Math 450
Fall 2000
Solutions to selected problems

Page 21.

14. *Suppose that n is a fixed positive integer, greater than 1. For any integers i and j show that*

$$i \mod n + j \mod n = (i + j) \mod n.$$

Proof. Let $i \mod n = k$ and $j \mod n = \ell$. Then we need to show that

$$n|((i + j) - (k + \ell)).$$

By definition, we can write

$$i = qn + k \text{ and } j = sn + \ell.$$

We rewrite this as

$$k = i - qn \text{ and } \ell = j - sn.$$

Now

$$(i + j) - (k + \ell) = (i + j) - ((i - qn) + (j - sn)) = n(q + s),$$

is divisible by n, and this finishes the problem. □

18. *Let $p_1, p_2, \ldots, p_n$ be distinct primes. Show that $p_1 p_2 \ldots p_n + 1$ is divisible by none of these primes.*

Proof. Recall that $n|a$ if and only if $a = 0 \mod n$. Since each p_i is prime, $p_i > 1$. Let $a = p_1 \ldots p_n + 1$. Then each $p_i|(a - 1)$, so $a = 1 \mod p_i$, and since $p_i > 1$, we see that $a \neq 0 \mod p_i$, and this shows that $p_i \not| a$. □

19. *Show that there are infinitely many primes.*

Proof. We argue by contradiction. Suppose to the contrary that there are only finitely many primes. In particular, suppose that $p_1, \ldots, p_n$ constitute all the primes. Let $a = p_1 p_2 \ldots p_n + 1$. By problem 18 $p_i \not| a$ for each $1 \leq i \leq n$. Thus, a must be a prime different from $p_1, \ldots, p_n$. This contradicts our assumption that $p_1, \ldots, p_n$ were all the primes. Consequently, there are infinitely many primes. □

25. *The Fibonacci numbers are* $1, 1, 2, 3, 5, 8, 13, 21, 34...$, *defined by* $f_1 = 1 = f_2$ *and* $f_{n+2} = f_{n+1} + f_n$ *for* $n = 1, 2, 3...$ *Prove that* $f_n < 2^n$.

Proof. We use the second principal of induction. We first note that $f_1 = 1 < 2^1 = 2$, and $f_2 = 1 < 2^2 = 4$. Now suppose that for some $n + 2 \geq 3$ we know that $f_k < 2^k$ for all $1 \leq k < n + 2$. Then, $f_{n+2} = f_{n+1} + f_n$, and by our inductive hypothesis, since $n + 1$ and n are both less than $n + 2$, we have

$$f_{n+2} = f_{n+1} + f_n < 2^{n+1} + 2^n \leq 2^{n+1} + 2^{n+1} = 2(2^{n+1}) = 2^{n+2}.$$

Thus, the statement holds true for $n + 2$, and thus for all $n \geq 1$ by induction. □

.

Page 35.

7. *In* D_n *explain geometrically why a rotation followed by a rotation must be a rotation.*

Proof. Recall that rotations are those symmetries of the n-gon which do not change the orientation of the plane, or of the vertices, while reflections reverse the orientation of the vertices. Thus, the composition of two rotations preserves the orientation of the plane, and hence must be a rotation (since it cannot be a reflection).

To be more precise, let $v_1, v_2, \ldots, v_n$ be the vertices of the n-gon, labeled in the clockwise direction. Let R be a rotation in D_n. We think of R as a function from $\{v_1, \ldots, v_n\}$, to itself, and also a function from $\{1, 2, \ldots, n\}$ to itself. Then $R(v_{k+1}) = v_{R(k)+1(\mod n)}$, for $k = 1, 2, \ldots, n - 1$. On the other hand, if Φ is a reflection in D_n, then $\Phi(v_{k+1}) = v_{\Phi(k)-1(\mod n)}$for $k = 1, 2, \ldots, n$. Note that if R_1 and R_2 are rotations, then

$$R_2(R_1(v_{k+1})) = R_2(v_{R_1(k)+1(modn)}) = v_{R-2(R_1(k)+1)(\mod n)} = v_{R_2(R_1(k))+1(\mod n)}$$

and hence R_2R_1 is a rotation. □

9. *Associate the number* $+1$ *with a rotation, and the number* -1 *with a reflection. Describe the analogy between multiplying these two numbers and multiplying elements of* D_n.

Solution. Note that $1 \cdot 1 = 1$ just as the product of two rotations is a rotation. Also, $-1 \cdot 1 = -1 = 1 \cdot -1$, just as the composition of a reflection with a rotation is a reflection, and the composition of a rotation with a reflection is a reflection. Finally, note that $-1 \cdot -1 = 1$, just as the product of two reflections is a reflection. Thus, multiplying elements of $\{1, -1\}$ is analogous to the effect of multiplying elements of D_n. □

Page 51.

8. *Let a and b be elements of a group, and let $n \in \mathbb{Z}$. Show that $(a^{-1}ba)^n = a^{-1}b^n a$.*

Proof. Note that if $n = 1$, then we have $(a^{-1}ba)^1 = a^{-1}b^1a,$, i.e. the statement holds trivially for $n = 1$. Note that for $n = 2$, $(a^{-1}ba)^2 = (a^{-1}ba)(a^{-1}ba) = a^{-1}b(aa^{-1})ba = a^{-1}b^2a$. Thus the claim holds for $n = 2$. Suppose the claim holds for some $n \geq 2$. That is, assume that $(a^{-1}ba)^n = a^{-1}b^n a$. Note that $(a^{-1}ba)^{n+1} = (a^{-1}ba)^n(a^{-1}ba)$. Now, by assumption, $(a^{-1}ba)^n = a^{-1}b^n a$. Thus,

$$(a^{-1}ba)^{n+1} = (a^{-1}b^n a)(a^{-1}ba) = a^{-1}b^n(aa^{-1})ba = a^{-1}b^n eba = a^{-1}b^{n+1}a.$$

Thus, by induction, the claim holds for $n \geq 1$.

