Math 345
10-1-2020

Review Problems for the Final

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. Prove that if n is an integer, then $(4n+6, 3n+4)$ is either 1 or 2. Give specific examples which show that both cases can occur.

2. Find the greatest common divisor of 847 and 133 and write it as a linear combination with integer coefficients of 847 and 133.

3. Show that the following set is a subgroup of $GL(2,\mathbb{R})$:

$$H = \left\{ \begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix} \;\middle|\; x, y \in \mathbb{R}, \quad xy \neq 0 \right\}$$

However, show that it is *not* a normal subgroup of $GL(2,\mathbb{R})$.

4. Consider the map $\phi : \mathbb{Z}_8 \to \mathbb{Z}_8$ given by $\phi(n) = n + 2 \pmod 8$. Is ϕ a group homomorphism? Why or why not?

5. Consider the map $\phi : \mathbb{Z} \to \mathbb{Z}$ given by $\phi(n) = n^2$. Is ϕ a group homomorphism? Why or why not?

6. $\mathbb{Z} \times \mathbb{Z}$ is a group under componentwise addition and $\mathbb{Z}$ is a group under addition. Prove that

$$\frac{\mathbb{Z} \times \mathbb{Z}}{\langle (7,25) \rangle} \approx \mathbb{Z}.$$

7. $\mathbb{R}^2$ is a group under componentwise addition and $\mathbb{R}$ is a group under addition. Let

$$H = \left\{ x \cdot (19, -\sqrt{7}) \;\middle|\; x \in \mathbb{R} \right\}.$$

Prove that $\dfrac{\mathbb{R}^2}{H} \approx \mathbb{R}$.

8. $\mathbb{Z} \times \mathbb{Z}$ and $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ are groups under componentwise addition. Let

$$H = \{ t \cdot (-4, 3, 1) \mid t \in \mathbb{Z} \}.$$

Show that

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

9. Here is the multiplication table for the Klein 4-group V:

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Write down all the subgroups of V.

10. Find all integer solutions (x, y) to

$$x^2 - y^2 + 2y = 12.$$

11. Find an element of order 30 in $\mathbb{Z}_{25} \times \mathbb{Z}_{12}$.

12. Find the primary decomposition of U_{16}.

13. (a) What is the order of the element a^4 in the cyclic group

$$\{a^k \mid a^{22} = 1\}?$$

(b) What is the order of the element 10 in $\mathbb{Z}_{45}$?

(c) What elements generate the cyclic group $\mathbb{Z}_{12}$?

14. Subgroups of cyclic groups are cyclic. Give an example of an abelian group which is not cyclic, but in which every proper subgroup is cyclic.

15. (a) Prove that a group cannot be the union of two proper subgroups.

(b) Find a group which is a union of *three* proper subgroups.

16. Let $\phi : G \to H$ be a group homomorphism. Prove that ϕ is injective if and only if $\ker \phi = \{1\}$.

17. Is there a group homomorphism $\phi : \mathbb{Z}_6 \to \mathbb{Z}_{12}$ such that $\ker \phi = \{0\}$? Construct such a homomorphism, or show that such a homomorphism cannot exist.

18. (a) Give an example of a finite group which is not abelian.

(b) Give an example of an abelian group which is not finite.

(c) Give an example of a group which is neither finite nor abelian.

19. Let $SL(2, \mathbb{R})$ denote the subgroup of $GL(2, \mathbb{R})$ consisting of matrices of determinant 1. Show that the following matrices lie in the same left coset of $SL(2, \mathbb{R})$:

$$\begin{bmatrix} 1 & 1 \\ 1 & 4 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 5 & 2 \\ 11 & 5 \end{bmatrix}.$$

20. Give an example of a finite commutative ring with 1 which is not an integral domain.

21. (a) Define $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ by

$$f(x, y) = x^3 + y^3.$$

Show that f is surjective.

(b) Define $g : \mathbb{R} \times \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ by

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

Show that g is surjective.

(c) Define $h : M(2, \mathbb{R}) \to M(2, \mathbb{R})$ by

$$h\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = \begin{bmatrix} a & 2b \\ 3c & 4d \end{bmatrix}.$$

Show that h is surjective.

(d) Define $k : \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ by
$$k(x) = (x, x).$$

Show that k is *not* surjective.

(e) Give an example of a group map $p : \mathbb{Z} \to \mathbb{Z}$ which is not surjective, and a surjective function $q : \mathbb{Z} \to \mathbb{Z}$ which is not a group map.

22. (a) Explain why $\mathbb{Q}$ is not a group under multiplication.

(b) Do the nonzero elements of $\mathbb{Z}_6$ form a group under multiplication mod 6?

(c) Show that the nonzero elements of $\mathbb{Z}_5$ form a group under multiplication mod 5. What group?

23. Reduce $32^{2011} \pmod{41}$ to an integer in the set $\{0, 1, \ldots, 40\}$.

24. Reduce $\dfrac{148!}{3 \cdot 75} \pmod{149}$ to an integer in the set $\{0, 1, \ldots, 148\}$. (Note: 149 is prime.)

25. The definition of a **subring** of a ring does not require that you check associativity for addition or multiplication. Explain why.

26. Prove that if I is an ideal in a ring R with identity and $1 \in I$, then $I = R$.

27. Show that the only (two-sided) ideals in $M(2, \mathbb{R})$ are the zero ideal and the whole ring.

28. Consider the following subset of the ring $\mathbb{Z} \times \mathbb{Z}$:
$$S = \{(m + n, m - n) \mid m, n \in \mathbb{Z}\}.$$

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

29. (a) Show that $x^2 + x + 1$ is irreducible in $\mathbb{Z}_5[x]$.

(b) Find $[(2x + 3) + \langle x^2 + x + 1\rangle]^{-1}$ in $\dfrac{\mathbb{Z}_5[x]}{\langle x^2 + x + 1\rangle}$.

(c) Compute the product of the cosets $\big((x^2 + 2) + \langle x^2 + x + 1\rangle\big) \cdot \big((3x + 4) + \langle x^2 + x + 1\rangle\big)$ in the quotient ring $\dfrac{\mathbb{Z}_5[x]}{\langle x^2 + x + 1\rangle}$. Write your answer in the form $(ax + b) + \langle x^2 + x + 1\rangle$, where $a, b \in \mathbb{Z}_5$.

30. Factor $x^4 + 64$ in $\mathbb{Q}[x]$.

31. (a) Show that $x^4 + 1$ has no roots in $\mathbb{Z}_5$.

(b) Show that $x^4 + 1$ factors in $\mathbb{Z}_5[x]$.

32. In the ring $\mathbb{R}[x]$, consider the subset
$$\langle x^2 - x - 2, x^2 - 1\rangle = \{a(x)(x^2 - x - 2) + b(x)(x^2 - 1) \mid a(x), b(x) \in \mathbb{R}[x]\}.$$

(a) Show that $\langle x^2 - x - 2, x^2 - 1\rangle$ is an ideal.

(b) Is $x^2 + x + 3$ in $\langle x^2 - x - 2, x^2 - 1\rangle$?

33. $x^2 + 2 = (x + 1)(x + 2)$ is a factorization of $x^2 + 2$ into irreducibles in $\mathbb{Z}_3[x]$. Find a different factorization of $x^2 + 2$ into irreducibles in $\mathbb{Z}_3[x]$.

34. Compute the product of the cycles $(2\ 4\ 6\ 3)(1\ 3\ 4)$ (right to left) and write the result as a product of disjoint cycles.

35. Define $\phi : \mathbb{Z}[x] \to \mathbb{Z}[x]$ by

$$\phi(f(x)) = f(x)^2.$$

Determine which of the axioms for a ring map are satisfied by ϕ. If an axiom is not satisfied, give a specific example which shows that the axiom is violated.

36. Define $\phi : \mathbb{Z}_2[x] \to \mathbb{Z}_2[x]$ by

$$\phi(f(x)) = f(x)^2.$$

(a) Show that ϕ is a ring map.

(b) Determine the kernel of ϕ.

(c) Show that $x^4 + 1 \in \operatorname{im} \phi$. Is ϕ surjective?

37. Find the quotient and the remainder when $2x^4 + 3x^3 + x + 1$ is divided by $3x^2 + 1$ in $\mathbb{Z}_5[x]$.

38. (a) Explain why $x^4 + 1$ has no roots in $\mathbb{R}$.

