# Ring Theory.

Alec Zabel-Mena

November 9, 2022

# Contents

# Chapter 1

# Rings.

## 1.1 Definitions and Examples.

**Definition.** A **ring** $R$ is a set together with two binary operations $+ : (a, b) \to a + b$ and $\cdot : (a, b) \to ab$ called **additon** and **multiplication** such that:

(1) $R$ is an Abelian group over $+$, where we denote the identity element as 0 and the inverse of each $a \in R$ as $-a$.

(2) $R$ is closed under $\cdot$ and $\cdot$ is associative. That is, $ab \in R$ whenever $a, b \in R$ and $a(bc) = (ab)c$.

(3) $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

If $ab = ba$ for all $a, b \in R$, then we call $R$ **commutative**. If there exists an element $1 \in R$ such that $a_1 = 1a = R$, then we call $R$ a ring with **identity**.

**Definition.** A ring $R$ with identity $1 \neq 0$ is called a **division ring** if for all $a \in R$, where $a \neq 0$, there exists a $b \in R$ such that $ab = ba = 1$. We call a commutative division ring a **field**.

**Example 1.1.** Let $R$ be an abelian group under an operation $+$, define the operation $\cdot$ by $(a, b) \to ab = 0$ for all $a, b \in R$. Then $R$ is a ring under $+$ and $\cdot$, called the **trivial ring**. If $R = \langle e \rangle$, the trivial group, then we call $R$ the **zero ring**.

(2) The integers $\mathbb{Z}$ form a ring under the usual addition and muiltiplication.

(3) The sets of rational numbers $\mathbb{Q}$ and the set of real numbers $\mathbb{R}$ are rings under their usual addition and multiplication; in fact, they are fields. The complex numbers $\mathbb{C}$ also form a field under complex addition and complex multiplication, where

$$+ : (a + ib, c + id) \to (a + c) + i(b + d)$$
$$\cdot : (a + ib, c + id) \to (ac - bd) + i(ad + bc)$$

(4) The factor group of integers modulo $n$, $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring under addition modulo $n$, and multiplication modulo $n$, $\mathbb{Z}/n\mathbb{Z}$ has identity $1 \mod n$. $\mathbb{Z}/n\mathbb{Z}$ forms a field if, and only if $n = p^r$, where $p$ is a prime.

(5) We define the **real quaternions** to be the set $\mathbb{H} = \{a + ib_jc_kd : a, b, c, d \in \mathbb{R}, i^2 = j^2 = k^2 = -1 \text{ and } ij = k, jk = i, \text{ and } ki = j\}$. $\mathbb{H}$ is a ring under addition and multiplication are defined for all $x = a + ib + jc + kd$ and $y = e + if + jg + kh$ to be:

$$+(x, y) : \to x + y = (a + e) + i(b + f) + j(c + g) + k(d + h)$$
$$\cdot(x, y) : \to xy = (a + ib + jc + kd)(e + if + jg + kh)$$

(6) Let $A$ be a ring and $R$ the set of all maps $f : X \to A$. Then $R$ forms a ring under function addition $f + g(x) = f(x) + g(x)$ and function multiplication $fg(x) = f(x)g(x)$. Notice that $R$ is commutative if, and only if $A$ is, moreover, $R$ has identity if, and only if $A$ has identity.

(7) We say a realvalued function $f : \mathbb{R} \to \mathbb{R}$ has **compact support** if there exist $a, b \in \mathbb{R}$ such that $f(x) = 0$ for all $x \notin [a, b]$. The set of all functions with compact support forms a ring without identity under function addition and function multiplication.

(8) Let $X, Y \subseteq \mathbb{R}$. We denote the set of all continuous functions $f : X \to Y$ by $C(X, Y)$. Then $C(X, Y)$ forms a commutative ring with identity under function addition and function multiplication.

**Lemma 1.1.1.** *Let $R$ be a ring. Then the following are true for all $a, b \in R$.*

*(1)* $0a = a0 = 0$.

*(2)* $(-a)b = a(-b) = -(ab)$.

*(3)* $(-a)(-b) = ab$

*(4) If $R$ has identity $1 \neq 0$, then $1$ is unique and $-a = (-1)a$.*

*Proof.* (1) Notice $0a = (0 + 0)a = 0a + 0a$, so that $0a = 0$. Likewise, $a0 = 0$ by the same reasoning.

(2) Notice that $b - b = 0$, so $a(b - b) = ab + a(-b) = 0$, so that $a(-b) = -(ab)$. The same argument with $(a - a)b$ gives $(-a)b = -(ab)$.

(3) By the inverse laws of addition in $R$, we have $-(a(-b)) = -(-(ab))$, so that $(-a)(-b) = ab$.

