MATH 417, HOMEWORK 7 & 8

CHARLES ANCEL

I know that homework for chapter III.16 was due last week so I understand that it may not be worth any points but please let me know if it is correct. Have a great night and thank you for grading all of our work!

Chapter III.16

Exercise 8(dfgh). Mark each of the following true or false.
d. Let X be a G-set with x_1, $x_2 \in X$ and $g \in G$. If $gx_1 = gx_2$, then $x_1 = x_2$.
f. Each orbit of a G-set X is a transitive sub-G-set.
g. Let X be a G-set and let $H \leq G$. Then X can be regarded in a natural way as an H-set.
h. With reference to (g), the orbits in X under H are the same as the orbits in X under G.

Proof. **d. Let X be a G-set with x_1, $x_2 \in X$ and $g \in G$. If $gx_1 = gx_2$, then $x_1 = x_2$.**

This statement is true if the action of G on X is faithful (or free). Recall that a group action is faithful if, whenever $g \cdot x = h \cdot x$ for all x in X, then $g = h$. In the context of this statement, if the action of g on both x_1 and x_2 results in the same element, then x_1 must equal x_2.

Answer: True(assuming the action is faithful).

—

f. Each orbit of a G-set X is a transitive sub-G-set.

By definition, the orbit of an element x in X under the action of G is the set of all elements of X to which x can be moved by the action of some element in G. Therefore, for any two elements y, z in the same orbit, there exists $g_1, g_2 \in G$ such that $g_1 \cdot x = y$ and $g_2 \cdot x = z$. It follows that $z = g_2 \cdot x = g_2 \cdot (g_1^{-1} \cdot y) = (g_2 g_1^{-1}) \cdot y$, where $g_2 g_1^{-1} \in G$. This shows that any two elements in the same orbit can be related by the action of some element in G, which means the orbit is a transitive subset of X.

Answer: True.

—

g. Let X be a G-set and let $H \leq G$. Then X can be regarded in a natural way as an H-set.

If H is a subgroup of G, then every element of H is also an element of G. This means that every action of H on X is also an action of G on X. So, X can naturally be regarded as an H-set using the same group action.

Answer: True.

—

h. With reference to (g), the orbits in X under H are the same as the orbits in X under G.

This is not necessarily true. Consider the group action of G on X. It's possible that H (being a subgroup) might not move X around as much as G does. Thus, while G might move an element x in X to a wide variety of other positions, H might only move x to a subset of those positions. This means that the orbits of X under the action of H might be smaller or at least different than the orbits of X under the action of G.

Answer: False.

— □

Exercise 12. Let X be a G-set and let $Y \subseteq X$. Let $G_Y = \{g \in G \mid, g_y = y \forall y \in Y\}$. Show G_Y is a subgroup of G, generalizing Theorem 16.12.

Proof. To prove that G_Y is a subgroup of G, we'll use the subgroup test. For G_Y to be a subgroup, it must satisfy:

1. The identity element of G, e, is in G_Y. 2. If $g_1, g_2 \in G_Y$, then their product $g_1 g_2$ is in G_Y. 3. If $g \in G_Y$, then its inverse g^{-1} is in G_Y.

Let's prove each of these properties:

1. **Identity element:** For any $y \in Y$, $ey = y$. Thus, $e \in G_Y$.

2. **Closure:** Let $g_1, g_2 \in G_Y$. This means that $g_1 y = y$ and $g_2 y = y$ for all $y \in Y$. We want to show that $(g_1 g_2)y = y$ for all $y \in Y$.

Given $g_1 y = y$ and $g_2 y = y$, we have:

$$(g_1 g_2)y = g_1(g_2 y) = g_1 y = y$$

This shows that $g_1 g_2 \in G_Y$ and thus G_Y is closed under the induced operation of G.

3. **Inverse:** Let $g \in G_Y$. This means $G_Y = y$ for all $y \in Y$. We want to show that $g^{-1}y = y$ for all $y \in Y$.

Since $G_Y = y$, we have:

$$y = ey = (g^{-1}g)y = g^{-1}(G_Y) = g^{-1}y$$

Thus, $g^{-1} \in G_Y$.