For $n = 0$, we have $a^{-1}b^0a = a^{-1}ea = e = (a^{-1}ba)^0$. Suppose $n < 0$. Then $-n > 0$, so by the above, $(a^{-1}ba)^{-n} = a^{-1}b^{-n}a$. Now,

$$(a^{-1}ba)^n = \left(\left(a^{-1}ba\right)^{-n}\right)^{-1} = (a^{-1}b^{-n}a)^{-1}.$$

Now show that $(a^{-1}b^{-n}a)^{-1} = a^{-1}b^n a$, and you're done. □

14. *Suppose that G is a group with the property that whenever $ab = ca$ we have $b = c$. Show that G is abelian.*

Proof. Let a and b be elements of G. Take $c = aba^{-1}$. Then $ca = aba^{-1}a = ab$. Since $ca = ab$, the hypothesis implies $c = b$, that is $aba^{-1} = b$. Now multiplying on the right by a, we get $ab = ba$ □

Page 65.

4. *Prove that in any group, an element and its inverse have the same order.*

Proof. Suppose a is of infinite order. If, for some $n > 0$, $(a^{-1})^n = e$, then $a^n = a^n e = a^n(a^{-1})^n = (aa^{-1})^n = e$, which contradicts our assumption on the order of a. Thus, a^{-1} is also of infinite order.

Now suppose $|a| = m$, and $|a^{-1}| = n$. If $m > n$, then we have $a^{m-n} = e$, with $m > m - n > 0$, which contradicts our assumption that $|a| = m$. Thus, $m \leq n$. Similarly, if $n > m$, then $(a^{-1})^{n-m} = e$, with $n > n - m > 0$, which contradicts our assumption that $|a^{-1}| = n$. Thus, $n \leq m$, so $n = m$ □

10. *Suppose that G is an abelian group with two elements of order two. Show that G has a subgroup of order four.*

Proof. Let $a, b \in G$ with $|a| = |b| = 2$. Then, since G is abelian, $ab = ba$. Furthermore $aba = aab = b$, and $abb = a$. Thus, the set $H = \{e, a, b, ab\}$ is closed under the group multiplication. Then, by the finite subgroup test, H must be a subgroup, and its order is four. □

14. *Let G be a group, and H and K subgroups of G. Show that $H \cap K$ is a subgroup of G,*

Proof. Note that since $e \in H$ and $e \in K$, we have $e \in H \cap K$, which shows that $H \cap K$ is nonempty. Now if $a, b \in H \cap K$, then since H is a subgroup $ab^{-1} \in H$. Similarly, since K is a subgroup, $ab^{-1} \in K$. Thus, if $a, b \in H \cap K$, then $ab^{-1} \in H \cap K$. Thus, by the ones step subgroup test, $H \cap K$ is a subgroup of G.

Page 79.

7. *Find an example of a noncyclic group, all of whose proper subgroups are cyclic.*

Solution. Let G be an abelian group of order 4, with elements $\{e, a, b, ab|\ |a| = |b| = 2\}$. Then the proper subgroups of G are: $H_1 = \{e, a\} =< a >$, $H_2 = \{e, b\} =< b >$, and $H_3 = \{e, ab\} =< ab >$. Note that, since the product of any two of a, b or ab is the third, that a subgroup with any two of a, b, and ab is equal to G. thus, all the proper subgroups of G are cyclic. On the other hand, G is not cyclic, since we see that $< a >$, $< b >$, and $< ab >$ are all proper subgroups of G. □

11. *Let G be a group and $a \in G$. Show that $< a >=< a^{-1} >$.*

Proof. Since $a \in< a >$, and $< a >$ is a subgroup, we have $a^{-1} \in< a >$. Thus, $< a^{-1} > \subset< a >$. Similarly, $a = (a^{-1})^{-1} \in< a^{-1} >$, so $< a > \subset< a^{-1} >$. Therefore $< a >=< a^{-1} >$. □

16. *If a cyclic group has an element of infinite order, how many elements of finite order does it have?*

Solution. Since $|e| = 1$, there is at least one element of G of finite order. Let $G =< a >$. Since G has an element of infinite order, a^k is of infinite order for some $k \neq 0$. Since $|b| = |b^{-1}|$, (problem 4 on pg. 63), we can assume that $k > 0$. Since a^k is of infinite order, Theorem 4.1 says that all the powers of a^k are distinct, i.e., if $m \neq n$, then $a^{kn} \neq a^{km}$. Therefore $< a^k >$ is an infinite cyclic group, and thus G is an infinite group. Suppose a^j is an element of finite order, for some $j \neq 0$. Then $(a^j)^n = e$, and therefore, $a^{jn} = e$. By the Corollary to Theorem 4.1, the order of a divides jn. Thus $|a| = \ell$ for some $\ell < \infty$. But, if $|a| = \ell$, then $G =< a >= \{e, a, a^2, \ldots, a^{\ell-1}\}$ is a finite group. This contradicts our assumption that G has an element of infinite order. Therefore, a^j is of infinite order for every $j \neq 0$, and therefore e is the only element of G of finite order.

Alternate proof that a^j has infinite order for $j \neq 0$.. Suppose $|a^j| = n$. Then $a^{jn} = e$, and thus $(a^k)^{jn} = a^{kjn} = (a^{jn})^k = e^k = e$. Therefore, by the Corollary to Theorem 4.1, $|a^k|$ divides jn. This contradicts our assumption that a^k has infinite order. □

38. *Let m and n be elements of $\mathbb{Z}$. Find a generator for the group* $< m > \cap < n >$.