(4) Suppose $R$ has identity $1 \neq 0$, and suppose there is an element $2 \in R$ for which $2a = a2 = a$ for all $a \in R$. Then we have that $1 \cdot 2 = 1$ and $1 \cdot 2 = 2$, making $1 = 2$; so 1 is unique. Now, we have that $a + (-a) = 0$, so that $1(a + (-a)) = 1a + 1(-a) = 1a + (-a) = 0$ So $(-a) = -(1a) = (-1)a$ by (2).

■

**Definition.** Let $R$ be a ring. We call an element $a \in R$ a **zero divisor** if $a \neq 0$ and there exists an element $b \neq 0$ such that $ab = 0$. Similarly, we call $a \in R$ a **unit** if there is a $b \in R$ for which $ab = ba = 1$.

**Example 1.2.** Notice if $R$ is a ring with identity 1, then 1 is a unit of $R$ by definition.

**Definition.** Let $R$ be a ring. We call the set of all units in $R$ the **group of units** and denote it $R^*$

**Lemma 1.1.2.** *Let $R$ be a ring with identity $1 \neq 0$. Then the group of units $R^\times$ forms a group under multiplication.*

*Proof.* Let $a, b \in R$ be units in $R$. Then there are $c, d \in R$ for which $ac = ca = 1$ and $bd = db = 1$. Consider then $ab$. Then $ab(dc) = a(bd)c = ac = 1$ and $(dc)ab = d(ca)b = db = 1$ so that $ab$ is also a unit in $R$. Moreover $R^*$ inherits the associativity of $\cdot$ and 1 serves as the identity element of $R^*$. Lastly, if $a \in R^*$ is a unit there is a $b \in R$ for which $ab = ba = 1$. This also makes $b$ a unit in $R$, and the inverse of $a$. ■

**Corollary.** *$a$ is a zero divisor if, and only if it is not a unit.*

*Proof.* Suppose that $a \neq 0$ is a zero divisor. Then there is a $b \in R$ such that $b \neq 0$ and $ab = 0$. Then for any $v \in R$, $v(ab) = (va)b = 0$ so that $a$ cannot be a unit. On the other hand let $a$ be a unit, and $ab = 0$ for some $b \neq 0$. Then there is a $v \in R$ for which $v(ab) = (va)b = 1b = b = 0$. Then $b = 0$ which is a contradiction. ■

**Corollary.** *If $R$ is a field, then it has no zero divisors.*

*Proof.* Notice by definition of a field, every element is a unit, except for 0. ■

**Example 1.3.** (1) $\mathbb{Z}$ has no zero divisors, and has as units the elements $-1$ and 1.

(2) For any $n \in \mathbb{Z}^+$, the units of $\mathbb{Z}/n\mathbb{Z}$ are all elements $a \mod n$ such that $(a, n) = 1$. That is ${\mathbb{Z}/n\mathbb{Z}}^* = U(\mathbb{Z}/n\mathbb{Z})$; recall that $U(\mathbb{Z}/n\mathbb{Z})$ is called the unit group, or group of units of $\mathbb{Z}/n\mathbb{Z}$.

(3) Let $D \in \mathbb{Q}$ be squarefree. Define $\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} : a, b \in \mathbb{Q}\}$. Then $\mathbb{Q}(\sqrt{D})$ is a field called the **quadratic field** under the operations

$$
\begin{aligned}
+ &: (a + b\sqrt{D}, c + d\sqrt{D}) \to (a + c) + (b + d)\sqrt{D} \\
&\cdot((a + b\sqrt{D}, c + d\sqrt{D})) \to (ac - bdD) + (ad - bc)\sqrt{D}
\end{aligned}
$$

Since $\mathbb{Q}(\sqrt{D})$ is a field, every element is a unit.

**Definition.** A commutative ring with identity $1 \neq 0$ is called an **integral domain** if it has no zero divisors.

**Lemma 1.1.3.** *Let $R$ be a ring, and $a$ not a zero divisor. Then if $ab = ac$, then either $a = 0$, or $b = c$.*

*Proof.* Notice that $ab = ac$ implies $ab - ac = a(b-c) = 0$. Since $a$ is not a zero divisor, either $a = 0$ or $b - c = 0$. ■

**Corollary.** *Any finite integral domain is a field.*

*Proof.* Let $R$ be a finite integral domain and consider the map on $R$, by $x \to ax$. By above, this map is 1–1, moreover since $R$ is finite, it is also onto. So there is a $b \in R$ for which $ab = 1$, making $a$ a unit. Since $a$ is abitrarily chosen, this makes $R$ a field. ■

**Corollary.** *If $R$ is a field it is a (not necessarily finite) integral domain.*

**Example 1.4.** We have that fields are integral domains, and finite integral domains are fields. However, notice that not every integral domain need be a field. $\mathbb{Z}$ is an integral domain that is not a field. Moreover, so are the real quaternions $\mathbb{H}$.

