cap C)$. This proves the desired equality of the sets.

11. The subsets of $S = \{1,2,3,4\}$ are 16 in number. They are: S, {1},{2},{3}, {4}, {1,2},{1,3},{1,4},{2,3},{2,4},{3,4},{1,2,3},{1,2,4},{1,3,4},{2,3,4}, and the empty set.

Middle-Level Problems.

12. (a). If $u \in (A \cap B)'$ then u cannot be in both A and B. If u is not in A then u is in A′ and if u is not in B then u is in B′, hence $u \in A' \cup B'$. Thus $(A \cap B)' \subset A' \cup B'$. Since $A \supset A \cap B$, $A' \subset (A \cap B)'$; similarly $B' \subset (A \cap B)'$, hence $A' \cup B' \subset (A \cap B)'$. This proves that $(A \cap B)' = A' \cup B'$.

(b) For any subset C of S, $(C')' = C$ from the very definition of C′. Thus, by Part (a), $(C' \cup D')' = (C')' \cap (D')' = C \cap D$. Let $A = C'$ and $B = D'$; we get $(A \cup B)' = (C')' \cap (D')' = A' \cap B'$.

13. (a). $A + B = (A - B) \cup (B - A) = (B - A) \cup (A - B) = B + A$.

(b). $A + 0 = (A - 0) \cup (0 - A) = A \cup 0 = A$.

(c). $AA = A \cap A = A$.

(d). $A + A = (A - A) \cup (A - A) = 0$.

(e). To show that $A + (B + C) = (A + B) + C$ we first prove the

Theorem. $A + (B + C) = (A \cup B \cup C) - [[(A \cap B) \cup (A \cap C) \cup (B \cap C)] - (A \cap B \cap C)]$.

Proof. Let $D = [[(A \cap B) \cup (A \cap C) \cup (B \cap C)] - (A \cap B \cap C)]$ and $E = (A \cup B \cup C) - D$.

If $u \in E$ and if u is not in A then $u \in B \cup C$. We claim that if u is in $B \cap C$ then $u \in A + B + C$. For, if $u \in B \cap C$, then, since u is not in A, so not in $A \cap B \cap C$, u must be in D, contradicting that it is in E. Thus u is not in $B \cap C$

and being in $B \cup C$ we have that $u \in B + C$, hence in $A + (B + C)$. On the other hand, if $u \in A$ then u then, if u is not in $B + C$ then $u \in A - (B + C) \subset A+(B+C)$. Hence $u \in A + (B + C)$ and so $E \subset A + (B + C)$.

To finish the proof we show that $A + (B + C) \subset E$. If $x \in A + (B + C)$ and if x is not in A then x is in $B + C$; therefore x is in $B \cup C$ but not in $B \cap C$, thus x is not in D, so must be in E. If x is in A then x is not in $B + C$; if x is not in $B \cup C$ then x is not in D hence must be in E. If, on the other hand, x is in $B \cup C$ then since it is in $B + C$ it is not in $B \cap C$ so is not in $A \cap B \cap C$ thus not in D , hence must be in E. This finishes the proof.

To finish Part (e) we note that $(A + B) + C = C + (A + B)$, and using the theorem above, $C + (A + B) = C \cup A \cup B - \{[(C \cap A) \cup (C \cap B) \cup (A \cap B)] - (A \cap B \cap C)\} = A + (B + C)$.

(f). If $A + B = A + C$ then $A + (A + B) = A + (A + C)$, so by Part (e) we get $(A + A) + B = (A + A) + C$. From Parts (d) and (b) we get that $B = C$.

(g). $A \cdot (B + C) = A \cap ((B - C) \cup (C - B)) = (A \cap (B - C)) \cup (A \cap (C - B))$ by the result of Problem 9. The analagous proof to that of Problem 9 shows that $A \cap (B - C) = (A \cap B) - (A \cap C)$. Thus, from the above,

$A \cdot (B + C) = \{(A \cap B) - (A \cap C)\} \cup \{(A \cap C) - (A \cap B)\} = A \cap B + A \cap C = AB + AC$.

15. Let $D = B \cup C$; then $m(A \cup B \cup C) = m(A \cup D) = m(A) + m(D) - m(A \cap D) = m(A) + m(B) + m(C) - m(B \cap C) - m((A \cap B) \cap (A \cap C)) = m(A) + m(B) + m(C) - m(B \cap C) - \{m(A \cap B) + m(A \cap C) - m(A \cap B \cap C)\} = m(A) + m(B) + m(C) - m(A \cap B) - m(A \cap C) - m(B \cap C) + m(A \cap B \cap C)$.

16. To obtain $m(A_1 \cup \ldots \cup A_n)$ we form the sum of the $m(A_i)$ for $i = 1, \ldots, n$ and subtract from this the sum of the m's of all the intersections of every $m - 1$ distinct A_i's plus the sum of the m's of all the intersections of

every $m - 2$ distinct A_i's and so on. (The formal proof can be carried out after we have studied induction in Section 6.)

17. Let A be the set of Americans that have gone to high-school and let B be the set of all Americans that read a daily newspaper. Then $A \cup B$ consists of at most all Americans. If there are n Americans then $n \geq m(A \cup B) = m(A) + m(B) - m(A \cap B) = .8n + .7n - m(A \cap B)$ from the data given. Hence $m(A \cap B) \geq .8n + .7n - n = .5n$, thus at least 50% of all Americans are in $A \cap B$, that is, have gone to high-school and read a daily newspaper.

19 18. Arguing as in the solution to Problem 17 we easily obtain that the set of veterans who lost an eye, an ear, and an arm is at least 25% of the group of disabled veterans. Thus those who, in addition, lost a leg is at least $85 + 25 - 100 = 10$ percent.

21 (20). (a). Let $S = \{a_1, \ldots, a_5\}$ and let A be a subset of S. We assign to A a binary number as follows: if $a_i \in A$ the i^{th} digit of this number is 1 and if a_i is not in A the i^{th} digit is 0. Thus the subset $\{a_1, a_3, a_4\}$ has the binary number 10110 assigned to it, S has 11111 assigned to it, the empty set has 00000 assigned to it, and so on. On the other hand, given a 5-digit binary number it is the number assigned to some subset of S. For instance, 01101 would come from the subset $\{a_2, a_3, a_5\}$. Since the number of 5-digit binary numbers is 32 there are 32 subsets in S. (Of course we could solve the problem by enumerating all 32 subsets of S.)

(b). Since there is only one subset of S having 4 elements which does not contain a given a_i and there are 5 a_i's we have exactly five 4-element subsets of S.

(c). The number of subsets of S having 2 elements is the number of ways we can pick 2 objects out of a set of 5 objects without regard to order. This number is 10 = 5.4/2.

22. (a). Arguing as above in the solution to Problem 21, by assigning an n-binary number to each subset of S we see that S has 2^n subsets.

(b). The number of subsets of S having exactly m elements is equal to the number of ways of picking m objects, without regard to order, out of a set on n objects. This number is n!/(m!(n-m)!). A formal proof of this can be more readily given once we have studied induction.

SECTION 3.

Easier Problems.

1. (a). f is not a mapping since not every woman has a husband.

(b). f is not a mapping of S into T for f(1) = 0 and 0 is not in T.

