Introduction to Abstract Algebra (II)

Dr. Abdullah Al-Azemi

Mathematics Department
Kuwait University

December 21, 2019

Contents

Chapter

0 Review

Section 0.1: Groups

Definition 0.1.1

A (**binary**) **operation** $*$ on a set S is a mapping from $S \times S$ to S so that for all $a, b \in S$, $(a, b) \mapsto a * b$. In that case, we say that S is closed under $*$. Moreover,

- $*$ is **associative** if $(a * b) * c = a * (b * c)$, for all $a, b, c \in S$.
- $*$ is **commutative** if $a * b = b * a$, for all $a, b \in S$.
- An element $e \in S$ is called the **identity** of S with respect to $*$ if $a * e = a = e * a$, for all $a \in S$.
- If a and b are two elements in S such that $b * a = e = a * b$, then we say that b is the **inverse** of a in S with respect to $*$.

Remark 0.1.1

In a set S with some operation $*$, we write a^{-1} for the multiplicative inverse so that $aa^{-1} = e = a^{-1}a$. While, we write $-a$ for the additive inverse with $a + (-a) = O = (-a) + a$.

Definition 0.1.2

A **group** $(G, *)$ is a set G closed under the operation $*$ satisfying the following conditions:

$\mathcal{G}_1$: $*$ is **associative**.

$\mathcal{G}_2$: there is an identity $e \in G$ such that $a * e = a = e * a$ for all $a \in G$.

$\mathcal{G}_3$: for each $a \in G$, there is $a^{-1} \in G$ such that $aa^{-1} = e = a^{-1}a$.

Moreover, G is said to be **abelian** group if $*$ is a commutative operation.

Definition 0.1.3

A subset H of a group G is a **subgroup** of G if H itself is a group with respect to the operation on G. In that case, we write $H \leq G$.

Theorem 0.1.1

If G is a group and H is a nonempty subset of G, i.e. $\phi \neq H \subseteq G$, then H is a subgroup of G iff if $a, b \in H$, then $a * b^{-1} \in H$.

The Division Algorithm in $\mathbb{Z}$

If $a, b \in \mathbb{Z}$ with $b > 0$, then there exist unique integers (**quotient**) q and (**remainder**) r such that

$$a = b \cdot q + r; \qquad 0 \leq r < b.$$

That is, $a \equiv r \pmod{b}$.

For example, $25 \equiv 1 \pmod{3}$ since $25 = 3 \cdot 8 + 1$.

Notation:

For any integers m and n, we write (m, n) and $[m, n]$ to denote their **greatest common divisor** and **least common multiple**, respectively.

Two integers m and n are said to be **relatively prime** (or **coprime**) if $(m, n) = 1$. For instance, 4 and 9 are coprime but 4 and 8 are not.

Definition 0.1.4

A group G is called **cyclic** if there is $a \in G$ with $G = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}$.

Theorem 0.1.2

- A group G of order p (p is prime) is isomorphic to $\mathbb{Z}_p$. That is, $G \approx \mathbb{Z}_p$.
- A group G is cyclic group of order m is isomorphic to $\mathbb{Z}_m$. That is, $G \approx \mathbb{Z}_m$.
- A group G is cyclic of infinite order is isomorphic to $\mathbb{Z}$. That is, $G \approx \mathbb{Z}$.

The group $\mathbb{Z}_m \times \mathbb{Z}_n \approx \mathbb{Z}_{mn}$ iff $(m, n) = 1$. Moreover, for any $n \in \mathbb{Z}^+$, there is a cyclic group of order n and each cyclic group of order n is isomorphic to $(\mathbb{Z}_n, +)$.

Note that $\mathbb{Z}_2 \times \mathbb{Z}_4$ is not cyclic and it is not isomorphic to $\mathbb{Z}_8$ since $(2, 4) = 2 \neq 1$. While $\mathbb{Z}_2 \times \mathbb{Z}_3$ is a cyclic group isomorphic to $\mathbb{Z}_6$.

Remark 0.1.2

- If $a \in \mathbb{Z}_n = \{0, 1, \cdots, n-1\}$ with $(a, n) = 1$, then $\mathbb{Z}_n = \langle\, a \,\rangle = \langle\, -a \,\rangle$.
- Moreover, if G is a cyclic with $G = \langle\, a \,\rangle$ for some $a \in G$, then $G = \langle\, a^{-1} \,\rangle$. In that case, we say that a is a **generator** for G.
- A subgroup of a cyclic group is cyclic.
- If G is a cyclic group, then G is an abelian group. The converse is not true in general, for instace $\mathbb{Z}_2 \times \mathbb{Z}_2$ (The Klein 4-group) is abelian group which is not cyclic.
- The subgroup of $\mathbb{Z}$ under addition are precisely $n\mathbb{Z} = \{0, \pm n, \pm 2n, \cdots\} = \langle\, n \,\rangle = \langle\, -n \,\rangle$ for any $n \in \mathbb{Z}$.

Chapter

1 Ring Theory

Section 1.1: Rings

Definition 1.1.1

A **ring** $(R, +, \cdot)$ is a set R together with two (binary) operations $+$ and $\cdot$, which are called addition and multiplication, defined on R such that:

$\mathcal{R}_1$: $(R, +)$ is an abelian group.

$\mathcal{R}_2$: Multiplication is associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, for all $a, b, c \in R$.

$\mathcal{R}_3$: For all $a, b, c \in R$, the following (**distribution laws**) hold:

- **Left distribution law**: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$, and
- **right distribution law**: $(a + b) \cdot c = (a \cdot c) + (b + c)$.

A **commutative** ring is a ring with a commutative multiplication operation.

Remark 1.1.1

We note that the group formed by R with addition, namely $(R, +)$, is referred to as the **additive group of** R. Its identity 0 is the zero of R, and the additive inverse for each $a \in R$, is denoted by $(-a)$.

Definition 1.1.2

An element e (or written as 1) in a ring R is called **unity** (or **identity**) for R if $ea = a = ae$ for each $a \in R$. It is simply the multiplicative identity in R. Note that, 1 is the unity of $\mathbb{Z}$, while $2\mathbb{Z}$ has no unity.

Theorem 1.1.1

Let R be a ring and $a, b, c \in R$. Then:

1. The zero element of R is unique.
2. Each element of R has a unique negative.
3. The **left cancellation laws**: If $a + b = a + c$ then $b = c$.
4. The **right cancellation laws**: If $a + c = b + c$ then $a = b$.
5. Each of the equations $a + x = b$ and $x + a = b$ has a unique solution.
6. $-(-a) = a$ and $-(a + b) = (-a) + (-b)$.
7. If $m, n \in \mathbb{Z}$, then $(m + n)a = ma + na$, $m(a + b) = ma + mb$, and $m(na) = (mn)b$.

Theorem 1.1.2

Let R be a ring, 0 the zero of R, and $a, b, c \in R$. Then:

1. $0a = a0 = 0$.
2. $a(-b) = (-a)b = -(ab)$.
3. $(-a)(-b) = ab$.
4. $a(b-c) = ab-ac$ and $(a-b)c = ac-bc$.

Proof:

1. Clearly, $0a + 0a = (0 + 0)a = 0a = 0a + 0$ and by the left cancellation law, we get $0a = 0$. The proof of $a0 = 0$ is similar.
2. The equation $x + ab = 0$ has a unique solution $x = -(ab)$. but $a(-b) + ab = a(-b + b) = a0 = 0$ implies that $x = a(-b)$ is another solution. By uniqueness of x, we get $-(ab) = a(-b)$. The proof of $-(ab) = (-a)b$ is similar.
3. Each element in R has a unique negative. By Part(2), $(-a)(-b) = (-(-a))(b) = ab$.
4. By Part(2), $a(b - c) = a(b + (-c)) = ab + a(-c) = ab + (-(ac)) = ab - ac$. The proof of $(a - b)c = ac - bc$ is similar.

Example 1.1.1

Each of the set $(\mathbb{Z}, +, \cdot)$, $(2\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, and $(\mathbb{C}, +, \cdot)$ are commutative rings.

Solution:

We only show that $\mathbb{Z}$ is a commutative ring. Note that $(\mathbb{Z}, +)$ is an abelian group. Also, $(a\ b)\ c = a\ (b\ c)$ for all $a, b, c \in \mathbb{Z}$. That is $\cdot$ is associative on $\mathbb{Z}$. Finally, for each $a, b, c \in \mathbb{Z}$, we have

$$a\,(b+c) = ab + ac \qquad \& \qquad (a+b)\,c = ac + bc.$$

Moreover, $ab = ba$ for any $a, b \in \mathbb{Z}$. Therefore, $(\mathbb{Z}, +, \cdot)$ is a commutative ring.

Example 1.1.2

Show that $(\mathbb{Z}_n, \oplus, \odot)$ is a commutative ring.

Solution:

We first show that $(\mathbb{Z}_n, \oplus)$ is an abelian group. This part is an exercise for YOU.

Note that for any $[a], [b], [c] \in \mathbb{Z}_n$, we have:

$$([a] \odot [b]) \odot [c] = [ab] \odot [c] = [(ab)c] = [a(bc)] = [a] \odot [bc] = [a] \odot ([b] \odot [c]),$$

where $(ab)c = a(bc)$ in $\mathbb{Z}$. Hence $\odot$ is associative on $\mathbb{Z}_n$.

We now prove the left distribution laws: Let $[a], [b], [c] \in \mathbb{Z}_n$, then

$$\begin{aligned}[a] \odot ([b] \oplus [c]) = [a] \odot ([b + c]) = [a(b + c)] = [ab + ac] \\ = [ab] \oplus [ac] = [a] \odot [b] \oplus [a] \odot [c],\end{aligned}$$

where the distribution laws are hold in $\mathbb{Z}$. The proof of right distribution law is similar.

Moreover, $[a] \odot [b] = [ab] = [ba] = [b] \odot [a]$ since $ab = ba$ in $\mathbb{Z}$. Therefore, $\odot$ is commutative in $\mathbb{Z}_n$, and hence $(\mathbb{Z}_n, \oplus, \odot)$ is a commutative ring.

Example 1.1.3

Let $\mathcal{F}$ deonte all the functions on $\mathbb{R}$. Define

$$(f + g)(x) = f(x) + g(x) \quad \text{and} \quad (fg)(x) = f(x)g(x)$$

for $f, g \in \mathcal{F}$ and for any $x \in \mathbb{R}$. Show that $\mathcal{F}$ is a commutative ring with respect to these addition and multiplication operations.

Solution:

Let $f, g, h \in \mathcal{F}$. Then • We first show that $(\mathcal{F}, +)$ is an abelian group.

$\mathcal{G}_1$: $+$ is associative on $\mathcal{F}$:

$$[(f+g)+h](x) = [f+g](x) + h(x) = [f(x)+g(x)] + h(x) = f(x) + [g(x)+h(x)]$$
$$= f(x) + [g+h](x) = [f+(g+h)](x).$$

$\mathcal{G}_2$: The zero element in $\mathcal{F}$ defined by $O(x) = 0$ for each $x \in \mathcal{F}$, since

$$(f+O)(x) = f(x) + O(x) = f(x) + 0 = f(x) = 0 + f(x) = O(x) + f(x) = (O+f)(x).$$

$\mathcal{G}_3$: Additive inverse: If $f \in \mathcal{F}$, then the negative (additive inverse) of f is $-f$ defined by $(-f)(x) = -f(x)$ as

$$(f + (-f))(x) = f(x) + (-f)(x) = f(x) + (-(f(x))) = 0 = O(x).$$

Therefore, $(\mathcal{F}, +)$ is a group. For any $f, g \in \mathcal{F}$, we have

$$(f+g)(x) = f(x) + g(x) = g(x) + f(x) = (g+f)(x).$$

Thus, $(\mathcal{F}, +)$ is an abelian group.

• We now show that $\cdot$ is associative on R.

$$[(fg)h](x) = [(fg)(x)]h(x) = [f(x)g(x)]h(x) = f(x)[g(x)h(x)]$$
$$= f(x)[(gh)(x)] = [f(gh)](x).$$

Moreover, $(fg)(x) = f(x)g(x) = g(x)f(x) = (gf)(x)$. Therefore, $\cdot$ is associative and commutative on $\mathcal{F}$.

• We now prove the left distribution law:

$$[f(g+h)](x) = f(x)[(g+h)(x)] = f(x)[g(x)+h(x)]$$
$$= f(x)(g) + f(x)h(x) = [fg](x) + [fh](x) = [fg+fh](x).$$

The proof of right distribution law is similar. Therefore, $\mathcal{F}$ is a commutative ring.

Definition 1.1.3

If R and S are two rings, then the **Cartesian product** $R \times S = \{(r, s) : r \in R \text{ and } s \in S\}$, where for any $(r_1, s_1), (r_2, s_2) \in R \times S$, we have

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2), \quad \text{and} \quad (r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2),$$

for any $r_1, r_2 \in R$ and any $s_1, s_2 \in S$.

Example 1.1.4

Let R and S be two rings. Show that $R \times S$ is a ring.

Solution:

Let $r_1, r_2, r_3 \in R$ and $s_1, s_2, s_3 \in S$ and hence $(r_1, s_1), (r_2, s_2), (r_3, s_3) \in R \times S$. Then

- We first show that $(R \times S, +)$ is an abelian group.

$\mathcal{G}_1$: $+$ is associative on $R \times S$: Note that $+$ is associative on R and S.

$$\begin{aligned}[(r_1, s_1) + (r_2, s_2)] + (r_3, s_3) &= (r_1 + r_2, s_1 + s_2) + (r_3, s_3) \\ &= ((r_1 + r_2) + r_3, (s_1 + s_2) + s_3) = (r_1 + (r_2 + r_3), s_1 + (s_2 + s_3)) \\ &= (r_1, s_1) + [(r_2 + r_3, s_2 + s_3)] = (r_1, s_1) + [(r_2, s_2) + (r_3, s_3)].\end{aligned}$$

$\mathcal{G}_2$: The zero element in $R \times S$ is $(0_R, 0_S)$, since for any $(r, s) \in R \times S$, we have

$$(r, s) + (0_R, 0_S) = (r + 0_R, s + 0_S) = (r, s) = (0_R + r, 0_S + s) = (0_R, 0_S) + (r, s).$$

$\mathcal{G}_3$: Additive inverse: If $(r, s) \in R \times S$, then the negative (additive inverse) of (r, s) is $(-r, -s)$ as $(r, s) + (-r, -s) = (r - r, s - s) = (0_R, 0_S)$.

Therefore, $(R \times S, +)$ is a group.

- We now show that $\cdot$ is associative on $R \times S$. Note that $\cdot$ is associative on R and S.

$$\begin{aligned}[(r_1, s_1)(r_2, s_2)](r_3, s_3) &= (r_1 r_2, s_1 s_2)(r_3, s_3) = ((r_1 r_2) r_3, (s_1 s_2) s_3) = (r_1 (r_2 r_3), s_1 (s_2 s_3)) \\ &= (r_1, s_1)[(r_2 r_3, s_2 s_3)] = (r_1, s_1)[(r_2, s_2)(r_3, s_3)].\end{aligned}$$

• We now prove the left distribution law: Note that left distribution law hold on R and S.

$$\begin{aligned}(r_1, s_1)[(r_2, s_2) + (r_3, s_3)] &= (r_1, s_1)[(r_2 + r_3, s_2 + s_3)] = (r_1(r_2 + r_3), s_1(s_2 + s_3)) \\ &= (r_1r_2 + r_1r_3, s_1s_2 + s_1s_3) = (r_1r_2, s_1s_2) + (r_1r_3, s_1s_3) \\ &= (r_1, s_1)(r_2, s_2) + (r_1, s_1)(r_3, s_3).\end{aligned}$$

The proof of right distribution law is similar. Therefore, $R \times S$ is a commutative ring.

Theorem 1.1.3

If $R_1, R_2, \cdots, R_n$ are rings, then the direct product $R = R_1 \times R_2 \times \cdots \times R_n$ is a ring where $R = \{(a_1, \cdots, a_n) : a_i \in R_i \text{ for } i = 1, 2, \cdots, n\}$. Moreover,

- $0_R = (0_{R_1}, 0_{R_2}, \cdots, 0_{R_n})$ and $-(a_1, a_2, \cdots, a_n) = (-a_1, -a_2, \cdots, -a_n)$.
- R is commutative iff R_i is commutative for all $i = 1, 2, \cdots, n$.
- $e_R = (e_{R_1}, e_{R_2}, \cdots, e_{R_n})$ is a unity for R iff e_{R_i} is a unity for R_i for all $i = 1, 2, \cdots, n$.
- $R_i \approx \{0_{R_1}\} \times \{0_{R_2}\} \times \cdots \times R_i \times \cdots \times \{0_{R_n}\} \leq R$ for each $i = 1, 2, \cdots, n$.

Example 1.1.5: #24.16 @*page* : 125

Show that $a^2 - b^2 = (a + b)(a - b)$ for all a and b in a ring R iff R is commutative.

Solution:

Let $a, b \in R$ (a ring). Then,

$$\begin{aligned}(a + b)(a - b) &= a(a + (-b)) + b(a + (-b)) = a^2 + a(-b) + ba + b(-b) \\ &= a^2 - ab + ba - b^2.\end{aligned}$$

Note that $a^2 - ab + ba - b^2 = a^2 - b^2$ iff $ab = ba$, that is R is commutative.

Exercise 1.1.1

Show that $(M_n(\mathbb{R}), +, \cdot)$ is a ring, where $M_n(\mathbb{R})$ is the set of all $n \times n$ matrices with real entries. The same result can be proved for $M_n(\mathbb{Z})$ and $M_n(\mathbb{Q})$.

Solution:

Clearly, $(M_n(\mathbb{R}), +)$ is an abelian group. Also, from **Math-111**, we know that $(AB)C = A(BC)$ for any $A, B, C \in M_n(\mathbb{R})$.

For any $A, B, C \in M_n(\mathbb{R})$, we have: The distribution laws hold:

$$A\,(B+C) = AB + AC \qquad \& \qquad (A+B)\,C = AC + BC.$$

Thus, $(M_n(\mathbb{R}), +, \cdot)$ is a ring. It is not a commutative ring since $AB \neq BA$ in general.

Exercise 1.1.2

Let $R = \mathbb{Z}[\sqrt{2}] = \left\{a + b\sqrt{2} : a, b \in \mathbb{Z}\right\}$. Then show that:

1. R is closed under the addition.
2. R is closed under the multiplication.
3. $(R, +, \cdot)$ is a commutative ring.

Solution:

Let $a + b\sqrt{2}, c + d\sqrt{2} \in \mathbb{R}$. Then

1. $(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in R$. Thus R is closed under addition.
2. $(a + b\sqrt{2}) + (c + d\sqrt{2}) = ac + ad\sqrt{2} + bc\sqrt{2} + 2bd = (ac + 2bd) + (ad + bc)\sqrt{2} \in R$. Therefore, R is closed under multiplication.
3. We show the three conditions of a ring: Let $a + b\sqrt{2}, c + d\sqrt{2}, m + n\sqrt{2} \in R$, then

• We first show that $(R, +)$ is an abelian group.

$\mathcal{G}_1$: $+$ is associative on R:

$$\begin{aligned}\Big[(a+b\sqrt{2})+(c+d\sqrt{2})\Big]+(m+n\sqrt{2}) &= \Big[(a+c)+(b+d)\sqrt{2}\Big]+(m+n\sqrt{2})\\ &= [(a+c)+m]+[(b+d)+n]\sqrt{2}\\ &= [a+(c+m)]+[b+(d+n)]\sqrt{2}\\ &= (a+b\sqrt{2})+[(c+m)+(d+n)]\sqrt{2}\\ &= (a+b\sqrt{2})+\Big[(c+d\sqrt{2})+(m+n\sqrt{2})\Big].\end{aligned}$$

$\mathcal{G}_2$: There is a zero element in R: $0 = 0 + 0\sqrt{2} \in R$.

$\mathcal{G}_3$: Additive inverse: If $a + b\sqrt{2} \in R$, then $(-a) + (-b)\sqrt{2} \in R$, and

$$(a+b\sqrt{2})+\Big[(-a)+(-b)\sqrt{2}\Big] = 0+0\sqrt{2} = 0.$$

Therefore, $(R, +)$ is a group. For any $a + b\sqrt{2}, c + d\sqrt{2} \in R$, we have

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

Thus, $(R, +)$ is an abelian group.

• We now show that $\cdot$ is associative on R.

$$\begin{aligned}&\Big[(a+b\sqrt{2})(c+d\sqrt{2})\Big]\Big(m+n\sqrt{2}\Big) = \Big[(ac+2bd)+(ad+bc)\sqrt{2}\Big]\Big(m+n\sqrt{2}\Big)\\ &= [m(ac+2bd)+2n(ad+bc)]+[n(ac+2bd)+m(ad+bc)]\sqrt{2}\\ &= [acm+2bdm+2adn+2bcn]+[acn+2bdn+adm+bcm]\sqrt{2}\\ &= [a(cm+2dn)+2b(dm+cn)]+[a(cn+dm)+b(cm+2dn)]\sqrt{2}\\ &= (a+b\sqrt{2})\Big[(cm+2dn)+(cn+dm)\sqrt{2}\Big]\\ &= (a+b\sqrt{2})\Big[(c+d\sqrt{2})(m+n\sqrt{2})\Big].\end{aligned}$$

Therefore, $\cdot$ is associative on R.

• We now prove the left distribution law:

$$\begin{aligned}&\Big[a+b\sqrt{2}\Big]\Big[(c+d\sqrt{2})+(m+n\sqrt{2})\Big] = \Big[a+b\sqrt{2}\Big]\Big[(c+m)+(d+n)\sqrt{2}\Big]\\ &= [a(c+m)+2b(d+n)]+[a(d+n)+b(c+m)]\sqrt{2}\\ &= \Big[(ac+2bd)+(ad+bc)\sqrt{2}\Big]+\Big[(am+2bn)+(2bn+bm)\sqrt{2}\Big]\\ &= \Big[(a+b\sqrt{2})(c+d\sqrt{2})\Big]+\Big[(a+b\sqrt{2})(m+n\sqrt{2})\Big].\end{aligned}$$

The proof of right distribution law is similar. Therefore, R is a ring.

$$\begin{aligned}\left(a+b\sqrt{2}\right)\left(c+d\sqrt{2}\right) &= (ac+2bd)+(ad+bc)\sqrt{2}\\ &= (ca+2db)+(cb+da)\sqrt{2} = \left(c+d\sqrt{2}\right)\left(a+b\sqrt{2}\right).\end{aligned}$$

Therefore, R is a commutative ring.

Exercise 1.1.3: #24.10 @*page* : 124

Let $\mathcal{F}$ deonte all the functions on $\mathbb{R}$. Define $(f+g)(x) = f(x)+g(x)$, and $(f\circ g)(x) = f(g(x))$ for $f, g \in \mathcal{F}$ and for any $x \in \mathbb{R}$. Show that $(\mathcal{F}, +, \circ)$ is not a ring.

Solution:

the left distribution law is not satisfied:

$$\begin{aligned}[f\circ(g+h)](x) &= f((g+h)(x)) = f(g(x)+h(x))\\ &\neq f(g(x))+f(h(x)) = [(f\circ g)+(f\circ h)](x).\end{aligned}$$

Check for instance if $f(x) = \sin x$, $g(x) = \frac{\pi}{2}$, and $h(x) = \frac{\pi}{2}$, where

$$\begin{aligned}&(f\circ(g+h))(x) = f(g(x)+h(x)) = f(\pi) = \sin\pi = 0, \text{ while}\\ &((f\circ g)+(f\circ h))(x) = f(g(x))+f(h(x)) = f\left(\frac{\pi}{2}\right)+f\left(\frac{\pi}{2}\right) = \sin\frac{\pi}{2}+\sin\frac{\pi}{2} = 2.\end{aligned}$$

Exercise 1.1.4: #24.14 @*page* : 125

Show that a ring has at most one unity.

Solution:

Assume that e_1 and e_2 are two unities for a ring R. Then,

$$e_1 = e_2e_1 = e_1e_2 = e_2.$$

Exercise 1.1.5: #24.15 @*page* : 125

Let E denote the set of even integers. Show that with the usual addition and with multiplication defined by $m * n = \frac{1}{2}mn$, E is a commutative ring. Is there a unity.

Solution:

Clearly, $(E, +)$ is an abelian group since it is exactly $(2\mathbb{Z}, +)$. Moreover,

$$(a * b) * c = \left(\frac{1}{2}ab\right) * c = \frac{1}{2}\left(\frac{1}{2}abc\right) = \frac{1}{2}a\left(\frac{1}{2}bc\right) = \frac{1}{2}a(b * c) = a * (b * c).$$

Further, $a * b = \frac{1}{2}ab = \frac{1}{2}ba = b * a$. Thus, $*$ is associative and commutative on E.

The left distribution law:

$$a * (b + c) = \frac{1}{2}a(b + c) = \frac{1}{2}ab + \frac{1}{2}ac = (a * b) + (a * c).$$

The proof of the right distribution law is similar. Therefore, E is a commutative ring.

The unity is 2 since $2 * a = \frac{1}{2}2a = a = \frac{1}{2}a2 = a * 2$.

Exercise 1.1.6: #24.17 @*page* : 125

Show that $(a + b)^2 = a^2 + 2ab + b^2$ for all a and b in a ring R iff R is commutative.

Solution:

Let $a, b \in R$ (a ring). Then,

$$(a + b)^2 = (a + b)(a + b) = a^2 + ab + ba + b^2.$$

Observe that $a^2 + ab + ba + b^2 = a^2 + 2ab + b^2$ iff $ab = ba$, that is R is commutative.

Exercise 1.1.7: #24.18 @*page* : 125

Show that if A is an abelian group with addition as the operation, and an operation $*$ is defined on A by $a * b = 0$ for all $a, b \in A$, then $(A, +, *)$ is a commutative ring.

Solution:

Note that it is given that $(A, +)$ is an abelian group. Let $a, b, c \in A$. Then

$$(a * b) * c = 0 * c = 0 = a * 0 = a * (b * c).$$

Thus, $*$ is associative on A. Further, $a * b = 0 = b * a$ and hence $*$ is commutative on A.

$$a * (b + c) = 0 = 0 + 0 = (a * b) + (a * c).$$

Thus, the left distribution law (and right distribution law as well) is satisfied. Hence A is a commutative ring.

Section 1.2: Subrings

Definition 1.2.1

A subset S of a ring R is called a **subring** of R if S itself is a ring with respect to the operations of R.

For example, $n\mathbb{Z}$ is a subring of $\mathbb{Z}$, even integer is a subring of $\mathbb{Z}$. But the odd integer is not a subring of $\mathbb{Z}$. Moreover, the set $\{0, 2, 4\}$ and $\{0, 3\}$ are two subrings of $\mathbb{Z}_6$.

In general, if R is a ring, then $\{0\}$ and R are two subrings of R.

Theorem 1.2.1

A subset S of a ring $(R, +, \cdot)$ is a subring of R iff S satisfies the following conditions:

$\mathcal{S}_1$: S is not empty.
$\mathcal{S}_2$: if $a, b \in S$, then $a - b \in S$.
$\mathcal{S}_3$: if $a, b \in S$, then $ab \in S$.

or

$\mathcal{S}_1$: S is not empty.
$\mathcal{S}_2$: if $a, b \in S$, then $a + b, ab \in S$.
$\mathcal{S}_3$: if $a \in S$, then $-a \in S$.

Proof:

" $\Rightarrow$ ": Clearly if S is a subring of R, then the Conditions $\mathcal{S}_1, \mathcal{S}_2$, and $\mathcal{S}_3$ are satisfied.