**Definition.** A **subring** of a ring $R$ is a subgroup of $R$ closed under multiplication.

**Example 1.5.** (1) We have the following sequence of subgrings $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

(2) The factor group $\mathbb{Z}/n\mathbb{Z}$ is not a subgring of $\mathbb{Z}$, well the multiplication and addition of $\mathbb{Z}$ is different from that of $\mathbb{Z}/n\mathbb{Z}$.

(3) The set $\mathbb{Z} + i\mathbb{Z} + j\mathbb{Z} + k\mathbb{Z} \subseteq \mathbb{H}$ is a subring of $\mathbb{H}$.

(4) If $F$ is a field, then any subring of $F$ is also an integral domain by inheretence.

(5) The set $\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} : a, b \in \mathbb{Z}\}$ is a subring of the quadratic field $\mathbb{Q}(\sqrt{D})$. Moreover if $D \equiv 1 \mod 4$, then the set

$$\mathbb{Z}[\frac{1+\sqrt{D}}{2}] = \{a + b\frac{1+\sqrt{D}}{2} : a, b \in \mathbb{Z}\}$$

is also a subring of $\mathbb{Q}(\sqrt{D})$. We call the subring $\mathbb{Z}[\omega]$, where

$$\omega = \begin{cases} \sqrt{D}, & \text{if } D \not\equiv 1 \mod 4 \\ \frac{1+\sqrt{D}}{2}, & \text{if D} \equiv 1 \mod 4 \end{cases}$$

the **ring of integers** in the quadratic field. When $D = -1$, we get the ring $\mathbb{Z}[i]$, with $i^2 = -1$ and call it the **Gaussian integers**. Notice then that $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$; in fact, it is field in $\mathbb{C}$.

(6) Consider $\mathbb{Q}(\sqrt{D})$ where $D$ is squarefree. We define the **field norm** $N : \mathbb{Q}(\sqrt{D}) \to D$ by taking $(a + b\sqrt{D}) \to (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2$. If $D = i^2 = -1$, then $N : a + ib \to a^2 + b^2$ which is the modulus of complex number restricted to $\mathbb{Q}$.

Notice that if $z = a + b\sqrt{D}$, $w = c + d\sqrt{D}$, then $N(zw) = N(z)N(w)$ moreover,

$$N(a + \omega b) = \begin{cases} a^2 - Db^2, & \text{if } D \equiv 2, 3 \mod 4 \\ a^2 + ab + \frac{1-D}{4}, & \text{if } D \equiv 1 \mod 4 \end{cases}$$

where

$$\omega = \begin{cases} \sqrt{D}, \text{ if } D \not\equiv 1 \mod 4 \\ \frac{1+\sqrt{D}}{2}, \text{ if } D \equiv 1 \mod 4 \end{cases}$$

In either case, $N : \mathbb{Z}[\omega] \to \mathbb{Z}$.

**Lemma 1.1.4.** *Let* $\omega = \begin{cases} \sqrt{D}, \text{ if } D \not\equiv 1 \mod 4 \\ \frac{1+\sqrt{D}}{2}, \text{ if } D \equiv 1 \mod 4 \end{cases}$ *where* $D \in \mathbb{Z}^+$ *is squarefree. Then an element of* $z \in \mathbb{Z}[\omega]$ *is a unit if, and only if* $N(z) = \pm 1$

*Proof.* Let $z = a + \omega b$ such that $N(z) = \pm 1$. Then we have

$$z^{-1} = \pm(a + \overline{\omega} b) \in \mathbb{Z}[\omega]$$

making it a unit. On the other hand, if $N(zw) = N(z)N(w) = \pm 1$, then since $N(z), N(w) \in \mathbb{Z}$, we must have that both $N(z) = \pm 1$ and $N(w) = \pm 1$. ■

## 1.2 Polynomail Rings, Matrix Rings, and Group Rings.

**Theorem 1.2.1.** *Let* $R$ *be a commutative ring with identity, and define* $R[x] = \{f(x) = a_0 + a_1 x + \cdots + a_n x^n : a_0, \ldots a_n \in R\}$. *Define the operations* $+$ *and* $\cdot$ *on* $R[x]$ *for* $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ *and* $g(x) = b_0 + b_1 x + \cdots + b_n x^n$ *by:*

$$f + g = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n$$

$$fg = c_0 + c_1 x + \cdots + c_k x^k \text{ where } c_j = \sum_{i=0}^{j} a_i b_{j-i} \text{ and } k = n + m$$

*Then* $R[x]$ *is a commutative ring with identity.*

**Definition.** Let $R$ be a commutative ring with identity. We call the ring $R[x]$ the **ring of polynomials** in $x$ with **coefficients** in $R$ whose elements of the form

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

where $n \geq 0$ are called **polynomails**. If $a_n \neq 0$, then the **degree** of $f$ is denoted $\deg f = n$, and $f$ is called **monic** if $a_n = 1$. We call $+$ and $\cdot$ the **addition** and **multiplication** of polynomials.

