Math 345
10-1-2020

Review Problems for Test 3

These problems are provided to help you study. The presence of a problem on this handout does not imply that there *will* be a similar problem on the test. And the absence of a topic does not imply that it *won't* appear on the test.

1. (a) List the elements of the subgroup of $\mathbb{Z}_4 \times \mathbb{Z}_6$ generated by $(2, 4)$.

(b) List the cosets of the subgroup $\langle(2, 4)\rangle$ of $\mathbb{Z}_4 \times \mathbb{Z}_6$. For each coset, list the elements of the coset.

(c) Construct an addition table for the quotient group $\dfrac{\mathbb{Z}_4 \times \mathbb{Z}_6}{\langle(2, 4)\rangle}$. Is the quotient group isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ or to $\mathbb{Z}_4$?

2. (a) List the elements of U_{16}.

(b) List the elements of $\langle 9\rangle$ in U_{16}.

(c) List the elements of each left coset of $\langle 9\rangle$ in U_{16}.

(d) Find the order of each coset in $\dfrac{U_{16}}{\langle 9\rangle}$. Use this information to find the primary decomposition of $\dfrac{U_{16}}{\langle 9\rangle}$.

3. $G = \{0, 2, 4, 6, 8, 10, 12, 14, 16\}$ is a group under addition mod 18.

(a) List the elements of the subgroup $\langle 6\rangle$.

(b) List the cosets of $\langle 6\rangle$ in G. For each coset, list the elements of the coset.

(c) Construct an addition table for $G/\langle 6\rangle$. What familiar group is isomorphic to $G/\langle 6\rangle$?

4. (a) U_{28} is the group of elements of $\mathbb{Z}_{28}$ which are relatively prime to 28, under multiplication mod 28. List the elements of U_{28}.

(b) List the elements of the subgroup $\langle 9\rangle$ of U_{28}.

(c) List the cosets of $\langle 9\rangle$ in U_{28}. For each coset, list the elements of the coset.

(d) Construct a multiplication table for the quotient group $\dfrac{U_{28}}{\langle 9\rangle}$. Use this information to find the primary decomposition of $\dfrac{U_{28}}{\langle 9\rangle}$.

5. (a) Let $f : G \to H$ be a group map. Show that if $x \in G$ has finite order n, then the order of $f(x)$ divides n.

(b) Show that if H is a normal subgroup of G, then the order of xH divides the order of x.

6. (a) List the elements of the cosets of the subgroup $\langle(0, 2)\rangle$ of $\mathbb{Z}_4 \times \mathbb{Z}_6$.

(b) Find the primary decomposition of the quotient group $\dfrac{\mathbb{Z}_4 \times \mathbb{Z}_6}{\langle(0, 2)\rangle}$.

7. $GL(2, \mathbb{Z}_2)$ denotes the group of 2×2 invertible matrices with entries in $\mathbb{Z}_2 = \{0, 1\}$:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}.$$

The operation in $GL(2, \mathbb{Z}_2)$ is matrix multiplication, but all the arithmetic is done in $\mathbb{Z}_2$ — so multiples of 2 equal 0.

(a) List the elements of the cyclic subgroup generated by $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.

(b) Is the cyclic subgroup generated by $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ a normal subgroup? Why or why not?

(c) Is $GL(2, \mathbb{Z}_2)$ abelian? Why or why not?

8. Here is the multiplication table for D_5, the group of symmetries of a regular pentagon:

	1	b	b^2	b^3	b^4	a	ab	ab^2	ab^3	ab^4
1	1	b	b^2	b^3	b^4	a	ab	ab^2	ab^3	ab^4
b	b	b^2	b^3	b^4	1	ab^4	a	ab	ab^2	ab^3
b^2	b^2	b^3	b^4	1	b	ab^3	ab^4	a	ab	ab^2
b^3	b^3	b^4	1	b	b^2	ab^2	ab^3	ab^4	a	ab
b^4	b^4	1	b	b^2	b^3	ab	ab^2	ab^3	ab^4	a
a	a	ab	ab^2	ab^3	ab^4	1	b	b^2	b^3	b^4
ab	ab	ab^2	ab^3	ab^4	a	b^4	1	b	b^2	b^3
ab^2	ab^2	ab^3	ab^4	a	ab	b^3	b^4	1	b	b^2
ab^3	ab^3	ab^4	a	ab	ab^2	b^2	b^3	b^4	1	b
ab^4	ab^4	a	ab	ab^2	ab^3	b	b^2	b^3	b^4	1

(a) Prove by specific example that the subgroup $\{1, a\}$ is not normal.

(b) Explain why the subgroup $\{1, b, b^2, b^3, b^4\}$ is normal.

9. Consider the group U_{15} consisting of elements of $\mathbb{Z}_{15}$ which are relatively prime to 15, with the operation being multiplication mod 15:

$$U_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}.$$

*	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

(a) U_{15} is an abelian group of order 8. Find its primary decomposition.

(b) List the elements of the quotient group $U_{15}/\langle 14 \rangle$.

(c) $\dfrac{U_{15}}{\langle 14 \rangle}$ is an abelian group of order 4. Find its primary decomposition.

10. Let H and K be subgroups of a group G. Suppose that H is normal. Let

$$HK = \{hk \mid h \in H, k \in K\}.$$

Prove that HK is a subgroup of G.

11. Use the First Isomorphism Theorem to prove that

$$\frac{\mathbb{Z} \times \mathbb{Z}}{\langle (4, -5) \rangle} \approx \mathbb{Z}.$$

12. Use the First Isomorphism Theorem to prove that

$$\frac{\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}}{\langle (2, 1, -3) \rangle} \approx \mathbb{Z} \times \mathbb{Z}.$$

13. Let

$$H = \{x \cdot (5, -\sqrt{3}) \mid x \in \mathbb{R}\}.$$

Prove that

$$\frac{\mathbb{R} \times \mathbb{R}}{H} \approx \mathbb{R}.$$

14. Consider the quotient group $\dfrac{\mathbb{Z} \times \mathbb{Z}}{\langle (6, 8) \rangle}$.

(a) Prove that $\dfrac{\mathbb{Z} \times \mathbb{Z}}{\langle (6, 8) \rangle}$ is infinite by showing that the cosets $(n, 0) + \langle (6, 8) \rangle$ for $n \in \mathbb{Z}$ are distinct.

(b) Define $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ by

$$f(x, y) = 8x - 6y.$$

Use the Universal Property of the Quotient to show that f induces a function $f' : \dfrac{\mathbb{Z} \times \mathbb{Z}}{\langle (6, 8) \rangle} \to \mathbb{Z}$ whose image is $2\mathbb{Z}$. Use this to give an alternate proof that $\dfrac{\mathbb{Z} \times \mathbb{Z}}{\langle (6, 8) \rangle}$ is infinite.

15. Use the Universal Property of the Quotient to show that the function $f : \mathbb{Z} \to \dfrac{\mathbb{Z}}{12\mathbb{Z}}$ defined by $f(x) = 8x + 12\mathbb{Z}$ induces a group map $\tilde{f} : \dfrac{\mathbb{Z}}{3\mathbb{Z}} \to \dfrac{\mathbb{Z}}{12\mathbb{Z}}$. What is the definition of $\tilde{f}$?

16. (a) Give an example of a noncommutative ring. You don't need to verify any of the ring axioms, but you should produce two elements of the ring which do not commute (and you should show that they do not commute).

(b) Is $GL(2, \mathbb{R})$ a ring under matrix addition and multiplication? Why or why not?

