Ring Theory and Module Theory.

Alec Zabel-Mena

October 19, 2023

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) For any $a, b \in R$, $ab \in R$ and $a(bc) = (ab)c$. That is, R is closed under multiplication, and multiplication is associative.

(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 $\mathcal{U}(R)$, or R^*.

Lemma 1.1.2. *Let R be a ring with identity $1 \neq 0$. Then the group of units $\mathcal{U}(R)$ 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

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

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 subgring of $\mathbb{Q}(\sqrt{D})$. We call the subgring $\mathbb{Z}[\omega]$, 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* $R[x] = \{f(x) = a_0 + a_1 x + \cdots + a_n x^n : a_0, \dots a_n \in R\}$. *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 ω 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) ϕ 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 ϕ to be the kernel of ϕ as a group homomorphism. That is

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

Moreover, if ϕ is 1–1 and onto, we call ϕ 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 $\phi(\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$. ϕ 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 $x \to nx$. ϕ_n, in general is not a ring homomorphism, as $\phi(xy) = n(xy)$ but $\phi(x)\phi(y) = nxny = n^2(xy)$. ϕ_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. ϕ is a ring homomorphism. Moreover, notice that if $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, then $f(0) = a_0 \in \mathbb{R}$. So that $\phi(R[x]) = R$ This makes ϕ 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, ϕ 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 $s_1 s_2 = \phi(r_1)\phi(r_2) = \phi(r_1 r_2) \in \phi(S)$. 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 $\phi(r_1)\phi(r_2) = \phi(r_1 r_2) = 0$ so that $r_1 r_2 \in \ker \phi$, 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 subgroup $I \leq R$ 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

$$\begin{aligned} R^{n\times n} &\to (R/J)^{n\times n} \\ (a_{ij}) &\to (a_{ij} + J) \end{aligned}$$

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

$$\begin{aligned} RG &\to R \\ \sum_{i=1}^{n} a_i g_i &\to \sum_{i=1}^{n} a_i \end{aligned}$$

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, ϕ 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*

$$\begin{tikzcd}[arrows=dash]
 & R \arrow[d] & \\
 & I+J \arrow[dl] \arrow[dr] & \\
I \arrow[dr] & & J \arrow[dl] \\
 & IJ \arrow[d] & \\
 & (0) &
\end{tikzcd}$$

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 $A = \{a_1, \ldots, a_n\}$, then we denote $(A) = (a_1, \ldots, a_n)$.

Example 1.13. (1) In any commutative ring with identity, the trivial ideal and R are the ideals generated by 0 and 1, respectively, so we write them as (0) and $R = (1)$.

(2) In $\mathbb{Z}$, we can write the ideals $n\mathbb{Z} = (n) = (-n)$. Notice that every ideal in $\mathbb{Z}$ is a principle ideal. Moreover, for $m, n \in \mathbb{Z}$, $n|m$ if, and only if $n\mathbb{Z} \subseteq n\mathbb{Z}$. Notice that $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$ is the ideal generated by n and n, where $d = (m, n)$ is the greatest common divisor of m and n. Indeed, by definition, $d|m, n$ so that $d\mathbb{Z} \subseteq m\mathbb{Z} + n\mathbb{Z}$, and if $c|m, n$, then $c|d$, making $m\mathbb{Z} + n\mathbb{Z} \subseteq d\mathbb{Z}$. Then $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$ is the ideal generated by the greatest common divisor (m, n) and consists of all diophantine equations of the form

$$mx + ny = (m, n)$$

In general, we can define the **greatest common divisor** for integers $n_1, n_2, \ldots, n_m$ to be the smallest such integer d generating the ideal $n_1\mathbb{Z} + \cdots + n_m\mathbb{Z} = d\mathbb{Z}$. We then write $d = (n_1, \ldots, n_m)$.

(3) Consider the ideal $(2, x)$ of $\mathbb{Z}[x]$. $(2, x)$ is not a principle ideal. We have that $(2, x) = \{2p_xq : p, q \in \mathbb{Z}[x]\}$, and that $(2, x) \neq \mathbb{Z}[x]$. Suppose that $(2, x) = (a)$ for some polynomial $a \in \mathbb{Z}[x]$, then $2 \in (a)$, so that $2 = p(x)a(x)$, of degree $\deg p + \deg a$. This makes p and a constant polynomials in $\mathbb{Z}[x]$. Now, since 2 is prime in $\mathbb{Z}$, then only values for p and q are $p = \pm 1$ and $a = \pm 2$. If $a(x) = \pm 1$, then every polynomial in $\mathbb{Z}[x]$ can be written as a polynomial in (a), so that $(a) = \mathbb{Z}[x]$, impossible. If $a(x) = \pm 2$, then since $x \in (a)$, we get $x = 2q(x)$ where $q \in \mathbb{Z}[x]$. This cannot happen, so that $(a) \neq (2, x)$.

(4) Consider $\mathbb{R}^{[0,1]}$ the ring of all functions $f : [0, 1] \to \mathbb{R}$. Let $M = \{f : f(\frac{1}{2}) = 0\}$. Then M is an ideal in $\mathbb{R}^{[0,1]}$, in fact, notice that it is the kernel of the valuation map at $\frac{1}{2}$.

Define $g : [0,1] \to \mathbb{R}$ by:

$$g(x) = \begin{cases} 1, & \text{if } x \neq \frac{1}{2} \\ 0, & \text{if } x = \frac{1}{2} \end{cases}$$

then $f = fg$ by definition of both f and g. So that $M = (g)$ which makes M a principle ideal. M is not principle in general, consider $C^{[0,1]}$ the set of all realvalued continuous functions on $[0,1]$.

(5) Let G be a finite group and R a commutative ring with identity. The augmentation ideal in RG is generated by the set $\{g - 1 : g \in G\}$, and we write $(g_1 - 1, \ldots, g_n - 1)$ where $\operatorname{ord} G = n$. If G is cyclic, then the augmentation ideal is just $(g - 1)$, and is principle.

Lemma 1.4.1. *Let I an ideal in ring R with identity. Then*

(1) $I = (1)$ if, and only if I contains a unit.

(2) If R is commutative, then R is a field if, and only if its only ideals are (0) and (1).

Proof. Recall that $R = (1)$. Now, if $I = (1)$, then $1 \in I$, and 1 is a unit. Conversly, suppose that $u \in I$ with u a unit. By definition, we have that $r = r \cdot 1 = r(uv) = r(vu) = (rv)u$, so that $1 \in I$. This makes $I = (1)$.

Now, if R is a field, then it is a commutative ring, moreover every $r \neq 0$ is a unit in R, which makes $r \in I$ for some ideal $I \neq (0)$. This makes every $I \neq (0)$ equal to (1). COnversly, if (0) and (1) are the only ideals of the commutative ring R, then every $r \neq 0 \in (1)$, which makes themn units. Hence all nonzero r is a unit in R. This makes R into a field. ■

Corollary. *If R is a field, then any nonzero ring homomorphism $\phi : R \to S$ is 1–1.*

Proof. If R is a field, then either $\ker \phi = (0)$ or $\ker \phi = (1)$. Now, since $\ker \phi \neq R$, we must have $\ker \phi = (0)$. ■

Definition. We call a ring D with identity a **division ring** if its only left and right ideals are (0) and (1) respectively.

Example 1.14. For any field F, the only two sided ideals of $F^{n \times n}$ are (0) and (1), so that $F^{n \times n}$ is a division ring.

Definition. For any ideal M in a ring R, we call M **maximal** if $M \neq R$, and if N is an ideal with $M \subseteq N \subseteq R$, then either $M = N$ or $N = R$.

Lemma 1.4.2. *IF R is a ring with identity, every proper ideal is contained in a maximal ideal.*

Proof. Let I a proper ideal of R. Let $\mathcal{S} = \{N : N \neq (1) \text{ is a proper ideal, and } I \subseteq N\}$. Then $\mathcal{S} \neq \emptyset$, as $I \in \mathcal{S}$, and the relation $\subseteq$ partially orders $\mathcal{S}$. Let $\mathcal{C}$ be a chain in and define

$$J = \bigcup_{A \in \mathcal{C}} A$$

We have that $J \neq \emptyset$ since $(0) \in J$. Now, let $a, b \in J$, then we have that either $(a) \subseteq (b)$ or $(b) \subseteq (a)$, but not both. In either case, we have $a - b \in J$ so that J is closed under additive inverse. Moreover, since $A \in \mathcal{C}$ is an ideal, by definition, J is closed with respect to absorbption. This makes J an ideal.

Now, if $1 \in J$, then $J = (1)$ and J is not proper, and $A = (1)$ by definition of J. This is a contradiction as A must be proper. Thereofre J must also be a proper ideal. Therefore, $\mathcal{C}$ has an upperbound in $\mathcal{S}$, therefore, by Zorn's lemma, $\mathcal{S}$ has a maximal element M, i.e. it has a maximal ideal M with $I \subseteq M$. ■

Lemma 1.4.3. *Let R be a commutative ring. An ideal M is maximal if, and only if R/M is a field.*

Proof. If M is maximal, then ther is no ideal $I \neq (1)$ for which $M \subseteq I \subseteq R$ By the fourth isomorphism theorem, the ideals of R containing M are in 1–1 correspondence with the those of R/M. Therefore M is maximal if, and only if the only ideals of R/M are (M) and $(1 + M)$. ■

Example 1.15. (1) Let $n \geq 0$ an integer. The ideal $n\mathbb{Z}$ is maximal in $\mathbb{Z}$ if and only if $\mathbb{Z}/n\mathbb{Z}$ is a field. Therefore $n\mathbb{Z}$ is maximal if, and only if $n = p$ a prime in $\mathbb{Z}$. So the maximal ideals of $\mathbb{Z}$ are those $p\mathbb{Z}$ where p is prime.

(2) $(2, x)$ is not principle in $\mathbb{Z}[x]$, but it is maximal in $\mathbb{Z}[x]$, as $\mathbb{Z}[x]/(2, x) \simeq \mathbb{Z}/2\mathbb{Z}$ which is a field.

(3) The ideal (x) is not maximal in $\mathbb{Z}/n\mathbb{Z}$, since $\mathbb{Z}/(x) \simeq \mathbb{Z}$, which is not a field. Moreover, $(x) \subseteq (2, x) \subseteq \mathbb{Z}[x]$. We construct this isomorphism by identifying $x = 0$, then all polynomials of $\mathbb{Z}[x]/(x)$ only have constant term in $\mathbb{Z}$.

(4) Let $a \in [0, 1]$, and $M_a = \{f : f(a) = 0\}$ the kernel of the valuation map at a. Then M is principle, moreover, we also have that since $f(a) \in \mathbb{R}$, then $\mathbb{R}^{[0,1]}/M_a \simeq \mathbb{R}$ which makes M_a maximal.

(5) If F is a field and G a finite group of order n, then the augmentation ideal $(g_1 - 1, \ldots, g_n - 1)$ is maximal in FG. Let $\pi : \sum g_i a_i \to \sum a_i$, then $\ker \pi = (g_1 - 1, \ldots, g_n - 1)$ and $\pi(FG) = F$. This makes $FG/(g_1 - 1, \ldots, g_n - 1) \simeq F$.

Definition. We call an ideal P in a commutative ring R **prime** if $P \neq (1)$ and if $ab \in P$ then either $a \in P$ or $b \in P$. Alternatively, if $(ab) \subseteq P$ then $(a) \subseteq P$ or $(b) \subseteq P$.

Example 1.16. The prime ideals of $\mathbb{Z}$ are $p\mathbb{Z}$ with p prime together with (0).

Lemma 1.4.4. *An ideal P in a commutative ring R, is prime if, and only if R/P is an integral domain.*

Proof. Suppose that P is prime, and let $(a + P)(b + P) = ab + P = P$. This gives us that $ab \in P$ and hence $a \in P$ or $b \in P$. Then either $a + P = P$ or $b + P = P$ in R/P. Conversely, if R/P is an integral domain, then for any $a + P, b + P$ $ab + P = P$ implies that either $a + P = P$ or $b + P = P$. Then $a \in P$ or $b \in P$, only when $ab \in P$. This makes P prime. ■

Corollary. *Every maximal ideal is a prime ideal.*

Example 1.17. (1) The prime ideals of $\mathbb{Z}$ are $p\mathbb{Z}$, where p is prime, which are the maximal ideals of $\mathbb{Z}$.

(2) The ideal (x) in $\mathbb{Z}[x]$ is a prime ideal, but it is not maximal as $(x) \subsetneq (2, x) \subsetneq \mathbb{Z}[x]$.

1.5 Rings of Fractions.

Lemma 1.5.1. *Let R a commutative ring, and $D \subseteq R$ be nonempty with $0 \notin D$ such that D contains no zero divisors of R and that it is closed under multiplication. Define the relation $\sim$ on $R \times D$ by*

$$(a, b) \sim (c, d) \text{ if, and only if } ad - bc = 0$$

Then $\sim$ is an equivalence relation on $R \times D$.

Proof. We have $ab - ab = 0$ so that $(a, b) \sim (a, b)$. Moreover, if $ad - bc = 0$, then $bc - ad = 0$ so that $(a, b) \sim (c, d)$ implies $(c, d) \sim (a, b)$. Lastly, let $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. Then $ad - bc = 0$ and $cf - ed = 0$, so $af - eb = (ad - bc)f + d(cf - de) = 0$ so that $(a, b) \sim (e, f)$. ∎

Theorem 1.5.2. *Let R a commutative ring, and $D \subseteq R$ be nonempty with $0 \notin D$ such that D contains no zero divisors of R and that it is closed under multiplication. Then there exists a commutative ring Q with identity such that every element of D is a unit of Q.*

Proof. Define the equivalence relation $\sim$ on $R \times D$ by

$$(a, b) \sim (c, d) \text{ if, and only if } ad - bc = 0$$

Label the equivalence classes of $\sim$ over $R \times D$ as $\frac{a}{b} = \{(c, d) \in R \times D : ad - bc = 0\}$. Let

$$Q = R/\sim$$

The factor set of $\sim$ over $R \times D$ and define binary operations $+$ and $\cdot$ by

$$\begin{aligned} \frac{a}{b} + \frac{c}{d} &= \frac{ad + bc}{bd} \\ \frac{a}{b}\frac{c}{d} &= \frac{ac}{bd} \end{aligned}$$

Suppose that $\frac{a}{b} = \frac{a'}{b'}$ and $\frac{c}{d} = \frac{c'}{d'}$. Then $ab' - a'b = 0$ and $cd' - c'd = 0$. Then

$$\begin{aligned} (ad + bc)(b'd') &= adb'd' + bcb'd' \\ &= ab'dd' + cd'bb' \\ &= a'bdd' + c'dbb' \\ &= (a'd'c'd')bd \end{aligned}$$

So that $+$ is well define. By similar reasoning, $\cdot$ is also well defined.

Now, let $\frac{a}{b}, \frac{c}{d} \in Q$. Then $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \in Q$, as $ad + bc \in R$, and since $b, d \in D$, $bd \in D$. Moreover

$$\frac{a}{b} + (\frac{c}{d} + \frac{e}{f}) = \frac{a}{b} + \frac{cf + de}{df} = \frac{adf + bcf + bde}{bdf}$$

and

$$(\frac{a}{b} + \frac{c}{d}) + \frac{e}{f} = \frac{ad - bc}{bd} + \frac{e}{f} = \frac{adf + bcf + bde}{bdf}$$

so that $+$ is associative. Now, take $c = 0$ and $d \in D$, and we have

$$\frac{a}{b} + \frac{0}{d} = \frac{ad}{bd} = \frac{a}{b}$$

Since, $abd - abd = 0$ making $\frac{ad}{bd} = \frac{a}{b}$. Similarly, take $c = -a$ and $d \in D$ and we get

$$\frac{a}{b} + \frac{-a}{d} = \frac{0}{b}$$

So $\frac{0}{d}$ is the identity, and $\frac{-a}{d}$ is the inverse of $\frac{a}{b}$. Lastly, since R is commutative, this makes

$$\frac{a}{b} + \frac{c}{d} = \frac{c}{d} + \frac{a}{b}$$

Now, notce that since D is closed under multiplication, we have

$$\frac{a}{b}\frac{c}{d} = \frac{ac}{bd} \in Q$$

Moreover,

$$\frac{a}{b}(\frac{c}{d}\frac{e}{f}) = \frac{a}{b}\frac{ce}{df} = \frac{ace}{bdf} = \frac{ac}{bd}\frac{e}{f} = (\frac{a}{b}\frac{c}{d})\frac{e}{f}$$

Additionally, since R is commutative, we get

$$\frac{a}{b}\frac{c}{d} = \frac{c}{d}\frac{a}{b}$$

Lastly, take $c = d$ and $d \in D$. Then

$$\frac{a}{b}\frac{d}{d} = \frac{ad}{bd} = \frac{a}{b}$$

This makes Q a commutative righ with identity. Moreover, every element of D is a unit in Q Moreover $R \subseteq Q$ by taking $r \to \frac{r}{d}$ for some $d \in D$. ∎

Corollary. *The ring Q satisfies the following*

(1) Q contains a copy of R as a subring, and every element of Q is of the form rd^{-1}. Moreover, if $D = R \backslash \{0\}$, then Q is a field.

(2) Q is unique and the smallest ring containing a copy of R for which every element of D is a unit.

Proof. Imbed R into Q first. Define the map $\iota : R \to Q$ by taking $r \to \frac{rd}{d}$ where $d \in D$. Notice that $\frac{rd}{d} = \frac{re}{e}$, so that ι is well defined. Now, since $\frac{d}{d}$ is the identity of Q, we have

$$\frac{rsd}{d} = \frac{arsd}{dd} = \frac{rd}{d}\frac{sd}{d}$$

So that ι is a ring homomorphism. Now, subce no $d \in D$ is a zero divisor, we have that $\ker \iota = (0)$ This makes ι 1–1. Therefore, by the first isomorphism theorem, we get

$$\iota(R) \simeq R$$

Since $\iota(R) \subseteq Q$, ι is the required imbedding.

Now, if $D = R\backslash\{0\}$, this makes every $r \in R$, nonzero into a unit of Q. Then Q has no zero divisors making it an integral domain, thus Q is a field.

Lastly, let $\phi : R \to S$ be a 1–1 ring homomorphsim such that every $\phi(d)$ is a unit in S, where S is a commutative ring with unit and $d \in D$. Define the map $\Phi : Q \to S$ by taking $rd^{-1} \to \phi(rd^{-1})$. Then Φ is a 1–1 ring homomorphism, so that by the first isomorphism theorem,

$$\Phi(Q) \simeq S$$

This makes Q unique. ■

Definition. Let R a commutative ring, and $D \subseteq R$ be nonempty with $0 \notin D$ such that D contains no zero divisors of R and that it is closed under multiplication. Define the equivalence relation $\sim$ on $R \times D$ by

$$(a, b) \sim (c, d) \text{ if, and only if } ad - bc = 0$$

and let

$$Q = {}^{R \times D}\!\big/\!_{\sim}$$

Then we call the commutative ring Q, with identity $1 = \frac{d}{d}$, the **ring of fractions** of R. If $D = R\backslash\{0\}$ and R is an integral domain, we call Q the **field of fractions**.

Lemma 1.5.3. *If R is an integral domain, and Q its field of fractions, and F is a field containing $R' \simeq R$, then the subfield of F generated by R is isomorphic to Q.*

Proof. Let $\phi : R \to R'$ the ring isomorphism between R and R'. Then the $\phi : R \to F$ is 1–1. Define then the map $\Phi : Q \to F$ by $rd^{-1} \to \phi(rd^{-1})$. Then Φ is 1–1 and by the first isomorphism theorem, $\Phi(Q) \simeq Q$. Moreover, $\Phi(R) = \phi(R) = R' \subseteq \Phi(Q)$. Now, for all $r, s \in R$, we have $\phi(rs^{-1}) \in \Phi(Q)$ and since every element of Q is of the form rs^{-1}, any subfield containiing R' contains $\Phi(Q)$. ■

Example 1.18. (1) The field of fractions of $\mathbb{Z}$ is $\mathbb{Q}$. Indeed, the construction of the ring of fractions of a commutative ring with identity is inspired by constructing $\mathbb{Q}$ from $\mathbb{Z}$.