**Example 1.6.** (1) Take $R$ any commutative ring with identity and form $R[x]$. One can verify that the polynomial $0(x) = 0 + 0x + \cdots + 0x^n + \cdots = 0$, in this case we call 0 the **zero polynomial**. Similarly, the additive inverse of $f(x) = a_0 + a_1 x^1 + \cdots + a_n x^n$ is the polynomial $-f(x) = -a_0 - a_1 x^1 - \cdots - a_n x^n$. Now, since $R[x]$ has identity, the **identity** polynomial is $1(x) = 1 + 0x + \cdots = 1$, that is, it is the identity in $R$. Lastly, we call a polynomial $f$ with $\deg f = 0$ a **constant polynomial**. Notice that 0 and 1 are constant polynomials.

(2) $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$ and $\mathbb{C}[x]$ are the polynomial rings in $x$ with coeffiients in $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ respectively.

(3) Notice that the rings $\mathbb{Z}[\omega]$ and $\mathbb{Z}[i]$ are polynomial rings in $\omega$ and $i$, respectively, with coefficients in $\mathbb{Z}$, and where $\omega = \sqrt{D}$ if $D \not\equiv 1 \mod 4$ or $\omega = \frac{1+\sqrt{D}}{2}$ otherwise, and $i^2 = -1$. Notice that the highest degree a polynomial in $\mathbb{Z}[i]$ can achieve is deg $= 1$; however, one may be able to form polynomial rings in other variables with coefficients in $\mathbb{Z}[i]$, i.e. take $Z[x]$, where $Z = \mathbb{Z}[i]$.

(4) ${}^{\mathbb{Z}}\!/_{3\mathbb{Z}}[x]$ is the polynomial ring with coefficients in ${}^{\mathbb{Z}}\!/_{3\mathbb{Z}}$.

**Theorem 1.2.2.** *Let $R$ be an integral domain, and let $p, q \neq 0$ be polynomials in $R[x]$. Then the following are true:*

*(1)* $\deg pq = \deg p + \deg q$.

*(2) The units of $R[x]$ are precisely the units of $R$*

*(3) $R[x]$ is an integral domain.*

*Proof.* Consider the leading terms $a_n x^n$ and $b_m x^m$ of $p$ and $q$ respectively. Then $a_n b_m x^{m+n}$ is the leading term of $pq$; moreover we require $a_n b_m \neq 0$. Now, if $\deg pq < m + n$, then $ab = 0$, making $a$ and $b$ zero divisors of $R$; impossoble. Therefore $ab \neq 0$. It also follows that since no term of $p$ is a zero divisor, then $p$ cannot be a zero divisor of $R[x]$. Lastly, if $pq = 1$, then $\deg p + \deg q = 0$, so that $pq$ is a constant polynomial. Noticing that constant polynomials are simply just elements of $R$, then $p$ and $q$ are units. ∎

**Theorem 1.2.3.** *Let $R$ be a ring. Let $R^{n\times n}$ be the set of all $n \times n$ matrices with entries in $R$ and define the operations $+$ and $\cdot$ by:*

$$(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij})$$

$$(a_{ij})(b_{ij}) = (c_{ij}), \text{ where } c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$$

*Then $R^{m\times n}$ forms a ring under $+$ and $\cdot$.*

**Definition.** For any ring $R$, we call the ring $R^{n\times n}$ the **matrix ring** of $n \times n$ matrices with entries in $R$.

**Example 1.7.** (1) Note that if $R$ is a commutative ring, then for $n \geq 2$, $R^{n\times n}$ need not be commutative.

(2) We call matrices of $R^{n\times n}$, for $n \in \mathbb{Z}^+$ **square matrices**. We call a matrix $(a_{ij}) \in R^{n\times n}$ **scalar** if $a_{ii} = 1$ for all $1 \leq i \leq n$ and $a_{ij} = 0$ whenever $i \neq j$.

(3) If $R$ has identity, then so does $R^{n\times n}$. We call the identity of $R^{n\times n}$ the **identity matrix** and denote it as the $n \times n$ scalar matrix $I$ with 1 across the diagonal. We call the units of $R^{n\times n}$ **invertible** matrices, and denote the unit group of invertible matrices to be $GL(n, R)$ the general linear group of degree $n$ over $R$.

