

Math 220B: Modern Algebra

Simon Rubinstein-Salzedo

March 11, 2004

0.1 Introduction

Professor: Adebisi Agboola

Office Hours: Tuesday: 11:15-12:30, Wednesday: 11:15-12:30, Thursday: 11:15-12:30.

Chapter 1

Rings

Definition 1.1 A **ring** $(R, +, \cdot)$ is an abelian group $(R, +)$ (with identity element 0) together with a function $m : R \times R \rightarrow R$ (we usually write $r_1 \cdot r_2$ for $m(r_1, r_2)$) such that

1. $\forall r_1, r_2, r_3 \in R, r_1(r_2r_3) = (r_1r_2)r_3$ (Multiplication is associative.)
2. $\forall r_1, r_2, r_3 \in R, r_1(r_2 + r_3) = r_1r_2 + r_1r_3$ and $(r_2 + r_3)r_1 = r_2r_1 + r_3r_1$.
3. \exists an element $1 \in R$ such that $\forall r \in R, r \cdot 1 = 1 \cdot r = r$. (Trivially, 1 is unique.)

Note

1. Multiplication is not required to be commutative, nor do multiplicative inverses necessarily exist.
2. The above definition (including (3)) defines a “ring with a 1.” Some authors omit (3) from the definition of a ring. Usually for us, all rings contain 1.

Examples

1. The **trivial ring** $\{0\}$.
2. The integers \mathbb{Z} with standard addition and multiplication.
3. Real $n \times n$ matrices under matrix addition and multiplication (noncommutative if $n \geq 2$).
4. $\mathbb{R}, \mathbb{Q}, \mathbb{C}$ are all rings. They are commutative, and all nonzero elements have multiplicative inverses, i.e. they are fields.
5. $\mathbb{Z}/n\mathbb{Z}$, the integers modulo n ($n \geq 1$) under addition and multiplication modulo n . This is a commutative ring. The existence of inverses depends on whether or not n is prime.
6. $\mathbb{Z}[x]$, polynomial ring in one variable over \mathbb{Z} .
7. Let G be an abelian group and $r = \{\text{all homomorphisms } G \rightarrow G\}$. Define $(\phi + \theta)(g) = \phi(g) + \theta(g) \forall \theta, \phi \in R, g \in G$. $(\theta\phi)(g) = \theta(\phi(g))$. “1” is the identity morphism.

Exercise Check that R is a ring, which in general is noncommutative.

8. Let A be any set, and let R be the collection of all subsets of A . Define $E+F = (E \cup F) - (E \cap F)$ $\forall E, F \in R$ and $E \cdot F = E \cap F$.

Exercise Show that R is a commutative ring.

Definition 1.2 Let R and S be rings. A **ring homomorphism** $f : R \rightarrow S$ is a map such that

1. $f(x + y) = f(x) + f(y) \forall x, y \in R$.
2. $f(xy) = f(x)f(y)$.
3. $f(1) = 1$.

Definition 1.3 A subset S of a ring R is a **subring** of R if S is closed under addition and multiplication and contains $1 \in R$.

Definition 1.4

1. A **left ideal** I of a ring R is a subset of R which is an additive subgroup and which is such that $RI \subseteq I$ (i.e. $r \in R, x \in I$ implies that $rx \in I$). Right ideals are defined similarly. An **ideal** is a two-sided ideal.
2. Suppose that I is a two-sided ideal of R . The quotient group R/I inherits a (uniquely defined) multiplication from R which makes it into a ring. This ring is called the **quotient ring** or **residue class ring** R/I . Elements of R/I are the cosets of I in R . The map

$$\begin{aligned} \phi : R &\rightarrow R/I \\ r &\mapsto r + I \end{aligned}$$

is a surjective ring homomorphism.

Fact There is a one-to-one, order-preserving correspondence between the ideals J of R which contain I and the ideals \bar{J} of R/I given by $J = \phi^{-1}(\bar{J})$ (Exercise).

3. If $f : R \rightarrow S$ is any ring homomorphism, the **kernel** of f ($= f^{-1}(0)$) is an ideal of R , and the image $f(R)$ of f is a subring of S . f induces a ring isomorphism

$$R/\ker(f) \simeq f(R).$$

4. The notation $x \equiv y \pmod{I}$ means $x - y \in I$.

Definition 1.5

1. A **zero divisor** of a ring R is an element x for which $\exists y \in R$ such that $y \neq 0$ and $xy = 0$ or $yx = 0$.
2. A commutative ring with no nonzero zero divisors is called an **integral domain**, e.g. \mathbb{Z} or $k[x_1, x_2, \dots, x_n]$ (k a field).

3. An element $r \in R$ is **nilpotent** if $r^n = 0$ for some $n > 0$. A nilpotent element is a zero divisor, but the converse is not true in general.
4. A **unit** in R is an element $r \in R$ that has both a left and a right multiplicative inverse, i.e. $\exists x \in R$ such that $rx = xr = 1$. The units form a multiplicative group.
5. The multiples rx of an element $x \in R$ form a **principal (left) ideal** denoted by Rx . x is a unit iff $Rx = R = R \cdot 1$. If R is commutative, then we write (x) for $Rx = xR$.
6. A **field** is a nonzero commutative ring R in which every nonzero element is a unit. So every field is an integral domain, but the converse is not necessarily true, e.g. \mathbb{Z} .

Proposition 1.6 Suppose that R is a nonzero commutative ring. Then the following statements are equivalent:

1. R is a field.
2. The only ideals in R are (0) and (1) .
3. Every homomorphism of R into a nonzero ring S is injective.

Proof First we show that (1) implies (2). Suppose that $I \neq (0)$ is an ideal in R . Then I contains a nonzero element x . x is a unit, so $I \supseteq (x) = (1)$. So $I = (1)$. Now we show that (2) implies (3). Let $\varphi : R \rightarrow S$ be a ring homomorphism. Then $\ker \varphi = (0)$, i.e. φ is injective. Finally we show that (3) implies (1). Suppose $x \in R$ is not a unit. Then $(x) \neq (1)$, and so $S = R/(x)$ is not the zero ring. Let $\varphi : R \rightarrow R/(x)$ be the natural map. Then $\ker \varphi = (x)$. By hypothesis, φ is injective, so $(x) = (0)$, and hence $x = 0$.

Definition 1.7

1. An ideal I in a ring R is a **prime ideal** if $rs \in I$ implies either r or s is in I (e.g. in \mathbb{Z} , the ideal (n) is prime iff n is prime).
2. An ideal I in a ring R is **maximal** if
 - (a) $I \neq R$
 - (b) If J is any ideal with $I \subseteq J \subseteq R$, then $J = I$ or $J = R$.

Theorem 1.8 R/I has no nonzero zero divisors iff I is prime.

Proof Suppose that R/I has no nonzero zero divisors. If $rs \in I$, then (in R/I) $(r+I)(s+I) = 0$. So $r+I = 0$ or $s+I = 0$, whence $r \in I$ or $s \in I$. Conversely, suppose that I is prime. If $(r+I)(s+I) = 0$ (in R/I), then $rs \in I$. Hence $r \in I$ or $s \in I$, and so either $r+I = 0$ or $s+I = 0$.

Corollary 1.9 If R is commutative, then R/I is an integral domain iff I is a prime ideal.

Theorem 1.10 R/I is simple (i.e. has no proper ideals) iff I is maximal (or $I = R$).

Proof Suppose that $I \neq R$ since the case $I = R$ is trivial. Suppose that R/I is simple, and $I \subseteq J \subseteq R$. Consider the quotient homomorphism $\theta : R \rightarrow R/I$. Applying θ to the chain $I \subseteq J \subseteq R$ gives $\{0\} \subseteq \theta(J) \subseteq R/I$. Now $\theta(J)$ is an ideal of R/I , so either $\theta(J) = \{0\}$ or $\theta(J) = R/I$ since R/I is simple. So either $J = I$ or $J = R$, whence I is maximal. Conversely, suppose that I is maximal. If J is a proper ideal of R/I , then $\theta^{-1}(J)$ is an ideal of R , and $I \subsetneq \theta^{-1}(J) \subsetneq R$. These are proper inclusions, so I is not maximal, which is a contradiction.

Corollary 1.11 If R/I is a division ring, then I is maximal.

Corollary 1.12 If R is a commutative ring, then I is a maximal ideal, which implies that I is prime.

Proof I is maximal implies that R/I is a field, which implies that R/I is an integral domain, which implies that I is prime.

Remarks

1. In the ring R of $n \times n$ matrices ($n \geq 2$) over the real numbers, the ideal $\{0\}$ is maximal but not prime (since R is simple (Exercise)). So the commutability hypothesis is essential in Corollary 1.12.
2. Let $R = \mathbb{Z}[x]$, $I = \{\text{polynomials with constant coefficient } 0\}$. Then I is an ideal, and I is prime since e.g. $\mathbb{Z}[x]/I \simeq \mathbb{Z}$ (prove this!), and \mathbb{Z} is an integral domain. However, I is not maximal since it is properly contained in the ideal $J = \{\text{polynomials with even constant coefficient}\}$.

Definition 1.13 Given a set A , a **partial ordering** on A is a relation \leq such that

1. If $x \leq y$ and $y \leq z$, then $x \leq z$.
2. $\forall x \in A, x \leq x$.

Definition 1.14 If B is a subset of A , then $x \in A$ is an **upper bound** for B if $\forall y \in B, y \leq x$. (Note that x does not have to be in B .)

Definition 1.15 A subset B of A is a **chain** if \leq is a **total ordering** on B , i.e. $\forall x, y \in B, x \leq y$ or $y \leq x$, and $x \leq y$ and $y \leq x$ implies that $x = y$.

Statement 1.16 (Zorn's Lemma) Let A be a partially ordered set such that each chain has an upper bound. Then A has a **maximal element**, i.e. an element x such that $\forall y \in A$, either $y \leq x$ or x and y are not related.

Theorem 1.17 Let I be a proper ideal in a ring R . Then \exists a maximal ideal J such that $I \subset J$.

Proof We use Zorn's Lemma with $A =$ set of all proper ideals containing I under set inclusion (this is a partial ordering). Let B be a chain in A , and let J be the union of all ideals in B . Verify that J is a proper ideal of R which contains I . Hence J is in A and is an upper bound for B . So A has a maximal element, i.e. a maximal ideal containing I .

Remark Hence if R is any nontrivial commutative ring, then it has a homomorphic image which is a field (namely R/I , where I is a maximal ideal).

Example and Exercise Let R be the ring of subsets of a set A (see example (8) after Definition 1.1). Then the ideal consisting of all subsets not containing a particular $x \in A$ is a maximal ideal. Amuse yourself by thinking about the ideal consisting of all finite subsets of an infinite set.

For the rest of this chapter, all rings are commutative.

Definition 1.18

1. A ring R with exactly one maximal ideal is called a **local ring**. The field $k = R/I$ is called the **residue field** of R .
2. A ring with only a finite number of maximal ideals is called **semilocal**.

Proposition 1.19

1. Let R be a ring, and let $\mathfrak{m} \neq (1)$ be an ideal of R such that $x \in R - \mathfrak{m}$ is a unit in R . Then R is a local ring, and \mathfrak{m} is its maximal ideal.
2. Let R be a ring, and let \mathfrak{m} be a maximal ideal of R such that every element in $1 + \mathfrak{m}$ is a unit in R . Then R is a local ring.

Proof

1. Every ideal $I \neq (1)$ in R consists of nonunits. Hence $I \subseteq \mathfrak{m}$, and so \mathfrak{m} is the only maximal ideal of R .
2. Suppose $x \in R - \mathfrak{m}$. Then \mathfrak{m} is maximal implies that the ideal generated by x and \mathfrak{m} is (1) . Thus $\exists y \in R, t \in \mathfrak{m}$ such that $xy + t = 1$. Thus $xy = 1 - t \in 1 + \mathfrak{m}$. So xy is a unit. Now the result follows from (1).

1.1 Nilradical and Jacobson Radical

Proposition 1.20 The set \mathfrak{N} of all nilpotent elements in a ring R is an ideal, and R/\mathfrak{N} has no nonzero nilpotent elements.

Proof If $x \in \mathfrak{N}$, then plainly $ax \in \mathfrak{N} \forall a \in R$. Now suppose that $xy \in \mathfrak{N}$ with $x^m = y^n = 0$. Then the binomial theorem implies that $(x+y)^{2m+2n} = 0$, whence $x+y \in \mathfrak{N}$. Hence \mathfrak{N} is an ideal. Suppose $\bar{x} \in R/\mathfrak{N}$ is represented by $x \in R$ and that \bar{x} is nilpotent with $\bar{x}^n = 0$ in R/\mathfrak{N} . Then $\bar{x}^n = 0$ implies that $x^n \in \mathfrak{N}$, which implies that $(x^n)^k = 0$ for some k , which implies that $x \in \mathfrak{N}$, which implies that $\bar{x} = 0$.

