Math 3110 # Suggested Homework **Updated Spring 2022**

Note: I used an automated tool to LaTeX-ify these problems. Beware of typos! If you spot one, please let me know. Thanks.

Chapter 0:

1) For $n = 5, 8, 12, 20$, and 25, find all positive integers less than n and relatively prime to n.

2) Determine $51 \bmod 13$, $342 \bmod 85$, $62 \bmod 15$, $10 \bmod 15$, $(82 \cdot 73) \bmod 7$, $(51+68) \bmod 7$, $(35 \cdot 24) \bmod 11$, and $(47 + 68) \bmod 11$.

3) Find integers s and t such that $1 = 7 \cdot s + 11 \cdot t$. Show that s and t are not unique.

4) Suppose a and b are integers that divide the integer c. If a and b are relatively prime, show that ab divides c. Show, by example, that if a and b are not relatively prime, then ab need not divide c.

5) Let $d = \gcd(a, b)$. If $a = da'$ and $b = db'$, show that $\gcd(a', b') = 1$.

6) Let n be a fixed positive integer greater than 1. If $a \bmod n = a'$ and $b \bmod n = b'$, prove that $(a + b) \bmod n = (a' + b') \bmod n$ and $(ab) \bmod n = (a'b') \bmod n$.

7) Let n and a be positive integers and let $d = \gcd(a, n)$. Show that the equation $ax \bmod n = 1$ has a solution if and only if $d = 1$.

8) Determine $7^{1000} \bmod 6$ and $6^{1001} \bmod 7$.

9) Show that $\gcd(a, bc) = 1$ if and only if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$.

10) Prove that $2^n 3^{2n} - 1$ is always divisible by 17 .

11) Prove that for every integer n, $n^3 \bmod 6 = n \bmod 6$.

12) Let S be the set of real numbers. If $a, b \in S$, define $a \sim b$ if $a - b$ is an integer. Show that $\sim$ is an equivalence relation on S. Describe the equivalence classes of S.

13) Let S be the set of integers. If $a, b \in S$, define aRb if $ab \geq 0$. Is R an equivalence relation on S?

14) Let S be the set of integers. If $a, b \in S$, define aRb if $a+b$ is even. Prove that R is an equivalence relation and determine the equivalence classes of S.

Chapter 0 (some solution suggestions):

1) $\{1, 2, 3, 4\}; \{1, 3, 5, 7\}; \{1, 5, 7, 11\}; \{1, 3, 7, 9, 11, 13, 17, 19\}; \{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24\}$

2) $12, 2, 2, 10, 1, 0, 4, 5$

6) Use the fact that a and b are equal mod n if and only if n divides $a - b$: Write $a = nq_1 + r_1$ and $b = nq_2 + r_2$, where $0 \leq r_1, r_2 < n$. We may assume that $r_1 \geq r_2$. Then $a - b = n(q_1 - q_2) + (r_1 - r_2)$, where $r_1 - r_2 \geq 0$. If $a \bmod n = b \bmod n$, then $r_1 = r_2$ and n divides $a - b$. If n divides $a - b$, then by the uniqueness of the remainder, we have $r_1 - r_2 = 0$.

7) Use Theorem that says the GCD is an integer linear combination.

9) Use Euclid's Lemma and the Fundamental Theorem of Arithmetic.

13) No. $(1, 0) \in R$ and $(0, -1) \in R$, but $(1, -1) \notin R$.

Chapter 1:

1) Write out a complete Cayley table for D_3. Is D_3 Abelian?

2) In D_4, find all elements X such that

(a) $X^3 = V$;
(b) $X^3 = R_{90}$;
(c) $X^3 = R_0$;
(d) $X^2 = R_0$;
(e) $X^2 = H$.

3) Associate the number 1 with a rotation and the number -1 with a reflection. Describe an analogy between multiplying these two numbers and multiplying elements of D_n.

4) If r_1, r_2, and r_3 represent rotations from D_n and f_1, f_2, and f_3 represent reflections from D_n, determine whether $r_1 r_2 f_1 r_3 f_2 f_3 r_3$ is a rotation or a reflection.

5) Find elements A, B, and C in D_4 such that $AB = BC$ but $A \neq C$. (Thus, "cross cancellation" is not valid.)

6) Consider an infinitely long strip of equally spaced H's: $\cdots$HHHH$\cdots$ Describe the symmetries of this strip. Is the group of symmetries of the strip Abelian?

7) 24. For each design below, determine the symmetry group (ignore imperfections).

Chapter 1 (some solution suggestions):

2) a. V b. R_{270} c. R_0 d. R_{180}, H, V, D, D' e. none

3) Observe that $1 \cdot 1 = 1; 1(-1) = -1; (-1)1 = -1; (-1)(-1) = 1$. These relationships also hold when 1 is replaced by "rotation" and -1 is replaced by "reflection."

5) In D_4, $HD = DV$ but $H \neq V$.

Chapter 2:

1) Which of the following binary operations are closed?

(a) subtraction of positive integers
(b) division of nonzero integers
(c) function composition of polynomials with real coefficients
(d) multiplication of 2×2 matrices with integer entries

2) Which of the following binary operations are associative?

(a) multiplication mod n
(b) division of nonzero rationals
(c) function composition of polynomials with real coefficients
(d) multiplication of 2×2 matrices with integer entries

3) In each case, find the inverse of the element under the given operation.

(a) 13 in $\mathbb{Z}_{20}$
(b) 13 in $U(14)$
(c) $n - 1$ in $U(n)$ (for $n > 2$)
(d) $3 - 2i$ in $\mathbb{C}_{\neq 0}$, the group of nonzero complex numbers under multiplication

4) Give two reasons why the set of odd integers under addition is not a group.

5) Show that the group $GL(2,\mathbb{R})$ (invertible 2×2 real matrices under matrix multiplication) is non-Abelian by exhibiting a pair of matrices A and B in $GL(2,\mathbb{R})$ such that $AB \neq BA$.

6) Find the inverse of the element $\begin{bmatrix} 2 & 6 \\ 3 & 5 \end{bmatrix}$ in $GL\left(2,\mathbb{Z}_{11}\right)$.

7) Translate each of the following multiplicative expressions into its additive counterpart. Assume that the operation is commutative.

(a) a^2b^3

(b) $a^{-2}\left(b^{-1}c\right)^2$

(c) $\left(ab^2\right)^{-3}c^2 = e$

8) (Socks-Shoes Property) Draw an analogy between the statement $(ab)^{-1} = b^{-1}a^{-1}$ and the act of putting on and taking off your socks and shoes. Find distinct nonidentity elements a and b from a non-Abelian group such that $(ab)^{-1} = a^{-1}b^{-1}$. Find an example that shows that in a group, it is possible to have $(ab)^{-2} \neq b^{-2}a^{-2}$. What would be an appropriate name for the group property $(abc)^{-1} = c^{-1}b^{-1}a^{-1}$?

9) Prove that a group G is Abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$ for all a and b in G.

10) Prove that in a group, $\left(a^{-1}\right)^{-1} = a$ for all a.

11) Give an example of a group with 105 elements. Give two examples of groups with 44 elements.

12) Prove that every group table is a Latin square; that is, each element of the group appears exactly once in each row and each column.

13) Suppose the table below is a group table. Fill in the blank entries.

	e	a	b	c	d
e	e	$-$	$-$	$-$	$-$
a	$-$	b	$-$	$-$	e
b	$-$	c	d	e	$-$
c	$-$	d	$-$	a	b
d	$-$	$-$	$-$	$-$	$-$

14) Prove that in a group, $(ab)^2 = a^2b^2$ if and only if $ab = ba$.

15) Prove that if G is a group with the property that the square of every element is the identity, then G is Abelian.

16) Let $G = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} \mid a \in \mathbf{R}, a \neq 0 \right\}$. Show that G is a group under matrix multiplication. Explain why each element of G has an inverse even though the matrices have 0 determinants. (Compare with $GL\left(2,\mathbb{R}\right)$.)

Chapter 2 (some solution suggestions):

1) c, d

3) $17; 13; n-1; \frac{3}{13} + \frac{2}{13}i$

4) Does not contain the identity; closure fails.

6) $\begin{bmatrix} 9 & 9 \\ 10 & 8 \end{bmatrix}$

7) (a) $2a + 3b$ (b) $-2a + 2(-b + c)$ (c) $-3(a + 2b) + 2c = 0$

12) Suppose x appears in a row labeled with a twice; say, $x = ab$ and $x = ac$. Then cancellation yields $b = c$. But we use distinct elements to label the columns.

13) Use the Latin Square property.

15) Since $a^2 = b^2 = (ab)^2 = e$, we have $aabb = abab$. Now cancel on the left and right.

Chapter 3:

1) For each group in the following list, find the order of the group and the order of each element in the group. What relation do you see between the orders of the elements of a group and the order of the group? $\mathbb{Z}_{12}$, $U(10)$, $U(12)$, $U(20)$, D_4

2) Let $\mathbb{Q}$ be the group of rational numbers under addition and let $\mathbb{Q}^*$ be the group of nonzero rational numbers under multiplication. In $\mathbb{Q}$, list the elements in $\left\langle \frac{1}{2} \right\rangle$. In $\mathbb{Q}^*$, list the elements in $\left\langle \frac{1}{2} \right\rangle$.

3) Let $\mathbb{Q}$ and $\mathbb{Q}^*$ be as in Exercise 2 . Find the order of each element in $\mathbb{Q}$ and in $\mathbb{Q}^*$.

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

5) If a, b, and c are group elements and $|a| = 6, |b| = 7$, express $\left(a^4c^{-2}b^4\right)^{-1}$ without using negative exponents.

6) Show that if a is an element of a group G, then $|a| \leq |G|$.

7) Show that $U(20) \neq \langle k \rangle$ for any k in $U(20)$. [Hence, $U(20)$ is not cyclic.]

8) Suppose that H is a proper subgroup of $\mathbb{Z}$ under addition and H contains 18,30, and 40. Determine H.

9) Suppose that H is a proper subgroup of $\mathbb{Z}$ under addition and that H contains 12,30, and 54. What are the possibilities for H?

10) If H and K are subgroups of G, show that $H \cap K$ is a subgroup of G. (Can you see that the same proof shows that the intersection of any number of subgroups of G, finite or infinite, is again a subgroup of G?)

11) Let G be a group. Show that $Z(G) = \cap_{a \in G} C(a)$. [This means the intersection of all subgroups of the form $C(a)$.]

12) Let G be a group, and let $a \in G$. Prove that $C(a) = C\left(a^{-1}\right)$.

13) Suppose G is the group defined by the following Cayley table.

	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	8	7	6	5	4	3
3	3	4	5	6	7	8	1	2
4	4	3	2	1	8	7	6	5
5	5	6	7	8	1	2	3	4
6	6	5	4	3	2	1	8	7
7	7	8	1	2	3	4	5	6
8	8	7	6	5	4	3	2	1

(a) Find the centralizer of each member of G.

(b) Find $Z(G)$.

(c) Find the order of each element of G. How are these orders arithmetically related to the order of the group?