" $\Leftarrow$ ": Assume that the Conditions $\mathcal{S}_1, \mathcal{S}_2$, and $\mathcal{S}_3$ are satisfied. Then $+$ is associative and commutative on $S \subseteq R$. Also $\cdot$ is associative on $S \subseteq R$. If $a \in S$ $(S \neq \phi)$, then $\mathcal{S}_2$ implies that $a - a = 0 \in S$. Then $0, a \in S$ implies that $0 - a = (-a) \in S$ by $\mathcal{S}_2$. Therefore, S is an abelian group under the addition and the multiplication is associative on S. We need further to prove the distribution laws: But since the distribution laws hold in R, they hold in S as well since $S \subseteq R$. Therefore, $(S, +, \cdot)$ is a ring contained in R and hence it is a subring of R.

Example 1.2.1

Let $\mathcal{F}$ denote the ring of all functions $f : \mathbb{R} \to \mathbb{R}$, where $(f + g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$ for all $f, g \in \mathcal{F}$ for each $x \in \mathbb{R}$. Show that $S = \{f \in \mathcal{F} : f(1) = 0\}$ is a subring of $\mathcal{F}$.

Solution:

Clearly,

1. The zero mapping $O_{\mathcal{F}}(1) = 0$ and hence $O_{\mathcal{F}} \in S$ is not empty.
2. Let $f, g \in S$. Then $f(1) = 0 = g(1)$ and hence $(f - g)(1) = f(1) - g(1) = 0 - 0 = 0$. Thus, $f - g \in S$.
3. Let $f, g \in S$. Then $f(1) = 0 = g(1)$ and hence $(fg)(1) = f(1)g(1) = 0 \cdot 0 = 0$. Thus, $fg \in S$.

Therefore, S is a subring of $\mathcal{F}$.

Example 1.2.2

The center of a ring R is defined to be $Z(R) = \{x \in R : ax = xa \text{ for all } a \in R\}$. Show that $Z(R)$ is a subring of R.

Solution:

1. $0_R \in Z(R)$ since $0a = a0 = 0$ for all $a \in R$. Thus $Z(R) \neq \phi$.
2. Let $x, y \in Z(R)$, then we have $xa = ax$ and $ya = ay$ for all $a \in R$. Hence $(x - y)a = xa - ya = ax - ay = a(x - y)$. That is, $x - y \in Z(R)$.
3. Let $x, y \in Z(R)$, then we have $xa = ax$ and $ya = ay$ for all $a \in R$. Hence $(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy)$. That is, $xy \in Z(R)$.

Therefore, $Z(R)$ is a subring of R.

Exercise 1.2.1

Decide whether $S = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{Z} \right\}$ is a subring of $M_2(\mathbb{Z})$. How about $T = \left\{ \begin{pmatrix} a & b \\ c & 0 \end{pmatrix} : a, b, c \in \mathbb{Z} \right\}$?

Solution:

We simply prove the three conditions of Theorem 1.2.1.

1. Clearly, $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in S$ and so $S \neq \phi$.

2. If $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \in S$, then

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} - \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} a-x & b-y \\ 0 & c-z \end{pmatrix} \in S.$$

3. If $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \in S$, then

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} ax & ay+bz \\ 0 & cz \end{pmatrix} \in S.$$

Therefore, S is a subring of $M_2(\mathbb{Z})$.
However, $\begin{pmatrix} a & b \\ c & 0 \end{pmatrix}, \begin{pmatrix} x & y \\ z & 0 \end{pmatrix} \in T$, while $\begin{pmatrix} a & b \\ c & 0 \end{pmatrix}, \begin{pmatrix} x & y \\ z & 0 \end{pmatrix} = \begin{pmatrix} ax+bz & ay \\ cx & cy \end{pmatrix} \notin T$. Thus, T is not a subring of $M_2(\mathbb{Z})$.

Exercise 1.2.2

Decide whether $S = \left\{ \begin{pmatrix} a & a+2b \\ a+2b & b \end{pmatrix} : a, b \in \mathbb{Z} \right\}$ is a subring of $M_2(\mathbb{Z})$.

Solution:

If $a = 1, b = 0 \in \mathbb{Z}$, then clearly S is not a subring of $M_2(\mathbb{Z})$, as

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \in S \text{ while } \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \notin S.$$

Exercise 1.2.3

Show that $S = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}$ is a subring of $M_2(\mathbb{R})$. Try to get back to this problem (after the isomorphism section) to show that $S \approx \mathbb{C}$.

Solution:

Exercise 1.2.4

Prove that if C denotes any collection of subrings of a ring R, then the intersection of all of the rings in C is also a subring of R. What about the union of subrings of R?

Solution:

Let $C = \{S_1, S_2, \cdots, S_k\}$ be a collection of subrings of R, for some $k \in \mathbb{N}$, and let $S = \bigcap_{i=1}^{k} S_i$.

1. All subrings in C contains 0_R and hence the intersection of subrings is not empty.
2. Let x and y be elements in S. Then $x, y \in S_i$ and hence $x - y \in S_i$ for all i. Therefore, $x - y \in S$.
3. Let x and y be elements in S. Then $x, y \in S_i$ and hence $xy \in S_i$ for all i. Therefore, $xy \in S$.

Therefore, S is a subring of R.

On the other hand, the union is not a subring of R. For instance, $2\mathbb{Z}$ and $3\mathbb{Z}$ are both subrings of $\mathbb{Z}$. $2, 3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$ however $3 - 2 = 1 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.

Section 1.3: Integral Domains

Note that, in the usual system of numbers, if $ab = 0$, then we conclude that either $a = 0$ or $b = 0$. This is not the case, in general, in rings.

Definition 1.3.1

Let R be a ring, and let $a \in R$. Then

- If $a \neq 0$, then a is called a **zero divisor** (or **divisor of zero**), if there exists $0 \neq b \in R$ such that $ab = 0$.
- If R has a unity, then a is called a **unit** if it has a multiplicative inverse in R.

For example, $\mathbb{Z}$ has no zero divisors, while $[2]$ and $[3]$ are two zero divisors in $\mathbb{Z}_6$.

Theorem 1.3.1

In the ring $\mathbb{Z}_n$, the zero divisors are precisely those elements that are not coprime to n.

Proof:

Let $0 \neq m \in \mathbb{Z}_n$, and let $(m, n) = d \neq 1$. Then $m\left(\frac{n}{d}\right) = \left(\frac{m}{d}\right)n = 0$ as $\left(\frac{m}{d}\right)n$ is a multiple of n. Thus, $m\left(\frac{n}{d}\right) = 0$ in $\mathbb{Z}_n$, while $m, \frac{n}{d} \neq 0$. Thus, m is a zero divisor in $\mathbb{Z}_n$.
On the other hand, let $m \in \mathbb{Z}_n$ with $(m, n) = 1$. If for $s \in \mathbb{Z}_n$, $ms = 0$, then $n \mid ms$. But since $(m, n) = 1$, we have $n \mid s$ and hence $s = 0$ in $\mathbb{Z}_n$.

Corollary 1.3.1

If p is a prime, then $\mathbb{Z}_p$ has no zero divisors.

As an example, the zero divisors in $\mathbb{Z}_{12}$ are $S = \{2, 3, 4, 6, 8, 9, 10\}$ since $(12, i) \neq 1$ for any $i \in S$. Furthermore, 1, 5, 7, and 11 are units in $\mathbb{Z}_{12}$.

Definition 1.3.2

A commutative ring D with unity $e \neq 0$ and no zero divisors is called an **integral domain**. Consequently, the set of nonzero elements in D is closed under multiplication.

Example 1.3.1

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ are integral domains.
- $2\mathbb{Z}$ has no unity and hence it is not an integral domain.
- $\mathbb{Z}_6$ has $[2]$ and $[3]$ as zero divisors and hence $\mathbb{Z}_6$ is not an integral domain.
- $M_2(\mathbb{R})$ is not an integral domain as it is not commutative. Moreover, $M_2(\mathbb{R})$ has zero divisors such as $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, since $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

Theorem 1.3.2

Let D be a commutative ring with unity $e \neq 0$, and let $a, b, c \in D$. Then D is an integral domain iff $a \neq 0$, and $ab = ac$ implies $b = c$. That is, D is an integral domain iff the cancellation laws hold.

Proof:

" $\Rightarrow$ ": Assume that D is an integral domain. Then D has no zero divisors and hence for $a \neq 0$, $ab = ac$ implies $ab - ac = a(b - c) = 0$ which impies that $b - c = 0$. That is $b = c$. Thus the left cancellation law holds (similarly, we can use right cancellation law).

" $\Leftarrow$ ": Assume that the left cancellation law holds in D. Then we only need to show that D has no zero divisors. Assume that $a \neq 0$ and $ab = 0$. Then $ab = 0 = a0$. By the left cancellation law, $b = 0$. Thus D has no zero diviros and hence it is an integral domain.

Remark 1.3.1

An integral domain is a commutative ring with unity $e \neq 0$ satisfying the cancellation laws.

Theorem 1.3.3

$\mathbb{Z}_p$ is an integral domain iff p is prime.

Proof:

" $\Rightarrow$ ": By contrapositive, assume that p is not a prime. Then there are $a, b \in \mathbb{Z}_p$ so that $ab = p$ where $1 \leq a, b < p$. That is $[a][b] = [ab] = [p] = [0]$. Thus $[a]$ and $[b]$ are zero divisors in $\mathbb{Z}_p$ and hence $\mathbb{Z}_p$ is not an integral domain. Which is not the case.

" $\Leftarrow$ ": Assume that p is a prime. Then we can simply use Corollary 1.3.1 to prove the

statement. **Or**: If $[a][b] = [ab] = [0]$ in $\mathbb{Z}_p$, then $p \mid ab$. As p is prime, we have $p \mid a$ or $p \mid b$ (or both). Thus, either $[a]_p = [0]_p$ or $[b]_p = [0]_p$ (or both). Therefore, $\mathbb{Z}_p$ has no zero divisors and thus it is an integral domain.

Theorem 1.3.4

Let S be a subring of a ring R. Then if R is an integral domain, then so is S.

Proof:

Since S is contained in R, if S has zero divisors, then so is R. Contradiction.

Example 1.3.2

Show that $\mathbb{Z}\left(\sqrt{2}\right) = \left\{a + b\sqrt{2} : a, b \in \mathbb{Z}\right\}$ is an integral domain.

Solution:

$\mathbb{Z}\left(\sqrt{2}\right)$ is an integral domain since it is a subring of $\mathbb{R}$ which is an integral domain.

Example 1.3.3

Let $\mathcal{F}$ denote the ring of all functions $f : \mathbb{R} \to \mathbb{R}$, where $(f + g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$ for all $f, g \in \mathcal{F}$ for each $x \in \mathbb{R}$. Show that $\mathcal{F}$ is not an integral domain.

Solution:

Let $f, g \in \mathcal{F}$ defined by

$$f(x) = \begin{cases} 1, & \text{if } x = 0 \\ 0, & \text{otherwise} \end{cases} \quad \text{, and} \quad g(x) = \begin{cases} 1, & \text{for } x = 1 \\ 0, & \text{otherwise} \end{cases}$$

Then, $f(x)g(x) = 0$ for all x, yet $f(x) \neq O(x) \neq g(x)$. Thus $\mathcal{F}$ is not an integral domain.

Example 1.3.4

Describe the units in $\mathbb{Z}$, $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Q}$, and in $\mathbb{Z}_4$ and $\mathbb{Z}_5$.

Example 1.3.5

Show that a zero divisor a in a commutative ring R with unity can have no multiplicative inverse.

Solution:

Let $a \in R$ be a zero divisor. Then there is $b \in R$ such that $b \neq 0$ and $ab = 0$. Assume that a^{-1} exists in R, then $a^{-1}ab = a^{-1}0 = 0$, and hence $b = 0$ which is not the case. Thus a^{-1} does not exist.

Example 1.3.6

Show that $D = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$ is a zero divisor in $M_2(\mathbb{Z})$.

Solution:

Simply find a matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $AD = 0$ or $DA = 0$. Thus, if $A = \begin{pmatrix} 2 & 0 \\ -1 & 0 \end{pmatrix}$, we have $DA = 0$.

Example 1.3.7

Solve the equation $x^2 + x = 0$ in $\mathbb{Z}_5$.

Solution:

Clearly, $x^2 + x = x(x + 1) = 0$. So trying all elements in $\mathbb{Z}_5 = \{0, 1, 2, 3 = -2, 4 = -1\}$, we get $x^2 + x = 0$ only for $x = 0$ and $x = 4$.

Example 1.3.8

Solve the equation $x^2 - 3 = 0$ in $\mathbb{Z}_5$.

Solution:

Simply trying all possibility of $x : 0, 1, 2, -1, -2$ we get no solution.

Example 1.3.9

Solve the equation $x^2 + 3x + 3 = 0$ in $\mathbb{Z}_7$.

Solution:

Note that $x^2 + 3x + 3 = x^2 - 4x + 3 = (x - 1)(x - 3) = 0$. Then trying all possibilities of $x : 0, 1, 2, 3, -3, -2, -1$, we only get $x = 1$ and $x = 3$ as the solutions.

Exercise 1.3.1

Solve the equation $x^2 - 4 = 0$ in $\mathbb{Z}_5$.

Solution:

Note that $x^2 - 4 = (x-2)(x+2) = 0$. Then trying all possibilities of $x : 0, 1, 2, -2, -1$, we only get $x = 2$ and $x = 3$ as the solutions.

Exercise 1.3.2

Solve the equation $x^2 + 2x + 4 = 0$ in $\mathbb{Z}_6$.

Solution:

Trying all possibilities of $x : 0, 1, 2, 3, -2, -1$, we only get $x = 2$ as the only solution.

Exercise 1.3.3

Let p be a prime. Show that in the ring $\mathbb{Z}_p$, we have $(a+b)^p = a^p + b^p$ for all $a, b \in \mathbb{Z}_p$.

Solution:

Using the binomial expansion, we get

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i \, b^{p-i}.$$

Not that the coefficients $\binom{p}{i}$ are all multiples of p for $1 \leq i \leq p-1$. Hence $\binom{p}{i} = 0$ for all $i = 1, 2, \cdots, p-1$. Therefore the only terms in the expansion whose coefficient is nonzero are a^p and b^p with coefficients $\binom{p}{0} = \binom{p}{p} = 1$.

Section 1.4: Fields

Definition 1.4.1

Let R be a ring with unity $e \neq 0$.

- An element $a \in R$ with the property $a^2 = a$ is called an **idempotent**.
- If $a^n = 0$, for some $n \in \mathbb{Z}^+$, then a is called a **nilpotent** .
- If every nonzero elements of R is a unit, then R is called a **division ring**.
- A commutative division ring is called a **field**.
- A noncommutative division ring is called a **skew field**.

Remark 1.4.1

$(F, +, \cdot)$ is a field if: $(F, +)$ is an abelian group with identity 0, $(F^*, \cdot)$ is an abelian group with identity e and the distribution law $a(b + c) = ab + ac$ holds for all $a, b, c \in F$.

Example 1.4.1

Show that a division ring contains exactly two idempotent elements.

Solution:

Since R is a division ring, $e \in R$. Then $a^2 = a$ implies that $a^2 - a = a(a - e) = 0$. Thus $a = 0$ (and hence $a^2 = 0$) or $a = e$ (and hence $a^2 = e$).

Example 1.4.2

Let R be a commutative ring. Show that if a and b are nilpotent elements in R, then so is $a + b$.

Solution:

We have $a^n = 0$ and $b^m = 0$ for some $n, m \in \mathbb{Z}^+$. Hence, using the binomial expansion (valid in commutative rings), we have

$$(a + b)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} a^i \, b^{m+n-i}.$$

Thus, if $i \geq n$, we get $a^i = 0$. Otherwise, if $i < n$, then $m + n - i > m$ and hence $b^{m+n-i} = 0$.

Therefore, the terms of the sum are all zero.

Example 1.4.3

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

Solution:

Let $a, b \in R$ be two idempotents. Then $a^2 = a$ and $b^2 = b$. Hence

$$(ab)^2 = abab = aabb = a^2b^2 = ab.$$

Example 1.4.4

$(\mathbb{Z}, +, \cdot)$ is not a field since for instance 2 has no multiplicative inverse in $\mathbb{Z}$. However, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields since each nonzero element a has its multiplicative inverse $\frac{1}{a}$.

Note that an integral domain $(R, +, \cdot)$ has no zero divisors and hence its set of nonzero elements, say S, is closed under multiplication. Also, multiplication is associative on S since $S \subseteq R$. R has its unity $e \neq 0$ and hence $e \in S$. Therefore, $(S, \cdot)$ is a group unless there is $a \in S$ which is not a unit.

Fields $\subset$ integral domains $\subset$ commutative rings $\subset$ rings.

Theorem 1.4.1

Every field F is an integral domain.

Proof:

Let $a, b \in F$ and suppose that $a \neq 0$. Then if $ab = 0$, we have $a^{-1}(ab) = a^{-1}0 = 0$ which implies that $b = 0$. Thus, there is no zero divisors in F and hence it is an integral domain.

Theorem 1.4.2

Every finite integral domain D is a field.

Proof:

We show that every nonzero element in D is a unit. Let $0 \neq a \in D$, define a mapping $f : D \to D$ by $f(x) = ax$. We now show that f is onto which implies that for $e \in D$, there is $b \in D$ such that $f(b) = ab = e$. But since D is finite, f is onto iff f is one-to-one. For any $x, y \in D$, $f(x) = f(y)$ implies $ax = ay$ which implies that $x = y$ (by left cancellation law). Thus, f is onto and there is $b \in D$ such that $ab = e$. Therefore, each nonzero element in D is a unit and hence D is a field.

Theorem 1.4.3

$\mathbb{Z}_p$ is a field iff p is a prime.

Proof:

If $\mathbb{Z}_p$ is a field, then it is an integral domain (by Theorem 1.4.1) and hence p is prime by Theorem 1.3.3. On the other hand, if p is a prime, then $\mathbb{Z}_p$ is an integral domain by Theorem 1.3.3. Since $\mathbb{Z}_p$ is finite, Theorem 1.4.2 implies that $\mathbb{Z}_p$ is a field.

Proof 2:

This is another proof of the same statement. " $\Rightarrow$ ": By contrapositive: Assume that $p \geq 2$ is not a prime. Then we can write $p = rq$ with $r, q \geq 2$. Hence in $\mathbb{Z}_p$, we have $[r][q] = [rq] = [p] = [0]$. Thus, $\mathbb{Z}_p$ is not a field which is not the case.

" $\Leftarrow$ ": Assume that p is a prime. Let $m \in \mathbb{Z}_p = \{0, 1, \cdots, p-1\}$ with no inverse. Then none of the numbers $m0, m1, \cdots, m(p-1)$ is 1. So this list must contains two equal numbers in $\mathbb{Z}_p$. Hence we have $mi \equiv mj \pmod{p}$ which implies $m(i-j) \equiv 0 \pmod{p}$ for some i and j with $0 < i - j < p$. Therefore, one of $i - j$ or m is a multiple of p. Since $0 < i - j < p$, we get m is a multiple of p. Thus, $m = 0$ in $\mathbb{Z}_p$ and the only element in $\mathbb{Z}_p$ with no inverse is the zero element. That is $\mathbb{Z}_p$ is a field.

Definition 1.4.2

A subset S of a field F is a subfield of F if S itself is a field with respect to the operations on F.

Theorem 1.4.4

A subset K of a field F is a **subfield** of F iff the following conditions hold:

1. K contains the zero and unity of F,
2. if $a, b \in K$, then $ab, a - b \in K$, and
3. if $0 \neq a \in K$, then $a^{-1} \in K$.

Proof:

" $\Rightarrow$ ": If K is a field, then clearly the conditions are satisfied.

" $\Leftarrow$ ": Assume that K is a subset of F satisfying the three conditions. Then, K is clearly closed under addition and multiplication. Moreover, $+$ is associative and commutative on F and hence on K. If $a \in K$, then $0 - a = -a \in K$ and hence $(K, +)$ is an abelian group. Also $\cdot$ is associative and commutative on F and hence on K. Further the distribution laws hold for F and hence for K. Thus, $(K, +, \cdot)$ is a commutative ring. By definition, F has no zero divisors and hence K has none as well. The last condition implies that each nonzero element of K has an inverse. Therefore, K is a field.

Example 1.4.5

Consider the integral domain $\mathbb{Z}\left(\sqrt{2}\right) = \left\{a + b\sqrt{2} : a, b \in \mathbb{Z}\right\}$.

1. Compute $\left(-2 + \sqrt{2}\right)^{-1}$ in $\mathbb{Z}\left(\sqrt{2}\right)$.
2. Is $\mathbb{Z}\left(\sqrt{2}\right)$ a field? Explain.
3. Is $\mathbb{Q}\left(\sqrt{2}\right) = \left\{a + b\sqrt{2} : a, b \in \mathbb{Q}\right\}$ a field? Explain.

Solution:

1. Consider $\left(-2 + \sqrt{2}\right)\left(a + b\sqrt{2}\right) = 1 + 0\sqrt{2}$ (the unity of $\mathbb{Z}\left(\sqrt{2}\right)$). Thus, $-2a + 2b = 1$ and $a - 2b = 0$ which implies that $a = -1$ and $b = -\frac{1}{2}$. Therefore,
$$\left(-2 + \sqrt{2}\right)^{-1} = \left(-1 - \frac{1}{2}\sqrt{2}\right) \notin \mathbb{Z}\left(\sqrt{2}\right).$$
2. Clearly $\mathbb{Z}\left(\sqrt{2}\right)$ is not a field as $\left(-2 + \sqrt{2}\right)$ has no inverse in $\mathbb{Z}\left(\sqrt{2}\right)$.
3. Yes. The unity is 1 and the inverse of a nonzero element $a + b\sqrt{2}$ is computed as
$$\left(a + b\sqrt{2}\right)^{-1} = \frac{1}{a + b\sqrt{2}} = \frac{1}{a + b\sqrt{2}} \cdot \frac{a - b\sqrt{2}}{a - b\sqrt{2}} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2},$$
which is indeed in $\mathbb{Q}\left(\sqrt{2}\right)$.

Section 1.5: Isomorphism

Definition 1.5.1

Let R and S be two rings. A mapping $\theta : R \to S$ is a **ring homomorphism** if for all $a, b \in R$, we have:

1. $\theta(a + b) = \theta(a) + \theta(b)$, and
2. $\theta(ab) = \theta(a)\theta(b)$.

Note that the operation $a + b$ and ab are both in R while $\theta(a) + \theta(b)$ and $\theta(a)\theta(b)$ are in S.

Remark 1.5.1

The trivial homomorphism is $\phi_0 : R \to S$ defined by $\phi_0(r) = 0_S$ for all $r \in R$.

Definition 1.5.2

An **isomorphism** of a ring R onto a ring S is a mapping $\theta : R \to S$ that is a bijection (one-to-one and onto) and a homomorphism. In that case, we say that R and S are **isomorphic** rings denoted $R \approx S$.

Example 1.5.1

Show that if R and S are two rings, $\theta : R \to S$ is an isomorphism, and e is the unity of R, then $\theta(e)$ is the unity of S.

Solution:

Let $b \in S$. Then there is $a \in R$ with $\theta(a) = b$. Then, $b = \theta(a) = \theta(ae) = \theta(a)\theta(e) = b\theta(e)$. In a similar way, we can prove that $b = \theta(e)b$. Therefore, $\theta(e)$ is the unity of S.

Example 1.5.2

Show that $\mathbb{Z} \not\approx 2\mathbb{Z}$.

Solution:

Clearly, 1 is the unity in $\mathbb{Z}$ while $2\mathbb{Z}$ has no unity.

Remark 1.5.2

In order to show that two rings are isomorphic, we find an isomorphism mapping from one to the other.

On the other hand, to show that two rings are not isomorphic, it is enough to find a property that is preserved by isomorphism and in the same time the two rings do not share it. Examples for such properties are commutativity, existance of unity, and some other properties we will introduce later.

Example 1.5.3

Let $\theta : \mathbb{Z} \to 2\mathbb{Z}$ be defined by $\theta(a) = 2a$. Show that θ is not a ring homomorphism.

Solution:

Note that for $a, b \in \mathbb{Z}$, we have $\theta(a + b) = 2(a + b) = 2a + 2b = \theta(a) + \theta(b)$. However,

$$\theta(ab) = 2(ab) = 2ab \neq \theta(a)\theta(b) = 2a\,2b = 4ab.$$

Thus, θ is not homomorphism.

Definition 1.5.3

Let R be a ring. If there is a positive integer n such that $na = 0$ for each $a \in R$, then the least such integer is called the **characteristic** of R. Otherwise, R is said to have characteristic 0.

Theorem 1.5.1

Isomorphism relation on the calss of all rings is an equivalence relation.

Remark 1.5.3

Rings (unity e): $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ $(e = 1)$, $\mathbb{Z}_n$ $(e = [1])$, $\mathbb{Z} \times \mathbb{Z}_n$ $(e = (1, [1]))$, $M_2(\mathbb{R})$ $(e = I_2)$. While the rings: $2\mathbb{Z}$, $3\mathbb{Z}$, $2\mathbb{Z} \times \mathbb{Q}$ are examples of rings with no unity.

Theorem 1.5.2

Show that $\mathbb{Z}_{mn} \approx \mathbb{Z}_m \times \mathbb{Z}_n$ iff $(m, n) = 1$.

Proof:

" $\Rightarrow$ ": Assume that $(m, n) = d > 1$. Then $\frac{mn}{d} < mn$ and it is a multiple of both m and n (it is the least common multiple). Consider $(r, s) \in \mathbb{Z}_m \times \mathbb{Z}_n$, then

$$\frac{mn}{d}(r, s) = \left(\frac{n}{d}mr, \frac{m}{d}ns\right) = (0, 0).$$

Thus, all elements of $\mathbb{Z}_m \times \mathbb{Z}_n$ have order less than mn (the order of the group), so none can be a generator for $\mathbb{Z}_m \times \mathbb{Z}_n$. Contradiction.

" $\Leftarrow$ ": Define $\theta : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ by $\theta([a]_{mn}) = ([a]_m, [a]_n)$. We show that θ is an isomorphism:

• θ is a ring homomorphism: Let $[a]_{mn}, [b]_{mn} \in \mathbb{Z}_{mn}$. Then

$$\begin{aligned}\theta([a]_{mn} + [b]_{mn}) &= \theta([a + b]_{mn}) = ([a + b]_m, [a + b]_n) \\ &= ([a]_m + [b]_m, [a]_n + [b]_n) = ([a]_m, [a]_n) + ([b]_m, [b]_n) \\ &= \theta([a]_{mn}) + \theta([a]_{mn}),\end{aligned}$$

and

$$\begin{aligned}\theta([a]_{mn}[b]_{mn}) &= \theta([ab]_{mn}) = ([ab]_m, [ab]_n) \\ &= ([a]_m[b]_m, [a]_n[b]_n) = ([a]_m, [a]_n)([b]_m, [b]_n) \\ &= \theta([a]_{mn})\theta([b]_{mn}),\end{aligned}$$

Thus, θ is a homomorphism.

• θ is a bijection: We first show that θ is one-to-one: Suppose that $\theta([a]_{mn}) = \theta([b]_{mn})$, then $([a]_m, [a]_n) = ([b]_m, [b]_n)$. That is, $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$ and hence $m \mid a - b$ and $n \mid a - b$. But since $(m, n) = 1$, then $mn \mid a - b$. That is, $a \equiv b \pmod{mn}$. Thus, $[a]_{mn} = [b]_{mn}$. Therefore, θ is one-to-one. Note that θ is then a bijection since it is a mapping from a finite set to a same (finite) size set.

Therefore, θ is an isomorphism and hence $\mathbb{Z}_{mn} \approx \mathbb{Z}_m \times \mathbb{Z}_n$.

Example 1.5.4: #27.3 @*page* : 134

Prove that if R and S are isomorphic rings and R is an integral domain, then S is an integral domain as well.