(2) The field of fractions of $\mathbb{Q}$ is $\mathbb{Q}$ itself. In general if F is a field, it is its own field of fractions.

(3) The field of fractions of $\mathbb{Z}[\sqrt{D}]$ is $\mathbb{Q}[\sqrt{D}]$.

(4) $2\mathbb{Z}$ as a subring has no zero divisors, so the field of fractions of $2\mathbb{Z}$ is also $\mathbb{Q}$.

1.6 Sun Tzu's Theorem.

Definition. Let $\{R_\alpha\}$ a collection of commutative rings with identity. We define the **direct product** of $\{R_\alpha\}$ to be the direct product of $\{R_\alpha\}$ as a group, nmade into a ring by the operation $(r_\alpha),(s_\alpha) \to (r_\alpha s_\alpha)$. We write $R = R_1 \times R_2 \times \dots$ when $\{R_\alpha\}$ is a countable collection.

Definition. We call the ideals $A, B \subseteq R$ of a ring R **comaximal** if $A + B = R$.

Example 1.19. If $(m,n) = 1$, then the ideals $n\mathbb{Z}$ $m\mathbb{Z}$ with $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$ are comaximal. $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$ is the set of all diophantine equations of the form

$$mx + ny = 1$$

Theorem 1.6.1 (Sun-Tzu's Theorem). *LEt $A_1, \dots, A_k$ be ideals in a commutative ring R with identity. Then the map*

$$\begin{aligned} R &\to R/A_1 \times \cdots \times R/A_k \\ r &\to (r + A_1, \dots, r + A_k) \end{aligned}$$

is a ring homomorphism with kernel

$$K = \bigcap_{i=1}^{k} A_i$$

Moreover if for all $1 \leq i, j \leq k$ with $i \neq j$, A_i and A_j are comaximal, then this map is onto with $\bigcap A_i = \prod A_i$ so that

$$R/A_1 \dots A_k \simeq R/A_1 \times \cdots \times R/A_k$$

Proof. Let $k = 2$, and $A_1 = A$ and $A_2 = B$. Consider the map

$$\begin{aligned} \phi : R &\to R \\ r &\to (r + A, r + B) \end{aligned}$$

Then $rs \to (rs+A, rs+B) = (r+A, r+B)(s+A, s+B)$ so that ϕ is a ring homomorphism. Now, let $r \in \ker \phi$, then $(r + A, r + B) = (A, B)$ so that $r \in A \cap B$, conversly if $r \in A \cap B$ then $r + A = A$ and $r + B = B$ so that $r \in \ker \phi$. Thereofore

$$\ker \phi = A \cap B$$

Now, suppose that A and B are comaximal, that is, $A+B = (1)$. Then there is an $x \in A$, and a $y \in B$ such that $x+y = 1$. Then $\phi(x) = (0, 1)$ and $\phi(y) = (1, 0)$ and $x = 1-y \in 1+B$. Now, take $r + A$, $s + B$, then

$$\phi(rx+sy) = \phi(r)\phi(x)+\phi(s)+\phi(y) = (r+A, r+B)(0, 1)+(s+A, s+B)(1, 0) = (r+A, s+B)$$

this makes ϕ onto, moreover notice that $AB \subseteq A \cap B$, and if $A + B = (1) = R$, then for every $x \in AB$, $c = c \cdot 1 = cx + cy \in AB$ so that $A \cap B = AB$.

Now, by induction on $k \geq 2$, takine $A = A_1$ and $B = A_2 \dots A_k$ by repeating the above argument, we get the result. ■

Corollary. *Let* $n = p_1^{a_1} \dots p_k^{a_k} \in \mathbb{Z}^+$ *be the prime factorization of* n*, where* $p_1 \neq \dots \neq p_k$*. Then*

$$\mathbb{Z}/n\mathbb{Z} \simeq U(\mathbb{Z}/p_1^{a_1}\mathbb{Z}) \times \cdots \times U(\mathbb{Z}/p_1^{a_1}\mathbb{Z})$$

Remark. Sun-Tzu's theorem is most commonly know as the Chines Remainder theorem, however it is the belief of the author that the name of the theorem should credit the author whenever possible. Also note that the Sun-Tzu of this theorem *is not* the same Sun-Tzu who penned *The Art of War*.

Chapter 2

Domains.

2.1 Eculidian Domains.

Definition. Let R be a commutative ring. We call a map $N : R \to \mathbb{N}$, with $N(0) = 0$ a **norm**, or, **degree**. If $N(a) \geq 0$, for all $a \in R$, then we call N **nonnegative** If $N(a) > 0$ for all $a \in R$ then we call N **positive**.

Definition. Let R be a commutative ring, and $N : R \to \mathbb{N}$ a norm. We say thay R is a **Euclidean domain** if for all $a, b \in R$, with $b \neq 0$, there exist elements $q, r \in R$ such that

$$a = qb + r \text{ where } r = 0 \text{ or } N(r) < N(b)$$

We call q the **quotient** and r the **remainder** of a when **divided** by b.

Example 2.1. (1) Let F be any field, and $N : F \to \mathbb{N}$ defined by $N(a) = 0$ for all $a \in F$. Then N makes F into a Euclidean domain. Take $a, b \in F$, with $b \neq 0$, and $q = ab^{-1}$. Then $a = qb + r$ where $r = 0$.

(2) The integers $\mathbb{Z}$ is a Euclidean domain with norm $N(a) = |a|$, the absolute value of a. In fact, the motivation for Euclidean rings comes from the division theorem, or Euclid's theorem for integers.

(3) Let F be a field, and consider $F[x]$. Let $N : F[x] \to \mathbb{N}$ be defined by $N : f \to \deg f$. Then f is a Euclidean domain. If F is not a field, then it is not necesarily true that $F[x]$ be a Euclidean domain.

(4) Let $D \in \mathbb{Z}^+$ be squarefree, and consider $\mathbb{Z}[\sqrt{D}]$. Define $N : \mathbb{Z}[\sqrt{D}] = \mathbb{N}$ to be the absolute value of the field norm, that is $N(a + b\sqrt{D}) = \|a + b\sqrt{D}\|^2 = a^2 + Db^2$. We notice that $\mathbb{Z}[\sqrt{D}]$ is an integral domain, but it is not a Euclidean domain. This depends on our choice of D. Let $D = -1$ so tha t $\sqrt{D} = i$, and $i^2 = -1$. Then the Gaussian integers, $\mathbb{Z}[i]$, is a Euclidean domeain. Let $x = a + ib$, $y = c + id$ with $y \neq 0$. In $\mathbb{Q}[i]$, the field of fractions, we have that $\frac{x}{y} = r + is$, where

$$r = \frac{ac + bd}{\|y\|^2} \text{ and } s = \frac{bc - ad}{\|y\|^2}$$

Now, let p and q be the integers closest to r and s, respectively so that

$$|r-p| \leq \frac{1}{2} \text{ and } |s-q| \leq \frac{1}{2}$$

Let $w = (r-p) + i(s-q)$, and take $z = wy$. Then we have $z = x - (p+iq)y$, so that $x = (p+iq)y + z$, moreover, we have $N(w) = (r-p)^2 + (q-s)^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$. Since $\|\cdot\|$ is multiplicative, we have

$$N(w)N(y) \leq \frac{1}{2}N(y)$$

which makes $\mathbb{Z}[i]$ into a Euclidean domain.

(5) Let K be a field. We define a **discrete valuation** to be a map $\nu : K^* \to \mathbb{Z}$ such that

(i) $\nu(ab) = \nu(a) + \nu(b)$.

(ii) ν is onto.

(iii) $\min\{\nu(x), \nu(y)\} \leq \nu(x+y)$, for all $x, y \in K^*$ for which $x + y \neq 0$.

We call the set $\nu K = \{x \in K^* : \nu(x) \geq 0\}$ the **valuation ring** of ν and is a subring of K^*. We call an integral domain R a **discrete valuation ring** if there exists a discrete valuation ν on the field of fractions of R, having νR as its valuation ring.

It can be shown that discrete valuation rings are Euclidean domains by the norm $N : 0 \to 0$ and $N = \nu$ on all R^*.

Lemma 2.1.1. *Every ideal in a Euclidean domain R, is a principle ideal.*

Proof. If $I = (0)$, we are done. Now, let $N : R \to \mathbb{N}$ be the norm of R, and consider the image $N(I) = \{N(a) : a \in I\}$. By the well ordering principle, $N(I)$ has a minimum element $N(d)$ for some $d \neq 0$ in I Notice that $(d) \subseteq I$. Now, let $a \in I$. Since R is a Euclidean domain, there exist $q, r \in R$ for which

$$a = qd + r \text{ where } r = 0 \text{ or } N(r) < N(d)$$

Then notice that

$$r = a - qd$$

putting $r \in I$ and $N(r) \in N(I)$. Since $N(d)$ is the minimum element, we must have $r = 0$ so that $a = qd$, which puts $a \in (d)$. Therefore $I = (d)$, making I principle. ■

Example 2.2. (1) The polynomial ring $\mathbb{Z}[x]$ is not a Euclidean domain. The ideal $(2, x)$ is not principle.

(2) Consider $\mathbb{Z}[\sqrt{-5}]$, i.e. $D = -5$. Suppose the ideal $(3, 2+\sqrt{-5})$ is a principle ideal, that is $(3, 2+\sqrt{5}) = (a+b\sqrt{-5})$ for some $a, b \in \mathbb{Z}$. Then we get that $3 = x(a+b\sqrt{-5})$ and $2+\sqrt{-5} = y(a+b\sqrt{-5})$. Then notice that $N(x) = a^2 + 5b^2 = 9$, and since $a^2 + 5b^2 \in \mathbb{Z}^+$, we must have that $a^2 + 5b^2 = 1, 3, 9$.

(i) If $a^2+5b^2=9$, then $N(x)=1$ making $x=\pm 1$ and $a+b\sqrt{-5}=\pm 3$, which cannot happen since $2+\sqrt{-5}$ is not divisible by 3.

(ii) the equation $a^2+5b^2=3$ cannot happen since it has no integer solutions. This makes

(iii) $a^2+b\sqrt{5}=1$, which makes $(a+\sqrt{-5})=\mathbb{Z}[\sqrt{-5}]$, moreover, we get the equation $3x+y(2+\sqrt{-5})=1$ for any $x,y\in\mathbb{Z}[\sqrt{-5}]$. Multplying both sides by $2-\sqrt{-5}$, we get that $3|(2-\sqrt{-5})$ which is impossible.

In all three cases, we were led to an impossibility, hence $\mathbb{Z}[\sqrt{-5}]$ cannot be a Euclidean domain.

Definition. Let R be a commutative ring, and $a,b\in R$ with $b\neq 0$. We say that b **divides** a if there is an $x\in R$ for which $a=bx$. We write $b|a$. We also say that a is a **multiple** of b.

Definition. Let R be a commutative ring. We call a nonzero element $d\in R$ a **greatest common divisor** of elements $a,b\in R$ if

(1) $d|a$ and $d|b$.

(2) If $c\in R$ is nonzero such that $c|a$ and $c|b$, then $c|d$.

We write $d=(a,b)$.

Lemma 2.1.2. *Let R be a commutative ring. For any $a,b\in R$ a nonzero element $d\in R$ is the greatest common divisor if*

(1) $(a,b)\subseteq(d)$.

(2) If $c\in R$ is nonzero with $(a,b)\subseteq(c)$, then $(d)\subseteq(c)$.

In particular, $d=(a,b)$.

Proof. The first two statements follow from definition, and the last follows lemma 2.1.1. ■

Lemma 2.1.3. *If R is a commutative ring, and $a,b\in R^*$, such that $(a,b)=(d)$ for some $d\in R^*$, then d is the greatest common divisor of a and b.*

Lemma 2.1.4. *Let R be an inetegral domain. If $c,d\in R$ generate the same principle ideal, i.e. $(d)=(c)$, then $d=uc$ for some unit $u\in R$.*

Proof. If $c=0$ or $d=0$, we are done. Suppose then that $c,d\neq 0$. Since $(d)=(c)$, we have that $d=xc$ and $c=yd$ for some $x,y\in R$. Then $d=(xy)d$, which makes $d(1-xy)=0$. Since $d\neq 0$, we get $xy=1$, making x and y units of R. ■

Corollary. *If R is commutative, then greatest common divisors are unique.*

Definition. We call an integral domain in which every principle ideal is generated by two elements a **Bezout domain**.

Lemma 2.1.5. *Every Euclidean domain is a Bezout domain.*

Theorem 2.1.6 (The Extended Euclidean Algorithm)**.** *Let R be a Euclidean and $a, b \neq 0$ elements of R. Let $d = r_n$ be the least nonzero remainder obtained by dividing a from b recursively $n+1$ times. Then*

(1) $d = (a, b)$ is the greatest common divisor of a and b.

(3) There exist $x, y \in R$ for which $ax + by = d$.

Proof. By lemma 2.1.1, we get that the ideal (a, b) is principle, so there exists a greatest common divisor of a and b. Now, let $d = r_n$ be obtained by dividing a and b recursively $(n+1)$ times. Then the $(n+1)^{st}$ equation gives $r_{n-1} = q_{n+1}r_n$, so that $r_n | r_{n-1}$. Now, by induction on n if $r_n | r + k + 1$ and $r_n | r_k$ then the $(k+1)^{st}$ equation gives $r_{k-1} = q_{k+1}r_k + r_{k+1}$, which implies that $r_n | r_{k-1}$. Therefore we get in the 1^{st} equation that $r_n | b$, and in the 0^{th} that $r_n | a$. That is, $d | a$ and $d | b$.

Now, notice that $r_0 \in (a, b)$ and that $r_1 = b - qr_0 \in (b, r_0) \subseteq (a, b)$. By induction on r_n, if $r_{k-1}, r_n \in (a, b)$ then

$$r_{k+1} = r_{k-1} - q_{k+1}r_k \in (r_{k-1}, r_n) \subseteq (a, b)$$

which puts $r_n \in (a, b)$ making $d = (a, b)$ the greatest common divisor. ∎

Definition. Let R be an integral domain, and let $\tilde{R} = R^* \cup \{0\}$ the set of units together with 0. We call an element $u \in R \backslash \tilde{R}$ a **universal side divisor** if for all $x \in R$, there is a $z \in \tilde{R}$ such that $u | x - z$.

Lemma 2.1.7. *Let R be an integral domain which is not a field. If R is a Euclidean domain, then there exist universal side divisors.*

Proof. Notice that since R is not a field, that $\tilde{R} \neq R$ and $R \backslash \tilde{R}$ is nonempty. Let N be the norm of R, and let $u \in R \backslash \tilde{R}$ be of minimal norm. Then for all $x \in R$, take $x = qu + r$ with $r = 0$ or $N(r) < N(u)$¿ By minimality of $N(u)$, we get $r \in \tilde{R}$. ∎

Example 2.3. Notice that ± 1 are the only units in the ring $\mathbb{Z}[1 + \frac{\sqrt{-19}}{2}]$, so that $\tilde{R} = \{0, 1, -1\}$. Suppose that $u \in R$ is a universal side divisor, and let $N = \| \cdot \|^2$ be the field norm; so that $N(a + (1 + \frac{\sqrt{-19}}{2})b) = a^2 + ab + 5b^2$. If $a, b \in \mathbb{Z}$ and $b \neq 0$, then we have $a^2 + ab + 5b^2 = (a + \frac{b}{2})^2 + \frac{19}{4b^2} \geq 5$ so that the smallest nonzero norms are 1 for $x = 1$ and 4 for $x = 2$. Now, if u is a universal side divisor, then $u | 2 - 0$ or $u | (2 \pm 1)$ that is $u | 2$, $u | 3$ or $u | 1$ making u a nonunit divsor. If $2 = xy$ then $4 = N(x)N(y)$ and so that $N(x) = 1$ or $N(y) = 1$. Hence the only divisors of 2 in $\mathbb{Z}[1 + \frac{\sqrt{-19}}{2}]$ are ± 1 or ± 2. Similarly the only divisors of 3 arew ± 1 or ± 3 hence $u = \pm 2$ or $u = \pm 3$. Letting $x = \frac{1 + \sqrt{-19}}{2}$, then x, nor $x \pm 1$ are divisible by any possible u. Therefore $\mathbb{Z}[1 + \frac{\sqrt{-19}}{2}]$ has no universal side divisors, and cannot be a Euclidean domain.

2.2 Principle Ideal Domains.

Definition. An integral domain R is called a **principle ideal domain (PID)** if every ideal in R is principle.

Example 2.4. (1) Every Euclidean domain is a PID, as dictated by lemma 2.1.1. Hence the rings $\mathbb{Z}$ and $\mathbb{Z}[i]$ are PIDs, however, the polynomial ring $\mathbb{Z}[x]$ is not principle, recall the ideal $(2, x)$.

(2) The ring $\mathbb{Z}[\sqrt{-5}]$ is not a PID, consider the ideal $(3, 2+\sqrt{-5})$. However, notice that $(3, 1+\sqrt{-5})(3, 1-\sqrt{-5}) = (3)$ is principle, despite $(3, 1+\sqrt{-5})$ and $(3, 1-\sqrt{-5})$ are not principle.

(3) The ring $\mathbb{Z}[1+\frac{\sqrt{-19}}{2}]$ is a PID, but not a Euclidean domain.

Lemma 2.2.1. *Let R be a principle ideal domain and let d be a generator for the ideal (a, b), for $a, b \in R$. Then the following are true.*

(1) $d = (a, b)$; i.e. d is the greatest common divisor of a and b.

(2) There exist $x, y \in R$ for which $ax + by = d$.

(3) d is unique up to unit.

Lemma 2.2.2. *Every nonzero prime ideal in a principle ideal domain R is maximal.*

Proof. Let $(p) \neq (0)$ be a prime ideal of R,. Let (m) be an ideal of R containing (p). Then $p \in (m)$ so that $p = rm$ for some $r \in R$. Now, since p is prime, and $rm \in (p)$, then either $r \in (p)$ or $m \in (p)$. If $m \in (p)$, then $(p) = (m)$. Otherwise, if $r \in (p)$, then $r = ps$ for some $s \in R$. Then $p = rm = pms = p(ms)$ which makes $ms = 1$, hence m is a unit, which makes $(m) = (0)$. ∎

Corollary. *If R is any commutative ring, such that the polynomial ring $R[x]$ is a principle ideal domain, then R is necessarily a field.*

Proof. If $R[x]$ is a PID, then $R \subseteq R[x]$, as a subring, must be an integral domain. Consider now, the ideal (x), then $R[x]/(x) \simeq R$ which makes (x) prime by lemma 1.4.4. Therefore (x) is maximal, which then makes R a field by lemma 1.4.3. ∎

Definition. Let R be a commutative ring, and $N : R \to \mathbb{N}$ a norm. We call N a **Dedekin-Hasse norm** if N is a positive norm suc that for all $a, b \in N$, either $a \in (b)$, or there exists an element $c \in (a, b)$ such that $N(c) < N(b)$.