14) If H is a subgroup of G, then by the centralizer $C(H)$ of H we mean the set $\{x \in G \mid xh = hx \text{ for all } h \in H\}$. Prove that $C(H)$ is a subgroup of G.

15) Consider the elements $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$ from $SL(2, \mathbb{R})$. Find |A|, |B|, and |AB|. Does your answer surprise you?

16) Consider the element $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ in $SL(2, \mathbb{R})$. What is the order of A? If we view $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ as a member of $SL\left(2, \mathbb{Z}_p\right)$ (p is a prime), what is the order of A ?

17) D_4 has seven cyclic subgroups. List them.

18) $U(15)$ has six cyclic subgroups. List them.

19) Let $G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{Z} \right\}$ under addition. Let $H = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G \mid a + b + c + d = 0 \right\}$. Prove that H is a subgroup of G. What if 0 is replaced by 1?

20) Let $H = \left\{a + bi \mid a, b \in \mathbb{R}, a^2 + b^2 = 1\right\}$. Prove or disprove that H is a subgroup of $\mathbb{C}^*$ under multiplication. Describe the elements of H geometrically.

21) Let G be a finite Abelian group and let a and b belong to G. Prove that the set $(a, b) = \left\{a^i b^j \mid i, j \in \mathbb{Z}\right\}$ is a subgroup of G. What can you say about $|(a, b\rangle|$ in terms of $|a|$ and $|b|$?

Chapter 3 (some solution suggestions):

1) $|\mathbb{Z}_{12}| = 12; |U(10)| = 4; |U(12)| = 4; |U(20)| = 8; |D_4| = 8$. In $\mathbb{Z}_{12}, |0| = 1; |1| = |5| = |7| = |11| = 12; |2| = |10|^4 = 6; |3| = |9| = 4; |4| = |8| = 3; |6| = 2$. In $U(10), |1| = 1; |3| = |7| = 4; |9| = 2$. In $U(12), 111 = 1; |5| = 2; |7| = 2; |11| = 2$. In $U(20), |1| = 1; |3| = |7| = |13| = |17| = 4; |9| = |11| = |19| = 2$. In $D_4, |R_0| = 1; |R_{90}| = |R_{270}| = 4; |R_{180}| = |H| = |V| = |D| = |D'| = 2$. In each case, notice that the order of the element divides the order of the group.

3) In $\mathbb{Q}, |0| = 1$ and all other elements have infinite order. In $\mathbb{Q}^*, |1| = 1, |-1| = 2$, and all other elements have infinite order.

5) $\left(a^4c^{-2}b^4\right)^{-1} = b^{-4}c^2a^{-4} = b^3c^2a^2$

6) If a has infinite order, then $e, a, a^2, \ldots$ are all distinct and belong to G, so G is infinite. If $|a| = n$, then $e, a, a^2, \ldots, a^{n-1}$ are distinct and belong to G.

7) By brute force, show that $k^4 = 1$ for all k.

9) $\langle 2\rangle, \langle 3\rangle, \langle 6\rangle$

11) If $x \in Z(G)$, then $x \in C(a)$ for all a, so $x \in \cap_{a\in G} C(a)$. If $x \in \cap_{a\in G} C(a)$, then $xa = ax$ for all a in G, so $x \in Z(G)$.

13) a. $C(5) = G; C(7) = \{1, 3, 5, 7\}$ b. $Z(G) = \{1, 5\}$ c. $|2| = 2; |3| = 4$. They divide the order of the group.

16) Note that $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$.

17) $\langle R_0\rangle, \langle R_{90}\rangle, \langle R_{180}\rangle, \langle D\rangle, \langle D'\rangle, \langle H\rangle, \langle V\rangle$ (Note that $\langle R_{90}\rangle = \langle R_{270}\rangle$)

19) Let $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ and $\begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}$ belong to H. It suffices to show that $a - a' + b - b' + c - c' + d - d' = 0$. This follows from $a + b + c + d = 0 = a' + b' + c' + d'$. If 0 is replaced by $1, H$ is not a subgroup.

20) If $a + bi$ and $c + di \in H$, then $(a + bi)(c + di)^{-1} = (ac + bd) + (bc - ad)i$ and $(ac + bd)^2 + (bc - ad)^2 = 1$, so that H is a subgroup. H is the unit circle in the complex plane.

Chapter 4:

1) Find all generators of $\mathbb{Z}_6, \mathbb{Z}_8$, and $\mathbb{Z}_{20}$.

2) List the elements of the subgroups $\langle 20\rangle$ and $\langle 10\rangle$ in $\mathbb{Z}_{30}$. Let a be a group element of order 30. List the elements of the subgroups $\langle a^{20}\rangle$ and $\langle a^{10}\rangle$.

3) Let a be an element of a group and let $|a| = 15$. Compute the orders of the following elements of G.

(a) a^3, a^6, a^9, a^{12}

(b) a^5, a^{10}

(c) a^2, a^4, a^8, a^{14}

4) Let G be a group and let $a \in G$. Prove that $\langle a^{-1}\rangle = \langle a\rangle$.

5) Let G be a group and let a be an element of G.

(a) If $a^{12} = e$, what can we say about the order of a ?

(b) If $a^m = e$, what can we say about the order of a ?

(c) Suppose that $|G| = 24$ and that G is cyclic. If $a^8 \neq e$ and $a^{12} \neq e$, show that $\langle a\rangle = G$.

6) List all the elements of order 8 in $\mathbb{Z}_{8000000}$. How do you know your list is complete? Let a be a group element such that $|a| = 8000000$. List all elements of order 8 in $\langle a\rangle$. How do you know your list is complete?

7) Determine the subgroup lattice for $\mathbb{Z}_{p^2q}$, where p and q are distinct primes.

8) Suppose that a and b are group elements that commute and have orders m and n. If $\langle a\rangle \cap \langle b\rangle = \{e\}$, prove that the group contains an element whose order is the least common multiple of m and n. Show that this need not be true if a and b do not commute.

9) Prove that an infinite group must have an infinite number of subgroups.

10) Determine the orders of the elements of D_{33} and how many there are of each.

11) Let a and b be elements of a group. If $|a| = 10$ and $|b| = 21$, show that $\langle a\rangle \cap \langle b\rangle = \{e\}$.

12) If $\left|a^5\right| = 12$, what are the possibilities for $|a|$? If $\left|a^4\right| = 12$, what are the possibilities for $|a|$?

13) If x is an element of a cyclic group of order 15 and exactly two of x^3, x^5, and x^9 are equal, determine $\left|x^{13}\right|$.

Chapter 4 (some solution suggestions):

1) For $\mathbb{Z}_6$, generators are 1 and 5 ; for $\mathbb{Z}_8$, generators are $1, 3, 5$, and 7; for $\mathbb{Z}_{20}$, generators are $1, 3, 7, 9, 11, 13, 17$, and 19.

2) $\langle 20\rangle = \{20, 10, 0\}; \langle 10\rangle = \{10, 20, 0\}; \langle a^{20}\rangle = \left\{a^{20}, a^{10}, a^0\right\}; \langle a^{10}\rangle = \left\{a^{10}, a^{20}, a^0\right]$

4) By definition, $a^{-1} \in \langle a\rangle$. So, $\langle a^{-1}\rangle \subseteq \langle a\rangle$. By definition, $a = \left(a^{-1}\right)^{-1} \in \langle a^{-1}\rangle$. So, $\langle a\rangle \subseteq \langle a^{-1}\rangle$.

5) a. $|a|$ divides 12. b. $|a|$ divides m. c. By a theorem, $|a| = 1, 2, 3, 4, 6, 8, 12$, or 24 . If $|a| = 2$, then $a^8 = \left(a^2\right)^4 = e^4 = e$. A similar argument eliminates all other possibilities except 24 .

6) 1000000, 3000000, 5000000, 7000000; by a theorem, $\langle 1000000\rangle$ is the unique subgroup of order 8 , and only those on the list are generators. $a^{1000000}, a^{3000000}, a^{5000000}, a^{7000000}$; by Theorem 4.3, $\left\langle a^{1000000}\right\rangle$ is the unique subgroup of order 8 , and only those on the list are generators.

7) Mimic the subgroup lattice examples from class.

8) Let $t = \text{lcm}(m, n)$ and $|ab| = s$. Then $(ab)^t = a^t b^t = e$, and therefore s divides t. Also, $e = (ab)^s = a^s b^s$, so that $a^s = b^{-s}$, and therefore a^s and b^{-s} belong to $\langle a\rangle \cap \langle b\rangle = \{e\}$. Thus, m divides s and n divides s, and, therefore, t divides s. This proves that $s = t$. For the second part, try D_3.

10) 1 of order 1; 33 of order 2; 2 of order 3; 10 of order 11; 20 of order 33

11) Consider possible orders.

12) 12 or 60; 48

Supplementary Problems for Chapters 1–4:

1) Let G be a group and let H be a subgroup of G. For any fixed x in G, define $xHx^{-1} = \left\{xhx^{-1} \mid h \in H\right\}$. Prove the following.

(a) xHx^{-1} is a subgroup of G.

(b) If H is cyclic, then xHx^{-1} is cyclic.

(c) If H is Abelian, then xHx^{-1} is Abelian.

The group xHx^{-1} is called a conjugate of H. (Note that conjugation preserves structure.)

2) Let G be a group and let H be a subgroup of G. Define $N(H) = \left\{x \in G \mid xHx^{-1} = H\right\}$. Prove that $N(H)$ (called the normalizer of H) is a subgroup of G.

3) The group defined by the following table is called the group of quaternions. Use the table to determine each of the following.

(a) The center

(b) cl(a)

(c) cl(b)

(d) All cyclic subgroups

	e	a	a^2	a^3	b	ba	ba^2	ba^3
e	e	a	a^2	a^3	b	ba	ba^2	ba^3
a	a	a^2	a^3	e	ba^3	b	ba	ba^2
a^2	a^2	a^3	e	a	ba^2	ba^3	b	ba
a^3	a^3	e	a	a^2	ba	ba^2	ba^3	b
b	b	ba	ba^2	ba^3	a^2	a^3	e	a
ba	ba	ba^2	ba^3	b	a	a^2	a^3	e
ba^2	ba^2	ba^3	b	ba	e	a	a^2	a^3
ba^3	ba^3	b	ba	ba^2	a^3	e	a	a^2

4) (Conjugation preserves order.) Prove that, in any group, $\left|xax^{-1}\right| = |a|$.

5) What are the orders of the elements of D_{15}? How many elements have each of these orders?

6) Let $G = \{a + b\sqrt{2}\}$, where a and b are rational numbers not both 0. Prove that G is a group under ordinary multiplication.

7) Prove that the subset of elements of finite order in an Abelian group forms a subgroup. (This subgroup is called the torsion subgroup.) Is the same thing true for non-Abelian groups?

8) Let $\mathrm{H}_1, \mathrm{H}_2, \mathrm{H}_3, \ldots$ be a sequence of subgroups of a group with the property that $\mathrm{H}_1 \subseteq \mathrm{H}_2 \subseteq \mathrm{H}_3 \ldots$ Prove that the union of the sequence is a subgroup.