(c). f is a mapping from the positive integers to the nonnegative ones.

(d). f is not a mapping of the nonnegative integers into themselves for f(0) = -1 which is not in T.

(e). f is a mapping on the set of all integers.

(f). f is not a mapping from the reals into themselves since $\sqrt{-1}$ is not a real number.

(g). f is a mapping from the positive real numbers into themselves because every positive real number has a positive square root.

3. If f is a 1-1 mapping of S onto T then f^{-1} defines a mapping from T to S since, given t in T, there is one and only one element s in S such that t = f(s), and s is defined to be $f^{-1}(t)$. That f^{-1} is onto and 1-1 follows from the fact that f is a 1-1 mapping from S onto T; that it is onto is a consequence of the fact that f is defined on all of S so that every element

s in S has image $t = f(s)$ in T, hence $s = f^{-1}(t)$. It is 1-1 because, if $f^{-1}(t_1) = f^{-1}(t_2)$ then $t_1 = f(f^{-1}(t_1)) = f(f^{-1}(t_2)) = t_2$.

5. Given u in U then $u = f(t)$ for some t in T since f maps T onto U; because f maps S onto T, the t above is of the form $t = f(s)$ for some s in S. Thus $u = f(t) = f(g(s)) = (f\ g)(s)$, whence $f\ g$ is a mapping of S onto U.

6. If t is in T then $t = f(s)$ for some s in S since f is onto. Thus $g(t) = g(f(s)) = (g\ f)(s) = (h\ f)(s) = h(f(s)) = h(t)$; therefore $g = h$.

8. (a). f defines a function from S to T.

(b). Since even + even is even, odd + odd is even, and even + odd is odd we easily verify that $f(s_1 + s_2) = f(s_1)f(s_2)$.

(c) By the definition of f, $f(3) = -1$ and $f(2) = 1$, yet $1 = f(6) \neq f(3)f(2) = -1$, hence $f(s_1 s_2)$ is, in general, not equal to $f(s_1)f(s_2)$.

9. (a). $f(s) = s^2$ and $g(s) = s + 1$ thus $(f\ g)(s) = f(g(s)) = f(s + 1) = (s + 1)^2$.

(b). $(g\ f)(s) = g(f(s)) = g(s^2) = s^2 + 1$.

(c). from (a) and (b) we see that $f\ g \neq g\ f$.

10. (a). $(f_{a,b}\ f_{c,d})(s) = f_{a,b}(cs + d) = a(cs + d) + b = acs + ad + b = f_{ac,ad+b}(s)$, hence $f_{a,b}\ f_{c,d} = f_{ac,ad+b}$.

(b). From the result of (a) we know that $f_{a,b}\ f_{c,d} = f_{ac,ad+b}$ and $f_{c,d}\ f_{a,b} = f_{ca,cb+d}$, thus these two products of mappings are equal if and only if $ad + b = cb + d$. This does not hold, for instance, if $a = b = d = 1$ and $c = 2$.

(c). If $c = d = 1$ then the result of (b) shows that for $f_{a,b}\ f_{1,1}$ to be equal to $f_{1,1}\ f_{a,b}$ we must have $a + b = b + d$, that is, $a = d$. So the only

ones satisfying the condition are all the $f_{a,a}$.

(d). Suppose that $f_{x,y} \circ f_{a,b} = f_{1,0}$, the identity mapping. By the formula of Part (a), $xa = 1$ and $xb + y = 0$. Thus $x = a^{-1}$ and $y = -a^{-1}b$ are solutions. Furthermore, for this x and y, $f_{a,b} \circ f_{x,y} = f_{ax,ay+b}$ and since $ax = 1$ and $ay + b = a(-a^{-1}b) + b = 0$ we see that $f_{a,b} \circ f_{x,y} = f_{1,0}$. Thus $f_{a^{-1},-a^{-1}b}$ is the required inverse for $f_{a,b}$.

Middle-Level Problems.

12. (a). the f so defined is not a mapping, since, for instance, $f(1/2) = 2^1 3^2$ while $f(1/2) = f(2/4) = 2^2 3^4 \neq 2^1 3^2$, so we cannot assign a unique value to f(1/2), hence f is not a mapping.

(b). given a positive rational number r we can write r as m/n where m and n are positive integers having no common factor. Then f defined on S to T by $f(r) = 2^m 3^n$ does define a legitimate function (mapping).

13. To show that f defines a function we must show that to every s in S, f assigns a unique element of T. If $2^m 3^n = 2^a 3^b$ where m,n,a,b are non-negative integers, then m = a and n = b. For suppose m > a, say; then n < b and $2^{m-a} = 3^{b-n}$, and since the left side of this is even while the right one is odd, this cannot happen. So every element in S has a unique representation in the form $2^m 3^n$ and the rule $f(2^m 3^n) = m/n$ is thus a mapping from S to T.

15. Let $f = f_{a,b}$ where $a \neq 0$ and b are integers. Applying the formula $f_{a,b} \circ f_{a,b} = f_{a^2,ab+b}$ we get that $f \circ f \circ f = f_{a,b} \circ f_{a^2,ab+b} = f_{a^3,a^2b+ab+b}$; in

(b). $g^2: \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix}$, $g^3: \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & x_1 & x_3 & x_4 \end{pmatrix}$

(c). $fg: \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_3 & x_2 & x_4 & x_1 \end{pmatrix}$ (d). $gf: \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_1 & x_3 & x_4 & x_2 \end{pmatrix}$

(e). A similar computation to the ones above shows that $(fg)^3 = i_S$ and $(gf)^3 = i_S$

(f). From (c) and (d) we see that $(fg)(x_1) = x_3$ while $(gf)(x_1) = x_1$, hence $fg \neq gf$.

11. See the solution for S_n for any n given for Problems 12 and 13.

Middle-Level Problems.

12. For the solution see that of Problem 31 in Section 2 which shows that, given s in S and f in S_n, there is a positive integer k, depending on s, such that $f^k(s) = s$. If m is the product of the k's for all the elements of S then $f^m(t) = t$ for all t in S. Thus $f^m = i$.

14. Let $S = \{x_1, x_2, \ldots, x_m\}$ and $T = \{y_1, y_2, \ldots, y_n\}$ where $m < n$. Define F from S_m to S_n by: if $f \in S_m$ and $f(x_i) = x_j$ (j depending on i) let F(f) be in S_n defined by $F(f)(y_i) = y_j$ for $1 \leq i \leq m$ and $F(f)(y_k) = y_k$ for $k > m$. Clearly F is 1-1 and from its very definition $F(fg) = F(f)F(g)$.

15. If S has 3 or more elements define $f: S \to S$ by $f(s_1) = s_2$, $f(s_2) = s_1$ and $f(s) = s$ for all the other s in S. Define $g: S \to S$ by $g(s_1) = s_3$, $g(s_3) = s_1$ and $g(s) = s$ for all the other s in S. Thus $(fg)(s_1) = f(g(s_1)) = f(s_3) = s_3$,

while $(gf)(s_1) = g(f(s_1)) = g(s_2) = s_1$. Thus $fg \neq gf$.