(b) Is $x^4 + 1$ irreducible in $\mathbb{R}[x]$?

39. List the zero divisors and the units in $\mathbb{Z}_2 \times \mathbb{Z}_3$.

40. Prove that if I is a left ideal in a division ring R, then either $I = \{0\}$ or $I = R$.

41. Let R be a ring, and let $r \in R$. The **centralizer** $C(r)$ of r is the set of elements of R which commute with r:

$$C(r) = \{a \in R \mid ra = ar\}.$$

Prove that $C(r)$ is a subring of R.

42. Let

$$I = \left\{ \begin{bmatrix} 0 & x & 0 \\ 0 & y & 0 \\ 0 & z & 0 \end{bmatrix} \,\middle|\, x, y, z \in \mathbb{R} \right\}.$$

Prove that I is a left ideal, but not a right ideal, in the ring $M(3, \mathbb{R})$.

43. (a) List the elements of U_{42}.

(b) List the elements of the subgroup $\langle 25 \rangle$ in U_{42}.

(c) List the cosets of the subgroup $\langle 25 \rangle$ in U_{42}.

(d) Is the quotient group isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ or $\mathbb{Z}_4$?

44. Find the primary decomposition and the invariant factor decomposition for $\mathbb{Z}_{24} \times \mathbb{Z}_{28} \times \mathbb{Z}_{21}$.

45. What is the largest possible order of an element of $\mathbb{Z}_{30} \times \mathbb{Z}_{45} \times \mathbb{Z}_{60}$?

46. Let $f, g : G \to H$ be group maps. Let

$$E = \left\{ x \in G \,\middle|\, f(x) = g(x) \right\}.$$

Prove that E is a subgroup of G. (E is called the **equalizer** of f and g.)

47. Let R be a ring such that for each $r \in R$, there is a unique element $s \in R$ such that $rsr = r$. Prove that R has no zero divisors.

48. Suppose $f : R \to S$ is a ring homomorphism and R and S are rings with identity, *but do not assume that* $f(1_R) = 1_S$. Prove that if f is surjective, then $f(1_R) = 1_S$.

49. Factor $3x^3 + 2x^2 + 3x + 2$ in $\mathbb{Z}_5[x]$.

50. Find the remainder when $x^{41} + 3x^{39} + 4x^{11} + 2x^9 + 5x + 3$ is divided by $x + 4$ in $\mathbb{Z}_5[x]$.

51. Calvin Butterball thinks $x^2 + 1 \in \mathbb{Z}_2[x]$ is irreducible, based on the fact that solving $x^2 + 1 = 0$ gives $x = \pm i$, which are complex numbers. Is he right?

52. Find the greatest common divisor of $x^4 + x^3 + x^2 + 2x + 3$ and $x^3 + 4x^2 + 2x + 3$ in $\mathbb{Z}_5[x]$ and express the greatest common divisor as a linear combination (with coefficients in $\mathbb{Z}_5[x]$) of the two polynomials.

53. The following set is an ideal in the ring $\mathbb{Z}_2 \times \mathbb{Z}_8$:

$$I = \{(0,0), (0,4), (1,0), (1,4)\}.$$

(a) List the cosets of I in $\mathbb{Z}_2 \times \mathbb{Z}_8$.

(b) Construct addition and multiplication tables for the quotient ring $\dfrac{\mathbb{Z}_2 \times \mathbb{Z}_8}{I}$.

(c) Is $\dfrac{\mathbb{Z}_2 \times \mathbb{Z}_8}{I}$ an integral domain?

Solutions to the Review Problems for the Final

1. Prove that if n is an integer, then $(4n + 6, 3n + 4)$ is either 1 or 2. Give specific examples which show that both cases can occur.

Note that

$$3(4n + 6) - 4(3n + 4) = 2.$$

Now $(4n+6, 3n+4)$ divides $4n+6$ and $3n+4$, so it divides $3(4n+6) - 4(3n+4)$, and hence it divides 2. The only positive integers that divide 2 are 1 and 2. Hence, $(4n + 6, 3n + 4)$ is either 1 or 2.

If $n = 1$, I have $4n + 6 = 10$ and $3n + 4 = 7$, and $(10, 7) = 1$.

If $n = 2$, I have $4n + 6 = 14$ and $3n + 4 = 10$, and $(14, 10) = 2$.

This shows that both cases can occur. $\square$

---

2. Find the greatest common divisor of 847 and 133 and write it as a linear combination with integer coefficients of 847 and 133.

847	-	51
133	6	8
49	2	3
35	1	2
14	2	1
7	2	0

The greatest common divisor is 7, and

$$7 = (-8)(847) + (51)(133). \quad \square$$

---

3. Show that the following set is a subgroup of $GL(2, \mathbb{R})$:

$$H = \left\{ \begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix} \;\middle|\; x, y \in \mathbb{R}, \quad xy \neq 0 \right\}$$

However, show that it is *not* a normal subgroup of $GL(2, \mathbb{R})$.

Since $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in H$, H contains the identity.
If $\begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix} \in H$, then

$$\begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix} = \begin{bmatrix} x^{-1} & 0 \\ 0 & y^{-1} \end{bmatrix} \in H.$$

(Note that $xy \neq 0$ implies $x \neq 0$ and $y \neq 0$, so x^{-1} and y^{-1} are defined.) Therefore, H is closed under taking inverses.

Finally,

$$\begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix} \begin{bmatrix} x' & 0 \\ 0 & y' \end{bmatrix} = \begin{bmatrix} xx' & 0 \\ 0 & yy' \end{bmatrix} \in H.$$

(If $xy \neq 0$ and $x'y' \neq 0$, then $x, x', y, y' \neq 0$, so $xx' \neq 0$ and $yy' \neq 0$.) Thus, H is closed under products. Hence, H is a subgroup.

However,

$$\begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 3 & -2 \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} -1 & 2 \\ -3 & 4 \end{bmatrix} \notin H.$$

Therefore, H is not a normal subgroup. $\square$

---

4. Consider the map $\phi : \mathbb{Z}_8 \to \mathbb{Z}_8$ given by $\phi(n) = n + 2 \pmod 8$. Is ϕ a group homomorphism? Why or why not?

A group homomorphism must map the identity in the domain to the identity in the range. The identity in $\mathbb{Z}_8$ is 0. However, $\phi(0) = 2$. Therefore, ϕ is not a homomorphism. $\square$

---

5. Consider the map $\phi : \mathbb{Z} \to \mathbb{Z}$ given by $\phi(n) = n^2$. Is ϕ a group homomorphism? Why or why not?

In this case, $\phi(0) = 0$, so ϕ *does* map the identity to the identity. However,

$$\phi(1 + 1) = \phi(2) = 2^2 = 4, \quad \text{but} \quad \phi(1) + \phi(1) = 1 + 1 = 2.$$

Since $\phi(a + b) \neq \phi(a) + \phi(b)$ for all a and b, ϕ is not a homomorphism. $\square$

---

6. $\mathbb{Z} \times \mathbb{Z}$ is a group under componentwise addition and $\mathbb{Z}$ is a group under addition. Prove that

$$\frac{\mathbb{Z} \times \mathbb{Z}}{\langle (7, 25) \rangle} \approx \mathbb{Z}.$$

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

$$f(x, y) = 25x - 7y.$$

f can be represented by matrix multiplication:

$$\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = \begin{bmatrix} 25 & -7 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}.$$

Hence, it's a group map.
Let $n(7, 25) = (7n, 25n) \in \langle (7, 25) \rangle$. Then

$$f((7n, 25n) = 25(7n) - 7(25n) = 0.$$

Thus, $\langle (7, 25) \rangle \subset \ker f$.
Let $(x, y) \in \ker f$. Then

$$\begin{aligned} f(x, y) &= 0 \\ 25x - 7y &= 0 \\ 25x &= 7y \end{aligned}$$

Now $25 \mid 7y$ but $(7, 25) = 1$. By Euclid's lemma, $25 \mid y$. Say $y = 25n$. Then

$$25x = 7(25n), \quad \text{so} \quad x = 7n.$$

Therefore,

$$(x, y) = (7n, 25n) = n(7, 25) \in \langle (7, 25) \rangle.$$

Thus, $\ker f \subset \langle (7, 25) \rangle$.
Hence, $\langle (7, 25) \rangle = \ker f$.
Let $z \in \mathbb{Z}$. Note that

$$1 = (25, -7) = 2 \cdot 25 + 7 \cdot (-7).$$

Multiplying by z, I get

$$z = 25(2z) - 7(7z).$$

Then

$$f(2z, 7z) = 25(2z) - 7(7z) = z.$$

This proves that $\operatorname{im} f = \mathbb{Z}$.
Hence,

$$\frac{\mathbb{Z} \times \mathbb{Z}}{\langle (7, 25) \rangle} = \frac{\mathbb{Z} \times \mathbb{Z}}{\ker f} \approx \operatorname{im} f = \mathbb{Z}. \quad \square$$

---

7. $\mathbb{R}^2$ is a group under componentwise addition and $\mathbb{R}$ is a group under addition. Let

$$H = \left\{ x \cdot (19, -\sqrt{7}) \;\middle|\; x \in \mathbb{R} \right\}.$$

Prove that $\dfrac{\mathbb{R}^2}{H} \approx \mathbb{R}$.