Definition 1.21 The ideal \mathfrak{N} is called the **nilradical** of R .

Proposition 1.22 The nilradical of R is the intersection of all prime ideals in R .

Proof Let \mathfrak{N} be the intersection of all the prime ideals in R . If $f \in R$ is nilpotent, and if \mathfrak{p} is a prime ideal, then $f^n = 0 \in \mathfrak{p}$ for some $n > 0$. So $f \in \mathfrak{p}$ (since \mathfrak{p} is prime), and therefore $f \in \mathfrak{N}$. Suppose conversely that f is not nilpotent. Let Σ be the set of ideals I satisfying the following property: $n > 0$ implies that $f^n \notin I$. Then $\Sigma \neq \emptyset$, since $(0) \in \Sigma$. Apply Zorn's Lemma to the set Σ ordered by inclusion, and conclude that Σ has a maximal element, \mathfrak{p} , say. We claim that \mathfrak{p} is a prime ideal. Suppose that $x, y \notin \mathfrak{p}$. Then $\mathfrak{p} \subset \mathfrak{p} + (x)$, and $\mathfrak{p} \subset \mathfrak{p} + (y)$ with strict inclusions, and so $\mathfrak{p} + (x)$ and $\mathfrak{p} + (y)$ do not belong to Σ . Hence $f^m \in \mathfrak{p} + (x)$, $f^n \in \mathfrak{p} + (y)$ for some $m, n > 0$. Thus $f^{m+n} \in \mathfrak{p} + (xy)$. Therefore $\mathfrak{p} + (xy) \notin \Sigma$, and so $xy \notin \mathfrak{p}$. Hence now we have a prime ideal \mathfrak{p} such that $f \notin \mathfrak{p}$, and thus $f \notin \mathfrak{N}$.

Definition 1.23 The **Jacobson radical** \mathcal{R} of R is defined to be the intersection of all maximal ideals of R .

Proposition 1.24 $x \in \mathcal{R}$ iff $1 - xy$ is a unit in R for $y \in R$.

Proof Suppose that $1 - xy$ is not a unit. Then $1 - xy \in \mathfrak{m}$, where \mathfrak{m} is some maximal ideal. But $x \in \mathcal{R} \subset \mathfrak{m}$, and so $1 \in \mathfrak{m}$, which is a contradiction. Conversely, suppose that $x \notin \mathcal{R}$ for some maximal ideal \mathfrak{m} . Then \mathfrak{m}, x generate (1) , so $u + xy = 1$ for some $u \in \mathfrak{m}$ and $y \in R$. Thus $1 - xy \in \mathfrak{m}$, and so $1 - xy$ is not a unit.

1.2 Operations on Ideals

Let $(\mathfrak{a}_i)_{i \in I}$ be any family of ideals in R . The **sum** $\sum_i \mathfrak{a}_i = \{\sum_i x_i : x_i \in \mathfrak{a}_i : \forall i, \text{ and almost all of the } x_i = 0\}$. Then $\sum_i \mathfrak{a}_i$ is an ideal. Also, the intersection $\bigcap_i \mathfrak{a}_i$ is an ideal. If $\mathfrak{a}_1, \mathfrak{a}_2, \dots, \mathfrak{a}_n$ is a finite set of ideals, then the **product** $\mathfrak{a}_1 \mathfrak{a}_2 \cdots \mathfrak{a}_n$ consists of all *finite* sums $\sum x_1 x_2 \cdots x_n$, where

$x_i \in \mathfrak{a}_i$. This is an ideal. So if \mathfrak{a} is an ideal, then \mathfrak{a}^n ($n > 0$) is defined. By convention, $\mathfrak{a}^0 = (1)$.

Examples

1. Suppose $R = \mathbb{Z}$, $\mathfrak{a}_1 = (m)$, $\mathfrak{a}_2 = (n)$. Then $\mathfrak{a}_1 + \mathfrak{a}_2$ = ideal generated by the GCD of m, n .
 $\mathfrak{a}_1 \cap \mathfrak{a}_2$ = ideal generated by the LCM of m, n . $\mathfrak{a}_1 \mathfrak{a}_2 = (mn)$.
2. $R = k[x_1, x_2, \dots, x_n]$, $\mathfrak{a} = (x_1, x_2, \dots, x_n)$. Then \mathfrak{a}^m = set of polynomials with no terms of degree $< m$. These operations are all commutative and associative. Also $\mathfrak{a}(\mathfrak{b} + \Sigma) = \mathfrak{a}\mathfrak{b} + \mathfrak{a}\Sigma$ by the Distributive law.

Note $(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{a}(\mathfrak{a} \cap \mathfrak{b}) + \mathfrak{b}(\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathfrak{a}\mathfrak{b}$. Since also $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$, we have $\mathfrak{a}\mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}$ provided that $\mathfrak{a} + \mathfrak{b} = (1)$. Two ideals $\mathfrak{a}, \mathfrak{b}$ with $\mathfrak{a} + \mathfrak{b} = (1)$ are said to be **coprime** or **comaximal**.

Definition 1.25 Let R_1, R_2, \dots, R_n be rings. Their **direct product** $R = \prod_{i=1}^n R_i = \{(x_1, x_2, \dots, x_n) : x_i \in R_i\}$ is a ring with respect to componentwise addition and multiplication. We have projections $P_i : R \rightarrow R_i$, $P_i(x) = x_i$. These are *surjective* ring homomorphisms.

Proposition 1.26 Now suppose that R is a ring and let $\mathfrak{a}_1, \mathfrak{a}_2, \dots, \mathfrak{a}_n$ be ideals in R . Define a homomorphism $\phi : R \rightarrow \prod_{i=1}^n R/\mathfrak{a}_i$, $x \mapsto (x + \mathfrak{a}_1, x + \mathfrak{a}_2, \dots, x + \mathfrak{a}_n)$.

1. If \mathfrak{a}_i and \mathfrak{a}_j are coprime whenever $i \neq j$, then $\prod_i \mathfrak{a}_i = \bigcap_i \mathfrak{a}_i$.
2. ϕ is surjective iff \mathfrak{a}_i and \mathfrak{a}_j are coprime whenever $i \neq j$.
3. ϕ is injective iff $\bigcap_i \mathfrak{a}_i = (0)$.

Proof

1. We prove this by induction n . (See above for $n = 2$.) Suppose that $n > 2$ and that the result is true for $\mathfrak{a}_1, \mathfrak{a}_2, \dots, \mathfrak{a}_{n-1}$. Let $\mathfrak{b} = \prod_{i=1}^{n-1} \mathfrak{a}_i = \bigcap_{i=1}^{n-1} \mathfrak{a}_i$ since $\mathfrak{a}_1 + \mathfrak{a}_i = (1)$ ($1 \leq i \leq n-1$). We have equations $x_i + y_i = 1$ ($x_i \in \mathfrak{a}_1, y_i \in \mathfrak{a}_n$). Therefore $\prod_{i=1}^{n-1} x_i = \prod_{i=1}^{n-1} (1 - y_i) \equiv 1 \pmod{\mathfrak{a}_n}$. Hence $\mathfrak{a}_n + \mathfrak{b} = (1)$. Thus $\prod_{i=1}^n \mathfrak{a}_i = \mathfrak{b}\mathfrak{a}_n = \mathfrak{b} \cap \mathfrak{a}_n = \bigcap_{i=1}^n \mathfrak{a}_i$, as required.
2. We must show that \mathfrak{a}_1 and \mathfrak{a}_2 are coprime. $\exists x \in R$ such that $\phi(x) = (1, 0, 0, \dots, 0)$ since ϕ is surjective. Hence $x \equiv 1 \pmod{\mathfrak{a}_1}$ and $x \equiv 0 \pmod{\mathfrak{a}_2}$. Thus $1 = (1 - x) + x \in \mathfrak{a}_1 + \mathfrak{a}_2$. For the converse, we still have to prove that $\exists x \in R$ such that $\phi(x) = (1, 0, 0, \dots, 0)$. Since $\mathfrak{a}_1 + \mathfrak{a}_i = (1)$ ($i > 1$), we have $u_i + v_i = 1$ ($u_i \in \mathfrak{a}_1, v_i \in \mathfrak{a}_i$). Take $x = \prod_{i=2}^n v_i = \prod_{i=2}^n (1 - u_i)$. Then $x \equiv 1 \pmod{\mathfrak{a}_1}$ and $x \equiv 0 \pmod{\mathfrak{a}_i}$ ($i > 1$). Hence $\phi(x) = (1, 0, 0, \dots, 0)$, as required.
3. Clear, since $\ker \phi = \bigcap_{i=1}^n \mathfrak{a}_i$.

Note In general, $\mathfrak{a} \cup \mathfrak{b}$ is not an ideal.

Proposition 1.27

1. Let $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_n$ be prime ideals, and let \mathfrak{a} be an ideal contained in $\bigcup_{i=1}^n \mathfrak{p}_i$. Then $\mathfrak{a} \subseteq \mathfrak{p}_i$ for some i .
2. Let $\mathfrak{a}_1, \mathfrak{a}_2, \dots, \mathfrak{a}_n$ be ideals, and let \mathfrak{p} be a prime ideal containing $\bigcap_{i=1}^n \mathfrak{a}_i$. Then $\mathfrak{p} \supseteq \mathfrak{a}_i$ for some i . If $\mathfrak{p} = \bigcap_{i=1}^n \mathfrak{a}_i$, then $\mathfrak{p} = \mathfrak{a}_i$ for some i .

Proof

1. We prove this by induction on n . We show that $\mathfrak{a} \not\subseteq \mathfrak{p}_i$ ($1 \leq i < n$) implies that $\mathfrak{a} \not\subseteq \bigcup_{i=1}^n \mathfrak{p}_i$. This is true for $n = 1$. Suppose that $n > 1$ and that the result is true for $n - 1$. Then for each i , $\exists x_i \in \mathfrak{a}$ such that $x_i \notin \mathfrak{p}_j$ whenever $j \neq i$. If, for some i , we have $x_i \notin \mathfrak{p}_i$, then we are done. Otherwise $x_i \in \mathfrak{p}_i \forall i$. Consider $y = \sum_{i=1}^n x_1 x_2 \cdots x_{i-1} x_{i+1} \cdots x_n$. Then $y \in \mathfrak{a}$ and $y \notin \mathfrak{p}_i$ ($1 \leq i \leq n$). So $\mathfrak{a} \not\subseteq \bigcup_{i=1}^n \mathfrak{p}_i$.
2. Suppose that $\mathfrak{a}_i \not\subseteq \mathfrak{p}$ for all i . Then $x_i \in \mathfrak{a}_i$ such that $x_i \notin \mathfrak{p} \forall i$. So $\prod x_i \in \prod \mathfrak{a}_i \subseteq \bigcap \mathfrak{a}_i$, but $\prod x_i \notin \mathfrak{p}$, since \mathfrak{p} is prime. Hence $\bigcap \mathfrak{a}_i \not\subseteq \mathfrak{p}$, which is a contradiction. So $\mathfrak{a}_i \subseteq \mathfrak{p}$ for some i . Finally, if $\mathfrak{p} = \bigcap \mathfrak{a}_i$, then $\mathfrak{p} \subseteq \mathfrak{a}_i$ for all i , and so $\mathfrak{p} = \mathfrak{a}_i$ for some i .

Definition 1.28 If \mathfrak{a} and \mathfrak{b} are ideals in a ring R , the **ideal quotient** $(\mathfrak{a} : \mathfrak{b}) = \{x \in R : x\mathfrak{b} \subseteq \mathfrak{a}\}$. This is an ideal.

Definition 1.29 $\text{Ann}(\mathfrak{b}) := (0 : \mathfrak{b}) = \{R : x\mathfrak{b} = 0\}$ is an ideal called the **annihilator** of \mathfrak{b} . So the set of all zero divisors in R is $D = \bigcup_{x \neq 0} \text{Ann}(x)$. If $\mathfrak{b} = (x)$, then write $(\mathfrak{a} : x)$ for $(\mathfrak{a} : (x))$.

Example Suppose that $R = \mathbb{Z}$, $\mathfrak{a} = (m)$, and $\mathfrak{b} = (n)$, where $m = \prod_p p^{\mu_p}$ and $n = \prod_p p^{\nu_p}$. Then $(\mathfrak{a} : \mathfrak{b}) = (q)$, where $q = \prod_p p^{\gamma_p}$, where $\gamma_p = \max(\mu_p - \nu_p, 0)$. So $q = m/(m, n)$, where (m, n) is the GCD of m and n .