(c) Find nonzero 2×2 matrices A and B with real entries such that $AB = A$, but B is *not* the identity matrix. Why doesn't this contradict the definition of a multiplicative identity?

17. Let R be a ring, $r, s \in R$. Use the ring axioms to prove that

$$(-r)(-s) = rs.$$

18. Let R be a ring, and let $r \in R$. If n is a positive integer, prove that

$$(-r)^n = \begin{cases} r^n & \text{if } n \text{ is even} \\ -r^n & \text{if } n \text{ is odd} \end{cases}.$$

19. Multiply the quaternions:

$$(3 + 2i - j + k) \cdot (1 + i - 2j + k).$$

20. The **characteristic** of a ring with unity R is the smallest positive integer n such that

$$n \cdot r = 0 \quad \text{for all} \quad r \in R.$$

If no such n exists, the ring has characteristic 0.

(a) What is the characteristic of $\mathbb{R}$? Of $\mathbb{Z}_{57}$?

(b) Give an example of an infinite integral domain with characteristic 2.

21. (a) Find the units in the ring $\mathbb{Z}_3 \times \mathbb{Z}_6$.

(b) Find the zero divisors in the ring $\mathbb{Z}_3 \times \mathbb{Z}_6$.

22. Let R be a ring. Let $e \in R$ be **idempotent**; that is, $e^2 = e$.

(a) Let

$$eRe = \left\{ere \,\middle|\, r \in R\right\}.$$

Show that eRe is a subring of R.

(b) Show that e is an identity element for eRe.

23. Give an example of a ring R and nonzero elements $r, s \in R$ such that $r^2 + s^2 = 0$.

24. Let R be a finite commutative ring with no zero divisors. Prove that R has a multiplicative identity.

25. Let

$$\{\ldots, -4, -1, 0, 1, 4, \ldots\}.$$

It consists of squares of integers and their negatives, and it is not a subring of $\mathbb{Z}$. What is the smallest subring of $\mathbb{Z}$ which contains this set?

26. Let x and y be elements in a ring R. Let

$$I = \{ax + by \mid a, b \in R\}.$$

Prove that I is a left ideal in R.

27. (a) Prove that the following set is an ideal in $\mathbb{Z}$:

$$I = \{4x + 14y + 16z \mid x, y, z \in \mathbb{Z}\}.$$

(b) Find an integer n such that $I = \langle n \rangle$ (and prove that your n works).

28. Prove that the following set is a subring in $\mathbb{Z}_3 \times \mathbb{Z}_3$, but not an ideal:

$$A = \{(0, 0), (1, 1), (2, 2)\}.$$

29. $\mathbb{Z} \times \mathbb{Z}$ is a ring under componentwise addition and multiplication. Consider the following subset of $\mathbb{Z} \times \mathbb{Z}$:

$$S = \{(a, b) \mid 2 \mid a \quad \text{or} \quad 2 \mid b\}.$$

Check each axiom for an ideal. If the axiom holds, prove it. If the axiom does not hold, give a specific counterexample.

30. Define $f : \mathbb{Z} \to \mathbb{Z}$ by

$$f(x) = |x|.$$

Check each axiom for a ring map. If the axiom holds, prove it. If the axiom doesn't hold, give a specific counterexample.

31. Define $f : \mathbb{R}^3 \to \mathbb{R}^2$ by

$$\phi(x, y, z) = (2x - y, 2y - z).$$

Check each axiom for a ring map. If the axiom holds, prove it. If the axiom doesn't hold, give a specific counterexample.

Solutions to the Review Problems for Test 3

1. (a) List the elements of the subgroup of $\mathbb{Z}_4 \times \mathbb{Z}_6$ generated by $(2, 4)$.

(b) List the cosets of the subgroup $\langle (2, 4) \rangle$ of $\mathbb{Z}_4 \times \mathbb{Z}_6$. For each coset, list the elements of the coset.

(c) Construct an addition table for the quotient group $\dfrac{\mathbb{Z}_4 \times \mathbb{Z}_6}{\langle (2, 4) \rangle}$. Is the quotient group isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ or to $\mathbb{Z}_4$?

(a)

$$\langle (2, 4) \rangle = \{(0, 0), (2, 4), (0, 2), (2, 0), (0, 4), (2, 2)\}. \quad \square$$

(b)

$$\begin{aligned} \langle (2, 4) \rangle &= \{(0, 0), (2, 4), (0, 2), (2, 0), (0, 4), (2, 2)\}, \\ (0, 1) + \langle (2, 4) \rangle &= \{(0, 1), (2, 5), (0, 3), (2, 1), (0, 5), (2, 3)\}, \\ (1, 0) + \langle (2, 4) \rangle &= \{(1, 0), (3, 4), (1, 2), (3, 0), (1, 4), (3, 2)\}, \\ (1, 1) + \langle (2, 4) \rangle &= \{(1, 1), (3, 5), (1, 3), (3, 1), (1, 5), (3, 3)\}. \end{aligned} \quad \square$$

(c) I'll use the representatives $(0, 0)$, $(1, 0)$, $(0, 1)$, and $(1, 1)$ to stand for their cosets.

$+$	$(0, 0)$	$(0, 1)$	$(1, 0)$	$(1, 1)$
$(0, 0)$	$(0, 0)$	$(0, 1)$	$(1, 0)$	$(1, 1)$
$(0, 1)$	$(0, 1)$	$(0, 0)$	$(1, 1)$	$(1, 0)$
$(1, 0)$	$(1, 0)$	$(1, 1)$	$(0, 0)$	$(0, 1)$
$(1, 1)$	$(1, 1)$	$(1, 0)$	$(0, 1)$	$(0, 0)$

Since every element has order 1 or 2, the quotient group is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. $\square$

---

2. (a) List the elements of U_{16}.

(b) List the elements of $\langle 9 \rangle$ in U_{16}.

(c) List the elements of each left coset of $\langle 9 \rangle$ in U_{16}.

(d) Find the order of each coset in $\dfrac{U_{16}}{\langle 9 \rangle}$. Use this information to find the primary decomposition of $\dfrac{U_{16}}{\langle 9 \rangle}$.

(a) This is the group of elements of $\mathbb{Z}_{16}$ which are relatively prime to 16. The operation is multiplication mod 16.

$$U_{16} = \{1, 3, 5, 7, 9, 11, 13, 15\}. \quad \square$$

(b) Since $9^2 = 81 = 1 \pmod{16}$, I have

$$\langle 9 \rangle = \{1, 9\}. \quad \square$$

(c) I list the elements of the original subgroup. Then I multiply the elements of the subgroup by other elements of the group, "crossing out" elements that have already been listed, until every element of the group has been listed exactly once.

$$\begin{aligned} \langle 9 \rangle &= \{1, 9\} \\ 3 \cdot \langle 9 \rangle &= \{3, 11\} \\ 5 \cdot \langle 9 \rangle &= \{5, 13\} \\ 7 \cdot \langle 9 \rangle &= \{7, 15\} \quad \square \end{aligned}$$

(d) Since $\dfrac{U_{16}}{\langle 9 \rangle}$ has order 4, it's isomorphic to $\mathbb{Z}_4$ or to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

coset	order
$\{3, 11\}$	2
$\{5, 13\}$	2
$\{7, 15\}$	2

For example,

$$\{5, 13\}^2 = (5 \cdot \{1, 9\})^2 = 5^2 \cdot \{1, 9\} = 9 \cdot \{1, 9\} = \{1, 9\}.$$

Since every element has order 1 or 2, the quotient group is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. $\square$

---

3. $G = \{0, 2, 4, 6, 8, 10, 12, 14, 16\}$ is a group under addition mod 18.