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

$$f(x, y) = \sqrt{7}x + 19y.$$

Note that

$$f\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = \begin{bmatrix} \sqrt{7} & 19 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}.$$

Since f can be expressed as multiplication by a constant matrix, it's a linear transformation, and hence a group map.

Let $x \cdot (19, -\sqrt{7}) \in H$. Then

$$f[x \cdot (19, -\sqrt{7})] = f(19x, -\sqrt{7}x) = \sqrt{7}(19x) + 19(-\sqrt{7}x) = 0.$$

Therefore, $x \cdot (19, -\sqrt{7}) \in \ker f$, and hence $H \subset \ker f$.
Let $(x, y) \in \ker f$. Then

$$\begin{aligned} f(x, y) &= 0 \\ \sqrt{7}x + 19y &= 0 \\ 19y &= -\sqrt{7}x \\ y &= -\frac{\sqrt{7}}{19}x \end{aligned}$$

Hence,

$$(x, y) = \left(x, -\frac{\sqrt{7}}{19}x\right) = \frac{1}{19}x \cdot (19, -\sqrt{7}) \in H.$$

Therefore, $\ker f \subset H$. Hence, $\ker f = H$.
Let $z \in \mathbb{R}$. Note that

$$f\left(\frac{1}{\sqrt{7}}z, 0\right) = \sqrt{7} \cdot \frac{1}{\sqrt{7}}z + 19 \cdot 0 = z.$$

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

$$\frac{\mathbb{R}^2}{H} = \frac{\mathbb{R}^2}{\ker f} \approx \operatorname{im} f = \mathbb{R}. \quad \square$$

---

8. $\mathbb{Z} \times \mathbb{Z}$ and $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ are groups under componentwise addition. Let

$$H = \{t \cdot (-4, 3, 1) \mid t \in \mathbb{Z}\}.$$

Show that

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

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

$$f(x, y, z) = (x + 4z, y - 3z).$$

Note that

$$f\left(\begin{bmatrix} x \\ y \\ z \end{bmatrix}\right) = \begin{bmatrix} 1 & 0 & 4 \\ 0 & 1 & -3 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix}.$$

Since f can be written as multiplication by a constant matrix, it is a group map.
Let $t \cdot (-4, 3, 1) = (-4t, 3t, t) \in H$. Then

$$f(-4t, 3t, t) = (-4t + 4t, 3t - 3t) = (0, 0).$$

Hence, $(-4t, 3t, t) \in \ker f$, so $H \subset \ker f$.
Let $(x, y, z) \in \ker f$. Then

$$\begin{aligned} f(x, y, z) &= (0, 0) \\ (x + 4z, y - 3z) &= (0, 0) \end{aligned}$$

This gives $x + 4z = 0$ and $y - 3z = 0$. The first equation gives $x = -4z$ and the second equation gives $y = 3z$. Hence,

$$(x, y, z) = (-4z, 3z, z) \in H.$$

Therefore, $\ker f \subset H$, and hence $\ker f = H$.

Let $(a, b) \in \mathbb{Z} \times \mathbb{Z}$. Then

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

Hence, f is surjective, and $\operatorname{im} f = \mathbb{Z} \times \mathbb{Z}$.

Therefore,

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

---

9. Here is the multiplication table for the Klein 4-group V:

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Write down all the subgroups of V.

By Lagrange's theorem, the order of a subgroup must divide the order of the group. Hence, there *could be* subgroups of order 1, 2, or 4.

The subgroup of order 1 is $\{1\}$; the subgroup of order 4 is the whole group. A subgroup of order 2 must contain the identity and another element; by closure under inverses, the other element must be its own inverse. Hence, the subgroups of V are:

$$V, \{1, a\}, \{1, b\}, \{1, c\}, \{1\}. \quad \square$$

---

10. Find all integer solutions (x, y) to

$$x^2 - y^2 + 2y = 12.$$

$$\begin{aligned} x^2 - y^2 + 2y &= 12 \\ x^2 - y^2 + 2y - 1 &= 12 - 1 \\ x^2 - (y - 1)^2 &= 11 \\ (x - (y - 1))(x + (y - 1)) &= 11 \\ (x - y + 1)(x + y - 1) &= 11 \end{aligned}$$

This equation expresses 11 as a product of two integers $x - y + 1$ and $x + y - 1$. There are four ways to do this.

Case 1.

$$\begin{aligned} x - y + 1 &= 11 \\ x + y - 1 &= 1 \end{aligned}$$

Solving simultaneously, I get $x = 6$ and $y = -4$.

Case 2.

$$\begin{aligned} x - y + 1 &= 1 \\ x + y - 1 &= 11 \end{aligned}$$

Solving simultaneously, I get $x = 6$ and $y = 6$.

Case 3.

$$\begin{aligned} x - y + 1 &= -1 \\ x + y - 1 &= -11 \end{aligned}$$

Solving simultaneously, I get $x = -6$ and $y = -4$.

Case 4.

$$\begin{aligned} x - y + 1 &= -11 \\ x + y - 1 &= -1 \end{aligned}$$

Solving simultaneously, I get $x = -6$ and $y = 6$.

The solutions are $(6, -4)$, $(6, 6)$, $(-6, -4)$, and $(-6, 6)$. $\square$

---

11. Find an element of order 30 in $\mathbb{Z}_{25} \times \mathbb{Z}_{12}$.

5 has order 5 in $\mathbb{Z}_{25}$.
2 has order 6 in $\mathbb{Z}_{12}$.
Hence, $(5, 2)$ has order $[5, 6] = 30$ in $\mathbb{Z}_{25} \times \mathbb{Z}_{12}$. $\square$

---

12. Find the primary decomposition of U_{16}.

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

The operation is multiplication mod 16. The possibilities are

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

I start computing the orders of elements. The order of an element can be 1, 2, 4, 8, or 16, so I can repeatedly square until I get the identity.

$$3^2 = 9, \quad 3^4 = 1.$$

Since 3 has order 4, and since every element of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ has order 2 or less, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ is ruled out.

$$5^2 = 9, \quad 5^4 = 1.$$

$$7^2 = 1.$$

$$9^2 = 1.$$

$$11^2 = 9, \quad 11^4 = 1.$$

$$13^2 = 9, \quad 13^4 = 1.$$

$$15^2 = 1.$$

Since there are no elements of order 8, the group can't be $\mathbb{Z}_8$. Hence, $U_{16} \approx \mathbb{Z}_2 \times \mathbb{Z}_4$. $\square$

---

13. (a) What is the order of the element a^4 in the cyclic group

$$\{a^k \mid a^{22} = 1\}?$$

(b) What is the order of the element 10 in $\mathbb{Z}_{45}$?

(c) What elements generate the cyclic group $\mathbb{Z}_{12}$?

(a) The order of a^k in the cyclic group of order n with generator a is $\dfrac{n}{(n,k)}$. So the order of a^4 in $\{a^k \mid a^{22} = 1\}$ is

$$\frac{22}{(4,22)} = \frac{22}{2} = 11. \quad \square$$

(b) The order of 10 in $\mathbb{Z}_{45}$ is

$$\frac{45}{(45,10)} = \frac{45}{5} = 9. \quad \square$$

(c) The order of the element $m \in \mathbb{Z}_{12}$ is $\dfrac{12}{(m,12)}$. If m generates $\mathbb{Z}_{12}$, it must have order 12, so

$$\frac{12}{(m,12)} = 12.$$

This implies that $(m,12) = 1$; that is, m is relatively prime to 12. Therefore, the generators are $\{1,5,7,11\}$. $\square$

---

14. Subgroups of cyclic groups are cyclic. Give an example of an abelian group which is not cyclic, but in which every proper subgroup is cyclic.