16. (a). Suppose that $f \in M$ moves only $s_1, s_2, \ldots, s_m$, leaving the other elements of S fixed, and $g \in M$ moves only $t_1, t_2, \ldots, t_n$, leaving the other elements of S fixed. Then, since $(fg)(s) = f(g(s))$, we see that fg leaves all elements of S fixed with the possible exception of $s_1, \ldots, s_m, t_1, t_2, \ldots, t_n$. Thus $f(s) \neq s$ for at most a finite number of s, hence, by the definition of M fg is in M.

(b). If $f \in M$ and $f(s) = s$ for all s other than $s_1, s_2, \ldots, s_m$ then $f^{-1}(s) = s$ for all s other than $s_1, s_2, \ldots, s_m$, hence $f^{-1} \in M$.

18. (a). Since U(T) is the set of all f in A(S) which take T into itself, and $i(t) = t$ for every t in T, clearly i takes T into itself. Thus $i \in U(T)$.

(b). If $f, g \in U(T)$ then g takes T into itself, so if $t \in T$ then $g(t) \in T$, hence $(fg)(t) = f(g(t))$ is in T since f takes T into itself. Thus $fg \in U(T)$.

Suppose that the elements of T are $t_1, \ldots, t_m$ and $f(t_i) = t_j$ where t_j is in T. Let the mapping F be defined by $F(f)(s_i) = s_j$, $1 \leq i \leq m$. F(f) lies in S_m and, from its definition, maps U(T) onto S_m, for if $\sigma \in S_m$ and $\sigma(s_i) = s_k$ for $1 \leq i \leq m$ then, if $f \in U(T)$ is such that $f(t_i) = t_k$ then $F(f)(s_i) = s_k$, hence $F(f) = \sigma$. To see that $F(fg) = F(f)F(g)$ note that if $f(t_j) = t_k$ and $g(t_i) = t_j$ then $(fg)(t_i) = t_k$, hence $F(f)(s_j) = s_k$, $F(g)(s_i) = s_j$, and $F(fg)(s_i) = s_k = (F(f)F(g))(s_i)$ for each $1 \leq i \leq m$. Thus $F(fg) = F(f)F(g)$.

20. Since U(T) has $m!(n-m)!$ elements and S_m has $m!$ elements, if F is 1-1 then $m! = m!(n-m)!$, and so $(n-m)! = 1$. This forces $n - m = 1$ or $n - m = 0$ ($0! = 1$

Problem 16 in Section 5 there is a 1-1 correspondence g of F onto N. Then gf is a 1-1 correspondence of A onto N.

22. If the complex number a is a root of $p(x) = x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n$ then $a^n + \alpha_1 a^{n-1} + \ldots + \alpha_n = 0$, hence $\overline{(a^n + \alpha_1 a^{n-1} + \ldots + \alpha_n)} = \bar{0}$. By the properties of the complex conjugate we get that $\bar{a}^n + \bar{\alpha}_1 \bar{a}^{n-1} + \ldots + \bar{\alpha}_n = 0$. If the α_i are all real then $\alpha_i = \alpha_i$, thus $\bar{a}^n + \alpha_1 \bar{a}^{n-1} + \ldots + \alpha_n = 0$. Thus $p(\bar{a}) = 0$ and $\bar{a}$ is a root of $p(x)$.

Harder Problems.

23. Let $z = r(\cos\theta + i \sin\theta)$ and $w = t(\cos\psi + i \sin\psi)$; thus $|z| = r$ and $|w| = t$. Also, $z + w = (r\cos\theta + t\cos\psi) + i(r\sin\theta + t\cos\psi)$, therefore $|z + w|^2 = (r\cos\theta + t\cos\psi)^2 + (r\sin\theta + t\sin\psi)^2 = r^2(\cos^2\theta + \sin^2\theta) + t^2(\cos^2\psi + \sin^2\psi) + 2rt(\cos\theta\cos\psi + \sin\theta\sin\psi) = r^2 + t^2 + 2rt\cos(\theta - \psi)$. We have that $|z + w| = |z| + |w|$ if and only if $(|z + w|)^2 = (|z| + |w|)^2$, that is, if and only if $r^2 + t^2 + 2rt\cos(\theta - \psi) = r^2 + t^2 + 2rt$, and so, if and only if $\cos(\theta - \psi) = 1$. This is true if and only if $\cos\theta = \cos\psi$. Therefore the necessary and sufficient condition that $|z + w| = |z| + |w|$ is that $z = r(\cos\theta + i \sin\theta)$ and $w = t(\cos\theta + i \sin\theta)$. This says that, viewed as vectors in the plane, z and w point in the same direction.

25. Suppose that $k = qn + r$ where $0 \leq r < n$. Then $1 = \theta^k = \theta^{qn+r} = (\theta^n)^q\theta^r = \theta^r$. Since $r < k$, by the choice of k, r cannot be positive. Thus $r = 0$ and so $k = qn$ and $n \mid k$.

26. All the complex numbers having order n are the numbers $\theta_k = \cos 2\pi k/n + i \sin 2\pi k/n$ where k is relatively prime to n.

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 $H = (T_{c,d} \in G \mid c$ rational, d 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, $(f^ih^j)^{-1} = h^{-j}f^{-1} = f^{-1}h^j$ 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, which only has k elements. Thus 2 of a, a^2, ... , a^{k+1} are equal; that is $a^{i} = a^{j}$ for some $1 \leq i < j \leq k + 1$, and so $a^{j-1} = e$, where $0 < j - i \leq k$. 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 $G = \{a_1, \ldots, a_n\}$. If $b \in G$ consider the elements $a_1*b, \ldots, a_n*b$; 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 $0 = F(1) = F((-1)^2) = F(-1)*F(-1) = F(-1) + F(-1) = 2F(-1)$, 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 $(ba)^{i+1} = (ab)^{i+1}$. Therefore $ba(ba)^i = a^{i+1}b^{i+1}$ $= (ab)^{i+1} = ab(ab)^i = ab(ba)^i$; cancelling the $(ba)^i$ 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 $H = (a^i \mid i$ 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 $\mathbf{R}$ 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 any x in the above form provided that 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 | $|U_m| = \varphi(a^n - 1)$.

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, $a^{n/d}$, $a^{2n/d}$, ... , $a^{(d-1)n/d}$ 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 $ada^{-1} = a^ica^{-1}$, leading to the contradiction that $d = a^{i-1}ca^{-(i-1)}$. 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 $b \in A$. 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

$g = za^l$ 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 $gh = za^lz'a^j = a^{l+j}zz' = z'a^jza^l = hg$ 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 $1 \le i \le r$ and for all $i \ne j$ 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 $1 \le i \le k$. 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 $s \ge mn$. 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 $7 | (i^5 - 1)$, and since, by Fermat's Theorem, $7 | (i^6 - 1)$ we get that $7 | (i - 1)$. 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 $g = n_i \ldots n_k = m_1 \ldots m_k$ where each m_i is also in N_i then we obtain that $n_i m_i^{-1} = m_1 \ldots m_{i-1} m_{i+1} \ldots m_k n_k^{-1} \ldots n_{i-1}^{-1} n_{i+1}^{-1} \ldots n_1^{-1} = (m_1 n_1) \ldots (m_k n_k^{-1})$ so $n_i m_i^{-1}$ is in $N_i \cap (N_1 \ldots N_{i-1} N_{i+1} \ldots N_k) = (e)$. Thus $n_i = m_i$ for each i, whence g has a unique representation in the form $g = n_1 \ldots n_k$. Therefore G is the direct product of $N_1, N_2, \ldots, N_k$.