Solution. Recall that $< m >= \{0, \pm m, \pm 2m, \dots\}$, i.e. $< m >$ is the set of multiples of m. Similarly, $< n >$ is the set of multiples of n. Thus, $< m > \cap < n >$ is the set of all integers which are multiples of both m and n, i.e., the set of all common multiples of m and n. In Chapter 0, we showed that any common multiple of m and n, is a multiple of the least common multiple, $lcm(m, n)$. So, $< m > \cap < n >=< lcm(m, n) >$. □

Page 107.

7. *Show that A_8 contains an element of order 15.*

Proof. Recall that a 3-cycle $(abc) = (ab)(ac)$ is even, and a 5-cycle $(abcxy) = (ab)(ac)(ax)(ay)$ is even. So $(123) \in A_8$ and $(45678) \in A_8$. Therefore, $\alpha = (123)(45678) \in A_8$. Since (123) and (45678) are disjoint, Ruffini's theorem says that $|\alpha| = 15$. □

12. *If α is even prove that α^{-1} is even. If α is odd, prove that α^{-1} is odd.*

Proof. . Suppose that α is even. Then we can write

$$\alpha = \alpha_1 \alpha_2 \dots \alpha_{2n}$$

with each a transposition. Then $\alpha_i^{-1} = \alpha_i$ for each $1 \leq i \leq 2n$, and thus

$$\alpha^{-1} = \alpha_{2n}^{-1} \alpha_{2n-1}^{-1} \dots \alpha_2^{-1} \alpha_1^{-1} = \alpha_{2n} \alpha_{2n-1} \dots \alpha_2 \alpha_1.$$

Thus, since α^{-1} can be written as a product of an even number of transpositions, α^{-1}n is even.

Now suppose that α is odd. If α^{-1} is even, then by the above, $(\alpha^{-1})^{-1} = \alpha$ is even, which it is not. Thus, α^{-1} is odd. □

31. *Let G be a group of permutations on a set X. Let $a \in X$, and define* $\text{stab}(a) = \{\alpha \in G | \alpha(a) = a\}$. *We call* $\text{stab}(a)$ *the stabilizer of a in G. Prove that* $\text{stab}(a)$ *is a subgroup of G.*

Proof. We will use the two step subgroup test. First note that $\text{stab}(a)$ is non-empty. If ε is the identity permutation on X, then, by definition, $\varepsilon(x) = x$ for all $x \in X$. In particular, $\varepsilon(a) = a$, and hence, $\varepsilon \in \text{stab}(a)$. Therefore, $\text{stab}(a)$ is non-empty. Now we need to show that if $\alpha, \beta \in \text{stab}(a)$, then $\alpha\beta$ and $\alpha^{-1} \in \text{stab}(a)$. First note that $\alpha\beta(a) = \alpha(\beta(a))$. Since $\beta \in \text{stab}(a)$, we know that $\beta(a) = a$. Therefore, $\alpha\beta(a) = \alpha(a) = a$, since $\alpha \in \text{stab}(a)$. Consequently, $\text{stab}(a)$ is closed under the group operation in G. Next suppose $\alpha(a) = a$. Then, by multiplying by α^{-1} on each side, i.e., applying the function α^{-1} to each side, we see that $\alpha^{-1}(\alpha(a)) = \alpha^{-1}(a)$, and thus, $\alpha^{-1}\alpha(a) = \varepsilon(a) = a = \alpha^{-1}(a)$. We conclude that if $\alpha \in \text{stab}(a)$, then $\alpha^{-1} \in \text{stab}(a)$. This completes the proof. □

40. *Prove S_n is non-abelian for all $n \geq 3$.*

Proof. Look at the two cycles $\alpha = (12)$ and $\beta = (23)$. (Note that these two elements are in S_n for all $n \geq 3$.) We have $\alpha\beta = (132)$ and $\beta\alpha = (123)$. Since $\alpha\beta \neq \beta\alpha$, we see that S_n is non-abelian. □

45. *Show that every element of A_n for $n \geq 3$ can be expressed as a product of 3-cycles.*

Proof. Let $\alpha \in A_n$. Then we know that, for some even positive integer $2n$, and some 2-cycles $\beta_1, \ldots, \beta_{2n}$, we have $\alpha = \beta_1\beta_2 \ldots \beta_{2n}$. We use the associative law to write this as $\alpha = (\beta_1\beta_2)(\beta_3\beta_4)\ldots(\beta_{2n-1}\beta_{2n})$. We see that it is enough to show that any product of two 2-cycles can be written as a product of 3-cycles.

Now let $\beta = (ab)$ and $\gamma = (cd)$ be 2-cycles. We consider three cases. If $a = c$ and $b = d$, then $\beta = \gamma$, and $\beta\gamma$ is the identity ε. Since $\varepsilon = (123)(132)$, we know that $\beta\gamma$ is a product of 3-cycles. If $a = c$ and $b \neq d$, then $\beta\gamma = (ab)(ad) = (abd)$, which is a 3-cycle. Therefore, in this case $\beta\gamma$ is a product of 3-cycles. Finally, suppose that β and γ are disjoint. Then $\beta\gamma = (ab)(cd) = (abc)(cad)$ is the product of two 3-cycles. Thus, we have shown that any $\alpha \in A_n$ is a product of 3-cycles. □

Page 126.