Proposition 1.30

1. $\mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b})$.
2. $(\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subseteq \mathfrak{a}$.
3. $((\mathfrak{a} : \mathfrak{b}) : \Sigma) = (\mathfrak{a} : \mathfrak{b}\Sigma) = ((\mathfrak{a} : \Sigma) : \mathfrak{b})$.
4. $(\bigcap_i \mathfrak{a}_i : \mathfrak{b}) = \bigcap_i (\mathfrak{a}_i : \mathfrak{b})$.
5. $(\mathfrak{a} : \sum_i \mathfrak{b}_i) = \bigcap_i (\mathfrak{a} : \mathfrak{b}_i)$.

Proof Exercise.

Definition 1.31 If \mathfrak{a} is an ideal of R , the **radical** of \mathfrak{a} is $r(\mathfrak{a}) = \{x \in R : x^n \in \mathfrak{a} \text{ for some } n > 0\}$. (This is sometimes written $\sqrt{\mathfrak{a}}$.) Observe that if $\phi : R \rightarrow R/\mathfrak{a}$ is the quotient homomorphism, then $r(\mathfrak{a}) = \phi^{-1}(\mathfrak{R}_{R/\mathfrak{a}})$. So $r(\mathfrak{a})$ is an ideal.

Proposition 1.32

1. $r(\mathfrak{a}) \supseteq \mathfrak{a}$.
2. $r(r(\mathfrak{a})) = r(\mathfrak{a})$.
3. $r(\mathfrak{a}\mathfrak{b}) = r(\mathfrak{a} \cap \mathfrak{b}) = r(\mathfrak{a}) \cap r(\mathfrak{b})$.
4. $r(\mathfrak{a}) = (1)$ iff $\mathfrak{a} = (1)$.
5. $r(\mathfrak{a} + \mathfrak{b}) = r(r(\mathfrak{a}) + r(\mathfrak{b}))$.
6. If \mathfrak{p} is a prime, then $r(\mathfrak{p}^n) = \mathfrak{p}$ for all $n > 0$.

Proof Exercise.

Proposition 1.33 $r(\mathfrak{a})$ is the intersection of the prime ideals which contain \mathfrak{a} .

Proof Apply Proposition 1.22 to R/\mathfrak{a} .

Remark For any subset E of R , we may define $r(E)$ in the same way. This is **not** an ideal in general.

We have $r(\bigcup_{\alpha} E_{\alpha}) = \bigcup_{\alpha} r(E_{\alpha})$ for any family of subsets E_{α} of R .

Proposition 1.34 $D = \text{set of zero divisors of } R = \bigcup_{x \neq 0} r(\text{Ann}(x))$.

Proof $D = r(D) = r(\bigcup_{x \neq 0} \text{Ann}(x)) = \bigcup_{x \neq 0} r(\text{Ann}(x))$.

Example If $R = \mathbb{Z}$ and $\mathfrak{a} = (m)$, let P_i ($1 \leq i \leq r$) be the distinct primes of m . Then $r(\mathfrak{a}) = (P_1 P_2 \cdots P_r) = \bigcap_{i=1}^r (P_i)$.

Proposition 1.35 Suppose that \mathfrak{a} and \mathfrak{b} are ideals in a ring R such that $r(\mathfrak{a})$ and $r(\mathfrak{b})$ are coprime. Then \mathfrak{a} and \mathfrak{b} are coprime.

Proof $(\mathfrak{a} + \mathfrak{b}) = r(r(\mathfrak{a} + r(\mathfrak{b}))) = r(1) = (1)$. Hence $\mathfrak{a} + \mathfrak{b} = (1)$ by Proposition 1.32(4).

1.3 Extension and Contraction of Ideals

Definition 1.36 Suppose that $f : R \rightarrow S$ is a ring homomorphism, and let \mathfrak{a} be an ideal in R . The **extension** \mathfrak{a}^e of \mathfrak{a} is the ideal generated by $f(\mathfrak{a})$ in S : $\mathfrak{a}^e = \{\sum y_i f(x_i) : x_i \in \mathfrak{a}, y_i \in S\}$. The **contraction** \mathfrak{b}^c of an ideal \mathfrak{b} in S is the ideal $f^{-1}(\mathfrak{b})$ in R .

Remark

1. If \mathfrak{a} is an ideal in R , then $f(\mathfrak{a})$ need not be an ideal in S , e.g. $\mathbb{Z} \hookrightarrow \mathbb{Q}$, \mathfrak{a} = any nonzero ideal in \mathbb{Z} .
2. If \mathfrak{b} is a prime ideal in S , then \mathfrak{b}^c is a prime ideal in R .
3. If \mathfrak{a} is a prime ideal in R , then \mathfrak{a}^e need not be a prime ideal in S (e.g. $\mathbb{Z} \hookrightarrow \mathbb{Q}$, $\mathfrak{a} \neq 0$, then $\mathfrak{a}^e = \mathbb{Q}$, and this is not a prime ideal).
4. Observe that we can factor $f : R \rightarrow S$ as follows:

$$R \xrightarrow{p} f(R) \xrightarrow{j} S,$$

where p is surjective and j is injective. For p there is a one-to-one correspondence between ideals of $f(R)$ and ideals of R which contain $\ker f$. Prime ideals correspond to prime ideals. For j the general situation is very complicated, cf. algebraic number theory.

Example Consider $\mathbb{Z} \hookrightarrow \mathbb{Z}[i]$. $\mathbb{Z}[i]$ is a Principal Ideal Domain since it is a Euclidean domain. A prime ideal (p) of \mathbb{Z} may or may not stay prime when extended to $\mathbb{Z}[i]$.

1. $(2)^e = ((1+i)^2)$, the square of a prime ideal in $\mathbb{Z}[i]$.
2. If $p \equiv 1 \pmod{4}$, then (p) is the product of two distinct prime ideals (e.g. $(5)^e = (2+i)(2-i)$).
3. If $p \equiv 3 \pmod{4}$, then $(p)^e$ is prime in $\mathbb{Z}[i]$.

(2) is nontrivial cf. Fermat's Theorem: If $p \equiv 1 \pmod{4}$, then p can be expressed as a sum of two squares.

Proposition 1.37 Let $f : R \rightarrow S$, and let $\mathfrak{a} \subset R, \mathfrak{b} \subset S$.

1. $\mathfrak{a} \subset \mathfrak{a}^{ec}, \mathfrak{b} \supset \mathfrak{b}^{ce}$.
2. $\mathfrak{b}^c = \mathfrak{b}^{cec}, \mathfrak{a}^e = \mathfrak{a}^{ece}$.
3. Let C be the set of contracted ideals in R . Let E be the set of extended ideals in S . Then $C = \{\mathfrak{a} : \mathfrak{a}^{ec} = \mathfrak{a}\}$, and $E = \{\mathfrak{b} : \mathfrak{b}^{ce} = \mathfrak{b}\}$, and $\mathfrak{a} \mapsto \mathfrak{a}^e$ is a bijective map $C \rightarrow E$ whose inverse is $\mathfrak{b} \mapsto \mathfrak{b}^c$.

Proof

1. Trivial.

2. Follows from (1).

3. Suppose $\mathfrak{a} \in C$. Then $\mathfrak{a} = \mathfrak{b}^c = \mathfrak{b}^{cec} = \mathfrak{a}^{ec}$. Conversely, if $\mathfrak{a} = \mathfrak{a}^{ec}$, then \mathfrak{a} is the contraction of \mathfrak{a}^e . A similar argument works for E .

Exercise If \mathfrak{a}_1 and \mathfrak{a}_2 are ideals of R and \mathfrak{b}_1 and \mathfrak{b}_2 are ideals of S , then $(\mathfrak{a}_1 + \mathfrak{a}_2)^e = \mathfrak{a}_1^e + \mathfrak{a}_2^e$, $(\mathfrak{a}_1 \cap \mathfrak{a}_2)^e \subseteq \mathfrak{a}_1^e \cap \mathfrak{a}_2^e$, $(\mathfrak{a}_1 \mathfrak{a}_2)^e = \mathfrak{a}_1^e \mathfrak{a}_2^e$, $(\mathfrak{a}_1 : \mathfrak{a}_2)^e \subseteq (\mathfrak{a}_1^e : \mathfrak{a}_2^e)$, and $r(\mathfrak{a})^e \subseteq r(\mathfrak{a}^e)$. Also, $(\mathfrak{b}_1 + \mathfrak{b}_2)^c \supseteq \mathfrak{b}_1^c + \mathfrak{b}_2^c$, $(\mathfrak{b}_1 \cap \mathfrak{b}_2)^c = \mathfrak{b}_1^c \cap \mathfrak{b}_2^c$, $(\mathfrak{b}_1 \mathfrak{b}_2)^c \supseteq (\mathfrak{b}_1^c \mathfrak{b}_2^c)$, $(\mathfrak{b}_1 : \mathfrak{b}_2)^c \subseteq \mathfrak{b}_1^c : \mathfrak{b}_2^c$, and $r(\mathfrak{b})^c = r(\mathfrak{b}^c)$.

The set E is closed under sum and product. The set C is closed under sum, product, and intersection.

1.4 Rings of Fractions and Localization

Motivation Recall how one constructs \mathbb{Q} from \mathbb{Z} (and embeds $\mathbb{Z} \hookrightarrow \mathbb{Q}$). This extends to any integral domain R and produces the **field of fractions** of R . Take all ordered pairs (a, s) , $a \in R$, $s \in R$, $s \neq 0$, and set up an equivalence relation

$$(a, s) \sim (b, t) \text{ iff } at - bs = 0.$$

Note This works only if R is an integral domain because the verification of transitivity involves cancellation.

Definition 1.38 Let R be any commutative ring. A **multiplicative subset** S of R is a subset such that $1 \in S$ and S is closed under multiplication.

Define a relation \sim on $R \times S$ by

$$(a, s) \sim (b, t) \text{ iff } (at - bs)u = 0$$

for some $u \in S$. We claim that \sim is an equivalence relation. \sim is clearly reflexive and symmetric. To prove transitivity, suppose that $(a, s) \sim (b, t)$ and $(b, t) \sim (c, u)$. Then $\exists v, w \in S$ such that $(at - bs)v = 0$ and $(bu - ct)w = 0$. Eliminating b gives $(au - cs)tvw = 0$. Since S is multiplicative, $tvw \in S$, so $(a, s) \sim (c, u)$.

Notation a/s is the equivalence class of (a, s) . $S^{-1}R$ is the set of equivalence classes. Put a ring structure on $S^{-1}R$: $\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st}$, $\frac{a}{s} \frac{b}{t} = \frac{ab}{st}$. Show that these are well-defined and give a ring structure. Also, we have a ring homomorphism $f : R \rightarrow S^{-1}R$, $f(x) = x/1$. f is not, in general, injective.

Remark

1. If R is an integral domain and $S = R - \{0\}$, then $S^{-1}R$ is the field of fractions of R .
2. The ring $S^{-1}R$ is called the ring of fractions of R with respect to S .

Proposition 1.39 (Universal Property of the Ring of Fractions) Let $g : R \rightarrow R_1$ be a ring homomorphism such that $g(s)$ is a unit in $R_1 \forall s \in S$. Then $\exists!$ ring homomorphism $h : S^{-1}R \rightarrow R_1$ such that $g = h \circ f$.

$$\begin{array}{ccc}
 R & \xrightarrow{g} & R_1 \\
 \downarrow f & \nearrow \exists! h & \\
 S^{-1}R & &
 \end{array}$$

Proof First we prove uniqueness. Suppose that h satisfies the condition. Then $h(a/1) = h \circ f(a) = g(a) \forall a \in R$. Hence if $s \in S$, $h(1/s) = h((s/1)^{-1}) = h(s/1)^{-1} = g(s)^{-1}$. So $h(a/s) = h(a/1)h(1/s) = g(a)g(s)^{-1}$, and thus h is uniquely determined by g . To prove existence, let $h(a/s) = g(a)g(s)^{-1}$. Then h is a ring homomorphism provided that it is well-defined. So suppose that $a/s = a'/s'$. Then $\exists f \in S$ such that $(as' - a's)t = 0$. Thus $(g(a)g(s') - g(a')g(s))g(t) = 0$. Now $g(t)$ is a unit in R_1 by hypothesis, and so $g(a)g(s') = g(a')g(s)$, as required.