9) Let $H = \{A \in GL(2, \mathrm{R}) \mid \det A \text{ is rational}\}$. Prove or disprove that H is a subgroup of $GL(2, \mathbf{R})$. What if "rational" is replaced by "an integer"?

10) Let G be a cyclic group of order n and let H be the subgroup of order d. Show that $H = \{x \in G \mid |x| \text{ divides } d\}$.

Supplementary Problems for Chapters 1–4 (some solution suggestions):

1) a. Let xh_1x^{-1} and xh_2x^{-1} belong to xHx^{-1}. Then $\left(xh_1x^{-1}\right)\left(xh_2x^{-1}\right)^{-1} = xh_1h_2{}^{-1}x^{-1} \in xHx^{-1}$ also. b. Let $\langle h\rangle = H$. Then $\left\langle xhx^{-1}\right\rangle = xHx^{-1}$. c. $\left(xh_1x^{-1}\right)\left(xh_2x^{-1}\right) = xh_1h_2x^{-1} = xh_2h_1x^{-1} = \left(xh_2x^{-1}\right)\left(xh_1x^{-1}\right)$

4) Observe that $\left(xax^{-1}\right)^k = xa^kx^{-1}$. Thus, $\left(xax^{-1}\right)^k = e$ if and only if $a^k = e$.

5) 1 of order 1, 15 of order 2, 8 of order 15, 4 of order 5, 2 of order 3

9) Use $\det(AB) = (\det A)(\det B)$ to prove H is a subgroup. H is not a subgroup when $\det A$ is an integer, since $\det A^{-1}$ need not be an integer.

10) Let $K = \{x \in G \mid |x| \text{ divides } d\}$. By a previous exercise, K is a subgroup. Let $x \in H$. By a theorem $|x|$ divides d. So, $H \subseteq K$. Let $y \in K$, $|y| = t$, and $d = tq$. By a theorem, H has a subgroup of order t and G has only one subgroup of order t. So, $\langle y\rangle \subseteq H$.

Chapter 5:

1) Let $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 8 & 6 \end{bmatrix}$ and $\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 8 & 7 & 6 & 5 & 2 & 4 \end{bmatrix}$. Write α, β, and $\alpha\beta$ as

(a) products of disjoint cycles;

(b) products of 2 -cycles.

2) Write each of the following permutations as a product of disjoint cycles.

(a) (1235)(413)

(b) (13256)(23)(46512)

(c) (12)(13)(23)(142)

3) Show that A_8 contains an element of order 15 .

4) What are the possible orders for the elements of S_6 and A_6? What about A_7?

5) Determine whether the following permutations are even or odd.

(a) (135)

(b) (1356)

(c) (13567)

(d) (12)(134)(152)

(e) (1243)(3521)

6) If α is even, prove that α^{-1} is even. If α is odd, prove that α^{-1} is odd.

7) Let α and β belong to S_n. Prove that $\alpha\beta$ is even if and only if α and β are both even or both odd.

8) Show that if H is a subgroup of S_n, then either every member of H is an even permutation or exactly half of the members are even.

9) Give two reasons why the set of odd permutations in S_n is not a subgroup.

10) How many elements of order 5 are in S_7?

11) Let G be a group of permutations on a set X. Let $a \in X$ and define $\text{stab}(a) = \{\alpha \in G \mid \alpha(a) = a\}$. We call stab(a) the stabilizer of a in G (since it consists of all members of G that leave a fixed). Prove that $\text{stab}(a)$ is a subgroup of G. (This subgroup was introduced by Galois in 1832.)

12) Represent the symmetry group of an equilateral triangle as a group of permutations of its vertices.

13) Prove that S_n is non-Abelian for all $n \geq 3$.

14) Find a cyclic subgroup of A_8 that has order 4.

15) Find a noncyclic subgroup of A_8 that has order 4.

16) Show that for $n \geq 3, Z(S_n) = \{\varepsilon\}$.

Chapter 5 (some solution suggestions):

2) a. (15)(234) b. (124)(35)(6) c. (1423)

4) For S_6, the possible orders are $1, 2, 3, 4, 5, 6$; for $A_6, 1, 2, 3, 4, 5$; for $A_7, 1, 2, 3, 4, 5, 6, 7$.

5) a. even b. odd c. even d. odd e. even

7) Suppose that α can be written as a product of m2-cycles and β can be written as a product of n 2-cycles. Then $\alpha\beta$ can be written as a product of $m+n$ 2-cycles. Now observe that $m+n$ is even if and only if m and n are both even or both odd.

8) Suppose H contains at least one odd permutation, say, σ. Consider the function $\tau \mapsto \sigma\tau$. This gives a bijection between the even permutations in H and the odd permuations in H.

9) The identity is even; the set is not closed.

11) Let $\alpha, \beta \in \text{stab}(a)$. Then $\alpha\beta(a) = \alpha(\beta(a)) = \alpha(a) = a$. Also, $\alpha(a) = a$ implies $\alpha^{-1}(\alpha(a)) = \alpha^{-1}(a)$ or $a = \alpha^{-1}(a)$.

13) $(123)(12) \neq (12)(123)$ in $S_n (n \geq 3)$.

15) One possibility is $\{(1), (12)(34), (56)(78), (12)(34)(56)(78)\}$.

Chapter 6:

1) Let $\mathbb{R}^+$be the group of positive real numbers under multiplication. Show that the mapping $\phi(x) = \sqrt{x}$ is an automorphism of $\mathbb{R}^+$.

2) Show that $U(8)$ is isomorphic to $U(12)$.

3) Prove that S_4 is not isomorphic to D_{12}.

4) Let G be a group. Prove that the mapping $\alpha(g) = g^{-1}$ for all g in G is an automorphism if and only if G is Abelian.

5) If G is a group, prove that $\text{Aut}(G)$ and $\text{Inn}(G)$ are groups.

6) The group $\left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \mid a \in \mathbb{Z} \right\}$ is isomorphic to what familiar group? What if $\mathbb{Z}$ is replaced by $\mathbb{R}$?

7) If ϕ and γ are isomorphisms from the cyclic group $\langle a \rangle$ to some group and $\phi(a) = \gamma(a)$, prove that $\phi = \gamma$.

8) Given $\varphi : G \to H$ is an isomorphism, show that $\varphi^{-1} : H \to G$ is an isomorphism.

9) Let $\varphi : G \to H$ be an isomorpihsm and K a subgroup of G. Show that $\varphi(K) = \{\varphi(x) \mid x \in K\}$ (i.e., the image of K under φ) is a subgroup of H.

10) Prove that the quaternion group $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ is not isomorphic to the dihedral group D_4.

11) Let $\mathbb{C}$ be the complex numbers and

$$M = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \mid a, b \in \mathbb{R} \right\}.$$

Prove that $\mathbb{C}$ and M are isomorphic under addition and that $\mathbb{C}^*$ and M^*, the nonzero elements of M, are isomorphic under multiplication.

12) Let G be a group and let $g \in G$. If $z \in Z(G)$, show that the inner automorphism induced by g is the same as the inner automorphism induced by zg (that is, that the mappings ϕ_g and ϕ_{zg} are equal).

13) Suppose the ϕ and γ are isomorphisms of some group G to the same group. Prove that $H = \{g \in G \mid \phi(g) = \gamma(g)\}$ is a subgroup of G.

14) Let a belong to a group G and let $|a|$ be finite. Let ϕ_a be the automorphism of G given by $\phi_a(x) = axa^{-1}$. Show that $|\phi_a|$ divides $|a|$. Exhibit an element a from a group for which $1 < |\phi_a| < |a|$.

15) Write the permutation corresponding to R_{90} in the left regular representation of D_4 in cycle form.

Chapter 6 (some solution suggestions):

1) $\phi(xy) = \sqrt{xy} = \sqrt{x}\sqrt{y} = \phi(x)\phi(y)$.

2) Try $1 \to 1, 3 \to 5, 5 \to 7, 7 \to 11$.

3) D_{12} has elements of order 12 and S_4 does not.

5) Let $\alpha \in \text{Aut}(G)$. We show that α^{-1} is operation-preserving: $\alpha^{-1}(xy) = \alpha^{-1}(x)\alpha^{-1}(y)$ if and only if $\alpha\left(\alpha^{-1}(xy)\right) = \alpha\left(\alpha^{-1}(x)\alpha^{-1}(y)\right)$, that is, if and only if $xy = \alpha\left(\alpha^{-1}(x)\right)\alpha\left(\alpha^{-1}(y)\right) = xy$. So α^{-1} is operation-preserving. That $\text{Inn}(G)$ is a group follows from the equation $\phi_g\phi_h = \phi_g$

7) Use the fact that $\phi(x^n) = \phi(x)^n$.

8) The inverse of a one-to-one function is one-to-one. For any $g \in G$, we have $\phi^{-1}(\phi(g)) = g$, and therefore ϕ^{-1} is onto. To verify that ϕ^{-1} is operation-preserving, notice that $\phi(\phi^{-1}(x)\phi^{-1}(y)) = \phi(\phi^{-1}(x))\phi(\phi^{-1}(y)) = xy = \phi(\phi^{-1}(xy))$ and apply ϕ^{-1} to this equation.

11) Try $a+bi \to \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$.

12) Observe that $\phi_g(y) = gyg^{-1}$ and $\phi_{zg}(y) = zgy(zg)^{-1} = zgyg^{-1}z^{-1} = gyg^{-1}$ since $z \in Z(G)$. So, $\phi_g = \phi_{zg}$.

13) Since both ϕ and γ take e to itself, H is not empty. Assume a and b belong to H. Then $\phi\left(ab^{-1}\right) = \phi(a)\phi\left(b^{-1}\right) = \phi(a)\phi(b)^{-1} = \gamma(a)\gamma(b)^{-1} = \gamma(a)\gamma\left(b^{-1}\right) = \gamma\left(ab^{-1}\right)$. Thus, ab^{-1} is in H.

14) Say $|a| = n$. Then $\phi_a^n(x) = a^n x a^{-n} = x$, so that ϕ_a^n is the identity. For the example, take $a = R_{90}$ in D_4.

15) $(R_0R_{90}R_{180}R_{270})\,(HD'VD)$.

Chapter 7:

1) Let $H = \{(1), (12)(34), (13)(24), (14)(23)\}$. Find the left cosets of H in A_4.

2) Let $H = \{0, \pm 3, \pm 6, \pm 9, \ldots\}$. Find all the left cosets of H in $\mathbb{Z}$.

3) Let $H = \{0, \pm 3, \pm 6, \pm 9, \ldots\}$. Decide whether or not the following cosets of H are the same.

(a) $11 + H$ and $17 + H$

(b) $-1 + H$ and $5 + H$

(c) $7 + H$ and $23 + H$

4) Suppose that a has order 15 . Find all of the left cosets of $\left\langle a^5 \right\rangle$ in $\langle a \rangle$.

5) If H and K are subgroups of G and g belongs to G, show that $g(H \cap K) = gH \cap gK$.

6) Suppose that K is a proper subgroup of H and H is a proper subgroup of G. If $|K| = 42$ and $|G| = 420$, what are the possible orders of H?

7) Let G be a group with $|G| = pq$, where p and q are prime. Prove that every proper subgroup of G is cyclic.