6. *Prove that the relation isomorphism is an equivalence relation.*

Proof. We need to show that $\cong$ is reflexive, symmetric, and transitive.
Reflexive: We need to show that $G \cong G$, for any group G. Let $\varphi : G \longrightarrow G$ be the map given by $\varphi(x) = x$. Then φ is clearly one-to-one and onto. Moreover, $\varphi(xy) = xy = \varphi(x)\varphi(y)$, so φ is an isomorphism. Thus $G \cong G$.
Symmetric: We need to show that if $G \cong H$, then $H \cong G$. If $\varphi : G \longrightarrow H$ is an isomorphism, then $\varphi^{-1} : H \longrightarrow G$ is both one to one and onto. Suppose $x, y \in H$. Recall that $\varphi^{-1}(x)$ is the unique element g of G with $\varphi(g) = x$. Similarly, let $s = \varphi^{-1}(y)$. Note that $\varphi(gs) = \varphi(g)\varphi(s) = xy$, since φ is an isomorphism. Therefore, $\varphi^{-1}(xy) = gs = \varphi^{-1}(x)\varphi^{-1}(y)$. Consequently, $\varphi^{-1} : H \longrightarrow G$ is an isomorphism. Thus, $G \cong H$ implies $H \cong G$.
Transitive: We need to show that if $G \cong H$ and $H \cong K$, then $G \cong K$. Let $\varphi : G \longrightarrow H$ and $\psi : H \longrightarrow K$ be isomorphisms. By Theorem 0.3, $\psi\varphi : G \longrightarrow K$ is both one-to-one and onto. Suppose $x, y \in G$. Then $\psi\varphi(xy) = \psi(\varphi(xy))$, and since φ is an isomorphism we have $\psi\varphi(xy) = \psi(\varphi(x)\varphi(y))$. Note that $\varphi(x)$ and $\varphi(y)$ are elements of H, and ψ is an isomorphism. Thus, $\psi(\varphi(x)\varphi(y)) = \psi(\varphi(x))\psi(\varphi(y)) = \psi\varphi(x)\psi\varphi(y)$. Therefore, $\psi\varphi$ is an isomorphism, and $G \cong K$. We have shown that $\cong$ is an equivalence relation. □

7. *Prove that S_4 is not isomorphic to D_{12}.*

Proof. Note that both groups are of order 24. In S_4, the values for the order of an element are 1, 2, 3, or 4. However, the element R_{30} of D_{12} has order 12. Thus, by property 5 of Theorem 6.1, D_{12} cannot be isomorphic to S_4. □

16. *Let $r \in U(n)$. Prove that the mapping $\alpha : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$ defined by $\alpha(s) = sr$ for all $s \in \mathbb{Z}_n$ is an automorphism of $\mathbb{Z}_n$.*

Proof. We need to to show that α is one-to-one, onto, and preserves the group operation in $\mathbb{Z}_n$. We begin by showing that α is onto. That is, we intend to show that, for each $y \in \mathbb{Z}_n$, there is an $s \in \mathbb{Z}_n$ with $\alpha(s) = y$. Since $r \in U(n)$, we know that $gcd(n, r) = 1$, and therefore the equation $xr = 1 (\text{mod } n)$ is solvable. So, for some $x \in \mathbb{Z}_n$, $\alpha(x) = 1$. Let $s = yx$. Then $\alpha(s) = sr = (yx)r = y(xr) = y(\text{ mod } n)$. Thus, we know that α is onto. Since α is an onto function from $\mathbb{Z}_n$ to itself, α is one-to-one. (A direct proof that α is one-to-one is as follows: If $\alpha(s) = \alpha(t)$, then $sr = tr \ (\text{mod } n)$. Thus, $n|r(s - t)$, and, since $gcd(n, r) = 1$, $n|(s - t)$. Thus, $s = t$.)

We finally need to show that α preserves the group operation. Let $s, t \in \mathbb{Z}_n$. Then $\alpha(s + t) = (s + t)r = sr + tr = \alpha(s) + \alpha(t) \ (\text{mod } n)$. Thus, α is an isomorphism. □

30. *Suppose that G is a finite abelian group which has no element of order 2. Show that the mapping $g \mapsto g^2$ is an automorphism of G. Show by example that if G is infinite the mapping need not be an automorphism.*

Proof. Let $\psi : G \longrightarrow G$ be given by $\psi(g) = g^2$. Note that since G is abelian,if $g, h \in G$ then $\psi(gh) = (gh)^2 = g^2h^2 = \psi(g)\psi(h)$. Thus, we need only show ψ is 1-1 and onto. Since $G$is finite, it is enough to show that ψ is 1-1. Suppose that $\psi(g) = p(h)$. Then $g^2 = h^2$, which says $g^2h^{-2} = (gh^{-1})^2 = e$. By assumption, G has no elements of order 2. Thus, since $|gh^{-1}|$ divides 2, we must have $gh^{-1} = e$, which says $g = h$. Thus, ψ is 1-1, and hence also onto. Therefore, ψ is an automorphism.

Note that if $G = \mathbb{Z}$, the the map is $n \mapsto 2n$, which is not onto, and hence cannot be an automorphism. □

Page 142.