(4) Notice that $2\mathbb{Z}^{n\times n} \subseteq \mathbb{Z}^{n\times n} \subseteq \mathbb{Q}^{n\times n} \subseteq \mathbb{R}^{n\times n} \subseteq \mathbb{C}^{n\times n}$.

(5) Let $R$ be a ring, and $R^{n\times n}$ its matrix ring. Let $U^{n\times n} = \{(a_{ij}) : a_{pq} = 0 \text{ whenever } p > q\}$ the set of **upper triangular matrices**. Then $U^{n\times n} \subseteq R^{n\times n}$ is a subring.

**Theorem 1.2.4.** *Let $R$ be a ring with identity, and let $G$ be a finite group of order $n$. Let $RG$ the set of all sums $a_1g_1+\cdots+a_ng_n$, where $a_i \in R$ for all $1 \leq i \leq n$. Define the operations $+$ and $\cdot$ by:*

$$(a_1g_1 + \cdots + a_ng_n) + (b_1g_1 + \cdots + b_ng_n) = (a_1 + b_1)g_1 + \cdots + (a_n + b_n)g_n$$
$$(a_1g_1 + \cdots + a_ng_n)(b_1g_1 + \cdots + b_ng_n) = c_1g_1 + \cdots + c_ng_n, \text{ where } c_k = \sum_{g_k=g_ig_j} a_ib_j$$

*Then $RG$ forms a ring with identity under $+$ and $\cdot$. Moreover, $RG$ is commutative if, and only if $G$ is abelian.*

**Definition.** Let $R$ be a ring with identity, and let $G$ be a finite group of order $n$. We call the ring $RG$ the **group ring** of $G$. We call the elements of $RG$ **formal sums** of the elements of $G$.

**Example 1.8.** (1) Consider $D_8 = \langle r, t : r^4 = t^2 = 1, rt = tr^{-1}\rangle$ and $\mathbb{Z}$. Let $a, b \in \mathbb{Z}D_8$ where $a = r + r^2 - 2t$ and $b = -3r^2 + rt$. Then

$$a + b = r - 2r^2 + rt - t$$
$$ab = -5r^3 + r^3t + 7r^2t - 3$$

(2) For any ring with identity $R$, and finite group $G$, $R \subseteq RG$, for take the elements of $R$ to be the sums $a_1 + \cdots + a_n$. $G \subseteq RG$, for $g_i = 1g_i$; moreover, each $g_i$ has an inverse in $RG$, so we call $G$ the subgroup of units of $RG$.

(3) Let $G$ be a group with $\operatorname{ord} G > 1$. Let $g \in G$ with $\operatorname{ord} g = m$. Notice that the elements $(1 - g), (1 + g + \cdots + g^{m-1}) \in RG$ are nonzero, but that

$$(1 - g)(1 + g + \cdots + g^{m-1}) = 1 - g^m = 1 - 1 = 0$$

which makes $1-g$ a zero divisor. In general, the ring $RG$ will always have zero divisors.

(4) Let $G$ be a finite group. We call the rings $\mathbb{Z}G$, $\mathbb{Q}G$, $\mathbb{R}G$, and $\mathbb{C}G$ the **integral**, **rational**, **real**, and **complex** group rings of $G$, respectively. Notice that $\mathbb{Z}G \subseteq \mathbb{Q}G \subseteq \mathbb{R}G \subseteq \mathbb{C}G$. Moreover, if $H \leq G$ is a subgroup of $G$, then $RH \subseteq RG$ is a subring.

## 1.3 Ring Homomorphisms and Factor Rings.

**Definition.** Let $R$ and $S$ be rings. We call a map $\phi : R \to S$ a **ring homomorphism** if

(1) $\phi$ is a group homomorphism with respect to addition.

(2) $\phi(ab) = \phi(a)\phi(b)$ for any $a, b \in R$.

We denote the **kernel** of $\phi$ to be the kernel of $\phi$ as a group homomorphism. That is

$$\ker\phi = \{r \in R : \phi(r) = 0\}$$

Moreover, if $\phi$ is 1–1 and onto, we call $\phi$ an **isomorphism** and say that $R$ and $S$ are **isomorphic**, and write $R \simeq S$.

**Example 1.9.** (1) $\phi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ defined by $n \to 0$ if $n$ is even and $n \to 1$ if $n$ is odd is a ring homomorphism, with $\ker\phi = 2\mathbb{Z}$. Notice that $\phi(\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$. $\phi$ is onto, but not 1–1.