8) Suppose H and K are subgroups of a group G. If $|H| = 12$ and $|K| = 35$, find $|H \cap K|$. Generalize.

9) Suppose that G is a group with more than one element and G has no proper, nontrivial subgroups. Prove that $|G|$ is prime. (Do not assume at the outset that G is finite.)

10) Let $G = \{(1), (12)(34), (1234)(56), (13)(24), (1432)(56), (56)(13), (14)(23), (24)(56)\}$.

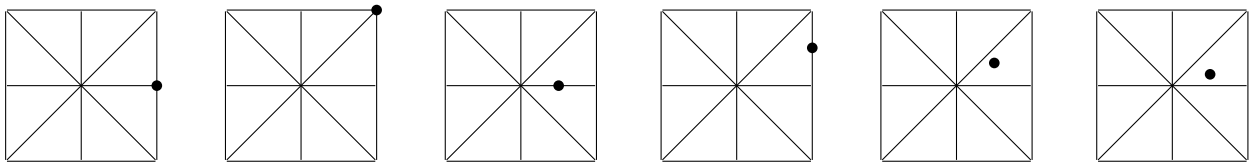
(a) Find the stabilizer of 1 and the orbit of 1.

(b) Find the stabilizer of 3 and the orbit of 3.

(c) Find the stabilizer of 5 and the orbit of 5 .

11) Let $G = GL(2, \mathbb{R})$ and $H = SL(2, \mathbb{R})$. Let $A \in G$ and suppose that $\det A = 2$. Prove that AH is the set of all 2×2 matrices in G that have determinant 2 .

12) The group D_4 acts as a group of permutations of the square regions shown below. (The axes of symmetry are drawn for reference purposes.) For each square region, locate the points in the orbit of the indicated point under D_4. In each case, determine the stabilizer of the indicated point.



13) Calculate the orders of the following (Google "Platonic solids" for pictures of these shapes).

(a) The group of rotations of a regular tetrahedron (a solid with four congruent equilateral triangles as faces)

(b) The group of rotations of a regular octahedron (a solid with eight congruent equilateral triangles as faces)

(c) The group of rotations of a regular dodecahedron (a solid with 12 congruent regular pentagons as faces)

(d) The group of rotations of a regular icosahedron (a solid with 20 congruent equilateral triangles as faces)

Chapter 7 (some solution suggestions):

1) $H = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$, $\alpha_5 H = \{\alpha_5, \alpha_8, \alpha_6, \alpha_7\}$, $\alpha_9 H = \{\alpha_9, \alpha_{11}, \alpha_{12}, \alpha_{10}\}$

2) $H, 1 + H, 2 + H$

3) a. yes b. yes c. no

5) Let ga belong to $g(H \cap K)$, where a is in $H \cap K$. Then by definition ga is in $gH \cap gK$. Now let $x \in gH \cap gK$. Then $x = gh$ for some $h \in H$, and $x = gk$ for some $k \in K$. Cancellation then gives $h = k$. Thus, $x \in g(H \cap K)$.

7) Use Lagrange's Theorem and the theorem stating that groups of prime order are cyclic.

10) a. $\text{stab}_G(1) = \{(1), (24)(56)\}$; $\text{orb}_G(1) = \{1, 2, 3, 4\}$ b. $\text{stab}_G(3) = \{(1), (24)(56)\}$; $\text{orb}_G(3) = \{3, 4, 1, 2\}$
c. $\text{stab}_G(5) = \{(1), (12)(34), (13)(24), (14)(23)\}$; $\text{orb}_G(5) = \{5, 6\}$

11) Suppose that $B \in G$ and $\det(B) = 2$. Then $\det\left(A^{-1}B\right) = 1$, so that $A^{-1}B \in H$ and therefore $B \in AH$. Conversely, for any $Ah \in AH$ we have $\det(Ah) = \det(A)\det(h) = 2 \cdot 1 = 2$.

Chapter 8:

1) Let G be a group with identity e_G and let H be a group with identity e_H. Prove that G is isomorphic to $G \oplus \{e_H\}$ and that H is isomorphic to $\{e_G\} \oplus H$.

2) Show that $G \oplus H$ is Abelian if and only if G and H are Abelian. State the general case.

3) Prove that $G_1 \oplus G_2$ is isomorphic to $G_2 \oplus G_1$. State the general case.

4) Is $\mathbb{Z}_3 \oplus \mathbb{Z}_9$ isomorphic to $\mathbb{Z}_{27}$? Why?

5) Is $\mathbb{Z}_3 \oplus \mathbb{Z}_5$ isomorphic to $\mathbb{Z}_{15}$? Why?

6) If $G \oplus H$ is cyclic, prove that G and H are cyclic. State the general case.

7) In $\mathbb{Z}_{40} \oplus \mathbb{Z}_{30}$, find two subgroups of order 12 .

8) What is the order of any nonidentity element of $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$? Generalize.

9) The group $S_3 \oplus \mathbb{Z}_2$ is isomorphic to one of the following groups: $\mathbb{Z}_{12}, \mathbb{Z}_6 \oplus \mathbb{Z}_2, A_4, D_6$. Determine which one by elimination.

10) What is the largest order of any element in $\mathbb{Z}_{30} \oplus \mathbb{Z}_{20}$?

11) What is the order of the largest cyclic subgroup of $\mathbb{Z}_6 \oplus \mathbb{Z}_{10} \oplus \mathbb{Z}_{15}$? What is the order of the largest cyclic subgroup of $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}$?

12) How many isomorphisms are there from $\mathbb{Z}_{12}$ to $\mathbb{Z}_4 \oplus \mathbb{Z}_3$?

13) What is the largest order of any element in $U(900)$?

Chapter 8 (some solution suggestions):

1) Use $g \to (g, e_H)$ and $h \to (e_G, h)$.

3) Use $(g_1, g_2) \to (g_2, g_1)$. In general, $G_1 \oplus G_2 \cdots \oplus G_n$ is isomorphic to the external direct product of any rearrangement of $G_1, G_2, \ldots, G_{n^*}$

5) Yes, direct products of cyclic groups are cyclic if and only if the orders of the product-ed groups are relatively prime.

6) Use the fact that subgroups of cyclic groups are cyclic along with the first exercise.

8) $|(a, b, c)| = \text{lcm}(|a|, |b|, |c|) = 3$, unless $a = b = c = 0$. In general, the order of every nonidentity element of $\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p$, where p is prime, is p.

10) 60

12) Using the fact that an isomorphism from $\mathbb{Z}_{12}$ is determined by the image of 1 and the fact that a generator must map to a generator, we determine that there are four isomorphisms.

13) 60

Supplementary Problems for Chapters 5–8:

1) A subgroup N of a group G is called a characteristic subgroup if $\phi(N) = N$ for all automorphisms ϕ of G. (The term characteristic was first applied by G. Frobenius in 1895.) Prove that every subgroup of a cyclic group is characteristic.

2) Prove that the center of a group is characteristic.

3) The commutator subgroup G' of a group G is the subgroup generated by the set $\left\{x^{-1}y^{-1}xy \mid x, y \in G\right\}$. (That is, every element of G' has the form $a_1^{i_1}a_2^{i_2}\cdots a_k^{i_k}$, where each a_j has the form $x^{-1}y^{-1}xy$, each $i_j = \pm 1$, and k is any positive integer.) Prove that G' is a characteristic subgroup of G. (This subgroup was first introduced by G. A. Miller in 1898.)

4) Suppose that H and K are subgroups of a group and that $|H|$ and $|K|$ are relatively prime. Show that $H \cap K = \{e\}$.

5) Prove that $\mathbb{Q}^*$ under multiplication is not isomorphic to $\mathbb{R}^*$ under multiplication.

6) Prove that $\mathbb{R}$ under addition is not isomorphic to $\mathbb{R}^*$ under multiplication.

7) Find a subgroup of $\mathbb{Z}_{12} \oplus \mathbb{Z}_{20}$ that is isomorphic to $\mathbb{Z}_4 \oplus \mathbb{Z}_5$.

8) Suppose that $G = G_1 \oplus G_2 \oplus \cdots \oplus G_n$. Prove that $Z(G) = Z(G_1) \oplus Z(G_2) \oplus \cdots \oplus Z(G_n)$.

9) Show that $D_{33} \ncong D_3 \oplus \mathbb{Z}_{11}$.

10) List four elements of $\mathbb{Z}_{20} \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{60}$ that form a noncyclic subgroup.

11) Find an element of order 10 in A_9.

12) How many elements of order 6 are in S_7?

13) Find a permutation β such that $\beta^2 = (13579)(268)$.

14) Let G be a group of permutations on the set $\{1, 2, \ldots, n\}$. Recall that $\text{stab}_G(1) = \{\alpha \in G \mid \alpha(1) = 1\}$. If γ sends 1 to k, prove that $\gamma \text{ stab}_G(1) = \{\beta \in G \mid \beta(1) = k\}$.

15) Let H be a subgroup of G and let $a, b \in G$. Show that $aH = bH$ if and only if $Ha^{-1} = Hb^{-1}$.

Supplementary Problems for Chapters 5–8 (some solution suggestions):

1) Consider the finite and infinite cases separately. In the finite case, note that $|H| = |\phi(H)|$. Use the fact that cyclic subgroups have a unique subgroup for each divisor order. For the infinite case, the only auto

3) Observe that $\phi\left(x^{-1}y^{-1}xy\right) = (\phi(x))^{-1}(\phi(y))^{-1}\phi(x)\phi(y)$, so ϕ carries the generators of G' to the generators of G'.

7) $\langle 3 \rangle \oplus \langle 4 \rangle$

9) Count elements of order 2.

11) (12)(34)(56789)

12) 1260

13) $\beta = (17395)(286)$

15) $aH = bH$ implies $a^{-1}b \in H$. So $\left(a^{-1}b\right)^{-1} = b^{-1}a \in H$. Thus, $Hb^{-1}a = H$ or $Hb^{-1} = Ha^{-1}$. These steps are reversible.

Chapter 9:

1) Let $H = \{(1), (12)\}$. Is H normal in S_3?

2) Prove that A_n is normal in S_n.

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

4) Let $G = GL(2, \mathbb{R})$ and let K be a subgroup of $\mathbb{R}^*$. Prove that $H = \{A \in G \mid \det A \in K\}$ is a normal subgroup of G.

5) The Index 2 Theorem: Prove that if H has index 2 in G, then H is normal in G.

6) Let $G = Z_4 \oplus U(4)$, $H = \langle (2, 3) \rangle$, and $K = \langle (2, 1) \rangle$. Show that G/H is not isomorphic to G/K. (This shows that $H \cong K$ does not imply that $G/H \cong G/K$.)

7) Prove that a factor group of a cyclic group is cyclic.

8) Prove that a factor group of an Abelian group is Abelian.

9) What is the order of the element $14 + \langle 8 \rangle$ in the factor group $\mathbb{Z}_{24}/\langle 8 \rangle$?

10) What is the order of the element $4\,U_5(105)$ in the factor group $U(105)/U_5(105)$?
Note: $U_5(105) = \{x \in U(105) \mid x = 1 \bmod 5\}$.