Since G_Y satisfies all three properties, we conclude that G_Y is a subgroup of G, generalizing Theorem 16.12. □

Chapter III.17

Exercise 1. Find the number of orbits in $\{1, 2, 3, 4, 5, 6, 7, 8\}$ under the cyclic subgroup $\langle(1, 3, 5, 6)\rangle$ of S_8.

To find the number of orbits in $\{1, 2, 3, 4, 5, 6, 7, 8\}$ under the cyclic subgroup $\langle(1, 3, 5, 6)\rangle$ of S_8, we'll first need to understand the action of the subgroup on the set.

Recall that in the symmetric group S_8, the cycle notation $(1, 3, 5, 6)$ represents the permutation that sends: 1. 1 to 3 2. 3 to 5 3. 5 to 6 4. 6 to 1 5. And leaves all other numbers fixed.

Since our subgroup is generated by this single cycle, the only elements in the subgroup are powers of this cycle and the identity: 1. e: the identity permutation (does nothing) 2. $(1, 3, 5, 6)$: described above 3. $(1, 3, 5, 6)^2 = (1, 5)(3, 6)$: sends 1 to 5, 5 to 1, 3 to 6, 6 to 3, and leaves all other numbers fixed. 4. $(1, 3, 5, 6)^3 = (1, 6, 5, 3)$: the inverse of the original cycle.

Let's compute the orbits:

Proof. 1. Start with 1: The powers of the cycle send 1 to 3, 5, 6, and then back to 1. So the orbit of 1 under the subgroup is $\{1, 3, 5, 6\}$.

2. Take 2: 2 is not affected by any element in our subgroup (it remains fixed). So its orbit is $\{2\}$.

3. Take 4: Similar to 2, 4 is not affected by any element in our subgroup. So its orbit is $\{4\}$.

4. Take 7: Again, 7 remains fixed under all elements of our subgroup. So its orbit is $\{7\}$.

5. Take 8: Similarly, 8 remains fixed under all elements of our subgroup. So its orbit is $\{8\}$.

So, the orbits are: $\{1, 3, 5, 6\}$, $\{2\}$, $\{4\}$, $\{7\}$, and $\{8\}$.

Hence, there are 5 orbits in $\{1, 2, 3, 4, 5, 6, 7, 8\}$ under the cyclic subgroup $\langle(1, 3, 5, 6)\rangle$ of S_8. □

Chapter VII.36

Exercise 2. To determine the order of a Sylow 3-subgroup of a group with order 54, let's first express 54 in terms of its prime factorization:

$$54 = 2 \times 3^3$$

The highest power of 3 that divides 54 is 3^3.

Given the Sylow Theorems, a Sylow p-subgroup of a group G of order $p^n \cdot m$ (where p does not divide m) has order p^n.

In this case, $p = 3$ and $n = 3$. Therefore, a Sylow 3-subgroup of a group of order 54 has order $3^3 = 27$.

Answer: A Sylow 3-subgroup of a group of order 54 has order $\boxed{27}$. **Exercise 10.**

Mark each of the following true or false. a. Any two Sylow p-subgroups of a finite group are conjugate.
b. Theorem 36.11 shows that a group of order 15 has only one Sylow 5-subgroup.
c. Every Sylow p-subgroup of a finite group has order a power of p.
d. Every p-subgroup of every finite group is a Sylow p-subgroup.
e. Every finite abelian group has exactly one Sylow p-subgroup for each prime p dividing the order of G.
f. The normalizer in G of a subgroup H of G is always a normal subgroup of G.
g. If H is a subgroup of G, then H is always a normal subgroup of $N[H]$.
h. A Sylow p-subgroup of a finite group G is normal in G if and only if it is the only Sylow p-subgroup of G.
i. If G is an abelian group and H is a subgroup of G, then $N[H] = H$.
j. A group of prime-power order p^n has no Sylow p-subgroup.

Proof. **a. Any two Sylow p-subgroups of a finite group are conjugate.**

Answer: True. This is one of the Sylow theorems.

—

b. Theorem 36.11 shows that a group of order 15 has only one Sylow 5-subgroup.