Lemma 2.2.3 (The Dedekin-Hasse Criterion)**.** *An integral domain R is a PID if, and only if it has a Dedekin-Hasse norm.*

Proof. Let $I \neq (0)$ an ideal of R. Let $a \in I$ a nonzero element, so that $(a, b) \subseteq I$. Since N is Dedekin-Hasse, and by minimality of b, we get that $a \in (b)$ so that $I = (b)$ is principle. ∎

Example 2.5. Consider the ring $\mathbb{Z}[1+\frac{\sqrt{-19}}{2}]$. With norm $N = \|\cdot\|^2$ the field norm. Let $x, y \in \mathbb{Z}[1+\frac{\sqrt{-19}}{2}]$ be nonzero elements and that $\frac{x}{y} \notin \mathbb{Z}[1+\frac{\sqrt{-19}}{2}]$. Write

$$\frac{x}{y} = \frac{a+b\sqrt{-19}}{c} \in \mathbb{Q}[1+\frac{\sqrt{-19}}{2}]$$

where a, b, c are all coprime, with $c > 1$. Then there are integers u, v, w with $av+bu+cw = 1$, then $au - 19bv = cq + r$ for some quotient q and remainder r with $N(r) \leq \frac{c}{2}$ and let $s = u + v\sqrt{-19}$ and $t = q - w\sqrt{-19}$. Then we find that

$$0 < N(\frac{x}{y}s - t) \leq \frac{1}{4} + \frac{19}{c^2}$$

Then $s = 1, t = \frac{(a-1)+b\sqrt{-19}}{2} \in R$ satisfy $0 < N(\frac{x}{y}s - t)$

Now, suppose that $c = 3$, then $3 \nmid (a^2 + 19b^2)$. Then $a^2 + 19b^2 = 3q + r$ with $r = 1$ or $r = 2$. Then $s = a - b\sqrt{-19}, t = q$ statisfy $0 < N(\frac{x}{y}s - t)$. Finally, for $c = 4$, with a, b not both even, so that $a^2 + 19b^2$ is odd. Then $a^2 + 19b^2 = 4q + r$ so for $q, r \in \mathbb{Z}$ with $0 < r < 4$, then $s = a - b\sqrt{-19}, t = q$ satisfy $0 < N(\frac{x}{y}s - t)$. Now, if both a and b are odd, then $a^2 + 19b^2 \equiv 1 + 3 \mod 8$ so taht $a^2 + 19b^2 = 8q + 4$ for some $q \in \mathbb{Z}$, then

$$s = \frac{a - b\sqrt{-19}}{2} \text{ and } t = q$$

satisfy $0 < N(\frac{x}{y}s - t)$.

2.3 Unique Factorization Domains.

Definition. Let R be an integral domain. A nonzero element $r \in R$ that is not an associate is called **irreducible** if whenever $r = ab$, then either a or b are units in R; otherwise, we call r **reducible**.

Definition. Let R be an integral domain. An element $p \in R$ is called **prime** if the ideal (p) is a prime ideal. That is p is not a unit and whenever $p|ab$, then either $p|a$ or $p|b$. We call two elements $a, b \in R$ **associates** if $a = ub$ for some unit $u \in R$.

Lemma 2.3.1. *In an integral domain, a prime element is always irreducible.*

Proof. Let (p) be a nonzero prime ideal with $p = ab$, for some $a, b \in R$. Then $ab \in (p)$, so that either $a \in (p)$, or $b \in (p)$. Suppose that $a \in (p)$. Then $a = pr$ for some $r \in R$, so that $p = (pr)b = p(rb)$, so that $rb = 1$. This makes b a unit. Similarly, we see that a is a unit if $b \in (p)$. In either case, p is irreducible. ∎

Example 2.6. (1) In the ring $\mathbb{Z}$ of integers, those elements which are irreducible are precisely those which are prime, since the ideals $2\mathbb{Z}, 3\mathbb{Z}, \ldots, p\mathbb{Z}, \ldots,$ for p a prime number are also the prime ideals of $\mathbb{Z}$

(2) Irreducible elements need not be prime. The element $3 \in \mathbb{Z}[\sqrt{-5}]$ is irreducible, as was shown in example 2.2, however it is not prime. Notice that $3|9 = (2+\sqrt{-5})(2-\sqrt{-5})$, but $3 \nmid (2 + \sqrt{-5})$ and $3 \nmid (2 - \sqrt{-5})$.

Lemma 2.3.2. *In a principle ideal domain, a nonzero element is prime if, and only if it is irreducible.*

Proof. Let R be a PID, and suppose that p is irreducible. Let (m) be the principle ideal containing (p), then $p = rm$, and by irreducibility, either r or m are units, in either case, we get that either $(p) = (m)$ or $(m) = (1)$. This makes (p) a maximal ideal, and hence a prime ideal. ■

Example 2.7. (1) Since 3 is not prime in $\mathbb{Z}[\sqrt{-5}]$, then (3) is not a prime ideal in this ring. Therefore $\mathbb{Z}[\sqrt{-5}]$ cannot be a PID.

(2) Notice that since $\mathbb{Z}$ is a PID, then the fact that irreducible and prime elements coincide is guaranteed by lemma 2.3.2.

Definition. We call an integral domain R a **unique factorization domain (UFD)** if for every nonzero element $r \in R$ which is not a unit, the following are true.

(1) r can be written as the product of, not necessarily distinct, irreducible elements. We call this product the **factorization** of r.

(2) The factorization of r is unique up to associates.

Example 2.8. (1) All fields are unique factorization domains.

(2) Polynomial rings are unique factorization domains whenever the ground ring R is a unique factorization domain.

(3) The subring $\mathbb{Z}[2i]$ of $\mathbb{Z}[i]$ is an integral domain, but it is not a UFD. Notice that both 2 and $2i$ are irreducible in $\mathbb{Z}[2i]$, but that $4 = 2 \cdot 2 = (2i) \cdot (-2i)$.

(4) $\mathbb{Z}[\sqrt{-5}]$ is another example of an integral domain that is not a UFD.

Lemma 2.3.3. *In a unique factorization domain R, a nonzero element is prime if, and only if it is irreducible.*

Proof. Since prime elements are irreducible, it remains to show that irreducible elements are prime. Let p be irreducible and suppose that $p|ab$, for $a, b \in R$. Then $ab = pc$ for some $c \in R$. Writing ab as a product of irreducibles, since R is a UFD, p must be associate to one of the irreducibles in the factorization of a, or to one in the factorization of b. In either case, we get that $p|a$ or $p|b$, and hence p is prime. ■

Lemma 2.3.4. *Let $a, b \in R$ nonzero elements of a unique factorization domain R. If $a = up_1^{e_1} \dots p_n^{e_n}$ and $b = vp_1^{f_1} \dots p_n^{f_n}$, where $u, v \in R$ are units, then the element*

$$d = p_1^{\min\{e_1,f_1\}} \dots p_n^{\min\{e_n,f_n\}}$$

os the greatest common divisor of a and b.

Proof. Notice that by definition of d, that $d|a$ and $d|b$. Now, let c be a common divisor of a and b with the unique prime factorization $c = q_1^{g_1} \dots q_m^{g_m}$. Since $q_i|c$ for each $1 \leq i \leq m$, then $q_i|p_j$ for each prime factor in the factorizations of a and b. Since both q_i and p_j are irreducible, they are associates. That implies that the primes of c are the primes of a and b. Moreover notice that since each $g_i \leq e_i, f_i$, that $c|d$, and so $d = (a, b)$. ■

Definition. Let R be a principle ideal domain. Let $\{a_n\}$ a sequence of elements of R. We call the increasing sequence of ideals $\{(a_n)\}$ an **infinite ascending chain** of ideals in R and write

$$(a_1) \subseteq (a_2) \subseteq \cdots \subseteq (a_n) \subseteq \cdots \subseteq R$$

We say that the infinite ascending chain $\{(a_n)\}$ **stabalizes** if for some $k \geq n$, we have $(a_n) = (a_k)$.

Lemma 2.3.5. *In any principle ideal domian, infinite ascending chains of ideals stabalize.*

Proof. Let $I_1 \subseteq I_2 \subseteq \cdots \subseteq R$ an infinite ascending chain of ideals and let $I = \bigcup I_k$. Then I is an ideal in R, and since R is a PID, $I = (a)$ for some $a \in R$. This makes $a \in I_n$ for some n, and hence $I_n \subseteq I$. This makes $I_n = I$ for some $n \geq 1$, and hence this chain stabalizes. ■

Theorem 2.3.6. *Every principle ideal domain is a unique factorization domain.*

Proof. Let R be a PID, and $r \in R$ a nonzero element which is not a unit. If r is irreducible, we are done. Otherwise, we have $r = r_1 r_2$ fr some $r_1, r_2 \in R$. Now, if both r_1 and r_2 are irreducible, we are done. Suppose then, without loss of generality, thart r_1 is reducible. Then $r_1 = r_{11} r_{12}$, and if both r_{11} and r_{12} are irreducible, we are done. Suppose then that r_{11} is reducible; continuing this process, we arrive at an infinite ascending chain of ideals

$$(r) \subseteq (r_1) \subseteq (r_{11}) \subseteq \cdots \subseteq R$$

and since R is a PID, this chain stabalizes. Thus r can be factored into irreducible elements; since this process terminates.

Now, by induction on n, for $n = 0$, we notice that r is a unit, and we are done. Suppose, then for $n \geq 1$, that $r = p_1 \ldots p_n = q_1 \ldots q_m$ for some $m \geq n$, and where each p_i and q_j are (not necessarily distinct) irreducibles for all $1 \leq i \leq n$ and $1 \leq j \leq m$. Notice that $p_1 | q_1 \ldots q_m$, and so $p_1 | q_j$ for some j. This makes p_1 and q_j associates; i.e. $q_j = p_1 u$, with $u \in R$ a unit. Cancelling the p_1 from both sides of the equation, we get $p_2 \ldots p_n = q_1 \ldots q_{j-1} q_{j+1} \ldots q_m$. Repeating this process, we get a 1–1 correspondence between associates, and hence the factorization of r is unique up to associates. Therefore R is a UFD. ■

Corollary. *Every Euclidean domain is a unique factorization domain.*

Proof. Notice that Euclidean domains are PIDs by lemma 2.1.1. ■

Corollary (The Fundamental Theorem of Arithmetic)**.** *$\mathbb{Z}$ is a unique factorization domain.*

Proof. Notce that $\mathbb{Z}$ is a Euclidean domain. ■

Corollary. *There exists a multiplicative Dedekind-Hasse norm on R.*

Proof. If R is a PID, then the theorem tells us it is a UFD. Define the norm $N : R \to \mathbb{N}$ by taking $0 \to 0$, $u \to 1$ if u is a unit, and $a \to 2^n$ where $a = p_1 \ldots p_n$, where each p_i is irreducible. Notice that for every $a, b \in R$, $N(ab) = N(a)N(b)$. Now, suppose further that $a, b \neq 0$ and consider the ideal $(a, b) = (r)$, for some $r \in R$. UIf $a \notin (b)$, nether is r, and hence $b \nmid r$. Now, since $b = xr$, $x \in R$, then x cannot be a unit in R, so that $N(b) = N(xr) = N(x)N(r) > N(r)$. This completes the proof. ■

2.4 Factorization in the Gaussian Integers.

Lemma 2.4.1. *Let $D \in \mathbb{Z}$ a square free integer. If for some $z \in \mathbb{Z}[\sqrt{D}]$, $N(z)$ is $\pm$ a prime, then z is irreducible in $\mathbb{Z}[\sqrt{D}]$.*

Proof. Let $z \in \mathbb{Z}[\sqrt{D}]$ an element with prime norm $N(z) = p$, where $N = \|\cdot\|^2$. Then f $z = vw$, for some $v, w \in \mathbb{Z}[\sqrt{D}]$, then $p = N(z) = N(v)N(r)$, so that either $N(v) = \pm 1$ or $N(w) = \pm 1$. In either case, v or w is a unit in $\mathbb{Z}[\sqrt{D}]$, which makes z irreducible. ■

Lemma 2.4.2. *A prime $\in \mathbb{Z}^+$ divides an integer of the form n^2+1, for some $n \in \mathbb{Z}$, if, and only if $p = 2$, or $p \equiv 1 \mod 4$, for p odd.*

Proof. Certainly, $2 = 1^2 + 1$. Now suppose that p is an odd prim.e. IF $p|n^2+1$, then $n^2 \equiv -1 \mod p$. That is n is of order 4 in the unit group $U(\mathbb{Z}/p\mathbb{Z})$. So $p|n^2+1$ if, and only if $U(\mathbb{Z}/p\mathbb{Z})$ contains an element of order 4; by Lagrange's theorem we then have that $4|p-1$, which makes $p \equiv 1 \mod 4$.

Conversely, if $p \equiv 1 \mod 4$, then $4|(p-1)$. Now, if $m \in \mathbb{Z}$ such that $m^2 \equiv 1 \mod p$, then $p|(m^2-1) = (m+1)(m-1)$ so that $m \equiv \pm 1 \mod p$ and m is unique. Now, $U(\mathbb{Z}/p\mathbb{Z})$ has a subgroup of order 4. Notice that since the Klein-4 group, V_4 has three elements of order 2, and $U(\mathbb{Z}/p\mathbb{Z})$ has only one, then this subgroup cannot be V_4. The only other option is $\mathbb{Z}/4\mathbb{Z}$. Thus $U(\mathbb{Z}/p\mathbb{Z})$ contains an element of order 4, and we are done. ■

Theorem 2.4.3. *$\mathbb{Z}[i]$ is a unique factorization domain.*

Proof. Notice that $\mathbb{Z}[i]$ is a Euclidean domain with norm $N = \|\cdot\|^2$ the field norm for complex numbers. ■

Corollary. *A prime p factors in $\mathbb{Z}[i]$ in precisely two irreducible elements if, and only if $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$. Otherwise, p is irreducible in $\mathbb{Z}[i]$.*

Proof. Consider first the ring $\mathbb{Z}[\sqrt{D}]$ (which is not necessarily a Euclidean domain). Suppose that $\pi \in \mathbb{Z}[\sqrt{D}]$ is prime. Then $(\pi) \cap \mathbb{Z}$ is a prime ideal, and since $N(\pi) \geq 0$ is an integer in (π), $(\pi) \cap \mathbb{Z} = p\mathbb{Z}$ for some prime $p \in \mathbb{Z}^+$. Then $p \in (\pi)$ so that $\pi|p$ and hence we can determine the prime elements of $\mathbb{Z}[\sqrt{D}]$ to see how the prime number p factors in $\mathbb{Z}[\sqrt{D}]$. Suppose that $p = \pi\pi'$, then $N(p) = N(\pi)N(\pi') = p$. Since π is not a unit, then either $\pi = \pm p^2$ or $\pi = \pm p$. In either case, we have that p is the product of precisely two irreducibles in $\mathbb{Z}[\sqrt{D}]$.

Now, suppose that $D = -1$, so that we have $\mathbb{Z}[i]$ (which is a Euclidean domain by theorem 2.4.3). The units of $\mathbb{Z}[i]$ are ± 1 and $\pm i$. Now, if $z = a + ib$, then $N(z) = z\overline{z} = (a+ib)(a-ib) = a^2 + b^2$ and we are done. ■

Theorem 2.4.4. *The following statements are true.*

(1) *A prime $p \in \mathbb{Z}^+$ is the sum of two integer squares if, and only if $p = 2$, or $p \equiv 1$ $\mod 4$, for p odd. This sum is unique up to ordering and sign.*

(2) *The irreducible elements of* $\mathbb{Z}[i]$ *are preciesly* $(1+i)$*, all primes* $p \in \mathbb{Z}$ *for which* $p \equiv 3 \mod 4$*, and all irreducible factors of all* $p \in \mathbb{Z}$ *of the form* $p = a^2 + b^2$*, for which* $p \equiv 1 \mod 4$*. These factors are of the form* $a \pm ib$*.*

Proof. Notice that $2 = 1^2 + 1^2$, and that $2 = (1+i)(1-i)$ in $\mathbb{Z}[i]$. Moreover $1-i = -i(1+i)$, which makes $1 \pm i$ associates.

Now, for any integer, its square is either $0 \mod 4$ or $1 \mod 4$. Hence, if p is an odd prime, then $p^2 \equiv 1 \mod 4$. So if $p \equiv 3 \mod 4$, it is not the sum of two squares, and hence it is irreducible in $\mathbb{Z}[i]$.

Now, if $p \equiv 1 \mod 4$, by lemma 2.4.2, we have $p|n^2+1$ for some integer $n \in \mathbb{Z}$. Then $p|(n+i)(n-i)$. Suppose then, that p was irreducible. Then either $p|(n+i)$ or $p|(n-i)$; however since p is a real number, we have p dividing both. Thus $p|((n+i)-(n-i)) = 2i$, which cannot happen, and hence p is reducible. Then by above, $p = a^2+b^2 = (a+ib)(a-ib)$ for some $a, b \in \mathbb{Z}$. ■

Corollary. *Let* $n \in \mathbb{Z}$ *be of the form*

$$n = 2^k p_1^{a_1} \dots p_r^{a_r} q_1^{b_1} \dots q_s^{b_s}$$

where each $p_i \equiv 1 \mod 4$ *is a distinct prime and each* $q_j \equiv 3 \mod 4$ *is a distinct prime. Then* n *is the sum of two integer squares if, and only if* b_j *is even. Moreover, the number of representations of* n *as a sum of two integer squares is*

$$4(a_1+1)\dots(a_r+1)$$

Proof. Notice that if $n = A^2+B^2$ for some $A, B \in \mathbb{Z}$, then $N(A+iB) = n$, for $A+iB \in \mathbb{Z}[i]$. Now, by the above theorem, we have proved the first assertion that if $n = A^2+B^2$, then the b_js are even. Suppose then that b_j is even for all $1 \leq j \leq s$. For each $p_i \equiv 1 \mod 4$, write $p_i = \pi_i \overline{\pi_i}$ where π_i is irreducible in $\mathbb{Z}[i]$ and $\overline{\pi_i}$ is its conjugate. Now, if $N(A+iB) = n$, then the factorization of $A+iB$ in $\mathbb{Z}[i]$ is

$$A+iB = (1+i)^k (\prod_{i=1}^{r} \pi^{a_{i,1}} \overline{\pi}^{a_{i,2}}) q_1^{\frac{b_1}{2}} \dots q_s^{\frac{b_s}{2}}$$

Where $a_{i,1} + a_{i,2} = a_i$. Now since each $a_{i,1}$ is one of a_i+1 possible choices, we have $(a_1+1)\dots(a_r+1)$ unique choices up to units. Since $\mathbb{Z}[i]$ has the 4 units $\pm 1, \pm i$, we get the result. ■

Chapter 3

Polynomial Rings.

3.1 Multivariate Polynomial Rings.

Theorem 3.1.1. *Let I be an ideal of R and $I[x]$ the ideal of $R[x]$ generated by I. Then*

$$R[x]/I[x] \simeq R/I[x]$$

Moreover, if I is a prime ideal in R, then $I[x]$ is a prime ideal in $R[x]$.

Proof. Consider the map $\pi : R[x] \to R/I[x]$ given by $f \to f \mod I$. That is, reduce f modulo I. Then π is a ring homomorphism with kernel $\ker \pi = I[x]$. By the first isomorphism theorem, we get

$$R[x]/I[x] \simeq R/I[x]$$

Now, let I be a prime ideal in R, Then we have that R/I is an integral domain, hence, so is $R/I[x]$, which makes $I[x]$ a prime ideal of $R[x]$. ■

Example 3.1. Consider the ideal $n\mathbb{Z}$ in $\mathbb{Z}$. By above, we have

$$\mathbb{Z}[x]/n\mathbb{Z}[x] \simeq \mathbb{Z}/n\mathbb{Z}[x]$$

with natural map reduction of polynomials modulo n. If n is composite, then the ring $\mathbb{Z}/n\mathbb{Z}[x]$ is not an integral domain. If $n = p$ a prime, then $\mathbb{Z}/n\mathbb{Z}[x]$ is an integral domain.

Definition. We define the **polynomial ring** in n **variables** $x_1, \dots, x_n$ with **coefficients** in R inductively to be

$$R[x_1, \dots, x_n] = R[x_1, \dots, x_{n-1}][x_n]$$

and is the set of all **multivariate polynomials** of the form $f(x_1, \dots, x_n) = \sum a x_1^{d_1} \dots x_n^{d_n}$. We call the monic term $x_1^{d_1} \dots x_n^{d_n}$ of f a **monomial**. We define the **degree** of a monomial to be $\deg x_1^{d_1} \dots x_n^{d_n} = d_1 + \cdots + d_n$ and we define the **degree** of f to be $\deg f = \max\{\deg x_1^{d_1} \dots x_n^{d_n}\}$ (i.e. the maximum degree of all monomials of f). If all the monomials of f have the same degree, we call f **homogeneous**, or, a **form**.

