Chapter 3 Homework

Homework #3.1 - Math 676

Maddie Kuehn

Section 3.1 - Fields of Complex Numbers.

- Choose 4 exercises.

2. Let $\mathbb{F}$ be a field and let a be an element of $\mathbb{F}$ different from 0. Prove that there exists a unique element b of $\mathbb{F}$ such that $a \cdot b = 1$.

Pf: Assume there are two elements of $\mathbb{F}$ that are the inverse of a, b_1 and b_2. So, this means that $a \cdot b_1 = 1$ and $a \cdot b_2 = 1$. I want to show that $b_1 = b_2$.

Since both equal 1,

$$\begin{aligned} b_1 &= b_1 \cdot 1 && \text{(unity element)} \\ &= b_1 \cdot (a \cdot b_2) && \text{(hypothesis)} \\ &= (b_1 \cdot a) \cdot b_2 && \text{(associativity)} \\ &= 1 \cdot b_2 && \text{(hypothesis)} \\ &= b_2 && \text{(unity element)} \end{aligned}$$

Thus, we have shown that $b_1 = b_2$. ∎

3. Let $\mathbb{F}$ be a field. Prove that for every element $a \in \mathbb{F}$, we have $0 \cdot a = 0$.

Pf: Let $a \in \mathbb{F}$.

$$\begin{aligned} 0 \cdot a &= 0 \cdot a + 0 && \text{(zero element)} \\ &= 0 \cdot a + a + -a && \text{(opposite)} \\ &= 0 \cdot a + 1 \cdot a + -a && \text{(unity element)} \\ &= a \cdot (0 + 1) + -a && \text{(distributive property)} \\ &= a \cdot 1 + -a && \text{(zero element)} \\ &= a + -a && \text{(unity element)} \\ &= 0 && \text{(opposite)} \end{aligned}$$

Thus, we have shown that $0 \cdot a = 0$. ∎

---

7. Let p be any rational number. Explain how to get p by using 1 and basic field operations.

Hint. You may want to review Remark 3.1.14.

Since p is a rational number, we know we can write it in the form $p = \frac{a}{b}$, where $b \neq 0$.

We can find b by adding together 1 b times. Then, we can find the inverse (reciprocal) of that value. We can then add $\frac{1}{b}$ together a times. This would give all positive rational numbers.

If p was negative, we would repeat the same process, but then at the end, we would find the opposite of $\frac{a}{b}$, since $\frac{a}{b} + -\frac{a}{b} = 0$.

8. Show that $\mathbb{Q}(\sqrt{2})$ is equal to the set

$$M := \{p + q\sqrt{2} \mid p, q \in \mathbb{Q}\}.$$

Pf: $M \subseteq \mathbb{Q}(\sqrt{2})$: Show Any element of M can be obtained from $\sqrt{2}$ by using a finite sequence of field operations.

Pf: Let α be an element of M, s.t. $\alpha = p + q\sqrt{2}$, where $p, q \in \mathbb{Q}$

We know that we can obtain p, q from $1 = \frac{\sqrt{2}}{\sqrt{2}}$, so we can find α from $\sqrt{2}$.

$\mathbb{Q}(\sqrt{2}) \subseteq M$: We know that $\sqrt{2} \in M$, because $\sqrt{2} = 0 + 1 \cdot \sqrt{2}$

- 1 is in M, because $1 = 1 + 0 \cdot \sqrt{2}$.
- Let $\alpha = p + q\sqrt{2}$ and $\beta = r + s\sqrt{2}$, s.t. $p, q, r, s \in \mathbb{Q}$.
  - ↳ We know that $\alpha + \beta = (p+r) + (q+s)\sqrt{2}$. We know that $\alpha + \beta \in M$, since $p+r \in \mathbb{Q}$ and $q+s \in \mathbb{Q}$
  - ↳ We know that $\alpha \cdot \beta = (p + q\sqrt{2}) \cdot (r + s\sqrt{2}) = pr + ps\sqrt{2} + qr\sqrt{2} + 2qs$
    $= (pr + 2qs) + (ps + qr)\sqrt{2}$
    We know this must be an element of M because $pr + 2qs \in \mathbb{Q}$ and $(ps + qr) \in \mathbb{Q}$.
- Let $\alpha = p + q\sqrt{2}$. We know that $-\alpha = (-p) + (-q)\sqrt{2}$, and $-p, -q \in \mathbb{Q}$, So $-\alpha \in M$.
- Let $\alpha = p + q\sqrt{2}$ s.t. $\alpha \neq 0$.
  find $\alpha^{-1} = \beta$.
  ↳ $\beta = \frac{p}{p^2 - 2q^2} + \frac{-q}{p^2 - 2q^2}\sqrt{2}$.

$\beta = \frac{1}{p+q\sqrt{2}} \frac{(p-q\sqrt{2})}{(p-q\sqrt{2})} = \frac{p - q\sqrt{2}}{p^2 - 2q^2}$

If $1 = 0$: $p^2 = 2q^2$, $\frac{p^2}{q^2} = 2$, $\frac{p}{q} = \sqrt{2}$, $\sqrt{2} \in \mathbb{Q}$ False!

We know that $\beta \in M$, because $p^2, 2q^2 \in \mathbb{Q}$ and $p^2 - 2q^2 \neq 0$.

So, $\mathbb{Q}\sqrt{2}$ is equal to M. ∎

Homework #3.2 - Math 676

Section 3.2 - Introduction to Rings. You can ignore Integral Domains and Characteristic.

- Choose 4 exercises.

2. Write the addition and multiplication tables for $\mathbb{Z}_6$.

$\mathbb{Z}_6$:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

---

3. Evaluate the following operation in $\mathbb{Z}_5[x]$:

$(2x+4)\cdot(3x+2) =$

$(2x+4)\cdot(3x+2) = 6x^2+4x+12x+8 = 6x^2+16x+8 \equiv 1x^2+1x+3 \bmod 5$

---

4. Prove that $\mathbb{Z}_5$ is a field.

Hint: it may be helpful to write the multiplication table for $\mathbb{Z}_5$.

- A commutative ring with unity $(R,+,\cdot)$ is called a *field* if for every element $a \in R$ different from 0, there exists another element $b \in R$ such that $a \cdot b = 1$. The element b is written a^{-1} and it is called the *reciprocal* of a.

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

We know that $\mathbb{Z}_5$ is a commutative ring with unity, so we need to show that for every non-zero element of $\mathbb{Z}_5$, there is another element of $\mathbb{Z}_5$ s.t $a \cdot b = 1$.

Since each element of $\mathbb{Z}_5$ where $a \neq 0$, exists an element where $a \cdot b = 1$, $\mathbb{Z}_5$ is a field.

6. Let R be a ring, then $a(b-c) = ab - ac$ and $(b-c)a = ba - ca$ for all elements a, b, and c of R.

- Show $a(b-c) = ab - ac$

$$\begin{aligned} a(b-c) &= a(b+(-c)) && \text{(inverse of } c \text{ because } R \text{ is abelian)} \\ &= ab + a(-c) && \text{(distributive property of addition w/ Rings)} \\ &= ab + -(ac) && \text{(Thm 3.2.10 (b))} \\ &= ab - ac \end{aligned}$$

- Show $(b-c)a = ba - bc$

$$\begin{aligned} (b-c)a &= (b+(-c))a && \text{(inverse of } c \text{ because } R \text{ is abelian)} \\ &= ba + (-c)a && \text{(distributive property of addition w/ Rings)} \\ &= ba + -(ca) && \text{(Thm 3.2.10 (b))} \\ &= ba - ca \end{aligned}$$

Homework #3.3 - Math 676

Mabie Kuehn

Section 3.3 - Polynomial Rings in One Variable.