Without the explicit content of Theorem 36.11, it's hard to say for certain, but the statement itself is true. A group of order 15 has only one Sylow 5-subgroup, which must be normal.

Answer: True.

—

c. Every Sylow p-subgroup of a finite group has order a power of p.

Answer: True. This is the definition of a Sylow p-subgroup.

—

d. Every p-subgroup of every finite group is a Sylow p-subgroup.

Answer: False. A Sylow p-subgroup is a p-subgroup of largest order. Not every p-subgroup has to be a Sylow p-subgroup.

—

e. Every finite abelian group has exactly one Sylow p-subgroup for each prime p dividing the order of G.

Answer: True. In an abelian group, any two subgroups of the same order are conjugate, and since Sylow subgroups are conjugate by the Sylow theorems, there can only be one distinct Sylow p-subgroup.

—

f. The normalizer in G of a subgroup H of G is always a normal subgroup of G.

Answer: False. The normalizer of H in G, denoted $N_G(H)$, is the largest subgroup of G in which H is normal. However, this doesn't mean $N_G(H)$ itself is normal in G.

—

g. If H is a subgroup of G, then H is always a normal subgroup of $N[H]$.

Answer: True. By definition, the normalizer $N[H]$ is the largest subgroup of G in which H is normal.

—

h. A Sylow p-subgroup of a finite group G is normal in G if and only if it is the only Sylow p-subgroup of G.

Answer: True. This follows from the Sylow theorems. If there is only one Sylow p-subgroup, it must be normal in G.

—

i. If G is an abelian group and H is a subgroup of G, then $N[H] = H$.

Answer: False. In an abelian group, every subgroup is normal. So, the normalizer of any subgroup H is the entire group G, i.e., $N[H] = G$.

—

j. A group of prime-power order p^n has no Sylow p-subgroup.

Answer: False. A group of order p^n has a Sylow p-subgroup of order p^n, which is the group itself.

□

Exercise 13. Show that every group of order 45 has a normal subgroup of order 9.

To show that every group G of order 45 has a normal subgroup of order 9, we can use the Sylow theorems. Let's break down the order of the group in terms of its prime factorization:

$$45 = 3^2 \times 5$$

From the Sylow theorems, the number of Sylow 3-subgroups (let's call it n_3) divides the order of the group, and $n_3 \equiv 1 \mod 3$. The possible values for n_3 are 1 or 5.

However, if n_3 were 5, then there would be $5(3^2 - 1) = 20$ elements of order 3 (since each Sylow 3-subgroup contributes $3^2 - 1$ elements of order 3, and these subgroups intersect trivially). This would leave only 25 elements in G not of order 3. But then, since the number of Sylow 5-subgroups divides 9 and is congruent to 1 mod 5, the only possible number of Sylow 5-subgroups is 1. This Sylow 5-subgroup has $5 - 1 = 4$ elements of order 5, leaving 21 elements unaccounted for, which is a contradiction.

Thus, n_3 cannot be 5. So, $n_3 = 1$, which means there is only one Sylow 3-subgroup, and it is therefore normal in G. This Sylow 3-subgroup has order $3^2 = 9$.

Proof. Let G be a group of order 45, and let n_3 be the number of Sylow 3-subgroups of G. From the Sylow theorems, n_3 divides 45 and $n_3 \equiv 1 \mod 3$. This means n_3 can only be 1 or 5.

Assume, for the sake of contradiction, that $n_3 = 5$. Then, there are $5(3^2 - 1) = 20$ elements of order 3 in G. This leaves only 25 elements not of order 3. Since the number of Sylow 5-subgroups divides 9 and is congruent to 1 mod 5, there can only be 1 Sylow 5-subgroup. This contributes 4 elements of order 5, leaving 21 elements unaccounted for, which is a contradiction.

Therefore, n_3 must be 1, and there is a unique Sylow 3-subgroup of G which is of order 9. Being the unique Sylow 3-subgroup, it is normal in G. □

Exercise 17. Show that every group of order $(35)^3$ has a normal subgroup of order 125.