6. *Let n be an integer greater than 1. Let $H = \{0, \pm n, \pm 2n, \pm 3n, \dots\}$. Find all the left cosets of H in $\mathbb{Z}$. How many of them are there?*

Solution. Suppose $a + H = b + H$. Then $b - a \in H$, which is equivalent to $n|(b - a)$. Thus $a + H = b + H$ if and only if $a = b \mod n$. Thus the left cosets of H in $\mathbb{Z}$ are $0 + H, 1 + H, \dots, (n - 1) + H$, and hence there are n of them. □

22. *Suppose that G is a group with more than one element, and G has no proper, nontrivial subgroup. Prove that $|G|$ is prime.*

Proof. Let $a \in G$, with $a \neq e$. Then $< a >$ is a nontrivial subgroup of G. Thus, by our hypothesis, $G =< a >$. If $|a|$ is infinite, then $G \simeq \mathbb{Z}$ (see Example 2 of Chapter 6). Then $< a^2 >$ is a proper, nontrivial subgroup of G, which contradicts our assumption. Thus, $|a|$ must be finite. Now, G is a finite cyclic group. If d divides $|G|$, then, by the Fundamental Theorem of Cyclic Groups, there is a cyclic subgroup of G of order d. Since G and $\{e\}$ are the only subgroups of G, we see that $|G|$ can have no proper divisors, i.e., $|G|$ must be prime. □

38. *Let G be the group of plane rotations about a point P in the plane. Describe the orbit of a point Q in the plane.*

Solution. Note that if Q' is in the orbit of Q, then there is a rotation of the plane about P, say $R_{\theta,P}$ of angle θ so that $R_{\theta,P}(Q) = Q'$ Thus Q' lies on the circle $C(P, |P-Q|)$ with center P and radius $|P - Q|$. On the other hand, if Q' is a point on $C(P, |P - Q|)$, then there us a well defined angle $\theta = \angle QPQ'$. Thus, $Q' = R_{\theta,P}(Q)$, hence is in the orbit of Q.

Thus, $\text{orb}(Q) = C(P, |P - Q|)$, i.e., the orbit of Q is the circle of elements whose distance from P is the same as that of Q form P. □

43. *if G is a group with fewer than* 100 *elements and G has subgroups of orders* 10 *and* 25, *what is $|G|$?*

Solution. Since G has a subgroup of order 25, we know 25 divides $|G|$. Similarly 10 divides $|G|$. Thus, 2 divides $|G|$ and 25 divides $|G|$. Since $gcd(2, 25) = 1$, we have 50 divides $|G|$. Since $|G| < 100$, we must have $|G| = 50$. □

Page 161.

6. *Prove, by comparing the orders of elements, that $\mathbb{Z}_8 \oplus \mathbb{Z}_2$ and $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ are not isomorphic.*

Proof. Note that $(1, 0)$ has order 8 in $\mathbb{Z}_8 \oplus \mathbb{Z}_2$. On the other hand, if $(a, b) \in \mathbb{Z}_4 \oplus \mathbb{Z}_4$, then $|a|$ and $|b|$ both divide 4, and hence their least common multiple also divides 4. therefore, $|(a, b)| = 1, 2$, or 4. Thus, $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ has no element of order 8, and hence cannot be isomorphic to $\mathbb{Z}_8 \oplus \mathbb{Z}_2$. □

12. *The dihedral group D_n of order $2n$ has a subgroup of n rotations and a subgroup of order* 2. *Explain why D_n cannot be isomorphic to the external direct product of two such groups.*

Explanation. Note that both of these subgroups are abelian, and hence their external direct product is abelian. On the other hand D_n is non-abelian, and hence cannot be isomorphic to the external direct product of the two given groups. □

33. *Prove that* $D_3 \oplus D_4 \ncong D_{12}$.

Proof. Note that in D_{12} the only elements of order 4 are the rotations R_{90} and R_{270}, thus there are two such elements. (equivalently, the only cyclic subgroups of order 4 are subgroups of $< R_{30} >$ and hence there is a unique one.) However in $D_3 \oplus D_4$ an element (a, b) has order four if $|a| = 1, 2$ and $|b| = 4$. Since there are 4 choices for a and 2 for b, there are 8 elements of order 4 in $D_3 \oplus D_4$. Thus, $D_{12} \ncong D_3 \oplus D_4$. □

40. *Express* $U(165)$ *as an external direct product of cyclic additive groups of the form* $\mathbb{Z}_n$.

Solution. Since $165 = 3 \cdot 5 \cdot 11$, we know that

$$U(165) = U(3) \oplus U(5) \oplus U(11) \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{10}. \quad \square$$

38. *The group* $\mathbb{Z}_2 \oplus D_3$ *is isomorphic to one of the following* $\mathbb{Z}_{12}, \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3, A_4, D_6$. *Determine which one.*

Proof. Since $\mathbb{Z}_{12}$ and $Z_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$ are abelian $\mathbb{Z}_2 \oplus D_3$ cannot be isomorphic to either of these. Since A_4 has no element of order 6, (8 elements of order 3, 3 of order 2 and 1 of order 1), and $\mathbb{Z}_2 \oplus D_3$ does, we must have $\mathbb{Z}_2 \oplus D_3 \simeq D_6$. □

50. *Show that* $U(55)^3 = \{x^3 | x \in U(50)\} = U(55)$.

Proof. Since $U(55) \simeq U(11) \oplus U(5)$, we have $U(55) \simeq \mathbb{Z}_{10} \oplus \mathbb{Z}_4$, so it is enough to prove that $\{(a, b)^3 | (a, b) \in \mathbb{Z}_{10} \oplus \mathbb{Z}_4\} = \mathbb{Z}_{10} \oplus \mathbb{Z}_4$. But $(a, b)^3 = (3a \mod 10, 3b \mod 4)$, and by Page 127 problem 16, multiplication by 3 is an isomorphism of both $\mathbb{Z}_1 0$ and $\mathbb{Z}_4$. Hence $x \mapsto x^3$ is one-to-one, and thus also onto. □

Page 185.

4. *Let* $H = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \middle| a, d \neq 0, b \in \mathbb{R} \right\}$. *Is* H *a normal subgroup of* $GL(2, \mathbb{R})$?