Lemma 3.1.2. *Let R be a ring. Then $R[x_1, \dots, x_n]$ is a ring.*

Example 3.2. (1) Consider the polynomial ring $\mathbb{Z}[x, y]$ in two variables x and y with integer coefficients. Then $p(x, y) = 2x^3 + xy - y^2$ and has $\deg p = 3$. The polynomial $q(x, y) = -3xy + 2y^2 + x^2y^3$ has $\deg q = 5$. The sum

$$p + q(x, y) = 2x^3 - 2xy + y^2 + x^2y^3 \text{ has degree } \deg p + q = 5$$

and the product

$$pq(x, y) = -6x^4y + 4x^3y^2 + 2x^5y^3 - 3x^2y^2 + 5xy^3 + x^3y^4 - 2y^4 - x^2y^5$$

had degree $\deg pq = 8$.

(2) The polynomial $p(x, y, z) = 4y^2z^5 - 3xy^3z + 2x^2y$ over $\mathbb{Z}[x, y, z]$ has degree $\deg p = 7$ and the polynomial $q(x, y, z) = 5x^2y^3z^4 - 9x^2z + 7x^2$ has degreee $\deg q = 9$. The polynomials

$$p + q(x, y, z) = 5x^2y^3z^4 + 4y^2z^5 - 3xy^3z + 2x^2y - 9x^2z + 7x^2$$

and

$$pq(x, y, z) = 20x^2y^5z^9 - 15x^3y^6z^5 + 10x^4y^4z^4 - 36x^2y^2z^6 + 28x^2y^2z^5 + 27x^3y^3z^2 - 21x^3y^3z - 18x^4yz + 14x^4y$$

have degrees $\deg(p + q) = 9$ and $\deg pq = 16$, respectively.

(3) Consider the polynomials p and q of the above example over $\mathbb{Z}/3\mathbb{Z}$, i.e. as polynomials in $\mathbb{Z}/3\mathbb{X}[x, y, z]$. Then we have

$$p(x, y, z) = xy^2z^5 + 2x^2y$$
$$q(x, y, z) = 2x^2y^3z^4 + x^2$$

which makes

$$p + q(x, y, z) = 2x^2y^3z^4 + y^2z^5 + 2x^2y + x^2$$

and

$$pq(x, y, z) = 2x^2y^5z^9 + 1x^4y^4z^4 + 1x^2y^2z^5 + 14x^4y$$

of degrees $\deg(p + q) = 9$ and $\deg pq = 16$, still.

Lemma 3.1.3. *Let R be a commutative ring, and π a permutation of the set $\{1, \dots n\}$. Then $R[x_1, \dots, x_n] \simeq R[x_{\pi(1)}, \dots, x_{\pi(n)}]$. That is, multivariate polynomial rings are independent of the ordering of their variables.*

Proof. Define the map $\Pi : R[x_1, \dots, x_n] \to R[x_{\pi(1)}, \dots, x_{\pi(n)}]$ termwise by first sending $x_1 \dots x_n \to x_{\pi(1)} \dots x_{\pi(n)}$. Then notice that Π defines a ring homomorphism, and moreover, for any $f \in R[x_1, \dots, x_n]$, Π permutes the terms of f. So that Π dictates the required isomorphism. ■

3.2 Unique Factorization of Polynomials.

Lemma 3.2.1 (Gauss). *Let R be a unique factorization ring, with field of fractions F. and let $p(x)$ a polynomial in $R[x]$. If p is reducible in $F[x]$, then p is reducible in $R[x]$. That is, if $p(x) = A(x)B(x)$, where $A, B \in F[x]$, then there exist $r, s \in F$, nonzero, for which $rA(x) = a(x) \in R[x]$, $sB(x) = b(x) \in R[x]$, and $p(x) = a(x)b(x)$.*

Proof. Since $A, B \in F[x]$, they are quotients of elements of R. Then multiplying by a nonzero common divisor $d \in R$, take $dp(x) = a'(x)b'(x)$, where $a', b' \in R[x]$. Now, if d is a unit, then take $a(x) = d^{-1}a'(x)$, and $b(x) = b'(x)$ and we are done. Suppose, then that d is not a unit. Then since R is a UFD, let

$$d = p_1 \dots p_n \text{ where } p_i \in R \text{ is irreducible}$$

the unique factorization of d into irreducible elements. Then the ideal (p_1) is prime in R, since R is a UFD, then $p_1R[x]$ is prime in $R[x]$, and so we get ${}^{R}\!/_{p_1R}[x]$ is an integral domain. Then reduce $dp - a'b'$ modulo p_1, and we get $a'(x)b'(x) \equiv 0 \mod (p_1)$. Hence, either $a' \equiv 0 \mod (p_1)$ or $b' \equiv 0 \mod (p_1)$. In either case, p_1 divides either a' or b'. That is, $\frac{a'}{p_1}(x)$ has coefficients in R. Now, this leaves d with one fewer irreducible factors. Hence repeating the process for $p_2, \dots, p_n$, cancel d in the two polynomials and we get $p(x) = a(x)b(x)$, where $a, b \in R$, and $a = rA$, $b = sB$ for some $r, s \in F$ nonzero. ■

Corollary. *If the coefficients of p are coprime, then p is irreducible in $R[x]$ if, and only if it is irreducible in $F[x]$.*

Proof. By above, if p is reducible in $F[x]$, it is reducible in $R[x]$. Conversley, let $a_0, \dots, a_n$ the coefficients of p, and suppose that $c = (a_0, \dots, a_1) = 1$. Now, if p is reducible in $R[x]$, since $d = 1$, $p(x) = a(x)b(x)$, where neither $a, b \in R[x]$ are constant in $R[x]$. This is also a factorization in $F[x]$. ■

Theorem 3.2.2. *A ring R is a unique factorization domain if, and only if $R[x]$ is a unique factorization domain.*

Proof. Certainly, if $R[x]$ is a UFD, so is R, since the constant polynomials are just elements of R. Now, suppose that R is a UFD, and let F be the field of fractions of R, and $p \in R[x]$ a polynomial with coefficients $a_0, \dots, a_n$. Let $d = (a_0, \dots, a_n)$. Then $p(x) = dp'(x)$, where the coefficients of p' are coprime. Then such factorization of is unique up to a unit, and since d can be uniquely factored in d, it suffices to show that p' can be uniquely factored in $R[x]$.

Let $c = 1$ the gratest common divisor of the coefficients of p'. Since $F[x]$ is a UFD, p' can be uniquely factored in $F[x]$. Hence, by Gauss' lemma, there is a factorization of p' in $R[x]$, whose factors are F-multiples of factoris in $F[x]$. Since $c = 1$, each of these factors must have coprime coefficients, and hence by the preceding corollary, each of these factors is irreducible in $R[x]$. That is, p' is a finite product of irreducibles.

Suppose now, that

$$p'(x) = p_1(x) \dots p_n(x) = q_1(x) \dots q_m(x)$$

are two factorizations of p' into irreducibles. Since $c = 1$, the coefficients of each factor in p_i and q_j must be coprime, and $\deg p_i > 0$ and $\deg q_j > 0$. Now, sicne the units of $F[x]$ are the elements of $\mathcal{U}(F)$, consider when $p'(x) = \frac{a}{b}q(x)$, where $a, b \in R$ are nonzero. Then the coefficients in q are coprime. Since the greatest commond divisror in a UFD is unique up to unit, $a = ub$ for some unit $u \in R$. And p' and q are associate in $R[x]$. This makes $R[x]$ a UFD. ∎

Corollary. *If R is a unique factorization domain, then the multivariate polynomial ring in n-variables $R[x_1, \ldots, x_n]$ is a unique factorization domain.*

Proof. By definition, $R[x_1, \ldots, x_n] = (R[x_1, \ldots, x_{n-1}])[x_n]$, and the rest follows recursively. ∎

Example 3.3. (1) Since $\mathbb{Z}$ is a UFD, so are $\mathbb{Z}[x]$ and $\mathbb{Z}[x, y]$, and these are examples of UFDs which are not PIDs.

(2) $\mathbb{Q}[x]$ and $\mathbb{Q}[x, y]$ are also UFDs.

(3) In general, if R is an integral domain, and p is a monic irreducible in $R[x]$, then it is not always true that p is irreducible in $F[x]$, F being the field of fractions of R. Consider the ring $\mathbb{Z}[2i]$, and let $p(x) = x^2 + 1$. Then the field of fractions in $\mathbb{Z}[2i]$ is $\mathbb{Q}[i]$, and the polynomial p factors into $p(x) = (x + i)(x - i)$, where $i^2 = -1$. Neither of these factors are in the polynomial ring $(\mathbb{Z}[2i])[x]$, so p is irreducible in $(\mathbb{Z}[2i])[x]$, and $(\mathbb{Z}[2i])[x]$ fails to be UFD.

3.3 Irreducibility of Polynomials.

Definition. Let R be a ring, and $p \in R[x]$. We call an element $\in R$ a **root** (or **zero**) of p if $p(\alpha) = 0$.

Lemma 3.3.1. *Let F be a field, and $p \in F[x]$. Then p has a linear factor if, and only if p has a root in F.*

Proof. If p has a linear factor, then it is of the form $(x - \alpha)$ (assuming it is monic), for some $\alpha \in F$. But then $p(\alpha) = (\alpha - \alpha)q(\alpha) = 0$ making α a root.

Conversely, suppose that p has a root $\alpha \in F$. By the division theorem, there exist $q, r \in F[x]$, $q(x) \neq 0$ for which

$$p(x) = q(x)(x - \alpha) + r(x) \text{ and } r(x) \text{ is constant}$$

Then $p(\alpha) = q(\alpha)(\alpha - \alpha) + r(\alpha)$ so that $r(\alpha) = 0$, which makes $r(x) = 0$, and hence we have a linear factor $(x - \alpha)$ of p. ∎

Lemma 3.3.2. *A polynomial p over a field F of degree $\deg p = 2, 3$ is irreducible if, and only if it has no root in F.*

Lemma 3.3.3. *Let R be a unique factorization domain, and*

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

a polynomial of degree n over R. Let F be the field of fractions of R,and $\frac{r}{s} \in F$ with r and s coprime. If $\frac{r}{s}$ is a root of p, then $r|a_0$ and $s|a_n$.

Proof. We have that $p(\frac{r}{s}) = 0 = a_0 + a_1(\frac{r}{s}) + \cdots + a_n(\frac{r}{s})^n$. Multiplying both sides by s^n, we have

$$s^n a_0 + s^n a_1(\frac{r}{s^{n-1}}) + \cdots + a_n r^n = 0$$

so that

$$a_n r^n = s(-a_0 s^{n-1} - \cdots - a_{n-1} r^{n-1})$$

which makes $s|a_n$, since $(r,s) = 1$. By simnilar reasoning, we conclude that $r|a_0$. ∎

Example 3.4. (1) The polynomial $x^3 + 3x - 1$ is irreducible in $\mathbb{Z}[x]$. By Gauss' lemma, it suffices to show that it has no roots in $\mathbb{Q}$. Indeed, the only possible roots for this polynomial are ± 1, and notice $1^2 + 3(1) - 1 = 1 + 3 - 1 = 3 \neq 0$, and $(-1)^3 + 3(-1) - 1 = -1 - 3 - 1 = -5 \neq 0$.

(2) For every prime p, $x^2 - p$ and $x^3 - p$ are irreducible in $\mathbb{Q}[x]$. Notice that since they are monic, the only possible roots are ± 1 and $\pm p$, none of which satisfy the polynomials.

(3) $x^2 + 1$ is reducible in ${}^{\mathbb{Z}}\!/_{2\mathbb{Z}}[x]$. Notice that $1^2 + 1 = 1 + 1 \equiv 0 \mod 2$. Then $x^2 + 1 = (x + t)(x + 1) = (x + 1)^2$ in ${}^{\mathbb{Z}}\!/_{2\mathbb{Z}}[x]$. Similarly, we can observe that $x^3 + x + 1$ is irreducible in ${}^{\mathbb{Z}}\!/_{2\mathbb{Z}}[x]$.

Lemma 3.3.4. *Let $I \neq (1)$ be a proper ideal of an integral domain R, and $p \in R[x]$, is a nonnegative monic polynomial. If $p \mod I$ cannot be factored in ${}^{R}\!/_{I}[x]$, then p is irreducible.*

Proof. Suppose that p failes to factor in ${}^{\mathbb{R}}\!/_{I}[x]$, but that it is reducible in $R[x]$. Then there exist $a, b \in R[x]$ monic and nonconstant polynomials for which $p(x) = a(x)b(x)$. Then $p \equiv ab \mod I$ which is a factorization in ${}^{R}\!/_{I}[x]$; a contradiction! ∎

Remark. The converse is not true.

Example 3.5. (1) Let $p(x) = x^2 + x + 1 \in \mathbb{Z}[x]$. Then $p \mod 2$ is irreducible in ${}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$, so that p is irreducible in $\mathbb{Z}[x]$.

(2) Notice that $x^2 + 1$ is irreducible in ${}^{\mathbb{Z}}\!/_{3\mathbb{Z}}[x]$, so that it is irreducible in $\mathbb{Z}[x]$.

(3) The polynomial $x^2 + xy + 1$ is irreducible in $\mathbb{Z}[x, y]$. Take the ideal (y), and notice that $x^2 + xy + 1 \mod (y) \equiv x^2 + 1$ in ${}^{\mathbb{Z}[x,y]}\!/_{(y)} \simeq \mathbb{Z}[x]$ which is irreducible.

(4) The polynomial $xy + x + y + 1 = (x + 1)(y + 1)$ is reducible, but is irreducible $\mod (x)$ and $\mod (y)$ as well. This occures since nonunit polynomials in $\mathbb{Z}[x, y]$ can reduce to units in the quotient. Hence, to determine irreduciblity in $\mathbb{Z}[x, y]$ using ideals, it is necessary to first observe which elements reduce to quotients in the quotient ring.

Theorem 3.3.5 (The Eisenstein-Schömann Criterion)**.** *Let P a prime ideal of an integral domain R, and let*

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

a polynomial in $R[x]$ of degree $n \geq 1$. If $a_0, \ldots, a_{n-1} \in P$, and $a_0 \notin P^2$, then f is irreducible.

Proof. Suppose that f is reducible; i.e. $f(x) = a(x)b(x)$, where $a, b \in R[x]$ are nonconstant polynomials. Reducing modulo P, and by the fact that $a_0, \ldots, a_{n-1} \in P$, we get $x^n \equiv ab \mod P$ in ${}^{R}\!/\!_{P}[x]$. Since P is prime, ${}^{R}\!/\!_{P}$ is an integral domain, so that either $a \mod P$ or $b \mod P$. have 0 constant term. constant term. constant term. constant term, by supposition. However, a_0 is the product of the constant terms of a and b, so that $a_0 \in P^2$, which is a contradiciton. ■

Corollary. *Let $p \in \mathbb{Z}$ be prime, and let*

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

a polynomial in $\mathbb{Z}[x]$ of degree $n \geq 1$. If $p | a_0, \ldots, a_{n-1}$ and $p^2 \nmid a_0$, then f is irreducible in $\mathbb{Z}[x]$, and in $\mathbb{Q}[x]$.

Example 3.6. (1) by Eisenstein's criterion for $p = 5$, $x^4 + 10x + 5$ is irreducible in $\mathbb{Z}[x]$.

(2) IF $a \in \mathbb{Z}$, and p is a prime such that $p|a$, but $p^2 \nmid a$, then the polynomial $x^n - a$ is irreducible in $\mathbb{Z}[x]$ for all $n \geq 1$.

(3) COnsider $f(x) = x^4 + 1$ in $\mathbb{Z}[x]$. Let $g(x) = f(x+1) = x^4 + 4x^3 + 6x^2 + 4x + 2$, and take $p = 2$. Then $p|2, 4, 6$, but $4 \nmid 2$, so tht $g(x)$ is irreducible. This implies that f is irreducible.

(4) Let p a prime, and let

$$\Phi_n(x) = \frac{x^p - 1}{x - 1} = x^p + x^{p-1} + \cdots + x + 1$$

Take $\Phi_p(x+1) = x^{p-1} + px^{p-1} + \cdots + \frac{p(p-1)}{2}x + p \in \mathbb{Z}[x]$. By Eisenstein's criterion, Φ_p is irreducible.

(2) Consider the polynomial $y^n - x \in \mathbb{Q}[x, y]$ for all $n \geq 0$. Notice that (x) is prime in $\mathbb{Q}[x]$ and that ${}^{\mathbb{Q}[x]}\!/\!_{(x)} \simeq \mathbb{Q}$, we have $y^n - x$ is irreducible in $\mathbb{Q}[x, y] = \mathbb{Q}[y][x]$.

3.4 Polynomial Rings over Fields.

Theorem 3.4.1. *Let F be a field. Then the polnomial ring $F[x]$ is a Euclidean domain. That is, if $a(x), b(x) \in F[x]$, with $b(x) \neq 0$, then there exist unique polynomials $q(x), r(x) \in F[x]$ such that*

$$a(x) = q(x)b(x) + r(x) \text{ where } r(x) = 0 \text{ or } \deg r < \deg b$$

Proof. If $a(x) = 0$, then take $q(x) = r(x) = 0$ and we are done. Now, suppose that $a(x) \neq 0$ and let $\deg a = n$. Then by induction on n, let $\deg b = m$. If $n < m$, then take $q(x) = 0$ and $r(x) = a(x)$. Otherwise, we have $n \geq m$. Now, write

$$a(x) = a_0 + a_1 x + \cdots + a_n x^n$$
$$b(x) = b_0 + b_1 x + \cdots + b_m x^m$$

Let $a'(x) = a(x) - \frac{a_n}{b_m} x^{n-m} b(x)$. Then $\deg a \leq n$, and since $a_n, b_m \in F$ and $b_m \neq 0$, $a'$is well defined. By induction, let $q'(x), r(x) \in F[x]$ such that

$$a'(x) = q'(x)b(x) + r(x) \text{ where } r(x) = 0 \text{ or } \deg r < \deg b$$

Then take $q(x) = q'(x) - \frac{a_n}{b_m} x^{n-m}$ Then we have

$$a(x) = q(x)b(x) + r(x) \text{ where } r(x) = 0 \text{ or } \deg r < \deg b$$

Now, for uniqueness, suppose that $q_1, r_1 \in F[x]$ are such that

$$a(x) = q_1(x)b(x) + r_1(x) \text{ where } r_1(x) = 0 \text{ or } \deg r_1 < \deg b$$

Then $r(x) = a(x) - q(x)b(x)$ and $r_1(x) = a(x) - q_1(x)b(x)$ both have degree $\deg < m$. Then the difference $r(x) - r_1(x) = b(x)(q(x) - q_1(x))$ also has degree less than m. Moreover, we have that $\deg b(q - q_1) = \deg b + \deg(q - q_1) = m + \deg(q - q_1)$. This makes $q(x) - q_1(x) = 0$, so that $q(x) = q_1(x)$. It follows then that $r(x) = r_1(x)$. ■

Corollary. *If F is a field, then $F[x]$ is a principle ideal domain. Moreover, it is a Unique Factorization Domain.*

Example 3.7. (1) We have yet another example of $\mathbb{Z}[x]$ not being a PID, and that is because $\mathbb{Z}$ is not a field.

(2) The ring $\mathbb{Q}[x]$ is a PID, since $\mathbb{Q}$ is a field. Moreover, notice that the ideal $(2, x)$ is not principle in $\mathbb{Z}[x]$, but is principle in $\mathbb{Q}[x]$, since 2 is a unit in $\mathbb{Q}[x]$. Moreover, $(2, x) = (1)$, making it the entire ring.

(3) If p is prime, then the ring $\mathbb{Z}/p\mathbb{Z}[x]$ is a PID, since $\mathbb{Z}/p\mathbb{Z}$ is a field. If $p = 2$, then the ideal $(2, x) = (x)$ and is prinicple in $\mathbb{Z}/2\mathbb{Z}[x]$. If $p \neq 2$, then 2 is a unit, making $(2, x) = (1)$; the entire ring.

(4) The multivariate polynomial ring $\mathbb{Q}[x, y] = \mathbb{Q}[x][y]$ is not a PID, since $\mathbb{Q}[x]$ is not a field. Notice also that (x, y) is not prinicple in $\mathbb{Q}[x, y]$.