11) Recall that $Z(D_6) = \{R_0, R_{180}\}$. What is the order of the element $R_{60}\,Z(D_6)$ in the factor group $D_6/Z(D_6)$?

12) What is the order of the factor group $(\mathbb{Z}_{10} \oplus U(10))/\langle (2, 9) \rangle$?

13) Determine the order of $(\mathbb{Z} \oplus \mathbb{Z})/\langle (4, 2) \rangle$. Is the group cyclic?

14) Let G be a finite group and let H be a normal subgroup of G. Prove that the order of the element gH in G/H must divide the order of g in G.

15) If H is a normal subgroup of a group G, prove that $C(H)$, the centralizer of H in G, is a normal subgroup of G.

16) Let p be a prime. Show that if H is a subgroup of a group of order $2p$ that is not normal, then H has order 2 .

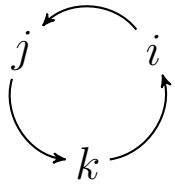
17) Suppose that G is a non-Abelian group of order p^3, where p is a prime, and $Z(G) \neq \{e\}$. Prove that $|Z(G)| = p$.

18) Let $Q = \{\pm 1, \pm i, \pm j, \pm k\}$, where $i^2 = j^2 = k^2 = -1, -i = (-1)i$, $1^2 = (-1)^2 = 1, ij = -ji = k, jk = -kj = i$, and $ki = -ik = j$.

(a) Construct the Cayley table for Q.

(b) Show that $H = \{1, -1\}$ is a subgroup of Q.

(c) Construct the Cayley table for Q/H. Is Q/H isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_2$? (The rules involving i, j, and k can be remembered by using the circle below.



Going clockwise, the product of two consecutive elements is the third one. The same is true for going counter-clockwise, except that we obtain the negative of the third element.) It was invented by William Hamilton in 1843. The quaternions are used to describe rotations in three-dimensional space, and they are used in physics. The quaternions can be used to extend the complex numbers in a natural way.

19) Show that the intersection of two normal subgroups of G is a normal subgroup of G. Generalize.

20) If G is non-Abelian, show that $\mathrm{Aut}(G)$ is not cyclic.

21) Suppose that H is a normal subgroup of a finite group G. If G/H has an element of order n, show that G has an element of order n. Show, by example, that the assumption that G is finite is necessary.

22) If $|G| = 30$ and $|Z(G)| = 5$, what is the structure of $G/Z(G)$?

Chapter 9 (some solution suggestions):

1) No.

4) Recall that if A and B are matrices, then $\det\left(ABA^{-1}\right) = (\det A)(\det B)(\det A)^{-1}$.

5) Let $x \in G$. If $x \in H$, then $xH = H = Hx$. If $x \notin H$, then xH is the set of elements in G, not in H. But Hx is also the set of elements in G, not in H.

6) $G/H \cong \mathbb{Z}_4$, but $G/K \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

8) Observe that $aHbH = abH = baH = bHaH$.

10) 2

12) $40/10 = 4$

13) ∞; no, $(6,3) + \langle(4,2)\rangle$ has order 2 .

14) Say $|g| = n$. Then $(gH)^n = g^nH = eH = H$. Now use the fact that when $X^n = e$ then the order of X must divide n.

15) Let $x \in C(H), g \in G$, and $h \in H$. We must show that $gxg^{-1}h = hgxg^{-1}$. Note that in the expression $\left(gxg^{-1}\right)h\left(gxg^{-1}\right)^{-1} = gxg^{-1}hgx^{-1}g^{-1}$, the terms x and x^{-1} cancel since $g^{-1}hg \in H$ and x commutes with every element of H. Then we have $\left(gxg^{-1}\right)h\left(gxg^{-1}\right)^{-1} = gxg^{-1}hgx^{-1}g^{-1} = gg^{-1}hgg^{-1} = h$. So, $gxg^{-1} \in C(H)$.

16) Use Lagrange's Theorem and the Index 2 Theorem (i.e., Exercise 5).

17) Use the G/Z Theorem.

20) Use the G/Z Theorem along with the Theorem: $G/Z(G) \cong \mathrm{Inn}(G)$.

21) Say $|gH| = n$. Then $|g| = nt$ (by Exercise 37) and $|g^t| = n$. For the second part, consider $Z/\langle k\rangle$.

22) Use the G/Z Theorem and the Theorem: Any group of order two times an odd prime is either cyclic or dihedral.

Chapter 10:

1) Let $\det : GL(2,\mathbb{R}) \to \mathbb{R}^*$ be the determinant mapping from invertible 2×2 real matrices into the non-zero real numbers. Show this map is a homomorphism.

2) Let $\phi : \mathbb{R}^* \to \mathbb{R}^*$ be defined by $\phi(x) = |x|$ (absolute value). Show ϕ is a homomorphism with kernel $\{1, -1\}$.

3) Let $\frac{d}{dx} : \mathbb{R}[x] \to \mathbb{R}[x]$ be the derivative map from real polynomials to themselves. Note that $\mathbb{R}[x]$ is a group under addition. Show that the derivative map is a homomorphism.

4) Let $\psi : S_n \to \mathbb{Z}_2$ be defined by $\psi(\sigma) = 0$ if σ is even and $\psi(\sigma) = 1$ if σ is odd. Show the ψ is a homomorphism.

5) If ϕ is a homomorphism from G to H and σ is a homomorphism from H to K, show that $\sigma \circ \phi$ is a homomorphism from G to K. How are Ker ϕ and Ker $\sigma \circ \phi$ related? If ϕ and σ are onto and G is finite, describe [Ker $\sigma \circ \phi$: Ker ϕ] in terms of $|H|$ and $|K|$.

6) Let G be a group of permutations. For each σ in G, define

$$\operatorname{sgn}(\sigma) = \begin{cases} +1 & \text{if } \sigma \text{ is an even permutation,} \\ -1 & \text{if } \sigma \text{ is an odd permutation.} \end{cases}$$

Prove that sgn is a homomorphism from G to the multiplicative group $\{+1, -1\}$. What is the kernel? Why does this homomorphism allow you to conclude that A_n is a normal subgroup of S_n of index 2? Why does this prove that exactly half of the permutations in S_n are even and half are odd?

7) Prove that the mapping from $G \oplus H$ to G given by $(g, h) \to g$ is a homomorphism. What is the kernel? This mapping is called the projection of $G \oplus H$ onto G.

8) Let G be a subgroup of some dihedral group. For each x in G, define

$$\phi(x) = \begin{cases} +1 & \text{if } x \text{ is a rotation,} \\ -1 & \text{if } x \text{ is a reflection.} \end{cases}$$

Prove that ϕ is a homomorphism from G to the multiplicative group $\{+1, -1\}$. What is the kernel? Why does this prove that half of the elements of D_n are rotations and half are reflections?

9) Prove that $(\mathbb{Z} \oplus \mathbb{Z})/(\langle (a, 0) \rangle \times \langle (0, b) \rangle)$ is isomorphic to $\mathbb{Z}_a \oplus \mathbb{Z}_b$.

10) Explain why the correspondence $x \to 3x$ from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{10}$ is not a homomorphism.

11) Prove that there is no homomorphism from $\mathbb{Z}_8 \oplus \mathbb{Z}_2$ onto $\mathbb{Z}_4 \oplus \mathbb{Z}_4$.

12) Suppose that there is a homomorphism ϕ from $\mathbb{Z}_{17}$ to some group and that ϕ is not one-to-one. Determine ϕ.

13) If ϕ is a homomorphism from $\mathbb{Z}_{30}$ onto a group of order 5, determine the kernel of ϕ.

14) Suppose that $\phi : \mathbb{Z}_{50} \to \mathbb{Z}_{15}$ is a group homomorphism with $\phi(7) = 6$.

(a) Determine $\phi(x)$.

(b) Determine the image of ϕ.

(c) Determine the kernel of ϕ.

(d) Determine $\phi^{-1}(3)$. That is, determine the set of all elements that map to 3 (i.e., the fiber over 3).

15) (Second Isomorphism Theorem) If K is a subgroup of G and N is a normal subgroup of G, prove that $K/(K \cap N)$ is isomorphic to KN/N.

16) (Third Isomorphism Theorem) If M and N are normal subgroups of G and $N \subseteq M$, prove that $(G/N)/(M/N) \cong G/M$.

17) Determine all homomorphic images of D_4 (up to isomorphism).

18) Suppose that G is a finite group and that $\mathbb{Z}_{10}$ is a homomorphic image of G. What can we say about $|G|$? Generalize.

19) Let N be a normal subgroup of a group G. Use the fact for homomorphisms that we have inverse images of subgroups are subgroups to prove that every subgroup of G/N has the form H/N, where H is a subgroup of G.

20) Use the First Isomorphism Theorem to prove $G/Z(G) \cong \operatorname{Inn}(G)$.

21) If H and K are normal subgroups of G and $H \cap K = \{e\}$, prove that G is isomorphic to a subgroup of $G/H \oplus G/K$.

Chapter 10 (some solution suggestions):

1) Note that $\det(AB) = (\det A)(\det B)$.

3) Note that $(f + g)' = f' + g'$.

5) $(\sigma\phi)(g_1 g_2) = \sigma(\phi(g_1 g_2)) = \sigma(\phi(g_1)\phi(g_2)) = \sigma(\phi(g_1))\sigma(\phi(g_2)) = (\sigma\phi)(g_1)(\sigma\phi)(g_2)$. Ker ϕ is a normal subgroup of Ker $\sigma\phi$. $|H|/|K| = [\operatorname{Ker}\sigma\phi : \operatorname{Ker}\phi]$.

7) $\phi((g, h)(g', h')) = \phi((gg', hh')) = gg' = \phi((g, h))\phi((g', h'))$. The kernel is $\{(e, h) \mid h \in H\}$.

9) Consider $\phi : \mathbb{Z} \oplus \mathbb{Z} \to \mathbb{Z}_a \oplus \mathbb{Z}_b$ given by $\phi((x, y)) = (x \bmod a, y \bmod b)$ and use the First Isomorphism Theorem.

12) Since $|\operatorname{Ker}\phi|$ is not 1 and divides 17, ϕ is the trivial map.

13) $\langle 5 \rangle$

15) Show that the mapping from K to KN/N given by $k \to kN$ is an onto homomorphism with kernel $K \cap N$.

17) $D_4, \{e\}, \mathbb{Z}_2, \mathbb{Z}_2 \oplus \mathbb{Z}_2$

18) It is divisible by 10. 10 can be replaced by any positive integer.

19) Let γ be the natural homomorphism from G onto G/N. Let $\bar{H}$ be a subgroup of G/N and let $\gamma^{-1}(\bar{H}) = H$. Then H is a subgroup of G and $H/N = \gamma(H) = \gamma\left(\gamma^{-1}(\bar{H})\right) = \bar{H}$.

21) The mapping $g \to \phi_g$ is a homomorphism with kernel $Z(G)$.

Chapter 11:

1) What is the smallest positive integer n such that there are two nonisomorphic groups of order n? Name the two groups.

2) What is the smallest positive integer n such that there are three nonisomorphic Abelian groups of order n? Name the three groups.