We will show that every group G of order $35^3 = 5^3 \times 7^3$ has a normal subgroup of order $125 = 5^3$. We'll use the Sylow Theorems in our proof.

According to the Sylow Theorems, the number of Sylow 5-subgroups (denoted as n_5) satisfies 1. $n_5 \equiv 1 \pmod 5$, 2. n_5 divides 7^3.

The possible values of n_5 that satisfy these conditions are $1, 7, 49$.

Proof. Assume that G is a group of order 35^3. We'll prove that G has a normal subgroup of order 125.

We first consider the Sylow 5-subgroups of G. Let n_5 be the number of such subgroups. By the Sylow theorems, n_5 must be congruent to 1 mod 5 and must divide 7^3. So, the possible values for n_5 are $1, 7, 49$.

We proceed by cases:

1. If $n_5 = 1$, then there is a unique Sylow 5-subgroup of G, and it is normal by the Sylow theorems. This subgroup has order $5^3 = 125$, which is what we want to prove.

2. If $n_5 = 7$ or 49, we consider the action of G on the set of Sylow 5-subgroups by conjugation. This action gives rise to a homomorphism

$$\phi : G \to S_{n_5}$$

where S_{n_5} is the symmetric group on n_5 elements. The kernel of this homomorphism, denoted by $\ker(\phi)$, is a normal subgroup of G. By the first isomorphism theorem, $G/\ker(\phi)$ is isomorphic to a subgroup of S_{n_5}, and therefore

$$[G : \ker(\phi)] \leq |S_{n_5}| = n_5!.$$

Because the order of G is 35^3 and n_5 is either 7 or 49, we have

$$\ker(\phi) \geq \frac{35^3}{49!} \geq 5^3.$$

Thus, the kernel has at least 5^3 elements. Since it is a subgroup of G, its order must divide 35^3, so its order is at least $5^3 = 125$. Moreover, as the kernel of a homomorphism, it is a normal subgroup of G.

So, in all cases, we have shown that there exists a normal subgroup of G of order 125. □

Exercise 18. Show that there are no simple groups of order $255 = (3)(5)(17)$.

To show that there are no simple groups of order $255 = 3 \times 5 \times 17$, we will use the Sylow Theorems. Let's consider a group G of order 255.

1. The number of Sylow 17-subgroups of G (denoted n_{17}) satisfies:
- $n_{17} \equiv 1 \pmod{17}$
- n_{17} divides $3 \times 5 = 15$

The only possibility is $n_{17} = 1$. Thus, there is a unique Sylow 17-subgroup, which is normal in G by the Sylow Theorems.

2. Similarly, the number of Sylow 5-subgroups of G (denoted n_5) satisfies:
- $n_5 \equiv 1 \pmod{5}$
- n_5 divides $3 \times 17 = 51$

The possible values for n_5 are 1 and 51. If $n_5 = 1$, then there is a unique Sylow 5-subgroup, which is normal in G.

3. Lastly, the number of Sylow 3-subgroups of G (denoted n_3) satisfies:
- $n_3 \equiv 1 \pmod 3$
- n_3 divides $5 \times 17 = 85$

The possible values for n_3 are 1, 5, 17, and 85. If $n_3 = 1$, then there is a unique Sylow 3-subgroup, which is normal in G.

Proof. From the Sylow Theorems, we have determined that:
1. There is a unique Sylow 17-subgroup of G, which is normal.
2. There may be a unique Sylow 5-subgroup of G, which, if it exists, is normal.
3. There may be a unique Sylow 3-subgroup of G, which, if it exists, is normal.

Since a simple group has no non-trivial normal subgroups, and we've established that G has at least one non-trivial normal subgroup (from point 1), it follows that G cannot be simple.

Therefore, there are no simple groups of order 255. □

Chapter IV.18

Exercise 3. Compute the product in the given ring: $(11)(-4)$ in $\mathbb{Z}_15$.