Lemma 3.4.2. *Let F be a field. The maximal ideals in $F[x]$ are (f) generated by irreducible polynomials $f \in F[x]$. That is, $F[x]/(f)$ is a field if, and only if f is irreducible.*

Lemma 3.4.3. *Let F be a field, and $g(x) \in F[x]$ a nonconstant monic polynomial such that $g(x) = f_1^{n_1}(x) \dots f_k^{n_k}(x)$ is its unique factorization. Then*

$$F[x]/(g) \simeq F[x]/(f_1^{n_1}) \times \cdots \times F[x]/(f_k^{n_k})$$

Proof. By Sun Tsu's theorem, notice that since $(f_i, f_j) = 1$ in $F[x]$, as a Euclidean domain, then $(f_i^{n_i}) + (f_j^{n_j}) = F[x]$. Then they are comaximal. ■

Theorem 3.4.4. *If f has roots $\alpha_1, \ldots, a_k$ in F, non necesarily distinct, then f has a factor of the form $(x - \alpha_1) \ldots (x - \alpha_k)$. That is, a polynomial of degree n in $F[x]$ has at most n roots.*

Proof. Notice that since α_1 is a root, f has the linear factor $(x - \alpha_1)$. Hence, proceeding recursively for $\alpha_2, \ldots, \alpha_k$, we get the linear factors $(x - \alpha_1), \ldots, (x - \alpha_k)$ of f. This makes $(x - \alpha_1) \ldots (x - \alpha_k)$ a factor of f. Now, since linear factors are irreducible and $F[x]$ is a UFD, then if $\deg f = n$, f factors into at most n linear factors of the above form. ■

Lemma 3.4.5. *A finite subgroup of the multiplicative group of a field is cyclic.*

Proof. Deferred until Direct and Semidirect products of groups are studied. ■

Corollary. *If F is a finite field, then $\mathcal{U}(F)$ is cyclic.*

Corollary. *For any prime p, the unit group $\mathcal{U}(\mathbb{Z}/p\mathbb{Z})$ is cyclic.*

Corollary. *Let $n \geq 2$ an integer with $n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ its unique factorization, where $p_1, \ldots, p_r \in \mathbb{Z}$ are distinct primes. Then the following are true.*

(1) $\mathcal{U}(\mathbb{Z}/n\mathbb{Z}) = \mathcal{U}(\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times \cdots \times \mathcal{U}(\mathbb{Z}/p_r^{\alpha_r}\mathbb{Z})$.

(2) $\mathcal{U}(\mathbb{Z}/2^\alpha\mathbb{Z})$ *is the direct product of a cyclic group of order 2 and a cyclic group of order* $2^{\alpha-2}$.

(3) $\mathcal{U}(\mathbb{Z}/p^\alpha\mathbb{Z})$ *is a cyclic group of order* $p^{\alpha-1}(p-1)$ *for all* $p \in \mathbb{Z}$ *an ood prime.*

Chapter 4

Modules

4.1 Definitions and Examples

Definition. Let R be a ring. A **left module** over R, or a **left R-module**, is a set M together with a binary operation $+ : M \times M \to M$, called **addition**, and a left action $R \times M \to M$ of R on M, defined by $(r, m) \to rm$, called **left scalar multiplication** such that M is an Abelian group under $+$, and for all $r, s \in R$ and $m, n \in M$

(1) $(r + s)m = rm + sm$

(2) $(rs)m = r(sm)$

(3) $r(m + n) = rm + rn$

We define **right modules** over R similarly, where the action is a right action $M \times R \to M$ defined by $(m, r) \to mr$.

Definition. Let R be a ring with identity 1, and M a left (or right module) over R. We call M **unital** if $1m = m$ (or $m1 = m$) for all $m \in M$.

Lemma 4.1.1. *If R is a commutative ring, then every left module of R is also a right module over R.*

Definition. Let R be a ring, and M be a module over R. A **submodule** of M over R is a subgroup N of M which is closed under the action of R on M; i.e. that is $rn \in N$ for all $r \in R$ and $n \in N$.

Example 4.1. (1) Every module M, has as itself, and the subgroup (0) as submodules. We call (0) the **trivial module**.

(2) If F is a field, then every F-module is a vector space over F. Moreover, every submodule of an F-module is a subspace of the overlying vector space. It can be shown that if F is a field, then the definition for modules and vector spaces coincide.

(3) If R is a ring, then R is a left module over itself with scalar multiplication being the the multipliaction of R. Moreover, R is a right module over itself (these structures need not coincide).

(4) Let R be a ring with identity 1, and $n \in \mathbb{Z}^+$. Make R^n into an left R-module by defining $+$ to be component wise addition, and left scalar multiplication $R \times R^n \to R^n$ defined by

$$r(a_1, \ldots, a_n) = (ra_1, \ldots, ra_n)$$

We call R^n the **free module** of **rank** n over R. Notice that if R is a field, then R^n become the usual n-space over R.

(5) The field $\mathbb{R}$ is an $\mathbb{R}$-module, a $\mathbb{Q}$-module, and a $\mathbb{Z}$-module. More generally, if R is a ring with identity 1_R, and S is a subring of R with identity 1_S, such that $1_R = 1_S$, then every R-module is also an S-module.

(6) Let R be a ring, and M an R-module, and let I be an ideal of R, such that $am = 0$ for all $a \in I$ and $m \in M$. Then we say that I **annihilates** M. Make M into an left $({}^{R}\!/_{I})$-module by defining the addition to be the addition of M, and left scalar multiplication to be the action ${}^{R}\!/_{I} \times M \to M$ defined by

$$(r + I)m = rm$$

(7) Let A be any Abelian group. We can make A into a left $\mathbb{Z}$-module by defining $+$ to be group operation on A, and defining left scalar multiplication $(n, a) \to na$ by

$$na = \begin{cases} a + \cdots + a \ (n\text{-times}), \ \text{if } n > 0 \\ 0, \ \text{if } n = 0 \\ (-a) + \cdots + (-a) \ (n\text{-times}), \ \text{if } n < 0 \end{cases}$$

Then it can be shown that this action makes A into a unital $\mathbb{Z}$-module (notice that since $\mathbb{Z}$ is commutative, A is also a right $\mathbb{Z}$-module).

Conversely, if we have M as a $\mathbb{Z}$-module, then by definition M is an Abelian group. That is, we have shown that every Abelian group is a $\mathbb{Z}$-module, having as $\mathbb{Z}$-submodules all subgroups.

Notice now, that if A is an Abelian group, and $x \in A$ is of order n, the $nx = 0$. Therefore, there exist scalars $n \in \mathbb{Z}$ and elements $x \in A$ for which $nx = 0$. Notice, then if $\operatorname{ord} A = m$, then by Lagrange's theorem, $mx = 0$ for all $x \in A$; this shows that A is also a $({}^{\mathbb{Z}}\!/_{m\mathbb{Z}})$-module.

(8) Consider the example above. If A is a $({}^{\mathbb{Z}}\!/_{p\mathbb{Z}})$-module, since ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ is a field, then A can be considered as a vector space over the finite field $\mathbb{F}_p = {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$. We call these group **elementary Abelian p-groups**. For example, the Klein 4-group, V_4 is an elementary Abelian 2 -group (it is a vector space over $\mathbb{F}_2$ of $\dim V_4 = 2$).

Example 4.2 (Polynomials). (1) Let F be a field, and consider the polynomial riong $F[x]$. Let V be a vector space over F, and let T be a linear transformation. Define $+$ on V to be the usual vector addition, and define the left action $F[x] \times V \to V$ by

$$p(x)v = (a_nT^n + \cdots + a_1T + a_0)v = a_nT^(v) + \cdots + a_1T(v) + a_0v$$

Where $p(x) = a_nx^n + \cdots + a_1x + a_0$, and $a_0, \ldots, a_n \in F$. Then $p(x)$ acts on V as the linear transofrmation T. Then the action $F[x] \times V \to V$ makes V into a left $F[x]$-module.

(2) Consider the vector space V over F as the affine n-space F^n, and consider the **left shift operator** $T(x_1, \ldots, x_n) = (x_2, \ldots, x_n, 0)$. Letting $\{e_1, \ldots, e_n\}$ the standard basis of F^n over F, notice that

$$T^k(e_i) = \begin{cases} e_{i-k}, & \text{if } i > k \\ 0, & \text{if } i \leq k \end{cases}$$

Then T determines the action of any polynomial $p \in F[x]$ on a vector $v \in V$. This shows that the action $F[x] \times V \to V$ depends on our choice of T. This gives a 1–1 correspondence between all V as $F[x]$-modules, and all pairs (V, T), where V is a vector space and T is a gien linear transformation.

(3) Consider the vector space V as an $F[x]$-module, with T the linear transformation givenby the action of x on V. Let $W \subseteq V$ be an $F[x]$-submodule. Then W must also be an F-module, and hence must be a subspace of V. Moreover, notice that T takes W onto itself; i.e. $T(w) \in W$ for all $w \in W$, so that W is **T-invariant**.

Conversely, if T is a T-invariant subspace of V as a vector space over F, then $T^n(W) \subseteq W$ for all $n \in \mathbb{Z}^+$. Moreover, any linear combination of T^n takes W onto itself, so that W is also invariant by the action of any polynomial in T. This makes W into an $F[x]$-submodule. That is, there is a 1–1 correspondence between $F[x]$-submodules, and T-invariant subspaces of V.

Remark. From here on, we will mean "module" to mean left module, and "scalar multiplaction" to mean left scalar multiplication, unless otherwise specified.

Lemma 4.1.2 (The Submodule Criterion for Unital Modules)**.** *Let R be a ring with identity, and M be a unital module over R. A nonempty subset N of M is a submodule over R if, and only if for every $r, s \in R$, and $x, y \in N$, $rx + sy \in N$.*

Proof. Suppose that N is a submodule for M. Then $0 \in N$, so that N is nonempty. Moreover, by the axioms for modules, observe that if we restrict the scalar multiplication of M to N (i.e. $R \times N \to N$), then $rx + sy \in N$ for all $x, y \in N$ and $r, s \in R$; that is the action of R on N takes N onto itself.

Conversely, suppose that N is nonempty, and that for any $x, y \in N$, and $r, s \in R$, that $rx + sy \in N$. Take $s = 0$, then we have that $rx \in N$, which makes N closed under scalar multiplication. Moreover, let $r = 1$ amd $s = 1$, then we get $x + y \in N$; and for $r = 0$ and $s = -1$, we have $-y \in N$. By the subgroup criterion, this makes $N \leq M$. Therefore N is a submodule of M. ■

Definition. Let R be a commutative ring with identity. An **R-algebra** is a ring A with identity, together with a ring homomorphism $f : R \to A$, taking $1_R \to 1_A$ such that the subring $f(R)$ of A is contained in the center of A; i.e. $f(R) \subseteq Z(A)$.

Lemma 4.1.3. *Let R be a commutative with with identity. If A is an R-algebra, then A is a left module of R, and a right module of R.*

Proof. Let $+$ be the usual addition for A, and define the actions $R \times A \to A$ and $A \times R \to A$ by

$$ra = f(r)a \text{ and } ar = af(r)$$

respectively. Notice by definition that $f(r)a = af(r)$, so that $ra = ar$. ■

Definition. Let R be a commutative wrng with identity, and let A and B R-algebras. A **R-algebra homomorphism** is a ring homomorphism $\phi : A \to B$, taking $1_A \to 1_B$, such that $\phi(ra) = r\phi(a)$ for all $r \in R$ and $a \in A$; where $ra = f(r)a$ is the underlying scalar multiplication of A. We call ϕ a **R-algebra isomorphism** if ϕ is a ring isomorphism.

Example 4.3. Let R be a commutative ring with identity 1_R.

(1) Every commutative ring with identity is a $\mathbb{Z}$-algebra. Take $f : \mathbb{Z} \to R$ via the map $f : n \to n \cdot 1_R$.

(2) For any ring A with identity 1_A, if R is a subring of the center $Z(A)$, containing 1_A, then A is an R-algebra. In particular, a commutative ring A with identity is an R-algebra for any subring R of $Z(A)$ containing 1_A.

(3) The polynomial ring $R[x]$, the multivariate polynomial ring $R[x_1, \ldots, x_n]$, and the ring RG, for any finite group G are all R-algebras.

(4) If A is an R-algebra, then the R-module structure of A depends on the image $f(R) \subseteq Z(A)$. In fact, every algebra A arises from a subring of $Z(A)$, containing 1_A, up to homomorphism.

(5) Let F be a field, and A an F-algebra. Then F itself is a subring of $Z(A)$ containing 1_A, in fact, $1_A = 1_F$.

Lemma 4.1.4. *Let R be a commutative ring with identity. Then a ring A with identity 1_A is an R-algebra if, and only if it is a unital module satisfying*

$$r(ab) = (ra)b = a(rb) \textit{ for all } r \in R \textit{ and } a, b \in A$$

where $ra = f(r)a$ is the underlying action of R on A.

Proof. Certainly, if A is an R-algebra, then it is a unital module. Moreover, notice that if $ra = f(r)a$, then $r(ab) = f(r)(ab) = (f(r)a)b = a(f(r)b)$, so that $r(ab) = (ra)b = a(rb)$.

Conversely, suppose that A is a unital module satisfying

$$r(ab) = (ra)b = a(rb) \text{ for all } r \in R \text{ and } a, b \in A$$

And where $ra = f(r)a$, where $f : R \to A$ is a ring homomorphism. Then $1_R a = f(1_R)a = a$, so that $f(1_R) = 1_A$; that is, $f : 1_R \to 1_A$. Moreover, since $r(ab) = (ra)b = a(rb)$, we have that $(f(r)a)b = a(f(r)b)$, i.e. that $f(r)a = af(r)$ for all $a, b \in A$ and $r \in R$. This makes $f(r) \in Z(A)$, so that $f(R) \subseteq Z(A)$. This makes A into an R-algebra. ■

4.2 Module Homomorphisms and Factor Modules

We make the conventions that when we say "ring", we mean a ring with identity, and when we say "module", we mean unital modules.

Definition. Let R be a ring, and M and N modules. We call a map $\phi : M \to N$ a **module homomorphism** over R (or an R**-module homomorphism**) if for all $x, y \in M$, and $r \in R$

(1) $\phi(x + y) = \phi(x) + \phi(y)$.

(2) $\phi(rx) = r\phi(x)$.

We call ϕ a **module isomorphism** (or an R**-module isomorphism**) if ϕ is 1–1 and takes M onto N; and we call M and N **isomorphic** and write $M \simeq N$.

Definition. Let R be a ring, M and N R-modules, and let $\phi : M \to N$ be a module homomorphism over R. We define the **kernel** of ϕ to be the set

$$\ker \phi = \{m \in M : \phi(m) = 0\}$$

We denote the set $\mathrm{Hom}_R(M, N)$ to be the set of all module homomorphisms over R from M into N.

Lemma 4.2.1. *Let R be a ring, and M, and N module s. let $\phi : M \to N$ be a module homomorphism of R. Then the following are true*

(1) $\ker \phi$ *is a submodule of M.*

(2) $\phi(M)$ *is a submodule of N.*

Proof. Notice that if $\phi : M \to N$ is a module homomorphism, then it is also a group homomorphism, since M and N are both groups under their respective additions. This makes $\ker \phi$ and $\phi(M)$ into subgroups of M and N respectively (this also implies that both $\ker \phi$ and $\phi(M)$ are nonempty).

Now, let $r, s \in R$, and $x, y \in \ker \phi$. Then we get $\phi(rx+sy) = r\phi(x)+s\phi(y) = r0+s0 = 0$, so that $rx+sy \in \ker \phi$. Similarly, if $\phi(x), \phi(y) \in \phi(M)$, then $r\phi(x)+s\phi(y) = \phi(rx)+\phi(sy) = \phi(rx + sy) \in \phi(M)$. By the submodule criterion for unital modules, we are done. ■

Example 4.4. (1) Module homomorphisms need not be ring homomorphisms. Consider the ring $\mathbb{Z}$ as a module over itself. Then the map $x \to 2x$ is a $\mathbb{Z}$-module homomorphism, but not a ring homomorphism, since this map takes $1 \to 2$, and $2 \neq 1$ in $\mathbb{Z}$. Likewise, ring homomorphisms need not be module homomorphisms. Let F be a field, and consider the map $f(x) \to f(x^2)$, where $f(x) \in F[x]$. This map is a ring homomorphism, but it is not an $F[x]$-module homomorphism when considering $F[x]$ as a module over itself.

(2) Let R be a ring, and $n \in \mathbb{Z}^+$ Consider the i**-th projection map** $\pi_i : R^n \to R$ defined by

$$\pi_i : (x_1, \ldots, x_n) \to x_i$$

Then π_i is an R-module homomorphism. Moreover, we have $\pi_i(R^n) = R$ (so that π_i is onto) and $\ker_i = \{(x_1, \ldots, x_n) : x_i = 0\}$.

(3) For any field F, and any vector spaces V and W over F, the usual linear transofrmations $T : V \to W$ are F-module homomorphisms by definition.

(4) $\mathbb{Z}$-module homomorphisms are Abelian group homomorphisms. Recall that module homomorphisms are group homomorphisms, and that $\mathbb{Z}$ is an Abelian group.

(5) Let R be a ring, and I an ideal of R. Suppose that M and N are R-modules which are annihilated by I. Then any R-module homomorphism of $M \to N$ is also an $({}^{R}\!/\!_{I})$-module homomorphism.

Lemma 4.2.2. *Let R be a ring, and let M, N, and L be modules over R. Then the following are true*

(1) A map $\phi : M \to N$ is a module homomorphism over R if, and only if $\phi(rx + sy) = r\phi(x) + s\phi(y)$ for any $x, y \in M$ and $r, s \in R$.

(2) $\mathrm{Hom}_R(M, N)$ is an Abelian group under function addition.

(3) If $\phi \in \mathrm{Hom}_R(M, N)$ and $\psi \in \mathrm{Hom}_R(N, L)$, then $\psi \circ \phi \in \mathrm{Hom}_R(M, L)$ where $\circ$ is the usual function composition.

(4) $\mathrm{Hom}_R(M, M)$ is a ring with identity under the operations of function addition and function composition.

Proof. We break the proof into its respective parts.

(1) By definition, if ϕ is a module homomorphism, then $\phi(rx + sy) = \phi(rx) + \phi(sy) = s\phi(x) + y\phi(y)$ for all $x, y \in M$ and $r, s \in R$. Conversely if $\phi(rx + sy) = r\phi(x) + s\phi(y)$, taking $r, s = 1$ gives $\phi(x + y) = \phi(x) + \phi(y)$, and taking $s = 0$ and $y = 0$ gives $\phi(rx) = r\phi(x)$.

(2) Now, consider $\phi, \psi \in \mathrm{Hom}_R(M, N)$. Observing that $(\phi + \psi)(x) = \phi(x) + \psi(x)$, we get for all $x, y \in M$ and $r, s \in R$ that

$$\begin{aligned}
(\phi + \psi)(rx + sy) &= \phi(rx + sy) + \psi(rx + sy) \\
&= (r\phi(x) + s\phi(y)) + (r\psi(x) + s\psi(y)) \\
&= (r\phi(x) + r\psi(x)) + (s\phi(y) + s\psi(y)) \\
&= r(\phi + \psi)(x) + s(\phi + \psi)(y)
\end{aligned}$$

Since $x, y \in M$ and $\phi(x), \phi(y), \psi(x), \psi(y) \in N$, this makes $\phi + \psi \in \mathrm{Hom}_R(M, N)$. Moreover, notice that $+$ is associative and commutative. We get the map $x \to 0$ as the identity homomorphism, and $(-\phi) : x \to -\phi(x)$ as the additive inverse of ϕ. This makes $\mathrm{Hom}_R(M, N)$ into a group.

(3) Let $\phi \in \operatorname{Hom}_R(M, N)$ and $\psi \in \operatorname{Hom}_R(N, L)$. Then for $x, y \in M$ and $r, s \in R$, and writing $\psi \circ \phi$ as $\psi\phi$ we get

$$\begin{aligned} \psi\phi(rx + sy) &= \psi(\phi(rx + sy)) \\ &= \psi(r\phi(x) + s\phi(y)) \\ &= r\psi\phi(x) + s\psi\psi(y) \end{aligned}$$

Since $x, y \in M$ and $\psi\phi(x), \psi\phi(y) \in L$, this makes $\psi \circ \phi \in \operatorname{Hom}_R(M, L)$.