Solution. No. Recall that H is normal in G if $aHa^{-1} = H$, for all $a \in G$. Let $h = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \in H$. Let $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Then $A^{-1} = A$, and

$$AhA^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \notin H.$$

Thus, H is not normal in $GL(2, \mathbb{R})$. □

30. *Prove that D_4 cannot be expressed ass the internal direct product of two proper subgroups.*

Proof. Note that the only proper normal subgroups of D_4 have order 2 and order 4. Thus, if $D_4 = H \times K$, for some H and K, we would have $D_4 \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_4$ or $D_4 \simeq \mathbb{Z}_2 \oplus (\mathbb{Z}_2 \oplus \_2)$, both of which imply D_4 is abelian, which is a contradiction.

Alternative proof. Note that $< R_{180} >$ is a subgroup of every order 4 subgroup of D_4 and $< R_{180} >$ is the unique normal subgroup of order 2. Thus, we cannot find $HK = G$, H, K normal, and $H \cap K = \{e\}$. □

Page 204.

26. *Suppose that $\varphi : G \longrightarrow \mathbb{Z}_6 \oplus \mathbb{Z}_2$, is onto and $|\ker \varphi| = 5$. Explain why G must have normal subgroups of orders $5, 10, 15, 10, 30,$ and 60.*

Explanation. Recall that if $K \subset Z_6 \oplus \mathbb{Z}_2$ is a subgroup, then $K \triangleleft \mathbb{Z}_6 \oplus \mathbb{Z}_2$ (since $\mathbb{Z}_6 \oplus \mathbb{Z}_2$ is abelian). Since φ is onto, $\varphi^{-1}(K) = \{g \in G | \varphi(g) \in K\}$ is normal in G (Theorem 10.1) Since $\ker \varphi$ is of order 5, part 10 of Theorem 10.1 implies that $|\varphi^{-1}(K)| = 5|K|$. Since the possible orders for K are $1, 2, 3, 4, 6$, and 12, we see that G has normal subgroups of order $5, 10, 15, 20, 30$, and 60. □

40. *Let N be a normal subgroup of a finite group G. Use the results of this chapter to prove that $|gN|$ divides $|g|$.*

Proof. Let $\psi : G \to G/N$ be given by $\psi(g) = gN$. Then ψ is a homomorphism (why) and so $|\psi(g)|$ divides $|g|$. thus immediately gives the result. □

47. *Use the First Isomorphism Theorem to prove Theorem 9.4.*

Proof. Theorem 9.4 is states that for any group G, we have $G/Z(G) \simeq Inn(G)$. Let $\psi : G \longrightarrow Inn(G)$ be given by $\psi(x) = \phi_x$, where $phi_x(g) = xgx^{-1}$. Then ψ is an onto homomorphism (prove this!) and $x \in \ker \psi$ if and only if ϕ_x is the identity map, i.e., if and only if $xgx^{-1} = g$, for all $g \in G$. This is clearly equivalent to $xg = gx$ for all $g \in G$, i.e., $\ker \psi = Z(G)$. Thus, by the First Isomorphism Theorem, $G/Z(G) \simeq Inn(G)$. □

page 217.

8. *Show there are two abelian groups of order 108 with exactly 13 subgroups of order 3.*

Proof. Since $108 = 2^2 3^3$, we know that any abelian group G of order 108 is of the form $H \oplus K$, with $|H| = 4$ and $|K| = 27$. We need to determine when there are exactly 26 elements of order 3. Nothe that if $(h, k) \in H \oplus K$, and if h is not the identity of H, then 2 divides the order of h, and hence divides the order of (h, k). Thus, an element of order 3

is of the form $(1_H, k)$, with $k \in K$. We know that K is isomorphic to one of the following groups: $\mathbb{Z}_{27}, \mathbb{Z}_3 \oplus \mathbb{Z}_9$, or $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$. Obnly in this last case does K have 26 elements of order 3, and hence exaclty 13 subgroups of order three. Thus, there are exactly two candidates for G, namely

$$G_1 \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3,$$

and

$$G_2 \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3. \square$$

32. *Let G be a finite abelian group and let a be an element of maximal order. Prove that if $b \in G$, then $|b|$ divides $|a|$.*

Proof. Let $|b| = p_1^{n_1} \dots p_k^{n_k}$, with the p_i distinct prime factors. Suppose that, for some i, we have $p_i \not| \, |a|$. Then $c = b^{|b|/p_i}$ has order p_i, which is relatively prime to $|a|$, so $|ac| = p_i|a| > |a|$, contradicting our choice of a. Now we see each p_i divides $|a|$. Suppose p^k is the largest power of a prime dividing $|b|$, and p^m is the corresponding power dividing $|a|$. Then if $k > m$, we take $c = a^{p^m}$ and $d = b^{|b|/p^k}$, then their orders are relatively prime and so $|cd| = |c||d| = (|a|/p^m)p^k = |a|p^{k-m} > |a|$, again contradicting our choice of a. Thus, $k \leq m$, and this now shows $|b|$ divides $|a|$. $\square$

Page 231.

9. *Show that a ring that is cyclic under addition is commutative.*

Proof. By assumption there is some $r \in R$, with $R = \{m \cdot r \,|m \in \mathbb{Z}\}$. Note that $(m \cdot r)(n \cdot r) = (mn) \cdot r^2 = (nm) \cdot r^2 = (n \cdot r)(m \cdot r)$. Thus R is commutative. $\square$

18. *Let R be a ring and $a \in R$. Set $S = \{x \in R | ax = 0\}$. Show that S is a subring of R.*

Proof. Note that $0 \in S$, since $a0 = 0$, so $S \neq \emptyset$. Further note that if $x, y \in S$, then $a(x-y) = ax-ay = 0-0 = 0$, and thus $x-y \in S$. Finally note that $a(xy) = (ax)y = 0y = 0$, and thus, $xy \in S$. Therefore, S is a subring of R.