Proof.

$$\begin{aligned} (11)(-4) &= -44 \\ -44 \mod 15 &= -14 \mod 15 \\ &= 1 \quad \text{(since -14 is congruent to 1 modulo 15)} \end{aligned}$$

Thus, the product $(11)(-4)$ in $\mathbb{Z}_{15}$ is 1. □

Exercise 9. Decide whether the indicated operations of addition and multiplication are defined (closed) on the set, and give a ring structure. If a ring is not formed, tell why this is the case. If a ring is formed, state whether the ring is commutative, whether it has unity, and whether it is a field.

- $\mathbb{Z} \times \mathbb{Z}$ with addition and multiplication by components.

Consider the set $\mathbb{Z}\times\mathbb{Z}$, which consists of ordered pairs of integers. We want to determine if the operations of addition and multiplication, defined component-wise, give a ring structure to this set.

Proof.
1. **Addition:** For any $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}$, the sum is defined as:

$$(a, b) + (c, d) = (a + c, b + d)$$

Since the sum of two integers is an integer, the result $(a + c, b + d)$ is still in $\mathbb{Z} \times \mathbb{Z}$. Thus, addition is closed.

2. **Multiplication:** For any $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}$, the product is defined as:

$$(a, b) \cdot (c, d) = (a \cdot c, b \cdot d)$$

Again, the product of two integers is an integer, so the result $(a \cdot c, b \cdot d)$ is in $\mathbb{Z} \times \mathbb{Z}$. Thus, multiplication is closed.

The usual ring axioms (associativity, distributivity, existence of an additive identity, existence of additive inverses, etc.) hold for $\mathbb{Z} \times \mathbb{Z}$ under these operations.

- The additive identity is $(0, 0)$ because for any (a, b), we have:

$$(a, b) + (0, 0) = (a + 0, b + 0) = (a, b)$$

- The additive inverse of (a, b) is $(-a, -b)$ because:

$$(a, b) + (-a, -b) = (a + (-a), b + (-b)) = (0, 0)$$

- The ring is **commutative** under both addition and multiplication. This is clear from the component-wise definitions of these operations.

- The ring has a **unity** or multiplicative identity, which is $(1, 1)$. For any (a, b), we have:

$$(a, b) \cdot (1, 1) = (a \cdot 1, b \cdot 1) = (a, b)$$

- However, the ring is **not a field**. To see why, consider the element $(1, 0)$. While $(1, 0)$ is not the zero element, it does not have a multiplicative inverse in $\mathbb{Z} \times \mathbb{Z}$. Any potential inverse (a, b) would need to satisfy $(1, 0) \cdot (a, b) = (1, 1)$, but this is impossible since the second component of the product is 0.

□

Exercise 11.
Decide whether the indicated operations of addition and multiplication are defined (closed) on the set, and give a ring structure. If a ring is not formed, tell why this is the case. If a ring is formed, state whether the ring is commutative, whether it has unity, and whether it is a field.

- $\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ with the usual addition and multiplication.

Consider the set $R = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$. We want to determine if the operations of addition and multiplication, as usually defined for real numbers, give a ring structure to this set.

Proof. 1. **Addition:** For any $x = a + b\sqrt{2}$ and $y = c + d\sqrt{2}$ in R, the sum is defined as:

$$x + y = (a + c) + (b + d)\sqrt{2}$$

Both $a + c$ and $b + d$ are integers, so $x + y$ belongs to R. Thus, addition is closed.

2. **Multiplication:** For any $x = a + b\sqrt{2}$ and $y = c + d\sqrt{2}$ in R, the product is defined as:

$$x \cdot y = (a \cdot c + 2b \cdot d) + (a \cdot d + b \cdot c)\sqrt{2}$$

Both $a \cdot c + 2b \cdot d$ and $a \cdot d + b \cdot c$ are integers, so $x \cdot y$ belongs to R. Thus, multiplication is closed.

The usual ring axioms (associativity, distributivity, existence of an additive identity, existence of additive inverses, etc.) hold for R under these operations.

• The additive identity is 0 because for any $x = a + b\sqrt{2}$, we have:

$$x + 0 = a + b\sqrt{2} + 0 = a + b\sqrt{2} = x$$

• The additive inverse of $x = a + b\sqrt{2}$ is $-x = -a - b\sqrt{2}$ because:

$$x + (-x) = a - a + b\sqrt{2} - b\sqrt{2} = 0$$

• The ring is **commutative** under both addition and multiplication. This is clear from the definitions of these operations.