3) What is the smallest positive integer n such that there are exactly four nonisomorphic Abelian groups of order n? Name the four groups.

4) Prove that any Abelian group of order 45 has an element of order 15. Does every Abelian group of order 45 have an element of order 9?

5) Find all Abelian groups (up to isomorphism) of order 360.

6) How many Abelian groups (up to isomorphism) are there

(a) of order 6?

(b) of order 15?

(c) of order 42?

(d) of order pq, where p and q are distinct primes?

(e) of order pqr, where p, q, and r are distinct primes?

(f) Generalize parts d and e.

7) The set $\{1, 9, 16, 22, 29, 53, 74, 79, 81\}$ is a group under multiplication modulo 91. Determine the isomorphism class of this group.

8) Suppose that G is an Abelian group of order 9. What is the maximum number of elements (excluding the identity) of which one needs to compute the order to determine the isomorphism class of G? What if G has order 18? What about 16?

9) Let G be an Abelian group of order 16. Suppose that there are elements a and b in G such that $|a| = |b| = 4$ and $a^2 \neq b^2$. Determine the isomorphism class of G.

Chapter 11 (some solution suggestions):

1) $n = 4; \mathbb{Z}_4, \mathbb{Z}_2 \oplus \mathbb{Z}_2$

3) $n = 36; \mathbb{Z}_9 \oplus \mathbb{Z}_4, \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4, \mathbb{Z}_9 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2, \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

4) The only Abelian groups of order 45 are $\mathbb{Z}_{45}$ and $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$. In the first group, $|3| = 15$; in the second one, $|(1, 1, 1)| = 15$. $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$ does not have an element of order 9.

6) a. 1 b. 1 c. 1 d. 1 e. 1 f. There is a unique Abelian group of order n if and only if n is not divisible by the square of any prime.

7) $\mathbb{Z}_3 \oplus \mathbb{Z}_3$

8) $3; 6; 12$

9) $\mathbb{Z}_4 \oplus \mathbb{Z}_4$

Supplementary Problems for Chapters 9–11:

1) Suppose that H is a subgroup of G and that each left coset of H in G is some right coset of H in G. Prove that H is normal in G.

2) Prove that $\text{Inn}(G) \triangleleft \text{Aut}(G)$.

3) Let H be a subgroup of G. Prove H is a normal subgroup if and only if, for all a and b in G, $ab \in H$ implies $ba \in H$.

4) The factor group $GL(2,\mathbb{R})/SL(2,\mathbb{R})$ is isomorphic to some very familiar group. What is the group?

5) Let k be a divisor of n. The factor group $(\mathbb{Z}/\langle n\rangle)/(\langle k\rangle/\langle n\rangle)$ is isomorphic to some very familiar group. What is the group?

6) Let

$$H = \left\{ \left[\begin{array}{ccc} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{array} \right] \middle| a, b, c \in \mathbb{Q} \right\}$$

This is a group under matrix multiplication.

(a) Find $Z(H)$.

(b) Prove that $Z(H)$ is isomorphic to $\mathbb{Q}$ under addition.

(c) Prove that $H/Z(H)$ is isomorphic to $\mathbb{Q} \oplus \mathbb{Q}$.

(d) Are your proofs for parts a and b valid when $\mathbb{Q}$ is replaced by $\mathbb{R}$? Are they valid when $\mathbb{Q}$ is replaced by $\mathbb{Z}_p$, where p is prime?

7) Prove that $D_4/Z(D_4)$ is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

8) Show that $\mathbb{Q}/\mathbb{Z}$ has a unique subgroup of order n for each positive integer n.

9) Let G be a group of odd order. Prove that the mapping $x \to x^2$ from G to itself is one-to-one.

10) Suppose that $G = H \times K$ and that N is a normal subgroup of H. Prove that N is normal in G.

11) Suppose that ϕ is a homomorphism of $U(36)$, $\operatorname{Ker}\phi = \{1, 13, 25\}$, and $\phi(5) = 17$. Determine all elements that map to 17.

12) Show that any group with more than two elements has an automorphism other than the identity mapping.

13) A proper subgroup H of a group G is called maximal if there is no subgroup K such that $H \subset K \subset G$. Prove that $\mathbb{Q}$ under addition has no maximal subgroups.

14) Let G be the group $\left\{ \left[\begin{array}{cc} 1 & a \\ 0 & b \end{array} \right] \middle| \text{ where } a, b \in \mathbb{R}, b \neq 0 \right\}$ and $H = \left\{ \left[\begin{array}{cc} 1 & x \\ 0 & 1 \end{array} \right] \middle| \text{ where } x \in \mathbb{R} \right\}$. Show that H is a subgroup of G. Is H a normal subgroup of G? Justify your answer.

15) Recall that H is a characteristic subgroup of K if $\phi(H) = H$ for every automorphism ϕ of K. Prove that if H is a characteristic subgroup of K, and K is a normal subgroup of G, then H is a normal subgroup of G.

Supplementary Problems for Chapters 9–11 (some solution suggestions):

1) Say $aH = Hb$. Then $a = hb$ for some h in H. Then $Ha = Hhb = Hb = aH$.

2) Let $\alpha \in \operatorname{Aut}(G)$ and $\phi_a \in \operatorname{Inn}(G)$. Then $\left(\alpha\phi_a\alpha^{-1}\right)(x) = (\alpha\phi_a)\left(\alpha^{-1}(x)\right) = \alpha\left(a\alpha^{-1}(x)a^{-1}\right) = \alpha(a)x(\alpha(a))^{-1} = \phi_{a(a)}(x)$.

4) $\mathbb{R}^*$. Use the determinant map and apply the First Isomorphism Theorem.

6) a. $Z(H) = \left\{ \left[\begin{array}{ccc} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array} \right] \middle| b \in \mathbb{Q} \right\}$ b. The mapping $\left[\begin{array}{ccc} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array} \right] \to b$ is an isomorphism.

c. The mapping $\left[\begin{array}{ccc} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{array} \right] \to (a, c)$ is a homomorphism with $Z(H)$ as the kernel.

d. The proofs are valid with $\mathbb{R}$ and $\mathbb{Z}_p$

12) If the group is not Abelian, for any element a not in the center, the inner automorphism induced by a is not the identity; if the group is Abelian and contains an element a with $|a| > 2$, then $x \to x^{-1}$ works; if every nonidentity element has order 2, then G is isomorphic to a group of the form $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2$. In this case, the automorphism that takes $(a_1, a_2, a_3, \ldots, a_k)$ to $(a_2, a_1, a_3, \ldots, , a_k)$ is not the identity.

14) Observe that $\left[\begin{array}{cc} 1 & x \\ 0 & 1 \end{array} \right]\left[\begin{array}{cc} 1 & y \\ 0 & 1 \end{array} \right] = \left[\begin{array}{cc} 1 & x+y \\ 0 & 1 \end{array} \right]$, so H is closed. Also, $\left[\begin{array}{cc} 1 & x \\ 0 & 1 \end{array} \right]^{-1} = \left[\begin{array}{cc} 1 & -x \\ 0 & 1 \end{array} \right]$, which is in H. Thus, H is a subgroup of G. Since $\left[\begin{array}{cc} 1 & a \\ 0 & b \end{array} \right]\left[\begin{array}{cc} 1 & x \\ 0 & 1 \end{array} \right]\left[\begin{array}{cc} 1 & a \\ 0 & b \end{array} \right]^{-1} = \left[\begin{array}{cc} 1 & a \\ 0 & b \end{array} \right]\left[\begin{array}{cc} 1 & x \\ 0 & 1 \end{array} \right]\left[\begin{array}{cc} 1 & -ab^{-1} \\ 0 & b^{-1} \end{array} \right] = \left[\begin{array}{cc} 1 & b^{-1}x \\ 0 & 1 \end{array} \right]$ belongs to H, we have that H is normal in G.

15) Let g belong to G. Since $gKg^{-1} = K$, conjugation is an automorphism of K. Thus $gHg^{-1} = H$.

Chapter 12:

1) The ring $\{0, 2, 4, 6, 8\}$ under addition and multiplication modulo 10 has a unity. Find it.

2) Give an example of a subset of a ring that is a subgroup under addition but not a subring.

3) Find an integer n that shows that the rings $\mathbb{Z}_n$ need not have the following properties that the ring of integers has:

(a) $a^2 = a$ implies $a = 0$ or $a = 1$.

(b) $ab = 0$ implies $a = 0$ or $b = 0$.

(c) $ab = ac$ and $a \neq 0$ imply $b = c$.

Is the n you found prime?

4) Show that the three properties listed in the exercise above do hold in $\mathbb{Z}_p$ when p is prime.

5) Prove that the intersection of any collection of subrings of a ring R is a subring of R.

6) Let a, b, and c be elements of a commutative ring, and suppose that a is a unit. Prove that b divides c if and only if ab divides c.

7) Let R be a ring. The center of R is the set $\{x \in R \mid ax = xa \text{ for all } a \text{ in } R\}$. Prove that the center of a ring is a subring.

8) Suppose that $R_1, R_2, \ldots, R_n$ are rings that contain nonzero elements. Show that $R_1 \oplus R_2 \oplus \cdots \oplus R_n$ has a unity if and only if each R_i has a unity.

9) Let R be a commutative ring with unity and let $U(R)$ denote the set of units of R. Prove that $U(R)$ is a group under the multiplication of R. (This group is called the group of units of R.)

10) Determine $U(\mathbb{Z}[x])$.

11) Let m and n be positive integers and let k be the least common multiple of m and n. Show that $m\mathbb{Z} \cap n\mathbb{Z} = k\mathbb{Z}$.

12) Explain why every subgroup of $\mathbb{Z}_n$ under addition is also a subring of $\mathbb{Z}_n$.

13) Let $M_2(\mathbb{Z})$ be the ring of all 2×2 matrices over the integers and let $R = \left\{ \begin{bmatrix} a & a-b \\ a-b & b \end{bmatrix} \middle| a, b \in \mathbb{Z} \right\}$. Prove or disprove that R is a subring of $M_2(\mathbb{Z})$.

14) Suppose that R is a ring and that $a^2 = a$ for all a in R. Show that R is commutative.

A ring in which $a^2 = a$ for all a is called a Boolean ring, in honor of the mathematician George Boole (1815–1864).

Chapter 12 (some solution suggestions):

2) In $\mathbb{R}$, consider $\{n\sqrt{2} \mid n \in \mathbb{Z}\}$.

4) In $\mathbb{Z}_p$, nonzero elements have multiplicative inverses. Use them.

5) If a and b belong to the intersection, then they belong to each member of the intersection. Thus, $a - b$ and ab belong to each member of the intersection. So, $a - b$ and ab belong to the intersection.

7) Let a, b belong to the center. Then $(a - b)x = ax - bx = xa - xb = x(a - b)$. Also, $(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$.

8) $(x_1, \ldots, x_n)(a_1, \ldots, a_n) = (x_1, \ldots, x_n)$ for all x_i in R_i if and only if $x_i a_i = x_i$ for all x_i in R_i and $i = 1, \ldots, n$.