23. *Determine $U(\mathbb{Z}[i])$.*

Proof. Let $a + bi \in \mathbb{Z}[i]$ be a unit. Then $(a + bi)(c + di) = 1$, for some $c, d \in \mathbb{Z}$. Since $\mathbb{Z}[i] \subset \mathbb{C}$ is a subring, we know that the inverse $c + di$ of $a + bi$ is also its inverse in $\mathbb{C}$. But,if $(a + bi) \neq 0$, then its $\mathbb{C}$–inverse is

$$(a + bi)^{-1} = \frac{(a - bi)}{a^2 + b^2}.$$

Thus, $a+bi$ is a unit if and only if $a/(a^2+b^2)$ and b/a^2+b^2 are integers. If both a and b are non-zero, then $a^2+b^2 > |a|, |b|$, so the above rationals are not integers. Now it is easy to see that $U(\mathbb{Z}[i]) = \{1, -1, i, -i\} \simeq \mathbb{Z}_4$. □

44. *Let R be a ring with unity e. Show that $S = \{ne | n \in \mathbb{Z}\}$ is a subring of R.*

Proof. Note $e \in S$, so S is not empty. Let $m, n \in \mathbb{Z}$. Then $me - ne = (m-n)e \in S$. Also $(me)(ne) = (mn)e \in S$, so S is a subring. □

Page 243.

11. *Give an example of a commutative ring without zero divisors that is not an integral domain.*

Solution. Since an integral domain is a commutative ring with unity and no zero divisors, such a ring must fail to have a unity. Let $R = 2\mathbb{Z}$. Then R has no zero divisors, but is not an integral domain.

19. *Find the isomorphism class of the group of units of $\mathbb{Z}_5[i]$.*

Proof. We know that $U(5) = U(\mathbb{Z}_5) = \{1, 2, 3, 4\}$. Thus, $1, 2, 3, 4$ are units of $\mathbb{Z}_5[i]$. Now, suppose that $a + bi \in \mathbb{Z}_5[i]$. Then $(a+bi)(a-bi) = a^2 + b^2 (\mod 5)$. If $a^2 + b^2 \neq 0 \mod 5$, then $a^2 + b^2$ is invertible in $\mathbb{Z}_5$, and hence $(a^2+b^2)c = 1$, for some $c \in \mathbb{Z}_5$. Thus, $(a+bi)((a-bi)c) = 1$, i.e. $(a-bi)c = (a+bi)^{-1}$, so $a + bi \in U(\mathbb{Z}_5[i])$. On the other hand, suppose $a^2 + b^2 = 0 \mod 5$. If $a + bi$ is invertible, then

$$(a-bi) = (a-bi)((a+bi)(a+bi)^{-1}) = (a^2+b^2)(a+bi)^{-1} = 0 \cdot (a+bi)^{-1} = 0.$$

Thus, $a = 0$, and $-b = 0$, which shows $a+bi = 0$, which clearly contradicts the invertibility of $a + bi$. Thus, if $a^2 + b^2 = 0 \mod 5$, then $a + bi$ is not a unit. Thus, we have shown that $U(\mathbb{Z}_5[i]) = \{a + bi | a^2 + b^2 \neq 0 \mod 5\}$. By inspection, we see that

$$U(\mathbb{Z}_5[i]) = \{1, 2, 3, 4, i, 2i, 3i, 4i, 1+i, 1+4i, 2+2i, 2+3i, 3+2i, 3+3i, 4+i, 4+4i\}.$$

Since $|U(\mathbb{Z}_5[i])| = 16$, and $U(\mathbb{Z}_5[i])$ is abelian, we know that $U(\mathbb{Z}_5[i])$ is one of the following groups: $\mathbb{Z}_1 6, \mathbb{Z}_8 \oplus \mathbb{Z}_2, \mathbb{Z}_4 \oplus \mathbb{Z}_4, \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, or $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Consider the following table:

GROUP	No. elts of order 2	No. elements of order 4
$\mathbb{Z}_{16}$	1	2
$\mathbb{Z}_8 \oplus \mathbb{Z}_2$	3	4
$\mathbb{Z}_4 \oplus \mathbb{Z}_4$	3	12
$\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$	8	7
$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$	15	0

and look at the order of the elements of our group:

x	1	2	3	4	i	$2i$	$3i$	$4i$	$1+i$	$1+4i$	$2+2i$	$2+3i$	$3+2i$
order of x	1	4	4	2	4	2	2	4	4	4	4	4	4

. Since $U(\mathbb{Z}_5[i])$ has at least 9 elements of order 4, we see that $U(\mathbb{Z}_5[i]) \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_4$. □

34. *Construct a multiplication table for* $\mathbb{Z}_2[i]$, *the ring of Gaussian integers modulo* 2. *Is this ring a field? Is it an integral domain?*

Solution.

$\cdot$	0	1	i	$1+i$
0	0	0	0	0
1	0	1	i	$1+i$
i	0	i	1	$1+i$
$1+i$	0	$1+i$	$1+i$	0

Note that $1+i$ has no multiplicative inverse, and thus $\mathbb{Z}_2[i]$ is not a field. Also, $(1+i)(1+i) = 0$, so, $\mathbb{Z}_2[i]$ is not an integral domain. □

Page 255.

2. *Find a subring of* $\mathbb{Z} \oplus \mathbb{Z}$ *which is not an ideal of* $\mathbb{Z} \oplus \mathbb{Z}$.