(2) Let $n \in \mathbb{Z}$ and consider the maps $\phi_n : \mathbb{Z} \to \mathbb{Z}$ by taking $x \to nx$. $\phi_n$, in general is not a ring homomorphism, as $\phi(xy) = n(xy)$ but $\phi(x)\phi(y) = nxny = n^2(xy)$. $\phi_n$, however is a group homomorphism for any $n$.

(3) For any ring $R$, define the **valuation** map $\phi : R[x] \to R$ by taking $f(x) \to f(0)$; i.e. the polynomial $f$ evaluated at 0. $\phi$ is a ring homomorphism. Moreover, notice that if $f(x) = a_0 + a_1x + \cdots + a_nx^n$, then $f(0) = a_0 \in \mathbb{R}$. So that $\phi(R[x]) = R$ This makes $\phi$ onto. Now, take $\phi(f) = 0$, Then those are all polynomials with constant term $a_0 = 0$ (this does not make $\ker\phi = \langle e \rangle$). Again, $\phi$ is onto, but it is not 1–1.

**Lemma 1.3.1.** *Let $R$ and $S$ be rings, and $\phi : R \to S$ a ring homomorphism. Then*

*(1) $\phi(R)$ is a subring of $S$.*

*(2) $\ker\phi$ is a subring of $R$.*

*Proof.* Let $s_1, s_2 \in \phi(R)$. Then $s_1 = \phi(r_1)$ and $s_2 = \phi(r_2)$ for some $r_1, r_2 \in R$. Then $s_1s_2 = \phi(r_1)\phi(r_2) = \phi(r_1r_2) \in \phi(S)$. Additionally, $s^{-1} = \phi^{-1}(r) = \phi(r^{-1})$ for some $s \in S$, $r \in R$. This is sufficient to make $S$ a subring of $S$.

By similar reasoning, if $r_1, r_2 \in \ker\phi$, then $\phi(r_1)\phi(r_2) = \phi(r_1r_2) = 0$ so that $r_1r_2 \in \ker\phi$, and $\phi(r^{-1}) = \phi^{-1}(r) = 0$ so $\phi^{-1} \in \ker\phi$. ■

**Corollary.** *For any $r \in R$ and $a \in \ker\phi$, then $ar \in \ker\phi$ and $ra \in \ker\phi$.*

*Proof.* We have $\phi(ar) = \phi(a)\phi(r) = \phi(a)0 = 0$ so $ar \in \ker\phi$. The same happens for $ra$. ■

**Definition.** Let $R$ be a ring. We call a subring $I \subseteq R$ of $R$ a **left ideal** in $R$ if for any $r \in R$ and $a \in I$, we have $ar \in I$. Similarly, we call $I$ a **right ideal** in $R$ if $ra \in I$. We call $I$ a (**two-sided**) **ideal** in $R$ if it is both a left, and a right ideal and we say that the ideals $I$ **absorb** $r$.

**Lemma 1.3.2.** *If $R$ is a commutative ring, then every left ideal is a right ideal.*

*Proof.* Notice that $ar = ra$ for all $a, r \in R$. ■

**Theorem 1.3.3.** *Let $R$ be aring, and $I$ an ideal in $R$. Let ${}^{R}\!/_{I}$ be the set of all $a+I$ with $a \in R$. Define operations $+$ and $\cdot$ by*

$$(a+I)+(b+I) = (a+b)+I$$
$$(a+I)(b+I) = ab+I$$

*Then ${}^{R}\!/_{I}$ forms a ring under $+$ and $\cdot$.*

*Proof.* Notice that $(a+I)+(b+I) = (a+b)+(I+I) = (a+b)+2I = (a+b)+I$. Moreover, ${}^{R}\!/_{I}$ inherits associativity in $+$ from addition in $R$. Now, take $0+I = I$ as the additive identity and $-a+I$ as the inverse of $a+I$ for each $I$.

Now, notice, that $(a+I)(b+I) = ab+aI+bI+I^2 = ab+(I+I+I) = ab+I$ by distribution of multiplication over addition in $R$. Moreover, ${}^{R}\!/_{I}$ also inherits associativity in $\cdot$ of ultiplication in $R$. Now, notice then that

$$(a+I)((b+I)+c+I) = (a+I)((b+c)+I) = a(b+c)+I = (ab+ac)+I = (ac+I)+(bc+I)$$

and

$$((a+I)+(b+I))(c+I) = ((a+b)+I)(c+I) = (a+b)c+I = (ac_bc)+I = (ac+I)+(bc+I)$$

Lastly, notice that $a+I$ is just the left coset of $a$ by $I$ in $R$ as a group under addition. So that $+$ and $\cdot$ are coset addition and multiplication, which are well defined. ■

**Corollary.** *If $R$ has identity $1$, then ${}^{R}\!/_{I}$ has identity $1+I$. Moreover if $R$ is commutative, then so is ${}^{R}\!/_{I}$.*

**Definition.** Let $R$ be a ring and $I$ an ideal in $R$. We call the ring ${}^{R}\!/_{I}$ under addition and muiltplication of cosets the **factor ring** (or **quotient ring**) of $R$ over $I$.