Solution:

Let $\theta : R \to S$ be an isomorphism and R be an integral domain. Then R has no zero divisors and $\theta(0_R) = 0_S$ since θ is a homomorphism. Let $x, y \in S$ with $x \neq 0$ and $xy = 0$. Then there are $a, b \in R$ such that $\theta(a) = x$ and $\theta(b) = y$ (θ is onto). Thus,

$$xy = \theta(a)\theta(b) = \theta(ab) = 0_S.$$

Thus, $ab = 0_R$. Since R has no zero divisors, $a = 0$ or $b = 0$. but $a \neq 0_R$ since $\theta(a) = x \neq 0$. Thus, $b = 0_R$ and hence $\theta(b) = \theta(0_R) = 0_S = y$. Thus S has no zero divisors. Moreover S is commutative ring with unity $\theta(e_R)$. Therefore, S is an integral domain.

Example 1.5.5: #27.15 @*page* : 135

Prove that if R and S are isomorphic rings, then their characteristic are equal.

Solution:

Let $\theta : R \to S$ be an isomorphism and assume that $char(R) = m$. Then for any $r \in R$, $mr = 0_R$. For $x \in S$, there is $a \in R$ such that $\theta(a) = x$ (θ is onto). Thus,

$$mx = m\theta(a) = \theta(ma) = \theta(0_R) = 0_S.$$

Hence $mx = 0_S$ and thus $char(S) = m$.

Exercise 1.5.1: #27.2 @*page* : 134

Prove that if R and S are isomorphic rings and R is commutative, then S is commutative as well.

Solution:

Let $\theta : R \to S$ be an isomorphism and R be commutative. For any $x, y \in S$, there are $a, b \in R$ such that $\theta(a) = x$ and $\theta b = y$ (θ is onto). Thus,

$$xy = \theta(a)\theta(b) = \theta(ab) = \theta(ba) = \theta(b)\theta(a) = yx.$$

Hence S is commutative.

Exercise 1.5.2: #27.4 @*page* : 134

Prove that if R and S are isomorphic rings and R is a field, then S is a field as well.

Solution:

Let $\theta : R \to S$ be an isomorphism and R be a field. Then R is an integral domain and hence S is an integral domain as well. So we need to show that every nonzero element in S is a unit.

Let $0 \neq x \in S$, then there is $0 \neq a \in R$ such that $\theta(a) = x$ (θ is onto). Thus $a^{-1} \in R$ (R is a field). Thus $\theta(a^{-1}) = \theta(a)^{-1} = x^{-1} \in S$. Therefore, S is a field.

Exercise 1.5.3: #27.9 @*page* : 135

Prove that if R and S are fields, $\theta : R \to S$ is an isomorphism, and $a \in R$, $a \neq 0$, then $\theta(a^{-1}) = \theta(a)^{-1}$.

Solution:

Let $0 \neq a \in R$. Then $aa^{-1} = e_R$ implies $\theta(aa^{-1}) = \theta(e_R) = e_S$. But since θ is a homomorphism,

$$\theta(aa^{-1}) = \theta(a)\theta(a^{-1}) = e_S.$$

That is $\theta(a^{-1}) = \theta(a)^{-1}$.

Exercise 1.5.4: #27.23 @*page* : 135

Let $R = \left\{a + b\sqrt{2} : a, b \in \mathbb{Q}\right\}$ and $S = \left\{a + b\sqrt{3} : a, b \in \mathbb{Q}\right\}$ be two subfields of $\mathbb{R}$. Verify that $\theta : R \to S$ defined by $\theta\left(a + b\sqrt{2}\right) = a + b\sqrt{3}$ is not a ring isomorphism (homomorphism).

Solution:

Clearly,

$$\theta\left(a + b\sqrt{2}\right)\theta\left(c + d\sqrt{2}\right) = \left(a + b\sqrt{3}\right)\left(c + d\sqrt{3}\right) = (ac + 3bd) + (ad + bc)\sqrt{3},$$

which is not equal to

$$\theta\left[\left(a + b\sqrt{2}\right)\left(c + d\sqrt{2}\right)\right] = \theta\left[(ac + 2bd) + (ad + bc)\sqrt{2}\right] = (ac + 2bd) + (ad + bc)\sqrt{3}.$$

Section 1.6: The Field of Quotients of Integral Domain

Recall that an integral domain (e.g. $\mathbb{Z}$) is not a field (e.g. $\mathbb{Q}$) if it has an element with no multiplicative inverse (e.g. 2 in $\mathbb{Z}$).

In this section, we construct (show how) that every integral domain can be regarded as being contained in a certain (minimal) field, a field of quotients of the integral domain.

The construction procedure of a field of quotient of an integral domain is exactly the same as the construction of the rational numbers (field) from the integer numbers (integral domain).

⋆ The Construction

Let D be an integral domain that we desire to enlarge to a field of quotient F.

• **Step #1: Elements of F:**

Let D be a given integral domain and consider $D \times D = \{(a, b) : a, b \in D\}$. Here (a, b) is representing a/b. That is if $D = \mathbb{Z}$, $(2, 3)$ represents $\frac{2}{3}$. Let $S \subseteq D \times D^*$ given by $S = \{(a, b) : a, b \in D, b \neq 0\}$. This is to ensure that elements like $(2, 0)$ is not in F. But then $(2, 3)$ and $(4, 6)$ are representing the same element in S.

Definition 1.6.1

Two elements (a, b) and (c, d) in $S = \{(x, y) \in D \times D^*\}$ are said to be **equivalent**, denoted $(a, b) \sim (c, d)$, iff $ad = bc$.

Lemma 1.6.1

The relation $\sim$ on $S \subseteq D \times D^*$ is an equivalence relation.

Proof:

- **reflexive**: Clearly $(a, b) \sim (a, b)$ since $ab = ba$ as D is a commutative ring.
- **symmetric**: Let $(a, b) \sim (c, d)$ in S. Then $ad = bc$ and hence $cb = da$ which implies $(c, d) \sim (a, b)$. Thus $(c, d) \sim (a, b)$.

- **transitive**: Let $(a,b) \sim (c,d)$ and $(c,d) \sim (m,n)$ in S. Then $ad = bc$ and $cn = dm$. Thus

$$(an)d = (ad)n = (bc)n = b(cn) = b(dm) = (bm)d.$$

Since $d \in D^*$, we conclude that $an = bm$ and hence $(a,b) \sim (m,n)$.

Therefore, $\sim$ is an equivalence relation on S.

We remark that $[(a,b)]$ denotes the equivalence class of (a,b) in S. Then, $F = \{[(a,b)] : (a,b) \in S\}$. That is if $D = \mathbb{Z}$, then $[(a,b)]$ is viewed as $\left(\frac{a}{b}\right) \in \mathbb{Q}$.

- **Step #2: Binary operations $+$ and $\cdot$ on F:**

Lemma 1.6.2

Let $[(a,b)]$ and $[(c,d)]$ be any two elements in F, then the equations

$$[(a,b)] + [(c,d)] = [(ad+bc, bd)] \quad \text{and} \quad [(a,b)][(c,d)] = [(ac,bd)],$$

are well defined operations of addition and multiplication on F.

- **Step #3: F is a field:**

1. **Additive in F is commutative**: Clearly

$$[(a,b)] + [(c,d)] = [(ad+bc,bd)] = [(cb+da,db)] = [(c,d)] + [(a,b)]$$

2. **Additive in F is associative**: Clearly

$$\begin{aligned}([(a,b)] + [(c,d)]) + [(m,n)] &= [(ad+bc,bd)] + [(m,n)] = [((ad+bc)n + (bd)m, (bd)n)] \\ &= [(a(dn) + b(cn+dm), b(dn))] = [(a,b)][(cn+dm, dn)] \\ &= [(a,b)] + ([(c,d)] + [(m,n)]).\end{aligned}$$

3. $0 = [(0,1)]$ **is the additive zero in** F: Clearly $[(a,b)] + [(0,1)] = [(a,b)] = [(0,1)] + [(a,b)]$.
4. $[(a,b)]^{-1} = [(-a,b)]$ **in** F: Clearly $[(a,b)] + [(-a,b)] = [(ab-ab, b^2)] = [(0,b^2)]$, where $[(0,b^2)] = [(0,1)]$ as equivalence classes.

Therefore, $(F, +)$ is an abelian group.

Example 1.6.1

Show that in F, we have $[(a, -b)] = [(-a, b)]$.

Solution:

We simply show that $(a, -b) \sim (-a, b)$. But this is true since $ab = (-a)(-b)$.

5. **Multiplication is associative on** F: Clearly

$$\begin{aligned}([(a,b)][(c,d)])[(m,n)] &= [(ac,bd)][(m,n)] = [((ac)m,(bd)n)] \\ &= [(a(cm),b(dn))] = [(a,b)][(cm,dn)] = [(a,b)]([(c,d)][(m,n)]).\end{aligned}$$

6. **Distribution laws are hold in** F: Clearly (FOR YOU)

$$[(a,b)]([(c,d)] + [(m,n)]) = [(a,b)][(c,d)] + [(a,b)][(m,n)].$$

   By commutativity, the right distribution law holds as well.

7. **Multiplication in** F **is commutative**: Clearly

$$[(a,b)][(c,d)] = [(ac,bd)] = [(ca,db)] = [(c,d)][(a,b)].$$

Therefore, $(F, +, \cdot)$ is a commutative ring.

8. $e = [(1,1)]$ **is the unity in** F: Clearly

$$[(a,b)][(1,1)] = [(a,b)] = [(1,1)][(a,b)].$$

9. **For each** $0 \neq [(a,b)] \in F$**, we have** $[(a,b)]^{-1} = [(b,a)]$: If $0 \neq [(a,b)] \in F$, then $[(a,b)] \neq [(0,1)]$. That is $a, b \neq 0$. Then

$$[(a,b)][(b,a)] = [(ab,ab)] = [(1,1)].$$

Therefore, F is a field.

- **Step #4: F contains a subdomain isomorphic to (integral domain) D:**

Theorem 1.6.1

The map $\theta : D \to F$ given by $\theta(a) = [(a, 1)]$ is an isomorphism of D onto a subdomain of F, namely $\theta(D)$.

Proof:

Clearly, $\theta(a + b) = [(a + b, 1)] = [(a \cdot 1 + 1 \cdot b, 1)] = [(a, 1)] + [(b, 1)] = \theta(a) + \theta(b)$ and $\theta(ab) = [(ab, 1)] = [(a, 1)][(b, 1)] = \theta(a)\theta(b)$. Thus θ is a homomorphism onto $\theta(D)$ (the onto part is clear by the definition of $\theta(D)$).

To show that θ is 1-1, we assume that $\theta(a) = \theta(b)$ which implies that $[(a, 1)] = [(b, 1)]$. That is $(a, 1) \sim (b, 1)$ which implies that $a \cdot 1 = b \cdot 1$. Thus $a = b$ and hence θ is 1-1 and therefore it is an isomorphism.

Theorem 1.6.2: Uniqueness

If D is an integral domain, then there exists a field F, the field of qoutients of D, such that:

1. F contains an integral domain isomorphic to D.
2. If K is any field containing an integral domain isomorphic to D, then K contains a field isomorphic to F.

Note that we say that an integral domain D can be embedded (or enlarged) to a field F. This field is the field of quotients of D.

Example 1.6.2

Describe the field of quotients F of the integral domain $D = \{a + bi : a, b \in \mathbb{Z}\}$ of $\mathbb{C}$. "Describe" here means give the elements of $\mathbb{C}$ that make up the field F.

Solution:

The field of quotients of D (elements of F is then $(a + bi, c + di) \in D \times D^*$) will be of the field containing all complex number of the form $\dfrac{a + bi}{c + di}$ for $a, b, c, d \in \mathbb{Z}$. Thus,

$$\frac{a + bi}{c + di} \cdot \frac{c - di}{c - di} = \frac{(a + bi)(c - di)}{c^2 + d^2}.$$

Since $c^2 + d^2 \in \mathbb{Z}$, then the complex number reduces to one of the form $x + yi$ where $x, y \in \mathbb{Q}$. Thus $F = \{x + yi : x, y \in \mathbb{Q}\}$.

Example 1.6.3

Describe the field of quotients F of the integral domain $D = \left\{a + b\sqrt{2} : a, b \in \mathbb{Z}\right\}$ of $\mathbb{R}$. "Describe" here means give the elements of $\mathbb{R}$ that make up the field F.

Solution:

Looking for elements of the form $\dfrac{a + b\sqrt{2}}{c + d\sqrt{2}}$ where $a, b, c, d \in \mathbb{Z}$. Thus

$$\frac{a + b\sqrt{2}}{c + d\sqrt{2}} \cdot \frac{c - d\sqrt{2}}{c - d\sqrt{2}} = \frac{\left(a + b\sqrt{2}\right)\left(c - d\sqrt{2}\right)}{c^2 - 2d^2}.$$

Since $c^2 - 2d^2 \in \mathbb{Z}^*$, we get $F = \left\{x + y\sqrt{2} : x, y \in \mathbb{Q}\right\}$.

Section 1.7: Fermat's and Euler's Theorem

Math-261

Recall: $(\mathbb{Z}_p^*, \odot)$ is a group off p is a prime. Note that $\mathbb{Z}_p^* = \{1, 2, \cdots, p-1\}$ with $\left|\mathbb{Z}_p^*\right| = p-1$. Moreover, the order of element a in a group G is the smallest positive integer n such that $a^n = e$ (if such n exists).

Theorem 1.7.1: Fermat's Little Theorem

Assume that p is a prime. If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Corollary 1.7.1

Assume that p is a prime. For all $a \in Z$, $a^p \equiv a \pmod{p}$.

Example 1.7.1

Find x if $2^{14} \equiv x \pmod{7}$.

Solution:

By Fermat's Little Theorem, $2^6 \equiv 1 \pmod{7}$. Thus $2^{14} = ((2^6)^2)2^2 \equiv 1^2 \cdot 4 \equiv 4 \pmod{7}$.

Example 1.7.2

Find x if $8^{103} \equiv x \pmod{13}$.

Solution:

Note that $8^{103} = (2^3)^{103} = 2^{309}$, and $309 = 12 \cdot 25 + 9$. Thus,

$$8^{103} = 2^{309} = (2^{12})^{25} \cdot 2^9 \equiv 1^{25} \cdot (2^4)^2 \cdot 2 \equiv 3^2 \cdot 2 \equiv 18 \equiv 5 \pmod{13}.$$

Example 1.7.3

Show that $2^{11,213} - 1$ is not divisible by 11.

Solution:

We simply show that $2^{11,213} - 1 \not\equiv 0 \pmod{11}$, or that $2^{11,213} \not\equiv 1 \pmod{11}$. Note that $11,213 = 10 \cdot 1,121 + 3$. Thus

$$2^{11,213} - 1 = (2^{10})^{1,121} \cdot 2^3 - 1 \equiv 1^{1,121} \cdot 8 - 1 \equiv 7 \pmod{11} \not\equiv 0 \pmod{11}.$$

Definition 1.7.1

Let n be a positive integer. Let $\phi(n)$ be defined as the number of positive integers less than n and relatively prime to n.

Remark 1.7.1

By Theorem 1.3.1, $\phi(n)$ is the number of elements in $\mathbb{Z}_n$ that are not zero divisors. It is called the "**Euler phi-function**".

Definition 1.7.2

Let G_n denote the set of nonzero elements of $\mathbb{Z}_n$ that are not zero divisors. That is $G_n = \{k : 1 \leq k < n \text{ and } (k, n) = 1\}$.

Theorem 1.7.2

For $n > 1$, $(G_n, \cdot)$ is a group and $|\, G_n \,| = \phi(n)$.

Math-261

Recall: $\phi(p) = p-1$ for any prime number p. For any positive integer n, with $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ where $p_1^{e_1} < p_2^{e_2} < \cdots < p_k^{e_k}$ are primes and $e_1, e_2, \cdots, e_k$ are positive integer, we have

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

Example 1.7.4

Compute $\phi(10)$ and $\phi(40)$.

Solution:

Note that $10 = (2)(5)$ and $40 = (2^3)(5)$. Thus

$$\phi(10) = 10\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 10\left(\frac{1}{2}\right)\left(\frac{4}{5}\right) = 4 \text{ , and}$$
$$\phi(40) = 40\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 40\left(\frac{1}{2}\right)\left(\frac{4}{5}\right) = 16 \text{ , and}$$

Theorem 1.7.3

If $a \in G_n$, then $a^{\phi(n)} - 1$ is divisible by n. That is if $(a, n) = 1$ and $1 \leq a < n$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Example 1.7.5

Find x for $7^4 \equiv x \pmod{12}$.

Solution:

Note that 12 is not a prime, but $(7, 12) = 1$. Hence $7^{\phi(12)} \equiv 1 \pmod{12}$. But, $\phi(12) = 12\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 4$. Therefore, $7^{\phi(12)} \equiv 1 \pmod{12}$ and hence $x = 1$.

Example 1.7.6

Solve the equation: $17^{23} \equiv x \pmod{12}$.

Solution:

Clearly $17 \equiv 5 \pmod{12}$. Thus, we consider $5^{23} \equiv x \pmod{12}$. Note that 12 is not a prime, but $(5, 12) = 1$ and by Euler's Theorem, $5^{\phi(12)} \equiv 5^4 \equiv 1 \pmod{12}$. Thus,

$$5^{23} \equiv \left(5^{20}\right)\left(5^3\right) \equiv \left(5^4\right)^5\left(5^3\right) \equiv 1 \cdot 25 \cdot 5^1 \equiv 1 \cdot 5 \equiv 5 \pmod{12}.$$

Thus, $x = 5$.

Example 1.7.7

Use Fermat's Little Theorem to find the remainder of 3^{47} when it is divisible by 23.

Solution:

$$3^{47} \equiv \left(3^{22}\right)^2 \cdot 3^3 1^2 \cdot 27 \equiv 4 \,(\text{mod } 23).$$

Chapter

2 Ring of Polynomials

Section 2.1: Polynomials

Definition 2.1.1

Let R be a ring. A **polynomial**, $f(x)$, in indeterminate x over R is an expression

$$\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n + \cdots , \tag{2.1.1}$$

where $a_i \in R$ and $a_i = 0$ for all but a finite number of values of i. The set of all polynomials in x over R will be denoted by $R[x]$.

The a_i are the coefficients of $f(x)$. The **degree** of $f(x)$ is the largest value of i for which $a_i \neq 0$. If all $a_i = 0$, then the degree of $f(x)$ is undefined, and $f(x)$ is the zero element of R. An element of R of degree 0 is a constant polynomial, $f(x) = a \in R$.

Remark 2.1.1

For simplicity, if $a_i = 0$ for all $i > n$, then we write

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n, \tag{2.1.2}$$

and omit all terms $0x^k$ for any $k > n$. In that case, we say that a_n is the leading coefficient of $f(x)$. If furthermore $a_n = 1$, we say that $f(x)$ is a **monic polynomial**. For instance, $x^3 - x + 1$, $1 + 4x^2$, 5, $2 + x$ are all examples of polynomials.

Definition 2.1.1: Operation for $R[x]$

For $m, n \geq 0$, let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, $g(x) = b_0 + b_1 x + \cdots + b_m x^m$ be two elements in $R[x]$ for some ring R. Then for addition, we have:

$$f(x) + g(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_k x^k,$$

where $k = maximum(n, m)$, and $c_i = a_i + b_i$. For multiplication, we have:

$$f(x)g(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_k x^k,$$

where $k = n + m$ and $c_i = a_0b_i + a_1b_{i-1} + a_2b_{i-2} + \cdots + a_ib_0 = \sum_{j=0}^{i} a_jb_{i-j}$. Note that if R is not commutative, we get $\sum_{j=0}^{i} a_jb_{i-j} \neq \sum_{j=0}^{i} b_ja_{i-j}$.

Example 2.1.1

Compute $f(x) + g(x)$ and $f(x)g(x)$ in what follows:

1. $f(x) = x^2 + 1$ and $g(x) = x + 3$ in $\mathbb{R}[x]$.
2. $f(x) = 2 + 2x$ and $g(x) = 2 + 3x - x^2$ in $\mathbb{Z}_4[x]$.

Solution:

1.
   - $f(x) + g(x) = (1 + 3) + (0 + 1)x + (1 + 0)x^2 = 4 + x + x^2$.
   -

$$\begin{aligned} f(x)g(x) &= (1 + 0 \cdot x + 1 \cdot x^2)(3 + 1 \cdot x) \\ &= (1)(3) + [(1)(1) + (0)(3)]x + [(1)(0) + (0)(1) + (1)(3)]x^2 \\ &\quad + [(1)(0) + (0)(0) + (1)(1) + (0)(3)]x^3 \\ &= 3 + x + 3x^2 + x^3. \end{aligned}$$

2.
   - $f(x) + g(x) = 4 + 5x - x^2 = 0 + x + 3x^2 = x + 3x^2$.
   - $f(x)g(x) = 4 + (6 + 4)x + (-2 + 6)x^2 + (-2)x^3 = 2x + 2x^3$.

Theorem 2.1.1

The set $R[x]$, **polynomial rings**, is a ring with respect to addition and multiplication defined above.

Example 2.1.2

Let $f(x) = x + 1$. Find $(f(x))^2$ and $2f(x) = f(x) + f(x)$ in $\mathbb{Z}_2[x]$.

Solution:

- $(f(x))^2 = (1 + x)(1 + x) = 1 + 2x + x^2 = 1 + x^2$.
- $2f(x) = f(x) + f(x) = (1 + x) + (1 + x) = 2 + 2x = 0$.

Remark 2.1.2

Note that $\mathbb{R}[x], \mathbb{Q}[x], \mathbb{Z}[x], \mathbb{Z}_3[x]$ are all examples of polynomial rings. Moreover,

- If R is a commutative ring, then $R[x]$ is commutative.
- If R has a unity e, then e is also a unity for $R[x]$.
- If D is an integral domain, then $D[x]$ is also an integral domain.
- The units of $D[x]$ are precisely the units of D. This is because any polynomial in $D[x]$ of degree at least 1 multiplied by any other nonzero element in $D[x]$ must be of degree at least 1 which is not the unity e (whose degree is 0).
- If F is a field, $F[x]$ is an integral domain (not a field). Note that $1 \in \mathbb{R}$ (field), then $1 \cdot x = x \in \mathbb{R}[x]$, but $x^{-1} = \frac{1}{x} \notin \mathbb{R}[x]$ since it is not a polynomial.

Example 2.1.3

Prove that if p is a zero divisor for every element of R, then it is a zero divisor for every element of $R[x]$.

Solution:

Let p be a zero divisor for every element of R. Then for any $r \in R$, we have $pr = 0$. Thus, for any $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$ of degree n, we have

$$p \cdot f(x) = pa_0 + pa_1x + \cdots + pa_nx^n = 0 + 0 + \cdots + 0 = 0.$$

That is $pf(x) = 0$, and hence p is a zero divisor of $R[x]$.

Exercise 2.1.1: #34.11 @*page* : 164

Prove that in any commutative ring R, characteristic of R equals the characteristic of $R[x]$.

Solution:

The zero and the unity in R and $R[x]$ are the same. Since R is a ring it is closed under repeated addition of this unity. Thus $n \cdot e$ in $R[x]$ is the same as $n \cdot e$ in R. Therefore, the characteristics of $R[x]$ and R are the same.

Example 2.1.4

Prove that if R is a commutaive ring with unity e. Then, R is an integral domain iff $R[x]$ is an integral domain.

Solution:

Note that if R is a commutative ring with unity e, then $R[x]$ is also a commutative ring with unity e.

" $\Rightarrow$ ": Assume that R is an integral domain. Let $f(x) = a_0 + \cdots + a_n x^n$, $g(x) = b_0 + \cdots + b_m x^m$ be any two nonzero elements in $R[x]$ so that $a_n, b_m \neq 0$. Then the leading coefficient of $f(x)g(x)$ is $a_n b_m \neq 0$ since $a_n, b_m \in R$ and R is an integral domain. Thus, $f(x)g(x) \neq 0$ in $R[x]$. Therefore, $R[x]$ is an integral domain.

" $\Leftarrow$ ": Assume that $R[x]$ is an integral domain. Let a and b be any two nonzero elements in R. Clearly, $a, b \in R[x]$ (constant polynomials) and hence $ab \neq 0$ since $R[x]$ is an integral domain. Therefore, R is an integral domain.

Exercise 2.1.2

Find the sum and the product of the following polynomials in the given polynomial ring:

1. $f(x) = 4x - 5, g(x) = 2x^2 - 4x + 2$ in $\mathbb{Z}_8[x]$.
2. $f(x) = x + 1, g(x) = x + 1$ in $\mathbb{Z}_2[x]$.
3. $f(x) = 2x^2 + 3x + 4, g(x) = 3x^2 + 2x + 3$ in $\mathbb{Z}_6[x]$.

Solution:

1. $f(x) + g(x) = 2x^2 + 5$ and $f(x)g(x) = 6x^2 + 4x + 6$.
2. $f(x) + g(x) = 0$ and $f(x)g(x) = x^2 + 1$.
3. $f(x) + g(x) = 5x^2 + 5x + 1$ and $f(x)g(x) = x^3 + 5x$.

Exercise 2.1.3

There are four different polynomials of degree 2 in $\mathbb{Z}_2[x]$. List them all.

Solution:

Any polynomial in $\mathbb{Z}_2[x]$ is of the form $ax^2 + bx + c$, where $a, b, c \in \mathbb{Z}_2$ and $a \neq 0$. Thus, $a = 1$ and b and c each has two options: 0 or 1. That is, the polynomials in $\mathbb{Z}_2[x]$ are:

$$x^2; x^2 + 1; x^2 + x; x^2 + x + 1.$$

Section 2.2: The Division Algorithm

The Division Algorithm

If $f(x)$ and $g(x)$ are polynomials over a field F, with $g(x) \neq 0$, then there exist unique polynomials $q(x)$ and $r(x)$ over F such that

$$f(x) = g(x)\,q(x) + r(x), \qquad \text{with } r(x) = 0 \text{ or } deg(r(x)) < \deg\,(g(x)). \tag{2.2.1}$$

The polynomials $q(x)$ and $r(x)$ are called the quotient and remainder, respectively, in the division of $f(x)$ by $g(x)$.

Example 2.2.1

Let $f(x) = 2x^4 + x^2 - x + 1$ and $g(x) = 2x - 1$ be two polynomials over $\mathbb{R}$. Find $q(x)$ and $r(x)$ using the Division Algorithm.

Solution:

We simply apply the long division to get $q(x) = x^3 + \frac{1}{2}x^2 + \frac{3}{4}x - \frac{1}{8}$ and $r(x) = \frac{7}{8}$.

$$\begin{array}{r|l}
 & x^3 + \frac{1}{2}x^2 + \frac{3}{4}x - \frac{1}{8} \\
\hline
2x - 1 & 2x^4 + x^2 - x + 1 \\
 & \underline{2x^4 - x^3} \\
 & x^3 + x^2 - x + 1 \\
 & \underline{x^3 - \frac{1}{2}x^2} \\
 & \frac{3}{2}x^2 - x + 1 \\
 & \underline{\frac{3}{2}x^2 - \frac{3}{4}x} \\
 & -\frac{1}{4}x + 1 \\
 & \underline{-\frac{1}{4}x + \frac{1}{8}} \\
 & \frac{7}{8}
\end{array}$$

Remark 2.2.1

Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$. For $c \in F$, we say that $f(c)$ is the substitution of c for x in $f(x)$. That is, $f(c) = a_0 + a_1c + \cdots + a_nc^n \in F$. Moreover, if $f(x) = g(x)$ in $F[x]$,

then $f(c) = g(c)$ in F.

Example 2.2.2

Determine $q(x)$ and $r(x)$ when applying the Division Algorithm for: $f(x) = 3 + x - 3x^4$ and $g(x) = x - 2$ in $\mathbb{Z}_5[x]$. Find $f(2)$.