V is not cyclic, since there are no elements of order 4. However, every subgroup of V is cyclic. $\square$

---

15. (a) Prove that a group cannot be the union of two proper subgroups.

(b) Find a group which is a union of *three* proper subgroups.

(a) Suppose G is a group, H and K are proper subgroups, and $G = H \cup K$. Since H is not all of G, I can find an element $k \in K$ such that $k \notin H$. Likewise, I can find an element $h \in H$ such that $h \notin K$.

Now consider the element hk. It's in G, so it's either in H or K. But $hk = h' \in H$ gives $k = h^{-1}h' \in H$, contradicting the assumption that $k \notin H$. And $hk = k' \in K$ gives $h = k'k^{-1} \in K$, which contradicts the assumption that $h \notin K$.

Therefore, G cannot be the union of H and K. $\square$

(b) Consider the Klein 4-group V:

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

V is the union of the proper subgroups $\{1, a\}$, $\{1, b\}$, and $\{1, c\}$. $\square$

---

16. Let $\phi : G \to H$ be a group homomorphism. Prove that ϕ is injective if and only if $\ker \phi = \{1\}$.

Suppose that ϕ is injective. (This means that different inputs go to different outputs, or alternatively, that $\phi(x) = \phi(y)$ implies $x = y$.) I want to show that $\ker \phi = \{1\}$.

Since $\{1\} \subset \ker \phi$, I need to show $x \in \ker \phi$ implies $x = 1$. Therefore, take $x \in \ker \phi$, so $\phi(x) = 1$. Now $\phi(1) = 1$, so $\phi(x) = 1 = \phi(1)$. Since ϕ is injective, this implies that $x = 1$, which is what I wanted to show.

Conversely, suppose $\ker \phi = \{1\}$. I want to show that ϕ is injective. To do this, suppose $\phi(x) = \phi(y)$. I need to show $x = y$. Rearrange the equation:

$$\phi(x) = \phi(y), \quad \phi(x)^{-1}\phi(x) = \phi(x)^{-1}\phi(y), \quad 1 = \phi(x)^{-1}\phi(y), \quad 1 = \phi(x^{-1})\phi(y), \quad 1 = \phi(x^{-1}y).$$

But this means that $x^{-1}y \in \ker \phi = \{1\}$, i.e.

$$x^{-1}y = 1, \quad \text{so} \quad x = y.$$

Therefore, ϕ is injective. $\square$

---

17. Is there a group homomorphism $\phi : \mathbb{Z}_6 \to \mathbb{Z}_{12}$ such that $\ker \phi = \{0\}$? Construct such a homomorphism, or show that such a homomorphism cannot exist.

If $\phi : \mathbb{Z}_6 \to \mathbb{Z}_{12}$ is a homomorphism such that $\ker \phi = \{0\}$, then ϕ is 1-1. Since the image of ϕ will be isomorphic to $\mathbb{Z}_6/\{0\} \approx \mathbb{Z}_6$, the image of such a map must be a cyclic subgroup of order 6.

The only subgroup of order 6 in $\mathbb{Z}_{12}$ is

$$\{0, 2, 4, 6, 8, 10\}.$$

The only possibility is that ϕ maps $\mathbb{Z}_6$ isomorphically onto this subgroup. Such an isomorphism must send the generator $1 \in \mathbb{Z}_6$ to a generator of $\{0, 2, 4, 6, 8, 10\}$. Since 2 generates $\{0, 2, 4, 6, 8, 10\}$, I will try $\phi(1) = 2$.

Since ϕ is supposed to be a group map, this forces $\phi(x) = 2x \pmod{12}$ for $x \in \mathbb{Z}_6$. Then if $x, y \in \mathbb{Z}_6$,

$$\phi(x + y) = 2(x + y) \pmod{12} = (2x + 2y) \pmod{12} = 2x \pmod{12} + 2y \pmod{12} = \phi(x) + \phi(y).$$

Hence, ϕ is a group map.

Finally, the only element of $\mathbb{Z}_6$ that maps to 0 is 0, by inspection. Thus, $\ker \phi = \{0\}$, and ϕ satisfies the conditions of the problem. $\square$

---

18. (a) Give an example of a finite group which is not abelian.

(b) Give an example of an abelian group which is not finite.

(c) Give an example of a group which is neither finite nor abelian.

(a) S_3 is finite, but not abelian. $\square$

(b) $\mathbb{Z}$ is abelian, but not finite. $\square$

(c) $GL(2, \mathbb{R})$ is an infinite group which is not abelian. For example,

$$\begin{bmatrix} 1 & 2 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 3 \\ 0 & 1 \end{bmatrix} \quad \text{but} \quad \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}. \quad \square$$

19. Let $SL(2,\mathbb{R})$ denote the subgroup of $GL(2,\mathbb{R})$ consisting of matrices of determinant 1. Show that the following matrices lie in the same left coset of $SL(2,\mathbb{R})$:

$$\begin{bmatrix} 1 & 1 \\ 1 & 4 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 5 & 2 \\ 11 & 5 \end{bmatrix}.$$

If H is a subgroup of a group G, then $aH = bH$ if and only if $b^{-1}a \in H$. In this case,

$$\begin{bmatrix} 5 & 2 \\ 11 & 5 \end{bmatrix}^{-1} \begin{bmatrix} 1 & 1 \\ 1 & 4 \end{bmatrix} = \frac{1}{3} \begin{bmatrix} 5 & -2 \\ -11 & 5 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 4 \end{bmatrix} = \frac{1}{3} \begin{bmatrix} 3 & -3 \\ -6 & 9 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ -2 & 3 \end{bmatrix}.$$

Now

$$\det \begin{bmatrix} 1 & -1 \\ -2 & 3 \end{bmatrix} = 3 - 2 = 1.$$

Hence,

$$\begin{bmatrix} 5 & 2 \\ 11 & 5 \end{bmatrix}^{-1} \begin{bmatrix} 1 & 1 \\ 1 & 4 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ -2 & 3 \end{bmatrix} \in SL(2,\mathbb{R}).$$

This shows that the matrices lie in the same left coset of $SL(2,\mathbb{R})$. $\square$

---

20. Give an example of a finite commutative ring with 1 which is not an integral domain.

$\mathbb{Z}_4$ is finite, commutative, and has a multiplicative identity 1. But $2 \cdot 2 = 0$, so it's not a domain. $\square$

---

21. (a) Define $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ by

$$f(x,y) = x^3 + y^3.$$

Show that f is surjective.

(b) Define $g : \mathbb{R} \times \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ by

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

Show that g is surjective.

(c) Define $h : M(2,\mathbb{R}) \to M(2,\mathbb{R})$ by

$$h\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = \begin{bmatrix} a & 2b \\ 3c & 4d \end{bmatrix}.$$

Show that h is surjective.

(d) Define $k : \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ by

$$k(x) = (x,x).$$

Show that k is *not* surjective.

(e) Give an example of a group map $p : \mathbb{Z} \to \mathbb{Z}$ which is not surjective, and a surjective function $q : \mathbb{Z} \to \mathbb{Z}$ which is not a group map.

(a) Let $z \in \mathbb{R}$. Then

$$f(\sqrt[3]{z}, 0) = (\sqrt[3]{z})^3 + 0^3 = z.$$

Therefore, f is surjective. $\square$

(b) Let $w \in \mathbb{R}$. Then

$$g(w, 0, 0) = w - 2 \cdot 0 + 3 \cdot 0 = w.$$

Therefore, g is surjective. $\square$

(c) Let $\begin{bmatrix} w & x \\ y & z \end{bmatrix} \in M(2, \mathbb{R})$. Then

$$h\left(\begin{bmatrix} w & \frac{x}{2} \\ \frac{y}{3} & \frac{z}{4} \end{bmatrix}\right) = \begin{bmatrix} w & x \\ y & z \end{bmatrix}.$$

Therefore, h is surjective. $\square$

(d) $(\sqrt{17}, \pi) \in \mathbb{R} \times \mathbb{R}$. But if

$$k(x) = (\sqrt{17}, \pi) \quad \text{then} \quad x = \sqrt{17} \quad \text{and} \quad x = \pi.$$

This contradiction shows that there is no $x \in \mathbb{R}$ such that $k(x) = (\sqrt{17}, \pi)$. Hence, k is not surjective. $\square$

(e) The function $p : \mathbb{Z} \to \mathbb{Z}$ defined by $p(x) = 2x$ is a group map, since

$$p(a + b) = 2(a + b) = 2a + 2b = p(a) + p(b).$$

However, p is not surjective, since (for example) there is no $n \in \mathbb{Z}$ such that $p(n) = 1$.