- Choose 9 exercises.
- Choose 3 among the following exercises:
  - Find the statement of the Division Algorithm in your College Algebra textbook and point out any difference. Summarize any proof or explanation of this theorem in your textbook. Alternatively, you can discuss any example.
  - Find where your College Algebra textbook introduces monic polynomials and describe an example given in the textbook.
  - Find in your College Algebra textbook the definition of greatest common divisor for polynomials and comment on any difference with the definition given in the notes.
  - Provide an example from your College Algebra textbook where the Unique Factorization Theorem is applied either explicitly or implicitly
  - Provide an example from your College Algebra textbook where simplification of polynomials is applied either explicitly or implicitly.

2. Perform the following computations in $\mathbb{Z}_3[i][x]$:

(a) $(ix+2)^2$,

$$(ix+2)^2 = (ix)^2 + 2(ix)(2) + 2^2$$
$$= i^2x^2 + 4ix + 4$$
$$= 2x^2 + 4ix + 4 \equiv 2x^2 + ix + 1 \mod 3$$

(b) $[(1+2i)x+i]\cdot[(2+2i)x+2i]$.

$(1+2i)x\cdot(2+2i)x = (2+2i+4i+4i^2)x^2 \Rightarrow (2+6i+4i^2) = (2+6i+4(-1)) = 2+6i-4 = -2+6i \equiv 1+0i \mod 3 = 1$

$(1+2i)x\cdot 2i = (2i+4i^2)x \Rightarrow 2i+4(-1) = 2i-4 \equiv 2i+2 \mod 3$

$i\cdot(2+2i)x = (2i+2i^2)x \Rightarrow 2i+2(-1) = 2i-2 \equiv 2i+1 \mod 3$

$i\cdot 2i = 2i^2 = 2(-1) = -2 \equiv 1 \mod 3$

$\hookrightarrow 1x^2 + (2i+2)x + (2i+1)x + 1 = x^2 + (4i+3)x + 1 \equiv x^2 + (1i+0)x + 1 \mod 3$

$= x^2 + ix + 1 \mod 3$

3. Evaluate the following operations in $\mathbb{Q}(i)[x]$:

(a) $(ix^3 - 2x^2 + (8+3i)x - 1) + (3x^3 + ix^2 + (1-3i)x + 1) =$

$(3+i)x^3 + (-2+i)x^2 + 9x$

(b) $(ix + 3 + 2i) \cdot (x - i) =$

$= ix^2 - i^2x + 3x - 3i + 2ix - 2i^2$
$= ix^2 - (-1)x + 3x - 3i + 2ix - 2(-1)$
$= ix^2 + x + 3x - 3i + 2ix + 2$
$= ix^2 + (4+2i)x + (2-3i)$

4. Determine a divisor of $P(x) = x^3 + 3x^2 - 2x - 6$ in $\mathbb{Q}(\sqrt{2})[x]$ which is not a divisor in $\mathbb{Q}(i)[x]$.

$P(x) = (x^3 + 3x^2)(2x - 6)$
$= x^2(x+3) - 2(x+3)$
$= (x+3)(x^2-2)$

Because we are factoring in $\mathbb{Q}(\sqrt{2})[x]$,
$= (x+3)(x-\sqrt{2})(x+\sqrt{2})$

Because $\sqrt{2} \notin \mathbb{Q}$, $\sqrt{2} \notin \mathbb{Q}(i)$, so $(x-\sqrt{2}) \notin \mathbb{Q}(i)[x]$

So, in particular, $(x-\sqrt{2})$ is a factor of $P(x)$ in $\mathbb{Q}(\sqrt{2})[x]$ but not $\mathbb{Q}(i)[x]$.

7. For each of the following polynomials over the given integral domain, either say that they are irreducible or show a suitable factorization to prove that they are reducible.

(a) $5x^2 + 10x - 25$ over $\mathbb{Z}$

$5(x^2 + 2x - 5)$ ← Positive degree
Not a unit
↳ Since 5 is not a unit, $P(x)$ is Reducible.

(b) $5x^2 + 10x - 25$ over $\mathbb{Q}$

$5(x^2 + 2x - 5)$ → Since $(-1 \pm \sqrt{6})$ is not a solution in $\mathbb{Q}$, $P(x)$ is irreducible.
unit

$\frac{-2 \pm \sqrt{4-4(-5)}}{2} = \frac{-2 \pm \sqrt{24}}{2} = \frac{-2 \pm 2\sqrt{6}}{2} = -1 \pm \sqrt{6}$
↳ not in $\mathbb{Q}$

$x = -1 + \sqrt{6}$ $\quad x = -1 - \sqrt{6}$
$x + 1 - \sqrt{6}$ $\quad x + 1 + \sqrt{6}$

Theorem 3.3.60. Reducibility Test for Degree 2 and 3 Let $\mathbb{K}$ be a field. If $P(x)$ is a polynomial in $\mathbb{K}[x]$ and the degree of $P(x)$ is either 2 or 3, then $P(x)$ is reducible in $\mathbb{K}[x]$ if and only if $P(x)$ has a zero in $\mathbb{K}$.

(c) $5x^2 + 10x - 25$ over $\mathbb{R}$

$5(x^2+2x-5) = \underbrace{5}_{\text{unit}}(x+1-\sqrt{6})(x+1+\sqrt{6}) \rightarrow$ Reducible.

$-1 \pm \sqrt{6} \in \mathbb{R}$, so

(d) $3x^2 + 6$ over $\mathbb{C}$

$x^2+2=0$
$x^2=-2$
$x=\pm i\sqrt{2}$

$3(x^2+2) = 3(x+i\sqrt{2})(x-i\sqrt{2}) \rightarrow$ Reducible

(e) $x^2 + x + 1$ over $\mathbb{R}$

$x = \frac{-1 \pm \sqrt{1^2-4(1)(1)}}{2} = \frac{-1 \pm \sqrt{-3}}{2} \notin \mathbb{R}$,

Irreducible!

(f) $x^2 + x + 1$ over $\mathbb{C}$

$x = \frac{-1 \pm i\sqrt{3}}{2} = -\frac{1}{2} \pm \frac{\sqrt{3}}{2} i$

$x^2+x+1 = (x+\frac{1}{2}-\frac{\sqrt{3}}{2}i)(x+\frac{1}{2}+\frac{\sqrt{3}}{2}i) \rightarrow$ Reducible!

(g) $x^2 + x + 1$ over $\mathbb{Z}_2$

$0 \rightarrow 0^2+0+1 = 1 \neq 0$
$1 \rightarrow 1^2+1+1 = 3 \equiv 1 \bmod 2 \neq 0$

Irreducible!