(a) List the elements of the subgroup $\langle 6 \rangle$.

(b) List the cosets of $\langle 6 \rangle$ in G. For each coset, list the elements of the coset.

(c) Construct an addition table for $G/\langle 6 \rangle$. What familiar group is isomorphic to $G/\langle 6 \rangle$?

(a)

$$\langle 6 \rangle = \{0, 6, 12\}. \quad \square$$

(b) Reminder: The operation is addition mod 18, and the group is $\{0, 2, 4, 6, 8, 10, 12, 14, 16\}$. So (for instance) elements like 1 or 9 in $\mathbb{Z}_{18}$ don't come into this problem.

There are 9 elements in G and 3 elements in the subgroup, so by Lagrange's theorem there are $\dfrac{9}{3} = 3$ cosets.

I start with the original subgroup. I take an element that isn't in the subgroup and *add* it to the subgroup (mod 18) to get a coset:

$$\{0, 6, 12\}, \quad 2 + \{0, 6, 12\} = \{2, 8, 14\}.$$

Next, I take an element which isn't in either of the first two cosets and add it to the original subgroup:

$$4 + \{0, 6, 12\} = \{4, 10, 16\}.$$

I have three distinct cosets, so that must be all of them. They are

$$\{0, 6, 12\}, \quad \{2, 8, 14\}, \quad \{4, 10, 16\}. \quad \square$$

(c)

$+$	$\{0, 6, 12\}$	$\{2, 8, 14\}$	$\{4, 10, 16\}$
$\{0, 6, 12\}$	$\{0, 6, 12\}$	$\{2, 8, 14\}$	$\{4, 10, 16\}$
$\{2, 8, 14\}$	$\{2, 8, 14\}$	$\{4, 10, 16\}$	$\{0, 6, 12\}$
$\{4, 10, 16\}$	$\{4, 10, 16\}$	$\{0, 6, 12\}$	$\{2, 8, 14\}$

Here's an example which shows how I constructed the table. To find $\{2,8,14\}+\{4,10,16\}$, I take representatives from each coset. It doesn't matter which elements I use; I'll take 2 from $\{2,8,14\}$ and 10 from $\{4,10,16\}$. Now $2+10=12$, and $12 \in \{0,6,12\}$. Therefore,

$$\{2,8,14\}+\{4,10,16\}=\{0,6,12\}.$$

The rest of the table is constructed in the same way.

$G/\langle 6\rangle$ is a group of order 3. The only group of order 3 is $\mathbb{Z}_3$, so it must be isomorphic to $\mathbb{Z}_3$. $\square$

---

4. (a) U_{28} is the group of elements of $\mathbb{Z}_{28}$ which are relatively prime to 28, under multiplication mod 28. List the elements of U_{28}.

(b) List the elements of the subgroup $\langle 9\rangle$ of U_{28}.

(c) List the cosets of $\langle 9\rangle$ in U_{28}. For each coset, list the elements of the coset.

(d) Construct a multiplication table for the quotient group $\dfrac{U_{28}}{\langle 9\rangle}$. Use this information to find the primary decomposition of $\dfrac{U_{28}}{\langle 9\rangle}$.

(a)

$$U_{28}=\{1,3,5,9,11,13,15,17,19,23,25,27\}. \quad \square$$

(b)

$$\langle 9\rangle=\{1,9,25\}. \quad \square$$

(c) First, since $|U_{28}|=12$ and $|\langle 9\rangle|=3$, there are $\dfrac{12}{3}=4$ cosets by Lagrange's theorem. They are

$$\begin{aligned} \langle 9\rangle &= \{1,9,25\} \\ 3\cdot\{1,9,25\} &= \{3,19,27\} \\ 5\cdot\{1,9,25\} &= \{5,13,17\} \\ 11\cdot\{1,9,25\} &= \{11,15,23\} \end{aligned} \quad \square$$

(d)

$+$	$\{1,9,25\}$	$\{3,19,27\}$	$\{5,13,17\}$	$\{11,15,23\}$
$\{1,9,25\}$	$\{1,9,25\}$	$\{3,19,27\}$	$\{5,13,17\}$	$\{11,15,23\}$
$\{3,19,27\}$	$\{3,19,27\}$	$\{1,9,25\}$	$\{11,15,23\}$	$\{5,13,17\}$
$\{5,13,17\}$	$\{5,13,17\}$	$\{11,15,23\}$	$\{1,9,25\}$	$\{3,19,27\}$
$\{11,15,23\}$	$\{11,15,23\}$	$\{5,13,17\}$	$\{3,19,27\}$	$\{1,9,25\}$

Here's an example to show how the table was constructed. To find $\{5,13,17\}\cdot\{11,15,23\}$, I take representatives from each coset. I'll take 5 from $\{5,13,17\}$ and 11 from $\{11,15,23\}$; it doesn't matter which elements I choose. Now $5\cdot 11=55=27 \pmod{28}$, and $27\in\{3,19,27\}$. Therefore,

$$\{5,13,17\}\cdot\{11,15,23\}=\{3,19,27\}.$$

The rest of the table is constructed in the same way.

The quotient group has order 4, and every element other than the identity has order 2 — notice the identity $\{1,9,25\}$ in each spot on the main diagonal. Therefore, the quotient group is isomorphic to $\mathbb{Z}_2\times\mathbb{Z}_2$. It can't be $\mathbb{Z}_4$, the other group of order 4, because there is no element of order 4. $\square$

5. (a) Let $f : G \to H$ be a group map. Show that if $x \in G$ has finite order n, then the order of $f(x)$ divides n.

(b) Show that if H is a normal subgroup of G and $x \in G$ has finite order, then the order of xH divides the order of x.

(a) Since x has order n, I have $x^n = 1$. Then

$$f(x^n) = f(1) = 1, \quad \text{so} \quad f(x)^n = 1.$$

This implies that the order of $f(x)$ divides n. $\square$

(b) The quotient map $\pi : G \to \dfrac{G}{H}$ satisfies $\pi(x) = xH$. Hence, the result follows immediately from (a). $\square$

Expressed in words, this says that the order of a coset divides the order of its representative.

6. (a) List the elements of the cosets of the subgroup $\langle(0,2)\rangle$ of $\mathbb{Z}_4 \times \mathbb{Z}_6$.

(b) Find the primary decomposition of the quotient group $\dfrac{\mathbb{Z}_4 \times \mathbb{Z}_6}{\langle(0,2)\rangle}$.