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).

3
The Symmetric Group

SECTION 1.

1. (a). $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 2 & 1 & 3 & 6 \end{pmatrix}$

(b). $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix}$

(c). $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$

4. (a). $o(\sigma) = 6$, $o(\sigma^2) = 3$, $o(\sigma^3) = 2$, $o(\sigma^4) = 3$, $o(\sigma^5) = 6$, $o(\sigma^6) = 1$.

(b). $o(\sigma) = 2$, $o(\sigma^2) = 1$.

(c). $o(\sigma) = 4$, $o(\sigma^2) = 2$, $o(\sigma^3) = 4$, $o(\sigma^4) = 1$.

SECTION 2.

Easier Problems.

1. If i does not occur in σ nor in τ then $\sigma(i) = \tau(i) = i$. If i occurs in σ it cannot occur in τ since σ and τ are disjoint. Thus $\tau(i) = i$ and $(\sigma\tau)(i) = \sigma(i)$. Also, since i occurs in σ we have that $\sigma(i)$ also occurs in σ, hence does not occur in τ. Therefore $\tau(\sigma(i)) = \sigma(i)$, which is to say, $(\tau\sigma)(i) = \sigma(i) = (\sigma\tau)(i)$. Similarly, if i occurs in τ but not in σ then $(\sigma\tau)(i) = (\tau\sigma)(i)$. Thus $\sigma\tau$ and $\tau\sigma$ agree on each i; hence $\sigma\tau = \tau\sigma$.

2. (a). (1 3 4 2)(5 7 9)(6)(8); its order is 12.

(b). (1 7)(2 6)(3 5)(4); its order is 2.

(c). (1 6)(2 5)(3 7)(4); its order is 2.

4. The cycle of σ to which i belongs is $(i, \sigma(i), \sigma^2(i), \ldots, \sigma^{m-1}(i))$ where m is the first positive integer such that $\sigma^m(i) = i$. These cycles are disjoint, for they consist of the orbits of each letter under σ, and we saw

that this is an equivalence relation. Each cycle above specifies that any letter j goes into $\sigma(j)$ by the action of that cycle. Hence the product of these disjoint cycles gives the same image for each letter j as does σ. Hence this product equals σ.

6. Let the shuffle place the i^{th} card in the $(i+1)^{st}$ position if $1 \le i \le 6$, the 7^{th} card in the first position, and for $8 \le i \le 12$ again let the i^{th} card be placed in the $(i+1)^{st}$ position, and the 13^{th} card in the 8^{th} position. This shuffle corresponds to th permutation (1 2 3 4 5 6 7)(8 9 10 11 12 13) which is of order 42. Thus this shuffle requires 42 repeats to restore the deck to its original order.

10. For any permutation σ, $\sigma(1\ 2)\sigma^{-1}$ has order 2 while (1 2 3) has order 3. Thus $\sigma(1\ 2)\sigma^{-1}$ cannot equal (1 2 3).

12. If (1 2) were the product of disjoint 3-cycles then $(1\ 2)^3$ = identity, for these 3-cycles commute and each of them is of order 3. But $(1\ 2)^2$ = identity. These relations would force that (1 2) = identity, a contradiction.

Middle-Level Problems.

13. Suppose that $\sigma(1) = i$, $\sigma(2) = j$, and $\sigma(3) = k$; let $\tau = (1\ 2\ 3)$. Then $(\sigma\tau\sigma^{-1})(i) = (\sigma\tau)(1) = \sigma(2) = j$. Similarly $(\sigma\tau\sigma^{-1})(j) = k$ and $(\sigma\tau\sigma^{-1})(k) = i$. If m is none of i, j, or k then $(\sigma\tau\sigma^{-1})(m) = m$. Thus $\sigma(1\ 2\ 3)\sigma^{-1}$ is a 3-cycle so only moves 3 letters, whereas (1 2 3)(4 5 6) moves 6 letters. So they cannot be equal.

16. Since (1 2) and (1 2 3) generate S_3 to find out what ϕ does to any element it is enought to find out what ϕ does to (1 2) and (1 2 3). Now $\phi((1\ 2\ 3))$ is of order 3 so can only be (1 2 3) or (1 3 2). Similarly, $\phi((1\ 2))$ can only be one of (1 2), (1 3), or (2 3).

Suppose that $\phi((1\ 2\ 3)) = (1\ 2\ 3)$. If $\phi((1\ 2)) = (1\ 2)$ then we easily

get that ϕ = identity map. If $\phi((1\ 2)) = (2\ 3) = (2\ 3)(1\ 2)(1\ 2\ 3)^{-1}$ we get that $\phi(\tau) = (1\ 2\ 3)\tau(1\ 2\ 3)^{-1}$ for every τ in S_3. Similarly, if $\phi((1\ 2)) = (1\ 3)$ we get that $\phi(\tau) = (1\ 3\ 2)\tau(1\ 3\ 2)^{-1}$ for every τ in S_3.

Suppose then that $\phi((1\ 2\ 3)) = (1\ 3\ 2)$. If $\phi((1\ 2)) = (1\ 2)$ then we easily see that $\phi(\tau) = (1\ 2)\tau(1\ 2)^{-1}$ for every τ in S_3. If $\phi((1\ 2)) = (1\ 3)$, we get that $\phi(\tau) = (2\ 3)\tau(2\ 3)^{-1}$ for every τ in S_3. Finally, if $\phi((1\ 2)) = (2\ 3)$ then $\phi(\tau) = (1\ 3)\tau(1\ 3)^{-1}$ for each τ in S_3. Thus in all posssibilities, $\phi(\tau) = \sigma\tau\sigma^{-1}$ for every τ in S_3 and a suitable σ in S_3.

17. We will show that every transposition can be obtained as a product of $(1\ 2)$'s and $(1\ 2 \ldots n)$'s. Now $(1\ 2 \ldots n)(1\ 2)(1\ 2 \ldots n)^{-1} = (2\ 3)$, $(1\ 2 \ldots n)(2\ 3)(1\ 2 \ldots n)^{-1} = (3\ 4)$, and $(1\ 2 \ldots n)(3\ 4)(1\ 2 \ldots n)^{-1} = (4\ 5)$, and continuing we obtain that $(i\ i+1)$ is so obtainable. Thus $(1\ 2)(2\ 3)(1\ 2) = (1\ 3)$, $(1\ 3)(3\ 4)(1\ 3) = (1\ 4)$, $(1\ 4)(4\ 5)(1\ 4) = (1\ 5)$, ..., $(1\ n)$ are generated from $(1\ 2)$ and $(1\ 2 \ldots n)$. But then $(1\ i)(1\ j)(1\ i) = (i\ j)$, if $i \neq j$, is in the subgroup generated by $(1\ 2)$ and $(1\ 2 \ldots n)$. Thus every transposition is reached this way, so all of S_n is generated by $(1\ 2)$ and $(1\ 2 \ldots n)$.