(h) $x^2 + x + 1$ over $\mathbb{Z}_3$

$0 \rightarrow 0^2+0+1 = 1 \neq 0$
$1 \rightarrow 1^2+1+1 = 3 \equiv 0 \bmod 3$ ← Reducible

$(x-1)$ is a factor $(x-1) \equiv (x+2) \bmod 3$

	1	1	1
1	↓	1	2
	1	2	$3 \equiv 0 \bmod 3$
	↳ $(x+2)$		

So, $x^2+x+1 = (x+2)(x+2) = (x+2)^2$

$(x+2)(x+2) = x^2+4x+4 \equiv x^2+x+1 \bmod 3$ ✓

8. Prove that the polynomial $x^2 - 5$ is irreducible in $\mathbb{Q}[x]$.

Theorem 3.3.60. Reducibility Test for Degree 2 and 3 Let $\mathbb{K}$ be a field. If $P(x)$ is a polynomial in $\mathbb{K}[x]$ and the degree of $P(x)$ is either 2 or 3, then $P(x)$ is reducible in $\mathbb{K}[x]$ if and only if $P(x)$ has a zero in $\mathbb{K}$.

Pf: We know that $\deg(x^2-5) = 2$. If we show that x^2-5 has no roots in $\mathbb{Q}$, it is irreducible.

Let $x^2-5=0$

$x^2 = 5$

$x = \pm\sqrt{5}$ → since $\pm\sqrt{5} \notin \mathbb{Q}$, there are no roots in $\mathbb{Q}$.

Thus, x^2-5 is irreducible in $\mathbb{Q}[x]$. ■

---

10. Apply the division algorithm to determine the quotient $Q(x)$ and the remainder $R(x)$ upon dividing the polynomial $P(x) = x^2 + x + 2$ by $D(x) = 2x + 1$.

$$\begin{array}{r} \frac{1}{2}x + \frac{1}{4} \\ 2x+1 \overline{)\, x^2 + x + 2} \\ -(x^2 + \frac{1}{2}x) \\ \hline \frac{1}{2}x + 2 \\ -(\frac{1}{2}x + \frac{1}{4}) \\ \hline 0 + \frac{7}{4} \end{array} \quad \text{Deg } R < \text{Deg } D$$

$Q(x) = \frac{1}{2}x + \frac{1}{4}$

$R(x) = \frac{7}{4}$

---

11. Apply the division algorithm to evaluate the following division with remainder:

$$(x^3 + \sqrt{2}x^2 + i) \div (x^2 + 2\sqrt{3}).$$

$$\begin{array}{r} x + \sqrt{2} \\ x^2+2\sqrt{3} \overline{)\, x^3 + \sqrt{2}x^2 + i} \\ -(x^3 + 2\sqrt{3}x) \\ \hline +\sqrt{2}x^2 - 2\sqrt{3}x + i \\ -(+\sqrt{2}x^2 + 2\sqrt{6}) \\ \hline -2\sqrt{3}x + i - 2\sqrt{6} \end{array} \quad \text{Deg } R < \text{Deg } D$$

$$x^3 + \sqrt{2}x^2 + i = \underbrace{(x^2+2\sqrt{3})(x+\sqrt{2})}_{Q(x)} + \underbrace{(-2\sqrt{3}x + i - 2\sqrt{6})}_{R(x)}$$

15. Determine two polynomials $A(x)$ and $B(x)$ such that

$$A(x)(x^2-9)+B(x)(x-2)=1.$$

$P(x)=x^2-9 \qquad Q(x)=(x-2) \qquad D(x)=1$

$P(x)=Q(x)\cdot D(x)+R(x) \Rightarrow$

$$\begin{array}{r|l} x^2-9 & x-2 \\ -(x^2-2x) & x+2 \\ \hline 2x-9 & \\ -(2x-4) & \\ \hline -5 \leftarrow R & \end{array}$$

$x^2-9=(x-2)(x+2)-5$

$(x^2-9)-(x-2)(x+2)=-5$

$-5 \qquad\qquad -5$

$-\frac{1}{5}(x^2-9)+\frac{(x+2)}{5}(x-2)=1$

So $A(x)=-\frac{1}{5}$

$B(x)=\frac{1}{5}(x+2)$

---

16. Determine two polynomials $A(x)$ and $B(x)$ such that

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

$$\begin{array}{r|l} x^2+1 & x+1 \\ -(x^2+x) & x-1 \\ \hline -x+1 & \\ -(-x-1) & \\ \hline 2 & \end{array}$$

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

$\frac{(x^2+1)-(x-1)(x+1)}{2}=\frac{2}{2}$

$\frac{1}{2}(x^2+1)+-\frac{1}{2}(x-1)(x+1)=1$

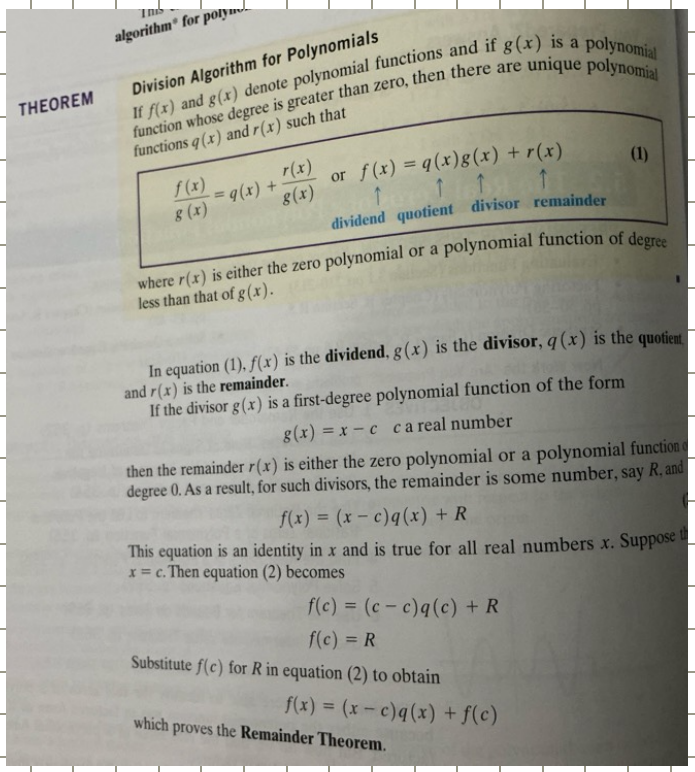
So, $A(x)=\frac{1}{2}$

$B(x)=-\frac{1}{2}(x-1)$

- Find the statement of the Division Algorithm in your College Algebra textbook and point out any difference. Summarize any proof or explanation of this theorem in your textbook. Alternatively, you can discuss any example.

Theorem 3.3.25. Division Algorithm Let $\mathbb{K}$ be a field. Given $P(x)$ and $D(x)$ in $\mathbb{K}[x]$ with $D(x) \neq 0$, there exist unique $Q(x)$ and $R(x)$ in $\mathbb{K}[x]$ such that

- $P(x) = D(x) \cdot Q(x) + R(x)$;
- $R(x) = 0$ or $\deg(R(x)) < \deg(D(x))$.



algorithm* for polyn...