Solution:

We have $q(x) = 2x^3 + 4x^2 + 3x + 2$, $r(x) = 2$, and $f(2) = 3 + 2 - 3(2^4) = -3 = 2$.

$$
\begin{array}{rl}
 & 2x^3 + 4x^2 + 3x + 2 \\
\cline{2-2}
x - 2 \;\big| & -3x^4 \qquad\qquad + x + 3 \\
 & 2x^4 - 4x^3 \\
\cline{2-2}
 & \qquad 4x^3 \qquad + x + 3 \\
 & \qquad 4x^3 - 3x^2 \\
\cline{2-2}
 & \qquad\qquad 3x^2 + x + 3 \\
 & \qquad\qquad 3x^2 - x \\
\cline{2-2}
 & \qquad\qquad\qquad 2x + 3 \\
 & \qquad\qquad\qquad 2x - 4 \\
\cline{2-2}
 & \qquad\qquad\qquad\quad 2
\end{array}
$$

Theorem 2.2.1: The Remainder Theorem

If $f(x) \in F[x]$ and $c \in F$, then the remainder in the division of $f(x)$ by $x - c$ is $f(c)$.

Proof:

Note that $deg(x - c) = 1$. By the Division Algorithm, the remainder in the division of $f(x)$ by $(x - c)$ must be either 0 or of degree 0. Thus, for some $q(x) \in F[x]$,

$$f(x) = (x - c)q(x) + r, \qquad \text{with } r \in F.$$

Thus, $f(c) = (c - c)q(c) + r = r$.

Definition 2.2.1

If $f(x), g(x) \in F[x]$, with $g(x) \neq 0$, then $f(x)$ is divisible by $g(x)$ over F if $f(x) = g(x)q(x)$ for some $q(x) \in F[x]$. That is, the remainder in the Division Algorithm is zero. Furthermore, we say that $g(x)$ is a **factor** of $f(x)$ over F.

Theorem 2.2.2: The Factor Theorem

If $f(x) \in F[x]$ and $c \in F$, then $x - c$ is a factor of $f(x)$ iff $f(c) = 0$.

Definition 2.2.2

An element $c \in F$ is called a **root** (or a **zero**) of a polynomial $f(x) \in F[x]$ if $f(c) = 0$. Consequently, c is a root of $f(x)$ iff $x - c$ is a factor of $f(x)$.

Example 2.2.3

Use the Remainder Theorem to determine the remainder when $f(x) = 2x^5 - 3x^3 + 2x + 1$ is divided by $x - 2$ in $\mathbb{Z}_7[x]$.

Solution:

By the Remainder Theorem, we simply compute $f(2)$. Thus,

$$f(2) = 2^6 - 3(8) + 4 + 1 = 1 + 4(1) + 4 + 1 = 3.$$

Example 2.2.4

Is $x - 3$ a factor of $f(x) = 3x^3 - 9x^2 - 7x + 21$ in $\mathbb{Q}[x]$? Explain your answer.

Solution:

By the Factor Theorem, Theorem 2.2.2, we can simply compute $f(3)$:

$$f(3) = 3(3^3) - 9(3^2) - 7(3) + 21 = 3^4 - 3^4 - 21 + 21 = 0.$$

Therefore, $x - 3$ is a factor of $f(x)$.

Example 2.2.5

Use the Factor Theorem to construct a polynomial $f(x) \in \mathbb{Z}_5[x]$ such that every element of $\mathbb{Z}_5$ is a root for $f(x)$.

Solution:

Note that $\mathbb{Z}_5$ is a cyclic group of order 5. Thus, $[a]^6 = [a]$ for any $[a] \in \mathbb{Z}_5$. That is $f(a) = a^5 - a = 0$ for any a. Therefore, every $a \in \mathbb{Z}_5$ is a root for $f(x) = x^5 - x$.

Theorem 2.2.3

A nonzero polynomial $f(x) \in F[x]$ of degree n can have at most n roots in a field F.

Proof:

By the Factor Theorem, if $a_1 \in F$ is a root of $f(x)$, then $f(x) = (x - a_1)q_1(x)$, where $q_1(x)$ is of degree $n - 1$. A root $a_2 \in F$ of $q_1(x)$ implies that $f(x) = (x - a_1)(x - a_2)q_2(x)$, where $q_2(x)$ is of degree $n - 2$. Continuing in this way, we get

$$f(x) = (x - a_1)(x - a_2) \cdots (x - a_r)q_r(x),$$

where $q_r(x)$ has no further roots in F. Since $deg(f) = n$, at most n factors $x - a_i$ can appear. So $r \leq n$. Also, if $b \neq a_i$ for $i = 1, 2, \cdots, r$ and $b \in F$, then

$$f(b) = (b - a_1)(b - a_2) \cdots (b - a_r)q_r(b) \neq 0$$

since F has no zero divisors and none of $b - a_i$ or $q_r(b)$ are zero by construction. Hence the a_i for $i = 1, 2, \cdots, r \leq n$ are all zeros in F of $f(x)$.

Exercise 2.2.1

Find $q(x)$ and $r(x)$ when dividing $f(x) = x^4 + x^2 + 3x + 1$ by $g(x) = x^2 + 2x + 3$ in $\mathbb{Z}_5[x]$.

Solution:

Applying the Division Algorithm we get $q(x) = x^2 + 3x + 2$ and $r(x) = 0$.

$$
\begin{array}{rl}
 & x^2 + 3x + 2 \\
\cline{2-2}
x^2 + 2x + 3 \;\big|\; & x^4 + x^2 + 3x + 1 \\
 & x^4 + 2x^3 + 3x^2 \\
\cline{2-2}
 & 3x^3 + 3x^2 + 3x + 1 \\
 & 3x^3 + x^2 + 4x \\
\cline{2-2}
 & 2x^2 + 4x + 1 \\
 & 2x^2 + 4x + 1 \\
\cline{2-2}
 & 0
\end{array}
$$

Exercise 2.2.2

Divide $f(x) = 2x^4 + x^2 - x + 1$ by $g(x) = 2x - 1$ in $\mathbb{Z}_5[x]$.

Solution:

Note that in $\mathbb{Z}_5$, we have $1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$, and $4^{-1} = 4$. Moreover, $(-1) = 4$, $(-2) = 3$, $(-3) = 2$, and $(-4) = 1$. Thus, applying the Division Algorithm we get $q(x) = x^3 + 3x^2 + 2x + 2$ and $r(x) = 4$.

$$
\begin{array}{rl}
 & x^3 + 3x^2 + 2x + 3 \\
\cline{2-2}
2x - 1 \;\big|\; & 2x^4 + x^2 - x + 1 \\
 & 2x^4 - x^3 \\
\cline{2-2}
 & x^3 + x^2 - x + 1 \\
 & x^3 - 3x^2 \\
\cline{2-2}
 & 4x^2 - x + 1 \\
 & 4x^2 - 2x \\
\cline{2-2}
 & x + 1 \\
 & x - 3 \\
\cline{2-2}
 & 4
\end{array}
$$

Exercise 2.2.3

Determine $q(x)$ and $r(x)$ when applying the Division Algorithm for $f(x) = x^3 - 2x^2 + 2$ and $g(x) = x - 3$ in $\mathbb{R}[x]$. Find $f(3)$.

Solution:

We have $q(x) = x^2 + x + 3$, $r(x) = 11$, and $f(3) = 3^3 - 2(3^2) + 2 = 27 - 18 + 2 = 11$.

$$\begin{array}{r|l}
x - 3 & \begin{array}{l} x^2 + x + 3 \\ \hline x^3 - 2x^2 \quad + 2 \\ x^3 - 3x^2 \\ \hline x^2 \quad + 2 \\ x^2 - 3x \\ \hline 3x + 2 \\ 3x - 9 \\ \hline 11 \end{array}
\end{array}$$

Exercise 2.2.4

Find $q(x)$ and $r(x)$ when dividing $f(x) = x^4 - 1$ by $g(x) = -x^2 + 2$ in $\mathbb{Q}[x]$.

Solution:

Applying the Division Algorithm we get $q(x) = -x^2 - 2$ and $r(x) = 3$.

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

Exercise 2.2.5

Find $q(x)$ and $r(x)$ when dividing $f(x) = 3x^4 + 2x^2 - 1$ by $g(x) = 2x^2 + 4x$ in $\mathbb{Z}_5[x]$.

Solution:

Applying the Division Algorithm we get $q(x) = 4x^2 + 2x + 2$ and $r(x) = 2x + 4$.

$$
\begin{array}{r|l}
 & 9x^2 - 3x + 2 \\
\hline
2x^2 + 4x & 3x^4 + 2x^2 - 1 \\
 & 18x^4 + 36x^3 \\
\hline
 & -x^3 + 2x^2 - 1 \\
 & -6x^3 - 12x^2 \\
\hline
 & 4x^2 - 1 \\
 & 4x^2 + 8x \\
\hline
 & -3x - 1
\end{array}
$$

Exercise 2.2.6

Use the Remainder Theorem to determine the remainder when $f(x) = 2x^5 - 3x^3 + 2x + 1$ is divided by $x - 2$ in $\mathbb{R}[x]$.

Solution:

By the Remainder Theorem, we simply compute $f(2)$. Thus,

$$f(2) = 2^6 - 3(2^3) + 4 + 1 = 2^3(2^3 - 3) + 5 = 8(5) + 5 = 45.$$

Exercise 2.2.7

Is $x + i$ a factor of $f(x) = ix^9 + 3x^7 + x^6 - 2ix + 1$ in $\mathbb{C}[x]$? Explain your answer.

Solution:

By the Factor Theorem, Theorem 2.2.2, we can simply compute $f(-i)$:

$$\begin{aligned} f(-i) &= i(-i)^9 + 3(-i)^7 + (-i)^6 - 2i(-i) + 1 \\ &= -(i)^{10} - 3(i)^7 - 1 - 2 + 1 \\ &= 1 + 3i - 3 + 1 = 3i - 1 \neq 0. \end{aligned}$$

Therefore, $x + i$ is not a factor of $f(x)$.

Exercise 2.2.8

Divide $f(x) = x^4 + 5x^3 - 3x^2$ by $g(x) = 5x^2 - x + 2$ in $\mathbb{Z}_{11}[x]$.

Solution:

Applying the Division Algorithm we get $q(x) = 9x^2 + 5x + 10$ and $r(x) = 2$.

$$
\begin{array}{rl}
 & 9x^2 + 5x + 10 \\
\cline{2-2}
5x^2 - x + 2 \;\big| & x^4 + 5x^3 - 3x^2 \\
 & x^4 - 9x^3 + 7x^2 \\
\cline{2-2}
 & 3x^3 + x^2 \\
 & 3x^3 - 5x^2 + 10x \\
\cline{2-2}
 & 6x^2 + x \\
 & 6x^2 - 10x + 9 \\
\cline{2-2}
 & 2
\end{array}
$$

Exercise 2.2.9

Is $f(x) = x^3 + 2x + 3$ an irreducible polynomial of $\mathbb{Z}_5[x]$? If not, then express it as a product of irreducible polynomials of $\mathbb{Z}_5[x]$.

Solution:

By inspection, -1 is a root of $f(x)$ in $\mathbb{Z}_5[x]$, so $f(x)$ is reducible in $\mathbb{Z}_5[x]$. Dividing (long division) $f(x)$ by $x + 1$, we get $f(x) = (x + 1)(x^2 - x + 3)$. Again by inspection, we get -1 and 2 are two roots of $x^2 - x + 3$. Hence

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

Section 2.3: Factorization of Polynomials

Theorem 2.3.1: Greatest Common Divisors of Two Polynomials

If $a(x)$ and $b(x)$ are two polynomials over a field F, not both the zero polynomial, then there is a unique polynomial $d(x)$ over F such that

1. $d(x) \mid a(x)$ and $d(x) \mid b(x)$, and
2. if $c(x)$ is a polynomial such that $c(x) \mid a(x)$ and $c(x) \mid b(x)$, then $c(x) \mid d(x)$.

The polynomial $d(x)$ is called the **greatest common divisors** of $a(x)$ and $b(x)$. Such a polynomial can be computed by the **Euclidean Algorithm** for polynomials.

Theorem 2.3.2

If $a(x)$ and $b(x)$ are polynomials over a field F, not both the zero polynomial, and $(a(x), b(x)) = d(x)$, then there exist polynomials $u(x)$ and $v(x)$ over F such that $d(x) = a(x)u(x) + b(x)v(x)$.

Example 2.3.1

Use the Euclidean Algorithm to compute $(a(x), b(x))$, where $a(x) = x^4 - x^3 - x^2 + 1$, and $b(x) = x^3 - 1$ in $\mathbb{Q}[x]$.

Solution:

We simply apply the Division Algorithm to compute $(a(x), b(x))$ by dividing $a(x)$ by $b(x)$:

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

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

Thus, $(a(x), b(x)) = x - 1$. Note that $x^3 - 1$ diveded by $-x^2 + x$ results in $-x - 1$ with a remainder $x - 1$.

Definition 2.3.1

- Two polynomial are said to be **associates** if $f(x) = cg(x)$ for some nonzero elements $c \in F$. For instance, $f(x) = 6x - 4$ and $g(x) = 3x - 2$ are associates since $f(x) = 2g(x)$
- A nonconstant polynomial (of degree ≥ 1) $f(x) \in F[x]$ is called **irreducible** (or **prime**) over F if $f(x)$ cannot be expressed as a product $g(x)h(x)$ of two polynomials in $F[x]$ with $0 < \deg g(x), \deg h(x) < \deg f(x)$. That is, if $f(x) = g(x)h(x)$ and $f(x)$ is irreducible, then one of $g(x)$ and $h(x)$ is of zero degree and the other is an associate of $f(x)$.
  If $f(x)$ is not irreducible, then we say that $f(x)$ is **reducible**.

For example, $x^2 + 1$ is irreducible in $\mathbb{R}[x]$. It is reducible in $\mathbb{C}[x]$ as $x^2 + 1 = (x - i)(x + i)$ in $\mathbb{C}[x]$.

Theorem 2.3.3

If F is a field, $a(x), b(x), p(x) \in F[x]$, $p(x)$ is irreducible, and $p(x) \mid a(x)b(x)$, then either $p(x) \mid a(x)$ or $p(x) \mid b(x)$.

Proof:

Assume that $p(x) \nmid a(x)$, then $(p(x), a(x)) = e$ (the unity of F). Then there are polynomials $u(x)$ and $v(x)$ such that $e = p(x)u(x) + a(x)v(x)$. Multiplying both sides by $b(x)$, we get $b(x) = p(x)u(x)b(x) + a(x)v(x)b(x)$. Since $p(x) \mid p(x)$ and $p(x) \mid a(x)b(x)$, we get

$$p(x) \mid [p(x)u(x)b(x) + a(x)v(x)b(x)] = b(x).$$

Corollary 2.3.1

If $p(x), a_1(x), a_2(x), \cdots, a_n(x)$ are polynomials over F, with $p(x)$ irreducible and $p(x) \mid a_1(x) \cdots a_n(x)$, then $p(x) \mid a_i(x)$ for some i, where $i = 1, 2, \cdots, n$.

Theorem 2.3.4: Unique Factorization Theorem

Each polynomial of degree at least one over a field F can be written as an element of F times a product of irreducible polynomials (each with leading coefficient e) over F, and, except for the order in which these irreducible polynomials are written, this can be done in only way.

Theorem 2.3.5

Suppose that $f(x) \in F[x]$ is of degree 2 or 3. Then $f(x)$ is reducible over F iff $f(x)$ has a root in F.

Proof:

" $\Rightarrow$ ": Assume that $f(x)$ is reducible. Then $f(x) = g(x)h(x)$, where

$$0 < \deg g(x), \deg h(x) < \deg f(x) = 2 \text{ or } 3.$$

Then, one of $g(x)$ or $h(x)$ is of degree 1 taking the form $x - a$ for some $a \in F$. By the Factor Theorem, $f(a) = 0$ and hence $f(x)$ has a root in F.

" $\Leftarrow$ ": If $a \in F$ is a root of $f(x)$, then by the Factor theorem $x - a$ is a factor of $f(x)$. Then $f(x)$ is reducible.

Example 2.3.2

Determine whether $f(x) = x^3 + x + 1$ is irreducible over $\mathbb{Z}_5$.

Solution:

Note that $f(x)$ is of degree 3. Thus, it is reducible over $\mathbb{Z}_5$ iff $f(x)$ has a root in $\mathbb{Z}_5$. Thus

$$f(0) = 1 \neq 0, f(1) = 3 \neq 0, f(2) = 8 + 2 + 1 = 1 \neq 0, f(3) = 27 + 3 + 1 = 1 \neq 0,$$
$$\text{and } f(4) = 64 + 4 + 1 = 4 \neq 0.$$

Therefore, $f(x)$ is irreducible over $\mathbb{Z}_5$.

Example 2.3.3

Determine whether $f(x) = x^4 + x^2 + x + 1$ is irreducible over $\mathbb{Z}_5$.

Solution:

Note that $f(0) = 1, f(1) = 4, f(2) = 3, f(3) = 4$, and $f(4) = 2$. Since none of these is zero, $f(x)$ has no factor $x - a$ for any $a \in \mathbb{Z}_5$. Assume that $f(x) = (x^2 + ax + b)(x^2 + cx + d)$ for some $a, b, c, d \in \mathbb{Z}_5$. Thus

$$f(x) = x^4 + x^2 + x + 1 = x^4 + (a + c)x^3 + (ac + b + d)x^2 + (ad + bc)x + bd.$$

Hence, $a + c = 0$ which implies that $a = -c$ and $bd = 1$. Thus $(b, d) = (1, 1), (2, 3), (3, 2)$, or $(4, 4)$. Also, $(ad + bc) = a(d - b) = 1$. Therefore, $(b, d, a) = (2, 3, 1)$ or $(3, 2, 4)$. But in both cases $ac + b + d = 4 \neq 1$. Therefore, $f(x)$ is irreducible over $\mathbb{Z}_5$.

Example 2.3.4

Factor $f(x) = x^3 + 2x + 2$ in $\mathbb{Z}_7[x]$.

Solution:

We first try to find a root for $f(x)$ in $\mathbb{Z}_7$. Clearly, $f(2) = 14 = 0$. Thus, $x - 2$ is a factor for $f(x)$. We now use the Division Algorithm to divide $f(x)$ by $x - 2$:

$$\begin{array}{r|l} x-2 & x^2 + 2x + 6 \\ \hline & x^3 + 2x + 2 \\ & x^3 - 2x^2 \\ \hline & 2x^2 + 2x + 2 \\ & 2x^2 - 4x \\ \hline & 6x + 2 \\ & 6x - 12 \\ \hline & 0 \end{array}$$

Thus, $f(x) = (x - 2)(x^2 + 2x + 6)$. Let $g(x) = x^2 + 2x + 6$. We further look for a root of $g(x)$. Clearly, $g(2) = 14 = 0$. Thus, 2 is a root of $g(x)$, and hence $g(x) = (x - 2)(x + 4)$. Therefore,

$$f(x) = (x - 2)^2(x + 4) = (x + 4)(x + 5)^2.$$

Example 2.3.5

Factor $f(x) = x^4 + 2$ in $\mathbb{Z}_3[x]$.

Solution:

Clearly,

$$f(x) = x^4 + 2 = x^4 - 1 = (x^2 - 1)(x^2 + 1) = (x - 1)(x + 1)(x^2 + 1).$$

$x^2 + 1$ is irreducible in $\mathbb{Z}_3[x]$ as it has no roots in $\mathbb{Z}_3$. Therefore,

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

Theorem 2.3.6: Eisenstein's Irreducibility Criterion

Assume that p is a prime, $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, $p \mid a_i$ for $0 \leq i \leq n-1$, $p^2 \nmid a_0$ and $p \nmid a_n$. Then $f(x)$ is irreducible over $\mathbb{Z}$.

Example 2.3.6: #36.23 @*page* : 172

Show that each of the following polynomials is irreducible in $\mathbb{Z}[x]$:

1. $f(x) = x^3 + 6x^2 + 3x + 3$, and
2. $g(x) = x^5 - 5x^3 + 15$.

Solution:

1. Take $p = 3$, $p \mid 3, 3, 6$ and $p^2 \nmid 3$ and $p \nmid 1$. Hence $f(x)$ is irreducible over $\mathbb{Z}$.
2. Take $p = 5$, $p \mid 15, -5$ and $p^2 \nmid 15$ and $p \nmid 1$. Hence $g(x)$ is irreducible over $\mathbb{Z}$.

Theorem 2.3.7

If $f(x) \in \mathbb{Z}[x]$, then $f(x)$ factors into a product of two polynomials of lower degrees m and n in $\mathbb{Q}[x]$ if and only if it has such a factorization with polynomials of the same degrees m and n in $\mathbb{Z}[x]$.

Corollary 2.3.2

If $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ with $a_0 \neq 0$, and if $f(x)$ has a zero in $\mathbb{Q}$, then it has a zero m in $\mathbb{Z}$, and m must divide a_0.

Example 2.3.7

Show that $f(x) = x^4 - 2x^2 + 8x + 1$ is irreducible over $\mathbb{Q}$.

Solution:

Assume that $f(x)$ has a zero in $\mathbb{Q}$ (linear factor), then $f(x)$ has a zero m in $\mathbb{Z}$ that divides $+1$. Thus, the only two possibilities are ± 1. But $f(1) = 8$ and $f(-1) = -8$. That is $f(x)$ has no linear factor in $\mathbb{Q}[x]$.

If we assume that $f(x)$ can be factored in two quadratic factors in $\mathbb{Q}[x]$, then it has a fac-

torization Then if $f(x) = (x^2 + ax + b)(x^2 + cx + d) \in \mathbb{Z}[x]$. Equating the coefficients, we get

$$bd = 1, \quad ad + bc = 8, \quad ac + b + d = 2, \quad \text{and } a + c = 0,$$

for integer $a, b, c, d \in \mathbb{Z}$. Since $bd = 1$ then $b = d = 1$ or $b = d = -1$ in either cases, we have $b = d$. Hence, $ad + bc = b(a + c) = 8$. But this is impossible since $a + c = 8$. Therefore, $f(x)$ can not be factored in two quadratic polynomials.

Therefore, $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Exercise 2.3.1

Use the Euclidean Algorithm to compute $(f(x), g(x))$, where $f(x) = x^3 - 3x^2 + 3x - 2$, and $g(x) = x^2 - 5x + 6$ over $\mathbb{Q}$.

Solution:

We first apply the Division Algorithm to compute $(f(x), g(x))$ by dividing $f(x)$ by $g(x)$:

$$\begin{array}{r|l} & x + 2 \\ \hline x^2 - 5x + 6 & x^3 - 3x^2 + 3x - 2 \\ & x^3 - 5x^2 + 6x \\ \hline & 2x^2 - 3x - 2 \\ & 2x^2 - 10x + 12 \\ \hline & 7\text{x} + 14 \end{array}$$

Thus,

$$x^3 - 3x^2 + 3x - 2 = (x^2 - 5x + 6)(x + 2) + (7x - 14)$$
$$x^2 - 5x + 6 = (7x - 14)(\frac{1}{7}x - \frac{1}{7}3) = (x - 2)(x - 3).$$

Thus, $(f(x), g(x)) = x - 2$.

Exercise 2.3.2

Use the Euclidean Algorithm to compute $(f(x), g(x))$, where $f(x) = x^4 + x^3 - 4x^2 - 2x + 4$, and $g(x) = x^2 + x - 1$ over $\mathbb{Q}$.

Solution:

We first apply the Division Algorithm to compute $(f(x), g(x))$ by dividing $f(x)$ by $g(x)$:

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

Thus,

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

Thus, $(f(x), g(x)) = -1$.

Exercise 2.3.3

Prove or disprove: a polynomial $ax + b$ is irreducible in $R[x]$, where R is a ring.

Solution:

Disprove. $f(x) = 6x + 1$ in $\mathbb{Z}_8[x]$ with $6x + 1 = (2x + 1)(4x + 1)$. Note that $\mathbb{Z}_8$ is not a field.

Exercise 2.3.4

Show that $f(x) = x^3 + 2x^2 + 3$ is irreducible in $\mathbb{Z}_5[x]$.

Solution:

The degree of $f(x)$ is 3, so we need only to show that $f(x)$ has no roots over $\mathbb{Z}_5$.

$$f(0) = 3, f(1) = 1, f(2) = 4, f(3 = -2) = 3, f(4 = -1) = -1 = 4.$$

As none of these is zero, $f(x)$ has no roots over $\mathbb{Z}_5$ and hence it is irreducible.

Exercise 2.3.5

Express $f(x) = x^4 + x$ as a product of irreducible polynomials in $\mathbb{Z}_5[x]$.

Solution:

$f(x) = x^4 + x = x(x^3 + 1) = x(x + 1)(x^2 - x + 1)$. Note that $g(x) = x^2 - x + 1$ is irreducible in $\mathbb{Z}_5[x]$ as it has no roots in $\mathbb{Z}_5$. $g(0) = 1, g(1) = 1, g(2) = 3, g(-2) = 2$, and $g(-1) = 3$. Therefore, $f(x) = x(x + 1)(x^2 - x + 1)$ is a product of irreducible polynomials in $\mathbb{Z}_5[x]$.

Exercise 2.3.6

Use the Euclidean Algorithm to compute $(f(x), g(x))$, where $f(x) = x^3 - 2x + 1$, and $g(x) = x^2 - x - 2$ over $\mathbb{Z}_5$.

Solution:

We first apply the Division Algorithm to get $f(x) = (x^2 - x - 2)(x + 1) + (x + 3)$. Note that in $\mathbb{Z}_5[x]$, have $x + 3 = x - 2$. Hence, $x^2 - x - 2 = (x - 2)(x + 1)$.
Therefore, $(f(x), g(x)) = x - 2 = x + 3$.

$$
\begin{array}{rl}
 & x + 1 \\
\cline{2-2}
x^2 - x - 2 \;\big|\; & x^3 \quad - 2x + 1 \\
 & x^3 - x^2 - 2x \\
\cline{2-2}
 & x^2 \quad + 1 \\
 & x^2 - x - 2 \\
\cline{2-2}
 & \mathrm{x} + 3
\end{array}
$$

Exercise 2.3.7

Factor $f(x) = x^4 + 1$ over $\mathbb{Z}_2$.

Solution:

$$
\begin{aligned}
f(x) = x^4 + 1 = x^4 - 1 = (x^2 - 1)(x^2 + 1) = \left(x^2 - 1\right)^2 \\
= ((x - 1)(x + 1))^2 = \left((x + 1)^2\right)^2 = (x + 1)^4.
\end{aligned}
$$

Exercise 2.3.8

Let F be a field, and $f(x) \in F[x]$. Show that $f(x)$ is irreducible over F iff $f(x + c)$ is irreducible over F, for any $c \in F$. You may use a contrapositive proof in both directions.

Solution:

" $\Rightarrow$ ": Assume that $f(x+c) = p(x)q(x)$ is reducible where $0 < \deg p(x), \deg q(x) < \deg f(x)$. If we replace x by $x - c$, we get $f((x - c) + c) = f(x) = p(x - c)q(x - c)$, which cannot be as $f(x)$ is irreducible. Thus, $f(x + c)$ is irreducible.

" $\Leftarrow$ ": Assume that $f(x) = p(x)q(x)$ is reducible where $0 < \deg p(x), \deg q(x) < \deg f(x)$. If we replace x by $x + c$, we get $f(x + c) = p(x + c)q(x + c)$, which cannot be as $f(x + c)$ is irreducible. Thus, $f(x)$ is irreducible.

Exercise 2.3.9: #36.24 @*page* : 173

Use Eisenstein's Irreducibility Criterion to show that if p is a prime, then the

$$f(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1,$$

is irreducible over $\mathbb{Z}$. "Try to substitute $x = y + 1$".