(a)

$$\begin{aligned}
\langle(0,2)\rangle &= \{(0,0),(0,2),(0,4)\} \\
(1,0) + \langle(0,2)\rangle &= \{(1,0),(1,2),(1,4)\} \\
(2,0) + \langle(0,2)\rangle &= \{(2,0),(2,2),(2,4)\} \\
(3,0) + \langle(0,2)\rangle &= \{(3,0),(3,2),(3,4)\} \\
(0,1) + \langle(0,2)\rangle &= \{(0,1),(0,3),(0,5)\} \\
(1,1) + \langle(0,2)\rangle &= \{(1,1),(1,3),(1,5)\} \\
(2,1) + \langle(0,2)\rangle &= \{(2,1),(2,3),(2,5)\} \\
(3,1) + \langle(0,2)\rangle &= \{(3,1),(3,3),(3,5)\} \quad \square
\end{aligned}$$

(b) The possible primary decompositions are

$$\mathbb{Z}_8, \quad \mathbb{Z}_2 \times \mathbb{Z}_4, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Note that $(1,0) + \langle(0,2)\rangle$ has order 4:

$$2 \cdot (1,0) + \langle(0,2)\rangle = (2,0) + \langle(0,2)\rangle,$$

$$3 \cdot (1,0) + \langle(0,2)\rangle = (3,0) + \langle(0,2)\rangle,$$

$$4 \cdot (1,0) + \langle(0,2)\rangle = (0,0) + \langle(0,2)\rangle.$$

This rules out $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

On the other hand, the original group $\mathbb{Z}_4 \times \mathbb{Z}_6$ has no elements of order 8. If $(a,b) \in \mathbb{Z}_4 \times \mathbb{Z}_6$, then the order of (a,b) is $[m,n]$, where m is the order of a and n is the order of b. But $m \mid 4$, so $m = 1,2,4$, and $n \mid 6$, so $n = 1,2,3,6$. No combination of these numbers will give $[m,n] = 8$.

Moreover, the largest order of an element of $\mathbb{Z}_4 \times \mathbb{Z}_6$ is $[4,6] = 12$.

If $(a,b) + \langle(0,2)\rangle$ had order 8, then the order of (a,b) would divide 8. Since no element of $\mathbb{Z}_4 \times \mathbb{Z}_6$ has order greater than 12, this means that (a,b) has order 8, which I ruled out above.

Thus, the quotient group has no elements of order 8, and it can't be $\mathbb{Z}_8$.

Therefore, $\dfrac{\mathbb{Z}_4 \times \mathbb{Z}_6}{\langle (0,2) \rangle} \approx \mathbb{Z}_2 \times \mathbb{Z}_4$. □

---

7. $GL(2, \mathbb{Z}_2)$ denotes the group of 2×2 invertible matrices with entries in $\mathbb{Z}_2 = \{0, 1\}$:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}.$$

The operation in $GL(2, \mathbb{Z}_2)$ is matrix multiplication, but all the arithmetic is done in $\mathbb{Z}_2$ — so multiples of 2 equal 0.

(a) List the elements of the cyclic subgroup generated by $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.

(b) Is the cyclic subgroup generated by $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ a normal subgroup? Why or why not?

(c) Is $GL(2, \mathbb{Z}_2)$ abelian? Why or why not?

(a)

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Hence, the cyclic subgroup is

$$\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\}. \quad □$$

(b) I'll show that the subgroup isn't normal. Let H denote the subgroup.

Use the formula

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

This gives

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^{-1} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}.$$

(Remember that $-1 = 1$ in $\mathbb{Z}_2$.) Then

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \notin H.$$

Hence, the subgroup isn't normal. □

(c) If $GL(2, \mathbb{Z}_2)$ were abelian, then every subgroup would be normal. Since I found a non-normal subgroup in (a) and (b), $GL(2, \mathbb{Z}_2)$ can't be abelian.

A specific counterexample:

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{but} \quad \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

Hence, $GL(2, \mathbb{Z}_2)$ is not abelian. □

---

8. Here is the multiplication table for D_5, the group of symmetries of a regular pentagon:

	1	b	b^2	b^3	b^4	a	ab	ab^2	ab^3	ab^4
1	1	b	b^2	b^3	b^4	a	ab	ab^2	ab^3	ab^4
b	b	b^2	b^3	b^4	1	ab^4	a	ab	ab^2	ab^3
b^2	b^2	b^3	b^4	1	b	ab^3	ab^4	a	ab	ab^2
b^3	b^3	b^4	1	b	b^2	ab^2	ab^3	ab^4	a	ab
b^4	b^4	1	b	b^2	b^3	ab	ab^2	ab^3	ab^4	a
a	a	ab	ab^2	ab^3	ab^4	1	b	b^2	b^3	b^4
ab	ab	ab^2	ab^3	ab^4	a	b^4	1	b	b^2	b^3
ab^2	ab^2	ab^3	ab^4	a	ab	b^3	b^4	1	b	b^2
ab^3	ab^3	ab^4	a	ab	ab^2	b^2	b^3	b^4	1	b
ab^4	ab^4	a	ab	ab^2	ab^3	b	b^2	b^3	b^4	1

(a) Prove by specific example that the subgroup $\{1, a\}$ is not normal.

(b) Explain why the subgroup $\{1, b, b^2, b^3, b^4\}$ is normal.

(a)

$$(ab)\{1, a\}(ab)^{-1} = (ab)\{1, a\}(ab) = \{1, ab^2\} \neq \{1, a\}.$$

Therefore, $\{1, a\}$ is not normal. □

(b) The group has 10 elements, and the subgroup $\{1, b, b^2, b^3, b^4\}$ has 5 elements. Therefore, the subgroup has index 2, and any subgroup of index 2 is normal. □

---

9. Consider the group U_{15} consisting of elements of $\mathbb{Z}_{15}$ which are relatively prime to 15, with the operation being multiplication mod 15:

$$U_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}.$$

*	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

(a) U_{15} is an abelian group of order 8. Find its primary decomposition.

(b) List the elements of the quotient group $U_{15}/\langle 14\rangle$.

(c) $\dfrac{U_{15}}{\langle 14\rangle}$ is an abelian group of order 4. Find its primary decomposition.

(a) The three abelian groups of order 8 are $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

U_{15} has no elements of order 8. This is clear from the multiplication table. 1 has order 1, while 4, 11, and 14 square to 1, and hence have order 2. The remaining elements square to 4, which squares to 1, so the remaining elements have order 4.

Since there are no elements of order 8, U_{15} can't be $\mathbb{Z}_8$.

On the other hand, every element of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ has order 2. whereas I've just shown that U_{15} has elements of order 4. Therefore, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ is ruled out, and hence $U_{15} \approx \mathbb{Z}_2 \times \mathbb{Z}_4$. $\Box$

(b) $\langle 14\rangle = \{1, 14\}$, so the quotient group has 4 elements.

They are

$$\begin{aligned} \langle 14\rangle &= \{1, 14\} \\ 2\langle 14\rangle &= \{2, 13\} \\ 4\langle 14\rangle &= \{4, 11\} \\ 7\langle 14\rangle &= \{7, 8\} \end{aligned} \quad \Box$$

(c) There are two groups of order 4: $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$. Here's the multiplication table for $U_{15}/\langle 14\rangle$:

*	$\{1,14\}$	$\{2,13\}$	$\{4,11\}$	$\{7,8\}$
$\{1,14\}$	$\{1,14\}$	$\{2,13\}$	$\{4,11\}$	$\{7,8\}$
$\{2,13\}$	$\{2,13\}$	$\{4,11\}$	$\{7,8\}$	$\{1,14\}$
$\{4,11\}$	$\{4,11\}$	$\{7,8\}$	$\{1,14\}$	$\{2,13\}$
$\{7,8\}$	$\{7,8\}$	$\{1,14\}$	$\{2,13\}$	$\{4,11\}$

The table shows that two elements don't square to the identity ($\{1, 14\}$) — that is, two elements do *not* have order 2. Since every element of $\mathbb{Z}_2 \times \mathbb{Z}_2$ has order 2, $\dfrac{U_{15}}{\langle 14\rangle}$ can't be $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Thus, $\dfrac{U_{15}}{\langle 14\rangle} \approx \mathbb{Z}_4$. $\Box$

---

10. Let H and K be subgroups of a group G. Suppose that H is normal. Let

$$HK = \{hk \mid h \in H, k \in K\}.$$

Prove that HK is a subgroup of G.