THEOREM

Division Algorithm for Polynomials

If $f(x)$ and $g(x)$ denote polynomial functions and if $g(x)$ is a polynomial function whose degree is greater than zero, then there are unique polynomial functions $q(x)$ and $r(x)$ such that

$$\frac{f(x)}{g(x)} = q(x) + \frac{r(x)}{g(x)} \quad \text{or} \quad f(x) = q(x)g(x) + r(x) \qquad (1)$$

dividend quotient divisor remainder

where $r(x)$ is either the zero polynomial or a polynomial function of degree less than that of $g(x)$.

In equation (1), $f(x)$ is the **dividend**, $g(x)$ is the **divisor**, $q(x)$ is the **quotient** and $r(x)$ is the **remainder**.

If the divisor $g(x)$ is a first-degree polynomial function of the form

$$g(x) = x - c \quad c \text{ a real number}$$

then the remainder $r(x)$ is either the zero polynomial or a polynomial function of degree 0. As a result, for such divisors, the remainder is some number, say R, and

$$f(x) = (x - c)q(x) + R$$

This equation is an identity in x and is true for all real numbers x. Suppose $x = c$. Then equation (2) becomes

$$f(c) = (c - c)q(c) + R$$

$$f(c) = R$$

Substitute $f(c)$ for R in equation (2) to obtain

$$f(x) = (x - c)q(x) + f(c)$$

which proves the **Remainder Theorem**.

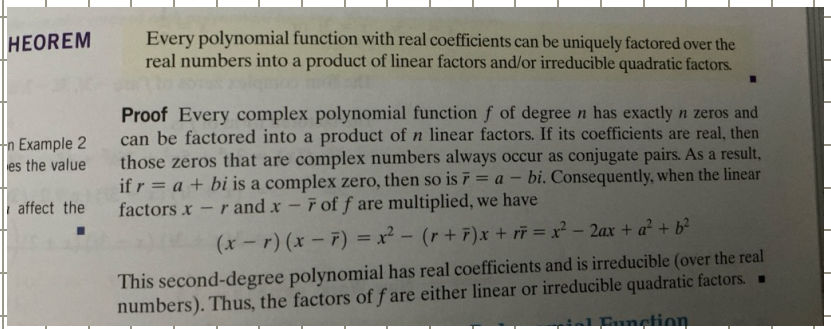
First, the Col. Algebra textbook gives the Thm without proof.

Additionally this textbook only talks about the division algorithm for polynomials in $\mathbb{Z}[x]$.

In this specific area of the textbook, it already assumes that students know how to divide polynomials and does not give any examples. In fact, it is only using the division algorithm to describe the Remainder Theorem for dividing by $(x-c)$.

- Provide an example from your College Algebra textbook where the Unique Factorization Theorem is applied either explicitly or implicitly

Unique Factorization Comes into play when the book is discussing finding the complex zeros. Immediately before this part, there is a thm where the book states that:



THEOREM

Every polynomial function with real coefficients can be uniquely factored over the real numbers into a product of linear factors and/or irreducible quadratic factors.

n Example 2
es the value
affect the

Proof Every complex polynomial function f of degree n has exactly n zeros and can be factored into a product of n linear factors. If its coefficients are real, then those zeros that are complex numbers always occur as conjugate pairs. As a result, if $r = a + bi$ is a complex zero, then so is $\bar{r} = a - bi$. Consequently, when the linear factors $x - r$ and $x - \bar{r}$ of f are multiplied, we have

$$(x - r)(x - \bar{r}) = x^2 - (r + \bar{r})x + r\bar{r} = x^2 - 2ax + a^2 + b^2$$

This second-degree polynomial has real coefficients and is irreducible (over the real numbers). Thus, the factors of f are either linear or irreducible quadratic factors.

The example then gives the equation $3x^4+5x^3+25x^2+45x-18$ and describes how to factor, using sythetic division, rational root thrm, and factoring, mentioning the quadratic that can only be factored by complex numbers.

- Provide an example from your College Algebra textbook where simplification of polynomials is applied either explicitly or implicitly.

In an example on finding Real zeros of a polynomial function, the textbook discusses how to find the zeros of $2x^3+11x^2-7x-6$. this example explicitly talks about how solving the depressed equation after dividing the 1st time to find additional zeros.

encouraged to verify the results shown.) After dividing f by $x + 6$, the quotient is $2x^2 - x - 1$, so

$$f(x) = 2x^3 + 11x^2 - 7x - 6$$
$$= (x + 6)(2x^2 - x - 1)$$

Now any solution of the equation $2x^2 - x - 1 = 0$ will be a zero of f. Because of this, the equation $2x^2 - x - 1 = 0$ is called a **depressed equation** of f. Because any solution to the equation $2x^2 - x - 1 = 0$ is a zero of f, work with the depressed equation to find the remaining zeros of f.

The depressed equation $2x^2 - x - 1 = 0$ is a quadratic equation with discriminant $b^2 - 4ac = (-1)^2 - 4(2)(-1) = 9 > 0$. The equation has two real solutions, which can be found by factoring.

$$2x^2 - x - 1 = (2x + 1)(x - 1) = 0$$
$$2x + 1 = 0 \quad \text{or} \quad x - 1 = 0$$
$$x = -\frac{1}{2} \quad \text{or} \quad x = 1$$

The zeros of f are -6, $-\frac{1}{2}$, and 1.

Factor f completely as follows:

$$f(x) = 2x^3 + 11x^2 - 7x - 6 = (x + 6)(2x^2 - x - 1) = (x + 6)(2x + 1)(x - 1)$$

Homework #3.4 - Math 676

Mabie Kuehn

Section 3.4 - Ideals. You can ignore the reference to Zorn's Lemma.

- Choose 4 exercises.

4. Consider the ring $\mathbb{Z}$. Determine the intersection between $2\mathbb{Z}$ and $3\mathbb{Z}$.

$2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4, 6, \ldots\}$
$3\mathbb{Z} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$

$2\mathbb{Z} \cap 3\mathbb{Z} = \{\ldots, -12, -6, 0, 6, 12, \ldots\} = 6\mathbb{Z}$

---

5. Consider the ring $\mathbb{Z}$. Determine the intersection between $4\mathbb{Z}$ and $6\mathbb{Z}$.

$4\mathbb{Z} = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$
$6\mathbb{Z} = \{\ldots, -12, -6, 0, 6, 12, \ldots\}$

$4\mathbb{Z} \cap 6\mathbb{Z} = \{\ldots, -24, -12, 0, 12, 24, \ldots\} = 12\mathbb{Z}$

---

8. Determine the ideal $(6, 8)$ in $\mathbb{Z}$. In other words, determine the ideal generated by 6 and 8 in $\mathbb{Z}$. You also need to prove your answer.

$(6,8) = \{6a + 8b \mid a, b \in \mathbb{Z}\} = 2\mathbb{Z} = (2)$

$6a + 8b = 2(\underbrace{3a + 4b}_{\in \mathbb{Z}})$

So, $(6,8) = (2)$

$\Rightarrow (6,8) \subseteq (2)$

Let $x = 6a + 8b$ s.t. $a, b \in \mathbb{Z}$ and $x \in (6,8)$.
since $x = 2(3a + 4b)$, and $3a + 4b \in \mathbb{Z}$, $x \in (2)$.