The ring $S^{-1}R$ and the homomorphism $f : R \rightarrow S^{-1}R$ satisfy the following properties:

1. $s \in S$ implies that $f(s)$ is a unit in $S^{-1}R$.
2. $f(a) = 0$ implies that $as = 0$ for some $s \in S$.
3. Every element of $S^{-1}R$ is of the form $f(a)f(s)^{-1}$ for some $a \in R, s \in S$.

Conversely, these three conditions determine the ring $S^{-1}R$ up to isomorphism.

Corollary 1.40 If $g : R \rightarrow R_1$ is a ring homomorphism such that

1. $s \in S$ implies that $g(s)$ is a unit in R_1 ,
2. $g(a) = 0$ implies that $as = 0$ for some $s \in S$, and
3. Every element of R_1 is of the form $g(a)g(s)^{-1}$ for some $a \in R, s \in S$,

then $\exists!$ isomorphism $h = S^{-1}R \rightarrow R_1$ such that $g = h \circ f$.

Proof By Proposition 1.39, we have to show that $h : S^{-1}R \rightarrow R_1$ defined by $h(a/s) = g(a)g(s)^{-1}$ is an isomorphism. (By part (1), this is well-defined.) Part (3) implies that h is surjective. To prove

injectivity, suppose that $h(a/s) = 0$. Then $g(a) = 0$. So part (1) implies that $at = 0$ for some $t \in S$. Thus $(a, s) \sim (0, 1)$, i.e. $a/s = 0$ in $S^{-1}R$.

Remark The pair $(S^{-1}R, f)$ is an example of a **universal object**.

Examples

1. Let \mathfrak{p} be a prime ideal of R . Then $S = R - \mathfrak{p}$ is a multiplicative subset of R . Write $R_{\mathfrak{p}} := S^{-1}R$. The elements a/s with $a \in \mathfrak{p}$ form an ideal \mathfrak{m} in $R_{\mathfrak{p}}$. If $b/t \in \mathfrak{m}$, then $b \notin \mathfrak{p}$, so $b \in S$, and therefore b/t is a unit in $R_{\mathfrak{p}}$. Thus if \mathfrak{a} is an ideal in $R_{\mathfrak{p}}$ and $\mathfrak{a} \neq \mathfrak{m}$, then \mathfrak{a} contains a unit, so $\mathfrak{a} = R_{\mathfrak{p}}$. Thus \mathfrak{m} is the only maximal ideal in $R_{\mathfrak{p}}$, i.e. $R_{\mathfrak{p}}$ is a local ring. Passing from R to $R_{\mathfrak{p}}$ is called a localization at \mathfrak{p} .
2. $S^{-1}R$ is the zero ring iff $0 \in S$.
3. Let $f \in R$ and $S = \{f^n\}_{n \geq 0}$. Write $R_f := S^{-1}R$ in this case.
4. Let \mathfrak{a} be any ideal in R , and let $S = 1 + \mathfrak{a}$. Then S is multiplicatively closed.
5. Special cases of (1) and (3):
 - (a) $R = \mathbb{Z}$, $\mathfrak{p} = (p)$, where p is prime. $R_{\mathfrak{p}} = \{m/n : n \text{ is coprime to } p\}$. If $f \in \mathbb{Z}$, with $f \neq 0$, then $R_f = \{m/n : n \text{ is a power of } f\}$.
 - (b) $R = k[t_1, t_2, \dots, t_n]$, k a field, t_i are indeterminates. Suppose that \mathfrak{p} is a prime ideal in R . Then $R_{\mathfrak{p}} =$ all rational functions f/g with $g \notin \mathfrak{p}$.
 - (c) Extended and contracted ideals in rings of fractions $R =$ a ring, $S =$ a multiplicative subset of R , $f : R \rightarrow S^{-1}R$, $a \mapsto a/1$, $C =$ set of contracted ideals in R , $E =$ set of extended ideals in $S^{-1}R$. If \mathfrak{a} is an ideal in R , then its extension \mathfrak{a}^e in $S^{-1}R$ is $S^{-1}R = \{a/s : a \in \mathfrak{a}, s \in S\}$.

Recall $(\mathfrak{a} : \mathfrak{b}) = \{x \in R : x\mathfrak{b} \subseteq \mathfrak{a}\}$.

Proposition 1.41

1. Every ideal in $S^{-1}R$ is an extended ideal.
2. If \mathfrak{a} is an ideal in R , then $\mathfrak{a}^{ec} = \bigcup_{s \in S} (\mathfrak{a} : S)$. Hence $\mathfrak{a}^e = (1)$ iff \mathfrak{a} meets S .
3. $\mathfrak{a} \in C$ iff no element of S is a zero divisor in R/\mathfrak{a} .
4. The prime ideals of $S^{-1}R$ are in one-to-one correspondence ($\mathfrak{p} \leftrightarrow S^{-1}\mathfrak{p}$) with the prime ideals of R that do not meet S .
5. The operation S^{-1} commutes with the formation of finite sums, products, intersections, and radicals.

Proof

1. Let \mathfrak{b} be an ideal in $S^{-1}R$, and let $X/S \in \mathfrak{b}$. Then $x/1 \in \mathfrak{b}$, and so $x \in \mathfrak{b}^c$, whence $x/1 \in \mathfrak{b}^{ce}$. Since $\mathfrak{b} \supseteq \mathfrak{b}^{ce}$ by Proposition 1.37, it follows that $\mathfrak{b} = \mathfrak{b}^{ce}$.
2. $x \in \mathfrak{a}^{ec} = (S^{-1}\mathfrak{a})^e$ iff $x/1 = a/s$ for some $a \in \mathfrak{a}$, $s \in S$ iff $(xs - a)t = 0$ for some $t \in S$ iff $xst \in \mathfrak{a}$ iff $\bigcup_{x \in S} (\mathfrak{a}, S)$.
3. $\mathfrak{a} \in C$ iff \mathfrak{a}^{ce} by Proposition 1.37 iff $(sx \in \mathfrak{a}$ for some $s \in S$ iff $x \in \mathfrak{a})$ (from part (2)) iff no $s \in S$ is a zero divisor in R/\mathfrak{a} .
4. If \mathfrak{q} is a prime ideal in $S^{-1}R$, then \mathfrak{q}^c is a prime ideal in R . Conversely, if \mathfrak{p} is a prime ideal in R , then R/\mathfrak{p} is an integral domain. If \bar{S} is the image of S in R/\mathfrak{p} , then we have that $S^{-1}R/S^{-1}\mathfrak{p} \simeq \bar{S}^{-1}(R/\mathfrak{p})$. (The map $\theta : S^{-1}R \rightarrow \bar{S}^{-1}(R/\mathfrak{p})$ given by $\theta(s^{-1}r) = \pi(s)^{-1}\pi(r)$ (where $\pi : R \rightarrow R/\mathfrak{p}$ is a reduction mod \mathfrak{p}) induces the above isomorphism.) Now $\bar{S}^{-1}(R/\mathfrak{p})$ is either 0 or else is contained in the field of fractions of R/\mathfrak{p} and is therefore an integral domain. So $S^{-1}\mathfrak{p}$ is either prime or is the unit ideal. Part (2) implies that the latter possibility occurs iff \mathfrak{p} meets S .
5. Exercise. (For sums and products, use the exercise after Proposition 1.37.)

Remark Recall Proposition 1.22. If $f \in R$ is not nilpotent, then \exists a prime ideal of R which does not contain f . Another way to see this is that since $S = \{f^n\}_{n \geq 0}$ does not contain 0, the ring $S^{-1}R = R_f$ is not the zero ring. Hence R_f has a maximal ideal \mathfrak{m} (which is prime). The contraction \mathfrak{m}^c of \mathfrak{m} is a prime ideal in R which does not meet S by Proposition 1.41(4). Hence $f \notin \mathfrak{m}^c$.

Corollary 1.42 If \mathfrak{N} is the nilradical of R , then the nilradical of $S^{-1}R$ is $S^{-1}\mathfrak{N}$.

Corollary 1.43 If \mathfrak{p} is a prime ideal in R , then the prime ideal of the local ring $R_{\mathfrak{p}}$ are in one-to-one correspondence with the prime ideals contained in \mathfrak{p} .

Proof Take $S = R - \mathfrak{p}$ in Proposition 1.41(4).

Remark Passing from R to $R_{\mathfrak{p}}$ eliminates all prime ideals except those contained in \mathfrak{p} . Passing from R to R/\mathfrak{p} eliminates all prime ideals except those containing \mathfrak{p} .

Chapter 2

Modules

Definition 2.1 Let R be a commutative ring. Then an abelian group M is called an R -**module** if \exists a function $\cdot : R \times M \rightarrow M$ (we write rm for $\cdot(r, m)$) such that

1. $\forall r \in R, m_1, m_2 \in M, r(m_1 + m_2) = rm_1 + rm_2,$
2. $\forall r_1, r_2 \in R, m \in M, (r_1 + r_2)m = r_1m + r_2m,$
3. $r_1(r_2m) = (r_1r_2)m,$
4. $\forall m \in M, 1m = m.$

Note If R is not commutative, then we can define a **left** R -**module** as above. Similarly, we can define a **right** R -**module** but with $M \times R \rightarrow M$. But we cannot convert left R -modules to right R -modules in the “obvious” way $rm \mapsto mr$ since (3) goes wrong: $(mr_2)r_1 \neq mr_1r_2$ in general.

Examples

1. If R is a commutative ring, then R is an R -module using the existing multiplication. Similarly, $R \oplus R$ is an R -module if we define $r(rr_1, rr_2) = (rr_1, rr_2)$. If S is a subring of R , then R is an S -module. In particular, $R[x]$ is an R -module. If I is an ideal of R , then I is an R -module.
2. If V is a vector space over a field F , then V is an F -module.
3. Let G be an abelian group. Then G is a \mathbb{Z} -module if we define \cdot . Suppose $x \in G$. Put $nx = x + x + \cdots + x$ (n times) if $n \geq 1$, $0x = 0$, $nx = (-n)(-x)$ if $n \leq -1$. This satisfies (1)-(4) of Definition 2.1.
4. Let V be a vector space over a field F , and let $\theta : V \rightarrow V$ be a linear map. (The pair (V, θ) is a **vector space with endomorphism**.) Regard V as an $F[x]$ -module by setting $(a_0 + a_1x + \cdots + a_nx^n)v = a_0v + a_1\theta(v) + \cdots + a_n\theta^n(v)$ ($a_0, a_1, \dots, a_n \in F, v \in V$). This works.

Proposition 2.2 Let M be an R -module. Then

1. $0m = 0 \forall m \in M.$

2. $(-r)m = r(-m) \forall r \in R, m \in M$.

Definition 2.3 Let M be an R -module. A subgroup N of the additive group M is a **submodule** if $\forall r \in R$ and $n \in N$ we have $rn \in N$, and N is an R -module with respect to this “scalar multiplication.”

Proposition 2.4 A subset N of M is a submodule iff

1. $N \neq \emptyset$,
2. $\forall n_1, n_2 \in N, n_1 + n_2 \in N$,
3. $\forall r \in R, n \in N, rn \in N$.

Note that by (3), if $n \in N$, then so is $-n = (-1)n$.

Examples

1. If R is a commutative ring regarded as an R -module, then a submodule is an ideal.
2. If V is a vector space of F (i.e. an F -module), then a submodule is a subspace.
3. If G is an abelian group viewed as a \mathbb{Z} -module, then a submodule is a subgroup.
4. If V is a vector space over F with endomorphism θ , viewed as an $F[x]$ -module, then a submodule is a vector subspace W such that $\theta(W) \subset W$ (i.e. W is an “invariant subspace”).

Definition 2.5 Let R be a commutative ring, and let M, N be R -modules. A group homomorphism $\theta : M \rightarrow N$ is called a **module homomorphism** (or **R -homomorphism**) if $\forall r \in R, m \in M, \theta(rm) = r\theta(m)$. If θ is also bijective, then θ is an isomorphism of modules, and we write $M \simeq N$.

Examples

1. If V, W are F -vector spaces, then an F -homomorphism $V \rightarrow W$ is the same as a linear map.
2. If G, H are abelian groups, then a \mathbb{Z} -homomorphism $G \rightarrow H$ is just an ordinary homomorphism.

Proposition 2.6 If $\theta : M \rightarrow N$ is an R -homomorphism, then $\theta(M)$ is a submodule of N , and $\ker \theta = \{m \in M | \theta(m) = 0\}$ is submodule of M .

Proof Exercise.

Definition 2.7

1. If M is an R -module and N is a submodule, then the quotient abelian group M/N can be made into an R -module by defining $r(m+N) = rm + N$. M/N is called a **quotient module**. $\theta : M \rightarrow M/N, m \mapsto m + N$ is called the **quotient homomorphism**.
2. If M, N are two R -modules, then their direct sum $M \oplus N$ is the direct sum of the abelian groups made into an R -module by defining $r(m, n) = (rm, rn)$.