18. If the two transpositions τ_1 and τ_2 have 2 letters in common they are equal so $\tau_1\tau_2$ = identity = $(1\ 2\ 3)(1\ 3\ 2)$, a product of 3-cycles. If they have one letter in common then $(i\ j)(i\ k) = (i\ k\ j)$ is a 3-cycle. If they have no letter in common then $(i\ j)(k\ m) = (i\ k\ j)(i\ k\ m)$ is a product of 3-cycles if i, j, k, and m are distinct.

19. If $\tau_1\tau_2\tau_3 = e$ then $\tau_1\tau_2 = \tau_3$; by the argument of Problem 18, $\tau_1\tau_2$ is either the identity, the product of two disjoint transpositions, or a 3-cycle, hence moves no letter, 4 letters or 3 letters, so cannot be a

3 | (b - d); thus [a] = [c] and [b] = [d]. Therefore for every choice of the pair [a] and [b] we get a distinct element of R/M. Since we can choose such a pair in $3^2 = 9$ ways, we get that R/M has 9 elements.

3. In R/M, $2 + M = -i + M$, so the image of any $c + di$ in R/M is of the form $(c - 2d) + M$. Thus R/M consists of $u + M$ where u is any integer. However $(2 + i)(2 - i) = 5$ is in M. So, if $u = 5k + r$, where $0 \leq r < 5$, then $u + M = r + 5k + M = r + M$. Thus R/M is isomorphic to Z_5, a field. By Theorem 4.4.3 M is a maximal ideal of R.

5. We showed in Problem 3 that $M = R(2 + i)$ is a maximal ideal of R and $R/M \cong Z_5$. A similar argument shows that $N = R(2 - i)$ is also a maximal ideal and $R/N \cong Z_5$. What is $M \cap N$? Since $5 = (2 + i)(2 - i)$, $5 \in M \cap N$, we have that $I \subset M \cap N$. If $x \in M \cap N$, $x = (a + bi)(2 + i)$ and $x = (c + di)(2 - i)$. These relations give us that $x^2 = 5(a + bi)(c + di)$, hence $x^2 \in I$. Thus, if $x = r + si$ then $x^2 = r^2 - s^2 + 2rsi$, we have, since x^2 is in I, that $5 \mid 2rs$ and $5 \mid (r^2 - s^2)$. These imply that $5 \mid r$ and $5 \mid s$. Thus x is in I. Therefore we get that $I = M \cap N$.

Since $M + N \neq M$ is an ideal of R, and M is a maximal ideal of R, $M + N = R$. Thus, given y in R, then $y = m + n$ for some m in M and some n in N. The mapping f from R into $R/M \oplus R/N$ defined by $f(y) = (y + M, y + N)$ is a homomorphism, and its kernel is $M \cap N = I$ (See Problem 20 in Section 3). We claim that it is onto. Given $(u + M, v + N)$ in $R/M \oplus R/N$, since $u = m_1 + n_1$ and $v = m_2 + n_2$, where m_1, m_2 are in M and n_1, n_2 are in N then $(u + M, v + N) = (n_1 + m_1 + M, m_2 + n_2 + N) = (n_1 + M, m_2 + N) = f(m_2 + n_1)$. So f is a homomorphism of R onto $R/M \oplus R/N$ with kernel $M \cap N = I$. Because

R/M and R/N are isomorphic to Z_5 we get that $R/I \cong Z_5 \oplus Z_5$.

7. A typical element in R/M is of the form [a] + [b]u where $u = \sqrt{2} + M$, and [a] and [b] are in Z_5. Moreover, [a] + [b]u = [c] + [d]u implies that $(a - c) + (b - d)\sqrt{2}$ is in M, hence $5 \mid (a - c)$ and $5 \mid (b - d)$, whence [a] = [c] and [b] = [d]. So every element in R/M has a unique representation in the form [a] + [b]u, and since we can choose [a] in 5 ways and [b] in 5 ways, R/M is a field having $25 = 5^2$ elements.

9. Let G be the group of non-zero elements in Z_p under multiplication. The quadratic residues are precisely those integers $1 \leq a \leq p - 1$ such that [a] is a square in G. The set of these [a]'s form a subgroup H of G; in fact $H = \{[x]^2 \mid [x] \in G\}$. The mapping f of G onto H defined by $f([x]) = [x]^2$ is a homomorphism of G onto H with kernel $K = \{[1], [-1]\}$. Since $H \cong G/K$, we get that $|H| = |G|/2 = (p - 1)/2$. So there are $(p - 1)/2$ quadratic residues mod p. The remaining $(p - 1) - (p - 1)/2 = (p - 1)/2$ elements are the quadratic non-residues mod p.

12. If m is a quadratic non-residue mod p then the only solution to the congruence $x^2 \equiv my^2 \bmod p$ is $x \equiv 0 \bmod p$ and $y \equiv 0 \bmod p$, for, if $y \not\equiv 0 \bmod p$ then y^{-1} exists mod p and $(xy^{-1})^2 \equiv m \bmod p$, contrary to m a non-residue. Thus $y \equiv 0 \bmod p$, and so $x \equiv 0 \bmod p$.

The argument that I_p is a maximal ideal of R is exactly as that given earlier for the case where m = 2 and p = 5.

SECTION 5.

Easier Problems.

1. If f(x) is invertible and g(x) is its inverse in F[x] then, since

$f(x)g(x) = 1$, $0 = \deg 1 = \deg (f(x)\,g(x)) = \deg f(x) + \deg g(x)$. Consequently $\deg f(x) = 0$, hence $f(x) = a$ where a is in F. On the other hand it is obvious that every non-zero element of F is invertible in $F[x]$.

2. (a). The highest power of x that can occur in $f(x)g(x)$ is x^{m+n} where x^m is the highest power in $f(x)$ and x^n the highest one in $g(x)$. The coefficient of x^{m+n} in $f(x)g(x)$ is ab where a is the coefficient of x^m in $f(x)$ and b that of x^n in $g(x)$. If $ab = 0$ then $\deg (f(x)g(x)) < \deg f(x) + \deg g(x)$.

(b). Let $R = Z_6$ and consider $f(x) = 2x + 1$ and $g(x) = 3x$; then $\deg f(x)$ is 1 as is $\deg g(x)$. But $f(x)g(x) = 3x(2x + 1) = 6x^2 + 3x = 3x$ since $6 = 0$ in Z_6. Thus $\deg (f(x)g(x)) = 1 < \deg f(x) + \deg g(x) = 2$.

6. If $g(x) \mid f(x)$ then $f(x) = g(x)h(x)$ where $h(x)$ is in $F[x]$; thus for any $t(x)$ in $F[x]$, $f(x)t(x) = g(x)h(x)t(x) = g(x)((h(x)t(x))$ so is in $(g(x))$, the ideal of $F[x]$ generated by $g(x)$. Since every element in $(f(x))$ is of the form $f(x)t(x)$ we see that $(f(x)) \subset (g(x))$.

8. Since $f(x) \mid h(x)$ and $g(x) \mid h(x)$, $h(x) = a(x)f(x) = b(x)g(x)$; thus $f(x) \mid b(x)g(x)$ and since $f(x)$ is relatively prime to $g(x)$ we must have that $f(x) \mid b(x)$. So $b(x) = c(x)f(x)$ and so $h(x) = c(x)f(x)g(x)$. Thus $f(x)g(x) \mid h(x)$.