$\Leftarrow (2) \subseteq (6,8)$

(show $(2) = \{2k \mid k \in \mathbb{Z}\} \in (6,8)$
$2k \in (6,8)$)

- Let $a = -1$ and $b = 1$.
$2 = 6a + 8b = 6(-1) + 8(1) = -6 + 8 = 2$. Thus $2 \in (6,8)$.

Since $k \in \mathbb{Z}$ and $2 \in (6,8)$, then $2k \in (6,8)$ and $k \cdot 2 \in (6,8)$.
Thus, $(2) \subseteq (6,8)$.

15. Determine wether each of the following ideals of $\mathbb{Z}$ is prime and justify your answers.

(a) (3)

(b) (6)

(c) (25)

a) (3) = prime.

We know that $(3) = \{3a \mid a \in \mathbb{Z}\}$, since Every element in (3) is divisible by 3, then $3 \in (3)$.

b) $(6) \rightarrow$ not prime.

Let $a=2$ and $b=3$

$a, b \in \mathbb{Z}$, and $a \cdot b = 6 \in (6)$, but $2 \notin (6)$ and $3 \notin (6)$.

c) $(25) \rightarrow$ not prime

Let $a, b = 5$

$a, b \in \mathbb{Z}$ and $a \cdot b = 25 \in (25)$, but $5 \notin (25)$.

Homework #3.5 - Math 676

Section 3.5 - Quotient Rings. You can ignore Theorem 3.5.9, Corollary 3.5.10, and Example 3.5.11.

- Choose 4 exercises.

2. Determine the inverse element of (the class of) x^2+x+1 in the quotient ring $\mathbb{Q}[x]/((x^2-7))$. Justify your answer.

First, $P(x) = (x^2-7)$ is irreducible in $\mathbb{Q}$.

$x^2 = 7$

So, we need to rationalize $\frac{1}{x^2+x+1} = \frac{1}{7+x+1} = \frac{1}{x+8}$

$\frac{1}{(x+8)} \cdot \frac{(x-8)}{(x-8)} = \frac{x-8}{x^2-64} = \frac{x-8}{7-64} = \frac{x-8}{-57} = \frac{8-x}{57}$

---

4. Prove that the quotient ring $\mathbb{R}[x]/((x^2+1))$ is a field. What field does it remind you? We will be able to formalize this idea of fields that look the same with the concept of isomorphism.

Pf: We know that $\mathbb{R}$ is a field, and $((x^2+1))$ is an ideal of $\mathbb{R}[x]$. Because (x^2+1) is irreducible in $\mathbb{R}[x]$, $((x^2+1))$ is maximal. Because it is maximal, thus $\mathbb{R}[x]/((x^2+1))$ is a field by Thm 3.5.7.

Lemma 3.4.21. Let $\mathbb{K}$ be a field, then an ideal $I = (P(x))$ of $\mathbb{K}[x]$ is maximal if and only if $P(x)$ is irreducible in $\mathbb{K}[x]$.

Theorem 3.5.7. Let R be a commutative ring with unity and let M an ideal in R. Then the quotient ring R/M is a field if and only if the ideal M is maximal.

$x^2+1=0 \Rightarrow x^2=-1$ → which reminds me of $i^2=-1$, so it reminds me of $\mathbb{C}[x]$.

---

5. Prove that the quotient ring $\mathbb{Z}_2[x]/(x^3+x+1)$ is a field. How many elements does it have?

To prove that $\mathbb{Z}_2[x]/(x^3+x+1)$, show (x^3+x+1) is irreducible.

Theorem 3.3.60. Reducibility Test for Degree 2 and 3 Let $\mathbb{K}$ be a field. If $P(x)$ is a polynomial in $\mathbb{K}[x]$ and the degree of $P(x)$ is either 2 or 3, then $P(x)$ is reducible in $\mathbb{K}[x]$ if and only if $P(x)$ has a zero in $\mathbb{K}$.

$0 \to 0^3+0+1 = 1 \neq 0$

$1 \to 1^3+1+1 = 3 \equiv 1 \bmod 2 \neq 0$

So, since there are no zeros, x^3+x+1 is irreducible. Thus, by Thm 3.5.7 and Lemma 3.4.21, $\mathbb{Z}_2[x]/(x^3+x+1)$ is a field. ■

↳ all Remainders are degree 2 or less w/ all coefficients 0 or 1

$\{ax^2+bx+c \mid a,b,c \in \mathbb{Z}_2\}$ so 2 options each for a,b,c. $2 \cdot 2 \cdot 2 = 8$ elements.

6. Determine a field with 9 elements.

A field with 9 elements is $\mathbb{Z}_3[i]$, as demonstrated by Example 3.2.4.

Additionally, we know $\mathbb{Z}_3[x]$ is not a field, but we can make it a field by finding a maximum ideal, that is irreducible.

$\mathbb{Z}_3[x]/(x^2+1)$

↳ x^2+1 is irreducible!

- $0 \to 0+1 = 1 \neq 0$
- $1 \to 1+1 = 2 \neq 0$
- $2 \to 4+1 \equiv 2 \bmod 3 \neq 0$

↳ All Remainders are degree 1 or less (smaller than 2) w/ all coefficients $0, 1, 2 \to$

$r(x) = ax+b \to$ 3 options each for a & b

$3 \cdot 3 = 9$

Homework #3.6 - Math 676

Section 3.6 - Reducibility Polynomials in Z[x].

- Do all 3 exercises.

1. Prove that the polynomial $11x^3 - 4x^2 + 8x + 21$ is irreducible in $\mathbb{Q}[x]$.

Consider the reduction mod 5:

$$11x^3 - 4x^2 + 8x + 21 = x^3 + x^2 + 3x + 1$$

Both degrees are equal to 3. Using the reducibility test for polynomials of degree 3, show 0,1,2,3,4 are not zeros in $\mathbb{Z}_5[x]$.

$0 \to 0^3 + 0^2 + 3(0) + 1 = 1$
$1 \to 1^3 + 1^2 + 3(1) + 1 = 1+1+3+1 = 6 \equiv 1 \bmod 5$
$2 \to 2^3 + 2^2 + 3(2) + 1 = 8+4+6+1 = 19 \equiv 4 \bmod 5$
$3 \to 3^3 + 3^2 + 3(3) + 1 = 27+9+9+1 = 46 \equiv 1 \bmod 5$
$4 \to 4^3 + 4^2 + 3(4) + 1 = 64+16+12+1 = 93 \equiv 3 \bmod 5$

So, since $x^3 + x^2 + 3x + 1$ is irreducible mod 5, thus $11x^3 - 4x^2 + 8x + 21$ is irreducible in $\mathbb{Q}[x]$.

---

2. This exercise gives an example of a polynomial that is irreducible in $\mathbb{Q}[x]$ but it is reducible modulo every prime number p.

(a) Prove that the polynomial $x^4 + 1$ is irreducible in $\mathbb{Q}[x]$.

x^4+1 is primitive in $\mathbb{Z}[x]$. so, if we can show that x^4+1 is irreducible in $\mathbb{Z}[x]$, it is irreducible in $\mathbb{Q}[x]$.