(4) Finaly, observe that since $\operatorname{Hom}_R(M, M)$ is an Abelian group under $+$, and $\circ$ is well defined for $\operatorname{Hom}_R(M, M)$, then it suffies to show the distributive laws and identity. Notice however that $\circ$ distributes (on both side) over $+$. Moreover, $: x \to x$ serves as the identity element for $\operatorname{Hom}_R(M, M)$ under $\circ$. That is $\operatorname{Hom}_R(M, M)$ is indeed a ring with identity.

■

Corollary. *If R is a commutative ring, then the following are true*

(1) $\operatorname{Hom}_R(M, N)$ *is a module over R, under the action $(r\phi)(x) = r(\phi(x))$.*

(2) $\operatorname{Hom}_R(M, M)$ *is an R-algebra under function addition and function composition.*

Proof. Again, spilitting the proof by parts

(1) Notice that for $r, s \in R$, that

$$\begin{aligned} (r\phi)(sx) &= r(\phi(sx)) \\ &= r(s\phi(x)) \\ &= (rs)\phi(x) \\ &= (sr)\phi(x) \\ &= s(r\phi(x)) \\ &= s((r\phi)(x)) \end{aligned}$$

This makes $r\phi \in \operatorname{Hom}_R(M, N)$, which makes it into a module over R.

(2) By (4) in the above lemma, we have that $\operatorname{Hom}_R(M, M)$ is a ring with identity. Moreover, notice that (1) in the above statement makes $\operatorname{Hom}_R(M, M)$ into a module over R. Then taking $\phi r = r\phi$, we get that $\operatorname{Hom}_R(M, M)$ is an R-algebra.

■

Definition. Let R be a ring, and M a module over R. We call the ring $\operatorname{Hom}_R(M, M)$ the **endomorphism ring** of M and denote it $\operatorname{End}_R M$, or $\operatorname{End} M$ (when context is clear). We call the elements of $\operatorname{End}_R M$ **endomorphisms**.

Example 4.5. Let R be a ring with ideal I, and M an R-module. The ring homomorphism $R \to \operatorname{End} M$ defined by $r \to rI$ need not be 1–1. Notice that the homomorphism $\mathbb{Z} \to \operatorname{End} \mathbb{Z}/2\mathbb{Z}$ defined by $2 \to 2\mathbb{Z}$ is not 1–1. Notice that $2x = 0$ for any $x \in \mathbb{Z}/2\mathbb{Z}$, so that the kernel is $\mathbb{Z}/2\mathbb{Z}$. However, if R is a field, then the homomorphism $r \to rI$ is 1–1. In this case, we call the imbedding of R into $\operatorname{End}_R M$ the ring of **scalar transformations**.

Lemma 4.2.3. *Let R be a ring, and M a module over R, and let $N \subseteq M$ a submodule. Then the additive quotient gorup M/N is a module over R, under the action $R \times M/N \to M/N$ defined by*

$$r(x + N) = rx + N$$

Proof. Since M is an Abelian group under its addition, $N \trianglelefteq M$, and M/N is an Abelian group. Now, consider $r \in R$, and suppose that $x + N = y + N$, for some $x, y \in N$. Then $x - y \in N$; since N is a submodule. Then $r(x - y) = rx - ry \in N$, which makes $rx + N = ry + N$. Therefore the action $R \times M/N \to M/N$ given by $r(x + N) \to rx + N$ is well defined.

Now, since M is an R-module, we get that

$$\begin{aligned}(r + s)(x + N) &= (r + s)x + N \\ &= (rx + sx) + N\end{aligned}$$

That

$$\begin{aligned}(rs)(x + N) &= (rs)x + N \\ &= r(sx) + N \\ &= r(s(x + N))\end{aligned}$$

that

$$\begin{aligned}r((x + N) + (y + N)) &= r((x + y) + N) \\ &= r(x + y) + N \\ &= (rx + ry) + N\end{aligned}$$

This makes M/N into an R-module. ■

Corollary. *The projection $\pi : M \to M/N$ given by $\pi : x \to x + N$ is a module homomorphism with* $\ker \pi = N$.

Proof. Notice by definition that $: x \to x + N$ is a group homomorphism with $\ker \pi = N$. Now, let $r \in R$, ten $\pi(rx) = rx + N = r(x + N) = r\pi(x)$. ■

Definition. Let M be a module, and let A and B submodules of M. We define the **sum** of A and B to be the set

$$A + B = \{a + b : a \in A \text{ and } b \in B\}$$

Lemma 4.2.4. *Let M be a module, and A and B submodules. Then $A + B$ is a submodule of M.*

Theorem 4.2.5 (The First Isomorphism Theorem)**.** *Let R be a ring, and M, N be modules over R and let $\phi : M \to N$ a module homomorphism over R. Then $\ker\phi$ and $\phi(M)$ are submodules of M, and*

$$M \big/ \ker\phi \simeq \phi(M)$$

Theorem 4.2.6 (The Second Isomorphism Theorem)**.** *Let R be a ring and M a module over M. Let A and B be submodules of M. Then*

$$(A + B) \big/ B \simeq A \big/ (A \cap B)$$

Theorem 4.2.7 (The Third Isomorphism Theorem)**.** *Let M be a module, and A and B submodules of M. Then*

$$(M \big/ A) \big/ (A \big/ B) \simeq M \big/ B$$

Theorem 4.2.8 (The Fourth Isomorphism Theorem)**.** *Let R be a ring, M be a module over R, and N be a submodule of M. Then there exists a 1–1 correspondence of submodules of M containing N, onto submodules of $M \big/ N$ given by the map*

$$A \to A \big/ N$$

for all $N \subseteq A$.

4.3 Direct Products and Free Modules.

Definition. Let M be an R-module, and $N_1, \ldots, N_n$ submodules of M. We define the **sum** of $N_1, \ldots, N_n$ to be the set

$$N_1 + \cdots + N_n = \{a_1 + \cdots + a_n : a_i \in N_i\}$$

For any subset $A \subseteq M$, we call the set

$$RA = \{r_1 a_1 + r_n a_n : r_j \in R \text{ and } a_i \in A\}$$

the submodule of M **generated** by A. If A is empty, we write $RA = (0)$. If A is finite, we write $RA = Ra_1 + \cdots + Ra_n$. We call a submodule N of M **finitely generated** if there is a finite set $A \subseteq M$ for which $N = RA$. We call N **cyclic** if there is an $a \in M$ for which $N = Ra$.

Example 4.6. (1) Let M be any $\mathbb{Z}$-modules, if $a \in M$, then $\mathbb{Z}a = \langle a \rangle$ is the cyclic group generated by a. Moreover, M is generated as a $\mathbb{Z}$-moduled, by a set A if, and only if A is an Abelian group.

(2) Let R be a ring with identity, and consider R as a left R-module over itself. Then R is finitely generated, and is in fact, cyclic. Indeed, $R = R1$. Now, if I is a cyclic subgroup of R, then R is a principle ideal of R. If I is finitely generated as a submodule of R, it is finitely generated as an ideal.

(3) Let R be a ring with identity, and consider R^n the free module of rank n ver R, Let $e_i = (0, \dots, 0, 1, 0, \dots, 0)$ the element where 1 appears in the i-th position, for all $1 \leq i \leq n$. Then we have

$$(s_1, \dots, s_n) = s_1 e_1 + \cdots + s_n e_n$$

so that M is generated by the set $\{e_1, \dots, e_n\}$. If R is commutative, then this is a generating set.

(4) Let F be a field, and let V be a vector space over F. Let $T : V \to V$ a linear transformation making V into an $F[x]$-moddule. Then V is a cyclic $F[x]$-module, with generator v, if, and only if $V = \{p(x)v : p \in F[x]\}$. That is, elements of V can be written as linear combinations of elements of the set $\{T^n v : n \geq 0\}$; that is, $\operatorname{span} V = \{v, Tv.T^2 v, \dots\}$

Definition. Let $M_1, \dots, M_n$ a a collection of R-modules. We define the **external direct product** of $M_1, \dots, M_n$ to be

$$M_1 \times \cdots \times M_n = \{(m_1, \dots, m_n) : m_i \in M_i\}$$

We define the addition and scalar multiplication on $M_1 \times M_n$ to be the addition and scalar multiplication of M_i component-wise for all $1 \leq i \leq n$.

Lemma 4.3.1. *Let $M_1, \dots, M_n$ be R-modules. Then the external direct product $M_1 \times \cdots \times M_n$ is an R-module.*

Lemma 4.3.2. *Let $N_1, \dots, N_n$ me submodules of an R-module M. The following statements are equivalent.*

(1) Then map $\pi : N_1 \times N_n \to N_1 + \cdots + N_n$ defined by $(a_1, \dots, a_n) \to a_1 + \cdots + a_n$ is an isomorphism.

(2) $N_i \cap (N_1 + \cdots + N_{i-1} + N_{i+1} + \cdots + N{+}_n) = (0)$ for all $1 \leq i \leq n$.

(3) Every $\xi \in N_1 + \cdots + N_n$, can be written uniquely as

$$x = a_1 + \cdots + a_n \text{ where } a_i \in N_i$$

Proof. First suppose that $N_1 \times \cdots \times N_n \simeq N_1 + \cdots + N_n$ via the isomorphism $\pi : (a_1, \dots, a_n) \to a_1 + \cdots + \alpha_n$. Suppose now that there exists an index $1 \leq i \leq n$ for which

$$N_i \cap (N_1 + \cdots + N_{i-1} + N_{i+1} + \cdots + N{+}_n) \neq (0)$$

for all i. Let $a_j \in N$ with $a_j \neq 0$. Then

$$a_i = a_1 + \cdots + a_{i-1} + a_{i+1} + \cdots + a_n$$

Then we get $(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n)$ is a nonzero element of $\ker \pi$, which contradicts that π is an isomorphism.

Now, suppose that

$$N_i \cap (N_1 + \cdots + N_{i-1} + N_{i+1} + \cdots + N +_n) = (0) \text{ for all } i$$

Let $a_i, b_i \in N_i$ and let $a_1 + \cdots + a_n = b_1 + \cdots + b_n$. Then

$$a_i - b_i = (a_1 - b_1) + \cdots + (a_{i-1} - b_{i-1}) + (a_{i+1} - b_{i+1}) + \cdots + (a_n - b_n)$$

Then $a_i - b_i \in N_1$ and $(a_1 - b_1) + \cdots + (a_{i-1} - b_{i-1}) + (a_{i+1} - b_{i+1}) + \cdots + (a_n - b_n) \in N$. So we get $a_i - b_i \in N$ so that $a_i = b_i$ for all $1 \leq i \leq n$.

Now, suppose that $x \in N$ can be written uniquely as $x = a_1 + \cdots + a_n$ where $a_i \in N_i$. Then $x \in N_1 + \cdots + N_n$. Observe that the map $\pi : (a_1, \ldots, a_n) \to a_1 + \cdots + a_n$ is onto. Then since $a_1 + \cdots + a_n$ uniquely determines elements in $N_1 + \cdots + N_n$, π is 1–1. ■

Definition. We call an R-module M an **internal direct product** of submodules $N_1, \ldots, N_n$ if $M = N_1 + \cdots + N_n$ and M satisfies one of the conditions of lemma 4.3.2. We write $M = N_1 \oplus \cdots \oplus N_n$.

Definition. We call an R-module F **free** on a subset $A \subseteq F$ if for every $x \in F$, there is are unique nonzero $r_1, \ldots, r_n$ and unique $a_1, \ldots, a_n \in A$ such that $x = r_1 a_1 + \cdots + r_n a_n$ for some $n \in \mathbb{Z}^+$. We call A a **basis** of F. If R is commutative, we call $|A|$ the **rank** of F and write $\operatorname{rank} F = |A|$.

Example 4.7. The module ${}^{\mathbb{Z}}\!/\!_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/\!_{2\mathbb{Z}}$ is not a free $\mathbb{Z}$-module on the set $\{(1,0),(0,1)\}$. It is not free on any set.

Theorem 4.3.3. *For any set A, there is a free R-module $F(A)$ on A, such that if M is any R-module, and $\phi : A \to M$ is any map, then there is a unique module homomorphism $\Phi : F(A) \to M$ such that $\Phi(a) = \phi(a)$ for all $a \in A$. That is, the following diagram commutes.*

$$\begin{tikzcd} A \arrow[r, "i"] \arrow[dr, "\phi"'] & F(A) \arrow[d, "\Phi"] \\ & M \end{tikzcd}$$

Moreover, if $A = \{a_1, \ldots, a_n\}$, then

$$F(A) = Ra_1 \oplus \cdots \oplus Ra_n \simeq R^n$$

Proof. Let $F(A) = (0)$. If A is empty, and the collection of all set functions $f : A \to R$ such that $f(a) = 0$ for all but finitely many $a \in A$, if A is nonempty. Make $F(A)$ into an R-module via pointwise adition and the action $R \times F(A) \to F(A)$ defined by $(rf)(a) = r(f(a))$ for all $a \in A$, $r \in R$, and $f, g \in F(A)$. Take the mape $a \to f_a$ where

$$f_a(x) = \begin{cases} 1, x = a \\ 0, x \neq a \end{cases}$$

This map makes $A \subseteq F(A)$. Then $F(A)$ can be expressed as all finite R-linear combination of elements of A by identifying each f with $r_1a_1 + \cdots + r_na_n$, where

$$f(x) = \begin{cases} r_i, x = a_i \\ 0, x \neq a_i \end{cases}$$

Moreover, each element of $F(A)$ has a unique expression.

Now, let $\phi : A \to R$ be a map and define $\Phi : F(A) \to R$ by taking $r_1a_1 + \cdots + r_na_n \to r_1\phi(a_1) + \cdots + r_n\phi(a_n)$. By the uniqueness of expression of elements in $F(A)$, Φ is a well defined R-module homomorphism. Moreover, by definition, $\Phi|_A = \phi$. Finally, since $F(A)$ is generated by A, and the values of any R-module homomorphism on $F(A)$ are uniquely determined, this makes Φ the unique extension of ϕ to $F(A)$.

Now, let $A = \{a_1, \ldots, a_n\}$. THen $F(A) = Ra_1 \oplus \cdots \oplus Ra_n$ by the above lemma. Moreover, since $R \simeq Ra_i$ for all $1 \leq i \leq n$, we get $F(A) \simeq R^n$. ∎

Corollary. *The following statements are true.*

(1) If F_1 and F_2 are free modules on A, there is a unique isomorphism between F_1 and F_2 which is the identity isomorphism on A.

(2) IF F is any free R-module with basis A, then $F \simeq F(A)$.

Definition. We call a free $\mathbb{Z}$-module on a set A the **free Abelian group** on A of **rank** $|A| = n$ (if A is finite).

4.4 Tensor Products of Modules

Definition. Let S be a ring, and R a subring of S. Let $f : S \to R$ a ring homomorphism with $f(1_S) = 1_R$ and let N be an R-module, with the scalar multiplication defined by $rn = f(r)n$. We call N a **restriction of scalars** from S to R. We call S an **extension** of R.

Example 4.8. (1) Let S a ring and R a subring of S. We can restrict an S-module N to be an R-module, but the reverse is not in general true. Consider $\mathbb{Z}$ as a $\mathbb{Z}$-module, then $\mathbb{Z}$ cannot be a $\mathbb{Q}$-module, for if it is, then the element $\frac{1}{2}1 = z$ is an element of $\mathbb{Z}$ for which $z + z = 1$, which cannot happen. Notice however that $\mathbb{Z}$ can be imbedded into a $\mathbb{Q}$-module, namely $\mathbb{Q}$ itself.

(2) Consider al possible $\mathbb{Z}$-module homomorphisms of $\mathbb{Z}/2\mathbb{Z}$ into a $\mathbb{Q}$-module V. Since $\mathbb{Q}$ is a field V is a vector space over $\mathbb{Q}$, and every element has infinite order. Since the elements of $\mathbb{Z}/2\mathbb{Z}$ are of finite order, then $x \to 0$ for all $x \in \mathbb{Z}/2\mathbb{Z}$. This shows that $\mathbb{Z}/2\mathbb{Z}$ cannot be imbedded into a $\mathbb{Q}$-module.

Definition. Let R and S be rings, and let N be an R-module. Consider the map $S \times N \to N$ defined by $(s, n) \to sn$. Consider H the subgroup generated by all elements of the form $(s_1 + s_1, n) - (s_1, n) - (s_2, n)$, $(s, n_1 + n_2) - (s, n_1) - (s, n_2)$, and $(sr, n) - (s, rn)$ for all $s, s_1, s_2 \in S$, $r \in R$, and $n, n_1, n_2 \in N$. We define the **tensor product** of S together with N over R to be the quotient group ${}^{N}\!/_{H}$. We denote this tensor product by $S \otimes_R N$. We denote the elements of $S \otimes_R N$ as $s \otimes n$ and call them **simple tensors**. We call sums of simple tensors **tensors**.

Lemma 4.4.1. *Let R and S be rings, and let N be an R-module. Then the following relations hold on the tensor product $S \otimes_R N$*

(1) $(s_1 + s_2) \otimes n = s_1 \otimes n + s_2 \otimes n$.

(2) $s \otimes (n_1 + n_2) = s \otimes n_1 + s \otimes n_2$.

(3) $sr \otimes n = s \otimes rn$.

Proof. Since $S \otimes_R N$ is the quotient group of N by H, where H the subgroup generated by all elements of the form $(s_1 + s_1, n) - (s_1, n) - (s_2, n)$, $(s, n_1 + n_2) - (s, n_1) - (s, n_2)$, and $(sr, n) - (s, rn)$; that is: $H = \langle (s_1 + s_1, n) - (s_1, n) - (s_2, n), (s, n_1 + n_2) - (s, n_1) - (s, n_2), (sr, n) - (s, rn) \rangle$. Then the tensors $s \otimes n$ are just cosets of H in N, and the relations defining H give us the relations on tensors. ■

Theorem 4.4.2. *Let S be a ring, and R a subring of S. Let N be an R-module, then the tensor product $S \otimes_R N$ is in S-module under the action*

$$s \sum s_i \otimes n_i = \sum (ss_i) \otimes n_i$$

where the sums are finite.

Proof. Let $s' \in S$, then

$$(s'(s_1 + s_2), n) - (s's_1, n) - (s's_2, n) = (s's_1 + s's_2, n) - (s's_1, n) - (s's_2, n)$$
$$(s's, n_1 n_2) - (s's, n_1) - (s's, n_2)$$
$$(s'(sr), n) - (s's, rn) = ((s's)r, n) - (s's, rn)$$

each belong to the generating set of $H = \langle (s_1 + s_1, n) - (s_1, n) - (s_2, n), (s, n_1 + n_2) - (s, n_1) - (s, n_2), (sr, n) - (s, rn) \rangle$. Since elements of H are sums of elements in H, for every $\sum (s_i, n_i) \in H$, we get $\sum (s's_i, n_i) \in H$

Now, suppose that $\sum s_i \otimes n_i = \sum s'_i \otimes n'_i$ are representatives of the same tensor in $S \otimes_R N$. Then $\sum (s_i, n_i) - \sum (s'_i, n'_i) \in H$ so that $\sum ss_i \otimes n = \sum ss'_i \otimes n \in S \otimes_R N$. This makes the action well defined.

Finally, observe that for every tensor $s_i \otimes n_i \in S \otimes_R N$, that the following relation holds, by lemma 4.4.1

$$(s + s')(s_i \otimes n_i) = s(s_i \otimes n_i) + s'(s_i \otimes n_i)$$

The other relations for modules also hold by lemma 4.4.1. ■

Definition. Let S be a rings and R a subring of S, and let N be an R-module. We call $S \otimes_R N$, as a module, the **left S-module obtained by an extension of scalars** from N.

Theorem 4.4.3. *Let R a subring of a ring S, and let N be a left R-module. Let $\iota : N \to S \otimes_R N$ be the R-module homomorphism defined by $\iota :\to 1 \otimes n$. If L is any left S-module, and $\phi : N \to L$ is an R-module homomorphism, then there exists a unique S-module homomorphism $\Phi : S \otimes_R N \to L$ for which $\phi = \Phi \circ \iota$. That is, the following diagram commutes.*

$$\begin{tikzcd} N \arrow[r, "\iota"] \arrow[dr, "\phi"'] & S \otimes_R N \arrow[d, "\Phi"] \\ & L \end{tikzcd}$$

Conversely, if $\Phi : S \otimes_R N \to L$ is an S-module homomorphism, then the map $\phi = \Phi \circ \iota$ is an R-module homomorphism.