• The ring has a **unity** or multiplicative identity, which is 1 because for any $x = a+b\sqrt{2}$, we have:

$$x \cdot 1 = (a + b\sqrt{2}) \cdot 1 = a + b\sqrt{2} = x$$

• To determine if the ring is a field, we'd need to check if every non-zero element has a multiplicative inverse in R. However, not every non-zero element in R has an inverse in R. For instance, the element $1 + \sqrt{2}$ does not have a multiplicative inverse in R. Thus, R is **not a field**.

□

Exercise 15. Describe all units in the given ring: • $\mathbb{Z} \times \mathbb{Z}$

For the ring $\mathbb{Z} \times \mathbb{Z}$, a unit (or invertible element) is an element that has a multiplicative inverse in the ring.

Proof. Consider an element (a, b) in $\mathbb{Z} \times \mathbb{Z}$. For (a, b) to be a unit, there must exist an element (c, d) in $\mathbb{Z} \times \mathbb{Z}$ such that:

$$(a, b) \cdot (c, d) = (1, 1)$$

From this, we get:

1) $ac = 1$ and 2) $bd = 1$

Given that a, b, c, and d are integers, the only way for ac to be 1 is if $a = c = 1$ or $a = c = -1$. Similarly, the only way for bd to be 1 is if $b = d = 1$ or $b = d = -1$.

From the above, we can deduce that the units in $\mathbb{Z} \times \mathbb{Z}$ are:

$$(1,1),\ (-1,-1),\ (1,-1),\ \text{and}\ (-1,1)$$

These are the only elements in $\mathbb{Z} \times \mathbb{Z}$ that have multiplicative inverses in the ring. □

So, the units in $\mathbb{Z} \times \mathbb{Z}$ are $(1,1), (-1,-1), (1,-1)$, and $(-1,1)$.

Exercise 24. Describe all ring homomorphisms of $\mathbb{Z}$ into $\mathbb{Z} \times \mathbb{Z}$.

To describe all ring homomorphisms $\phi : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$, we need to consider the properties that must be satisfied by a ring homomorphism. Specifically, for all $a, b \in \mathbb{Z}$:
1. $\phi(a + b) = \phi(a) + \phi(b)$
2. $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$
3. $\phi(1) = 1$ where 1 in $\mathbb{Z} \times \mathbb{Z}$ is the multiplicative identity, which is $(1, 1)$.

Proof. Let's use the properties of ring homomorphisms to determine the structure of ϕ:

1. Given $\phi(1) = (1, 1)$, we can determine ϕ for all integers. For any positive integer n, we have:

$$\phi(n) = \phi(1 + 1 + \cdots + 1) = \phi(1) + \phi(1) + \cdots + \phi(1) = (n, n)$$

Similarly, for any negative integer $-n$, we have:

$$\phi(-n) = -\phi(n) = (-n, -n)$$

2. For $a, b \in \mathbb{Z}$, using the properties of ring homomorphisms, we have:

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b)$$
$$\phi(a + b) = \phi(a) + \phi(b)$$

These properties confirm our above derivation for $\phi(n)$ and $\phi(-n)$.

Given these results, we can conclude that the only ring homomorphism $\phi : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ is given by:

$$\phi(n) = (n, n)$$

for all $n \in \mathbb{Z}$. □

Thus, the only ring homomorphism from $\mathbb{Z}$ into $\mathbb{Z} \times \mathbb{Z}$ maps each integer n to the ordered pair (n, n). **Exercise 33.** Mark each of the following true or false.

a. Every field is also a ring.
b. Every ring has a multiplicative identity.
c. Every ring with unity has at least two units.
d. Every ring with unity has at most two units.
e. It is possible for a subset of some field to be a ring but not a subfield, under the induced operations.
f. The distributive laws for a ring are not very important.

g. Multiplication in a field is commutative.
h. The nonzero elements of a field form a group under the multiplication in the field.
i. Addition in every ring is commutative.
j. Every element in a ring has an additive inverse.