Solution. Let $S = \{(n,n) | n \in \mathbb{Z}\}$. Then S is a subring of $\mathbb{Z} \oplus \mathbb{Z}$. However, note that $(1,1) \in S$, and $(2,7) \cdot (1,1) = (2,7) \notin S$. Therefore, S is not an ideal. □

48. *Show that* $\mathbb{Z}[i]/ < 1-i >$ *is a field. How many elements does this field have?*

We give two proofs. The first is the one given in class.

Proof 1. We know that it is enough to prove that $< 1-i >$ is a maximal ideal. Note that $(1-i)^2 = -2i \in < 1-i >$, and therefore, $2 = i(-2i) \in < 1-i >$. Now, suppose

that B is an ideal of $\mathbb{Z}[i]$ with $B \supsetneq < 1-i >$. We need to show that $B = \mathbb{Z}[i]$. Let $a+bi \in B$ with $a+bi \notin < 1-i >$. Note that we can write $a+bi = a(1-i)+(a+b)i$. Since $a(1-i) \in < 1-i > \subset B$ and $a+bi \in B$, we have $(a+b)i = a+bi-a(1-i) \in B$. We claim that $a+b$ is odd. Suppose to the contrary that $a+b$ is even. Then $(a+b)i = 2(ki)$ for some $k \in \mathbb{Z}$, and since $2 \in < 1-i > (a+b)i \in < 1+i >$ and then $a+bi = a(1-i)+(a+b)i \in < 1-i >$, which contradicts our choice of $a+bi$. Thus, we have substantiated our claim that $a+b$ is odd. Write $a+b = 2k+1$ for some integer k. Note that we know that $2ki \in < 1-i >$ and $(a+b)i = (2k+1)i \in B$. Thus, since B is an ideal

$$1 = -i\left((2k+1)\,i - 2ki\right) \in B.$$

Thus, $B \supset < 1 >= Z[i]$, which implies $B = \mathbb{Z}[i]$, and thus $< 1-i >$ is maximal. Consequently, $\mathbb{Z}[i]/ < 1-i >$ is a field.

Note that if $a+bi \in \mathbb{Z}[i]$, then $a = 2k+\varepsilon$ and $b = 2j+\delta$, with $\varepsilon, \delta \in \{0,1\}$. Thus,

$$a+bi+ < 1-i >= (\varepsilon + \dot{\imath}) + (2k+2ji)+ < 1-i >= \varepsilon + \dot{\imath}+ < 1-i >,$$

since 2 and $2i$ are elements of $< 1-i >$. Thus, every element of $\mathbb{Z}[i]/ < 1-i >$ is of the form $\varepsilon+\dot{\imath}+ < 1-i >$. However, these are not distinct.Note that $1+ < 1-i >= i+ < 1-i >$ and, since $1+i = i(1-i)$ we have $1+i+ < 1-i >=< 1-i >$. Thus, there are two elements of $\mathbb{Z}[i]/ < 1-i >$, namely, $< 1-i >$ and $1+ < 1-i >$. □

Proof 2:. We start again by noting that $2, 2i \in < 1-i >$. and thus if $a+bi \notin < 1-i >$ then $a+b$ is odd. Now suppose that $a+bi+ < 1-i > \neq < 1-i >$. Then, in the factor ring

$$(a+bi+ < 1-i >)^2 = a^2 - b^2 + 2abi+ < 1-i >= a^2-b^2+ < 1-i >,$$

since $2abi \in < 1-i >$. But now, $(a^2-b^2) = (a+b)(a-b)$ is odd, so

$$(a^2-b^2)+ < 1-i >= 1+ < 1-i >,$$

which is the identity of $\mathbb{Z}[i]/ < 1-i >$. Thus, for every non-zero element $x \in \mathbb{Z}[i]/ < 1-i >$, we see $x^2 = 1+ < 1-i >$, and thus x is invertible. Therefore, $\mathbb{Z}[i]/ < 1-i >$ is a field. The counting argument is then as in Proof 1. □

Page 277.

51. *Suppose that $\phi : R \longrightarrow S$ is a ring homomorphism and that the inage if ϕ is not $\{0_S\}$. If R has a unity and S is an integral domain, show that ϕ carries the unity of R to the unity of S.*

Proof. Let 1_R be the identity of R. Choose $r \in R$ with $y = \phi(r) \neq 0$. Now

$$y = \phi(r) = \phi(1_R r) = \phi(1_R)\phi(r) = \phi(1_R)y.$$

Thus $y(1_S - \phi(1_R)) = 0$. Since S is an integral domain, and $y \neq 0$, we have $\phi(1_R) = 1_S$, proving ther claim.

For a counterexample in the case where S is not an integral domain, let $R = S = \mathbb{Z}_2[i]$. Then the map $\phi : \alpha \mapsto \alpha i$ is a ring homomorphism (prove this!!) with $\phi(1) = i$. □

Page 288.

22. *Prove that $\mathbb{Z}[x]$ is not a proncipal ideal domain.*

Proof. We need to show there is an ideal I so that I is not principal, i.e., $I \neq < f(x) >$ for any $f(x) \in \mathbb{Z}[x]$. Let $I =< x, 2 >= \{xf(x) + 2g(x) | f(x), g(x) \in \mathbb{Z}[x]$. Note that $I = \{f | f(0) \in 2\mathbb{Z}\} \subsetneq \mathbb{Z}[x]$. Now,if $I =< f(x) >$, then $f(x)|x$ and $f(x)|2$. But their only common divisor is 1. However, $< 1 >= \mathbb{Z}[x] \neq I$. Thus, I is not principal and hence $\mathbb{Z}[x]$ is not a principal ideal domain. □