Solution:

Let $x = y + 1$, then

$$\begin{aligned} f(x) = f(y+1) &= \frac{(y+1)^p - 1}{y} = \frac{1}{y}[(y+1)^p - 1] \\ &= \frac{1}{y}\left[\sum_{k=0}^{p} \binom{p}{k} y^k - 1\right] = \sum_{k=0}^{p} \binom{p}{k} y^{k-1} - \frac{1}{y} \\ &= \sum_{k=1}^{p} \binom{p}{k} y^{k-1}, \end{aligned}$$

where at $k = 0$, we have $\binom{p}{0} y^{-1} = \frac{1}{y}$. We have $p \mid \binom{p}{k}$ for $1 \leq k < p$, and $p \nmid \binom{p}{p} = 1$. Furthermore, $P^2 \nmid \binom{p}{1} = p$. Thus, $f(x)$ is irreducible in $\mathbb{Z}[x]$.

Exercise 2.3.10

Show that $f(x) = x^2 + 8x - 2$ is irreducible over $\mathbb{Q}$.

Solution:

Simply, $f(x)$ satisfies the Eisenstein's Conditions for irreducibility over $\mathbb{Q}$ with $p = 2$. Therefore, $f(x)$ is irreducible over $\mathbb{Q}$.

Exercise 2.3.11

Show that $f(x) = x^3 + 3x^2 - 8$ is irreducible over $\mathbb{Q}$.

Solution:

If $f(x)$ is reducible over $\mathbb{Q}$, then it factors in $\mathbb{Z}[x]$ and hence it must has a linear factor of the form $x - a$ in $\mathbb{Z}[x]$. Then a is a root of $f(x)$ and it must divides -8. Thus, a might be $\pm 1, \pm 2, \pm 4$, or ± 8. Compting $f(x)$ at these eight values, we find none of them is a zero of $f(x)$. Therefore, $f(x)$ is irreducible over $\mathbb{Q}$.

Exercise 2.3.12

Show that $f(x) = x^4 - 22x^2 + 1$ is irreducible over $\mathbb{Q}$.

Solution:

If $f(x)$ is reducible over $\mathbb{Q}$, then it factors in $\mathbb{Z}[x]$ and hence it has a linear factor of the form $x - a$ in $\mathbb{Z}[x]$ or it factors into two quadratic factors in $\mathbb{Z}[x]$. First if it has a linear factor $x - a$, then a must divides 1 and hence $a = 1$ or $a = -1$. But neither values of a is a root of $f(x)$. Then, we assume that $f(x) = (x^2 + ax + b)(x^2 + cx + d)$. Equating the coefficients, we get

$$bd = 1, \quad ad + bc = 0, \quad ac + b + d = -22, \quad \text{and } a + c = 0,$$

Thus $a = -c$ and either $b = d = 1$ or $b = d = -1$. Assume that $b = d = 1$, then $ac + 1 + 1 = -22$ implies that $ac = -24$. Thus $c^2 = 24$ which is impossible. Otherwise, if $b = d = -1$, we get $c^2 = 20$ which is also impossible. Therefore, $f(x)$ is irreducible over $\mathbb{Q}$.

Exercise 2.3.13

Show that for a prime p, $f(x) = x^p + a \in \mathbb{Z}_p[x]$ is not irreducible for any $a \in \mathbb{Z}_p$.

Solution:

Note that by the Corollary of Fermat's Little Theorem, we get $x^p + a = x^p + a^p = (x + a)^p$, and hence $x = -a$ is a root of $f(x)$.

Chapter

3 Quotient Rings

Section 3.1: Homomorphism of Rings and Ideals

Definition 3.1.1

If R and S are rings, then a mapping $\theta : R \to S$ is a (ring) **homomorphism** if for all $a, b \in R$

$$\theta(a+b) = \theta(a) + \theta(b), \qquad \text{and } \theta(ab) = \theta(a)\theta(b).$$

Note that if $\theta : R \to S$ is a ring homomorphism, then θ is a group homomorphism from the additive group of R to the additive group of S. That is, $\theta(0_R) = 0_S$ and $\theta(-a) = -\theta(a)$ for all $a \in R$.

Example 3.1.1

Show that $\theta : \mathbb{Z} \to \mathbb{Z}_n$ defined by $\theta(a) = [a]$ is a ring homomorphism.

Solution:

Clearly θ is a ring homomorphism since for any $a, b \in R$, we have:

$$\theta(a+b) = [a+b] = [a] + [b] = \theta(a) + \theta(b), \text{ and}$$

$$\theta(ab) = [ab] = [a][b] = \theta(a)\theta(b).$$

Example 3.1.2: Projection Homomorphism

Let R and S be two rings. Show that $\pi_1 : R \times S \to R$ and $\pi_2 : R \times S \to S$, defined by $\pi(r, s) = r$ and $\pi_2(r, s) = s$ are ring homomorphism.

Solution:

We show that π_1 is a ring homomorphism: Let $(r_1, s_1), (r_2, s_2) \in R \times S$. Then

$$\pi_1((r_1, s_1) + (r_2, s_2)) = \pi_1(r_1 + r_2, s_1 + s_2) = r_1 + r_2 = \pi_1(r_1, s_1) + \pi_1(r_2, s_2), \text{ and}$$

$$\pi_1((r_1, s_1)(r_2, s_2)) = \pi_1(r_1 r_2, s_1 s_2) = r_1 r_2 = \pi_1(r_1, s_1)\pi_1(r_2, s_2).$$

Thus, π_1 is a ring homomorphism. The proof for π_2 is similar.

Definition 3.1.2

Let $\theta : R \to S$ be a ring homomorphism. The **kernel** of θ, $\ker\theta$, is the set of all elements $r \in R$ such that $\theta(r) = 0_S$.

Note that the kernel of ring homomorphism $\theta : R \to S$ is just the kernel of θ as a homomorphism of the additive group of the rings. Recall that $\ker\theta$ is a (**normal**) subgroup of the additive group of R. In rings, $\ker\theta$ is forming a subring of R that is called an **ideal**.

Definition 3.1.3

A subring I of a ring R is called an **ideal** of R if $ar \in I$ and $ra \in I$ for all $a \in I$ and all $r \in R$.

We note that if R is a commutative ring, then the conditions ra and ar are equivalent. Moreover, recall that I is being a subring of R means that I is being closed under multiplication and subtraction. Thus, we get the following Theorem.

Theorem 3.1.1

A nonempty set I in a ring R is an ideal iff it satisfies:

1. if $a, b \in I$, then $a - b \in I$, and
2. if $r \in R$ and $a \in I$, then $ar \in I$ and $ra \in I$.

Note that $\mathbb{Z}$ is a subring of $\mathbb{Q}$, but $\mathbb{Z}$ is not an ideal of $\mathbb{Q}$ since $1 \in \mathbb{Z}$ and $\frac{1}{2} \in \mathbb{Q}$, but $1 \cdot \frac{1}{2} = \frac{1}{2} \notin \mathbb{Z}$.

Theorem 3.1.2: Analogue Homomorphism Properties From Math-261

Let $\theta : R \to S$ be a ring homomorphism. Then:

1. $\theta(0_R) = 0_S$.
2. $\theta(-a) = -\theta(a)$ for all $a \in R$.
3. If N is a subring of R, then $\theta(N)$ is a subring of S.
4. If M is a subring of S, then $\theta^{-1}(M)$ is a subring of R.
5. If R has a unity e, then $\theta(e)$ is unity of $\theta(R)$.
6. $\ker\theta$ is a subring of R.
7. θ is one-to-one iff $\ker\theta = \{0_R\}$.

Theorem 3.1.3

Let $\theta : R \to S$ be a ring homomorphism. Then

1. $\theta(R)$ is a subring of S.
2. $\ker\theta$ is an ideal of R.

Proof:

Clearly, $\theta(R)$ is an additive group of S (From Math-261). So $\theta(R)$ is not empty, closed under addition, and contains the negative of each of its elements.

1. We use Theorem 3.1.2 with R itself a subring of R.
2. Note that $\ker\theta$ is a subring of R by Theorem 3.1.2. So, we only show that $ar, ra \in \ker\theta$ for all $r \in R$ and $a \in \ker\theta$. If $a \in \ker\theta$ and $r \in R$, then $\theta(ar) = \theta(a)\theta(r) = 0 \cdot \theta(r) = 0$. Thus, $ar \in \ker\theta$. Similarly $ra \in \ker\theta$. Therefore, $\ker\theta$ is an ideal of R.

Example 3.1.3

If $\theta : \mathbb{Z} \to \mathbb{Z}_n$ is defined by $\theta(a) = [a]$, then $\ker\theta = \{kn : k \in \mathbb{Z}\} \approx n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

If $\pi_1 : R \times S \to R$ is defined by $\pi_1(r, s) = r$, then $\ker\theta = \{(0, s) : s \in S\} \approx S$. This is the ideal of $R \times S$.

Example 3.1.4

Show that $\theta : \mathbb{Z}_6 \to \mathbb{Z}_3$ defined by $\theta([a]_6) = [a]_3$ is a ring homomorphism and find its kernel. Is the mapping $f : \mathbb{Z}_3 \to \mathbb{Z}_6$ defined by $f([a]_3) = [a]_6$ well-defined? Explain.

Solution:

Let $[a], [b] \in \mathbb{Z}_6$. Then

- $\theta([a]_6 + [b]_6) = \theta([a + b]_6) = [a + b]_3 = [a]_3 + [b]_3 = \theta([a]_6) + \theta([b]_6)$.
- $\theta([a]_6[b]_6) = \theta([ab]_6) = [ab]_3 = [a]_3[b]_3 = \theta([a]_6)\theta([b]_6)$.

Therefore, θ is a ring homomorphism. Further, $\ker\theta = \{[a]_6 \in \mathbb{Z}_6 : \theta([a]_6) = [a]_3 = [0]_3\}$. Thus, $3 \mid a$ and hence $a = 3k, k \in \mathbb{Z}$. Thus $\ker\theta = \{[0], [3]\} \subseteq \mathbb{Z}_6$.

Note that f is not well-defined since $[0]_3 = [3]_3$, but $f([0]_3) \neq f([3]_3)$ as $[0]_6 \neq [3]_6$.

In general, the mapping $f : \mathbb{Z}_m \to \mathbb{Z}_n$ defined by $\theta([a]_m) = [a]_n$ is well-defined whenever $n \mid m$.

Example 3.1.5

Let $\theta : R \to S$ be a ring homomorphism with $\theta(R) \neq \{0\}$. Show that if R has a unity e and S has no zero divisors, then $\theta(e)$ is the unity of S.

Solution:

By Theorem 3.1.2, $\theta(e)$ is the unity of $\theta(R) \neq \{0\}$. If $\theta(e) = 0$, then for any $r \in R$ we have $\theta(r) = \theta(re) = \theta(r)\theta(e) = 0$ and hence $\theta(R) = \{0\}$ which is not the case. Then we may assume that $\theta(e) \neq 0$. Assume that e' is the unity of S. Then $e'\theta(e) = \theta(e) = \theta(e)\theta(e)$ which implies that $(e' - \theta(e))\theta(e) = 0$. Since, S has no zero divisors and $\theta(e) \neq 0$, then $e' - \theta(e) = 0$ and hence $e' = \theta(e)$.

Exercise 3.1.1

Determine whether $\theta : \mathbb{Z} \to \mathbb{Z}$ defined by $\theta(a) = a^2$ is a ring homomorphism? If so, find its kernel.

Solution:

For any $a, b \in \mathbb{Z}$, we have

$$\theta(a+b) = (a+b)^2 = a^2 + 2ab + b^2 = \theta(a) + 2ab + \theta(b).$$

Thus, θ is not a ring homomorphism.

Exercise 3.1.2

Determine whether $\theta : M_2(\mathbb{Z}) \to M_2(\mathbb{Z})$ defined by $\theta\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$ is a ring homomorphism? If so, find its kernel.

Solution:

Let $\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \begin{bmatrix} x & y \\ z & w \end{bmatrix} \in M_2(\mathbb{Z})$. Then

$$\theta\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} x & y \\ z & w \end{bmatrix}\right) = \theta\left(\begin{bmatrix} a+x & b+y \\ c+z & d+w \end{bmatrix}\right) = \begin{bmatrix} a+x & c+z \\ b+y & d+w \end{bmatrix}$$
$$= \begin{bmatrix} a & c \\ b & d \end{bmatrix} + \begin{bmatrix} x & z \\ y & w \end{bmatrix} = \theta\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) + \theta\left(\begin{bmatrix} x & y \\ z & w \end{bmatrix}\right), \text{ and}$$

$$\theta\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} x & y \\ z & w \end{bmatrix}\right) = \theta\left(\begin{bmatrix} ax+bz & ay+bw \\ cx+dz & cy+dw \end{bmatrix}\right) = \begin{bmatrix} ax+bz & cx+dz \\ ay+bw & cy+dw \end{bmatrix}, \text{ while}$$
$$\theta\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right)\theta\left(\begin{bmatrix} x & y \\ z & w \end{bmatrix}\right) = \begin{bmatrix} a & c \\ b & d \end{bmatrix}\begin{bmatrix} x & z \\ y & w \end{bmatrix} = \begin{bmatrix} ax+cy & az+cw \\ bx+dy & bz+dw \end{bmatrix}.$$

Thus, θ is not a ring homomorphism.

Exercise 3.1.3: #38.7 @*page* : 180

Show that if R and S are rings, and $\theta : R \to S$ is defined by $\theta(r) = 0_S$ for each $r \in R$, then θ is a ring homomorphism.

Solution:

Let $x, y \in R$. Then

- $\theta(x+y) = 0 = 0+0 = \theta(x)+\theta(y)$.
- $\theta(xy) = 0 = 0 \cdot 0 = \theta(x)\theta(y)$.

Therefore, θ is a ring homomorphism.

Exercise 3.1.4: #38.8 @*page* : 180

Let R and S be two rings.

1. Show that the mapping $\pi_1 : R \times S \to R$ defined by $\pi_1(r,s) = r$ is a homomorphism.
2. Show that $\ker \pi_1 \approx S$.

Solution:

1. Let $(r_1, s_1), (r_2, s_2) \in R \times S$. Then
   (a) $\pi_1((r_1,s_1)+(r_2,s_2)) = \pi_1(r_1+r_2, s_1+s_2) = r_1+r_2 = \pi_1(r_1,s_1)+\pi_1(r_2,s_2)$.
   (b) $\pi_1((r_1,s_1)(r_2,s_2)) = \pi_1(r_1r_2, s_1s_2) = r_1r_2 = \pi_1(r_1,s_1)\pi_1(r_2,s_2)$.

   Therefore, π_1 is a ring homomorphism.
2. $\ker \pi_1 = \{(r,s) : \pi_1(r,s) = r = 0_R\} = \{(0,s) : s \in S\} = \{0\} \times S$. Define $\theta : S \to \{0\} \times S$ by $\theta(s) = (0,s)$. We now show that θ is a ring isomorphism.
   (a) 1-1: Let $\theta(a) = \theta(b)$ for $a, b \in S$. Then $(0,a) = (0,b)$ implies that $a = b$. Thus, θ is 1-1.
   (b) Onto: Let $(0,a) \in \{0\} \times S$. Then $a \in S$ and $\theta(a) = (0,a)$. Thus θ is onto.
   (c) Homomorphism: Let $a, b \in S$. Then
   - $\theta(a+b) = (0, a+b) = (0,a)+(0,b) = \theta(a)+\theta(b)$.
   - $\theta(ab) = (0,ab) = (0,a)(0,b) = \theta(a)\theta(b)$.

   Therefore, θ is homomorphism.

   Therefore, θ is an isomorphism and hence $S \approx \ker \theta = \{0\} \times S$.

Exercise 3.1.5: #38.9 @*page* : 180

Show that if R is a commutative ring and $\theta : R \to S$ is a ring homomorphism, then $\theta(R)$ is commutative.

Solution:

Let $a, b \in \theta(R)$. Then there are $r_1, r_2 \in R$ with $\theta(r_1) = a$ and $\theta(r_2) = b$. Then,

$$ab = \theta(r_1)\theta(r_2) = \theta(r_1 r_2) = \theta(r_2 r_1) = \theta(r_2)\theta(r_1) = ba.$$

Exercise 3.1.6: #38.10 @*page* : 180

Show that if R is a ring with unity e, then every homomorphic image of R has a unity.

Solution:

Let $\theta : R \to S$ be any ring homomorphism. Then for any $s \in \theta(R)$, there is $r \in R$ such that

$$s = \theta(r) = \theta(e_R r) = \theta(e_R)\theta(r) = \theta(e_R)s.$$

In a similar way, we can prove that $s = s\theta(e_R)$ as well. Therefore, $\theta(e_R)$ is a unity for $\theta(R)$.

Exercise 3.1.7

Let R be a ring with unity e, and let I be an ideal of R. If I contains a unit u of R, then $I = R$.

Solution:

Let u^{-1} be the inverse of u in R. Then $u \in I$ implies that $e = u^{-1}u \in I$. Then for any $r \in R$, we have $r = re \in I$. Thus $I = R$.

Exercise 3.1.8

Let $\theta : R \to S$ be a ring homomorphism and let N be an ideal of R. Show that $\theta(N)$ is an ideal of $\theta(R)$.

Solution:

Clearly by Theorem 3.1.2, we have $\theta(N)$ is a subring of S which is contained in the subring $\theta(R)$ of S. Thus $\theta(N)$ is a subring of $\theta(R)$. So, we only need to show that $\theta(r)\theta(n), \theta(n)\theta(r) \in$

$\theta(N)$ for all $\theta(r) \in \theta(R)$ and $\theta(n) \in \theta(N)$. If $r \in R$ and $n \in N$, then $rn, nr \in N$ as N is an ideal of R. Thus, $\theta(r)\theta(n) = \theta(rn) \in \theta(N)$ since $rn \in N$. The proof of $\theta(n)\theta(r) \in \theta(N)$ is similar. Therefore, $\theta(N)$ is an ideal of $\theta(R)$.

Exercise 3.1.9

Let θ be a homomorphism of a ring R with unity e onto a nonzero ring S. Let u be a unit in R. Show that $\theta(u)$ is a unit in S.

Solution:

Since θ is onto, we know that $\theta(R) = S$ and hence $\theta(e)$ is the unity of S. Let u be a unit in R. Then there is u^{-1} with $uu^{-1} = u^{-1}u = e$. Therefore, $\theta(uu^{-1}) = \theta(e) = \theta(u^{-1}u)$ which implies that $\theta(u)\theta(u^{-1}) = \theta(e) = \theta(u^{-1})\theta(u)$. Therefore, $\theta(u)$ is a unit in S.

Section 3.2: More on Ideals

Definition 3.2.1

Let R be a commutative ring with unity e, and let $a \in R$. Then (a) is the set of all multiple of a by elements of R. That is $(a) = \{ra : r \in R\}$. A set of the form (a) is an ideal of R and this ideal is called a **principal ideal**.

Theorem 3.2.1

Every ideal of $\mathbb{Z}_n$ is a principal ideal.

Theorem 3.2.2

Let R be a commutative ring with $a \in R$. The set (a) is an ideal of R. It is called the principal ideal of R generated by a. Moreover, (a) is the smallest ideal of R containing a.

Proof:

We simply prove the conditions of Theorem 3.1.1:

1. Clearly, $0 = 0a \in (a) \neq \phi$.
2. If $ra, sa \in (a)$ for some $r, s \in R$, then $ra - sa = (r - s)a \in (a)$ as $r - s \in R$.
3. If $ra \in (a)$ and $s \in R$, then $s(ra) = (sr)a \in (a)$ as $sr \in R$. Therefore, (a) is an ideal of R. It is clear that if I is an ideal containing a, then I must contains all multiple of a. That is, $(a) \subseteq I$.

We note that if R is any ring, then (0) and R are ideals of R.

Example 3.2.1

Show that if F is a field, then F has no ideals other than (0) and F.

Solution:

Assume that $I \neq (0)$ is an ideal of F. We will show that $I = F$. Let $0 \neq a \in I$. Then $a^{-1} \in F$ (F is field). If e is the unity of F, then $e = a^{-1}a \in I$ since I is an ideal of F. Thus for any $r \in F$, $r = re \in I$. Therefore, $I = F$.

Example 3.2.2: #38.15 @*page* : 181

Show that if R is a commutative ring with unity e, and R has no ideals other than (0) and R, then R is a field.

Solution:

For each $0 \neq a \in R$, we have $a \in (a) \neq \{0\}$ and hence $(a) = R$. We show that R is a field by showing that each nonzero element in $(a) = R$ has a multiplicative inverse. Note that $e \in R = (a)$. Thus, there is $r \in R$ with $ra = e \in (a)$. Thus, for each nonzero element a, we have $r \in R$ such that $ra = e$. Thus each nonzero element in R has a multiplicative inverse in R. We now need to show that R has no zero divisors. Assume that $ab = 0$ and $a \neq 0$ for any $a, b \in R$. Then $a^{-1}\,ab = a^{-1}\,0 = 0$. Then $b = 0$. Therefore, R has no zero divisors and hence R is a field.

Example 3.2.3: #38.17 @*page* : 181

Prove that if I is an ideal of $\mathbb{Z}$, then either $I = (0)$ or $I = (n)$, where n is the least positive integer in I.

Solution:

If $I = \{0\}$, then $I = (0)$. Otherwise $I \neq (0)$. Let $0 \neq a \in I$, and hence $-a \in I$ as it is ideal. Clearly, either a or $-a$ is positive in I. That is, I contains a positive integer.

Let n be the least positive integer in I. By addition closure of rings, $(n) \subseteq I$. So we need only to show that $I \subseteq (n)$. Let $a \in I$. Then by the division algorithm there are $r, s \in \mathbb{Z}$ such that $a = rn + s$ and $0 \leq s < n$. But since n is the least positive element, we have $s = 0$. That is $a = rn$ and hence $a \in (n)$. Thus $I \subseteq (n)$ and therefore $I = (n)$.

Definition 3.2.2

An ideal P of a commutative ring R is a **prime** if $P \neq R$ and for all $a, b \in R$, $ab \in P$ implies that $a \in P$ or $b \in P$.

Definition 3.2.3

An ideal M of a ring R is a **maximal** if $M \neq R$ and there is no ideal I of R such that $M \subsetneqq I \subsetneqq R$.

Example 3.2.4

Let m and n be nonzero integers. Show that $(m) \subseteq (n)$ iff $n \mid m$.

Solution:

" $\Rightarrow$ ": Assume that $(m) \subseteq (n)$. Then $m \in (m) \subseteq (n)$ and hence $m \in (n)$. Thus, $m = nk$ for some $k \in \mathbb{Z}$. Therefore, $n \mid m$.

" $\Leftarrow$ ": Assume that $n \mid m$. Then $m = nk$ for some $k \in \mathbb{Z}$. Thus, $m \in (n)$ since (m) is the smallest ideal of $\mathbb{Z}$ containing m, we have $(m) \subseteq (n)$.

Example 3.2.5: #39.7 @*page* : 184

Show that if n is a positive integer, then (n) is a prime ideal of $\mathbb{Z}$ iff n is a prime.

Solution:

" $\Rightarrow$ ": Suppose that n is not a prime. Then there are $a, b \in \mathbb{Z}$ such that $ab = n$ where $1 < a, b < n$. Clearly, $ab \in (ab) = (n)$. Thus, $ab \mid ab$, but $ab \nmid a$ and $ab \nmid b$. Hence (ab) is not a prime ideal of $\mathbb{Z}$.

" $\Leftarrow$ ": Assume that n is a prime. If $ab \in (n)$, then $n \mid ab$ which implies that $n \mid a$ or $n \mid b$. That is $a \in (n)$ or $b \in (n)$. Therefore, (n) is a prime ideal of $\mathbb{Z}$.

Theorem 3.2.3

If F is a field, then every ideal of $F[x]$ is principal.

Proof:

Let I be an ideal of $F[x]$. If $I = \{0\}$, then $I = (0)$ and we are done. Otherwise, assume that $I \neq \{0\}$. Let $f(x)$ be a nonzero element of I of minimal degree. If the degree of $f(x)$ is 0 (constant element), then $f(x) \in F$ and is a unit (F is a field). Thus $I = F = (e)$. Assume that the degree of $f(x)$ is at least 1. Let $g(x) \in I$. Then by the Division Algorithm there are $q(x), r(x) \in F[x]$ such that $g(x) = f(x)q(x)+r(x)$ with $r(x) = 0$ or $\deg r(x) < \deg f(x)$. Since $g(x), f(x)q(x) \in I$, we have $r(x) = g(x) - f(x)q(x) \in I$ (ideal properties). But since $f(x)$ is of minimal degree in I, we get $r(x) = 0$ and hence $g(x) = f(x)q(x)$. Therefore, $I = (f(x))$.

Example 3.2.6

Determine all of the ideals of $\mathbb{Z}_6$, $\mathbb{Z}_9$, and $\mathbb{Z}_{12}$.

Solution:

Recall that all ideals of $\mathbb{Z}_n$ is principal. Thus for $\mathbb{Z}_6$ we have

$$(0) = 6\mathbb{Z}_6 = \{0\},$$
$$(1) = \mathbb{Z}_6 = (5), \text{ where } (5,6) = 1$$
$$(2) = 2\mathbb{Z}_6 = \{0,2,4\} = (4),$$
$$(3) = 3\mathbb{Z}_6 = \{0,3\}.$$

Note that $1, 2, 3$, and 6 are divisors of 6. While the divisors of 9 are $1, 3$, and 9 and hence for $\mathbb{Z}_9$ we have

$$(0) = 9\mathbb{Z}_9 = \{0\},$$
$$(1) = \mathbb{Z}_9 = (2) = (4) = (5) = (7) = (8), \text{ and}$$
$$(3) = 3\mathbb{Z}_9 = \{0,3,6\} = (6).$$

And the divisors of 12 are $1, 2, 3, 4, 6$, and 12. Thus the ideals of $\mathbb{Z}_{12}$ are:

$$(0) = 12\mathbb{Z}_{12} = \{0\},$$
$$(1) = \mathbb{Z}_{12} = (5) = (7) = (11),$$
$$(2) = 2\mathbb{Z}_{12} = \{0,2,4,6,8,10\} = (10),$$
$$(3) = 3\mathbb{Z}_{12} = \{0,3,6,9\} = (9),$$
$$(4) = 4\mathbb{Z}_{12} = \{0,4,8\} = (8), \text{ and}$$
$$(6) = 6\mathbb{Z}_{12} = \{0,6\}.$$

Exercise 3.2.1: #38.12 @*page* : 180

Show that every subring of $\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

Solution:

Let S be a subring of $\mathbb{Z}$. For any $s \in S$, $\sum_{i=1}^{n} s \in S$ (additive closure). But $\sum_{i=1}^{n} s = ns \in S$. Thus, S is an ideal of $\mathbb{Z}$.

Exercise 3.2.2: #38.13 @*page* : 180

Show that the constant polynomials in $\mathbb{Z}[x]$ form a subring that is not an ideal of $\mathbb{Z}[x]$.

Solution:

Clearly, constant polynomials in $\mathbb{Z}[x]$ is a subring since $\mathbb{Z}$ is a ring. Furthermore, 3 is a constant polynomial and $x \in \mathbb{Z}[x]$, but $3x$ is not a constant polynomial. Hence the constant polynomials is not an ideal of $\mathbb{Z}[x]$.

Exercise 3.2.3: #38.14 @*page* : 181

Show that if R is a commutative ring with unity e, and $a \in R$, then (a) is the smallest ideal of R containing a.

Solution:

Let I be any ideal of R containing a. We prove that $(a) \subseteq I$. Let $b \in (a)$. Then there is $r \in R$ such that $b = ar$, but $ar \in I$ since $a \in I$. Hence $ar = b \in I$. That is $(a) \subseteq I$.

Exercise 3.2.4: Non-principal ideal #38.18 @*page* : 181

Let I denote the set of all polynomials in $\mathbb{Z}[x]$ that have an even number as the constant term.