- x^4+1 is irreducible in $\mathbb{Z}[x]$
  - ↳ by rational root thm, the only possible values are ± 1,
    - $1^4+1 = 2$
    - $(-1)^4+1 = 2$
  - ↳ two quadratics?

Let $x^4+1 = (x^2+ax+b)(x^2+cx+d)$ s.t. $a,b,c,d \in \mathbb{Z}$

So, $= x^4 + (a+c)x^3 + (ac+b+d)x^2 + (ad+bc)x + bd$

Thus
$a+c=0 \to c=-a$
$ac+b+d=0 \Rightarrow -a^2+b+d=0$
$ad+bc=0 \Rightarrow ad-ab = a(d-b)=0$
$bd=1$

Case1: $a=0$.

$0\cdot 0 + b+d=0 \Rightarrow b+d=0 \Rightarrow d=-b$

If $d=-b$, $bd = -b^2 = 1$, so $b^2=-1$, which is impossible in $\mathbb{Z}$.

Case2: $a \neq 0$

↳ $d-b=0$, so $d=b$.

If $b=d$, $-a^2+2b=0 \Rightarrow 2b=a^2 \Rightarrow b=\frac{a^2}{2}$

So, $bd = b^2 = \left(\frac{a^2}{2}\right)^2 = \frac{a^4}{4} = 1 \Rightarrow a^4 = 4 \Rightarrow a^2 = 2$, so $a = \sqrt{2}$, but $\sqrt{2} \notin \mathbb{Z}$.

Thus, x^4+1 is irreducible in $\mathbb{Z}[x]$ and also in $\mathbb{Q}[x]$.

(b) Prove that the polynomial $x^4 + 1$ is reducible over $\mathbb{Z}_p$ for every prime p by following the given guidelines.

- Show that the polynomial $x^4 + 1$ is reducible in $\mathbb{Z}_2[x]$.

By rational root thm, $x=1$ is a root.
↳ $1^4+1 = 2 \equiv 0 \bmod 2$. $(x-1) \equiv (x+1) \bmod 2$

1	1	0	0	0	1
		↓	1	1	1
	1	1	1	1	0

mod 2 → 1 is a root

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

1	1	1	1	1
	↓	1	0	1
	1	0	1	0

mod 2 → 1 is a root

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

1	1	0	1
	↓	1	1
	1	1	0

mod 2

$(x+1)(x+1)(x+1)(x+1) = (x+1)^4$

So, $x^4+1 = (x+1)^4$ in $\mathbb{Z}_2[x]$, so it is reducible.

- Show that if p is an odd prime then there exists an element a in $\mathbb{Z}_p$ that satisfies one of the following possibilities:

$$\begin{aligned} a^2 &\equiv -1 \mod p, \\ a^2 &\equiv 2 \mod p, \\ a^2 &\equiv -2 \mod p. \end{aligned}$$

Hint. For this part you may need to do some research about quadratic residues modulus an odd prime, which is a topic in Number Theory. You can cite without proof any result about quadratic residues modulus an odd prime.

Using Euler's Criterion, if p is an odd prime, and $a \not\equiv 0 \bmod p$, then $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \bmod p$.
↳ By Legendre Symbols,

$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$
$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$

I looked at lots of examples for this!

↳ Split into cases mod 8

① $p \equiv 1 \bmod 8$
$\left(\frac{-1}{p}\right) = 1$, so -1 is a quad. residue
$\left(\frac{2}{p}\right) = 1$, so 2 is a quad. residue
$\left(\frac{-2}{p}\right) = 1$, so -2 is a quad residue

② $p \equiv 3 \bmod 8$
$\left(\frac{-1}{p}\right) = -1$
$\left(\frac{2}{p}\right) = -1$
$\left(\frac{-2}{p}\right) = (-1)(-1) = 1$, so -2 is a quad. residue

③ $p \equiv 5 \bmod 8$
$\left(\frac{-1}{p}\right) = 1$, so -1 is a quad. residue
$\left(\frac{2}{p}\right) = -1$
$\left(\frac{-2}{p}\right) = -1$

④ $p \equiv 7 \bmod 8$
$\left(\frac{-1}{p}\right) = -1$
$\left(\frac{2}{p}\right) = 1$, so 2 is a quad. residue
$\left(\frac{-2}{p}\right) = -1$.

So, if p is an odd prime, there is an element that satisfies one of those 3 possibilities.

- Show that there exists an element a in $\mathbb{Z}_p$ that satisfies one of the following identities in $\mathbb{Z}_p[x]$:

$$\begin{aligned} (1)\ x^4+1 &= (x^2+a)(x^2-a), \\ (2)\ x^4+1 &= (x^2+ax+1)(x^2-ax+1), \\ (3)\ x^4+1 &= (x^2+ax-1)(x^2-ax-1). \end{aligned}$$

Using the ideas of quadratic residues mod (odd prime), if p is an odd prime it will satisfy one of the 3 possibilities.

(1) If $a^2 \equiv -1 \bmod p$, then $x^4+1 = x^4-(-1) = x^4-a^2 = (x^2+a)(x^2-a)$

(2) $(x^2+ax+1)(x^2-ax+1) = x^4-ax^3+x^2+ax^3-a^2x^2+ax+x^2-ax+1 = x^4+(2-a^2)x+1 = x^4+1$, if $a^2 \equiv 2 \bmod p$.

$2-a^2=0$

$-a^2=-2$

$a^2=2$

(3) $(x^2+ax-1)(x^2-ax-1) = x^4-ax^3-x^2+ax^3-a^2x^2-ax-x^2+ax+1 = x^4+(-2-a^2)x+1 = x^4+1$, if $a^2 \equiv -2 \bmod p$

$-2-a^2=0$

$-a^2=2$

$a^2=-2$

So, because every odd prime p falls into one of those cases, all odd primes are reducible in $\mathbb{Z}_p[x]$

Thus, x^4+1 is reducible over $\mathbb{Z}_p$ for every prime p. ∎

---

3. Prove that the polynomial $7x^4+15x^3+25x^2+10x+35$ is irreducible in $\mathbb{Q}[x]$ by applying Eisenstein's Criterion.

Let p=5. Because 5 does not divide $a_n=7$, but does divide 15, 25, 10, & 35. and additionally because $5^2=25$ does not divide 35,

thus $7x^4+15x^3+25x^2+10x+35$ is irreducible over $\mathbb{Q}$.

Homework #3.7 - Math 676

Mabie Kuehn

Section 3.7 - Ring Homomorphisms.

- Choose 8 exercises.

1. Let R and S be two commutative rings (not necessarily with unity). Prove that the 0-map: $f : R \to S$, $f(r) = 0$ for all r in R is a ring homomorphism.

Pf: Let $a, b \in R$. We need to show both prop a+b from 3.7.1.

↳(a) $f(a+b) = 0$ ✓
$f(a)+f(b) = 0+0 = 0$ ✓
So, $f(a+b) = f(a)+f(b)$.

↳(b) $f(a\cdot b) = 0$ ✓
$f(a)\cdot f(b) = 0\cdot 0 = 0$ ✓
So $f(a\cdot b) = f(a)\cdot f(b)$.