10) $f(x) = 1$ and $g(x) = -1$.

12) Every subgroup of $\mathbb{Z}_n$ is closed under multiplication.

13) The Subring Test is satisfied.

Chapter 13:

1) Which of following integral domains are fields? $\mathbb{Z}$, $\mathbb{Z}[i] = \{a + bi \mid a, b\mathbb{Z}\}$ (the Gaussian Integers), $\mathbb{Z}[x]$ (polynomials with integer coefficients), $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$, $\mathbb{Z}_p$ (p prime).

2) Show that every nonzero element of $\mathbb{Z}_n$ is a unit or a zero-divisor.

3) Find a nonzero element in a ring that is neither a zero-divisor nor a unit.

4) Let R be a finite commutative ring with unity. Prove that every nonzero element of R is either a zero-divisor or a unit. What happens if we drop the "finite" condition on R?

5) A ring element a is called an idempotent if $a^2 = a$. Prove that the only idempotents in an integral domain are 0 and 1.

6) (Subfield Test) Let F be a field and let K be a subset of F with at least two elements. Prove that K is a subfield of F if, for any $a, b \in K$ such that $b \neq 0$, we have $a - b$ and ab^{-1} belong to K.

7) 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?

8) The nonzero elements of $\mathbb{Z}_3[i]$ form an Abelian group of order 8 under multiplication. Is it isomorphic to $\mathbb{Z}_8, \mathbb{Z}_4 \oplus \mathbb{Z}_2$, or $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$?

9) Suppose that R is a commutative ring without zero-divisors. Show that the characteristic of R is 0 or prime.

10) Let R be a ring and let $M_2(R)$ be the ring of 2×2 matrices with entries from R. Explain why these two rings have the same characteristic.

11) Consider the equation $x^2 - 5x + 6 = 0$.

(a) How many solutions does this equation have in $\mathbb{Z}_7$?

(b) Find all solutions of this equation in $\mathbb{Z}_8$.

(c) Find all solutions of this equation in $\mathbb{Z}_{12}$.

(d) Find all solutions of this equation in $\mathbb{Z}_{14}$.

12) Describe the smallest subfield of the field of real numbers that contains $\sqrt{2}$. (That is, describe the subfield K with the property that K contains $\sqrt{2}$ and if F is any subfield containing $\sqrt{2}$, then F contains K.)

13) Let F be a field of order 32. Show that the only subfields of F are F itself and $\{0, 1\}$.

Chapter 13 (some solution suggestions):

2) Let $k \in \mathbb{Z}_n$. If $\gcd(k, n) = 1$, then k is a unit. If $\gcd(k, n) = d > 1$, write $k = sd$. Then $k(n/d) = sd(n/d) = sn = 0$.

4) Let $s \in R, s \neq 0$. Consider the set $S = \{sr \mid r \in R\}$. If $S = R$, then $sr = 1$ (the unity) for some r. If $S \neq R$, then there are distinct r_1 and r_2 such that $sr_1 = sr_2$. In this case, $s(r_1 - r_2) = 0$. To see what happens when the "finite" condition is dropped, consider $\mathbb{Z}$.

6) See the one-step subgroup test and subring test.

8) $\mathbb{Z}_8$

10) $n \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ for all members of $M_2(R)$ if and only if $na = 0$ for all a in R.

11) a. 2 b. 2,3 c. $2, 3, 6, 11$ d. $2, 3, 9, 10$

12) This is $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

Chapter 14:

1) Verify that principal ideals are in fact ideals: Let R be a commutative ring with unity and $a \in R$. Show that $(a) = \{ra \mid r \in R\}$ is an ideal of R.

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

3) Find all maximal ideals in

(a) $\mathbb{Z}_8$.

(b) $\mathbb{Z}_{10}$.

(c) $\mathbb{Z}_{12}$.

(d) $\mathbb{Z}_n$.

4) If n is an integer greater than 1, show that $(n) = n\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$ if and only if n is prime.

5) If A and B are ideals of a ring, show that the sum of A and B, $A + B = \{a + b \mid a \in A, b \in B\}$, is an ideal.

6) In the ring of integers, find a positive integer a such that

(a) $(a) = (2) + (3)$.

(b) $(a) = (6) + (8)$.

(c) $(a) = (m) + (n)$.

7) If A and B are ideals of a ring, show that the product of A and B, $AB = \{a_1b_1 + \cdots + a_nb_n \mid a_i \in A, b_i \in B\}$, is an ideal.

8) Find a positive integer a such that

(a) $(a) = (3)(4)$.

(b) $(a) = (6)(8)$.

(c) $(a) = (m)(n)$.

9) If A is an ideal of a ring R and 1 belongs to A, prove that $A = R$.

10) If an ideal I of a ring R contains a unit, show that $I = R$.

11) Let $I = (2)$. Prove that $I[x]$ is not a maximal ideal of $\mathbb{Z}[x]$ even though I is a maximal ideal of $\mathbb{Z}$.

12) If R is a commutative ring with unity and A is a proper ideal of R, show that R/A is a commutative ring with unity.

13) Prove that the only ideals of a field F are $\{0\}$ and F itself.

14) Show that $A = \{(3x, y) \mid x, y \in \mathbb{Z}\}$ is a maximal ideal of $\mathbb{Z} \oplus \mathbb{Z}$. What happens if $3x$ is replaced by $4x$? Generalize.

15) In $\mathbb{Z} \oplus \mathbb{Z}$, let $I = \{(a, 0) \mid a \in \mathbb{Z}\}$. Show that I is a prime ideal but not a maximal ideal.

16) In $\mathbb{Z}_5[x]$, let $I = \left(x^2 + x + 2\right)$. Find the multiplicative inverse of $2x + 3 + I$ in $\mathbb{Z}_5[x]/I$.

17) An integral domain D is called a principal ideal domain if every ideal of D has the form $(a) = \{ad \mid d \in D\}$ for some a in D. Show that $\mathbb{Z}$ is a principal ideal domain.

18) Let R be a commutative ring and let A be any subset of R. Show that the annihilator of $A, \text{Ann}(A) = \{r \in R \mid \text{ra} = 0$ for all a in $A\}$, is an ideal.

19) Show that $\mathbb{Z}_3[x]/\left(x^2 + x + 1\right)$ is not a field.

20) Let R be a commutative ring with unity and let $a, b \in R$. Show that (a, b), the smallest ideal of R containing a and b, is $I = \{ra + sb \mid r, s \in R\}$. That is, show I contains a and b and that any ideal containing them also contains I.

Chapter 14 (some solution suggestions):

1) Let r_1a and r_2a belong to (a). Then $r_1a - r_2a = (r_1 - r_2)\, a \in (a)$. If $r \in R$ and $r_1a \in (a)$, then $r\,(r_1a) = (r_1)\, a \in (a)$.

4) If n is prime, use Euclid's Lemma. If n is not prime, say $n = st$ where $s < n$ and $t < n$; then st belongs to $n\mathbb{Z}$ but s and t do not.

6) a. $a = 1$ b. $a = 2$ c. $a = \gcd(m, n)$

8) a. $a = 12$ b. $a = 48$. To see this, note that every element of $(6)(8)$ has the form $6t_18k_1 + 6t_28k_2 + \cdots + 6t_n8k_n = 48s \in (48)$. So, $(6)(8) \subseteq (48)$. Also, since $48 \in (6)(8)$, we have $(48) \subseteq (6)(8)$. c. $a = mn$

9) Let $r \in R$. Then $r = 1r \in A$.

10) Let $u \in I$ be a unit and let $r \in R$. Then $r = r\left(u^{-1}u\right) = \left(ru^{-1}\right) u \in I$.

13) Use the previous exercise.

15) Use the Theorem: Let R be a commutative ring with unity and I an ideal of R. Then (a) I is prime if and only if R/I is an integral domain and (b) I is maximal if and only if R/I is a field.

16) $3x + 1 + I$

17) Every ideal is a subgroup. Every subgroup of a cyclic group is cyclic.

18) Say $b, c \in \text{Ann}(A)$. Then $(b - c)a = ba - ca = 0 - 0 = 0$. Also, $(rb)a = r(ba) = r \cdot 0 = 0$.

19) $x + 2 + \left(x^2 + x + 1\right)$ is not zero, but its square is.

20) Taking $r = 1$ and $s = 0$ shows that $a \in I$. Taking $r = 0$ and $s = 1$ shows that $b \in I$. If J is any ideal that contains a and b, then it contains I because of the closure conditions.

Supplementary Problems for Chapters 12–14:

1) Let R be a commutative ring with more than one element. Prove that if for every nonzero element a of R we have $aR = R$, then R is a field.

2) Let A, B, and C be ideals of a ring R. If $AB \subseteq C$ and C is a prime ideal of R, show that $A \subseteq C$ or $B \subseteq C$. (Compare this with Euclid's Lemma.)

3) Show, by example, that the intersection of two prime ideals need not be a prime ideal.

4) Let $\mathbb{R}$ denote the ring of real numbers. Determine all ideals of $\mathbb{R} \oplus \mathbb{R}$. What happens if $\mathbb{R}$ is replaced by any field F?

5) Determine all factor rings of $\mathbb{Z}$.

6) Let A, B, and C be subrings of a ring R. If $A \subseteq B \cup C$, show that $A \subseteq B$ or $A \subseteq C$.

7) Show that $\mathbb{Z}_n[x]$ has characteristic n.

8) Show that the direct sum of two integral domains is not an integral domain.

9) Consider the ring $R = \{0, 2, 4, 6, 8, 10\}$ under addition and multiplication modulo 12. What is the characteristic of R?

10) What is the characteristic of $\mathbb{Z}_m \oplus \mathbb{Z}_n$? Generalize.

11) Let R be a commutative ring with unity. Suppose that the only ideals of R are $\{0\}$ and R. Show that R is a field.

12) Show that in the ring $\mathbb{Z}[x]/(2x+1)$, the element $x + (2x+1)$ is a unit.

13) Let $a \in \mathbb{Z}$. Show that (a) is not a maximal ideal in $\mathbb{Z}[x]$.

14) If R is a finite commutative ring with unity, prove that every prime ideal of R is a maximal ideal of R.

15) Find the characteristic of $\mathbb{Z}[i]/(2+i)$.

16) Show that $4x^2 + 6x + 3$ is a unit in $\mathbb{Z}_8[x]$.

17) Prove that (x, y) is a maximal ideal in $\mathbb{Z}_5[x, y]$.

18) If x is a nilpotent element in a commutative ring R, prove that rx is nilpotent for all r in R.

19) List the distinct elements in the ring $\mathbb{Z}[x]/\left\langle 3, x^2+1 \right\rangle$. Show that this ring is a field.

Supplementary Problems for Chapters 12–14 (some solution suggestions):

2) Suppose $A \not\subseteq C$ and $B \not\subseteq C$. Pick $a \in A$ and $b \in B$ such that $a, b \notin C$. But $ab \in C$ and C is prime.

4) $\{0\} \oplus \{0\}, \mathbb{R} \oplus \mathbb{R}, \mathbb{R} \oplus \{0\}$, and $\{0\} \oplus \mathbb{R}$. The ideals of $F \oplus F$ are $\{0\} \oplus \{0\}, F \oplus F$, $F \oplus \{0\}$, and $\{0\} \oplus F$.