1. Show that I is an ideal of $\mathbb{Z}[x]$.
2. Show that I is not a princial ideal of $\mathbb{Z}[x]$.

Solution:

1. Clearly $0 \in I$ so I is not empty. If $r = 2a_0 + a_1x + \cdots, s = 2b_0 + b_1x + \cdots \in I$, then $-s \in I$ since $-2b_0$ is an even number and hence $r - s = 2(a_0 - b_0) + \cdots \in I$. Also,

Let $f(x) = 2a_0 + a_1x + \cdots \in I$ and $g(x) = b_0 + b_1x + \cdots \in \mathbb{Z}[x]$. Then $f(x)g(x) = c_0 + c_1x + c_2x^2 + \cdots$, where $c_0 = 2a_0b_0$ which is even. Thus $f(x)g(x) \in I$. Thus I is an ideal of $\mathbb{Z}[x]$.

2. Note that $f(x) = x + 2$ and $g(x) = x + 4$ are two irreducible polynomials in $\mathbb{Z}[x]$ and they are both contained in I. Assume that $I = (a)$ for some nonzero $a \in \mathbb{Z}[x]$. Then both $f(x)$ and $g(x)$ are multiples of a. But since $(f(x), g(x)) = 1$, we have $f(x) \cdot u + g(x) \cdot v = 1 \in (a)$, for any $u, v \in \mathbb{Z}[x]$. But clearly $1 \notin I$. Therefore, I cannot be a principal ideal.

Exercise 3.2.5

If R is a commutative ring and $a \in R$, show that $I_a = \{x \in R : ax = 0\}$ is an ideal of R.

Solution:

Clearly, $a0 = 0 \in I_a$ implies that I_a is not empty. For $x, y \in I_a$, we have $ax = ay = 0$. Hence $a(x - y) = 0$. Thus, $x - y \in I_a$. Further $a(xy) = (ax)y = 0y = 0$ implies that $xy \in I_a$. Therefore, I_a is a subring of R. Let $r \in R$ and $x \in I_a$. Then $ax = 0$, and hence $a(xr) = (ax)r = 0$. Thus $xr \in I_a$. As R is commutative, we get $rx \in I_a$. Therefore I_a is an ideal of R.

Exercise 3.2.6

Given the set $S = \left\{ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} : x, y, z \in \mathbb{Z} \right\}$ is a ring with respect to matrix addition and multiplication. Show that $I = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in \mathbb{Z} \right\}$ is an ideal of S.

Solution:

Clearly $I \neq \phi$ as the zero matrix $O \in I$. Let $A = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}, B = \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} \in I$. Then

$$A - B = \begin{pmatrix} a - c & b - d \\ 0 & 0 \end{pmatrix} \in I, \text{ and } AB = \begin{pmatrix} ac & ad \\ 0 & 0 \end{pmatrix} \in I.$$

Thus I is a subring of S. If $C = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \in S$ and $A = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in I$, then

$$AC = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} ax & ay + bz \\ 0 & 0 \end{pmatrix} \in I, \text{ and}$$

$$CA = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ax & bx \\ 0 & 0 \end{pmatrix} \in I.$$

Therefore, I is an ideal of S.

Exercise 3.2.7

Show that the set of all nilpotent elements in a commutative ring R forms an ideal of R.

Solution:

Let $I = \{a \in R : a^n = 0 \text{ for some } n \in \mathbb{N}\}$. Clearly $I \neq \phi$ since $0^1 = 0 \in I$. Let $a, b \in I$. Then $a^n = 0$ and $b^m = 0$ for some $n, m \in \mathbb{N}$. Using the Bionomial Theorem (R is commutative), we have

$$(a-b)^{n+m} = \sum_{k=0}^{n+m} c_k a^k (-b)^{n+m-k}, \quad \text{where } c_k \in \mathbb{Z}.$$

If $k \geq n$, then $a^k = 0$ and hence $c_k a^k (-b)^{n+m-k} = 0$. If otherwise $k < n$, then $n + m - k \geq m$ and hence $c_k a^k (-b)^{n+m-k} = 0$ since $b^{n+m-k} = 0$. Thus, $a - b \in I$. Further $(ab)^n = a^n b^n = 0b^n = 0$ and hence $ab \in I$. Therefore, I is a subring of R.

Let $r \in R$, then $(ar)^n = a^n r^n = 0r^n = 0$. That is $ar \in I$, and by commutativity, we get $ra \in I$. Therefore, I is an ideal of R.

Exercise 3.2.8

Let R be a commutative ring with unity and that I is an ideal of R. Show that $S = \{a \in R : a^n \in I, \text{ for some } n \in \mathbb{N}\}$ is an ideal of R.

Solution:

Clearly $0^1 = 0 \in I$ and hence $0 \in S \neq \phi$. Let $a, b \in S$. Then $a^n, b^m \in I$ for some $n, m \in \mathbb{N}$. Using the Bionomial Theorem (R is commutative), we have

$$(a-b)^{n+m} = \sum_{k=0}^{n+m} c_k a^k (-b)^{n+m-k}, \quad \text{where } c_k \in \mathbb{Z}.$$

If $k \geq n$, then $a^k = a^n a^{k-n} \in I$ since I is an ideal and $a^n \in I$. Thus $c_k a^k (-b)^{n+m-k} \in I$. If otherwise $k < n$, then $n+m-k \geq m$ and hence $c_k a^k (-b)^{n+m-k} \in I$ since $b^{n+m-k} = b^m b^{n-k} \in I$. Thus, $(a-b)^{n+m} \in I$ and hence $a - b \in S$. Further $(ab)^n = a^n b^n \in I$ since $a^n \in I$. Therefore, $ab \in S$. Therefore, S is a subring of R.

Let $r \in R$ and $a \in S$, then $(ar)^n = a^n r^n \in I$ since $a^n \in I$ and I is an ideal. That is $ar \in S$, and by commutativity, we get $ra \in S$. Therefore, S is an ideal of R.

Exercise 3.2.9: #38.20 @*page* : 181

Prove that if F is a field, R is a ring, and $\theta : F \to R$ is a ring homomorphism, then either θ is one-to-one or $\theta(a) = 0$ for all $a \in F$.

Solution:

Note that $\ker \theta$ is an ideal of F. An ideal of a field is either $\{0\}$ or F. If $\ker \theta = \{0\}$, then θ is one-to-one. Otherwise, $\ker \theta = F$ and hence $a \in \ker \theta$ for all $a \in F$. Thus, $\theta(a) = 0$ for all $a \in F$.

Section 3.3: Quotient Rings

Remark 3.3.1

If I is an ideal of a ring R, then I is a normal subgroup of the additive group of R. This is because the additive group of R is abelian by definition of rings.

Theorem 3.3.1

Let I be an ideal of a ring R, and let R/I denote the set of all left cosets of I considered as a subgroup of the additive subgroup of R. For $a+I, b+I \in R/I$, for any $a, b \in R$ let

$$(a+I)+(b+I)=(a+b)+I, \qquad \text{and} \qquad (a+I)(b+I)=ab+I.$$

With these operations, R/I is a ring. This ring is called the **quotient ring of R by I**.

Proof:

From Math-261, R/I is an abelian (quotient) group. Now let $a+I, b+I, c+I \in R/I$, then

$$\begin{aligned}[(a+I)(b+I)](c+I) &= (ab+I)(c+I) = (ab)c+I = a(bc)+I \\ &= (a+I)+(bc+I) = (a+I)[(b+I)(c+I)].\end{aligned}$$

Thus, multiplication is associative on R/I. Moreover,

$$\begin{aligned}(a+I)[(b+I)+(c+I)] &= (a+I)[(b+c)+I] = a(b+c)+I = (ab+ac)+I \\ &= (ab+I)+(ac+I) = (a+I)(b+I)+(a+I)(c+I).\end{aligned}$$

Thus, the left distribution law is satisfied. The proof of right distribution law is similar. Therefore R/I is ring.

Theorem 3.3.2

Let R be a ring and I be an ideal of R. Then,

1. If R is commutative, then R/I is commutative.
2. If e is the unity of R, then $e+I$ is the unity of R/I.

Example 3.3.1: #39.6 @*page* : 183

Show that if I is an ideal of a ring R, then R/I is commutative iff $ab-ba \in I$ for all $a, b \in R$.

Solution:

Let $a, b \in R$ and $a+I, b+I \in R/I$. Then,

$$\begin{aligned}(a+I)(b+I) = (b+I)(a+I) &\text{ iff } ab+I = ba+I \\ &\text{iff } (ab+I)-(ba+I) = 0+I \\ &\text{iff } (ab-ba)+I = 0+I = I \\ &\text{iff } ab-ba \in I.\end{aligned}$$

Theorem 3.3.3

If R is a ring and I is an ideal of R, then the mapping $\theta : R \to R/I$ defined by $\theta(a) = a+I$, for each $a \in R$, is a homomorphism of R onto R/I, and $\ker\theta = I$.

Proof:

For any $a, b \in R$, we have:

- $\theta(a+b) = (a+b)+I = (a+I)+(b+I) = \theta(a)+\theta(b)$.
- $\theta(ab) = ab+I = (a+I)(b+I) = \theta(a)\theta(b)$.

Therefore, θ is a homomorphism, and for any $a+I \in R/I$, we have $a \in R$ with $\theta(a) = a+I$. Thus θ is a homomorphism onto R/I. To show that $\ker\theta = I$, note that

$$a \in \ker\theta \text{ iff } \theta(a) = 0+I \text{ iff } a+I = 0+I = I \text{ iff } a \in I.$$

Theorem 3.3.4: The Fundamental Homomorphism Theorem For Rings

Let R and S be rings, and let $\theta : R \to S$ be a homomorphism from R onto S with $\ker\theta = I$. Then the mapping $\phi : R/I \to S$ defined by

$$\phi(a+I) = \theta(a), \quad \text{for each } a+I \in R/I$$

is an isomorphism of R/I onto S. Therefore, $R/I \approx S$.

Theorem 3.3.5

Let R be a commutative ring with unity. Then:

1. If $M \neq R$ is an ideal of R, then M is maximal iff R/M is a field.
2. If $P \neq R$ is an ideal of R, then P is prime iff R/P is an integral domain.
3. Every maximal ideal of R is a prime ideal of R.

Proof:

1. " $\Rightarrow$ ": Let M be a maximal ideal of R. We show that if $a+M \in R/M$ is a nonzero element, then it has a multiplicative inverse $b+M$ such that $(a+M)(b+M) = e+M$. Note that $a+M \neq 0+M$ iff $a \notin M$. Let $J = \{r+ax : r \in M \text{ and } x \in R\}$ be an ideal of R that contains properly M. But since M is maximal, we have $J = R$ and hence $e \in J$. Therefore, $e = r+ab$ for some $r \in M$ and $b \in R$. Thus

$$(a+M)(b+M) - (e+M) = (ab-e) + M = (-r) + M = M = 0+M.$$

That is $(a+M)(b+M) = e+M$. Therefore, R/M is a field.
" $\Leftarrow$ ": Suppose R/M is a field and $M \subsetneq J$ for some ideal J. We need to show $J = R$. As $J \neq M$, there is some $a \in J - M$. Then clearly $a \neq 0$ since $0 \in M$. As R/M is a field, there is $b \in R$ such that $(a+M)(b+M) = e+M = (b+M)(a+M)$. Thus, $ab+M = e+M$. That is $ab-e \in M$. But then $ab \in J$ and $ab-e \in M \subset J$ implies that $e = ab-(ab-e) \in J$. Therefore, $J = R$ which implies that M is maximal.
2. We note that the zero of R/P is $0+P = P$. Then R/P is an integral domain iff $(a+P)(b+P) = 0+P$ implies $a+P = P$ or $b+P = P$ iff $ab+P = P$ implies $a+P = P$ or $b+P = P$ iff $ab \in P$ implies $a \in P$ or $b \in P$ iff P is a prime ideal of R.
3. Assume that M is a maximal ideal of R. Then R/M is a field and hence it is an integral domain. Therefore, M is a prime ideal of R.

Example 3.3.2

What are prime and maximal ideals of $\mathbb{Z}_6$ and $\mathbb{Z}_{12}$.

Solution:

Note that a finite integral domain is a field. Thus the maximal and the prime ideals are the same.

For $\mathbb{Z}_6$, we have $(2) = \{0, 2, 4\}$ and $(3) = \{0, 3\}$ are both prime and maximal ideals, because the corresponding factor rings, namely $\mathbb{Z}_6 / (2)$ and $\mathbb{Z}_6 / (3)$, are isomorphic to the fields $\mathbb{Z}_2$ and $\mathbb{Z}_3$.

For $\mathbb{Z}_{12}$, we have $(2) = \{0, 2, 4, 6, 8, 10\}$ and $(3) = \{0, 3, 6, 9\}$ are both prime and maximal ideals, because the corresponding factor rings, namely $\mathbb{Z}_{12} / (2)$ and $\mathbb{Z}_{12} / (3)$, are isomorphic to the fields $\mathbb{Z}_2$ and $\mathbb{Z}_3$.

Exercise 3.3.1

Show that if R is a finite commutative ring with unity, then every prime ideal in R is maximal.

Solution:

Let P be a prime ideal of R. Then R/P is a "finite" integral domain and hence it is a field. Therefore, P is maximal.

Exercise 3.3.2

Consider the ring $R = \mathbb{Z}[x]$ and let $I = (x) = \{xf(x) : f(x) \in R\}$ be an ideal of R. Show that $R/I \approx \mathbb{Z}$.

Hint: Use the Fundamental Homomorphism Theorem For Rings with $\theta : R \to \mathbb{Z}$ defined by $\theta(a_n x^n + \cdots + a_0) = a_0$.

Solution:

Note that for any $f(x), g(x) \in R$, $f(x) - g(x) \in I$ iff $f(x)$ and $g(x)$ have the same constant term. We use the Fundamental Homomorphism Theorem For Rings: Let $\theta : R \to \mathbb{Z}$ defined by $\theta(a_n x^n + \cdots + a_0) = a_0$. Let $f(x) = a_n x^n + \cdots + a_0, g(x) = b_m x^m + \cdots + b_0 \in R$. Then

- $\theta(f(x) + g(x)) = \theta(c_l x^l + \cdots + c_0) = c_0 = a_0 + b_0 = \theta(f(x)) + \theta(g(x))$, and
- $\theta(f(x)g(x)) = \theta(d_k x^k + \cdots + d_0) = d_0 = a_0 b_0 = \theta(f(x))\theta(g(x))$,

where we only focus on the constant terms in the addition and multiplication of $f(x)$ and $g(x)$. Therefore, θ is a ring homomorphism. We now prove that θ is onto $\mathbb{Z}$. Let $a \in \mathbb{Z}$. Then $f(x) = a_n x^n + \cdots + a \in R$ with $\theta(f(x)) = a$. Thus θ is onto $\mathbb{Z}$.

We now show that $\ker\theta = I$. Clearly,

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \ker\theta \text{ iff } \theta(f(x)) = 0 \text{ iff } a_0 = 0$$
$$\text{iff } f(x) = x(a_n x^{n-1} + \cdots + a_1) \text{ iff } f(x) \in I.$$

Thus, $\ker\theta = I$. By the Fundamental Homomorphism Theorem For Rings, we have $R/I \approx \mathbb{Z}$.

Exercise 3.3.3: Part of #39.9 @*page* : 184

Let I and J be two ideals of a ring R, and define $I + J = \{a + b : a \in I \text{ and } b \in J\}$. Then

1. Show that $I + J$ is an ideal of R containing each of I and J.
2. Show that I (or equivalently J) is an ideal of $I + J$.
3. Show that $I \cap J$ is an ideal of I (or equivalently J).
4. Show that if $J \subseteq I$, then $I \,/\, J$ is an ideal of $R \,/\, J$.
5. **The First Isomorphism Theorem For Rings**: Show that $I \,/\, (I \cap J) \approx (I + J) \,/\, J$.
6. **The Second Isomorphism Theorem For Rings**: Show that if $J \subseteq I$, then $I \,/\, J$ is an ideal of $R \,/\, J$, and $(R \,/\, J) \,/\, (I \,/\, J) \approx R \,/\, I$.

Solution:

1. Clearly, $0 = 0+0 \in I+J$ and hence $I+J$ is not empty. Let $x, y \in I+J$. Then $x = a_1+b_1$ and $y = a_2 + b_2$, where $a_1, a_2 \in I$ and $b_1, b_2 \in J$. Then $x - y = (a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2) \in I + J$.
   Finally for any $r \in R$, $(a + b)r = ar + br \in I + J$ as $ar \in I$ and $br \in J$. Note that for any $a \in I$, $a = a + 0 \in I + J$ and hence $I \subseteq I + J$. In a similar way, $J \subseteq I + J$.
2. Part (1) implies that I is a subring of $I + J$. Further if $a \in I$ and $x \in I + J \subseteq R$, then $ax, xa \in I$ since I is an ideal of R.
3. If I and J are subrings of R, then so is $I \cap J$. Moreover, $I \cap J \subseteq I$ and hence $I \cap J$ is a subring of I. Let $x \in I \cap J \subseteq R$ and $a \in I$. Then clearly $ax, xa \in I$ (I is an ideal of R).
4. Clearly, $I \,/\, J$ and $R \,/\, J$ are both rings and $I \,/\, J = \{i + J : i \in I\} \subseteq R \,/\, J$. Thus, $I \,/\, J$ is a subring of $R \,/\, J$. Moreover, if $r + J \in R \,/\, J$ and $a + J \in I \,/\, J$. Then $(r + J)(a + J) = ra + J$ with $ra \in I$ as it is an ideal of R. Therefore, $ra + J \in I \,/\, J$. The proof of $(a + J)(r + J) \in I \,/\, J$ is similar. Therefore, $I \,/\, J$ is an ideal of $R \,/\, J$.
5. We simply show the statement using the Fundamental Theorem for Ring Homomorphism. Let $\theta : I \to (I + J) \,/\, J$, defined by $\theta(a) = a + J$ for any $a \in I$. Let $a, b \in I$. Then
   - $\theta(a + b) = (a + b) + J = (a + J) + (b + J) = \theta(a) + \theta(b)$, and
   - $\theta(ab) = (ab) + J = (a + J)(b + J) = \theta(a)\theta(b)$.

   Therefore, θ is a ring homomorphism. We now prove that θ is onto. Assume that $x + J \in (I + J) \,/\, J$. Then, $x = a + b \in I + J$ for some $a \in I$ and $b \in J$. That is,

$\theta(a) = a + J = a + (b + J) = (a + b) + J = x + J$. Therefore, θ is onto homomorphism. We now prove that $\ker\theta = I \cap J$. For any $a \in I$, we have

$$a \in \ker\theta \text{ iff } \theta(a) = 0 + J \text{ iff } a + J = 0 + J \text{ iff } a \in J \text{ iff } a \in I \cap J.$$

Thus, $\ker\theta = I \cap J$. By the Fundamental Theorem of ring homomorphism, we have $I \,/\, (I \cap J) \approx (I + J) \,/\, J$.

6. We first show that $I \,/\, J$ is an ideal of $R \,/\, J$. Clearly, $I \,/\, J$ and $R \,/\, J$ are both rings and $I \,/\, J = \{i + J : i \in I\} \subseteq R \,/\, J$. Thus, $I \,/\, J$ is a subring of $R \,/\, J$. Moreover, if $r + J \in R \,/\, J$ and $a + J \in I \,/\, J$. Then $(r + J)(a + J) = ra + J$ with $ra \in I$ as it is an ideal of R. Therefore, $ra + J \in I \,/\, J$. The proof of $(a + J)(r + J) \in I \,/\, J$ is similar. Therefore, $I \,/\, J$ is an ideal of $R \,/\, J$.

   We now show the isomorphism part of the statement. Let $\theta : R \,/\, J \to R \,/\, I$, defined by $\theta(r + J) = r + I$ for any $r \in R$. Let $a, b \in R$ so that $a + J, b + J \in R \,/\, J$. Then:

   - $\theta((a + J) + (b + J)) = \theta((a + b) + J) = (a + b) + I = (a + I) + (b + I) = \theta(a + J) + \theta(b + J)$, and
   - $\theta((a + J)(b + J)) = \theta((ab) + J) = (ab) + I = (a + I)(b + I) = \theta(a + J)\theta(b + J)$.

   Therefore, θ is a ring homomorphism. We now prove that θ is onto. Assume that $r + I \in R \,/\, I$ for some $r \in R$. That is, $\theta(r + J) = r + I$, and hence θ is onto homomorphism. We now prove that $\ker\theta = I \,/\, J$.

$$a + J \in \ker\theta \text{ iff } \theta(a + J) = 0 + I \text{ iff } a + I = 0 + I \text{ iff } a \in I \text{ iff } a + J \in I \,/\, J.$$

   Thus, $\ker\theta = I \,/\, J$. By the Fundamental Theorem of ring homomorphism, we have $(R \,/\, J) \,/\, (I \,/\, J) \approx R \,/\, I$.

Section 3.4: Quotient Rings of F[x]

Theorem 3.4.1

For a field F an ideal $I = (p(x)) \neq \{0\}$ of $F[x]$ is maximal iff $p(x)$ is irreducible in $F[x]$.

Proof:

" $\Rightarrow$ ": Since I is a maximal ideal of $F[x]$, it is a prime ideal. If $p(x) = f(x)g(x)$ is a factorization of $p(x)$ in $F[x]$. Then either $f(x) \in I$ or $g(x) \in I$. Thus either $f(x)$ a multiple of $p(x)$ or $g(x)$ is a multiple of $p(x)$. But then we cannot have the degrees of both $f(x)$ and $g(x)$ less than the degree of $p(x)$. Therefore no such factorization exist and hence $p(x)$ is irreducible in $F[x]$.

" $\Leftarrow$ ": Assume that $p(x)$ is irreducible over F. Let N be an ideal so that $I \subseteq N \subseteq F[x]$. Now N is a principal ideal of $F[x]$ (Since F is a field). Thus $N = (g(x))$ for some $g(x) \in N$. Then $p(x) \in N$ implies that $p(x) = g(x)q(x)$ for some $q(x) \in F[x]$. But since $p(x)$ is irreducible, we must have either $g(x)$ or $q(x)$ is of degree 0. If $\deg g(x) = 0$, then it is a nonzero constant (unit) in F and hence $(g(x)) = N = F[x]$. If $\deg q(x) = 0$, then $q(x) = c$ and hence $g(x) = c^{-1}p(x) \in (p(x))$. So $(p(x)) = N$. Therefore, it is not possible to have $I \subseteq N \subseteq F[x]$. Thus $(p(x))$ is maximal ideal of $F[x]$.

Theorem 3.4.2

If F is a field and $I = (p(x))$ is a nonzero element in $F[x]$, then $F[x] / I$ is a field iff $(p(x))$ is maximal of $F[x]$ iff $p(x)$ is irreducible over F.

Example 3.4.1

Find all $c \in \mathbb{Z}_3$ such that $\mathbb{Z}_3[x] / (x^2 + c)$ is a field.

Solution:

Simply $\mathbb{Z}_3[x] / (x^2 + c)$ is a field iff $x^2 + c$ is irreducible over $\mathbb{Z}_3$. Let $f(x) = x^2 \in \mathbb{Z}_3[x]$. Then $f(0) = 0$, $f(1) = 1$, and $f(2) = 1$. We need to find a value for $c \in \mathbb{Z}_3$ so that $0 + c$ and $1 + c$ are both nonzero. Therefore $c = 1$.

Example 3.4.2

Find all $c \in \mathbb{Z}_3$ such that $\mathbb{Z}_3[x] / (x^3 + cx^2 + 1)$ is a field.

Solution:

Simply $\mathbb{Z}_3[x] / (x^3 + cx^2 + 1)$ is a field iff $f(x) = x^3 + cx^2 + 1$ is irreducible over $\mathbb{Z}_3$. If $c = 0$, then $f(2) = 0$ and when $c = 1$, then $f(1) = 0$. But if $c = 2$, we get $f(x) = x^3 + 2x + 1$ with no zeros. Thus $c = 2$ is the only choice.

Theorem 3.4.3

Assume that F is a field, $p(x)$ is a polynomial of degree n over F, and $I = (p(x))$ is an ideal of $F[x]$. Then each element of $F[x] / I$ can be expressed uniquely in the form

$$(b_0 + b_1 x + \cdots + b_{n-1} x^{n-1}) + I, \qquad \text{with } b_0, b_1, \cdots, b_{n-1} \in F. \tag{3.4.1}$$

Moreover, $\{b + I : b \in F\}$ is a subfield of $F[x] / I$ isomorphic to F.

Proof:

If $f(x) + I \in F[x] / I$, then by the Division Algorithm, $f(x) = p(x)q(x) + r(x)$ for some $q(x), r(x) \in F[x]$ with $r(x) = 0$ or $\deg r(x) < \deg p(x)$. Thus, $f(x) - r(x) = p(x)q(x) \in I$, and hence $f(x) + I = r(x) + I$. Therefore, each element of $F[x] / I$ can be expressed in at least one way in the form (3.4.1).

On the other hand, if

$$(b_0 + b_1 x + \cdots b_{n-1} x^{n-1}) + I = (c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}) + I,$$

then

$$(b_0 - c_0) + (b_1 - c_1)x + \cdots + (b_{n-1} - c_{n-1})x^{n-1} \in I,$$

so that $p(x)$ divides $(b_0 - c_0) + \cdots + (b_{n-1} - c_{n-1})x^{n-1}$. But since $\deg p(x) = n > n - 1$, we have $(b_0 - c_0) + \cdots + (b_{n-1} - c_{n-1})x^{n-1} = 0$. Therefore, $b_0 = c_0, b_1 = c_1, \cdots, b_{n-1} = c_{n-1}$. This proves uniqueness.

Let $\theta : F \to E$, defined by $\theta(b) = b + I$, where $E = \{b + I : b \in F\}$, where b is a polynomial of degree at most $n - 1$. Clearly, θ is onto homomorphism. Also θ is one-to-one as it is proved above. Therefore, θ is an isomorphism and then $E \approx F$.

Remark 3.4.1

The proof of the previous Theorem shows that if $f(x) \in F[x]$, and if $f(x) = p(x)q(x) + r(x)$ with $r(x) = 0$ or $\deg r(x) < \deg p(x)$, then $f(x) + I = r(x) + I$. This allows us to represent elements of $F[x] / (p(x))$ by polynomials of degree less than $\deg p(x)$.

Example 3.4.3

Construct the field $\mathbb{C}$ from the field $\mathbb{R}$. **Or**: Let $I = (1 + x^2)$. Show that $\mathbb{R}[x] / I \approx \mathbb{C}$.

Solution:

Let $p(x) = 1 + x^2$ and $I = (p(x))$. Note that $p(x)$ is irreducible over $\mathbb{R}$ and hence $\mathbb{R}[x] / I$ is a field. By Theorem 3.4.3, each element of $\mathbb{R}[x] / I$ can be written uniquely as $(a + bx) + I$ with $a, b \in \mathbb{R}$.

Define $\theta : \mathbb{R}[x] / I \to \mathbb{C}$ by $\theta((a + bx) + I) = a + bi$. Then we show that θ an isomorphism:

- θ is 1-1: Let $\theta((a + bx) + I) = \theta((c + dx) + I)$. Then $a + bi = c + di$ which implies that $a = c$ and $b = d$. Thus, $a + bx = c + dx$ and hence the result.
- θ is onto: For any $a + bi \in \mathbb{C}$, $a, b \in \mathbb{R}$ with $\theta((a + bx) + I) = a + bi$. Thus, θ is onto.
- θ is homomorphism: Let $(a + bx) + I, (c + dx) + I \in \mathbb{R}[x] / I$. Then:

$$\begin{aligned}\theta((a + bx) + I + (c + dx) + I) &= \theta(((a + c) + (b + d)x) + I) = (a + c) + (b + d)i \\ &= (a + bi) + (c + di) \\ &= \theta((a + bx) + I) + \theta((c + dx) + I).\end{aligned}$$

For multiplication, we have:

$$\theta(((a + bx) + I)((c + dx) + I)) = \theta((ac + (ad + bc)x + (bd)x^2) + I).$$

So, we use Theorem 3.4.3 to represent $(ac + (ad + bc)x + (bd)x^2) + I$ as $(u + vx) + I$. We use long division to get: $ac + (ad + bc)x + (bd)x^2 = (1 + x^2)bd + (ac - bd) + (ad + bc)x$. So that $u + vx = (ac - bd) + (ad + bc)x$. Thus,

$$\begin{aligned}\theta(((a + bx) + I)((c + dx) + I)) &= \theta((ac + (ad + bc)x + (bdx^2) + I) \\ &= \theta(((ac - bd) + (ad + bc)x) + I) = (ac - bd) + (ad + bc)i \\ &= (a + bi)(c + di) = \theta((a + bx) + I)\theta((c + dx) + I).\end{aligned}$$

Therefore, θ is an isomorphism and hence $\mathbb{R}[x] / I \approx \mathbb{C}$.