Remember that since H is normal,

$$(\text{anything}) \cdot (\text{something in } H) \cdot (\text{anything})^{-1} \in H.$$

I'll need to use this twice in the proof.

Since $1 \in H$ and $1 \in K$, $1 = 1 \cdot 1 \in HK$. This proves that the identity is in HK.

Let $h \in H$, $k \in K$. Then $hk \in HK$, and

$$(hk)^{-1} = k^{-1}h^{-1} = (k^{-1}h^{-1}k)k^{-1} \in HK.$$

Reason: $h^{-1} \in H$, and H is normal, so $k^{-1}h^{-1}k \in H$. Obviously, $k^{-1} \in K$. Therefore, $(k^{-1}h^{-1}k)k^{-1}$ is something in H times something in K.

Thus, HK is closed under taking inverses.

Finally, let $h_1, h_2 \in H$, $k_1, k_2 \in K$, so $h_1k_1, h_2k_2 \in HK$. Then

$$(h_1k_1)(h_2k_2) = [h_1(k_1h_2k_1^{-1})][k_1k_2] \in HK.$$

Reason: $h_2 \in H$, so $k_1h_2k_1^{-1} \in H$, because H is normal. Therefore, $h_1(k_1h_2k_1^{-1}) \in H$. Obviously, $k_1k_2 \in K$. Therefore, $[h_1(k_1h_2k_1^{-1})][k_1k_2]$ is something in H times something in K.

This shows that HK is closed under products.

Hence, HK is a subgroup. □

---

11. Use the First Isomorphism Theorem to prove that

$$\frac{\mathbb{Z}\times\mathbb{Z}}{\langle(4,-5)\rangle}\approx\mathbb{Z}.$$

Define $f:\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$ by

$$f(x,y)=5x+4y.$$

(Note how this definition relates to the subgroup $\langle(4,-5)\rangle$.)

If $(a,b),(c,d)\in\mathbb{Z}\times\mathbb{Z}$, then

$$f\left[(a,b)+(c,d)\right]=f(a+c,b+d)=5(a+c)+4(b+d)=(5a+4b)+(5c+4d)=f(a,b)+f(c,d).$$

Therefore, f is a group map.

An element of $\langle(4,-5)\rangle$ has the form $k(4,-5)=(4k,-5k)$. Now

$$f(4k,-5k)=5\cdot 4k+4\cdot(-5k)=0.$$

Therefore, $\langle(4,-5)\rangle\subset\ker f$.

Conversely, suppose $f(x,y)=0$, so $5x+4y=0$ or $5x=-4y$. Now 5 divides $5x$, so it divides $-4y$; 5 is relatively prime to 4, so it must divide y. Say $y=5k$. Substituting this into $5x=-4y$, I get $5x=-20k$, or $x=-4k$. Therefore,

$$(x,y)=(-4k,5k)=(-k)(4,-5)\in\langle(4,-5)\rangle.$$

Hence, $\ker f\subset\langle(4,-5)\rangle$, and so $\ker f=\langle(4,-5)\rangle$.

Let $z\in\mathbb{Z}$. Then

$$f(z,-z)=5z-4z=z.$$

Hence, f is surjective, i.e. $\operatorname{im} f=\mathbb{Z}$.

Finally,

$$\frac{\mathbb{Z}\times\mathbb{Z}}{\langle(4,-5)\rangle}=\frac{\mathbb{Z}\times\mathbb{Z}}{\ker f}\approx\operatorname{im} f=\mathbb{Z}.$$

The first equality follows from $\ker f=\langle(4,-5)\rangle$. The isomorphism is given by the First Isomorphism Theorem. And the last equality follows from the fact that f is surjective. □

---

12. Use the First Isomorphism Theorem to prove that

$$\frac{\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}}{\langle(2,1,-3)\rangle}\approx\mathbb{Z}\times\mathbb{Z}.$$

I need a group map $\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}\times\mathbb{Z}$; I want it to be surjective, and I want the kernel to be $\langle(2,1,-3)\rangle$.

Define $f(x,y,z)=(x-2y,3y+z)$. (I chose $x-2y$ and $3y+z$ so that $(2,1,-3)$ will give $(0,0)$. I also want to make sure that two components are "independent" — i.e. not multiples of one another.)

First,

$$f\left[(x,y,z)+(x',y',z')\right]=f(x+x',y+y',z+z')=((x+x')-2(y+y'),3(y+y')+(z+z'))=$$

$$(x-2y,3y+z)+(x'-2y',3y'+z')=f(x,y,z)+f(x',y',z').$$

Therefore, f is a group map.

Let $k(2,1,-3) \in \langle(2,1,-3)\rangle$. Then

$$f(k(2,1,-3)) = f(2k,k,-3k) = (2k-2k, 3k-3k) = (0,0).$$

Hence, $k(2,1,-3) \in \ker f$, so $\langle(2,1,-3)\rangle \subset \ker f$.

Suppose $(x,y,z) \in \ker f$. Then

$$f(x,y,z) = (0,0), \quad \text{so} \quad (x-2y, 3y+z) = (0,0).$$

Equating corresponding components, I get $x - 2y = 0$ and $3y + z = 0$. Therefore, $x = 2y$ and $z = -3y$. Hence,

$$(x,y,z) = (2y, y, -3y) = y \cdot (2,1,-3) \in \langle(2,1,-3)\rangle.$$

It follows that $\ker f \subset \langle(2,1,-3)\rangle$, so $\langle(2,1,-3)\rangle = \ker f$.

Next, I'll show that f is surjective. Let $(a,b) \in \mathbb{Z} \times \mathbb{Z}$. I need to find (x,y,z) so that $f(x,y,z) = (a,b)$, or $(x-2y, 3y+z) = (a,b)$.

I have three variables and two equations, so I just juggle the numbers till I find a combination that works. And in fact, if $x = a$, $y = 0$, and $z = b$, I get

$$f(a,0,b) = (a,b).$$

Therefore, f is surjective.

By the First Isomorphism Theorem,

$$\frac{\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}}{\langle(2,1,-3)\rangle} = \frac{\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}}{\ker f} \approx \operatorname{im} f = \mathbb{Z} \times \mathbb{Z}. \quad \square$$

---

13. Let

$$H = \{x \cdot (5, -\sqrt{3}) \mid x \in \mathbb{R}\}.$$

Prove that

$$\frac{\mathbb{R} \times \mathbb{R}}{H} \approx \mathbb{R}.$$

Define $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ by

$$f(x,y) = \sqrt{3}x + 5y.$$

f is a group map:

$$f((x_1,y_1) + (x_2,y_2)) = f(x_1 + x_2, y_1 + y_2) = \sqrt{3}(x_1 + x_2) + 5(y_1 + y_2) =$$

$$(\sqrt{3}x_1 + 5y_1) + (\sqrt{3}x_2 + 5y_2) = f(x_1,y_1) + f(x_2,y_2).$$

Next, I'll show that $H = \ker f$.

First, let $x \cdot (5, -\sqrt{3}) \in H$. Then

$$f\left(x \cdot (5, -\sqrt{3})\right) = f\left(5x, -\sqrt{3}x\right) = \sqrt{3}(5x) + 5(-\sqrt{3}x) = 0.$$

Therefore, $x \cdot (5, -\sqrt{3}) \in \ker f$. Hence, $H \subset \ker f$.