Thus, the 0-map is a ring homomorphism. ∎//

Definition 3.7.1. Let $\phi : R \to S$ be a function between two com
unity). We say that ϕ is a *ring homomorphism* if, for all a and b i
(a) $\phi(a+b) = \phi(a) + \phi(b)$;
(b) $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$.
If R and S are commutative rings **with unity**, we define a *ring*
rings with unity as a ring homomorphism, that also satisfies the fo
$\phi(1) = 1$.

---

2. Prove that the function: $f : \mathbb{Z} \to \mathbb{Z}$, $f(n) = n^2$ is not a ring homomorphism.

Pf: We know that if we can disprove either prop. a or b, it is not a homomorphism.

Let $a = 1$ and $b = 1$, which $\in \mathbb{Z}$.

a) $f(1+1) = f(2) = 2^2 = 4$
$f(1)+f(1) = 1^2+1^2 = 1+1 = 2$

Since $f(1+1) \neq f(1)+f(1)$, f is not a ring homomorphism. ∎

---

3. Prove that the function: $f : \mathbb{Z} \to \mathbb{Z}$, $f(n) = 2n$ is not a ring homomorphism.

Pf: Let $a = 1$ and $b = 1 \in \mathbb{Z}$.

b) $f(1\cdot 1) = f(1) = 2(1) = 2$
$f(1)\cdot f(1) = 2(1)\cdot 2(1) = 2\cdot 2 = 4$

Since $f(1\cdot 1) \neq f(1)\cdot f(1)$, f is not a ring homomorphism. ∎

5. Consider the function:

$\{0,1\}$ $\{0,1,2,3,4,5\}$

$$\begin{aligned} f : \mathbb{Z}_2 &\to \mathbb{Z}_6 \\ x &\mapsto 3x \text{ (here the product } 3x \text{ is evaluated in } \mathbb{Z}). \end{aligned}$$

Prove that f is a ring homomorphism but $f(1) \neq 1$.

Hint: since f is a function between finite sets you can just check all the cases.

Pf: Property (a) → Check all $x \in \mathbb{Z}_2$.
Property (b)

- $a=0, b=0$

(a) $f(0+0) = f(0) = 3(0) = 0$
$f(0)+f(0) = 3(0)+3(0) = 0+0 = 0$ ✓

(b) $f(0\cdot 0) = f(0) = 3(0) = 0$
$f(0)\cdot f(0) = 3(0)\cdot 3(0) = 0$ ✓

- $a=0, b=1$

(a) $f(0+1) = f(1) = 3(1) = 3$
$f(0)+f(1) = 3(0)+3(1) = 0+3 = 3.$ ✓

(b) $f(0\cdot 1) = f(0) = 3(0) = 0$
$f(0)\cdot f(1) = 3(0)\cdot 3(1) = 0\cdot 3 = 0$ ✓

- $a=1, b=0$

(a) $f(1+0) = f(1) = 3(1) = 3$
$f(1)+f(0) = 3(1)+3(0) = 3+0 = 3$ ✓

(b) $f(1\cdot 0) = f(0) = 3(0) = 0$
$f(1)\cdot f(0) = 3(1)\cdot 3(0) = 3\cdot 0 = 0$ ✓

- $a=1, b=1$

(a) $f(1+1) = f(2) = 3(2) = 6 \equiv 0 \bmod 6$
$f(1)+f(1) = 3(1)+3(1) = 3+3 = 6 \equiv 0 \bmod 6$

(b) $f(1\cdot 1) = f(1) = 3(1) = 3$
$f(1)\cdot f(1) = 3(1)\cdot 3(1) = 3\cdot 3 = 9 \equiv 3 \bmod 6$ ✓

$f(1) = 3(1) = 3 \neq 1.$

So, f is a ring homomorphism, but $f(1) \neq 1$.

8. Let $\phi : R \to S$ be a ring homomorphism between commutative rings with unity. Complete the proof of Lemma 3.7.13 by proving the following statements.

(a) The set $\mathrm{Im}(\phi)$ is closed for the product.

Let $x, y \in \mathrm{Im}(\phi)$. We want to show that $x \cdot y \in \mathrm{Im}(\phi)$.

Because $x, y \in \mathrm{Im}(\phi)$, $\exists\ \phi(a) = x$ and $\phi(b) = y$ s.t. $a, b \in R$.

So: $x \cdot y = \phi(a) \cdot \phi(b) = \phi(a \cdot b)$. And since $x \cdot y = \phi(a \cdot b)$, $x \cdot y \in \mathrm{Im}(\phi)$.

(b) Given an element x of $\mathrm{Im}(\phi)$, then the opposite of x is also in $\mathrm{Im}(\phi)$.

Let $x \in \mathrm{Im}(\phi)$. Thus, there is an $a \in R$ s.t. $\phi(a) = x$. We want to show $-x \in \mathrm{Im}(\phi)$.

Since $a \in R$, a ring, there is $-a \in R$. So, there exists a $y \in \mathrm{Im}(\phi)$ s.t. $y = \phi(-a)$. If we can show $y = -x$, then $-x \in \mathrm{Im}(\phi)$.

Because ϕ is a ring homomorphism, $f(a+b) = f(a) + f(b)$.

$$\phi(a + (-a)) = \phi(a) + \phi(-a)$$
$$\phi(0) = x + y$$
$$0 = x + y$$
$$-x = y.$$

So $-x = y$, and so since $y \in \mathrm{Im}(\phi)$, $-x \in \mathrm{Im}(\phi)$. ∎

10. Prove that the function ψ: $\{0,2,4,6,8\}$ $\{0,1,2,3,4\}$

$$\begin{aligned} \psi : 2\mathbb{Z}_{10} &\to \mathbb{Z}_5 \\ x &\mapsto \text{the remainder of } x \text{ divided by } 5, \end{aligned}$$

as defined in Example 3.7.17 is a ring isomorphism.

Hints:

- Since ψ is a function between finite sets, to prove that ϕ is bijective, it may be easier to evaluate ψ explicitly for every element of $2\mathbb{Z}_{10}$.
- A straightforward proof could be to verify the properties of ring homomorphism for all (finite) possible cases. You are certainly encouraged to find a creative and clear way to show all possible cases.

Pf: Bijective: $\psi(0)=0$, $\psi(2)=2$, $\psi(4)=4$, $\psi(6)=1 \bmod 5$, $\psi(8)=3 \bmod 5$

Injective → Since $\ker(\psi)=0$, ψ is injective.
Surjective → Since every element is reached, ψ is surjective.

Thus, ψ is Bijective.

Ring Homomorphism.