Proof.

a. Every field is also a ring.
Answer: True. By definition, a field is a set with two operations (addition and multiplication) that satisfy the properties of a ring, and in addition, every non-zero element has a multiplicative inverse. So, a field satisfies all properties of a ring.

b. Every ring has a multiplicative identity.
Answer: False. There are rings without a multiplicative identity. Such rings are called non-unital rings.

c. Every ring with unity has at least two units.
Answer: True. The unity (or 1) is a unit by definition, and the additive inverse of the unity, -1, is also a unit. Thus, there are at least these two units in any ring with unity.

d. Every ring with unity has at most two units.
Answer: False. Consider the ring $\mathbb{Z}$. Both 1 and -1 are units, but so are any other integers coprime to the modulus.

e. It is possible for a subset of some field to be a ring but not a subfield, under the induced operations.
Answer: True. Consider the field $\mathbb{R}$ of real numbers. The subset $\mathbb{Z}$ of integers is a ring under the induced operations, but it's not a subfield because it lacks multiplicative inverses for all non-zero integers.

f. The distributive laws for a ring are not very important.
Answer: False. The distributive laws are essential for the structure of a ring. They ensure the compatibility of the two operations: addition and multiplication.

g. Multiplication in a field is commutative.
Answer: True. By definition, a field is a commutative ring where every non-zero element has a multiplicative inverse.

h. The nonzero elements of a field form a group under the multiplication in the field.
Answer: True. In a field, the set of non-zero elements is closed under multiplication, each element has a multiplicative inverse, and multiplication is associative. Thus, they form a group.

i. Addition in every ring is commutative.
Answer: True. Commutativity of addition is one of the defining properties of a ring.

j. Every element in a ring has an additive inverse.
Answer: True. The existence of additive inverses is one of the defining properties of a ring. □

Exercise 41. (Freshman exponentiation) Let p be a prime. Show that in the ring $\mathbb{Z}_p$ we have $(a+b)^p = a^p + b^p$ for all $a, b \in Zp$. [Hint: Observe that the usual binomial expansion for $(a+b)^n$ is valid in a commutative ring.]

Proof. To prove the statement, we'll first consider the binomial expansion of $(a+b)^p$ in a commutative ring:

$$(a+b)^p = \binom{p}{0}a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \cdots + \binom{p}{p-1}ab^{p-1} + \binom{p}{p}b^p$$

Now, for any integer $1 \leq k \leq p-1$, the binomial coefficient $\binom{p}{k}$ is given by:

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

Observe that the numerator $p!$ has p as a factor (since $p! = p \times (p-1)!$), but neither $k!$ nor $(p-k)!$ have p as a factor (since $1 \leq k \leq p-1$). Therefore, when working in $\mathbb{Z}_p$, $\binom{p}{k}$ is equivalent to 0 for all $1 \leq k \leq p-1$ since it's a multiple of p.

So, the only terms that remain in the expansion of $(a+b)^p$ in $\mathbb{Z}_p$ are:

$$(a+b)^p \equiv a^p + b^p \pmod{p}$$

And since $\mathbb{Z}_p$ is defined mod p, we can conclude that:

$$(a+b)^p = a^p + b^p$$

in $\mathbb{Z}_p$ for all $a, b \in \mathbb{Z}_p$. □

Exercise 44. An element a of a ring R is idempotent if $a^2 = a$.
a. Show that the set of all idempotent elements of a commutative ring is closed under multiplication.
b. Find all idempotents in the ring $\mathbb{Z}_6 \times \mathbb{Z}_{12}$.

Let's address each part individually:

a. Show that the set of all idempotent elements of a commutative ring is closed under multiplication.

Proof. Let R be a commutative ring, and let a and b be idempotent elements of R. This means $a^2 = a$ and $b^2 = b$.

To show closure under multiplication for the set of idempotents, we need to show that ab is also idempotent.

Considering $(ab)^2$:

$$(ab)^2 = abab = a(b^2)a = aba = a^2b = ab$$

Thus, ab is also idempotent. Therefore, the set of idempotent elements in a commutative ring is closed under multiplication. □

b. Find all idempotents in the ring $\mathbb{Z}_6 \times \mathbb{Z}_{12}$.