Next, let $(x,y) \in \ker f$. Then $f(x,y) = 0$, so

$$\sqrt{3}x + 5y = 0, \quad \text{and} \quad y = -\frac{\sqrt{3}}{5}x.$$

Hence,

$$(x,y) = \left(x, -\frac{\sqrt{3}}{5}x\right) = \frac{1}{5}x \cdot (5, -\sqrt{3}) \in H.$$

Thus, $\ker f \subset H$, and so $H = \ker f$.

Next, I'll show that $\operatorname{im} f = \mathbb{R}$. Let $z \in \mathbb{R}$. I need an input $(x,y) \in \mathbb{R} \times \mathbb{R}$ such that $f(x,y) = z$, i.e. such that $\sqrt{3}x + 5y = z$. I can choose x and y as I please, as long as this equation is satisfied. So I'll set $x = 0$; then $5y = z$, and $y = \dfrac{1}{5}z$. Check it:

$$f\left(0, \frac{1}{5}z\right) = \sqrt{3}(0) + 5\left(\frac{1}{5}z\right) = z.$$

Therefore, $\operatorname{im} f = \mathbb{R}$.

Finally, by the First Isomorphism Theorem, I have

$$\frac{\mathbb{R} \times \mathbb{R}}{H} = \frac{\mathbb{R} \times \mathbb{R}}{\ker f} \approx \operatorname{im} f = \mathbb{R}. \quad \square$$

---

14. Consider the quotient group $\dfrac{\mathbb{Z} \times \mathbb{Z}}{\langle (6,8) \rangle}$.

(a) Prove that $\dfrac{\mathbb{Z} \times \mathbb{Z}}{\langle (6,8) \rangle}$ is infinite by showing that the cosets $(n,0) + \langle (6,8) \rangle$ for $n \in \mathbb{Z}$ are distinct.

(b) Define $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ by

$$f(x,y) = 8x - 6y.$$

Use the Universal Property of the Quotient to show that f induces a function $f' : \dfrac{\mathbb{Z} \times \mathbb{Z}}{\langle (6,8) \rangle} \to \mathbb{Z}$ whose image is $2\mathbb{Z}$. Use this to give an alternate proof that $\dfrac{\mathbb{Z} \times \mathbb{Z}}{\langle (6,8) \rangle}$ is infinite.

(a) Suppose

$$(m,0) + \langle (6,8) \rangle = (n,0) + \langle (6,8) \rangle.$$

Then $(m,0) - (n,0) \in \langle (6,8) \rangle$, so

$$\begin{aligned} (m,0) - (n,0) &= k \cdot (6,8) \\ (m-n, 0) &= (6k, 8k) \end{aligned}$$

Equating the second components, I get $8k = 0$, or $k = 0$. Then equating the first components, I have $m - n = 6k = 0$, so $m = n$. This shows that that the cosets $(n,0) + \langle (6,8) \rangle$ for $n \in \mathbb{Z}$ are distinct. Since there are an infinite number of these cosets, the quotient group $\dfrac{\mathbb{Z} \times \mathbb{Z}}{\langle (6,8) \rangle}$ is infinite. $\square$

(b) f is a group map, since

$$f[(a,b) + (c,d) = f(a+c, b+d) = 8(a+c) - 6(b+d) = (8a - 6b) + (8c - 6d) = f(a,b) + f(c,d).$$

Let $k \cdot (6,8) \in \langle (6,8) \rangle$. Then

$$f[k \cdot (6,8)] = f(6k, 8k) = 8(6k) - 6(8k) = 0.$$

Thus, $\langle (6,8) \rangle \subset \ker f$. By the Universal Property of the Quotient, f induces a function $f' : \dfrac{\mathbb{Z} \times \mathbb{Z}}{\langle (6,8) \rangle} \to \mathbb{Z}$ given by

$$f'[(x,y) + \langle (6,8) \rangle] = 8x - 6y.$$

Since $8x - 6y = 2(4x - 3y) \in 2\mathbb{Z}$, it follows that $\operatorname{im} f' \subset 2\mathbb{Z}$. Conversely, suppose $2n \in 2\mathbb{Z}$. Then

$$\begin{aligned} 2 &= 8 - 6 \\ 2n &= 8n - 6n \\ 2n &= f'[(n, n) + \langle(6, 8)\rangle] \end{aligned}$$

This shows that $2\mathbb{Z} \subset \operatorname{im} f'$. Hence, $2\mathbb{Z} = \operatorname{im} f'$.

But $2\mathbb{Z}$ is infinite. Hence, $\dfrac{\mathbb{Z} \times \mathbb{Z}}{\langle(6, 8)\rangle}$ must be infinite, because a function can't take a finite set onto an infinite set. □

---

15. Use the Universal Property of the Quotient to show that the function $f : \mathbb{Z} \to \dfrac{\mathbb{Z}}{12\mathbb{Z}}$ defined by $f(x) = 8x + 12\mathbb{Z}$ induces a group map $\tilde{f} : \dfrac{\mathbb{Z}}{3\mathbb{Z}} \to \dfrac{\mathbb{Z}}{12\mathbb{Z}}$. What is the definition of $\tilde{f}$?

First,

$$f(x + y) = 8(x + y) + 12\mathbb{Z} = 8x + 8y + 12\mathbb{Z} = (8x + 12\mathbb{Z}) + (8y + 12\mathbb{Z}) = f(x) + f(y).$$

Hence, f is a group map.
Next, if $3n \in 3\mathbb{Z}$, then

$$f(3n) = 24n + 12\mathbb{Z} = 12\mathbb{Z}.$$

This follows from the fact that $24n \in 12\mathbb{Z}$.
By the Universal Property of the Quotient, f induces induces a group map $\tilde{f} : \dfrac{\mathbb{Z}}{3\mathbb{Z}} to \dfrac{\mathbb{Z}}{12\mathbb{Z}}$. $\tilde{f}$ is given by

$$\tilde{f}(x + 3\mathbb{Z}) = f(x) = 8x + 12\mathbb{Z}. \quad \square$$

---

16. (a) Give an example of a noncommutative ring. You don't need to verify any of the ring axioms, but you should produce two elements of the ring which do not commute (and you should show that they do not commute).

(b) Is $GL(2, \mathbb{R})$ a ring under matrix addition and multiplication? Why or why not?

(c) Find nonzero 2×2 matrices A and B with real entries such that $AB = A$, but B is *not* the identity matrix. Why doesn't this contradict the definition of a multiplicative identity?

(a) The standard examples of noncommutative rings are rings of matrices. For example, take $M(2, \mathbb{R})$, the ring of 2×2 matrices with real entries.

$$\begin{bmatrix} 1 & -1 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \quad \text{but} \quad \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ 0 & 0 \end{bmatrix}. \quad \square$$

(b) $GL(2, \mathbb{R})$ is the *invertible* 2×2 matrices with real entries. It is *not* a ring under matrix addition and multiplication.