10. The best way to do Problem 10 is to note that if a polynomial $f(x)$ of degree 3 or less over a field F is not irreducible it has a factor of degree one, hence there exists an element a in F such that $f(a) = 0$. (See Problem 11 below).

(a). If $x^2 + 1$ is not irreducible over $\mathbf{R}$ then, by the remark made above there is a real a such that $a^2 + 1 = 0$; this is clearly not possible. So $x^2 + 1$ is irreducible over $\mathbf{R}$.

(b). Using the remark, if $x^3 - 3x + 3$ is not irreducible over Q there is a rational number $r = a/b$, where a and b are relatively prime integers such

that $a^3/b^3 - 3a/b + 3 = 0$, hence $a^3 - 3ab^2 + 3b^3 = 0$. Thus $a \mid 3b^3$ and since $(a, b) = 1$, we must have $a \mid 3$. Therefore $a = \pm 1$ or ± 3. Similarly, $b \mid 1$, so $b = \pm 1$; thus $r = \pm 1$ or ± 3. A direct check of these shows that $r^3 - 3r + 3 \neq 0$ for these four possible r's.

(c). If $x^2 + x + 1$ is not irreducible over Z_2 there exists an element a in Z_2 such that $a^2 + a + 1 = 0$. Since the only choices for a in Z_2 are $a = [0]$ or $a = [1]$, neither of which satisfies the given equation we conclude that $x^2 + x + 1$ is irreducible over Z_2.

(d). Checking all the possible 19 elements in Z_{19} reveals that there is no element a in Z_{19} such that $a^2 + 1 = 0$. Thus $x^2 + 1$ is irreducible over Z_{19}.

(e). Checking the 13 elements in Z_{13} shows that none of these satisfies $a^3 - 9 = 0$, hence $x^3 - 9$ is irreducible over Z_{13}.

(f). If $x^4 + 2x^2 + 2$ is not irreducible over Q then it is the product of two quadratic polynomials over Q; furthermore we may assume that these quadratic polynomials are monic (Prove!). Thus $x^4 + 2x^2 + 2 = (x^2 + ax + b)(x^2 + cx + d) = x^4 + (a + c)x^3 + (b + d + ac)x^2 + (bc + ad)x + bd$ where a, b, c, and d are in Q. Thus $a + c = 0$, $b + d + ac = 2$, $bc + ad = 0$, $bd = 2$ from which we get $a(b - d) = 0$, hence $a = 0$ or $b = d$. However, if $b = d$ then $2 = bd = b^2$, contradicting that $\sqrt{2}$ is irrational. Thus $a = 0$, hence $c = -a = 0$ and so $b + d + ac = b + d = 2$. Since $d = 2/b$ we get $b + 2/b = 2$, and so $b^2 - 2b + 2 = 0$, that is, $(b - 1)^2 = -1$. This is impossible for any real, hence for any rational, number. Thus the given polynomial is irreducible over Q. (Note: the irreducibilty of the polynomials in Parts (b) and (f) is an

immediate consequence of the Eisenstein Criterion in Section 6).

11. If $p(x)$ is not irreducible it is the product of two polynomials of degree less than 3. So one of these is of degree 1, hence is of the form $ax + b$, where $a \neq 0$ and b are in F. Thus $p(x) = (ax + b)(cx^2 + dx + e)$; hence if $r = -b/a$ then r is in F and $p(r) = 0$.

Middle-Level Problems.

13. Let J be the ideal $(x^2 + 1)$. If $u = x + J$ is the image of x in $\mathbf{R}[x]/J$ then every element in $A = \mathbf{R}[x]/J$ is of the form $a + bu$. This is true since for every polynomial $f(x)$ in $\mathbf{R}[x]$, $f(x) = g(x)(x^2 + 1) + (a + bx)$, by the division algorithm, hence $f(x) + J = (a + bx) + g(x)(x^2 + 1) + J = (a + bx) + J = a + bu$, since $g(x)(x^2 + 1)$ is in the ideal $J = (x^2 + 1)$. Also, $u^2 = (x + J)^2 = x^2 + J = -1 + J$, which is -1 in $A = \mathbf{R}[x]/J$. The mapping φ from A to $\mathbb{C}$ defined by $\varphi(a + bu) = a + bi$ is clearly an isomorphism of A onto $\mathbb{C}$.

14. (a). There is no a in Z_{11} such that $a^2 + 1 = 0$, as can be verified by a direct check of the 11 elements in $F = Z_{11}$. Thus by the remark preceding Problem 10 (or by a quadratic version of Problem 11), $x^2 + 1$ is irreducible in $Z_{11}[x]$. Therefore $F[x]/(x^2 + 1)$ is a field. Exactly as in Problem 13, every element in $F[x]/(x^2 + 1)$ is of the form $a + bu$, where $u = x + (x^2 + 1)$ and $a, b \in F$. Moreover every element is of the unique form $a + bu$, for if $a + bu = c + du$ then $(a - c) + (b - d)u = 0$. Hence $(a - c) + (b - d)x$ is in $(x^2 + 1)$; since every non-zero element in $(x^2 + 1)$ is a multiple of $x^2 + 1$ it has degree at least 2. Thus $(a - c) + (b - d)x = 0$, and so $a = c$ and $b = d$. Since we have 11^2 independent choices for a and b and two different choices give rise to different elements in $F[x]/(x^2 + 1)$, $F[x]/(x^2 + 1)$ has $11^2 = 121$ elements.

(b). A direct check of all the elements in $F = Z_{11}$ reveals that for no a in F is $a^3 + a + 4 = 0$. Thus, as before, $p(x) = x^3 + x + 4$ is irreducible in F[x], hence F[x]/(p(x)) is a field. Similar to the argument in Part (a), every element in F[x]/(p(x)) has the unique form $a + bu + cu^2$ where $u = x + (p(x))$ and a, b, c are in F. Thus F[x]/(p(x)) has 11^3 elements.

17. Define the mapping φ from F[x] into $F[x]/(p_1(x)) \oplus \ldots \oplus F[x]/(p_k(x))$ by $\varphi(f(x)) = (f(x) + (p_1(x)), f(x) + (p_2(x)), \ldots, f(x) + (p_k(x)))$ for every f(x) in F[x]. This mapping is a homomorphism, since this is true in every component. Furthermore, Ker $\varphi = \{f(x) \in F[x] \mid f(x) \in (p_i(x)) \text{ for } i = 1, \ldots, k\}$, that is, Ker $\varphi = (p_1(x)) \cap (p_2(x)) \cap \ldots \cap (p_k(x))$.

We claim that φ maps F[x] onto $F[x]/(p_1(x)) \oplus \ldots \oplus F[x]/(p_k(x))$. This is a special case of what in algebra is called the Chinese Remainder Theorem. We prove this more general result and apply it to the problem at hand. Let R be a commutative ring with 1 and $M_1, \ldots, M_n$ distinct maximal ideals of R, then $R/(M_1 \cap M_2 \cap \ldots \cap M_n) \cong R/M_1 \oplus R/M_2 \oplus \ldots \oplus R/M_n$. We proove it for n = 2, leaving the few details needed for induction to the reader goes as follows. Since $M_1 \neq M_2$ are maximal ideals of R, $M_1 + M_2 = R$; thus, given x and y in R, $x = m_1 + m_2$ and $y = n_1 + n_2$ where m_1 and n_1 are in M_1 and m_2 and n_2 are in M_2. Thus $(x + M_1, y + M_2) = (m_1 + m_2 + M_1, n_1 + n_2 + M_2) = (m_2 + M_1, n_1 + n_2 + M_2) = \varphi(r)$, where the element $r = m_2 + n_1$. Thus φ is onto.