For the ring $\mathbb{Z}_6$, the idempotent elements are solutions to the equation $x^2 \equiv x \pmod 6$. Similarly, for $\mathbb{Z}_{12}$, the idempotent elements are solutions to the equation $x^2 \equiv x \pmod{12}$.

The idempotents in $\mathbb{Z}_6$ are $\{0, 1, 3, 4\}$, and the idempotents in $\mathbb{Z}_{12}$ are $\{0, 1, 4, 9\}$.

Now, for the ring $\mathbb{Z}_6 \times \mathbb{Z}_{12}$, the idempotents are given by the Cartesian product of these two sets. Let's list them out.

The idempotents in the ring $\mathbb{Z}_6 \times \mathbb{Z}_{12}$ are:

$$\{(0,0), (0,1), (0,4), (0,9), (1,0), (1,1), (1,4), (1,9), (3,0), (3,1), (3,4), (3,9), (4,0), (4,1), (4,4), (4,9)\}$$

Exercise 46. An element a of a ring R is **nilpotent** if $a^n = 0$ for some $n \in \mathbb{Z}^+$. Show that if a and b are nilpotent elements of a commutative ring, then $a + b$ is also nilpotent.

To prove the statement, let's assume a and b are nilpotent elements in a commutative ring R. This means there exist positive integers m and n such that $a^m = 0$ and $b^n = 0$.

Let $k = \max(m, n)$. We want to show that $(a + b)^{2k} = 0$.

Proof. Consider the expansion of $(a + b)^{2k}$ using the binomial theorem:

$$(a+b)^{2k} = \sum_{i=0}^{2k} \binom{2k}{i} a^i b^{2k-i}$$

Given that $a^m = 0$ and $b^n = 0$, any term in the above sum where $i \geq m$ or $2k - i \geq n$ will be zero.

Since k is the larger of m and n, and we're considering the expansion up to the power $2k$, all terms will have either a raised to a power greater than or equal to m or b raised to a power greater than or equal to n. Thus, every term in the expansion will be zero.

Therefore, $(a + b)^{2k} = 0$, which means $a + b$ is nilpotent. □

So, if a and b are nilpotent elements in a commutative ring, then $a+b$ is also nilpotent.

Exercise 52. (Chinese Remainder Theorem for two congruences) Let r and s be positive integers such that $\gcd(r,s)=1$. Use the isomorphism in Example 18.15 to show that for $m,\ n \in Z$, there exists an integer x such that $x \equiv m \pmod{r}$ and $x \equiv n \pmod{s}$.

To prove the Chinese Remainder Theorem for two congruences, we'll make use of the isomorphism provided in Example 18.15. This example shows that if $\gcd(r,s)=1$, then the rings $\mathbb{Z}_{rs}$ and $\mathbb{Z}_r \times \mathbb{Z}_s$ are isomorphic.

Given this isomorphism, let's denote the isomorphism by ϕ, such that:

$$\phi : \mathbb{Z}_{rs} \to \mathbb{Z}_r \times \mathbb{Z}_s$$

The isomorphism is given by:

$$\phi(x) = (x \pmod{r}, x \pmod{s})$$

Proof. Given the congruences:
1. $x \equiv m \pmod{r}$
2. $x \equiv n \pmod{s}$

We can look for an element in $\mathbb{Z}_r \times \mathbb{Z}_s$ of the form (m,n). Since ϕ is an isomorphism, there exists an element x in $\mathbb{Z}_{rs}$ such that:

$$\phi(x) = (m,n)$$

From the definition of ϕ, this gives:

$$\begin{aligned} x \pmod{r} &= m \\ x \pmod{s} &= n \end{aligned}$$

Which are precisely the given congruences. Hence, an integer x exists such that it satisfies both congruences.

Since $\gcd(r,s)=1$, the isomorphism ensures that we can find a unique solution x modulo rs that satisfies both congruences. □

Therefore, for any integers m and n, there exists an integer x such that $x \equiv m \pmod{r}$ and $x \equiv n \pmod{s}$ when $\gcd(r,s)=1$.