You could give several reasons; for instance, it is not closed under matrix addition. As a specific example of this,

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{is invertible,}$$

$$\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \quad \text{is invertible,}$$

$$\text{but} \quad \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \quad \text{is not invertible.} \quad \square$$

(c) No. For example,

$$\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, \quad \text{but} \quad \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \neq I.$$

This does not contradict the definition of a multiplicative identity for two reasons. First, $AB = A$ works for the particular matrix A, whereas an identity I must satisfy $XI = X$ *for all* X. Second, multiplication is not necessarily commutative, so there's no reason to suppose that $AB = A$ implies $BA = A$. In fact, it doesn't even work for this particular matrix A. □

---

17. Let R be a ring, $r, s \in R$. Use the ring axioms to prove that

$$(-r)(-s) = rs.$$

$$(-r)(-s) + (-r)s = (-r)(s + (-s)) = (-r)(0) = 0.$$

Therefore, $(-r)(-s)$ is the additive inverse of $(-r)s$: $(-r)(-s) = -[(-r)s]$.
But

$$rs + (-r)s = (r + (-r))s = (0)(s) = 0.$$

Therefore, rs is the additive inverse of $(-r)s$: $rs = -[(-r)s]$.
Hence, $rs = (-r)(-s)$. □

---

18. Let R be a ring, and let $r \in R$. If n is a positive integer, prove that

$$(-r)^n = \begin{cases} r^n & \text{if } n \text{ is even} \\ -r^n & \text{if } n \text{ is odd} \end{cases}.$$

For $n = 1$, $(-r)^1 = -r$ — the result is true.
For $n = 2$, I want to show that $(-r)^2 = r^2$. This follows from Problem 2: $(-r)^2 = (-r)(-r) = r \cdot r = r^2$.
Now take $n > 2$, and assume the result is true for $n - 1$.
If n is even, then $n - 1$ is odd. So

$$(-r)^n = (-r)(-r)^{n-1} = (-r)(-r^{n-1}) = rr^{n-1} = r^n.$$

If n is odd, then $n - 1$ is even. So

$$(-r)^n = (-r)(-r)^{n-1} = (-r)(r^{n-1}) = -(rr^{n-1}) = -r^n.$$

Therefore, the result is true for all n by induction. □

---

19. Multiply the quaternions:

$$(3 + 2i - j + k) \cdot (1 + i - 2j + k).$$

$\cdot$	1	i	$-2j$	k
3	3	$3i$	$-6j$	$3k$
$2i$	$2i$	-2	$-4k$	$-2j$
$-j$	$-j$	k	-2	$-i$
k	k	j	$2i$	-1

$$(3 + 2i - j + k) \cdot (1 + i - 2j + k) = -2 + 6i - 8j + k. \quad \square$$

---

20. The **characteristic** of a ring with unity R is the smallest positive integer n such that

$$n \cdot r = 0 \quad \text{for all} \quad r \in R.$$

If no such n exists, the ring has characteristic 0.

(a) What is the characteristic of $\mathbb{R}$? Of $\mathbb{Z}_{57}$?

(b) Give an example of an infinite integral domain with characteristic 2.

(a) $\mathbb{R}$ has characteristic 0: For no positive integer n is $n \cdot 1$ equal to 0.
$\mathbb{Z}_{57}$ has characteristic 57, since $57 \cdot 1 = 0$ in $\mathbb{Z}_{57}$. $\square$

(b) Polynomial rings over fields are integral domains, $\mathbb{Z}_2[x]$ is a domain. Moreover, 2 times anything is 0 in $\mathbb{Z}_2[x]$, so $\mathbb{Z}_2[x]$ has characteristic 2. $\square$

---

21. (a) Find the units in the ring $\mathbb{Z}_3 \times \mathbb{Z}_6$.

(b) Find the zero divisors in the ring $\mathbb{Z}_3 \times \mathbb{Z}_6$.

(a) The multiplicative identity is $(1, 1)$. To show an element is a unit, I must find an element whose product with the first element is $(1, 1)$.

$$(1, 1)(1, 1) = (1, 1), \quad (1, 5)(1, 5) = (1, 1), \quad (2, 1)(2, 1) = (1, 1), \quad (2, 5)(2, 5) = (1, 1).$$

The units are $(1, 1)$, $(1, 5)$, $(2, 1)$, and $(2, 5)$. $\square$

(b) To show an element is a zero divisor, I must find an element whose product with the first element is $(0, 0)$.

Before starting, I note that $\mathbb{Z}_3 \times \mathbb{Z}_6$ has 18 elements. $(0, 0)$ is neither a unit nor a zero divisor, and no element is both a unit or a zero divisor. Since I found 4 units in part (a), there are at most $18 - 1 - 4 = 13$ zero divisors, and I just need to check the nonunits as possibilities.

$$(0, 1)(1, 0) = (0, 0), \quad (0, 2)(1, 0) = (0, 0), \quad (0, 3)(1, 0) = (0, 0), \quad (0, 4)(1, 0) = (0, 0), \quad (0, 5)(1, 0) = (0, 0),$$

$$(1, 0)(0, 1) = (0, 0), \quad (2, 0)(0, 1) = (0, 0),$$

$$(1, 2)(0, 3) = (0, 0), \quad (1, 3)(0, 2) = (0, 0), \quad (1, 4)(0, 3) = (0, 0),$$

$$(2, 2)(0, 3) = (0, 0), \quad (2, 3)(0, 2) = (0, 0), \quad (2, 4)(0, 3) = (0, 0).$$

The 13 elements which are the first elements of each product above are the zero divisors. It turns out that the elements of $\mathbb{Z}_3 \times \mathbb{Z}_6$ consist of $(0, 0)$, the units, and the zero divisors. (This doesn't *have* to happen in every ring.) $\square$

---

22. Let R be a ring. Let $e \in R$ be **idempotent**; that is, $e^2 = e$.

(a) Let

$$eRe = \left\{ere \;\middle|\; r \in R\right\}.$$

Show that eRe is a subring of R.

(b) Show that e is an identity element for eRe.

(a) Let $ere, ese \in eRe$. Then

$$ere + ese = e(r + s)e \in eRe.$$

Therefore, eRe is closed under addition.

eRe contains the additive identity, since $0 = e \cdot 0 \cdot e \in eRe$.

Let $ere \in eRe$. Then $-(ere) = e(-r)e \in eRe$, so eRe is closed under taking additive inverses.

Finally, let $ere, ese \in eRe$. Then

$$ere \cdot ese = e(res)e \in eRe.$$

Therefore, eRe is closed under multiplication.

Hence, eRe is a subring.

Note that the proof didn't use the fact that e is idempotent. In general if $a \in R$, then aRa is a subring. □

(b) Let $ere \in eRe$. Then

$$e(ere) = e^2re = ere \quad \text{and} \quad (ere)e = ere^2 = ere.$$

Therefore, e is an identity element for eRe. □

---

23. Give an example of a ring R and nonzero elements $r, s \in R$ such that $r^2 + s^2 = 0$.

In $\mathbb{Z}_2$, $1^2 + 1^2 = 0$. □

---

24. Let R be a finite commutative ring with no zero divisors. Prove that R has a multiplicative identity.

First, if $R = \{0\}$, 0 is a multiplicative identity for the ring.

Assume then that R has elements other than 0: Suppose the elements are

$$R = \{0, r_1, r_2, \ldots, r_n\}.$$

The first thing I'll do is find a "candidate" for the identity.

How can I figure out which of the r's is 1? One way is to multiply everything by an element — say r_1 — and see which product is r_1. So look at

$$r_1 \cdot 0, r_1^2, r_1 \cdot r_2, \ldots, r_1 \cdot r_n.$$

Notice that if $r_1 \cdot r_i = r_1 \cdot r_j$, then cancelling the r_1's — as I can, since there are no zero divisors — I get $r_i = r_j$. This means that all these products are distinct. Since I started with $n + 1$ elements and I now have $n + 1$ *distinct* products, these products must be all the elements in the ring.

In particular, one of the products must be r_1. Suppose $r_1 \cdot r_2 = r_1$. This suggests that r_2 *might be* the identity (so I have my candidate). Now I'll try to prove it.

Note first that, by commutativity, $r_2 \cdot r_1 = r_1$ as well.