**Example 1.10.** (1) We call $(0) = \{0\}$ the **trivial ideal**, notice also that $R$ is also an ideal.

(2) For any $n \in \mathbb{Z}$, notice that if $a \in \mathbb{Z}$ and $m \in n\mathbb{Z}$, then $m = nk$, for some $k \in \mathbb{Z}$ so that $am = n(ak) = ma \in n\mathbb{Z}$. So $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$, with factor ring ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$. So ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ is a factor ring on top of also being a factor group. We call the ring homomorphisme $\phi : \mathbb{Z} \to {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ by $a \to a \mod n$ the **reduction homomorphism**.

(2) Let $R$ a ring, and consider $R[x]$. Let $I$ the set of all polynomials of degree greater than 2 together with 0. Then if $f \in I$, $\deg f > 2$ or $f = 0$. Then for any $g \in R[x]$, $\deg fg > 2$ or, $fg = 0$ and $\deg gf > 2$ or $gf = 0$. This makes $I$ an ideal of $R[x]$. Moreover, $p, q \in I$ if and only if they have the same constant term. Notice then that ${}^{t\mathbb{R}[x]}\!/_{I} = \{a+bx : a, b \in R\}$.

Now, if $R$ has no zero divisors, it is possible that ${}^{R[x]}\!/_{I}$ has zero divisors. Consider ${}^{\mathbb{Z}[x]}\!/_{I}$.

(3) Let $A$ a ring, and $X \neq \emptyset$. For the ring of functionss $A^X$, for a given $c \in X$, define the **valuation** map at $c$ by $E_c : f(x) \to f(c)$. Notice that $E_c$ is a ring homomorphism, so that ${}^{A^X}\!/_{\ker E_c}$ forms a factor ring. IN particular, if $A^X = A[x]$ the polynomial ring over $A$, and $c = 0$, then $E_c$ is just the valuation map of polynomials.

Now, if $X = (0, 1]$, and $R = \mathbb{R}^{(0,1]}$, by the first isomorphism theorem, we have $\mathbb{R} \simeq {}^{\mathbb{R}^{(0,1]}}\!/_{\ker E_c}$, since $E_c(\mathbb{R}^{(0,1]}) = \mathbb{R}$.

(4) Let $n \geq 2$ and consider $R^{n\times n}$. Let $J$ an ideal of $R$. Then $J^{n\times n} = \{(a_{ij}) : a_{ij \in J}\}$ is an ideal of $R^{n\times n}$. Take the ring homomorphism

$$R^{n\times n} \to ({}^{R}\!/_{J})^{n\times n}$$
$$(a_{ij}) \to (a_{ij} + J)$$

Then $J^{n\times n}$ is the kernel of this homomorphism, so that

$${}^{R^{n\times n}}\!/_{J^{n\times n}} \simeq ({}^{R}\!/_{J})^{n\times n}$$

For example, with $n = 3$, we have

$${}^{\mathbb{Z}^{3\times 3}}\!/_{2\mathbb{Z}^{3\times 3}} \simeq ({}^{Z}\!/_{2\mathbb{Z}})^{3\times 3}$$

(5) Let $R$ a commutative ring with identity, and $G$ a finite group of order $n$. Define the **augmentation** map to be the map

$$RG \to R$$
$$\sum_{i=1}^{n} a_i g_i \to \sum_{i=1}^{n} a_i$$

We call the kernel of this map the **augmentation ideal** which is the set of all formal sums whose coefficients sum to 0. Another ideal of $RG$ is the set $I = \{\sum a g_i : g_i \in G\}$ the set of all formal sums whose coefficients are all equal.

**Theorem 1.3.4** (The First Isomorphism Theorem). *If $\phi : R \to S$ is a ring homomorphism from rings $R$ into $S$, then* $\ker \phi$ *is an ideal of $R$ and*

$$\phi(R) \simeq {}^{R}\!/_{\ker \phi}$$

$$\begin{tikzcd}
R \arrow[r, "\phi"] \arrow[d, "\pi"'] & S \\
{}^{R}\!/_{\ker \phi} \arrow[ur, "\overline{\phi}"'] &
\end{tikzcd}$$

*Proof.* By the first isomorphism theorem for groups, $\phi$ is a group isomorphism. Now, let $K = \ker \phi$ and consider the map $\pi : R \to R/I$ by $a \xrightarrow{\pi} a+K$. Define the map $\overline{\phi} : R/K \to \phi(R)$ such that $\overline{\phi} \circ \pi = \phi$, then $\overline{\phi}$ defines the ring isomorphism. ■