Returning to our problem, if $p_1(x), \ldots, p_k(x)$ are irreducible

polynomials in F[x], then the ideals $(p_1(x)), \ldots, (p_k(x))$ are distinct maximal ideals of F[x], thus a direct application of the Chinese Remainder Theorem proves the desired result.

18. Suppose that the irreducible polynomials of F[x] are bounded in degree; then, since F is finite, there would only be a finite number of irreducible polynomials in F[x]. If these are $p_1(x), \ldots, p_k(x)$, consider the polynomial $q(x) = 1 + p_1(x)\ldots p_k(x)$; $q(x)$ must be divisible by some irreducible polynomial, that is, by some $p_i(x)$. But this is clearly false. With this contradiction we get that there must be irreducible polynomials of arbitrarily high degree in F[x].

22. Since R does not have a unit element we know, by Problem 21, that R is not a Euclidean ring. We claim that $d(2) \leq d(a)$ for any non-zero even integer. For, if $d(a) < d(2)$ then, if the Euclidean algorithm held in R, we would have $2 = qa + r$, where $r = 0$ or $d(r) < d(a)$, and q is even. By the choice of a, we must have $r = 0$ and $2 = qa$ where q and a are even, which is impossible. If we consider 2 and 6 in R and if $6 = 2m + b$ where m is even, since d(b) cannot be less than d(2), we must have $b = 0$ and $6 = 2m$ where m is even. This is nonsense, so the Euclidean algorithm does not hold for 2 and 6.

Harder Problems.

23. That $x^3 - 2$ and $x^3 + 2$ are irreducible follows from Problem 11, since a direct check shows that there are no elements a and b in Z_7 such that $a^3 = 2$ or $b^3 = -2$. If $A = F[x]/(x^3 - 2)$ and $r = x + (x^3 - 2)$ in A then every element in A is of the form $a + br + cr^2$ where a, b, c are in Z_7 and

$r^3 = 2$. Similarly, if $B = F[x]/(x^3 + 2)$ and $s = x + (x^3 + 2)$ in B every element in B is of the form $u + vs + ws^2$ where u, v, w are in Z_7 and $s^3 = -2$. Map A onto B by defining $\varphi(a + br + cr^2) = a - bs + cs^2$. Checking the action of φ on sums and products by a direct calculation shows that φ is an isomorphism of A onto B.

24. By Problem 11, $x^2 + x + 1$ is irreducible over Q, so $F[x]/(x^2 + x + 1)$ is a field in which $r = x + (x^2 + x + 1)$ satisfies $r^2 + r + 1 = 0$ and such that every element is of the form $a + br$ where a, b are in Q. Map the set $A = \{a + b\alpha \mid a, b \in Q\}$ onto $F[x]/(x^2 + x + 1)$ by sending $a + b\alpha$ onto $a + br$. This is easily seen to be an isomorphism; since A is isomorphic to the field $F[x]/(x^2 + x + 1)$, A is itself a field.

Suppose that $a + b\alpha \neq 0$; we claim that $(a + b\alpha)(c + d\alpha) = 1$ has a solution with c and d rational. For, $(a + b\alpha)(c + d\alpha) = (ac - bd) + (ad + bc - bd)\alpha$, hence we want that $ac - bd = 1$ and $bc + (a - b)d = 0$ have a solution in Q for c and d. This is possible provided $a(a - b) + b^2 \neq 0$; but if $a^2 + b^2 - ab = 0$ then $0 < a^2 + b^2 = ab$ and $a^2 + b^2 - ab = (a - b)^2 + 2ab > 0$ unless $a = b = 0$. So A is a field since every non-zero element in A has its inverse in A.

25. See the part on the Eisenstein Criterion in the next section.

26. If $t^r = 0$ in R then $(t^{r-1})^2 = 0$ so, by hypothesis, $t^{r-1} = 0$; continuing this way we get $t = 0$. Suppose now that $a_0x^n + a_1x^{n-1} + \ldots + a_n \neq 0$ is a zero-divisor in R; then $(a_0x^n + \ldots + a_n)(b_0x^m + b_1x^{m-1} + \ldots b_m) = 0$ with $b_0 \neq 0$. Thus $a_0b_0 = 0$, $a_0b_1 + a_1b_0 = 0$, $a_0b_2 + a_1b_1 + a_2b_0 = 0$, ... Thus $a_0b_1b_0 + a_1b_0^2 = 0$, from which we get $a_1b_0^2 = 0$ and so $(a_1b_0)^2 = 0$, giving us $a_1b_0 = 0$. Also $a_0b_2b_0^2 + a_1b_1b_0^2 + a_2b_0^3 = 0$ from which we get that

$a_2b_0^3 = 0$ and so $(a_2b_0)^3 = 0$ and so $a_2b_0 = 0$. Continuing with the other coefficients we obtain $a_ib_0^i = 0$, hence $(a_ib_0)^i = 0$ and so $a_ib_0 = 0$ for each $i = 0, 1, \ldots, n$. Thus $b_0 \neq 0$ does the trick.

27. (a). We shall show that $I[x]$ is an ideal of $R[x]$ by showing in Part (b) that $I[x]$ is the kernel of a homomorphism.

(b). Define $\varphi : R[x] \to (R/I)[x]$ by :

$\varphi(a_0x^n + a_1x^{n-1} + \ldots a_n) = (a_0 + I)x^n + (a_1 + I)x^{n-1} + \ldots + (a_n + I)$. It is immediate from the addition and multiplication of polynomials that φ is a homomorphism of $R[x]$ onto $(R/I)[x]$. What is Ker φ ? It is precisely the set of polynomials such that $a_0 + I = I$, $a_1 + I = I$, $\ldots$, $a_n + I = I$, that is the set of polynomials such that $a_0, a_1, \ldots, a_n$ are all in I. In other words, Ker $\varphi = I[x]$. Thus $R[x]/I[x] \cong (R/I)[x]$.

Very Hard Problems.

28. Suppose that $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$, $g(x) = b_0x^m + \ldots + b_m \neq 0$ are such that $f(x)g(x) = 0$ and $g(x)$ is of lowest degree with this property. Then $b_m \neq 0$ (Prove!). We claim that $f(x)b_m = 0$. Certainly $a_nb_m = 0$ since this is the coefficient of the lowest term in $f(x)g(x)$. If $a_ib_m = 0$ for all i then $f(x)b_m = 0$ and we would be done. Suppose then that $a_{n-i}b_m = 0$ for $i < t$, and $a_{n-t}b_m \neq 0$. Thus for $i < t$, $g(x)a_{n-i} = a_{n-i}b_0x^n + \ldots + a_{n-i}b_{m-1}x = (a_{n-i}b_0x^{n-1} + \ldots + a_{n-i})x$ and $f(x)(g(x)a_{n-i}) = 0$, which leads us to the fact that $f(x)(a_{n-1}b_0x^{n-1} + \ldots + a_{n-1}b_m) = 0$, contradicting that $g(x)$ is the

polynomial of lowest degree with this property. Therefore $g(x)a_{n-i} = 0$ for all $i < t$. Thus $0 = f(x)g(x) = (a_0x^n + \dots + a_{n-t}x^t + \dots + a_n)g(x) = (a_0x^n + \dots + a_{n-t}x^t)(b_0x^m + \dots + b_m)$; but this implies the contradiction that $a_{n-t}b_m = 0$.