Examples

1. For an F -vector space, a quotient F -module is a quotient vector space. The case of direct sums is similar.
2. For abelian groups (i.e. \mathbb{Z} -modules), “quotient” and “direct sum” for modules have the same meanings as for abelian groups.
3. Suppose that V is an F -vector space and θ is an endomorphism of V . We may view V as being an $F[x]$ -module. Suppose that W is an $F[x]$ submodule of V (so W is a subspace of V with $\theta(W) \subset W$). Then the quotient $F[x]$ -module V/W is the quotient vector space with the action of $F[x]$ given by the endomorphism $\bar{\theta} : V/W \rightarrow V/W$ induced by θ .

Theorem 2.8 If $\theta : M \rightarrow N$ is an R -homomorphism, then $\theta(M) \simeq M/\ker \theta$.

Proof Exercise.

Proposition 2.9 Let M be an R -module, and let $\theta : S \rightarrow R$ be a ring homomorphism. Then M is an S -module.

Proof Define $S \times M \rightarrow M$ to be the composite $S \times M \rightarrow R \times M \rightarrow M, (s, m) \mapsto (\theta(s), m) \mapsto \theta(s)m$. Then M is an S -module (since θ is a homomorphism).

Examples

1. Let R be a ring, and let I be an ideal of R . Then the quotient ring R/I is an R/I -module. We may convert it into an R -module via the quotient map $\theta : R \rightarrow R/I$. This R -module is the quotient R -module R/I .
2. The direct sum of rings $R \oplus R$ is an $R \oplus R$ -module. We may convert it into an R -module via the ring homomorphism $\theta : R \rightarrow R \oplus R$ defined by $\theta(r) = (r, r)$. This is the direct sum of modules $R \oplus R$.
3. Let M be any R -module. Define $\theta : \mathbb{Z} \rightarrow R$ by $\theta(n) = n \cdot 1_R$. This is a ring homomorphism, and it converts M into a \mathbb{Z} -module, i.e. an abelian group.

Proposition 2.10 Let M be an R -module, and let $I \subset R$ be the subset of elements r of R such that $rm = 0 \forall m \in M$. Then I is an ideal (the **annihilator ideal of M**), and M is an R/I -module.

Proof To show that I is an ideal, note that $0 \in I$, and also $r_1, r_2 \in I$ implies that $r_1 - r_2 \in I$. Furthermore, if $R \in I$ and $s \in R$, then $sr \in I$. To make M into an R/I -module, define $(r + I)m = rm$. This works.

Remark Similarly, if J is an ideal of R with $J \subset I$, then M is an R/J -module.

Boring Remark If we use Proposition 2.9 to convert M back into an R -module, we get the original R -module back again.

Example Let V be an F -vector space with endomorphism θ , and view V as an $F[x]$ -module. The annihilator ideal I of $V = \{f(x) \in F[x] \mid f(\theta) = 0\}$ is a principal ideal generated by $m(x)$, the **minimum polynomial of θ** . Hence V is an $F[x]/(m(x))$ -module and even an $F[x]/(m(x))$ -vector space if $m(x)$ is irreducible.

For a finite dimensional vector space over a field F , \exists a basis e_1, e_2, \dots, e_n such that each element has a unique expression of the form $\lambda_1 e_1 + \lambda_2 e_2 + \dots + \lambda_n e_n$ ($\lambda_1, \lambda_2, \dots, \lambda_n \in F$). This is *not* always true for R -modules, e.g. consider \mathbb{Z}_2 as a \mathbb{Z} -module. Then $\{1\}$ is not a basis since $1 \cdot 1 = 3 \cdot 1$, so uniqueness is not possible.

Definition 2.11 Let M be an R -module, and let A be a subset of M . The **submodule generated by A** is the intersection of all submodules containing A . (This is another submodule whose elements are of the form $\sum_{i=1}^n \lambda_i a_i$, $\lambda_i \in R$, $a_i \in A$.) If the submodule generated by A is all of M , we say that M is generated by A .

Definition 2.12 M is **finitely generated** if \exists a finite set A such that M is generated by A .

Definition 2.13 If M is generated by A , and each $m \in M$ is uniquely expressible in the form $\sum_{i=1}^n r_i a_i$, where each $r_i \in R$, $a_i \in A$, and the a_i s are distinct, then M is **free**, and A is a **basis**.

Note that A is a basis iff

1. $\forall m \in M$, \exists an expression $m = \sum_{i=1}^n r_i a_i$ (i.e. A spans M).
2. If $\sum_{i=1}^m r_i a_i = 0$ and the a_i s are distinct, then $r_1 = r_2 = \dots = r_n = 0$ (i.e. the elements in A are linearly independent).

Note If M is $f \cdot g$ and free, then any two bases have the same size. (This is not obvious, and we'll prove it later.)

Examples

1. If F is a field, then every F -module (i.e. F -vector space) is free. However, if R is a principal ideal domain, not every R -module is free (e.g. \mathbb{Z}_2 as a \mathbb{Z} -module).
2. If R is any nontrivial commutative ring, then R is a *free* R -module since $\{1\}$ is a basis. Similarly, $R^n := R \oplus R \oplus \cdots \oplus R$ (n times) is a free R -module since e_1, e_2, \dots, e_n is a basis (where $e_i = (0, 0, \dots, 0, 1, 0, \dots, 0)$ with the 1 in the i th place). Note that if M is a free R -module with basis A and N is any R -module, then any *function* $f : A \rightarrow N$ can be extended uniquely to an R -homomorphism $\theta : M \rightarrow N$ by defining

$$\theta\left(\sum_{i=1}^n r_i a_i\right) = \sum_{i=1}^n r_i f(a_i).$$

Proposition 2.14 Suppose we are given R -modules and homomorphisms

$$\begin{array}{ccc} & & L \\ & \nearrow \psi & \downarrow \theta \\ M & \xrightarrow{\phi} & N \end{array}$$

where L is free and ϕ is surjective. Then \exists an R -homomorphism $\psi : L \rightarrow M$ such that $\phi\psi = \theta$.

Proof Let A be a basis of L . For each $a_i \in A$, choose $m_i \in M$ such that $\phi(m_i) = \theta(a_i)$. (We may do this since ϕ is surjective.) Define $f : A \rightarrow M$ by $f(a_i) = m_i$, and extend f to a homomorphism $\psi : L \rightarrow M$. Then $\phi\psi(a_i) = \theta(a_i)$, and so $\phi\psi = \theta$, by uniqueness.

Note Proposition 2.14 does not necessarily hold if L is not free, e.g. consider the modules

$$\varphi(n) = \begin{cases} 1 & n \text{ odd} \\ 0 & n \text{ even.} \end{cases}$$

$$\begin{array}{ccc} & & \mathbb{Z}_2 \\ & \nearrow \psi & \downarrow id \\ \mathbb{Z} & \xrightarrow{\varphi} & \mathbb{Z}_2 \end{array}$$

If $\psi : \mathbb{Z}_2 \rightarrow \mathbb{Z}$ is a homomorphism and $\psi(1) = n$, say, then $2n = \psi(2) = 0$, so $n = 0$, and hence $\psi = 0$. Thus $\theta\psi \neq \text{identity}$.

Proposition 2.15 Let M be any R -module. Then \exists a free R -module L and a submodule K of L such that $M \simeq L/K$. Hence every R -module is a homomorphic image of a free module.

Proof Given any set A , we may construct a free R -module whose basis is A by taking all formal finite sums $\sum_{i=1}^n r_i a_i$ (hence the a_i are distinct elements of A , $r_i \in R$, and $n \geq 1$) with the “obvious” addition and scalar multiplication. This new set becomes a module which is clearly free, with A as basis. This module is called the **free module generated by A** .

Now take L to be the free module generated by A , where A is any subset of M that generates M (e.g. $A = M$). Finally, define a homomorphism $\theta : L \rightarrow M$ by extending the function $f : A \rightarrow M$, where f is inclusion. Since A generates M , θ is onto. Hence $M \simeq L/\ker \theta$ by Theorem 2.8.

Note If M is fg , then we can take L to be fg also (take A to be finite).

Definition 2.16 A sequence of R -modules and R -homomorphisms

$$\cdots \rightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \rightarrow \cdots \quad (*)$$

is said to be **exact at M_i** if $\text{Im}(f_i) = \ker f_{i+1}$. The sequence is **exact** if f is exact at each M_i . So

1. $0 \rightarrow M' \xrightarrow{f} M$ is exact iff f is injective.
2. $M \xrightarrow{g} M'' \rightarrow 0$ is exact iff g is surjective.
3. $0 \rightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \rightarrow 0$ is exact iff f is injective, g is surjective, and g induces an isomorphism $\text{coker } f := M/f(M') \simeq M''$.

An exact sequence of type (3) is called a **short exact sequence**. Any long exact sequence (*) can be split up into short exact sequences, for if $N_i = m(f_i) = \ker f_{i+1}$, then we have short exact sequences $0 \rightarrow N_i \rightarrow M_i \rightarrow N_{i+1} \rightarrow 0$.

Proposition 2.17

1. Let

$$M' \xrightarrow{u} M \xrightarrow{v} M'' \rightarrow 0 \quad (1)$$

be a sequence of R -modules and homomorphisms. Then (1) is exact iff for all R -modules N , the sequence

$$0 \rightarrow \text{hom}(M'', N) \xrightarrow{\bar{v}} \text{hom}(M, N) \xrightarrow{\bar{u}} \text{hom}(M', N) \quad (1')$$

is exact.

2. Let

$$0 \rightarrow N' \xrightarrow{u} N \xrightarrow{v} N'' \quad (2)$$

be a sequence of R -modules and homomorphisms. Then (2) is exact iff for all R -modules M , the sequence

$$0 \rightarrow \text{hom}(M, N') \xrightarrow{\bar{u}} \text{hom}(M, N) \xrightarrow{\bar{v}} \text{hom}(M, N'') \quad (2')$$

is exact.

Proof Exercise, but e.g. suppose that (1') is exact $\forall N$. Then \bar{v} is injective $\forall N$, and so v is surjective.

$$\begin{array}{ccc} M'' & \xrightarrow{q} & M''/v(M) \\ \uparrow v & \nearrow & \\ M & & \end{array}$$

Next $\bar{u} \circ \bar{v} = 0$, i.e. $f \circ v \circ u = 0 \forall f : M'' \rightarrow N$. Take $N = M''$ and $f = \text{identity}$. Then $v \circ u = 0$, i.e. $\text{Im}(u) \subseteq \ker v$. Next take $N = M/\text{Im}(u)$, and let $\phi : M \rightarrow M/\text{Im}(u)$ be the quotient map. Then $\phi \in \ker \bar{u}$. So $\exists \psi : M'' \rightarrow M/\text{Im}(u)$ such that $\psi \circ v = \phi$. Hence $\text{Im}(u) = \ker \phi \supseteq \ker v$.

Proposition 2.18 (The Snake Lemma) Let

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{u} & M & \xrightarrow{v} & M'' & \longrightarrow & 0 \\ & & \downarrow f' & & \downarrow f & & \downarrow f'' & & \\ 0 & \longrightarrow & N' & \xrightarrow{u'} & N & \xrightarrow{v'} & N'' & \longrightarrow & 0 \end{array}$$

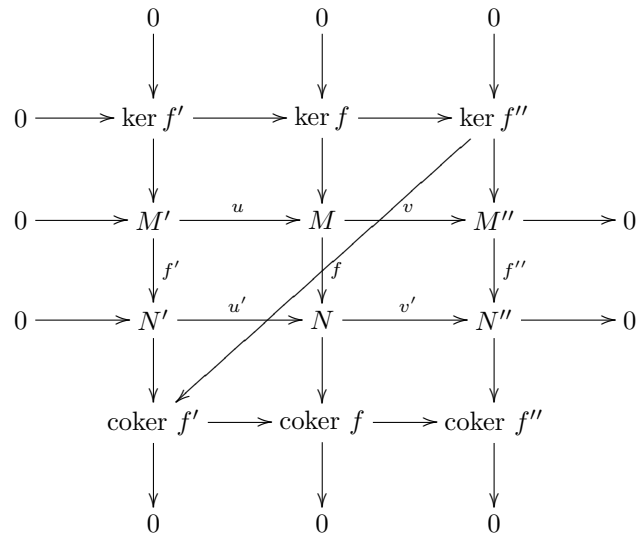
be a commutative diagram of R -modules and homomorphisms with the rows exact. Then \exists an exact sequence

$$0 \rightarrow \ker f' \xrightarrow{\bar{u}} \ker f \xrightarrow{\bar{v}} \ker f'' \xrightarrow{d} \text{coker } f' \xrightarrow{\bar{u}'} \text{coker } f \xrightarrow{\bar{v}'} \text{coker } f''.$$

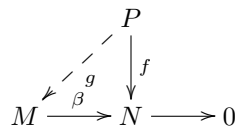
Here \bar{u} and \bar{v} are the restrictions of u and v , and \bar{u}' and \bar{v}' are induced by u' and v' .