*Proof.* The map $\pi : R \to R/I$ defined by $a \to a + I$, for any ideal $I$, is onto, with $\ker \pi = I$. ■

**Theorem 1.3.5** (The Second Isomorphism Theorem)**.** *Let $A \subseteq R$ a subring of $R$, and let $B$ an ideal in $R$. Define $A + B = \{a + b : a \in A \text{ and } b \in B\}$. Then $A + BR$ is a subring and $A \cap B$ is an ideal in $A$. Then*

$$A + B/B \simeq A/A \cap B$$

**Theorem 1.3.6** (The Third Isomorphism Theorem)**.** *Let $I$ and $J$ be ideals in a ring $R$, with $I \subseteq J$. Then $J/I$ is an ideal of $R/I$ and*

$$R/J = (R/I)/(J/I)$$

**Theorem 1.3.7** (The Fourth Isomorphism Theorem)**.** *Let $I$ an ideal in a ring $R$, then the correspondence between $A$ and $A/I$, for any subring $A \subseteq R$ is an inclusion preserving bijection between subrings of $A$ containing $I$ and $R/I$. Moreover, $A$ is an ideal if, and only if $A/I$ is an ideal.*

**Example 1.11.** We have $12\mathbb{Z}$ is an ideal of $\mathbb{Z}$, and that $\mathbb{Z}/12\mathbb{Z}$ has as ideals

$$\mathbb{Z}/12\mathbb{Z} \qquad 2\mathbb{Z}/12\mathbb{Z} \qquad 3\mathbb{Z}/12\mathbb{Z} \qquad 4\mathbb{Z}/12\mathbb{Z} \qquad 6\mathbb{Z}/12\mathbb{Z} \qquad 12\mathbb{Z}/12\mathbb{Z}$$

**Lemma 1.3.8.** *Let $R$ be a ring with ideals $I$ and $J$. Then $I + J$, $IJ$ and $I^n$, for any $n \geq 0$ are ideals of $R$ and we have the lattice*

$$\begin{tikzcd}
 & R \arrow[d, no head] & \\
 & I+J \arrow[dl, no head] \arrow[dr, no head] & \\
I \arrow[dr, no head] & & J \arrow[dl, no head] \\
 & IJ \arrow[d, no head] & \\
 & (0) &
\end{tikzcd}$$

**Example 1.12.** (1) COnsider the ideals $6\mathbb{Z}$ and $10\mathbb{Z}$ of $\mathbb{Z}$. Then $6\mathbb{Z} + 10\mathbb{Z}$ is the ideal consisting of all integers of the form $6x + 10y$. Now, for $x, y \in \mathbb{Z}$, since $(6, 10) = 2$, we have that $6\mathbb{Z} + 10\mathbb{Z} \subseteq 2\mathbb{Z}$ since $6x + 10y = 2(3x + 5y)$. Now, we also have that $2 = 6 \cdot 2 + 10 \cdot -1$ so that $2 \in 6\mathbb{Z} + 10\mathbb{Z}$ which makes $2\mathbb{Z} \subseteq 6\mathbb{Z} + 10\mathbb{Z}$. Thus, we have $6\mathbb{Z} + 10\mathbb{Z} = 2\mathbb{Z}$. In general, we have that $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$ where $d = (m, n)$ is the greatest common divisor of $m$ and $n$. The ideal $6\mathbb{Z}10\mathbb{Z}$ gives all integers of the form $6x10y = 6 \cdot 10(xy) = 60(xy)$, so that $6\mathbb{Z}10\mathbb{Z} = 60\mathbb{Z}$.

(2) Let $I \subseteq \mathbb{Z}[x]$ the ideal of polynomials with even constant term. Notce that $2, x = x + 0 \in I$ so tht $4, x^2 \in I^2 = II$. So that $4 + x^2 \in I^2$ which is not in general divisible by elements in $I$.

## 1.4 Ideals.

**Definition.** Let $R$ be a commutative ring with identity. We call the smallest ideal containing a nonempty subset $A$ in $R$ the **ideal generated** by $A$, and we write $(A)$. We call an ideal **principle** if it is generated by a single element of $R$, i.e. $I = (a)$ for some $a \in I$. We say that the ideal $(A)$ is **finitely generated** if $|A|$ is finite, and if $A = \{a_1, \dots, a_n\}$, then we denote $(A) = (a_1, \dots, a_n)$.

# Bibliography

[1] D. Dummit, *Abstract algebra.* Hoboken, NJ: John Wiley & Sons, Inc, 2004.

[2] I. N. Herstein, *Topics in algebra.* New York: Wiley, 1975.