29. If n is a positive integer and $u + vi$ is in R then $u = a_1n + r_1$ and $v = a_2n + r_2$ where $|r_1| \leq n/2$ and $|r_2| \leq n/2$, that is, $d(r_1) \leq n^2/4$ and $d(r_2) \leq n^2/4$. Thus $d(r_1 + r_2i) = |r_1 + r_2i|^2 \leq n^2/4 + n^2/4 < n^2 = d(n)$, and $u + vi = (a_1 + a_2i) + (r_1 + r_2i) = qn + r$ where $d(r) < d(n)$. Thus the Euclidean algorithm holds for this special choice. Let $0 \neq a + bi$ and $c + di$ be in R; then $(a + bi)(a - bi) = a^2 + b^2 = n$, a positive integer. So, by the above, $(c + di)(a - bi) = qn + r = q(a + bi)(a - bi) + r$ where $d(r) < d(n) = d(a^2 + b^2) = (a^2 + b^2)^2$. From the equation above we see that $r = s(a - bi)$, and so $d(r) = |r|^2 = |s|^2|a - bi|^2 = d(s)(a^2 + b^2) < d(n) = (a^2 + b^2)^2$. This gives us that $d(s) < (a^2 + b^2) = d(a + bi)$. However, from the relation above, $(c + di)(a - bi) = q(a + bi)(a - bi) + s(a - bi)$, hence $c + di = q(a + bi) + s$ and $s < d(a + bi)$. So the Euclidean algorithm holds in R.

Also, if $a + bi \neq 0$ then $d(a + bi)$ is a positive integer, so that for any g in R, $d(g(a + bi)) = d(g)d(a + bi) \geq d(g)$. Thus Properties (1) and (2) defining a Euclidean ring hold for R; hence R is a Euclidean ring.

SECTION 6.

Problems.

1. If φ is an automorphism of $Q[x]$ and $\varphi(f(x))$ is irreducible in $Q[x]$ then

f(x) is irreducible in Q[x]. For, if $f(x) = a(x)b(x)$ then $\varphi(f(x)) = \varphi(a(x)b(x)) = \varphi(a(x))\varphi(b(x))$ giving us a non-trivial factorization of $\varphi(f(x))$ in Q[x].

The mapping $\varphi : Q[x] \to Q[x]$ defined by $\varphi(f(x)) = f(x + 1)$ is an automorphism of Q[x], thus in Example 5 we do get from the irreducibility of g(x) that of f(x).

2. Consider $g(x) = f(x + 1) = (x + 1)^3 + 3(x + 1) + 2 = x^3 + 3x^2 + 6x + 6$. Thus the Eisenstein criterion applies with $p = 3$ to give us the irreducibility of g(x). By the remark in Problem 1 we get that f(x) is irreducible in Q[x].

5. Let $g(x) = f(x + 1) = (x + 1)^{p-1} + (x + 1)^p + \ldots + (x + 1) + 1 = [(x + 1)^p - 1)]/[(x + 1) - 1)] = [(x + 1)^p - 1)]/x = x^{p-1} + px^{p-2} + \ldots + p!/i!(p-i)!x^{i-i} + \ldots + [p(p - 1)2]x + p$. Since all the coefficients except the first are divisible by p, and the last coefficient is not divisible by p^2, by the Eisenstein Criterion g(x) is irreducible in Q[x]. Thus by the above, f(x) is irreducible in Q[x].

7. That $\varphi(a) = a$ for every a in F is clear. Also $\varphi(f(x) + g(x)) = f(x + 1) + g(x + 1) = \varphi(f(x)) + \varphi(g(x))$, and similarly, $\varphi(f(x)g(x)) = \varphi(f(x))\varphi(g(x))$. Also φ is onto since $f(x) = \varphi(f(x - 1))$. Thus φ is a homomorphism of F[x] onto itself. Also if f(x) is in Ker φ then $f(x + 1) = 0$, which implies that $f(x) = 0$. Thus φ is an automorphism of F[x].

10. We solve this problem as a consequence of Problem 11. Since every automorphism φ of F[x] leaving each element of F fixed is of the form $\varphi(f(x)) = f(bx + c)$ for $b \neq 0$, c in F it is immediate that deg $\varphi(f(x))$ = deg f(x).

11. Suppose that φ is an automorphism of F[x] such that $\varphi(a) = a$ for every a in F. We claim that $\varphi(x) = bx + c$ for some $b \neq 0$ and c in F. If not, $\varphi(x)$ is of degree $m > 1$. But then $\varphi(a_0x^n + a_1x^{n-1} + \ldots + a_n) = a_0\varphi(x)^n +$

$a_1\varphi(x)^{n-1} + \ldots + a_n$ is of degree $mn > n$. Thus x, which is of degree 1, cannot be the image of any polynomial in F[x]. Thus we get that $\varphi(x) = bx + c$ for some $b \neq 0$ and c in F. But then, since $\varphi(a) = a$ for every a in F, $\varphi(f(x)) = f(\varphi(x)) = f(bx + c)$.

13. The only invertible elements in Q[x] are the elements of Q. If φ is an automorphism of Q[x] then $\varphi(a)$ is invertible if a is. Thus $\varphi(Q) \subset Q$. So φ induces an automorphism of Q. But any automorphism of Q must be the identity map. For $\varphi(1) = 1$ since φ is an automorphism. Therefore if $n > 0$ is an integer $\varphi(n) = \varphi(1 + 1 + \ldots + 1) = \varphi(1) + \varphi(1) + \ldots + \varphi(1) = 1 + 1 + \ldots + 1 = n$. Also $\varphi(-1) \neq \varphi(1)$ since φ is 1-1; but $(\varphi(-1))^2 = \varphi((-1)^2) = \varphi(1) = 1$. Thus $\varphi(-1) = -1$. From this we get that $\varphi(m) = m$ for all integers. If $r = m/n$ is rational (m and n integers) then $\varphi(r) = \varphi(m/n) = \varphi(m)/\varphi(n) = m/n = r$. So any automorphism of Q[x] automatically leaves every element of Q fixed.

SECTION 7.

Problems.

1. $([a, b] + [c, d]) + [e, f] = [ad + bc, bd] + [e, f] = [(ad + bc)f + bde, bdf] = [adf + bcf + bde, bdf]$, while $[a, b] + ([c, d] + [e, f]) = [a, b] + [cf + de, df] = [adf + b(cf + de), bdf] = [adf + bcf + bde, bdf]$. We thus see that the associative law of addition in F checks out.

4. If K is a field which contains D then K must contain all fractions a/b where a and $b \neq 0$ are in D. Since the set of all these fractions is precisely F, we get that $K \supset F$.