The function $q : \mathbb{Z} \to \mathbb{Z}$ given by $q(x) = x + 1$ is surjective: If $y \in \mathbb{Z}$, then

$$q(y - 1) = (y - 1) + 1 = y.$$

But q is not a group map: $q(0) = 1$, so q does not map the identity to the identity.

For that matter, the identity map $\text{id} : \mathbb{Z} \to \mathbb{Z}$ is a surjective group map, and the function $r : \mathbb{Z} \to \mathbb{Z}$ given by $r(x) = x^2$ is neither surjective nor a group map. The properties of surjectivity and being a group map are *independent*. $\square$

---

22. (a) Explain why $\mathbb{Q}$ is not a group under multiplication.

(b) Do the nonzero elements of $\mathbb{Z}_6$ form a group under multiplication mod 6?

(c) Show that the nonzero elements of $\mathbb{Z}_5$ form a group under multiplication mod 5. What group?

(a) $\mathbb{Q}$ is not a group under multiplication because not every element has a multiplicative inverse. To be specific, $0 \in \mathbb{Q}$ does not have a multiplicative inverse. $\square$

(b) $\{1, 2, 3, 4, 5\}$ is not a group under multiplication mod 6, because it is not closed under the operation: $2 \cdot 3 = 0 \notin \{1, 2, 3, 4, 5\}$, for instance. $\square$

(c) Here is the operation table:

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

The table shows that set is closed under the operation. Take for granted that multiplication mod 6 is associative (since $\mathbb{Z}_6$ is a ring under addition and multiplication mod 6). 1 is the identity element. The inverse of 2 is 3, the inverse of 3 is 2, and 4 is its own inverse. Therefore, this set is a group; it's usually denoted $\mathbb{Z}_5^*$.

$\mathbb{Z}_5^*$ a group with 4 elements. and the table shows that not every element has order 2. Therefore, $\mathbb{Z}_5^*$ is not isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$; it must be isomorphic to $\mathbb{Z}_4$. $\square$

---

23. Reduce $32^{2011} \pmod{41}$ to an integer in the set $\{0, 1, \ldots, 40\}$.

$41 \not| 32$, so by Fermat's theorem, $32^{40} = 1 \pmod{41}$. Therefore,

$$32^{2011} = 32^{2000} \cdot 32^{11} = (32^{40})^{50} \cdot 32^{11} =$$

$$1^{50} \cdot (32^5)^2 \cdot 32 = 33554432^2 \cdot 32 \pmod{41}.$$

Since $33554432 = 818400 \cdot 41 + 32$, $33554432 = 32 \pmod{41}$. Hence,

$$33554432^2 \cdot 32 = 32^3 = 9 \pmod{41}. \quad \square$$

---

24. Reduce $\dfrac{148!}{3 \cdot 75} \pmod{149}$ to an integer in the set $\{0, 1, \ldots, 148\}$. (Note: 149 is prime.)

$$x = \frac{148!}{3 \cdot 75} \pmod{149}$$
$$3 \cdot 75x = 148! = -1 \pmod{149}$$

At this point, you could use the Extended Euclidean Algorithm to find the inverses of 3 and 75 mod 149. But it's easier to note that

$$150 = 149 + 1 = 1 \pmod{149}.$$

Since $2 \cdot 75 = 150$ and $50 \cdot 3 = 150$, I have

$$2 \cdot 50 \cdot 3 \cdot 75x = 2 \cdot 50 \cdot (-1) \pmod{149}$$
$$x = -100 = 49 \pmod{149} \quad \square$$

---

25. The definition of a **subring** of a ring does not require that you check associativity for addition or multiplication. Explain why.

When you consider a subset S of a ring R, addition and multiplication are associative as operations in R. In showing that S is a subring, you're confining the operations to a *subset*, so they must continue to be associative.

(People often say that associativity is **inherited** from R by S.) For similar reasons, the definition of a **subgroup** does not require that you check associativity. $\square$

---

26. Prove that if I is an ideal in a ring R with identity and $1 \in I$, then $I = R$.

Since $I \subset R$ by definition, I only need to prove the opposite containment. Let $r \in R$. Now $1 \in I$, so $r \cdot 1 \in I$, i.e. $r \in I$. Hence, $R \subset I$, so $I = R$. $\square$

---

27. Show that the only (two-sided) ideals in $M(2, \mathbb{R})$ are the zero ideal and the whole ring.

Let S be an ideal in $M(2, \mathbb{R})$, and suppose S is nonzero. I'll show that $S = M(2, \mathbb{R})$.

S contains a nonzero matrix A. If A is invertible, then $A \in S$ implies $A^{-1}A \in S$, i.e. $I \in S$, where I is the identity matrix. By the last problem, this implies that $S = M(2, \mathbb{R})$.

Suppose then that A is not invertible. Any 2×2 matrix row reduces to one of the following:

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

A is not invertible, so it doesn't row reduce to I; it's nonzero, so it doesn't row reduce to the zero matrix.

Suppose A row reduces to $\begin{bmatrix} 1 & * \\ 0 & 0 \end{bmatrix}$. There are elementary matrices $E_1, \ldots, E_k$ such that

$$E_1 \cdots E_k A = \begin{bmatrix} 1 & * \\ 0 & 0 \end{bmatrix}.$$

Since $A \in S$, this equation shows that $\begin{bmatrix} 1 & * \\ 0 & 0 \end{bmatrix} \in S$.

Since S is an ideal,

$$\begin{bmatrix} 1 & * \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & -* \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in S.$$

Again, since S is an ideal,

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \in S.$$

And again, since S is an ideal,

$$\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \in S.$$

Hence,

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in S.$$

Hence, $S = M(2, \mathbb{R})$.

A similar argument shows that if A row reduces to $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, then $S = M(2, \mathbb{R})$.

Therefore, the only ideals in $M(2, \mathbb{R})$ are the zero ideal and the whole ring. □

---

28. Consider the following subset of the ring $\mathbb{Z} \times \mathbb{Z}$:

$$S = \{(m + n, m - n) \mid m, n \in \mathbb{Z}\}.$$

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

The zero element is in S, since $(0, 0) = (0 + 0, 0 - 0) \in S$.

Let $(m + n, m - n) \in S$. Then

$$-(m + n, m - n) = (-m - n, -m + n) = ((-m) + (-n), (-m) - (-n)) \in S.$$

Let $(a + b, a - b), (c + d, c - d) \in S$. Then

$$(a + b, a - b) + (c + d, c - d) = ((a + c) + (b + d), (a + c) - (b + d)) \in S.$$

I have $(5,1) = (3+2, 3-2) \in S$. Then

$$(1,0) \cdot (5,1) = (5,0).$$

But $(5,0) \notin S$. For suppose $(5,0) = (m+n, m-n)$ for $m, n \in \mathbb{Z}$. Then

$$m + n = 5 \quad \text{and} \quad m - n = 0.$$

Adding the two equations gives $2m = 5$, but this equation has no integer solutions.
Thus, S is not an ideal in $\mathbb{Z} \times \mathbb{Z}$. $\square$

---

29. (a) Show that $x^2 + x + 1$ is irreducible in $\mathbb{Z}_5[x]$.

(b) Find $[(2x+3) + \langle x^2 + x + 1\rangle]^{-1}$ in $\dfrac{\mathbb{Z}_5[x]}{\langle x^2 + x + 1\rangle}$.

(c) Compute the product of the cosets $\big((x^2+2) + \langle x^2 + x + 1\rangle\big) \cdot \big((3x+4) + \langle x^2 + x + 1\rangle\big)$ in the quotient ring $\dfrac{\mathbb{Z}_5[x]}{\langle x^2 + x + 1\rangle}$. Write your answer in the form $(ax+b) + \langle x^2 + x + 1\rangle$, where $a, b \in \mathbb{Z}_5$.