Proof Exercise, but here's how you define the **boundary homomorphism** d : Suppose that $x \in \ker f''$. Then $x'' = v(x)$ for some $x \in M$, and $v'(f(x)) = f''(v(x)) = 0$. So $f(x) \in \ker v' = \text{Im } u'$, i.e. $f(x) = u'(y)$ for some $y \in N'$. Then $d(x'') := \text{image of } y \text{ in } \text{coker } f'$. Show that d is well-defined and that the sequence is exact.

Diagram



Definition 2.19 An R -module P is **projective** if it satisfies the following property: Given R -modules and homomorphisms



with β surjective, then $\exists g$ with $\beta g = f$.

There are a number of other ways of giving this definition.

Theorem 2.20 The following conditions are equivalent:

1. P is projective
2. Every short exact sequence $0 \longrightarrow M \longrightarrow N \xrightarrow{\beta} P \longrightarrow 0$ splits (so $N \simeq M \oplus P$).
3. P is a direct summand of a free R -module, i.e. \exists a free module F and an R -module M such that $F \simeq M \oplus P$.
4. If $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$ is any short sequence of R -modules, then the sequence $\text{hom}(P, M') \rightarrow \text{hom}(P, M) \rightarrow \text{hom}(P, M'')$ is also a short exact sequence.

Proof Exercise.

Chapter 3

Finitely Generated and Noetherian Modules and Rings

Question Suppose that R is a commutative ring. Then R is a finitely generated free R -module. Does this imply that every ideal of R is finitely generated?

Example Let R be the ring of all subsets of $[0, 1]$ (see chapter 1). Suppose that I is the ideal of R generated by E_1, E_2, \dots, E_n . We claim that I is the ideal of all subsets of $E_1 \cup E_2 \cup \dots \cup E_n$, for

1. This ideal contains E_1, E_2, \dots, E_n and thus contains I .
2. Also I contains $E_1 \cup E_2 \cup \dots \cup E_n$ (since e.g. $E_1 \cup E_2 = (E_1 + E_2)(E_1 \cdot E_2)$, etc.), and hence I contains all subsets of $E_1 \cup E_2 \cup \dots \cup E_n$.

Hence every finitely generated ideal of R is actually principal. However, the ideal J consisting of all subsets of $[0, 1]$ is not principal since it does not consist of all subsets of a proper subset of $[0, 1]$. Hence

1. R is a finitely generated free R -module.
2. J has a submodule R which is not finitely generated.

Definition 3.1 An R -module M is a **noetherian** R -module if all submodules of M (including M itself) are finitely generated. If R is commutative, R is a **noetherian ring** if it is a noetherian R -module, i.e. if all ideals of R are finitely generated.

Examples

1. If F is a field, then F is a noetherian ring. Also, if V is an F -module (i.e. an F -vector space), then V is finitely generated iff V is finite dimensional, in which case every subspace is finite dimensional (i.e. every submodule is finitely generated). So F -modules are finitely generated iff they are noetherian.

2. If R is a principal ideal domain, then R is a noetherian ring (e.g. $\mathbb{Z}, F[x]$). In fact, if R is a noetherian ring and M is a finitely generated R -module, then M is a noetherian R -module (see later). (Hence, in particular, taking $R = \mathbb{Z}$, it follows that every subgroup of a finitely generated abelian group is finitely generated.) Also, if R is a noetherian ring, then $R[x]$ is a noetherian ring (see later).

Proposition 3.2 If M is a noetherian R -module, then so is every submodule and quotient module of M .

Proof The submodule part is trivial. For quotients, suppose that N is a submodule of M , and let L be a submodule of M/N . Let $q : M \rightarrow M/N$ be the quotient map, and set $\bar{L} = q^{-1}(L)$. Then L is a submodule of M/N (easy exercise) and is thus finitely generated by a_1, a_2, \dots, a_n , say. Then $q(a_1), q(a_2), \dots, q(a_n)$ is a set of generators of L .

Definition 3.3 An R -module M satisfies the **ascending chain condition** if given any chain $N_1 \subset N_2 \subset \dots$ of submodules of M , $\exists r$ such that $N_s = N_r \forall s \geq r$.

Theorem 3.4 M is a noetherian R -module iff M satisfies the ascending chain condition.

Proof Let $N_1 \subset N_2 \subset \dots$ be a sequence of submodules of M . Let $N = \bigcup_{i=1}^{\infty} N_i$. This is a submodule of M and is thus finitely generated by a_1, a_2, \dots, a_s , say. Then $\exists r$ such that $a_1, a_2, \dots, a_s \in N_r$. Hence $N_r = N$, and so $N_r = N_{r+1} = \dots$. Conversely, let N be a submodule of M . Choose $a_1 \in N$, and let N_1 be the submodule generated by a_1 . Either $N = N_1$ (in which case we are done) or we can choose $a_2 \in N \setminus N_1$. Let $N_2 = \langle a_1, a_2 \rangle$. Continue this process if necessary. After, say, r steps, we have $N_r = N$, or we'll get an infinite ascending chain of submodules of M , which is a contradiction.

Proposition 3.5 If M is an R -module and N is a noetherian submodule and M/N is noetherian, then M is noetherian.

Proof Let $q : M \rightarrow M/N$ be the quotient map. Let $L_1 \subset L_2 \subset \dots$ be a chain of submodules of M . Then $L_1 \cap N \subset L_2 \cap N \subset \dots$ is a chain of submodules of N . $q(L_1) \subset q(L_2) \subset \dots$ is a chain of submodules of M/N . So $\exists r$ such that

$$\begin{cases} L_s \cap N = L_r \cap N & \forall s \geq r \\ q(L_s) = q(L_r) & \forall s \geq r. \end{cases}$$

Let $m \in L_s$ ($s \geq r$). Then $q(m) \in q(L_s) = q(L_r)$. Thus $m = x + y$, where $x \in L_r$, $y \in N$. Thus $y = m - x \in L_s \cap N = L_r \cap N \subseteq L_r$. Hence we have $m \in L_r$ also, and so $L_r = L_{r+1} = \dots$. Thus M is noetherian.

Corollary 3.6 If M and N are noetherian R -modules, then so is $M \oplus N$.

Proof Observe that $\frac{M \oplus N}{\{0\} \oplus N} \simeq M$ and apply Proposition 3.5.

Proposition 3.7 If R is a noetherian ring and M is a finitely generated R -module, then M is a noetherian module.

Proof Let $A \subset M$ be a set of generators of M with $A = \{a_1, a_2, \dots, a_m\}$, say. Then M is isomorphic to a quotient of the free R -module L generated by $\{a_1, a_2, \dots, a_m\}$. But $L \simeq R^m$, and R^m is noetherian. Hence M is noetherian.

Theorem 3.8 (Hilbert Basis Theorem) If R is a noetherian ring, then $R[x]$ is a noetherian ring.

Proof We first define some notation. An element of $R[x]$ will be written in the form $rx^n + \dots$, where “ \dots ” consists of *lower* powers of x . Let I be an ideal of $R[x]$. Define (for $n \geq 0$) $I_n = \{r \in R : \exists \text{ a polynomial } rx^n + \dots \in I\}$. Then each I_n is an ideal in R . Furthermore, $I_0 \subset I_1 \subset I_2 \subset \dots$ since if $rx^n + \dots \in I$, then $x(rx^n + \dots) = rx^{n+1} + \dots$ is also in I . Hence, as R is noetherian, $\exists N$ such that $I_N = I_{N+1} = \dots$. Since each I_n is finitely generated (as R is noetherian), we can find a finite set of generators $a_{n1}, a_{n2}, \dots, a_{nm_n}$ for I_n , $0 \leq n \leq N$.

For each a_{nm} , choose a polynomial $f_{nm}(x) = a_{nm}x^n + \dots$ in I . We claim that $\{f_{nm}(x) : 0 \leq n \leq N, 1 \leq m \leq m_n\}$ generates I . To prove this, choose $g(x) \in I$ with $g(x) = rx^p + \dots$. The proof is by induction on $p = \deg(g(x))$. If $p = 0$, then $r \in I_0$, and I_0 lies in the ideal J generated by $\{f_{nm}(x) | 0 \leq n \leq N, 1 \leq m \leq m_n\}$. So suppose that $p > 0$. Now $r \in I_p$ (and $I_p = I_N$ if $p > N$). Write $r = l_1 a_{p1} + l_2 a_{p2} + \dots + l_{m_p} a_{pm_p}$ ($l_i \in R$). Consider $h(x) = l_1 f_{p1} + l_2 f_{p2} + \dots + l_{m_p} f_{pm_p}$. Then $h(x) \in J$. If $p \leq N$, then $\deg(g(x) - h(x)) < \deg(g(x))$. Thus $g(x) - h(x) \in J$ by induction. Thus $g(x) \in J$. If $p > N$, then $\deg(g(x) - x^{p-N} h(x)) < \deg(g(x))$. Thus $g(x) - x^{p-N} h(x) \in J$ by induction. Thus $g(x) \in J$. It follows therefore that $J = I$, and so I is a finitely generated $R[x]$ -module.

Corollary 3.9 If R is a noetherian ring, then so is $R[x_1, x_2, \dots, x_n]$ for any $n \geq 1$.

Question Suppose we know that $R^m \simeq R^n$ is an R -module. Is $m = n$?

Chapter 4

Tensor Products and Alternating Products of Modules

Assume from now on the R is a *commutative* ring.

Suppose that L and M are R -modules, and let $\text{hom}_R(L, M)$ be the collection of R -homomorphisms $L \rightarrow M$. Then $\text{hom}_R(L, M)$ is itself an R -module in a natural way: $(\theta_1 + \theta_2)(l) = \theta_1(l) + \theta_2(l)$, $(r\theta)(l) = r\theta(l)$.

Basic Properties

1. Suppose that $L = L_1 \oplus L_2$, $\theta \in \text{hom}_R(L, M)$. Let $\theta_1(l_1) = \theta(l_1 \oplus 0)$, $\theta_2(l_2) = \theta(0 \oplus l_2)$ ($\forall l_i \in L_i$, $i = 1, 2$). Then $\theta_i \in \text{hom}_R(L_i, M)$ ($i = 1, 2$), and the map $\theta \mapsto (\theta_1, \theta_2)$ is an R -module isomorphism, i.e. $\text{hom}_R(L_1 \oplus L_2, M) \simeq \text{hom}_R(L_1, M) \oplus \text{hom}_R(L_2, M)$.
2. If $M = M_1 \oplus M_2$ and $\theta \in \text{hom}_R(L, M)$, we can write $\theta(l) = \theta(l)_1 \oplus \theta(l)_2$. Let $\theta_1(l) := \theta(l)_1$, $\theta_2(l) := \theta(l)_2$. Then $\theta_i \in \text{hom}_R(L, M_i)$ ($i = 1, 2$), and $\theta \in \text{hom}_R(L, M_1) \oplus \text{hom}_R(L, M_2)$.
3. Suppose that $\theta \in \text{hom}_R(R, M)$. Let $T_\theta = \theta(1)$. Then $T_{r(\theta)} = r\theta(1) = rT_\theta$. $T_{\theta_1 + \theta_2} = (\theta_1 + \theta_2)(1) = \theta_1(1) + \theta_2(1) = T_{\theta_1} + T_{\theta_2}$. Hence the map $\theta \mapsto T_\theta$ is an R -homomorphism $\text{hom}_R(R, M) \rightarrow M$. If $m \in M$, let $h(m)(r) = rm$. Check that the map $m \mapsto h(m)$ is an R -homomorphism $M \rightarrow \text{hom}_R(R, M)$. Also, the maps $\theta \mapsto T_\theta$ and $m \mapsto h(m)$ are inverse to one another. Thus $M \simeq \text{hom}_R(R, M)$.
4. It follows from (1)-(3) that $\text{hom}_R(R^m, R^n) \simeq R^{mn}$ ($m \times n$ -matrices with entries in R).