Since $r_2 \cdot 0$, I only have to show that $r_2 \cdot r_i = r_i$ for any i. Referring to the list of products above, I know that $r_1 \cdot r_j = r_i$ for some j. So

$$r_2 \cdot r_i = r_2 \cdot (r_1 \cdot r_j) = (r_2 \cdot r_1) \cdot r_j = r_1 \cdot r_j = r_i.$$

This shows that r_2 is a multiplicative identity.

Incidentally, R is now known to be a commutative ring with identity having no zero divisors — that is, R is an integral domain. But every finite integral domain is a field, so I've actually proved: A finite commutative ring with no zero divisors is a field. □

25. Let

$$\{\ldots, -4, -1, 0, 1, 4, \ldots\}.$$

It consists of squares of integers and their negatives, and it is not a subring of $\mathbb{Z}$. What is the smallest subring of $\mathbb{Z}$ which contains this set?

Let R be the smallest subring of $\mathbb{Z}$ which contains the set. Since R is closed under addition, and since $-1, 1 \in R$, every integer is contained in R (since any integer can be represented as a sum of 1's or -1's). Therefore, $R = \mathbb{Z}$. $\square$

---

26. Let x and y be elements in a ring R. Let

$$I = \{ax + by \mid a, b \in R\}.$$

Prove that I is a left ideal in R.

First, $0 = a \cdot x + 0 \cdot y \in I$.
If $ax + by \in I$, then $-(ax + by) = (-a)x + (-b)y \in I$.
If $ax + by, cx + dy \in I$, then

$$(ax + by) + (cx + dy) = (a + c)x + (b + d)y \in I.$$

Finally, if $ax + by \in I$ and $r \in R$, then

$$r(ax + by) = (ra)x + (rb)y \in I.$$

Therefore, I is a left ideal in R. $\square$

---

27. (a) Prove that the following set is an ideal in $\mathbb{Z}$:

$$I = \{4x + 14y + 16z \mid x, y, z \in \mathbb{Z}\}.$$

(b) Find an integer n such that $I = \langle n \rangle$ (and prove that your n works).

(a) First, $0 = 4 \cdot 0 + 14 \cdot 0 + 16 \cdot 0 \in I$.
If $4x + 14y + 16z, 4x' + 14y' + 16z' \in I$, then

$$(4x + 14y + 16z) + (4x' + 14y' + 16z') = 4(x + x') + 14(y + y') + 16(z + z') \in I.$$

If $4x + 14y + 16z \in I$, then

$$-(4x + 14y + 16z) = 4(-x) + 14(-y) + 16(-z) \in I.$$

Finally, if $4x + 14y + 16z \in I$ and $m \in \mathbb{Z}$, then

$$m \cdot (4x + 14y + 16z) = 4(mx) + 14(my) + 16(mz) \in I.$$

Therefore, I is an ideal in $\mathbb{Z}$. $\square$

(b) Since $(4, 14, 16) = 2$, I claim that $I = \langle 2 \rangle$.

First, if $4x + 14y + 16z \in I$, then

$$4x + 14y + 16z = 2(2x + 7z + 8z) \in \langle 2 \rangle.$$

Therefore, $I \subset \langle 2 \rangle$.
Conversely, I note that by inspection I can write 2 as a linear combination of 4, 14, and 16:

$$2 = (-1) \cdot 14 + 16.$$

Thus, if $2n \in \langle 2 \rangle$, then

$$2n = 4 \cdot 0 + 14 \cdot (-n) + 16 \cdot n \in I.$$

Therefore, $\langle 2 \rangle \subset I$.
Hence, $I = \langle 2 \rangle$. $\square$

---

28. Prove that the following set is a subring in $\mathbb{Z}_3 \times \mathbb{Z}_3$, but not an ideal:

$$A = \{(0,0), (1,1), (2,2)\}.$$

$\{(0,0), (1,1), (2,2)\}$ is $\langle (1,1) \rangle$, the subgroup generated by $(1,1)$. Therefore, it's a subgroup under addition.

Elements of A have the form (x,x), where $x \in \mathbb{Z}_3$. Now

$$(x,x) \cdot (y,y) = (xy, xy) \in A.$$

Hence, A is closed under multiplication, and it's a subring.
It is not an ideal, since $(2,2) \in A$, $(1,2) \in \mathbb{Z}_3 \times \mathbb{Z}_3$, but

$$(1,2) \cdot (2,2) = (2,1) \notin A. \quad \square$$

---

29. $\mathbb{Z} \times \mathbb{Z}$ is a ring under componentwise addition and multiplication. Consider the following subset of $\mathbb{Z} \times \mathbb{Z}$:

$$S = \{(a,b) \mid 2 \mid a \quad \text{or} \quad 2 \mid b\}.$$

Check each axiom for an ideal. If the axiom holds, prove it. If the axiom does not hold, give a specific counterexample.

Since $2 \mid 0$, I have $(0,0) \in S$. Thus, S contains the zero element.
Suppose $(a,b) \in S$. Then either $2 \mid a$ or $2 \mid b$.
If $2 \mid a$, then $2 \mid -a$, so $-(a,b) = (-a,-b) \in S$.
If $2 \mid b$, then $2 \mid -b$, so $-(a,b) = (-a,-b) \in S$.
Thus, S is closed under additive inverses.
Since $2 \mid 2$, I have $(2,1) \in S$ and $(1,2) \in S$. But

$$(2,1) + (1,2) = (3,3) \notin S.$$

Hence, S is not closed under sums.
Let $(a,b) \in S$ and $(r,s) \in \mathbb{Z} \times \mathbb{Z}$. Then

$$(r,s)(a,b) = (ra, sb).$$

If $2 \mid a$, then $2 \mid ra$, so $(r,s)(a,b) = (ra, sb) \in S$.

If $2 \mid b$, then $2 \mid sb$, so $(r,s)(a,b) = (ra, sb) \in S$.
Thus, S is closed under products by ring elements. □

---

30. Define $f : \mathbb{Z} \to \mathbb{Z}$ by

$$f(x) = |x|.$$

Check each axiom for a ring map. If the axiom holds, prove it. If the axiom doesn't hold, give a specific counterexample.

The identity axiom holds:

$$f(1) = |1| = 1.$$

The addition axiom does not hold:

$$f[2 + (-1)] = f(1) = |1| = 1, \quad \text{but} \quad f(2) + f(-1) = |2| + |-1| = 3.$$

The multiplication axiom holds:

$$f(xy) = |xy| = |x||y| = f(x)f(y). \quad \square$$

---

31. Define $f : \mathbb{R}^3 \to \mathbb{R}^2$ by

$$f(x,y,z) = (2x - y, 2y - z).$$

Check each axiom for a ring map. If the axiom holds, prove it. If the axiom doesn't hold, give a specific counterexample.

The identity axiom holds:

$$f(1,1,1) = (2 - 1, 2 - 1) = (1,1).$$

The addition axiom holds:

$$f[(a,b,c) + (d,e,f)] = f(a + d, b + e, c + f) = (2a + 2d - b - e, 2b + 2e - c - f),$$

$$f(a,b,c) + f(d,e,f) = (2a - b, 2b - c) + (2d - e, 2e - f) = (2a + 2d - b - e, 2b + 2e - c - f).$$

The multiplication axiom doesn't hold:

$$f[(1,2,3) \cdot (4,5,6)] = f(4, 1018) = (-2, 2),$$

$$f(1,2,3) \cdot f(4,5,6) = (0,1) \cdot (3,4) = (0,4). \quad \square$$

To understand a new idea break an old habit. - Jean Toomer