Cases

a \ b	0	2	4	6	8
0	✓	✓	✓	✓	✓
2	✓	✓	✓	✓	✓
4	✓	✓	✓	✓	✓
6	✓	✓	✓	✓	✓
8	✓	✓	✓	✓	✓

- If $a=0$ or $b=0$:

WLOG, $a=0$
(a) $\psi(0+b)=\psi(b)=b \bmod 5$ ✓
$\psi(0)+\psi(b)=0+b \bmod 5 = b \bmod 5$
(b) $\psi(0\cdot b)=\psi(0)=0$ ✓
$\psi(0)\cdot\psi(b)=0\cdot b \bmod 5 = 0$

If $a=2$: (WLOG, $b=2$) 2,2
↳ $b=2$:
(a) $\psi(2+2)=\psi(4)=4$ ✓
$\psi(2)+\psi(2)=2+2=4$
(b) $\psi(2\cdot 2)=\psi(4)=4$ ✓
$\psi(2)\cdot\psi(2)=2\cdot 2=4$

2,4 + 4,2
$b=4$:
(a) $\psi(2+4)=\psi(6)=1$ ✓
$\psi(2)+\psi(4)=2+4=6\equiv 1$
(b) $\psi(2\cdot 4)=\psi(8)=3$ ✓
$\psi(2)\cdot\psi(4)=2\cdot 4=8\equiv 3$

2,6 + 6,2
$b=6$:
(a) $\psi(2+6)=\psi(8)=3$ ✓
$\psi(2)+\psi(6)=2+6=8\equiv 3$
(b) $\psi(2\cdot 6)=\psi(12)=\psi(2)=2$ ✓
$\psi(2)\cdot\psi(6)=2\cdot 1=2$

2,8 + 8,2
$b=8$:
(a) $\psi(2+8)=\psi(10)=\psi(0)=0$
$\psi(2)+\psi(8)=2+3=5\equiv 0$ ✓
(b) $\psi(2\cdot 8)=\psi(16)=\psi(1)=1$ ✓
$\psi(2)\cdot\psi(8)=2\cdot 3=6\equiv 1$

If $a=4$: (WLOG, also $b=4$) 4,4
↳ $b=4$:
(a) $\psi(4+4)=\psi(8)=3$
$\psi(4)+\psi(4)=4+4=8\equiv 3$
(b) $\psi(4\cdot 4)=\psi(16)=\psi(1)=1$
$\psi(4)\cdot\psi(4)=4\cdot 4=16\equiv 1$

4,6 + 6,4
$b=6$:
(a) $\psi(4+6)=\psi(10)=\psi(0)=0$
$\psi(4)+\psi(6)=4+6=10\equiv 0$
(b) $\psi(4\cdot 6)=\psi(24)=\psi(4)=4$
$\psi(4)\cdot\psi(6)=4\cdot 1=4$

4,8 + 8,4
$b=8$:
(a) $\psi(4+8)=\psi(12)=\psi(2)=2$ ✓
$\psi(4)+\psi(8)=4+3=7\equiv 2$
(b) $\psi(4\cdot 8)=\psi(32)=\psi(2)=2$ ✓
$\psi(4)\cdot\psi(8)=4\cdot 3=12\equiv 2$

If $a=6$: (WLOG, also $b=6$) 6,6
↳ $b=6$:
(a) $\psi(6+6)=\psi(12)=\psi(2)=2$
$\psi(6)+\psi(6)=1+1=2$
(b) $\psi(6\cdot 6)=\psi(36)=\psi(6)=1$
$\psi(6)\cdot\psi(6)=1\cdot 1=1$

6,8 + 8,6
$b=8$:
(a) $\psi(6+8)=\psi(14)=\psi(4)=4$
$\psi(6)+\psi(8)=1+3=4$
(b) $\psi(6\cdot 8)=\psi(48)=\psi(8)=3$
$\psi(6)\cdot\psi(8)=1\cdot 3=3$

If $a=8$: (WLOG, also $b=$) 8,8
↳ $b=8$:
(a) $\psi(8+8)=\psi(16)=\psi(6)=1$
$\psi(8)+\psi(8)=3+3=6\equiv 1$
(b) $\psi(8\cdot 8)=\psi(64)=\psi(4)=4$
$\psi(8)\cdot\psi(8)=3\cdot 3=9\equiv 4.$

17. Prove that $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^3$ is not a field homomorphism.

Definition 3.7.25. A *field homomorphism* between two fields $\mathbb{K}$ and $\phi : \mathbb{K} \to \mathbb{F}$. More precisely, ϕ is a function with the following prope

- $\phi(a+b) = \phi(a) + \phi(b)$ for all a, b in $\mathbb{K}$;
- $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$ for all a, b in $\mathbb{K}$;
- ϕ is not the 0-homomorphism.

Pf. If f is a field homomorphism, $f(a+b) = f(a)+f(b)$.

Let $a=1$ $b=1$:

$f(a+b) = f(1+1) = f(2) = 2^3 = 8$

$f(a)+f(b) = f(1)+f(1) = 1^3+1^3 = 1+1 = 2$

So, f is not a field homomorphism

---

18. The set $\mathbb{K} := \{p + q\sqrt{2} \mid p, q \in \mathbb{Q}\}$ is a subfield of $\mathbb{C}$ (no need to prove this part). Prove that the function

$$\begin{array}{rcl} f : \mathbb{K} & \to & \mathbb{K} \\ p + q\sqrt{2} & \mapsto & p - q\sqrt{2} \end{array}$$

where p and q are rational numbers, is an automorphism of $\mathbb{K}$.

Pf: Field Homomorphism: $f(1)=1 \to$ In $\mathbb{K}$, $1 = 1+0\sqrt{2}$. So, $f(1) = f(1+0\sqrt{2}) = 1-0\sqrt{2} = 1$. ✓

$f(a+b) = f(a)+f(b) \to$ Let $a = p_1 + q_1\sqrt{2}$ $b = p_2 + q_2\sqrt{2}$

$f(a+b)$
$= f((p_1+q_1\sqrt{2}) + (p_2+q_2\sqrt{2}))$
$= f((p_1+p_2) + (q_1+q_2)\sqrt{2})$
$= (p_1+p_2) - (q_1+q_2)\sqrt{2}$

$f(a)+f(b)$
$= f((p_1+q_1\sqrt{2})) + f((p_2+q_2\sqrt{2}))$
$= p_1 - q_1\sqrt{2} + p_2 - q_2\sqrt{2}$
$= (p_1+p_2) - (q_1+q_2)\sqrt{2}$

$f(a \cdot b) = f(a) \cdot f(b) \to$ Let $a = p_1 + q_1\sqrt{2}$ $b = p_2 + q_2\sqrt{2}$

$f(a \cdot b)$
$= f((p_1+q_1\sqrt{2}) \cdot (p_2+q_2\sqrt{2}))$
$= f(p_1p_2 + p_1q_2\sqrt{2} + p_2q_1\sqrt{2} + 2q_1q_2)$
$= f((p_1p_2+2q_1q_2) + (p_1q_2+p_2q_1)\sqrt{2})$
$= (p_1p_2+2q_1q_2) - (p_1q_2+p_2q_1)\sqrt{2}$

$f(a) \cdot f(b)$
$= f(p_1+q_1\sqrt{2}) \cdot f(p_2+q_2\sqrt{2})$
$= (p_1 - q_1\sqrt{2}) \cdot (p_2 - q_2\sqrt{2})$
$= p_1p_2 - p_1q_2\sqrt{2} - p_2q_1\sqrt{2} + 2q_1q_2$
$= (p_1p_2+2q_1q_2) - (p_1q_2+p_2q_1)\sqrt{2}$

Bijective: Since f is a field homomorphism, f is 1-1.

Let $p+q\sqrt{2}$ be an element of $\mathbb{K}$. Since $f(p-q\sqrt{2}) = p - -q\sqrt{2} = p+q\sqrt{2}$, f is surjective.

Since f satisfies Lemma 3.7.15 & Def. 3.7.34, f is an automorphism.