Definition 4.1 Suppose that L , M , and N are R -modules. A map $\theta : L \times M \rightarrow N$ is said to be an **R -bilinear mapping** if

1. $\theta(l_1 + l_2, m) = \theta(l_1, m) + \theta(l_2, m)$
2. $\theta(l, m_1 + m_2) = \theta(l, m_1) + \theta(l, m_2)$

$$3. \theta(rl, m) = r\theta(l, m) = \theta(l, rm).$$

So $\theta(rl, sm) = r\theta(l, sm) = sr\theta(l, m)$. $\theta(rl, sm) = s\theta(rl, m) = rs\theta(l, m)$. One may define R -multilinear mappings in a similar way.

Let $B_R(L, M; N)$ be the collection of all R -bilinear mappings $L \times M \rightarrow N$.

Basic Properties

1. $B_R(L, M; N)$ is an R -module in a natural way.
2. If $\theta \in B_R(L, M; N)$, set $\theta'(m, l) = \theta(l, m) \forall l \in L, m \in M$. Then $\theta' \in B_R(M, L; N)$ and $\theta \mapsto \theta'$ is an isomorphism. Hence $B_R(L, M; N) \simeq B_R(M, L; N)$.
3. $B_R(L_1 \oplus L_2, M; N) \simeq B_R(L_1, M; N) + B_R(L_2, M; N)$.
4. If $\theta \in B_R(L, M; N)$ and $l \in L$, then let $(T_l(\theta))(m) = \theta(l, m) \forall m \in M$. Then $T_l(\theta) \in \text{hom}_R(M, N)$. The map T^θ , given by $l \mapsto T_l(\theta)$, is in $\text{hom}_R(L, \text{hom}_R(M, N))$. The map given by $\theta \mapsto T^\theta$ is an R -homomorphism $B_R(L, M; N) \rightarrow \text{hom}_R(L, \text{hom}_R(M, N))$. Suppose that $J \in \text{hom}_R(L, \text{hom}_R(M, N))$. Let $S(J)(l, m) = J(l)(m) \forall l \in L, m \in M$. Then $S(J) \in B_R(L, M; N)$. The map $S : \text{hom}_R(L, \text{hom}_R(M, N)) \rightarrow B_R(L, M; N)$ is an R -homomorphism. T and S are inverse to each other. Thus $B_R(L, M; N) \simeq \text{hom}_R(L, \text{hom}_R(M, N))$. So $B_R(R, M; N) \simeq \text{hom}_R(R, \text{hom}_R(M, N)) \simeq \text{hom}_R(M, N)$.

Examples

1. Suppose that G is any abelian group (i.e. \mathbb{Z} -module) and that m and n are coprime integers. Let $\theta \in B_{\mathbb{Z}}(\mathbb{Z}_m \mathbb{Z}_n; G)$ (so $\theta : \mathbb{Z}_m \times \mathbb{Z}_n \rightarrow G$). $\exists r, s \in \mathbb{Z}$ such that $rm + sn = 1$. If $(h, k) \in \mathbb{Z}_m \times \mathbb{Z}_n$, then $\theta(h, k) = rm\theta(h, k) + sn\theta(h, k) = r\theta(mh, k) + s\theta(h, nk) = r\theta(0, k) + s\theta(h, 0) = 0$. Hence $B_{\mathbb{Z}}(\mathbb{Z}_m, \mathbb{Z}_n; G) = \{0\}$.
2. Suppose that G is a finite abelian group of order n . Let H be any abelian group. Suppose that $\theta \in B_{\mathbb{Z}}(G, H; \mathbb{Z})$. If $(g, h) \in G \times H$, then $n\theta(g, h)\theta(ng, h) = 0$. Thus $\theta(g, h) = 0$. So $B_{\mathbb{Z}}(G, H; \mathbb{Z}) = \{0\}$.
3. Suppose that R is a commutative ring and that J_1 and J_2 are ideals in R . Then $R/J_1, R/J_2$, and $R/(J_1 + J_2)$ are all R -modules. Observe that if $r + J_1 \in R/J_1$, then $r + J_1 = r(1 + J_1)$. Hence R/J_1 is generated by $1 + J_1$ (and similarly for R/J_2 and $R/(J_1 + J_2)$). Consider $B_R(R/J_1, R/J_2; R/(J_1 + J_2))$. If $\theta \in B_R(R/J_1, R/J_2; R/(J_1 + J_2))$, set $\alpha(\theta) = \theta(1 + J_1, 1 + J_2) \in R/(J_1 + J_2)$. The map α defined by $\theta \mapsto \alpha(\theta)$ is an R -homomorphism $B_R(R/J_1, R/J_2; R/(J_1 + J_2)) \rightarrow R/(J_1 + J_2)$. Now suppose that $r + (J_1 + J_2) \in R/(J_1 + J_2)$. Let $\beta_{r+(J_1+J_2)}(s + J_1, t + J_2) = rst + J_1 + J_2 \in R/(J_1 + J_2)$. Check that $\beta_{r+(J_1+J_2)}$ is well-defined in terms of r, s , and t . Check that $\beta_{r+(J_1+J_2)} \in B_R(R/J_1, R/J_2; R/(J_1 + J_2))$. The map $\beta : r + (J_1 + J_2) \mapsto \beta_{r+(J_1+J_2)}$ is an R -homomorphism $B_R(R/J_1, R/J_2; R/(J_1 + J_2)) \leftarrow R/(J_1 + J_2)$. Check that $\alpha\beta$ and $\beta\alpha$ are identity maps. So $B_R(R/J_1, R/J_2; R/(J_1 + J_2)) \simeq R/(J_1 + J_2)$.

Suppose that R is fixed and that M_1 and M_2 are R -modules. Suppose that $\theta \in B_R(M_1, M_2; N)$ for some R -module N . We seek an R -module $M_1 \otimes_R M_2$ and a bilinear map $\otimes_R : M_1 \times M_2 \rightarrow M_1 \otimes_R M_2$ such that $\forall \theta$ and $N, \exists!$ R -homomorphism $\tilde{\theta} : M_1 \otimes_R M_2 \rightarrow N$ such that $\tilde{\theta} \circ \otimes_R = \theta$:

Diagram

$$\begin{array}{ccc} M_1 \times M_2 & \xrightarrow{\theta} & N \\ \downarrow \otimes_R & \nearrow \tilde{\theta} & \\ M_1 \otimes_R M_2 & & \end{array}$$

Definition 4.2 A **tensor product** $M_1 \otimes M_2$ is an R -module with a bilinear map which solves the above problem.

We have to establish existence as well as uniqueness and properties. We obtain the properties of the tensor product from its definition and *not* from its construction.

Notation We write $m_1 \otimes_R m_2$ for $\otimes_R(m_1, m_2)$, $m_1 \in M_1, m_2 \in M_2$. So we have $rm_1 \otimes_R m_2 = m_1 \otimes_R rm_2 = r(m_1 \otimes_R m_2) \forall r \in R$.

Theorem 4.3 Suppose that $M_1 \otimes_R M_2$ and $M_1 \otimes'_R M_2$ are two tensor products. Then $\exists!$ isomorphism $J : M_1 \otimes_R M_2 \rightarrow M_1 \otimes'_R M_2$ such that $J(m_1 \otimes_R m_2) = m_1 \otimes'_R m_2$.

Proof

$$\begin{array}{ccccc} M_1 \times M_2 & \xrightarrow{id} & M_1 \times M_2 & \xrightarrow{id} & M_1 \times M_2 \\ \downarrow \otimes_R & & \downarrow \otimes'_R & & \downarrow \otimes_R \\ M_1 \otimes_R M_2 & \xrightarrow{\tilde{id}} & M_1 \otimes'_R M_2 & \xrightarrow{\tilde{id}'} & M_1 \otimes_R M_2 \end{array}$$

$\otimes'_R \circ id$ is bilinear, so $\exists!$ R -homomorphism $\tilde{id} : M_1 \otimes_R M_2 \rightarrow M_1 \otimes'_R M_2$ which makes the diagram commute. Similarly, $\exists!$ R -homomorphism $\tilde{id}' : M_1 \otimes'_R M_2 \rightarrow M_1 \otimes_R M_2$ which makes the diagram commute. Now consider

$$\begin{array}{ccc} M_1 \times M_2 & \xrightarrow{id} & M_1 \times M_2 \\ \downarrow \otimes_R & & \downarrow \otimes_R \\ M_1 \otimes_R M_2 & \dashrightarrow & M_1 \otimes_R M_2 \end{array}$$

$\exists!$ R -homomorphism making this diagram commute. This homomorphism must be the identity map (since this works). So $\tilde{id} \circ id' = \text{identity}$. Thus $J = \tilde{id}$ is the required isomorphism.

Theorem 4.4 Suppose that $T_1 : M_1 \rightarrow N_1$ and $T_2 : M_2 \rightarrow N_2$ are R -homomorphisms. Then $\exists!$ R -homomorphism $S : M_1 \otimes_R M_2 \rightarrow N_1 \otimes_R N_2$ such that $S(m_1 \otimes_R m_2) = T_1(m_1) \otimes_R T_2(m_2)$ $\forall m_1 \in M_1, m_2 \in M_2$.

Proof Consider the diagram

$$\begin{array}{ccc} M_1 \times M_2 & \xrightarrow{(T_1, T_2)} & N_1 \times N_2 \\ \downarrow \otimes_R & & \downarrow \otimes_R \\ M_1 \otimes_R M_2 & \xrightarrow{S} & N_1 \otimes_R N_2 \end{array}$$

The map $(m_1, m_2) \mapsto T_1(m_1) \otimes_R T_2(m_2)$ is bilinear. Hence, via the universal property of tensor products, we can complete the diagram uniquely.

Notation We write $T_1 \otimes_R T_2$ for the mapping S .

Theorem 4.5 $M_1 \otimes_R M_2 \simeq M_2 \otimes_R M_1$.

Proof Consider the following diagram:

$$\begin{array}{ccccc} M_1 \times M_2 & \longrightarrow & M_2 \times M_1 & \longrightarrow & M_1 \otimes M_2 \\ \downarrow \otimes_R & & \downarrow \otimes_R & & \downarrow \otimes_R \\ M_1 \otimes_R M_2 & \xrightarrow{j} & M_2 \otimes_R M_1 & \xrightarrow{k} & M_1 \otimes_R M_2 \end{array}$$

We have $k \circ j = \text{identity}$. Similarly $j \circ k = \text{identity}$. Hence j and k are isomorphisms, and $j(m_1 \otimes_R m_2) = m_2 \otimes_R m_1$.

Theorem 4.6 Suppose that L, M , and N are R -modules. Then $L \otimes_R (M \otimes_R N) \simeq (L \otimes_R M) \otimes_R N$.

Proof Let K be any R -module, and let γ be a trilinear map $\gamma : L \times M \times N \rightarrow K$. Suppose that $l \in L$ and let $T_l(m, n) = \gamma(l, m, n)$. Then $T_l \in B_R(M, N; K)$. So we have

$$\begin{array}{ccc} (l, m, n) & & (L, M, N) \xrightarrow{\gamma} K \\ \downarrow & & \downarrow \quad \nearrow J \\ (l, m \otimes_R n) & & L \times (M \otimes_R N) \end{array}$$

with J unique. We shall now show that J is a bilinear map.

1. First observe that for each fixed $l \in L$, the map $M \otimes_R N \rightarrow K$ given by $h \mapsto J(l, h)$ is an R -homomorphism.

2. Next suppose that $l_1, l_2 \in L$ and $r_1, r_2 \in R$. Let $z(m, n) = \gamma(r_1 l_1 + r_2 l_2, m, n) - r_1 \gamma(l_1, m, n) - r_2 \gamma(l_2, m, n)$. Then $z(m, n) = 0 \forall m, n \in N$.

$$\begin{array}{ccc} M \times N & \longrightarrow & K \\ \downarrow \otimes_R & \nearrow 0 & \\ M \otimes_R N & & \end{array}$$

Now the map $M \otimes_R N \rightarrow K$ given by $h \mapsto J(r_1 l_1 + r_2 l_2, h) - r_1 J(l_1, h) - r_2 J(l_2, h)$ also makes the diagram commute. Hence we have $J(r_1 l_1 + r_2 l_2, h) - r_1 J(l_1, h) - r_2 J(l_2, h) = 0 \forall h \in M \otimes_R N$. Now (1) and (2) imply that J is bilinear.

$$\begin{array}{ccc} L \times M \times N & \xrightarrow{\gamma} & K \\ \downarrow & \nearrow J & \\ L \times (M \otimes_R N) & \nearrow \tilde{J} & \\ \downarrow \otimes_R & & \\ L \otimes_R (M \otimes_R N) & & \end{array}$$

Hence there is a unique map \tilde{J} such that the diagram commutes. This shows that $L \otimes_R (M \otimes_R N)$ satisfies the universal property of trilinear maps:

$$\begin{array}{ccc} L \times M \times N & \xrightarrow{\gamma} & K \\ \downarrow & \nearrow \exists! \tilde{\gamma} & \\ L \otimes_R (M \otimes_R N) & & \end{array}$$

Similarly, one shows that $(L \otimes_R M) \otimes_R N$ has the same property. Now use an argument similar to that of Theorem 4.3 to conclude that $L \otimes_R (M \otimes_R N) \simeq (L \otimes_R M) \otimes_R N$.