Example 3.4.4

Show that if F is a field, then every proper nontrivial prime ideal of $F[x]$ is maximal.

Solution:

Recall that every ideal of $F[x]$ is principal. Let $(f(x)) \neq \{0\}$ be a proper prime ideal of $F[x]$. Then every polynomial in $(f(x))$ is of degree greater than or equal to degree of $f(x)$. Thus if $f(x) = g(x)h(x) \in F[x]$ where $\deg g(x)$ and $\deg h(x)$ are less than $\deg f(x)$, then neither $g(x)$ nor $h(x)$ can be in $(f(x))$. But this contradict the definition of prime ideals. Therefore, no factorization of $f(x)$ in $F[x]$ can exist. That is $f(x)$ is irreducible in $F[x]$. Therefore, $(f(x))$ is maximal ideal in $F[x]$.

Exercise 3.4.1: #40.1 @*page* : 187

Show that if F is a field with unity e, and I is an ideal of $F[x]$, then $F[x]\,/\,I$ is commutative with unity $e + I$.

Solution:

Clearly, F is a field and hence F is commutative. Thus $F[x]$ is commutative and hence $F[x]\,/\,I$ is also commutative. For any $a + I \in F[x]\,/\,I$, we have

$$(a + I)(e + I) = ae + I = a + I = ea + I = (e + I)(a + I).$$

Therefore, $e + I$ is a unity of $F[x]\,/\,I$.

Exercise 3.4.2: #40.2 @*page* : 187

Prove that if F is a field and $f(x), p(x) \in F[x]$, with $p(x)$ is irreducible and $p(x) \nmid f(x)$, then $(p(x), f(x)) = e$, the unity of F.

Solution:

Let $d(x) = (p(x), f(x))$. Then $d(x) \mid p(x)$ and $d(x) \mid f(x)$. But since $p(x)$ is irreducible polynomial, $d(x)$ is either an associate of e or an associate of $p(x)$. Since $p(x) \nmid f(x)$, $d(x)$ is not associate of $p(x)$. Therefore, $d(x)$ is an associate of e. Thus, $(p(x), f(x)) = e$.

Exercise 3.4.3: #40.5 @*page* : 187

Prove that if F is a subfield of a field E, $c \in E$, then $\theta : F[x] \to E$ defined by $\theta(f(x)) = f(c)$ is a homomorphism.

Solution:

Let $f(x), g(x) \in F[x]$, then

$$\theta(f(x) + g(x)) = \theta((f + g)(x)) = (f + g)(c) = f(c) + g(c) = \theta(f(x)) + \theta(g(x)), \text{ and}$$
$$\theta(f(x)g(x)) = \theta((fg)(x)) = (fg)(c) = f(c)g(c) = \theta(f(x))\theta(g(x)).$$

Exercise 3.4.4: #40.11 @*page* : 187

Suppose that F is a field and $f(x), g(x) \in F[x]$. Show that $(f(x)) = (g(x))$ iff $f(x)$ and $g(x)$ are associates.

Solution:

" $\Rightarrow$ ": Assume that $(f(x)) = (g(x))$. Clearly $f(x) \in (g(x))$ and $g(x) \in (f(x))$. Then there are $q(x), r(x) \in F[x]$ such that $g(x) = f(x)q(x)$ and $f(x) = g(x)r(x)$. Hence $f(x) \mid g(x)$ and $g(x) \mid f(x)$. Therefore, $f(x)$ and $g(x)$ are associates.

" $\Leftarrow$ ": Assume that $f(x)$ and $g(x)$ are associates. Then $f(x) = c\,g(x)$ for some $c \in F$. Hence $f(x) \in (g(x))$ which implies that $(f(x)) \subseteq (g(x))$. Similarly, $(g(x)) \subseteq (f(x))$ and hence $(f(x)) = (g(x))$.

Exercise 3.4.5

Find all $c \in \mathbb{Z}_3$ such that $\mathbb{Z}_3[x] \,/\, (x^3 + x^2 + c)$ is a field.

Solution:

Simply $\mathbb{Z}_3[x] \,/\, (x^3 + x^2 + c)$ is a field iff $x^3 + x^2 + c$ is irreducible over $\mathbb{Z}_3$. Let $f(x) = x^3 + x^2 \in \mathbb{Z}_3[x]$. Then $f(0) = 0$, $f(1) = 2$, and $f(2) = 0$. We need to find a value for $c \in \mathbb{Z}_3$ so that $0 + c$ and $2 + c$ are both nonzero. Therefore $c = 2$.

Exercise 3.4.6

Find all $c \in \mathbb{Z}_5$ such that $\mathbb{Z}_5[x] \,/\, (x^2 + x + c)$ is a field.

Solution:

Simply $\mathbb{Z}_5[x] \,/\, (x^2 + x + c)$ is a field iff $x^2 + x + c$ is irreducible over $\mathbb{Z}_5$. Let $f(x) = x^2 + x \in \mathbb{Z}_5[x]$. Then $f(0) = 0$, $f(1) = 2$, $f(2) = 1$, $f(3) = 2$, and $f(4) = 0$. We need to find a value for $c \in \mathbb{Z}_5$ so that $0 + c$, $1 + c$ and $2 + c$ are all nonzero. Therefore c can be either 1 or 2.

Exercise 3.4.7

Find all $c \in \mathbb{Z}_5$ such that $\mathbb{Z}_5[x] \,/\, (x^2 + cx + 1)$ is a field.

Solution:

Simply $\mathbb{Z}_5[x]\,/\,(x^2+cx+1)$ is a field iff $f(x)=x^2+cx+1$ is irreducible over $\mathbb{Z}_5$. If $c=0$, then $f(2)=0$; when $c=1$, then $f(x)$ has no zeros; when $c=2$, then $f(-1)=0$; when $c=3$, then $f(1)=0$; and when $c=4$, then $f(x)$ has no zeros. Therefore, c can be either 1 or 4.

Chapter

4 Field Extension

Section 4.1: Adjoining Roots

Definition 4.1.1

A field E is called an **extension** of a field F, if E contains a subfield isomorphic to F. Often, F is thought of as actually being a subfield of E. Further, Any field is an extension of itself.

For instance, $\mathbb{R}$ is an extension of $\mathbb{Q}$, and $\mathbb{C}$ is an extension of both $\mathbb{R}$ and $\mathbb{Q}$.

Theorem 4.1.1

Let F be a field and let $f(x)$ be a nonconstant polynomial in $F[x]$. Then there exists an extension field E of F and an $a \in E$ such that $f(a) = 0$.

Let E be an extension of a field F. Assume that $F \subseteq E$. Let S be a subset of E. Then there is at least one subfield of E containing both F and S, namely E. Let $F(S)$ denote the intersection of all subfields of E containing both F and S. Then $F(S)$ is a subfield of E. Moreover, if $S \subseteq F$, then $F(S) = F$.

If $S = \{a_1, a_2, \cdots, a_n\}$, then $F(a_1, a_2, \cdots, a_n)$ denotes $F(S)$. For example, $\mathbb{R}(i) = \mathbb{C}$. In other-words, $F(S)$ consists of all the element in E that can be obtained from F and S by repeated addition, multiplication, and taking additive and multiplicative inverses in E. If $E = F(a)$ for some $a \in E$, then E is said to be a **simple extension** of F.

Definition 4.1.2

An element a of an extension field E of a field F is **algebraic over** F if $f(a) = 0$ for some nonzero $f(x) \in F[x]$. If a is not algebraic over F, then a is **transcendental over** F.
The extension field E of F is called a **simple extension** of F if $E = F(a)$ for some $a \in E$. If a is algebraic over F, then E is called a **simple algebraic extension** of F. Further, E is called an **algebraic extension** of F if every element in E is algebraic over F.

Theorem 4.1.2

If E is an extension field of a field F, with $E = F(a)$ and a algebraic over F, then there is a unique (up to a constant factor in F) irreducible nonconstant polynomial of minimal degree $p(x)$ in $F[x]$ having a as a root. That is

$$E \approx F[x] / (p(x)),$$

Moreover, if $f(a) = 0$ for a nonzero $f(x) \in F[x]$, then $p(x)$ divides $f(x)$.

Definition 4.1.3

Let E be an extension field of a field F, and let $a \in E$ be algebraic over F. The unique monic polynomial $p(x)$ having the property described in Theorem 4.1.2 is called the **irreducible polynomial for** a **over** F and will be denoted by $irr(a, F)$. The **degree of** $irr(a, F)$ is the degree of a over F, denoted by $\deg(a, F)$.

Remark 4.1.1

Theorem 3.4.3 states that if F is a field and $p(x) \in F[x]$ is irreducible over F, then each element of $F[x] / (p(x))$ can be expressed uniquely in the form

$$(b_0 + b_1 x + \cdots + b_{n-1}x^{n-1}) + I, \quad \text{with } b_0, b_1, \cdots, b_{n-1} \in F. \tag{4.1.1}$$

That is as $\alpha = x + I$, each element in $F[x] / (p(x))$ can be expressed uniquely as

$$b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}, \quad \text{with } b_0, b_1, \cdots, b_{n-1} \in F. \tag{4.1.2}$$

Example 4.1.1

The polynomial $p(x) = x^2 - 2$ is irreducible over $\mathbb{Q}$. Thus, $\mathbb{Q}[x] / (p(x))$ is an extension field of $\mathbb{Q}$, which contains a root α of $p(x)$. Clearly, $\sqrt{2}$ is a root of $p(x)$ which is algebraic over $\mathbb{Q}$. To see that, $\alpha = \sqrt{2}$ implies that $\alpha^2 = 2$ and hence $\alpha^2 - 2 = 0$. Therefore, $\alpha = \sqrt{2}$ is a root for $p(x) = x^2 - 2 \in \mathbb{Q}[x]$.

Thus, each element in $\mathbb{Q}[x] / (p(x))$ can be written uniquely in the form $a + b\alpha$, where $a, b \in \mathbb{Q}$ and $\alpha = x + (x^2 - 2)$. Moreover, $irr\left(\sqrt{2}, \mathbb{Q}\right) = x^2 - 2$ with degree 2.

Theorem 4.1.3

Assume that F is a field and $p(x) \in F[x]$ is irreducible over F. Then $F[x]/(p(x))$ is a field extension of F, and $p(x)$ has a root in $F[x]/(p(x))$.

Proof:

Let $I = (p(x))$. Since F is a field and $p(x)$ is irreducible in $F[x]$, then $F[x]/I$ is a field. Note that $\{b + I : b \in F\}$ is a subfield of $F[x]/I$ that is isomorphic to F. Hence $F[x]/I$ is an extension of F.

Assume that $p(x) = a_0 + a_1x + \cdots + a_nx^n$, and let α denote the element $x + I \in F[x]/I$. Then

$$\begin{aligned} p(\alpha) &= a_0 + a_1(x + I) + \cdots a_n(x + I)^n \\ &= (a_0 + a_1x + \cdots + a_nx^n) + I = p(x) + I = I \end{aligned}$$

But I is the zero element in $F[x]/I$. Thus α is a root of $p(x)$ in $F[x]/I$.

Corollary 4.1.1

Assume that F is a field and $p(x) \in F[x]$ is irreducible over F. Then $F[x]/(p(x))$ contains a root α of $p(x)$, and each element of $F[x]/(p(x))$ can be expressed uniquely in the form (4.1.2). Moreover, elements of the form (4.1.2) are added and subtracted using the usual addition and subtraction of polynomials. To multiply elements $f(\alpha)$ and $g(\alpha)$ of the form (4.1.2), multiply them as polynomials and divide the result by $p(\alpha)$; the remainder will equal $f(\alpha)\,g(\alpha)$.

Example 4.1.2

Show that every element in $\mathbb{Q}\left(\sqrt{5}\right)$ can be written in the form $a + b\sqrt{5}$ with $a, b \in \mathbb{Q}$.

Solution:

Note that $\mathbb{Q}[x]/(x^2 - 5) \approx \mathbb{Q}\left(\sqrt{5}\right)$ and hence every element in $\mathbb{Q}[x]/(x^2 - 5)$ can be written as $a + b\alpha$, where α is a root of $x^2 - 5$ and $a, b \in \mathbb{Q}$. Thus, using the isomorphism mapping $\theta : \mathbb{Q}[x]/(x^2 - 5) \to \mathbb{Q}\left(\sqrt{5}\right)$ defined by $\theta(a + b\alpha) = a + b\sqrt{5}$, we can see that every element of $\mathbb{Q}\left(\sqrt{5}\right)$ can be expressed in the form $a + b\sqrt{5}$ with $a, b \in \mathbb{Q}$.

We discuss the same problem in the next example in more details.

Example 4.1.3

Show that $\theta : \mathbb{Q}[x]/(x^2-2) \to \mathbb{Q}(\sqrt{2})$ defined by $\theta(a+b\alpha) = a+b\sqrt{2}$, where α is a root of $x^2-2 \in \mathbb{Q}[x]$, is an isomorphism and compute $(1-2\alpha)(2+\alpha)$ in $\mathbb{Q}[x]/(x^2-2)$.

Solution:

We first prove the isomorphism part:

- θ is 1-1: Let $\theta(a+b\alpha) = \theta(c+d\alpha)$ and hence $a+b\sqrt{2} = c+d\sqrt{2}$. Thus $a=c$ and $b=d$. Therefore, $a+b\alpha = c+d\alpha$ and hence θ is 1-1.
- θ is onto: Clearly, for any $a+b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, we have $a+b\alpha \in \mathbb{Q}[x]/(x^2-2)$ such that $\theta(a+b\alpha) = a+b\sqrt{2}$. Thus θ is onto.
- θ is homomorphism:

$$\begin{aligned}\theta((a+b\alpha)+(c+d\alpha)) &= \theta((a+c)+(b+d)\alpha) = (a+c)+(b+d)\sqrt{2}\\ &= \left(a+b\sqrt{2}\right)+\left(c+d\sqrt{2}\right) = \theta(a+b\alpha)+\theta(c+d\alpha).\end{aligned}$$

Further, for $a+b\alpha, c+d\alpha \in \mathbb{Q}[x]/(x^2-2)$, we have

$$\begin{aligned}(a+b\alpha)(c+d\alpha) &= ac+(ad+bc)\alpha+bd\alpha^2 = bd\alpha^2-2bd+2bd+ac+(ad+bc)\alpha\\ &= bd(\alpha^2-2)+(ac+2bd)+(ad+bc)\alpha.\end{aligned}$$

That is $(a+b\alpha)(c+d\alpha) = (ac+2bd)+(ad+bc)\alpha$ in $\mathbb{Q}[x]/(x^2-2)$. Hence

$$\begin{aligned}\theta((a+b\alpha)(c+d\alpha)) &= \theta((ac+2bd)+(ad+bc)\alpha) = (ac+2bd)+(ad+bc)\sqrt{2}\\ &= \left(a+b\sqrt{2}\right)\left(c+d\sqrt{2}\right) = \theta(a+b\alpha)\theta(c+d\alpha).\end{aligned}$$

Therefore, θ is an isomorphism and hence $\mathbb{Q}[x]/(x^2-2) \approx \mathbb{Q}(\sqrt{2})$.
To compute $(1-2\alpha)(2+\alpha)$, we compute it first in $\mathbb{Q}[x]/(x^2-2)$ as

$$\begin{aligned}(1-2\alpha)(2+\alpha) &= 2-3\alpha-2\alpha^2 = -\left[2\alpha^2+3\alpha-2+(4-4)\right]\\ &= -\left[2(\alpha^2-2)+3\alpha+2\right] = -2(\alpha^2-2)-3\alpha-2 = -3\alpha-2.\end{aligned}$$

Or we compute it in $\mathbb{Q}(\sqrt{2})$ as

$$\left(1-2\sqrt{2}\right)\left(2+\sqrt{2}\right) = 2+\sqrt{2}-4\sqrt{2}-4 = -3\sqrt{2}-2.$$

Here you can see how θ simplified in $\mathbb{Q}(\sqrt{2})$.

We note that $\sqrt{2}, i$, and $\sqrt[3]{3}$ are all algebraic over $\mathbb{Q}$ as they are zeros of x^2-2, x^2+1, and x^3-3, respectively.

Example 4.1.4

Show that $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right) = \mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)$, where $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right) = \left\{a+b\sqrt{2}+c\sqrt{3} : a,b,c \in \mathbb{Q}\right\}$ and $\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right) = \left\{a+b\left(\sqrt{2}+\sqrt{3}\right) : a,b \in \mathbb{Q}\right\}$.

Solution:

Clearly, $\sqrt{2},\sqrt{3} \in \mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$ and hence $\sqrt{2}+\sqrt{3} \in \mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$ which implies that $\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right) \subseteq \mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$.

We need now to prove the other direction of the inclusion by showing that both $\sqrt{2}$ and $\sqrt{3}$ are contained in $\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)$. Clearly, $\sqrt{2}+\sqrt{3} \in \mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)$ and so is its inverse

$$\left(\sqrt{2}+\sqrt{3}\right)^{-1} = \frac{1}{\sqrt{2}+\sqrt{3}}\frac{\sqrt{2}-\sqrt{3}}{\sqrt{2}-\sqrt{3}} = \frac{\sqrt{2}-\sqrt{3}}{-1} = \sqrt{3}-\sqrt{2} \in \mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right).$$

Therefore, $\left(\sqrt{2}+\sqrt{3}\right)+\left(\sqrt{3}-\sqrt{2}\right) = 2\sqrt{3} \in \mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)$, and thus $\sqrt{3} \in \mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)$. Similarly $\left(\sqrt{2}+\sqrt{3}\right)-\left(\sqrt{3}-\sqrt{2}\right) = 2\sqrt{2} \in \mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)$ implies $\sqrt{2} \in \mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)$. So $\sqrt{2},\sqrt{3} \in \mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)$ which implies that $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right) \subseteq \mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)$ and therefore $\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right) = \mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$.

Example 4.1.5

Show that $\beta = \sqrt{2}+\sqrt{3}$ is algebraic over $\mathbb{Q}$. Find $\deg(\beta,\mathbb{Q})$.

Solution:

Note that $\beta = \sqrt{2}+\sqrt{3}$ implies that $\beta^2 = 2+2\sqrt{6}+3$. Then $\beta^2-5 = 2\sqrt{6}$. Squaring both sides again, we get $\beta^4-10\beta^2+25 = 24$. That is, $\beta^4-10\beta^2+1 = 0$.

Therefore, $f(x) = x^4-10x^2+1 \in \mathbb{Q}[x]$ (irreducible over $\mathbb{Q}$, prove it!) with β is a root of $f(x)$.

Note that $irr(\beta,\mathbb{Q}) = f(x)$ of degree 4. Hence $\deg(\beta,\mathbb{Q}) = 4$. Hence $f(x)$ is a nonzero polynomial in $\mathbb{Q}[x]$ whose root is β and hence β is algebraic.

Exercise 4.1.1

Let $\alpha \in \mathbb{Q}[x]/(x^2-7)$ be a root of the irreducible polynomial $x^2-7 \in \mathbb{Q}[x]$. Express each of the following elements in the form $a+b\alpha$ with $a,b \in \mathbb{Q}$.

1. α^3,
2. $(1-\alpha)(2+\alpha)$,
3. $(1+\alpha)^2$, and
4. $(1+\alpha)^{-1}$.

Solution:

1. $\alpha^3 = \alpha(\alpha^2-7+7) = \alpha(\alpha^2-7)+7\alpha = 7\alpha$.
2. $(1-\alpha)(2+\alpha) = 2-\alpha-\alpha^2 = 2-\alpha-\alpha^2+7-7 = -(\alpha^2-7)-\alpha-5 = -\alpha-5$.
3. $(1+\alpha)^2 = 1+2\alpha+\alpha^7 = 1+2\alpha+\alpha^7-7+7 = (\alpha^2-7)+2\alpha+8 = 2\alpha+8$.
4. $(1+\alpha)^{-1} = \dfrac{1}{1+\alpha}\dfrac{1-\alpha}{1-\alpha} = \dfrac{1-\alpha}{-(\alpha^2-1)} = \dfrac{1-\alpha}{-(\alpha^2-7+7-1)} = \dfrac{1-\alpha}{-(\alpha^2-7)-6}$.
   That is $(1+\alpha)^{-1} = \dfrac{1-\alpha}{-6} = -\dfrac{1}{6}+\dfrac{\alpha}{6}$.

Exercise 4.1.2: #42.5 @*page* : 197

Prove that $\mathbb{Q}(\sqrt{2}) \neq \mathbb{Q}(\sqrt{3})$.

Solution:

Assume that $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{3})$. Then $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{3})$ and in particular $\sqrt{2} \in \mathbb{Q}(\sqrt{3})$. That is $\sqrt{2} = a+b\sqrt{3}$ for some $a,b \in \mathbb{Q}$. Squaring both sides, we get $2 = a^2+2ab\sqrt{3}+3b^2$. Therefore, $\sqrt{3} = \dfrac{2-a^2-3b^2}{2ab}$ which cannot be as the right hand side is a rational number while the left hand side is not rational. By contradiction proof, we get the result.

Exercise 4.1.3: #42.6 @*page* : 197

Show that every element of $\mathbb{Q}(\sqrt[3]{5})$ can be written in the form $a+b\sqrt[3]{5}+c\sqrt[3]{25}$, with $a,b,c \in \mathbb{Q}$.

Solution:

Clearly, $\mathbb{Q}[x]/(x^3-5) \approx \mathbb{Q}(\sqrt[3]{5})$. The isomorphism mapping is $\theta : \mathbb{Q}[x]/(x^3-5) \to \mathbb{Q}(\sqrt[3]{5})$ is given by $\theta(a+b\alpha+c\alpha^2) = a+b\sqrt[3]{5}+c\sqrt[3]{5^2}$ where $a,b,c \in \mathbb{Q}$, and α is a root for x^3-5 in

$\mathbb{Q}[x]$. Thus, the result.

Exercise 4.1.4

Show that $\alpha = \sqrt{1+\sqrt{3}}$ is algebraic over $\mathbb{Q}$ and find $\deg(\alpha, \mathbb{Q})$.

Solution:

Clearly, $\alpha = \sqrt{1+\sqrt{3}}$ and hence $\alpha^2 = 1+\sqrt{3}$ implies that $(\alpha^2-1)^2 = 3$. Thus, $\alpha^4-2\alpha^2-2 = 0$. Therefore $p(x) = x^4 - 2x^2 - 2 \in \mathbb{Q}[x]$ is irreducible over $\mathbb{Q}$ (by Eisenstein test with $p = 2$, for instance) with a root α. Therefore, α is algebraic over $\mathbb{Q}$ and $\deg(\alpha, \mathbb{Q}) = 4$.

Exercise 4.1.5

Let p and q be two distinct primes. Show that $\alpha = \sqrt{p} + \sqrt{q}$ is algebraic over $\mathbb{Q}$ by finding an appropriate (quartic) polynomial in $\mathbb{Q}[x]$ with α as a root.

Solution:

Let $\alpha = \sqrt{p} + \sqrt{q}$. Then $\alpha^2 = p + 2\sqrt{pq} + q$ and hence $\alpha^2 - (p+q) = 2\sqrt{pq}$ implies that $(\alpha^2 - (p+q))^2 = 4pq$. Therefore,

$$\alpha^4 - 2(p+q)\alpha^2 + (p+q)^2 - 4pq = 0 \;\Rightarrow\; \alpha^4 - 2(p+q)\alpha^2 + (p-q)^2 = 0.$$

Therefore, the polynomial $f(x) = x^4 - 2(p+q)x^2 + (p-q)$ is a quartic polynomial in $\mathbb{Q}[x]$ with α as a root.

Exercise 4.1.6

For any positive integers a and b, show that $\mathbb{Q}\big(\sqrt{a}, \sqrt{b}\big) = \mathbb{Q}\big(\sqrt{a} + \sqrt{b}\big)$.

Solution:

If $a = b$, then $\mathbb{Q}(\sqrt{a}, \sqrt{a}) = \mathbb{Q}(\sqrt{a}) = \mathbb{Q}(2\sqrt{a})$. Otherwise assume that $a \neq b$. Clearly, $\sqrt{a}, \sqrt{b} \in \mathbb{Q}\big(\sqrt{a}, \sqrt{b}\big)$ and hence $\sqrt{a} + \sqrt{b} \in \mathbb{Q}\big(\sqrt{a}, \sqrt{b}\big)$ which implies that $\mathbb{Q}\big(\sqrt{a} + \sqrt{b}\big) \subseteq \mathbb{Q}\big(\sqrt{a}, \sqrt{b}\big)$.

We need now to prove the other direction of the inclusion by showing that both $\sqrt{a}$ and $\sqrt{b}$

are contained in $\mathbb{Q}\big(\sqrt{a}+\sqrt{b}\big)$. Clearly, $\sqrt{a}+\sqrt{b} \in \mathbb{Q}\big(\sqrt{a}+\sqrt{b}\big)$ and so is its inverse

$$\big(\sqrt{a}+\sqrt{b}\big)^{-1} = \frac{1}{\sqrt{a}+\sqrt{b}}\frac{\sqrt{a}-\sqrt{b}}{\sqrt{a}-\sqrt{b}} = \frac{1}{a-b}\big(\sqrt{a}-\sqrt{b}\big) \in \mathbb{Q}\big(\sqrt{a}+\sqrt{b}\big).$$

Since $0 \neq a-b \in \mathbb{Q}$, we get $\sqrt{a}-\sqrt{b} \in \mathbb{Q}\big(\sqrt{a}+\sqrt{b}\big)$.
Therefore, $\big(\sqrt{a}+\sqrt{b}\big)+\big(\sqrt{a}-\sqrt{b}\big) = 2\sqrt{a} \in \mathbb{Q}\big(\sqrt{a}+\sqrt{b}\big)$, and thus $\sqrt{a} \in \mathbb{Q}\big(\sqrt{a}+\sqrt{b}\big)$.
Similarly $\big(\sqrt{a}+\sqrt{b}\big)-\big(\sqrt{a}-\sqrt{b}\big) = 2\sqrt{b} \in \mathbb{Q}\big(\sqrt{a}+\sqrt{b}\big)$ implies $\sqrt{b} \in \mathbb{Q}\big(\sqrt{a}+\sqrt{b}\big)$.
So $\sqrt{a},\sqrt{b} \in \mathbb{Q}\big(\sqrt{a}+\sqrt{b}\big)$ which implies that $\mathbb{Q}\big(\sqrt{a},\sqrt{b}\big) \subseteq \mathbb{Q}\big(\sqrt{a}+\sqrt{b}\big)$ and therefore $\mathbb{Q}\big(\sqrt{a}+\sqrt{b}\big) = \mathbb{Q}\big(\sqrt{a},\sqrt{b}\big)$.