(a) Since it's a quadratic, it suffices to show that it has no roots in $\mathbb{Z}_5$.

x	$x^2 + x + 1 \pmod 5$
0	1
1	3
2	2
3	3
4	1

It has no roots in $\mathbb{Z}_5$, so it's irreducible over $\mathbb{Z}_5$. $\square$

(b) In general, you can find an inverse using the Extended Euclidean Algorithm. In this case, the coset representative $2x+3$ is linear, so I can just Apply the Division Algorithm:

$$\begin{aligned}
x^2 + x + 1 &= (3x+1)(2x+3) + 3 \\
(x^2 + x + 1) - (3x+1)(2x+3) &= 3 \\
2(x^2 + x + 1) - 2(3x+1)(2x+3) &= 2 \cdot 3 \\
2(x^2 + x + 1) - (x+2)(2x+3) &= 1 \\
2(x^2 + x + 1) + (4x+3)(2x+3) &= 1 \\
2(x^2 + x + 1) + (4x+3)(2x+3) + \langle x^2 + x + 1\rangle &= 1 + \langle x^2 + x + 1\rangle \\
(4x+3)(2x+3) + \langle x^2 + x + 1\rangle &= 1 + \langle x^2 + x + 1\rangle \\
[(4x+3) + \langle x^2 + x + 1\rangle][(2x+3) + \langle x^2 + x + 1\rangle] &= 1 + \langle x^2 + x + 1\rangle
\end{aligned}$$

Hence,

$$[(2x+3) + \langle x^2 + x + 1\rangle]^{-1} = (4x+3) + \langle x^2 + x + 1\rangle. \quad \square$$

(c) First,

$$\big((x^2+2) + \langle x^2 + x + 1\rangle\big) \cdot \big((3x+4) + \langle x^2 + x + 1\rangle\big) = (x^2+2)(3x+4) + \langle x^2 + x + 1\rangle =$$

$$(3x^3 + 4x^2 + x + 3) + \langle x^2 + x + 1\rangle.$$

Apply the Division Algorithm:

$$3x^3 + 4x^2 + x + 3 = (x^2 + x + 1)(3x + 1) + (2x + 2).$$

Therefore, the product is

$$(3x^3 + 4x^2 + x + 3) + \langle x^2 + x + 1\rangle = (2x + 2) + \langle x^2 + x + 1\rangle. \quad \square$$

---

30. Factor $x^4 + 64$ in $\mathbb{Q}[x]$.

The idea is to add a middle term to complete the square, then subtract it back off:

$$x^4 + 64 = x^4 + 16x^2 + 64 - 16x^2 = (x^2 + 8)^2 - (4x)^2 = (x^2 + 8 + 4x)(x^2 + 8 - 4x) = (x^2 + 4x + 8)(x^2 - 4x + 8).$$

You can check using the Quadratic Formula that $x^2 + 4x + 8$ and $x^2 - 4x + 8$ do not factor over $\mathbb{Q}$. $\square$

---

31. (a) Show that $x^4 + 1$ has no roots in $\mathbb{Z}_5$.

(b) Show that $x^4 + 1$ factors in $\mathbb{Z}_5[x]$.

(a)

x	0	1	2	3	4
$x^4 + 1$	1	2	2	2	2

$\square$

(b) $x^4 + 1 = (x^2 + 2)(x^2 + 3)$. $\square$

---

32. In the ring $\mathbb{R}[x]$, consider the subset

$$\langle x^2 - x - 2, x^2 - 1\rangle = \{a(x)(x^2 - x - 2) + b(x)(x^2 - 1) \mid a(x), b(x) \in \mathbb{R}[x]\}.$$

(a) Show that $\langle x^2 - x - 2, x^2 - 1\rangle$ is an ideal.

(b) Is $x^2 + x + 3$ in $\langle x^2 - x - 2, x^2 - 1\rangle$?

(a) Suppose $a(x)(x^2 - x - 2) + b(x)(x^2 - 1), c(x)(x^2 - x - 2) + d(x)(x^2 - 1) \in \langle x^2 - x - 2, x^2 - 1\rangle$, where $a(x), b(x), c(x), d(x) \in \mathbb{R}[x]$. Then

$$[a(x)(x^2 - x - 2) + b(x)(x^2 - 1)] + [c(x)(x^2 - x - 2) + d(x)(x^2 - 1)] =$$

$$[a(x) + c(x)](x^2 - x - 2) + [b(x) + d(x)](x^2 - 1) \in \langle x^2 - x - 2, x^2 - 1\rangle.$$

I have

$$0 = 0 \cdot (x^2 - x - 2) + 0 \cdot (x^2 - 1) \in \langle x^2 - x - 2, x^2 - 1\rangle.$$

Let $a(x)(x^2 - x - 2) + b(x)(x^2 - 1) \in \langle x^2 - x - 2, x^2 - 1\rangle$. Then

$$-[a(x)(x^2 - x - 2) + b(x)(x^2 - 1)] = (-a(x))(x^2 - x - 2) + (-b(x))(x^2 - 1) \in \langle x^2 - x - 2, x^2 - 1\rangle.$$

Finally, let $f(x) \in \mathbb{R}[x]$ and let $a(x)(x^2 - x - 2) + b(x)(x^2 - 1) \in \langle x^2 - x - 2, x^2 - 1\rangle$. Then

$$f(x)[a(x)(x^2 - x - 2) + b(x)(x^2 - 1)] = [f(x)a(x)](x^2 - x - 2) + [f(x)b(x)](x^2 - 1) \in \langle x^2 - x - 2, x^2 - 1\rangle.$$

(Note that $\mathbb{R}[x]$ is commutative, so I only need to check multiplication on the left.) Hence, $\langle x^2 - x - 2, x^2 - 1\rangle$ is an ideal. $\square$

(b) The greatest common divisor of $x^2 - x - 2 = (x-2)(x+1)$ and $x^2 - 1 = (x-1)(x+1)$ is $x+1$, and it must divide any linear combination $a(x)(x^2 - x - 2) + b(x)(x^2 - 1)$. Suppose then that

$$x^2 + x + 3 = a(x)(x^2 - x - 2) + b(x)(x^2 - 1).$$

Then $x + 1 \mid x^2 + x + 3$. But in fact,

$$x^2 + x + 3 = x(x+1) + 3.$$

Thus, $x + 1 \not| x^2 + x + 3$, and so $x^2 + x + 3$ cannot be an element of $\langle x^2 - x - 2, x^2 - 1\rangle$. $\square$

---

33. $x^2 + 2 = (x+1)(x+2)$ is a factorization of $x^2 + 2$ into irreducibles in $\mathbb{Z}_3[x]$. Find a different factorization of $x^2 + 2$ into irreducibles in $\mathbb{Z}_3[x]$.

Since $2 \cdot 2 = 1$ in $\mathbb{Z}_3$,

$$x^2 + 2 = (x+1)(x+2) = 2(x+1) \cdot 2(x+2) = (2x+2)(2x+1). \quad \square$$

---

34. Compute the product of the cycles (2 4 6 3)(1 3 4) (right to left) and write the result as a product of disjoint cycles.

$$\begin{array}{cccccc}
1 & 2 & 3 & 4 & 5 & 6 \\
\multicolumn{6}{r}{(134)} \\
3 & 2 & 4 & 1 & 5 & 6 \\
\multicolumn{6}{r}{(2463)} \\
2 & 4 & 6 & 1 & 5 & 3
\end{array}$$

The product is (124)(36). $\square$

---

35. Define $\phi : \mathbb{Z}[x] \to \mathbb{Z}[x]$ by

$$\phi(f(x)) = f(x)^2.$$

Determine which of the axioms for a ring map are satisfied by ϕ. If an axiom is not satisfied, give a specific example which shows that the axiom is violated.

First, $\phi(1) = 1^2 = 1$.
If $f(x), g(x) \in \mathbb{Z}[x]$,

$$\phi(f(x)g(x)) = (f(x)g(x))^2 = f(x)^2 g(x)^2 = \phi(f(x))\phi(g(x)).$$

However,

$$\phi(x + x) = \phi(2x) = 4x^2, \quad \text{but} \quad \phi(x) + \phi(x) = x^2 + x^2 = 2x^2.$$

Thus, $\phi(x + x) \neq \phi(x) + \phi(x)$. $\square$

---

36. Define $\phi : \mathbb{Z}_2[x] \to \mathbb{Z}_2[x]$ by

$$\phi(f(x)) = f(x)^2.$$

(a) Show that ϕ is a ring map.