Proof. Let $\phi : N \to L$ an R-module homomorphism. By the uiversal property of free modules, there exists a $\mathbb{Z}$-module homomorphism from the free $\mathbb{Z}$-module $F(S \times N)$ to L defined by $(s, n) \to s\phi(n)$. Since ϕ is an R-module homomorphism, the generators of $S \otimes_R N$, as a quotient group, map to 0 in L. Therefore, there exists a well define $\mathbb{Z}$-module homomorphism $\Phi : S \otimes_R N \to L$ taking $s \otimes n \to s\phi(n)$. Then for simple tensors, we get $s'\Phi(s \otimes n) = s'(s\phi(n)) = (s's)\phi(n) = \Phi(s'(s \otimes n))$ for all $s' \in S$. Since Φ is additive, we get an S-module homomorphism.

Now, $S \otimes_R N$, as an S-module, is generated by all $1 \otimes n$, and any S-module homomorphism is uniquely determined by its value on these elements. Now, observe that $\Phi(1 \otimes n) = 1\phi(n) = \phi(n)$, so $\phi = \Phi \circ \iota$ and Φ is uniquely determined by ϕ.

Now, if we have the map $\phi = \Phi \circ \iota$, where Φ is defined as above, and $\iota : n \to 1 \otimes n$, then since Φ is an S-module homomorphsm, and ι is an R-module homomorphism, then ϕ must be an R-module homomorphism. ■

Corollary. *$N/\ker \iota$ is the largest unique quotient of N that can be imbedded into any S-module. In particular, N can be imbedded as an R-module into some left S-module if, and only if ι is 1–1.*

Proof. We have that $N/\ker \iota$ is mapped into $S \otimes_R N$ injectively. Now, let ϕ be an 1–1 R-module taking $N/\ker \iota \to L$. Then $\ker \iota \to (0)$ by ϕ so that $\ker \iota \leq \ker \phi$. This makes $N/\ker \phi$ a quotient of $N/\ker \iota$. ■

Example 4.9. (1) Let N be an R-module, and take $\phi : N \to N, n \to n$. Then $R \otimes_R N \simeq R$ via this map. In particular, if A is any Abelian group, then $\mathbb{Z} \otimes_{\mathbb{Z}} A \simeq A$.

(2) Let A be a finite Abelian group of order n. THen $\mathbb{Q} \otimes_{\mathbb{Z}} A = (0)$. Observe that $1 \otimes 0 = 1 \otimes (0 + 0) = 1 \otimes 0 + 1 \otimes 0$, so that $1 \otimes 0 = 0$. Then for any $q \otimes a \in \mathbb{Q} \otimes_{\mathbb{Z}} A$, we have $q \otimes a = (\frac{q}{n} n) \otimes a = \frac{q}{n} \otimes na = \frac{q}{n} \otimes 0 = \frac{q}{n}(1 \otimes 0) = \frac{q}{n} 0 = 0$; since $na = 0$. Moreover, the map $\iota : A \to \mathbb{Q} \otimes_{\mathbb{Z}} A$ is the zero map, so that if $A \neq \langle 0 \rangle$, any map $\phi : \mathbb{Q} \to A$ is also the zeromap.

(3) Let R be a ring, and consider the free module R^n, of rank n. Then $S \otimes_R R^n \simeq S^n$, the free module over S of rank n. Then $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}^n \simeq \mathbb{Q}^n$. Moreover, observe that $\mathbb{Z}^n$ is a subgroup of $\mathbb{Q}^n$.

(4) Let K be a field, and F a subfield of K. Let V an n-dimensional vector space over F. Then $K \otimes_F V \simeq K^n$. We recall that $V \simeq F^n$.

(5) Let R be a commutative ring with identity, and G a finite group. Let $H \leq G$. For any RH-module N, we define the **induced module** $RG \otimes_{RH} N$ obtained as an extension of scalars from N as an RG-module.

Definition. Let R be a ring, and N a left R-module, and M a right R-module. THe quotient of the free $\mathbb{Z}$-module on $M \times N$ by the subgroup

$$H = \langle (m_1 + m_1, n) - (m_1, n) - (m_2, n), (m, n_1 + n_2) - (m, n_1) - (m, n_2), (mr, n) - (m, rn) \rangle$$

is called the **tensor product** of $M \times N$ over R, and denoted $M \otimes_R N$. We call the elements $m \times n$ **simple tensors**, and we call sums of simple tensors **tensors**.

Lemma 4.4.4. *Let R be a ring, and N and M left and right R-modules, respectively. Then the following relations hold.*

(1) $(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n.$

(2) $m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2.$

(3) $mr \otimes n = m \otimes rn.$

Proof. The proof is identical to that of lemma 4.4.1. ∎

Definition. Let R be a ring, and let M and N be right and left R-modules, respectively, and let L be an Abelian group. We call the map $\phi : M \times N \to L$ R**-balanced** or **middle linear** with resepct to R if for all $m_1, m_2 \in M$, and $n_1, n_2 \in N$, and $r \in R$

(1) $\phi(m_1 + m_2, n) = \phi(m_1, n) + \phi(m_2, n).$

(2) $\phi(m, n + 1 + n_2) = \phi(m, n_1) + \phi(m, n_2)$

(3) $\phi(mr, n) = \phi(m, rn).$

Lemma 4.4.5. *Let R be a ring, and M and N right, and left R-modules respectively. The map $\iota : M \times N \to M \otimes_R N$ defined by $\iota : (m, n) \to m \otimes n$ is R-balanced.*

Proof. This is by definition of the tensor product. ∎

Theorem 4.4.6. *Let R be a ring with identity, and M and N right and left modules, respectively. Let $\iota : M \times N \to M \otimes_R N$ the R-balanced map defined by $\iota : (m, n) \to m \otimes n$. Then the following are true.*

(1) If $\Phi : M \otimes_R N \to L$ is a group homomorphsm and L an Abelian group, then the map $\phi = \Phi \circ \iota$ is R-balanced from $M \times N \to L$.

(2) If L is an Abelian group, and $\phi : M \times N \to L$ is an R-balanced map, then there exists a unique group homomorphism $\Phi : M \otimes_R N \to L$ for wich $\phi = \Phi \circ \iota$.

Proof. We first have that if $\phi(m, n) = \Phi(m \otimes n)$, then $\phi(m_1 + m_2, n) = \Phi((m_1 + m_2) \otimes n) = \Phi(m_1 \otimes n) + \Phi(m_2 \otimes n) = \phi(m_1, n) + \phi(m_2, n)$. Similarly, the rest of the conditions for R-balanced maps hold for ϕ, making it R balanced.

Conversely by the universal propery, ϕ defines a unique $\mathbb{Z}$-module homomorphism $\tilde{\phi} : F(M \times N) \to L$ for wich $\tilde{\phi}(m, n) = \phi(m, n) \in L$. Now, if ϕ is R-balanced, then $\tilde{\phi}$ takes $(m, n) \to 0$, that is, we get $\tilde{\phi}((mr, n) - (m, rn)) = 0$. Then the subgroup H defined by

$$H = \langle (m_1 + m_1, n) - (m_1, n) - (m_2, n), (m, n_1 + n_2) - (m, n_1) - (m, n_2), (mr, n) - (m, rn) \rangle$$

is a subgroup of $\tilde{\phi}(F(M \times N))$. Then $\tilde{\phi}$ indues a homomorphism $\Phi : M \otimes_R N \to L$. By definition we have $\Phi(m \otimes n) = \tilde{\phi}(m, n) = \phi(m, n)$. ■

Corollary. *Let D be an Abelian group, and $\iota' : M \times N \to D$ such that*

(1) $\iota'(M \times N)$ generates D as a group.

(2) Every R-balanced map on $M \times N$ factors through ι'.

Then there exists an isomorphism $f : M \otimes_R N \to D$ with $\iota' = f \circ \iota$.

Proof. Since ι' is R-balanced, there is a unique group homomorphism $f : M \otimes_R N \to D$ such that $\iota' = f \circ \iota$. Then $\iota' = (f(m \otimes n))$. Since we also have that $D = \langle \iota'(M \times N) \rangle$, we get that f is onto. Since ι' is R-balanced, there exists a unique group homomorphism $g : D \to M \otimes_R N$ with $\iota = g \circ \iota'$. Then $m \otimes n = (g \circ f)(m \otimes n)$, and since every $m \otimes n$ generates $M \otimes_R N$, we get $g \circ f = i_D$ (the identity on D), so that f is 1–1. ■

Definition. Let R and S be rings with identity. An Abelian group M is caled an **(S, R)-bimodule** if M is a left S-module, a right R-module, and $s(mr) = (sm)r$ for all $s \in S$, $r \in R$, and $m \in M$.

Example 4.10. (1) Let S be a ring with identity and R a subring of S with $1_R = 1_S$. Then S is an (S, R)-bimodule by associativity in S. Now, if $f : R \to S$ is a ring homomorphism with $f(1_R) = 1_S$, then S is a right R-module under the action $sr = sf(r)$.

(2) Let I be an ideal of a ring R. The quotient ring ${}^{R}\!/\!{}_{I}$ is an $({}^{R}\!/\!{}_{I}, R)$-bimodule.

(3) Let R be a commutative ring (not necessarily with identity), then any R-module M is an (R, R)-bimodule, since $rm = mr$ for all $m \in M$ and $r \in R$. We call M the **standard R-module structure** over R.

(4) Let R and S be rings where $R \subseteq Z(S)$. Let M be a left S-module, then R is a commutative ring, and we have for all $s \in S$, $r \in R$, and $m \in M$ that $(sm)r = r(sm) = (sr)m = s(rm) = s(mr)$. So M can be considered as a right R-module. This makes M an (S, R)-bimodule under the right action of R.

Definition. Let R be a commutative ring with identity, and let M and N, and L be left R-modules. We call a map $\phi : M \times N \to L$ **R-bilinear** if it is R-linear in each factor. That is,

$$\begin{aligned} \phi(r_1m_1 + r_2m_2, n) &= r_1\phi(m_1, n) + r_2\phi(m_2, n) \\ \phi(m, r_1n_1 + r_2n_2) &= r_1\phi(m, n_1) + r_2\phi(m, n_2) \end{aligned}$$

for all $r_1, r_2 \in R$, $m_1, m_2, m \in M$, and $n_1, n_2, n \in N$.

Lemma 4.4.7. *Let R be a commutative ring, and let M and N be left R-modules. Let M have the standard R-module structure. Then $M \otimes_R N$ is a left R-module with*

$$r(m \otimes n) = rm \otimes n = m \otimes (rn)$$

Moreover, the map $\iota : (m, n) \to m \otimes n$ is R-bilinear.

Proof. Since M and N are left R-modules, and since M has an (R, R)-bimodule structure, the tensor product $M \otimes_R N$ is a left R-module. Moreover, notice that $\iota : (m, n) \to m \otimes n$ is additive in each factor since $r(m \otimes n) = rm \otimes n = mr \otimes n = m \otimes rn$. This makes ι a bilinear map. ■

Corollary. *There exists a 1–1 correspondence of R-bilinear maps from $M \times N \to L$ onto R-module homomorphisms from $M \otimes_R N \to L$ given by the following diagram*

$$\begin{tikzcd} M \times N \arrow[r, "\iota"] \arrow[dr, "\phi"'] & M \otimes_R N \arrow[d, "\Phi"] \\ & L \end{tikzcd}$$

Proof. If $\phi : M \times N \to L$ is bilinear, then it is R-balanced. So the corresponding map $\Phi : M \otimes_R N \to L$ is a group homomorphism. Notice now that

$$\Phi((rm) \otimes n) = \phi(rm, n) = r\phi(m, n) = r\Phi(m \otimes n)$$

Since Φ is additive, this makes Φ a ring homomorphism. Now, if Φ is an R-module homomorphism with $\phi = \Phi \circ \iota$, since ι is a bilenar map, it is easy to check that ϕ must also be bilinear. ■

Example 4.11. (1) In $M \otimes_R N$, $m \otimes 0 = m \otimes (0 + 0) = m \otimes 0 + m \otimes 0$, so $m \otimes 0 = 0$.

(2) Notice for any $a \in \mathbb{Z}/2\mathbb{Z}$, $3a = a$, so for every $b \in \mathbb{Z}/3\mathbb{Z}$, $a \otimes b = 3a \otimes b = a \otimes 3b = a \otimes 0 = 0$. This shows that every simple tensor in $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z}$ reduces to 0. In particular, $1 \otimes 1 = 0$. Thus there are no nonzero bilinear maps mapping $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z}$ onto any Abelian group.

(3) Consider $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$. This tensor product is generated by $0 \otimes 0 = 1 \otimes 0 = 0 \otimes 1 = 0$, and $1 \otimes 1$. The map

$$\begin{aligned} \mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} &\to \mathbb{Z}/2\mathbb{Z} \\ a \otimes b &\to ab \mod 2 \end{aligned}$$

is a nonzero and bilenear map. Moreover, notice that $2(1 \otimes 1) = 0$, so that $\operatorname{ord}(1 \otimes 1) = 2$. That is

$$\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z}$$

(4) In general, whenever $m, n \in \mathbb{Z}^+$ have greatest common divisor d, then

$$\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/d\mathbb{Z}$$

Moreover, observe that $a \otimes b = ab(1 \otimes 1)$, so that

$$\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} = \langle 1 \otimes 1 \rangle$$

making it cyclic. Moreover, $\operatorname{ord} \langle 1 \otimes 1 \rangle | d$.

Now, the map

$$\begin{aligned} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} &\to \mathbb{Z}/d\mathbb{Z} \\ a \times b &\to ab \mod d \end{aligned}$$

is well defined since $d = (m, n)$. Moreover, ϕ is a $\mathbb{Z}$-bilinear map. Now, the induced map $\Phi : \mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ maps $1 \otimes 1 \to 1 \mod d$, so that $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z}$ has order atleast d. Since $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$ is cyclic and has order dividing d, by Lagrange's theorem its order is preciesly d. This proves the isomorphims.

(5) In $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z}$, the simple tensors have the form

$$\frac{a}{b} \mod \mathbb{Z} \otimes \frac{c}{d} \mod \mathbb{Z}$$

Then

$$\frac{a}{b} \otimes \frac{c}{d} = d(\frac{a}{bd}) \otimes \frac{c}{d} = \frac{a}{bd} \otimes d(\frac{c}{d}) = \frac{a}{bd} \otimes c = \frac{a}{bd} \otimes 0 = 0$$

so that $\mathbb{Q}/\mathbb{Z} \otimes \mathbb{Q}/\mathbb{Z} = (0)$. Similarly, $A \otimes_{\mathbb{Z}} B = (0)$ for any divisible Abelian group A, and any torsion Abelian group B.

(6) We have $\mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{Q} \simeq \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$ as left $\mathbb{Q}$-modules, and $\mathbb{C} \otimes_{\mathbb{C}} \mathbb{C} \simeq \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ as left $\mathbb{C}$-modules.

(7) Let $f : R \to S$ be a ring homomorphism with $f(1_R) = 1_S$. Then the action $(s, r) \to sf(r)$ gives S the right R-module structure so that S is an (S, R)-bimodule. Then for any left R-module N, the tensor product $S \otimes_R N$ is a left R-module obtained by **changing the base** from R to S.

(8) Let $f : R \to S$ a ring homomorphism with $f(1_R) = 1_S$, then $S \otimes_R R \simeq S$ as a left S-module. Consider now $\phi : S \times R \to S$ by $(s, r) \to sr$. Then ϕ is R-balanced and

$$\begin{aligned} \phi(s_1 + s_2, r) &= \phi(s_1, r) + \phi(s_2, r) \\ \phi(sr, r') &= \phi(s, rr') \end{aligned}$$

Now, there exists a group homomorphism $\Phi : S \otimes_R R \to S$ with $\Phi(s \otimes r) = sr$, since

$$\Phi(s'(s \otimes r)) = \Phi(ss' \otimes r) = (ss')r = (s's)r = s'(sr) = s'\Phi(s \otimes r)$$

then Φ is also an S-module homomorphism. Now, take the map $\Phi' : S \to S \otimes_R R$ by $s \to s \otimes 1$. THis map gives an inverse to Φ, since $\Phi \circ \Phi'(s) = \Phi(s \otimes 1) = s$ and $\Phi' \circ \Phi(s \otimes r) = \Phi'(sr) = sr \otimes 1 = sr$. So that $\Phi' \circ \Phi = \Phi \circ \Phi' = i$, the identity map.

(9) Let R be a ring and I an ideal in R. Let N be a left R module, since R/I is an $(R/I, R)$-bimodule, $R/I \otimes_R N$ is a left R/I module. Define now

$$IN = \left\{ \sum a_i n_i : a_i \in I, n_i \in N \right\}$$

where the sums taken are finite. Then

$$R/I \otimes_R N \simeq N/IN$$

Moreover, it is generated, as an Abelian group by the simple tensors of the form

$$(r \mod I) \otimes n = r(1 \otimes n)$$

That is, $1 \otimes n$ generates $R/I \otimes_R N$ as an R/I-module for every $n \in N$.

Now, the map $n \to 1 \otimes n$, takes $a_i n_i \to 1 \otimes a_i n_i = a_i \otimes n_i = 0$, so that IN is in the kernel of this map. Thus, we have an R-module homomorphism f from N/IN onto $R/I \otimes_R N$ with $f(n) = 1 \otimes n$. Then the map

$$\begin{aligned} R/I \times N &\to R/I \otimes_R N \\ (r, n) &\to rn \mod IN \end{aligned}$$

is a well defined R-balanced map. There there exists a group homomorphism $g : R/I \times_R N \to N/IN$ with $g(r \otimes n) = rn \mod IN$. Then $fg = gf = i$, wich makes f 1–1. Therefore

$$N/IN \simeq R/I \otimes_R N$$

Theorem 4.4.8. *Let R be a ring, and let M, M' be right R-modules, and let N, N' be left R modules, and suppose that $\phi : M \to M'$ and $\psi : N \to N'$ are R-module homomorphisms. Then the following are true.*

(1) There exists a unique group homomorphism $\phi \otimes \psi : M \otimes_R N \to M' \otimes_R N'$ such that for all $m \in M$ and $n \in N$

$$\phi \otimes \psi(m \otimes n) = \phi(m) \otimes \psi(n)$$

(2) If M and M' are (S, R)-bimodules, for a given ring S, and ϕ is also an S-module homomorphism, then $\phi \otimes \psi$ is a homomorphism of left S-modules. In particular, if R is commutative, then $\phi \otimes \psi$ is an R-module homomorphism for (R, R)-bimodules.

(3) If $\lambda : M' \to M''$ and $\mu : N' \to N''$ are R-module homomorphisms, then

$$(\lambda \otimes \mu) \circ (\phi \otimes \psi) = (\lambda \circ \phi) \otimes (\mu \circ \psi)$$

Proof. Consider the map $(m, n) \to \phi(m) \otimes \psi(n)$ from $M \times N \to M' \otimes_R N'$. Since ϕ and ψ are R-module homomorphisms, this map is R-balanced, and so by theorem 4.4.6, assertion (1) follows.

Now, for assertion (2), notice that the left action of S on M and ϕ being an S-module homomorphism gives $\phi \otimes \psi(s(m \otimes n)) = s\phi(n) \otimes \psi()$. Since $\phi \otimes \psi$ is additive, we get that $\phi \otimes \psi$ is an S-module homomorphism. Finally, for assetion (3), the uniqueness condition of theorem 4.4.6 gives us the result. ■

Theorem 4.4.9. *Let R, and T be rings, and let M a right R-module, let N be an (R, T)-bimodule, and let L be a left T module. Then there exists a unique isomorphsim of Abelian groups, taking $(m \otimes n) \otimes l \to m \otimes (n \otimes l)$, for which*

$$(M \otimes_R N) \otimes_T L \simeq M \otimes_R (N \otimes_T L)$$

Moreover, if M is an (S, R)-bimodule for some ring S, then we have an isomorphism of S-modules.