Exercise 4.1.7

Show that $\mathbb{Q}\big(\sqrt{2},i\big) = \mathbb{Q}\big(\sqrt{2}+i\sqrt{2}\big)$. Show that $\mathbb{Q}\big(\sqrt{2},i\big) = \mathbb{Q}\big(\sqrt{2}+i\big)$

Solution:

Clearly, $\sqrt{2},i \in \mathbb{Q}\big(\sqrt{2},i\big)$ which implies $i\sqrt{2} \in \mathbb{Q}\big(\sqrt{2},i\big)$ and hence $\sqrt{2}+i\sqrt{2} \in \mathbb{Q}\big(\sqrt{2},i\big)$ which implies that $\mathbb{Q}\big(\sqrt{2}+i\sqrt{2}\big) \subseteq \mathbb{Q}\big(\sqrt{2},i\big)$.
We need now to prove the other direction of the inclusion by showing that both $\sqrt{2}$ and i are contained in $\mathbb{Q}\big(\sqrt{2}+i\sqrt{2}\big)$. Clearly, $\sqrt{2}+i\sqrt{2} \in \mathbb{Q}\big(\sqrt{2}+i\sqrt{2}\big)$ and so is its inverse

$$\big(\sqrt{2}+i\sqrt{2}\big)^{-1} = \frac{1}{\sqrt{2}+i\sqrt{2}}\frac{\sqrt{2}-i\sqrt{2}}{\sqrt{2}-i\sqrt{2}} = \frac{1}{4}\big(\sqrt{2}-i\sqrt{2}\big) \in \mathbb{Q}\big(\sqrt{2}+i\sqrt{2}\big).$$

Since $4 \in \mathbb{Q}$, we get $\sqrt{2}-i\sqrt{2} \in \mathbb{Q}\big(\sqrt{2}+i\sqrt{2}\big)$.
Therefore, $\big(\sqrt{2}+i\sqrt{2}\big)+\big(\sqrt{2}-i\sqrt{2}\big) = 2\sqrt{2} \in \mathbb{Q}\big(\sqrt{2}+i\sqrt{2}\big)$, and thus $\sqrt{2} \in \mathbb{Q}\big(\sqrt{2}+i\sqrt{2}\big)$.
Similarly $\big(\sqrt{2}+i\sqrt{2}\big)-\big(\sqrt{2}-i\sqrt{2}\big) = 2i\sqrt{2} \in \mathbb{Q}\big(\sqrt{2}+i\sqrt{2}\big)$ implies $i\sqrt{2} \in \mathbb{Q}\big(\sqrt{2}+i\sqrt{2}\big)$.
So $\sqrt{2},i\sqrt{2} \in \mathbb{Q}\big(\sqrt{2}+i\sqrt{2}\big)$ which implies that $\mathbb{Q}\big(\sqrt{2},i\big) \subseteq \mathbb{Q}\big(\sqrt{2}+i\sqrt{2}\big)$ and therefore $\mathbb{Q}\big(\sqrt{2}+i\sqrt{2}\big) = \mathbb{Q}\big(\sqrt{2},i\big)$.

Section 4.2: Splitting Fields

Definition 4.2.1

A nonconstant polynomial $p(x)$ over a field F **splits over** an extension field E of F if $p(x)$ can be factored into linear factors over E, that is

$$p(x) = a(x - c_1)(x - c_2)\cdots(x - c_n),$$

where $a \in F$ and $c_1, c_2, \cdots, c_n$ are the roots of $p(x)$ in E.

Theorem 4.2.1: The Fundamental Theorem of Algebra

Every nonconstant polynomial $f(x) \in \mathbb{C}[x]$ has a root in $\mathbb{C}$. That is, $\mathbb{C}$ is algebraically closed. In other words, each polynomial of degree $n \geq 1$ over $\mathbb{C}$ has n roots.

Definition 4.2.2

An extension field E of a field F is called a **splitting field** for $f(x) \in F[x]$ over F if:

1. $f(x)$ factors into linear factors (splits completely) in $E[x]$, and
2. $f(x)$ does not split completely in $K[x]$ for any $F \subsetneqq K \subsetneqq E$.

Theorem 4.2.2

For any field F and $f(x) \in F[x]$, there is an extension field E of F which is a splitting field for $f(x)$ over F.

Theorem 4.2.3

Let E be an extension of a field F and $f(x) \in F[x]$. If E contains roots $\alpha_1, \cdots, \alpha_n$ of $f(x)$ and $f(x)$ splits in $F(\alpha_1, \cdots, \alpha_n)[x]$, then $F(\alpha_1, \cdots, \alpha_n)$ is a splitting field for $f(x)$ over F.

Example 4.2.1

Any first degree polynomial over F splits over F, since $ax + b$ with $a \neq 0$ has the form $ax + b = a(x - \alpha)$ root $\alpha = -a^{-1}b \in F$.

Example 4.2.2

Note that $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ does not splits over $\mathbb{Q}$. Clearly, $f(x) = (x - \sqrt{2})(x + \sqrt{2})$ which splits over the extension field $\mathbb{R}$ of $\mathbb{Q}$. But $\mathbb{R}$ is not a splitting field for $f(x)$ over $\mathbb{Q}$ since $f(x)$ splits over a smaller extension field $\mathbb{Q}\left(\sqrt{2}\right)$ which is contained in $\mathbb{R}$. Thus $\mathbb{Q}\left(\sqrt{2}\right)$ is a splitting field for $f(x)$ over $\mathbb{Q}$.

Another example is $g(x) = x^2 + 1 \in \mathbb{R}[x]$ which does not split in $\mathbb{R}[x]$. It does split in $\mathbb{C}[x]$ since $g(x) = (x - i)(x + i) \in \mathbb{C}[x]$. Here $\mathbb{C} = \mathbb{R}(i)$ is a splitting field for $g(x)$ over $\mathbb{R}$.

Example 4.2.3

Construct a splitting field for $f(x) = x^2 - 2 \in \mathbb{Q}[x]$.

Solution:

Clearly $f(x)$ is irreducible over $\mathbb{Q}$ using for instance Eisenstein criterion for $p = 2$. Note that

$$f(x) = x^2 - 2 = \left(x - \sqrt{2}\right)\left(x + \sqrt{2}\right),$$

with roots $\left\{\sqrt{2}, -\sqrt{2}\right\} \notin \mathbb{Q}$. But $\sqrt{2}$ generates all roots of $f(x)$.

Therefore, $\mathbb{Q}\left(\sqrt{2}\right) \approx \mathbb{Q}[x] / (x^2 - 2)$ is a splitting field for $f(x)$ over $\mathbb{Q}$.

Example 4.2.4

Construct a splitting field for $f(x) = x^4 - 4 \in \mathbb{Q}[x]$.

Solution:

Clearly $f(x) = x^4 - 4 = (x^2 - 2)(x^2 + 2)$ where both factors irreducible over $\mathbb{Q}$ using for instance Eisenstein criterion for $p = 2$ for both factors. Factoring $f(x)$, we get

$$f(x) = (x^2 - 2)(x^2 + 2) = \left(x - \sqrt{2}\right)\left(x + \sqrt{2}\right)\left(x - i\sqrt{2}\right)\left(x + i\sqrt{2}\right).$$

So the roots of $f(x)$ are $\left\{\sqrt{2}, -\sqrt{2}, i\sqrt{2}, -i\sqrt{2}\right\} \notin \mathbb{Q}$. Note that $\sqrt{2}$ and i generate all the roots of $f(x)$.

Therefore, $\mathbb{Q}\left(\sqrt{2}, i\right) \approx \mathbb{Q}[x] / (x^4 - 4)$ is the splitting field for $f(x)$ over $\mathbb{Q}$.

Example 4.2.5

Find a polynomial $f(x) \in \mathbb{Q}[x]$ so that $F = \mathbb{Q}\left(\sqrt{1+\sqrt{5}}\right)$ is the splitting field for $f(x)$ over $\mathbb{Q}$.

Solution:

We simply need to find an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ which has $\sqrt{1+\sqrt{5}}$ as a root. Let $\alpha = \sqrt{1+\sqrt{5}}$. Then $\alpha^2 = 1+\sqrt{5}$ and hence $\alpha^2 - 1 = \sqrt{5}$. That is, $\alpha^4 - 2\alpha^2 + 1 = 5$ and thus $\alpha^4 - 2\alpha^2 - 6 = 0$. Therefore, if $f(x) = x^4 - 2x^2 - 6 \in \mathbb{Q}[x]$, then it is irreducible over $\mathbb{Q}$ and it has $\sqrt{1+\sqrt{5}}$ among its roots.

Thus, $f(x)$ is a polynomial whose splitting field is F over $\mathbb{Q}$.

Exercise 4.2.1

Construct a splitting field for $f(x) = x^3 - 2 \in \mathbb{Q}[x]$.

Solution:

Clearly $f(x)$ is irreducible over $\mathbb{Q}$ using for instance Eisenstein criterion for $p = 2$. Using Factor Theorem, we see that $\sqrt[3]{2}$ is a root for $f(x)$, since $f\left(\sqrt[3]{2}\right) = 0$. Applying the Division Algorithm to get $f(x) = x^3 - 2 = \left(x - \sqrt[3]{2}\right)\left(x^2 + \sqrt[3]{2}x + \sqrt[3]{2^2}\right)$. Furthermore, we use the quadratic formula to get

$$f(x) = x^3 - 2 = \left(x - \sqrt[3]{2}\right)\left(\frac{-\sqrt[3]{2}}{2} + \frac{i\sqrt[3]{2}\sqrt{3}}{2}\right)\left(\frac{-\sqrt[3]{2}}{2} - \frac{i\sqrt[3]{2}\sqrt{3}}{2}\right).$$

So the roots of $f(x)$ are $\left\{\sqrt[3]{2}, \frac{\sqrt[3]{2}}{2}\left(-1 + i\sqrt{3}\right), \frac{\sqrt[3]{2}}{2}\left(-1 - i\sqrt{3}\right)\right\}$. Clearly, $\sqrt[3]{2}$ and $i\sqrt{3}$ generate all roots of $f(x)$. Therefore $\mathbb{Q}\left(\sqrt[3]{2}, i\sqrt{3}\right) \approx \mathbb{Q}[x] / (x^3 - 2)$ is a splitting field for $f(x)$ over $\mathbb{Q}$.

Exercise 4.2.2

Construct a splitting field for $f(x) = x^4 - 5x^2 + 6 \in \mathbb{Q}[x]$.

Solution:

Clearly $f(x) = x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3)$ where both factors irreducible over $\mathbb{Q}$ using for instance Eisenstein criterion for $p = 2$ and $p = 3$, respectively. Factoring $f(x)$, we get

$$f(x) = (x^2 - 2)(x^2 - 3) = \left(x - \sqrt{2}\right)\left(x + \sqrt{2}\right)\left(x - \sqrt{3}\right)\left(x + \sqrt{3}\right).$$

So the roots of $f(x)$ are $\left\{\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}\right\} \notin \mathbb{Q}$. Note that $\sqrt{2}$ and $\sqrt{3}$ generate all the roots of $f(x)$. Therefore, $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) \approx \mathbb{Q}[x] / (x^4 - 5x^2 + 6)$ is the splitting field for $f(x)$ over $\mathbb{Q}$.

Exercise 4.2.3

Construct a splitting field for $f(x) = x^4 + 4 \in \mathbb{Q}[x]$.

Solution:

Factoring $f(x)$, we get

$$f(x) = x^4 + 4 = x^4 + 4x^2 + 4 - 4x^2 = (x^2 + 2)^2 - (2x)^2 = ((x^2 + 2) + 2x)((x^2 + 2) - 2x).$$

Thus, $f(x) = (x^2 + 2x + 2)(x^2 - 2x + 2)$, where both factors irreducible over $\mathbb{Q}$ using for instance Eisenstein criterion for $p = 2$ for both factors. So the roots of $f(x)$ are $\{1+i, 1-i, -1+i, -1-i\} \notin \mathbb{Q}$. Note that i generates all the roots of $f(x)$. Therefore, $\mathbb{Q}(i) \approx \mathbb{Q}[x] / (x^4 + 4)$ is the splitting field for $f(x)$ over $\mathbb{Q}$.

Exercise 4.2.4

Show that $f(x) = x^4 - 2x^2 - 3$ splits over $\mathbb{Q}\left(i, \sqrt{3}\right)$.

Solution:

Note that $f(x) = (x^2 - 3)(x^2 + 1) = \left(x - \sqrt{3}\right)\left(x + \sqrt{3}\right)(x - i)(x + i)$. Thus, the roots of $f(x)$ are $\left\{\pm\sqrt{3}, \pm i\right\}$ which can be generated by only $\sqrt{3}$ and i. Therefore $f(x)$ splits over $\mathbb{Q}\left(i, \sqrt{3}\right)$.

Exercise 4.2.5

Show that $\mathbb{Q}\left(\sqrt{7}, i\right)$ is the splitting field for $f(x) = x^4 - 6x^2 - 7$ over $\mathbb{Q}$.

Solution:

Note that $f(x) = (x^2 - 7)(x^2 + 1) = \left(x - \sqrt{7}\right)\left(x + \sqrt{7}\right)(x - i)(x + i)$. Thus, the roots of $f(x)$ are $\left\{\pm\sqrt{7}, \pm i\right\}$ which can be generated by only $\sqrt{7}$ and i. Therefore $f(x)$ splits over $\mathbb{Q}\left(i, \sqrt{7}\right)$.

Exercise 4.2.6

Find a polynomial $f(x) \in \mathbb{Q}[x]$ so that $F = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$ is the splitting field for $f(x)$ over $\mathbb{Q}$.

Solution:

We simply need to find an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ which has $\sqrt{2}$ and $\sqrt{3}$ as roots. But since $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) = \mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right)$, we look for irreducible polynomial $f(x) \in \mathbb{Q}[x]$ which has $\sqrt{2} + \sqrt{3}$ as a root. Let $\alpha = \sqrt{2} + \sqrt{3}$. Then $\alpha^2 = 2 + 2\sqrt{6} + 3$ and hence $\alpha^2 - 5 = 2\sqrt{6}$. That is, $\alpha^4 - 10\alpha^2 + 25 = 24$ and thus $\alpha^4 - 10\alpha^2 + 1 = 0$. Therefore, if $f(x) = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$, then it is irreducible over $\mathbb{Q}$ and it has $\sqrt{2}$ and $\sqrt{3}$ among its

roots. Thus, $f(x)$ is a polynomial whose splitting field is F over $\mathbb{Q}$.

Exercise 4.2.7

Find a polynomial $f(x) \in \mathbb{Q}[x]$ so that $F = \mathbb{Q}\left(\sqrt{2} + i\sqrt{3}\right)$ is the splitting field for $f(x)$ over $\mathbb{Q}$.

Solution:

We simply need to find an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ which has $\sqrt{2} + i\sqrt{3}$ as a root. Let $\alpha = \sqrt{2} + i\sqrt{3}$. Then $\alpha^2 = 2 + 2i\sqrt{6} - 3$ and hence $\alpha^2 + 1 = 2i\sqrt{6}$. That is, $\alpha^4 + 2\alpha^2 + 1 = -24$ and thus $\alpha^4 + 2\alpha^2 + 25 = 0$. Therefore, if $f(x) = x^4 + 2x^2 + 25 \in \mathbb{Q}[x]$, then it is irreducible over $\mathbb{Q}$ and it has $\sqrt{2} + i\sqrt{3}$ as a root. Thus, $f(x)$ is a polynomial whose splitting field is F over $\mathbb{Q}$.

Section 4.3: Finite Fields

Recall that $\mathbb{Z}_p$ is a (finite) field if and only if p is a prime number. Here we write $\mathbf{F}_p$ to denote a field of size p.

Theorem 4.3.1

There is a finite field of order n iff n is a power of a prime.

Remark 4.3.1

- Every finite field has a prime power order.
- For every prime power, there is a finite field of that order.
- Any two finite fields of the same order are isomorphic.
- The multiplicative group of a finite field is cyclic.

Theorem 4.3.2

For a prime p and a monic irreducible polynomial $p(x) \in \mathbf{F}_p[x]$ of degree n, the ring $\mathbf{F}_p[x] / (p(x))$ is a field of order p^n.

Example 4.3.1

Consider the ring $\mathbb{Z}_2[x] / (x^2)$. Construct the addition and multiplication Cayley tables for $\mathbb{Z}_2[x] / (x^2)$. Show that $\mathbb{Z}_2[x] / (x^2)$ is not a field.

Solution:

Note that $\mathbb{Z}_2[x] / (x^2) = \{0 + (x^2), 1 + (x^2), x + (x^2), 1 + x + (x^2)\}$. For simplicity, we write $\mathbb{Z}_2[x] / (x^2) = \{0, 1, x, 1 + x\}$. Hence, the addition and multiplication tables are:

$+$	0	1	x	$1+x$
0	0	1	x	$1+x$
1	1	0	$1+x$	x
x	x	$1+x$	0	1
$1+x$	$1+x$	x	1	0

$\cdot$	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	0	x
$1+x$	0	$1+x$	x	1

Clearly, $\mathbb{Z}_2[x] / (x^2)$ is not a field since it has $x \cdot x = 0$ (in the table). Moreover, x^2 is not irreducible in $\mathbb{Z}_2[x]$ as $x^2 = x \cdot x$.

Example 4.3.2

Construct a field of order 4. Find a generator for the multiplicative group of that field.

Solution:

Note that $4 = 2^2$. Since x^2+x+1 is an irreducible polynomial in $\mathbb{Z}_2[x]$ (using Factor Theorem for instance), We conclude that $\mathbf{F} = \mathbb{Z}_2[x] / (x^2 + x + 1)$ is a field with $2^2 = 4$ elements. The field $\mathbf{F}$ contains a root α of x^2+x+1. Therefore, any element in $\mathbb{Z}_2(\alpha) \approx \mathbb{Z}_2[x] / (x^2 + x + 1)$ can be uniquely expressed as $a + b\alpha$, where $a, b \in \mathbb{Z}_2$. That is $\mathbb{Z}_2(\alpha) = \{0, 1, \alpha, 1 + \alpha\}$. The addition and multiplication tables of $\mathbb{Z}_2(\alpha)$ are:

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

$\cdot$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

We note that the addition table is clearly done. In the multiplication table, we consider some entries as follows:

The entry $\alpha \cdot \alpha = \alpha^2 = -1 - \alpha$ since $\alpha^2 + \alpha + 1 = 0$. But then $\alpha^2 = -1 - \alpha = 1 + \alpha$ in $\mathbb{Z}_2$. Moreover, we have $(1 + \alpha)(1 + \alpha) = \alpha^2 + 2\alpha + 1$. Since $2\alpha = 0$ in $\mathbb{Z}_2$ and $\alpha^2 = 1 + \alpha$ as we have proved, we get $(1 + \alpha)(1 + \alpha) = \alpha^2 + 2\alpha + 1 = 1 + \alpha + 0 + 1 = 2 + \alpha = \alpha$.

To find a generator for the multiplicative group (not including 0) of $\mathbb{Z}_2(\alpha)$, we try to find an element in $\mathbb{Z}_2^*(\alpha)$ whose powers generate all elements in the group.

Note that $\alpha^1 = \alpha$, $\alpha^2 = 1 + \alpha$ (as we have seen), and $\alpha^3 = \alpha\,\alpha^2 = \alpha(1 + \alpha) = \alpha + \alpha^2 = 1 + 2\alpha = 1$. Therefore, $\mathbb{Z}_2^*(\alpha) = \{\alpha, \alpha^2, \alpha^3\}$, and hence α is a generator for the multiplicative group of $\mathbb{Z}_2(\alpha)$.

It is also true that $\mathbb{Z}_2^*(\alpha) = \{1 + \alpha, (1 + \alpha)^2, (1 + \alpha)^3\}$. Can you show that?

Example 4.3.3

Construct a field of order 9. Find a generator for the multiplicative group of that field.

Solution:

Note that x^2+1 is an irreducible polynomial in $\mathbb{Z}_3[x]$. Thus $\mathbf{F} = \mathbb{Z}_3[x]/(x^2+1)$ is a field with $3^2 = 9$ elements. The field $\mathbf{F}$ contains a root α of x^2+1. Therefore, any element in $\mathbb{Z}_3(\alpha) \approx \mathbb{Z}_3[x]/(x^2+1)$ can be uniquely expressed as $a+b\alpha$, where $a, b \in \mathbb{Z}_3$. That is $\mathbb{Z}_3(\alpha) = \{0, 1, 2, \alpha, 2\alpha, 1+\alpha, 1+2\alpha, 2+\alpha, 2+2\alpha\}$. The tables of $\mathbb{Z}_3(\alpha)$ are:

$+$	0	1	2	α	2α	$1+\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$
0	0	1	2	α	2α	$1+\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$
1	1	2	0	$1+\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$	α	2α
2	2	0	1	$2+\alpha$	$2+2\alpha$	α	2α	$1+\alpha$	$1+2\alpha$
α	α	$1+\alpha$	$2+\alpha$	2α	0	$1+2\alpha$	1	$2+2\alpha$	2
2α	2α	$1+2\alpha$	$2+2\alpha$	0	α	1	$1+\alpha$	2	$2+\alpha$
$1+\alpha$	$1+\alpha$	$2+\alpha$	α	$1+2\alpha$	1	$2+2\alpha$	2	2α	0
$1+2\alpha$	$1+2\alpha$	$2+2\alpha$	2α	1	$1+\alpha$	2	$2+\alpha$	0	α
$2+\alpha$	$2+\alpha$	α	$1+\alpha$	$2+2\alpha$	2	2α	0	$1+2\alpha$	1
$2+2\alpha$	$2+2\alpha$	2α	$1+2\alpha$	2	$2+\alpha$	0	α	1	$1+\alpha$

$\cdot$	0	1	2	α	2α	$1+\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	α	2α	$1+\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$
2	0	2	1	2α	α	$2+2\alpha$	$2+\alpha$	$1+2\alpha$	$1+\alpha$
α	0	α	2α	2	1	$2+\alpha$	$1+\alpha$	$2+2\alpha$	$1+2\alpha$
2α	0	2α	α	1	2	$1+2\alpha$	$2+2\alpha$	$1+\alpha$	$2+\alpha$
$1+\alpha$	0	$1+\alpha$	$2+2\alpha$	$2+\alpha$	$1+2\alpha$	2α	2	1	α
$1+2\alpha$	0	$1+2\alpha$	$2+\alpha$	$1+\alpha$	$2+2\alpha$	2	α	2α	1
$2+\alpha$	0	$2+\alpha$	$1+2\alpha$	$2+2\alpha$	$1+\alpha$	1	2α	α	2
$2+2\alpha$	0	$2+2\alpha$	$1+\alpha$	$1+2\alpha$	$2+\alpha$	α	1	2	2α

Here, we note that $\alpha^2+1 = 0$ and the coefficients are reduced by the rules in $\mathbb{Z}_3$. Thus, in the multiplication table, we have $\alpha \cdot \alpha = \alpha^2 = -1 = 2$. Hence

$$(1+2\alpha)(2+2\alpha) = 2+6\alpha+4\alpha^2 = 2+\alpha^2 = 4 = 1.$$

Further, $(1+\alpha)(2+2\alpha) = 2+4\alpha+2\alpha^2 = 2+\alpha+4 = 6+\alpha = \alpha$.

Moreover, $1+\alpha$, $1+2\alpha$, $2+\alpha$, and $2+2\alpha$ are all the generators of $(\mathbb{Z}_2^*(\alpha), \cdot)$.

Exercise 4.3.1

Construct a field of order 8. Find a generator for the multiplicative group of that field.

Solution:

Note that x^3+x+1 is an irreducible polynomial in $\mathbb{Z}_2[x]$. Thus $\mathbf{F} = \mathbb{Z}_2[x]/(x^3+x+1)$ is a field with $2^3 = 8$ elements. The field $\mathbf{F}$ contains a root α of x^3+x+1. Therefore, any element in $\mathbb{Z}_2(\alpha) \approx \mathbb{Z}_2[x]/(x^3+x+1)$ can be uniquely expressed as $a+b\alpha+c\alpha^2$, where $a,b,c \in \mathbb{Z}_2$. That is $\mathbb{Z}_2(\alpha) = \{0, 1, \alpha, 1+\alpha, \alpha^2, 1+\alpha^2, \alpha+\alpha^2, 1+\alpha+\alpha^2\}$. The tables of $\mathbb{Z}_2(\alpha)$ are:

$+$	0	1	α	$1+\alpha$	α^2	$1+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$
0	0	1	α	$1+\alpha$	α^2	$1+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$
1	1	0	$1+\alpha$	α	$1+\alpha^2$	α^2	$1+\alpha+\alpha^2$	$\alpha+\alpha^2$
α	α	$1+\alpha$	0	1	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$	α^2	$1+\alpha^2$
$1+\alpha$	$1+\alpha$	α	1	0	$1+\alpha+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha^2$	α^2
α^2	α^2	$1+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$	0	1	α	$1+\alpha$
$1+\alpha^2$	$1+\alpha^2$	α^2	$1+\alpha+\alpha^2$	$\alpha+\alpha^2$	1	0	$1+\alpha$	α
$\alpha+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$	α^2	$1+\alpha^2$	α	$1+\alpha$	0	1
$1+\alpha+\alpha^2$	$1+\alpha+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha^2$	α^2	$1+\alpha$	α	1	0

$\cdot$	0	1	α	$1+\alpha$	α^2	$1+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$
0	0	0	0	0	0	0	0	0
1	0	1	α	$1+\alpha$	α^2	$1+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$
α	0	α	α^2	$\alpha+\alpha^2$	$1+\alpha$	1	$1+\alpha+\alpha^2$	$1+\alpha^2$
$1+\alpha$	0	$1+\alpha$	$\alpha+\alpha^2$	$1+\alpha^2$	$1+\alpha+\alpha^2$	α^2	1	α
α^2	0	α^2	$1+\alpha$	$1+\alpha+\alpha^2$	$\alpha+\alpha^2$	α	$1+\alpha^2$	1
$1+\alpha^2$	0	$1+\alpha^2$	1	α^2	α	$1+\alpha+\alpha^2$	$1+\alpha$	$\alpha+\alpha^2$
$\alpha+\alpha^2$	0	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$	1	$1+\alpha^2$	$1+\alpha$	α	α^2
$1+\alpha+\alpha^2$	0	$1+\alpha+\alpha^2$	$1+\alpha^2$	α	1	$\alpha+\alpha^2$	α^2	$1+\alpha$

Here, we note that $\alpha^3+\alpha+1=0$ and the coefficients are reduced by the rules in $\mathbb{Z}_2$. Thus, in the multiplication table, we have $\alpha \cdot \alpha^2 = \alpha^3 = -1-\alpha = 1+\alpha$. Hence

$$(1+\alpha)(\alpha+\alpha^2) = \alpha + 2\alpha^2 + \alpha^3 = \alpha + 1 + \alpha = 1.$$

Further, $(1+\alpha)(1+\alpha+\alpha^2) = 1+2\alpha+2\alpha^2+\alpha^3 = 1+1+\alpha = \alpha$.

Moreover, $1+\alpha$ is a generator of $(\mathbb{Z}_2^*(\alpha), \cdot)$, can you find another one?

Exercise 4.3.2

Find an appropriate irreducible polynomial $p(x)$ in $\mathbb{Z}_2[x]$ so that $\mathbb{Z}_2[x]/(p(x))$ is a finite filed of order 16.

Solution:

Note that $16 = 2^4$, and hence we need an irreducible polynomial $p(x)$ of degree 4 in $\mathbb{Z}_2[x]$. So $p(x) = x^4 + ax^3 + bx^2 + cx + d$, where $a,b,c,d \in \mathbb{Z}_2$. Computing $p(0) = d$ and $p(1) =$

$1+a+b+c+d$. Insisting that $p(x) \neq 0$ for $x = 0, 1 \in \mathbb{Z}_2$, we see that $d \neq 0$ and hence $d = 1$.

Hence $a + b + c \neq 0$, so we can choose $a = b = 0$ and $c = 1$.

Therefore, $p(x) = x^4 + x + 1 \in \mathbb{Z}_2[x]$ and $\mathbf{F}_{16} = \mathbf{F}_{2^4} \approx \mathbb{Z}_2[x] \,/\, (p(x))$.

The Index