6) Suppose $a_1, a_2 \in A$ but $a_1 \notin B$ and $a_2 \notin C$. Use $a_1 + a_2$ to derive a contradiction.

9) 6

11) Consider a non-zero element and look at its principal ideal. This must contain 1.

12) Since $2x+1+(2x+1) = 0+(2x+1)$, we have $-2x+(2x+1) = 1+(2x+1)$. So, $(-2+(2x+1))(x+(2x+1)) = 1+(2x+1)$.

14) Finite integral domains are fields. Now use the theorem that says, for a commutative ring with unity R and ideal I, R/I is an integral domain if and only if I is prime and that R/I is a field if and only if I is maximal.

15) 5

16) The inverse is $2x + 3$.

17) Observe that $\mathbb{Z}_5[x, y]/(x, y) = \mathbb{Z}_5$ and use the fact that in a commutative ring with unity, quotients are fields exactly when ideals are maximal.

18) If $x^n = 0$, then $(rx)^n = r^n x^n = 0$.

Chapter 15:

1) Prove basic properties of homomorphisms: Let $\phi : R \to S$ be a homomorphism between rings R and S. Let A be a subring of R and B be an ideal of S.

(a) $\phi(nr) = n\phi(r)$ for all $r \in R$ and $n \in \mathbb{Z}$. When $n > 0$ we also have $\phi(r^n) = \phi(r)^n$.

(b) $\phi(A) = \{\phi(x) \mid x \in A\}$ is a subring of S.

(c) If A is an ideal of R and ϕ is onto, then $\phi(A)$ is an ideal of S.

(d) $\phi^{-1}(B) = \{x \in R \mid \phi(x) \in B\}$ is an ideal of R.

(e) If R is commutative, then $\phi(R)$ is commutative.

(f) If R has unity, $S \neq \{0\}$, and ϕ is onto, then $\phi(1)$ is the unity of S.

(g) ϕ is an isomorphism if and only if ϕ is onto and $\text{Ker}(\phi) = \{r \in R \mid \phi(r) = 0\} = \{0\}$.

(h) If ϕ is an isomorphism from R onto S, then ϕ^{-1} is an isomorphism from S onto R.

2) If $\phi : R \to S$ is a homomorphism, then $\text{Ker}(\phi)$ is an ideal of R.

3) Let $\phi : R \to S$ be a homomorphism. The mapping from $R/\text{Ker}(\phi)$ to $\phi(R)$ given by $r + \text{Ker}(\phi) \mapsto \phi(r)$ is an isomorphism. In particular, $R/\text{Ker}(\phi) \cong \phi(R)$.

4) Every ideal of a ring R is the kernel of some ring homomorphism of R. In particular, an ideal A is the kernel of the mapping $r \mapsto r + A$ from R to R/A (i.e., the projection mapping).

5) Show that the correspondence $x \to 5x$ from $\mathbb{Z}_5$ to $\mathbb{Z}_{10}$ does not preserve addition.

6) Show that the correspondence $x \to 3x$ from $\mathbb{Z}_4$ to $\mathbb{Z}_{12}$ does not preserve multiplication.

7) Prove that the intersection of any collection of subfields of a field F is a subfield of F.

8) Let $\mathbb{Z}_3[i] = \{a + bi \mid a, b \in \mathbb{Z}_3\}$. Show that the field $\mathbb{Z}_3[i]$ is ring-isomorphic to the field $\mathbb{Z}_3[x]/\left(x^2 + 1\right)$.

9) Let

$$S = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \mid a, b \in \mathbb{R} \right\}$$

Show that $\phi : \mathbb{C} \to S$ given by

$$\phi(a + bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

is a ring isomorphism.

10) Let $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ and

$$H = \left\{ \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \mid a, b \in \mathbb{Z} \right\}.$$

Show that $\mathbb{Z}[\sqrt{2}]$ and H are isomorphic as rings.

11) Describe the kernel of the homomorphism $\phi : \mathbb{R}[x] \to \mathbb{R}$ given by $\phi(f(x)) = f(1)$.

12) Determine all ring homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}$.

13) Show that $(\mathbb{Z} \oplus \mathbb{Z})/((a) \oplus (b))$ is ring-isomorphic to $\mathbb{Z}_a \oplus \mathbb{Z}_b$

14) Let m be a positive integer and let n be an integer obtained from m by rearranging the digits of m in some way. (For example, 72345 is a rearrangement of 35274 .) Show that $m - n$ is divisible by 9 .

15) (Test for Divisibility by 11) Let n be an integer with decimal representation $a_k a_{k-1} \cdots a_1 a_0$. Prove that n is divisible by 11 if and only if $a_0 - a_1 + a_2 - \cdots (-1)^k a_k$ is divisible by 11.

16) Is there a ring homomorphism from the reals to some ring whose kernel is the integers?

17) Suppose that R and S are commutative rings with unities. Let ϕ be a ring homomorphism from R onto S and let A be an ideal of S.

(a) If A is prime in S, show that $\phi^{-1}(A) = \{x \in R \mid \phi(x) \in A\}$ is prime in R.

(b) If A is maximal in S, show that $\phi^{-1}(A)$ is maximal in R.

18) Let R and S be rings.

(a) Show that the mapping from $R \oplus S$ onto R given by $(a, b) \to a$ is a ring homomorphism.

(b) Show that the mapping from R to $R \oplus S$ given by $a \to (a, 0)$ is a one-to-one ring homomorphism.

(c) Show that $R \oplus S$ is ring-isomorphic to $S \oplus R$.

19) Let $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ and $\mathbb{Q}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$. Show that these two rings are not ring-isomorphic.

20) Let $R = \left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} \mid a, b \in \mathbb{Z} \right\}$, and let ϕ be the mapping that takes $\begin{bmatrix} a & b \\ b & a \end{bmatrix}$ to $a - b$.

(a) Show that ϕ is a homomorphism.

(b) Determine the kernel of ϕ.

(c) Show that $R/\text{Ker}\phi$ is isomorphic to $\mathbb{Z}$.

(d) Is Ker ϕ a prime ideal?

(e) Is Ker ϕ a maximal ideal?

Chapter 15 (some solution suggestions):

1) Property c: $\phi(A)$ is a subgroup because ϕ is a group homomorphism. Let $s \in S$ and $\phi(r) = s$. Then $s\phi(a) = \phi(r)\phi(a) = \phi(ra)$ and $\phi(a)s = \phi(a)\phi(r) = \phi(ar)$. Property d: Let a and b belong to $\phi^{-1}(B)$ and r belong to R. Then $\phi(a)$ and $\phi(b)$ are in B. So, $\phi(a) - \phi(b) = \phi(a) + \phi(-b) = \phi(a - b) \in B$. Thus, $a - b \in B$. Also, ϕ(ra) $= \phi(r)\phi(a) \in B$ and $\phi(ar) = \phi(a)\phi(r) \in B$. So, ra and $ar \in \phi^{-1}(B)$.

3) We already know the mapping is an isomorphism of groups. Let $\Phi(x + \operatorname{Ker}\phi) = \phi(x)$. Note that $\Phi((r + \operatorname{Ker}\phi)(s + \operatorname{Ker}\phi)) = \Phi(rs + \operatorname{Ker}\phi) = \phi(rs) = \phi(r)\phi(s) = \Phi(r + \operatorname{Ker}\phi)\Phi(s + \operatorname{Ker}\phi)$.

5) $\phi(2 + 4) = \phi(1) = 5$, whereas $\phi(2) + \phi(4) = 0 + 0 = 0$.

7) If a and b ($b \neq 0$) belong to every member of the collection, then so do $a - b$ and ab^{-1}. Thus, by the Subfield Test, the intersection is a subfield.

9) Apply the definition.

11) The set of all polynomials passing through the point $(1, 0)$.

12) The zero map and the identity map.

14) Say $m = a_k a_{k-1} \ldots a_1 a_0$ and $n = b_k b_{k-1} \ldots b_1 b_0$. Then $m - n = (a_k - b_k)\,10^k + (a_{k-1} - b_{k-1})\,10^{k-1} + \cdots + (a_1 - b_1)\,10 + (a_0 - b_0)$. Now use the test for divisibility by 9 .

16) No. The kernel must be an ideal.

17) a. Suppose $ab \in \phi^{-1}(A)$. Then $\phi(a)\phi(b) \in A$, so that $a \in \phi^{-1}(A)$ or $b \in \phi^{-1}(A)$. b. Consider the natural homomorphism from R to S/A. Then use the First Isomorphism Theorem and that (for commutative rings with 1) S/A is a field if and only if A is maximal.

18) a. $\phi((a, b) + (a', b')) = \phi((a + a', b + b')) = a + a' = \phi((a, b)) + \phi((a', b'))$, so ϕ preserves addition. Also, $\phi((a, b)(a', b')) = \phi((aa', bb')) = aa' = \phi((a, b))\phi((a', b'))$. b. $\phi(a) = \phi(b)$ implies that $(a, 0) = (b, 0)$, which implies that $a = b \cdot \phi(a + b) = (a + b, 0) = (a, 0) + (b, 0) = \phi(a) + \phi(b)$. Also, $\phi(ab) = (ab, 0) = (a, 0)(b, 0) = \phi(a)\phi(b)$. c. Use $(r, s) \to (s, r)$.

Original Problem Numbers:

Note: These problems and solution suggestions are drawn from Gallian's *Contemporary Abstract Algebra* 8th edition.
I renumbered the problems (using consecutive numbers). The original numbers are listed below:

Chapter	Problem #	Chapter	Problem #
0	1,3,4,6,8,9,11,16,19,28,38,58–60	Supp. 5–8	1–3,12,14,16,21,22,29,34,43,45,47,50,51
1	2,3,9–11,16,24	9	1,2,6,7,9,11–16,19,23,37,39,45,49,54,56,65,67,71
2	1,2,5,7,10,11,13,24–26,30,31,33,34,47,52	10	1–4,7–11,14,16,19,21,24,41,42,45,47,51,53,58
3	1–4,7,21,23,28,29,32–34,37,42,52,53,57,58, 67,73,74	11	1–3,5,10,15,21,29,31
4	1,3,8,11,21,29,33,41,52,57,63,69,76	Supp. 9–11	1,5–10,14,16,18,22,35,36,39,41
Supp. 1–4	1,2,4,5,13,18,20,32,35,47	12	2,3,6,7,9,12,19,21,22,25,36,37,41,50
5	2,3,8,9,11,16,19,23,25,28,35,44,45,62,63,66	13	2,5–7,18,29,42,43,48,53,57,61,68
6	3,5,7,10,15,28,29,31,32,38,39,43,49,53,57	14	1,4,6,9–13,15,17,22,26,27,30,35,39,41,45,53,63
7	1,3,5,8,11,16,17,22,26,45,57,60,62	Supp. 12–14	4–8,11,14,16–19,21,22,29,39,41,43,51,52
8	3,4,7–9,17,18,23,26,31,32,55,71	15	1–6,11–14,19,23,28,31,32,45,47,49,56,66