(b) Determine the kernel of ϕ.

(c) Show that $x^4 + 1 \in \operatorname{im} \phi$. Is ϕ surjective?

(a) If $f(x), g(x) \in \mathbb{Z}[x]$,

$$\phi\left(f(x)g(x)\right) = \left(f(x)g(x)\right)^2 = f(x)^2 g(x)^2 = \phi(f(x))\phi(g(x)),$$

$$\phi\left(f(x) + g(x)\right) = \left(f(x) + g(x)\right)^2 = f(x)^2 + 2f(x)g(x) + g(x)^2 = f(x)^2 + g(x)^2 = \phi(f(x)) + \phi(g(x)).$$

$$\phi(1) = 1^2 = 1.$$

Therefore, ϕ is a ring map. □

(b) $\phi(f(x)) = 0$ means $f(x)^2 = 0$, which is only possible if $f(x) = 0$ (since $\mathbb{Z}_2[x]$ is an integral domain). Therefore, $\ker \phi = \{0\}$. □

(c)

$$x^4 + 1 = x^4 + 2x^2 + 1 = (x^2 + 1)^2 = \phi(x^2 + 1).$$

ϕ is not surjective. If $\phi(f(x)) = x$, then $f(x)^2 = x$. This implies $\deg f(x)^2 = \deg x = 1$, or $2 \deg f(x) = 1$. Obviously, $2 \not| 1$. This contradiction shows that x is not in the image of ϕ, and ϕ is not surjective. □

---

37. Find the quotient and the remainder when $2x^4 + 3x^3 + x + 1$ is divided by $3x^2 + 1$ in $\mathbb{Z}_5[x]$.

$$\begin{array}{r|l}
 & 4x^2 + x + 2 \\ \hline
3x^2 + 1 & 2x^4 + 3x^3 + x + 1 \\
 & 2x^4 + 4x^2 \\ \hline
 & \quad 3x^3 + x^2 + x \\
 & \quad 3x^3 \quad\; + x \\ \hline
 & \qquad\quad x^2 + 1 \\
 & \qquad\quad x^2 + 2 \\ \hline
 & \qquad\qquad\quad 4
\end{array}$$

The quotient is $4x^2 + x + 2$ and the remainder is 4. □

---

38. (a) Explain why $x^4 + 1$ has no roots in $\mathbb{R}$.

(b) Is $x^4 + 1$ irreducible in $\mathbb{R}[x]$?

(a) Since $x^4 \geq 0$ for all x, it follows that $x^4 + 1 \geq 1 > 0$. In particular, no real value of x makes it 0. □

(b)

$$x^4 + 1 = (x^4 + 2x^2 + 1) - 2x^2 = (x^2 + 1)^2 - 2x^2 = (x^2 + 1 - \sqrt{2}x)(x^2 + 1 + \sqrt{2}x).$$

Hence, $x^4 + 1$ is not irreducible in $\mathbb{R}[x]$. □

---

39. List the zero divisors and the units in $\mathbb{Z}_2 \times \mathbb{Z}_3$.

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

The zero divisors are $(0,1)$, $(0,2)$, and $(1,0)$.

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

The units are $(1,1)$ and $(1,2)$. □

---

40. Prove that if I is a left ideal in a division ring R, then either $I = \{0\}$ or $I = R$.

Suppose $I \neq \{0\}$. Then I can find a nonzero element $x \in I$. Since R is a division ring, x is invertible. Since I is a left ideal, $x^{-1} \cdot x \in I$. But $x^{-1} \cdot x = 1$, so $1 \in I$. An ideal that contains 1 is the whole ring, so $I = R$. □

---

41. Let R be a ring, and let $r \in R$. The **centralizer** $C(r)$ of r is the set of elements of R which commute with r:

$$C(r) = \{a \in R \mid ra = ar\}.$$

Prove that $C(r)$ is a subring of R.

Let $a, b \in C(r)$, so $ar = ra$ and $br = rb$. Then

$$(a+b)r = ar + br = ra + rb = r(a+b).$$

Therefore, $a + b \in C(r)$.
Since $0 \cdot r = 0 = r \cdot 0$, I have $0 \in C(r)$.
Let $a \in C(r)$, so $ar = ra$. Then

$$(-a)r = -(ar) = -(ra) = r(-a).$$

Hence, $-a \in C(r)$.
Let $a, b \in C(r)$, so $ar = ra$ and $br = rb$. Then

$$(ab)r = a(br) = a(rb) = (ar)b = (ra)b = r(ab).$$

Therefore, $ab \in C(r)$.
Hence, $C(r)$ is a subring. □

---

42. Let

$$I = \left\{ \begin{bmatrix} 0 & x & 0 \\ 0 & y & 0 \\ 0 & z & 0 \end{bmatrix} \;\middle|\; x, y, z \in \mathbb{R} \right\}.$$

Prove that I is a left ideal, but not a right ideal, in the ring $M(3, \mathbb{R})$.

$$\begin{bmatrix} 0 & x & 0 \\ 0 & y & 0 \\ 0 & z & 0 \end{bmatrix} + \begin{bmatrix} 0 & x' & 0 \\ 0 & y' & 0 \\ 0 & z' & 0 \end{bmatrix} = \begin{bmatrix} 0 & x+x' & 0 \\ 0 & y+y' & 0 \\ 0 & z+z' & 0 \end{bmatrix} \in I.$$

Hence, I is closed under sums.

Elements of I are exactly the 3×3 matrices with all-zero first and third columns. Thus,

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \in I.$$

If

$$\begin{bmatrix} 0 & x & 0 \\ 0 & y & 0 \\ 0 & z & 0 \end{bmatrix} \in I, \quad \text{then} \quad -\begin{bmatrix} 0 & x & 0 \\ 0 & y & 0 \\ 0 & z & 0 \end{bmatrix} = \begin{bmatrix} 0 & -x & 0 \\ 0 & -y & 0 \\ 0 & -z & 0 \end{bmatrix} \in I.$$

Thus, I is closed under taking additive inverses.
Let

$$\begin{bmatrix} 0 & x & 0 \\ 0 & y & 0 \\ 0 & z & 0 \end{bmatrix} \in I \quad \text{and} \quad \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \in M(3, \mathbb{R}).$$

Then

$$\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \begin{bmatrix} 0 & x & 0 \\ 0 & y & 0 \\ 0 & z & 0 \end{bmatrix} = \begin{bmatrix} 0 & ax + by + cz & 0 \\ 0 & dx + ey + fz & 0 \\ 0 & gx + hy + iz & 0 \end{bmatrix} \in I.$$

Hence, I is a left ideal.
However,

$$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} \in I \quad \text{and} \quad \begin{bmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix} \in M(3, \mathbb{R}).$$

But

$$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \notin I.$$

Hence, I is not a right ideal. $\square$

---

43. (a) List the elements of U_{42}.

(b) List the elements of the subgroup $\langle 25 \rangle$ in U_{42}.

(c) List the cosets of the subgroup $\langle 25 \rangle$ in U_{42}.

(d) Is the quotient group isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ or $\mathbb{Z}_4$?