Proof. The (R, T)-bimodule structure of N makes $M \otimes_R N$ into a right T-module, and $N \otimes_T L$ into a left R-module. Thus the isomorphism is well defined. Now, for every $l \in L$, fixed, the map $(m, n) \to m \otimes (n \otimes l)$ is R-balanced, and hence, there is a homomorphism

$$\begin{array}{rcl} M \otimes_R N & \to & M \otimes_R (N \otimes_T L) \\ (m, n) & \to & m \otimes (n \otimes l) \end{array}$$

That is, we have a map

$$\begin{array}{rcl} (M \otimes_R N) \times L & \to & M \otimes_R (N \otimes_T L) \\ (m \otimes n, l) & \to & m \otimes (n \otimes l) \end{array}$$

which is also well defined. Moreover it is T-balanced, and so induces a homomorphism

$$\begin{array}{rcl} (M \otimes_R N) \otimes_T L & \to & M \otimes_R (N \otimes_T L) \\ (m \otimes n) \otimes l & \to & m \otimes (n \otimes l) \end{array}$$

By similar reasoning, we can construct the inverse of this map and establish the isomorphism.

Now, suppose that M is an (S, R)-bimodule. THen for $s \in S$, and $t \in T$, we have

$$s((m \otimes n)t) = (s(m \otimes n))t$$

so $M \otimes_R N$ is an (S, T)-bimodule. This makes $(M \otimes_R N) \otimes_T L$ into a left S-module. Since $N_T L$ is a left R-module, then $M \otimes_R (N \otimes_T L)$ is a left S-module, and the group isomorphism follows to be a homomorphism of S-modules. ■

Corollary. *If R is commutative, and M, N, and L are R-modules, then $(M \otimes N) \otimes L = M \otimes (N \otimes L)$ as (R, R)-bimodules.*

Definition. Let R be a commutative ring with identity, and let $M_1, \ldots, M_n$, and L be R-modules with the standard R-module structure. A map $\phi : M_1 \times \cdots \times M_n \to L$ is called n**-multilinear** over R if it is an R-module homomorphism in each factor.

Lemma 4.4.10. *Let R be a commutative ring, and let $M_1, \ldots, M_n$, L be R-modules. Let $\iota : M_1 \times \cdots \times M_n \to M_1 \otimes \cdots \otimes M_n$ be defined by $(m_1, \ldots, m_n) \to m_1 \otimes \cdots \otimes m_n$. The following are true.*

(1) For every R-moduel homomorphism $\Phi : M_1 \otimes \cdots \otimes M_n \to L$, the map $\phi = \Phi \circ \iota$ is n-multilinear.

(2) If $\phi : M_1 \times \cdots \times M_1 \to L$ is n-multilinear, then there exists a unique R-module homomorphism $\Phi : M_1 \otimes \cdots \otimes M_n \to L$ for wich $\phi = \Phi \circ \iota$.

Theorem 4.4.11. *Let R be a ring, and M and M' be right R-modules, and let N and N' be left R-modules. Then there exists unique group isomorphisms for which*

$$\begin{aligned}(M \oplus M') \otimes_R N &\simeq (M \otimes_R N) \oplus (M' \otimes_R N)\\ M \otimes_R (N \oplus N') &\simeq (M \otimes_R N) \oplus (M \otimes_R N')\end{aligned}$$

such that $(m, m') \otimes n \to (m \otimes n, m' \otimes n)$ and $m \otimes (n, n') \to (m \otimes n, m \otimes n')$. If M and M' are (S, R)-bimodules, then the isomorphisms are isomorphism of S-modules. If R is commutative, then we have an isomorphism of R-modules.

Proof. The map $(M \oplus M') \times N \to (M \otimes_R N) \oplus (M' \otimes_R N)$ defined by $((m, m'), n) \to (m \otimes n, m' \otimes n)$ is well define. Moreover, it is R-balanced, and hence induces a homomorphism $f : (M \oplus M') \otimes_R N \to (M \otimes_R N) \oplus (M' \otimes N)$ for which $f((m, m'), n) = (m \otimes n, m' \otimes n)$. Consider now the R-balanced maps

$$\begin{aligned}M \times N &\to (M \oplus M') \otimes_R N\\ M' \times N &\to (M \oplus M') \otimes_R N\end{aligned}$$

given by

$$\begin{array}{rcl}(m,n) & \to & (m,0)\otimes n\\ (m',n) & \to & (0,m')\otimes n\end{array}$$

Define now homomorphisms $M\otimes_R N\to(M\oplus M')\otimes_R N$ and $M'\otimes_R N\to(M\oplus M')\otimes_R N$. Then we get a homomorphism $g:(M\otimes_R N)\oplus(M'\otimes_R N)\to(M\oplus M')\otimes_R N$ with

$$g((m\otimes n_1, m'\otimes n_2)) = (m,0)\otimes n_1 + (0,m')\otimes n_2$$

Then $fg = gf$, the identity map, and are S-module homomorphisms when M and M' are (S,R)-bimodules. By similar reasoning, we get the same results for the isomorphism $M\otimes_R(N\oplus N')\simeq(M\otimes_R N)\oplus(M\otimes_R N')$ ■

Corollary. $M\otimes_R\bigoplus N_i\simeq\bigoplus(M\otimes_R N_i)$.

Corollary. *The module obtained from the free R-module R^n by extension of scalars from R to S is the free S-module S^n.*

Corollary. *If R is commutative, and $M\simeq R^s$, and $N\simeq R^t$, the free R-modules with bases $\{m_1,\dots,m_s\}$ and $\{n_1,\dots,n_t\}$, respectively, then $M\otimes_R N$ is a free R-module of rank st with basis $\{m_i\otimes n_j\}$ for all $1\le i\le s$ and $1\le j\le t$.*

Lemma 4.4.12. *Let R be a commutative ring, and M and N left R-modules, considered as (R,R)-bimodules. Then there exists a unique R-module isomorphism, taking $m\otimes n\to n\otimes m$ for which*

$$M\otimes_R N\simeq N\otimes_R M$$

Proof. The map $M\times N\to N\otimes M$ defined by $(m,n)\to n\otimes m$ is R-balanced, and so induces a unique homomorphism $f:M\otimes N\to N\otimes M$ by $m\otimes n\to n\otimes m$. Likewise, there exists a unique homomorphism $f:N\otimes M\to M\otimes N$ by $n\otimes m\to m\otimes n$, and $fg=gf=i$, the identity map. ■

Lemma 4.4.13. *Let R be a commutative ring, and A and B R-algebras. Then teh multiplication*

$$(a\otimes b)(a'\otimes b) = aa'\otimes bb'$$

is well defined, and makes $A\otimes_R B$ into an R-algebra.

Proof. Notice that by definition, $r(a\otimes b)=ra\otimes b=a\otimes br=(a\otimes b)r$ for every $r\in R$, $a\in A$, and $b\in B$. Now, the map $\phi:(A\times B)\times(A\times B)\to A\otimes_R B$ defined by $(a,b,a',b')\to aa'\otimes bb'$ is multilinear over R. Then there exists an R-module homomorphism $\Phi:(A\otimes_R B)\otimes_R(A\otimes_R B)\to A\otimes_R B$ taking $(a\otimes b)\otimes(a'\otimes b')\to aa'\otimes bb'$. This gives us a bilinear map $\Phi:(A\otimes_R B)\otimes_R(A\otimes_R B)\to A\otimes_R B$ defined by $(a\otimes b, a'\otimes b')\to aa'\otimes bb'$. This makes multiplication well defined. Moreover, this multiplication satisfies the distributive laws, so that $A\otimes_R B$ is an R-algebra. ■

Example 4.12. The tensor product $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C} \simeq \mathbb{C}^4$ is a free $\mathbb{R}$-module of rank 4, with the basis $\{1\otimes 1, 1\otimes i, i\otimes 1, i\otimes i\}$, where $i^2+1=0$. Moreover, this tensor product is a commutative ring. Notice then that $(i\otimes i)(i\otimes i) = i^2\otimes i^2 = -1\otimes -1 = (-1)(-1)\otimes 1 = 1$ Then we have $(i\otimes i)(i\otimes i+1) = 0$ so that $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C}$ is not an integral domain. Now, notce also that $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C}$ is an $\mathbb{R}$-algebra whose left and right actions are the same. Then $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C}$ is a left $\mathbb{C}$-module, since $\mathbb{C}$ is a $(\mathbb{C},\mathbb{R})$-bimodule. Likewise, $\mathbb{C}\otimes_{\mathbb{R}}\mathbb{C}$ is aright $\mathbb{C}$ module.

4.5 Exact Sequences of Modules

Definition. Let A and C be modules. We call a module B, containing A an **extension** of C by A if ${}^{B}\!/_{A} \simeq C$.

Example 4.13. Let A, B, and C be modules. If A is a submodule of B, then there exists a map 1–1 $\psi : A \to B$ such that $A \simeq \psi(A) \subseteq B$. If ${}^{B}\!/_{\psi(A)} \simeq C$, then there exists a map $\phi : B \to C$ wich is onto, for which $\ker\phi = \psi(A)$. Then we get the following diagram.

$$A \xrightarrow{\psi} B \xrightarrow{\phi} C$$

Definition. Let $\{A_n\}$ a collection of modules. By a **sequence**, we mean a diagram

$$\ldots \to A_{n-1} \to A_n \to A_{n+1} \to \ldots$$

where each A_i is mapped to A_{i+1} by some module homomorphism.

Definition. Let A, B, and C be modules. We call a pair of module homomorphisms α, β, defined by the diagram

$$A \xrightarrow{\alpha} B \xrightarrow{\beta} C$$

exact at B if $\alpha(A) = \ker\beta$. If $\{A_n\}$ is a collection of modules, we call a sequence defined by the diagram

$$\ldots \to A_{n-1} \to A_n \to A_{n+1} \to \ldots$$

an **exact sequence** if it is exact at each A_n.

Example 4.14. The sequence from example 4.13, $A \xrightarrow{\psi} B \xrightarrow{\phi} C$, is exact at B, since $\ker\phi = \psi(A)$.

Lemma 4.5.1. *Let R be a ring, and A, B, and C R-modules. The following are true for any R-module homomorphisms $\psi : A \to B$ and $\psi : B \to C$*

(1) $(0) \xrightarrow{\iota} A \xrightarrow{\psi} B$ *is exact at A if, and only if ψ is 1–1.*

(2) $B \xrightarrow{\phi} C \xrightarrow{\iota'} (0)$ *is exact at B if, and only if ϕ is onto.*

Corollary. *The sequence $(0) \to A \xrightarrow{\psi} B \xrightarrow{\phi} C \to (0)$ is an exact sequence if, and only if ψ is 1–1, ϕ is onto, and $\ker\phi = \psi(A)$; that is, B is an extension of C by A.*

Definition. We call an exact sequence of the form $(0) \to A \xrightarrow{\psi} B \xrightarrow{\phi} C \to (0)$ a **short exact sequence**.

Lemma 4.5.2. *If $A \xrightarrow{\alpha} B \xrightarrow{\beta} C$ is exact at Y, then $(0) \to \alpha(A) \to B \to B/_{\ker\beta} \to (0)$ is a short exact sequence.*

Example 4.15. (1) Let A, and C be modules. Consider the sequence

$$(0) \to A \xrightarrow{\iota} A \oplus C \xrightarrow{\pi} C \to (0)$$

where ι is the inclusion map, and π is the projection map about the second coordinate; i.e. $\pi : (a, c) \to c$. This sequence is a short exact sequence, since $\iota(A) = \ker\pi$.

(2) Consider the $\mathbb{Z}$-modules $\mathbb{Z}$ and $\mathbb{Z}/_{n\mathbb{Z}}$, the sequence

$$(0) \to \mathbb{Z} \xrightarrow{\iota} \mathbb{Z} \oplus \mathbb{Z}/_{n\mathbb{Z}} \xrightarrow{\phi} \mathbb{Z}/_{n\mathbb{Z}} \to (0)$$

is a short exact sequence giving an extension of $\mathbb{Z}/_{n\mathbb{Z}}$ by $\mathbb{Z}$. Another extension is given by the short exact sequence

$$(0) \to \mathbb{Z} \xrightarrow{\eta} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/_{n\mathbb{Z}} \to (0)$$

where $n : x \to nx$, and $\pi : x \to x \mod n$ is the natural map. THese are "inequivalent" extensions of $\mathbb{Z}/_{n\mathbb{Z}}$ by $\mathbb{Z}$.

(3) If $\phi : B \to C$ is any module homomorphism, form the exact sequence

$$(0) \to \ker\phi \xrightarrow{\iota} B \xrightarrow{\phi} \phi(B) \to (0)$$

where ι is the inclusion map. If ϕ is onto, we may extend the sequence $B \xrightarrow{\phi} C$ (i.e. extend ϕ) to a short exact sequence with $A = \ker\phi$.

(4) Let R be a ring, and M an R-module homomorphism. Let S be a set of generators for M, and consider the free R-module $F(S)$ on S. Then

$$(0) \to K \xrightarrow{\iota} F(S) \overset{\phi}{\twoheadrightarrow} M \to (0)$$

is a short exact sequence, where ϕ is the unique R-module homomorphism which is the identity on S, and $K = \ker\phi$.

Definition. Let $(0) \to A \to B \to C \to (0)$ and $(0) \to A' \to B' \to C' \to (0)$ be short exact sequences. A **homomorphism** of sequences is a triple (α, β, γ) of module homomorphisms, such that the following diagram commutes

$$\begin{tikzcd}
(0) \arrow[r] & A \arrow[r] \arrow[d, "\alpha"] & B \arrow[r] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & (0) \\
(0) \arrow[r] & A' \arrow[r] & B' \arrow[r] & C' \arrow[r] & (0)
\end{tikzcd}$$

If α, β, and γ are module isomorphisms, we call (α, β, γ) an isomorphism of sequences.

Definition. We call two exact sequences $A \to B \to C$ and $A' \to C' \to B'$ **equivalent** if $A = A'$, $C = C'$, and there exists an isomorphism of sequences between them. We call the corresponding extensions B and B' **equivalent**.

Lemma 4.5.3. *The composition of homomorphisms of exact sequences is a homomorphism of sequences.*

Lemma 4.5.4. *Isomorphisms of exact sequences form an equivalence relation on any set of exact sequences.*

Example 4.16. (1) Let $m, n \in \mathbb{Z}^+$ integers greater than 1, and suppose that $n|m$. Let $k = \frac{m}{n}$, and define a map from the exact sequences of $\mathbb{Z}$-modules described by the following diagram

$$\begin{tikzcd}
(0) \arrow[r] & \mathbb{Z} \arrow[r, "n"] \arrow[d, "\alpha"'] & \mathbb{Z} \arrow[r, "\pi"] \arrow[d, "\beta"'] & \mathbb{Z}/n\mathbb{Z} \arrow[r] \arrow[d, "\gamma"'] & (0) \\
(0) \arrow[r] & \mathbb{Z}/k\mathbb{Z} \arrow[r, "\iota"] & \mathbb{Z}/k\mathbb{Z} \arrow[r, "\pi'"] & \mathbb{Z}/n\mathbb{Z} \arrow[r] & (0)
\end{tikzcd}$$

where $n : x \to nx$, $\pi : x \to x \mod n$, α, β are the natural projections, and γ is the identity. For the second sequnece, we take $\iota : a \mod k \to na \mod m$, and π' the natural projection of $\mathbb{Z}/m\mathbb{Z}$ onto $(\mathbb{Z}/m\mathbb{Z})/(n\mathbb{Z}/m\mathbb{Z}) \mathbb{Z}/n\mathbb{Z}$. Then (α, β, γ) describe a homorphism of short exact sequences.

(2) If $(0) \to \mathbb{Z} \xrightarrow{n} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/n\mathbb{Z} \to (0)$ is the short exact sequence defined in example 4.15, mapping each module to itself via the map $x \to -x$ gives a isomorphism of short exact sequences, which take this sequence onto itself. Notice however that this isomorphism is not an equeivalence, since it is not the identity on $\mathbb{Z}$.

(3) Consider the diagram

$$\begin{tikzcd}
(0) \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r, "\psi"] \arrow[d, "i"'] & \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \arrow[r, "\phi"] \arrow[d, "\beta"'] & \mathbb{Z}/2\mathbb{Z} \arrow[r] \arrow[d, "i"'] & (0) \\
(0) \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r, "\psi'"'] & \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \arrow[r, "\phi'"'] & \mathbb{Z}/2\mathbb{Z} \arrow[r] & (0)
\end{tikzcd}$$

Where i is the identity map, ψ is a 1–1 map mapping into the first component of $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, and ϕ projects $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ onto its second component, and where ψ' and ϕ' behave just as ψ and ϕ. If β maps $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ by exchanging the factors; that is $\beta : (m, n) \to (n, m)$, then this diagram commutes and gives an equivalence of short exact sequences which is not the identity.

Lemma 4.5.5 (The Short Five Lemma)**.** *Let (α, β, γ) be a homomorphism of short exact sequences given by the diagram*

$$\begin{tikzcd}
(0) \arrow[r] & A \arrow[r] \arrow[d, "\alpha"'] & B \arrow[r] \arrow[d, "\beta"'] & C \arrow[r] \arrow[d, "\gamma"'] & (0) \\
(0) \arrow[r] & A' \arrow[r] & B' \arrow[r] & C' \arrow[r] & (0)
\end{tikzcd}$$

then the following are true

(1) If α and γ are 1–1, then so is β.

(2) If α and γ are onto, then so is β.

(3) If α and γ are isomorphisms, then so is β.

Proof. We chase the elements of the following diagram.

$$\begin{tikzcd}
(0) \arrow[r] & A \arrow[r, "\psi"] \arrow[d, "\alpha"'] & B \arrow[r, "\phi"] \arrow[d, "\beta"'] & C \arrow[r] \arrow[d, "\gamma"'] & (0) \\
(0) \arrow[r] & A' \arrow[r, "\psi'"'] & B' \arrow[r, "\phi'"] & C' \arrow[r] & (0)
\end{tikzcd}$$

Suppose that α and γ are 1–1, and choose an element $b \in \ker \beta$. Then $\beta(b) = 0$, and $\phi'\beta(b) = 0$. Moreover, since this diagram commutes, we have that $\phi'\beta = \gamma\phi$, so that $\phi'\beta(b) = \gamma\phi(b)$, which implies that $\phi(b) = 0$, since γ is 1–1. This makes $b \in \ker \phi$. Now, since the sequences are also exact, we have $\ker \phi = \psi(A)$, so that $b \in \psi(A)$. That is, there is an $a \in A$ for wich $b = \psi(a)$. Now, by commutativity again, we have $\beta\psi = \psi'\alpha$. So $\beta\psi(b) = \beta(b) = 0$, which makes $\psi'\alpha(a) = 0$, so that $\alpha(a) = 0$. Since α is 1–1, this makes $a = 0$ and we get $b = \psi(a) = 0$ which makes $\ker \beta = (0)$. That is, β is 1–1.

Now, suppose that α and γ are onto, and let $b' \in B'$. Then $\phi'(b) = \gamma(c)$ for some $c \in C$; since γ is onto. Now, by lemma 4.5.1 ϕ is onto, so there is a $b \in B$ for which $b = \gamma(c)$. By the commutativity of the diagram $\phi'\beta(b) = \gamma(\phi(b)) = \gamma(c) = \phi'(b')$, so $\phi'(b' - \beta(b)) = 0$ which puts $b' - \beta(b) \in \ker \phi'$. Now, by the exactness of the sequences, $\ker \phi' = \psi'(A')$, so there is an $a' \in A'$ for which $b' - \beta(b) = \psi'(a) = a \in A$, since α is onto. Then $a \in \ker \phi'$. Now, by commutativity, observe that $\psi(a) = \psi(b' - \beta(b)) = 0$, and since ψ is 1–1, we get $b' - \beta(b) = 0$. That is $b' = \beta(b)$ and $\beta(B) = B'$, which makes β onto. Lastly, observe that if α and γ are isomorphisms, then they are 1–1 and onto, which makes β 1–1 and onto, and hence an isomorphism as well. ■

Bibliography

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

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