(a)

$$U_{42} = \{1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41\}. \quad \square$$

(b)

$$\langle 25 \rangle = \{1, 25, 37\}. \quad \square$$

(c)

$$\begin{aligned} \langle 25 \rangle &= \{1, 25, 37\} \\ 5 \cdot \langle 25 \rangle &= \{5, 41, 17\} \\ 11 \cdot \langle 25 \rangle &= \{11, 23, 29\} \\ 13 \cdot \langle 25 \rangle &= \{13, 31, 19\} \end{aligned} \quad \square$$

(d) Note that

$$5^2 = 25, \quad 11^2 = 37, \quad 13^2 = 1.$$

The results are all elements of the identity coset $\{1, 25, 37\}$.
So all three cosets have order 2.
$\dfrac{U_{42}}{\langle 25\rangle}$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, since every element squares to the identity. $\square$

---

44. Find the primary decomposition and the invariant factor decomposition for $\mathbb{Z}_{24} \times \mathbb{Z}_{28} \times \mathbb{Z}_{21}$.

$$\begin{aligned} \mathbb{Z}_{24} &\approx \mathbb{Z}_3 \times \mathbb{Z}_8 \\ \mathbb{Z}_{28} &\approx \mathbb{Z}_4 \times \mathbb{Z}_7 \\ \mathbb{Z}_{21} &\approx \mathbb{Z}_3 \times \mathbb{Z}_7 \end{aligned}$$

Therefore, the primary decomposition is

$$\mathbb{Z}_4 \times \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_7.$$

Here's the work for the invariant factor decomposition:

$$\begin{array}{cc} 4 & 8 \\ 3 & 3 \\ 7 & 7 \\ \hline 84 & 168 \end{array}$$

The invariant factor decomposition is $\mathbb{Z}_{84} \times \mathbb{Z}_{168}$. $\square$

---

45. What is the largest possible order of an element of $\mathbb{Z}_{30} \times \mathbb{Z}_{45} \times \mathbb{Z}_{60}$?

The primary decomposition is

$$\mathbb{Z}_{30} \times \mathbb{Z}_{45} \times \mathbb{Z}_{60} \approx \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5.$$

Compute the invariant factor decomposition:

$$\begin{array}{ccc} & 2 & 4 \\ 3 & 3 & 9 \\ 5 & 5 & 5 \\ \hline 15 & 30 & 180 \end{array}$$

The invariant factor decomposition is $\mathbb{Z}_{15} \times \mathbb{Z}_{30} \times \mathbb{Z}_{180}$. Hence, the largest possible order of an element is 180. $\square$

---

46. Let $f, g : G \to H$ be group maps. Let

$$E = \left\{ x \in G \,\middle|\, f(x) = g(x) \right\}.$$

Prove that E is a subgroup of G. (E is called the **equalizer** of f and g.)

Let $x, y \in E$, so $f(x) = g(x)$ and $f(y) = g(y)$. Then

$$f(x)f(y) = g(x)g(y), \quad \text{so} \quad f(xy) = g(xy).$$

Therefore, $xy \in E$.
Since $f(1) = 1 = g(1)$, $1 \in E$.

Let $x \in E$, so $f(x) = g(x)$. Then $f(x)^{-1} = g(x)^{-1}$, so $f(x^{-1}) = g(x^{-1})$. Hence, $x^{-1} \in E$. Therefore, E is a subgroup of G. $\square$

---

47. Let R be a ring such that for each $r \in R$, there is a unique element $s \in R$ such that $rsr = r$. Prove that R has no zero divisors.

Suppose that $r \in R$ is a zero divisor, so $r \neq 0$ and $rt = 0$ for some $t \neq 0$. Let s be the unique element of R such that $rsr = r$. Then

$$r(s+t)r = rsr + rtr = r + 0 = r.$$

But $x = s$ was the unique solution to $rxr = r$, so $s = s + t$, and $t = 0$. This contradiction implies that there is no such t, so R has no zero divisors. $\square$

---

48. Suppose $f : R \to S$ is a ring homomorphism and R and S are rings with identity, *but do not assume that* $f(1_R) = 1_S$. Prove that if f is surjective, then $f(1_R) = 1_S$.

Since f is surjective, there is an element $e \in R$ such that $f(e) = 1_S$. Then

$$1_S = f(e) = f(e \cdot 1_R) = f(e) \cdot f(1_R) = 1_S \cdot f(1_R) = f(1_R). \quad \square$$

---

49. Factor $3x^3 + 2x^2 + 3x + 2$ in $\mathbb{Z}_5[x]$.

If a cubic or quadratic polynomial over a field factors, it must have a linear factor, i.e. a root. Therefore, I'll try the elements of $\mathbb{Z}_5$ to find the roots.

x	$3x^3 + 2x^2 + 3x + 2$
0	2
1	0
2	0
3	0
4	4

1, 2, and 3 are roots, so $x - 1 = x + 4$, $x - 2 = x + 3$, and $x - 3 = x + 2$ are factors. Since the leading coefficient is 3, I must have

$$3x^3 + 2x^2 + 3x + 2 = 3(x+4)(x+3)(x+2). \quad \square$$

---

50. Find the remainder when $x^{41} + 3x^{39} + 4x^{11} + 2x^9 + 5x + 3$ is divided by $x + 4$ in $\mathbb{Z}_5[x]$.

Notice that $x + 4 = x - 1$ in $\mathbb{Z}_5[x]$. By the Remainder Theorem, the remainder is

$$1^{41} + 3 \cdot 1^{39} + 4 \cdot 1^{11} + 2 \cdot 1^9 + 5 \cdot 1 + 3 = 3. \quad \square$$

---

51. Calvin Butterball thinks $x^2 + 1 \in \mathbb{Z}_2[x]$ is irreducible, based on the fact that solving $x^2 + 1 = 0$ gives $x = \pm i$, which are complex numbers. Is he right?

In fact, since $2 = 0$ in $\mathbb{Z}_2$,

$$(x+1)^2 = x^2 + 2x + 1 = x^2 + 1.$$

Thus, $x^2 + 1$ is *not* irreducible in $\mathbb{Z}_2[x]$. $\square$

---

52. Find the greatest common divisor of $x^4 + x^3 + x^2 + 2x + 3$ and $x^3 + 4x^2 + 2x + 3$ in $\mathbb{Z}_5[x]$ and express the greatest common divisor as a linear combination (with coefficients in $\mathbb{Z}_5[x]$) of the two polynomials.

a	q	y
$x^4 + x^3 + x^2 + 2x + 3$		$x + 2$
$x^3 + 4x^2 + 2x + 3$	$x + 2$	1
$x^2 + 2$	$x + 4$	0

The greatest common divisor is $x + 2$, and

$$1 \cdot (x^4 + x^3 + x^2 + 2x + 3) - (x+2)(x^3 + 4x^2 + 2x + 3) = x + 2. \quad \square$$

---

53. The following set is an ideal in the ring $\mathbb{Z}_2 \times \mathbb{Z}_8$:

$$I = \{(0,0), (0,4), (1,0), (1,4)\}.$$

(a) List the cosets of I in $\mathbb{Z}_2 \times \mathbb{Z}_8$.

(b) Construct addition and multiplication tables for the quotient ring $\dfrac{\mathbb{Z}_2 \times \mathbb{Z}_8}{I}$.

(c) Is $\dfrac{\mathbb{Z}_2 \times \mathbb{Z}_8}{I}$ an integral domain?

(a)

$$\begin{aligned} I &= \{(0,0), (0,4), (1,0), (1,4)\} \\ (0,1) + I &= \{(0,1), (0,5), (1,1), (1,5)\} \\ (0,2) + I &= \{(0,2), (0,6), (1,2), (1,6)\} \\ (0,3) + I &= \{(0,3), (0,7), (1,3), (1,7)\} \end{aligned} \quad \square$$

(b) I will let $(0,0)$, $(0,1)$, $(0,2)$, and $(0,3)$ stand for their respective cosets.

$+$	$(0,0)$	$(0,1)$	$(0,2)$	$(0,3)$
$(0,0)$	$(0,0)$	$(0,1)$	$(0,2)$	$(0,3)$
$(0,1)$	$(0,1)$	$(0,2)$	$(0,3)$	$(0,0)$
$(0,2)$	$(0,2)$	$(0,3)$	$(0,0)$	$(0,1)$
$(0,3)$	$(0,3)$	$(0,0)$	$(0,1)$	$(0,2)$

$\cdot$	$(0,0)$	$(0,1)$	$(0,2)$	$(0,3)$
$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$
$(0,1)$	$(0,0)$	$(0,1)$	$(0,2)$	$(0,3)$
$(0,2)$	$(0,0)$	$(0,2)$	$(0,0)$	$(0,2)$
$(0,3)$	$(0,0)$	$(0,3)$	$(0,2)$	$(0,1)$

$\square$

(c) Since $((0,2)+I)((0,2)+I) = I$ (which is the zero element in $\dfrac{\mathbb{Z}_2 \times \mathbb{Z}_8}{I}$), the quotient ring $\dfrac{\mathbb{Z}_2 \times \mathbb{Z}_8}{I}$ is not an integral domain. $\square$

The best thing for being sad is to learn something. - Merlyn, in T. H. White's *The Once and Future King*