Theorem 4.7 $M \otimes_R (N_1 \oplus N_2) \simeq (M \otimes_R N_1) \oplus (M \otimes_R N_2)$.

Proof Let $P : M \times (N_1 \oplus N_2) \rightarrow (M \times N_1) \oplus (M \times N_2) \rightarrow (M \otimes_R N_1) \oplus (M \otimes_R N_2)$ by $(m, n_1 \oplus n_2) \mapsto (m, n_1) \oplus (m, n_2) \mapsto (m \otimes_R n_1) \oplus (m \otimes_R n_2)$. Define $i_1 : M \times N_1 \rightarrow M \times (N_1 \oplus N_2)$ by $i_1(m, n_1) = (m, n_1 \oplus 0)$. Define i_2 similarly. Then $P \circ i_1 : M \times N_1 \rightarrow (M \otimes_R N_1) \oplus (M \otimes_R N_2)$ is bilinear.

$$\begin{array}{ccc} M \times N_1 & \xrightarrow{i_1} & M \times (N_1 \oplus N_2) \xrightarrow{P} & (M \otimes_R N_1) \oplus (M \otimes_R N_2) \\ \downarrow \otimes_R & & \downarrow \otimes_R & \downarrow \otimes_R \\ M \otimes_R N_1 & \xrightarrow{j_1} & (M \otimes_R N_1) \oplus (M \otimes_R N_2) & \end{array}$$

Hence via the universal mapping property, $\exists!$ R -homomorphism j_1 making the diagram commute.

Consider $k_1 : M \otimes_R N_1 \rightarrow (M \otimes_R N_1) \oplus (M \otimes_R N_2)$ defined by $k_1(h) = h \oplus 0$. Then k_1 makes the diagram commute, and so $k_1 = j_1$. Next let $b : M \times (N_1 \oplus N_2) \rightarrow K$ be a bilinear map, and consider the map $bi_1 : M \times N_1 \rightarrow K$. This map is bilinear, and so $\exists!$ R -homomorphism $l_1 : M \otimes_R N_1 \rightarrow K$ such that $bi_1 = l_1 \circ (\otimes_R)$. Similarly, $\exists!$ R -homomorphism $l_2 : M \otimes_R N_2 \rightarrow K$ such that $bi_2 = l_2 \circ (\otimes_R)$. Define $l : (M \otimes_R N_1) \oplus (M \otimes_R N_2) \rightarrow K$ by $l = l_1 + l_2$. Then $lP(m, n_1 \oplus n_2) = l[(m \otimes_R n_1) \oplus (m \otimes_R n_2)] = l_1(m \otimes_R n_1) + l_2(m \otimes_R n_2)$ (by the definition of l). In turn, $l_1(m \otimes_R n_1) + l_2(m \otimes_R n_2) = bi_1(m, n_1) + bi_2(m, n_2) = b(m, n_1 + n_2)$. So l makes the diagram commute. Finally, l is the only mapping with this property, for suppose that l' is another. Then $b(m, n_1 \oplus 0) = bi_1(m, n_1) = l_1(m \otimes_R n_1) = l'P(m, n_1 \oplus 0) = l'[(m \otimes_R n_1) \oplus 0] = l'j_1(m \otimes_R n_1) = l'j_1(m \otimes_R n_1)$. Hence $l'j_1 = l_1$. Similarly, $l'j_2 = l_2$. Now since $(x_1, x_2) \in (M \otimes_R N_1) \oplus (M \otimes_R N_2)$, $l(x_1, x_2) = l_1(x_1) + l_2(x_2) = l'j_1(x_1) + l'j_2(x_2) = l'(x_1, x_2)$, so $l = l'$.

Examples

1. Suppose that M and K are R -modules.

$$\begin{array}{ccc} R \times M & \xrightarrow{b} & K \\ \downarrow \otimes_R & \nearrow \tilde{b} & \\ M & & \end{array}$$

Observe that $b(r, m) = rb(1, m)$. Let $r \otimes_R m = rm$ ($r \in R, m \in M$). Define $\tilde{b}(m) = b(1, m)$. Then \tilde{b} is the unique R -homomorphism making the diagram commute. Hence $R \otimes_R M \simeq M$.

2. $R^m \otimes_R M = (R \oplus R \oplus \cdots \oplus R) \otimes_R M \simeq (R \otimes_R M) \oplus (R \otimes_R M) \oplus \cdots \oplus (R \otimes_R M)$ (m times) $\simeq M \oplus M \oplus \cdots \oplus M$ (m times) $= M^m$.
3. $R^m \otimes_R R^n \simeq R^{mn}$.

Explicitly Suppose that $r = (r_1, r_2, \dots, r_m) \in R^m$, i.e. $r = r_1e_1 + r_2e_2 + \cdots + r_me_m$, where e_i is the standard basis vector of R^m and $s = (s_1, s_2, \dots, s_n) \in R^n$, i.e. $s = s_1f_1 + s_2f_2 + \cdots + s_nf_n$, where f_i is the standard basis vector of R^n . Then $r \otimes_R s = \sum_{i,j} r_i s_j e_i \otimes_R f_j$.

R^m is freely generated by e_1, e_2, \dots, e_m . R^n is freely generated by f_1, f_2, \dots, f_n . $R^m \otimes_R R^n$ is freely generated by $\{e_i \otimes_R f_j : 1 \leq i \leq m, 1 \leq j \leq n\}$.

Note In general if M and N are R -modules, then \otimes_R does not map onto a submodule of $M \otimes_R N$. However, every element of $M \otimes_R N$ can be written in the form $x = \sum_{j=1}^k m_j \otimes_R n_j$ ($m_j \otimes_R n_j$ is called an elementary tensor). This is because the set $\mathcal{L} = \{\sum m_j \otimes_R n_j\}$ is a submodule of $M \otimes_R N$, and it satisfies the universal mapping property.

$$\begin{array}{ccc} M \times N & \xrightarrow{b} & K \\ \downarrow \otimes_R & \nearrow \tilde{b} & \\ \mathcal{L} & & \end{array}$$

Define $\tilde{b}(\sum_{j=1}^k m_j \otimes_R n_j) = \sum_{j=1}^k b(m_j, n_j)$. Hence Theorem 4.3 implies that the inclusion $\mathcal{L} \hookrightarrow M \otimes_R N$ is in fact an isomorphism.

Warning The representation is not unique in general.

4.1 Existence of the Tensor Product

Let S be the set $M \times N$. Let $R^{(S)}$ be the free R -module generated by S . So $R^{(S)}$ has basis $\{m \otimes n : m \in M, n \in N\}$ (notation). If $x \in R^{(S)}$, then we may write $x = \sum_{j=1}^k r_j m_j \otimes n_j$. Observe that $m_1 \otimes n + m_2 \otimes n \neq (m_1 + m_2) \otimes n$. Let K be the submodule of $R^{(S)}$ generated by the following set: $\{m_1 \otimes n + m_2 \otimes n - (m_1 + m_2) \otimes n, m \otimes n_1 + m \otimes n_2 - m \otimes (n_1 + n_2), (rm) \otimes n - r(m \otimes n), m \otimes (rn) - r(m \otimes n) \mid m_1, m_2, m \in M, n_1, n_2, n \in N, r \in R\}$.

Theorem 4.8 Let $q : R^{(S)} \rightarrow R^{(S)}/K$ be the quotient map. Let \otimes_R be defined by $m \otimes_R n = q(m \otimes n)$. Let $M \otimes_R N = R^{(S)}/K$. Then $M \otimes_R N$ is a tensor product of M and N .

Proof First observe that $\otimes_R : M \times N \rightarrow M \otimes_R N$ is bilinear. Let's take a look at an example: $(m_1 + m_2) \otimes n = q(m_1 \otimes n + m_2 \otimes n)$ (by construction of K) $= q(m_1 \otimes n) + q(m_2 \otimes n)$ (since q is a homomorphism) $= m_1 \otimes_R n + m_2 \otimes_R n$.

Next we note that if $x \in M \otimes_R N$, then we may write $x = \sum_{i=1}^k m_i \otimes_R n_i$ (since $R^{(S)}$ is freely generated by $\{m \otimes n : m \in M, n \in N\}$).

$$\begin{array}{ccc} M \times N & \xrightarrow{b} & L \\ \downarrow \otimes_R & \nearrow \tilde{b} & \\ M \otimes_R N & & \end{array}$$

Suppose that b is a bilinear map. Define $\tilde{b}(x) = \sum_{i=1}^k b(m_i, n_i)$. There are a few questions we need to answer:

1. Why is this well-defined?
2. Does it have the required properties?

Now since $R^{(S)}$ is *freely* generated over $\{m \otimes n\}$, \exists an R -homomorphism $\lambda : R^{(S)} \rightarrow L$ such that $\lambda(m \otimes n) = b(m, n)$. If x is any of K , then $\lambda(x) = 0$ (e.g. $\lambda((m_1 + m_2) \otimes n - m_1 \otimes n - m_2 \otimes n) = \lambda((m_1 + m_2) \otimes n) - \lambda(m_1 \otimes n) - \lambda(m_2 \otimes n) = b(m_1 + m_2, n) - b(m_1, n) - b(m_2, n) = 0$ (since λ is bilinear)). Hence if $y \in K$, then $\lambda(y) = 0$, so λ is constant on cosets of K . Define $\tilde{b}(w + K) = \lambda(w)$. Then $\tilde{b} : R^{(S)}/K \rightarrow L$ is an R -homomorphism. Furthermore, $\tilde{b}(m \otimes_R n) = \tilde{b}(q(m \otimes n)) = \lambda(m \otimes n + K) = \lambda(m \otimes n) = b(m, n)$. Hence the diagram commutes. Finally \tilde{b} is

unique, for suppose that \tilde{b}' were another R -homomorphism making the diagram commute. Then $\tilde{b}(m \otimes_R n) = \tilde{b}'(m \otimes_R n) \forall m \in M, \forall n \in N$. If $z \in M \otimes_R N$, with $z = \sum_{i=1}^k r_i m_i \otimes_R n_i$, then $\tilde{b}(z) = \sum_{i=1}^k r_i \tilde{b}(m_i \otimes_R n_i) = \sum_{i=1}^k r_i \tilde{b}'(m_i \otimes_R n_i) = \tilde{b}'(z)$.

Example and Exercise Suppose that R is a ring and I and J are ideals in R . Then R/I , R/J and $R/(I+J)$ are R -modules.

$$\begin{array}{ccc} (R/I) \times (R/J)^\theta & \xrightarrow{\quad} & N \\ \downarrow \beta & \nearrow \tilde{\theta} & \\ R/(I+J) & & \end{array}$$

Define β by $\beta(r+I, s+J) = rs + I + J$. Then β is bilinear, and $\beta(1+I, 1+J) = 1 + I + J$. Since θ is bilinear, we have $\theta(r+I, s+J) = rs[\theta(1+I, 1+J)]$. Define $\tilde{\theta} : R/(I+J) \rightarrow N$ by $\tilde{\theta}(t+I+J) = t\theta(1+I, 1+J)$.

1. Show that $\tilde{\theta}$ is well-defined.
2. Show that $\tilde{\theta}$ is the unique homomorphism which makes the diagram commute.

Hence $(R/I) \otimes_R (R/J) \simeq R/(I+J)$. If $I+J = R$, then $R/(I+J) = \{0\}$, e.g. if $(m, n) = 1$, then $(\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z}) = \{0\}$. If $(m, n) = h$, then $(\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/h\mathbb{Z}$.

Remark The notation $x \otimes_R y$ is ambiguous unless we specify the tensor product to which $x \otimes_R y$ belongs. Suppose M and N are R -modules with submodules M' and N' , respectively. Let $x \in M'$ and $y \in N'$. Then it can happen that $x \otimes_R y \in M \otimes_R N$ is zero while $x \otimes_R y \in M' \otimes_R N'$ is nonzero, e.g. take $R = \mathbb{Z}$, $M\mathbb{Z}$, $M' = 2\mathbb{Z}$, $N' = N = \mathbb{Z}/2\mathbb{Z}$. Let x be the nonzero element of N , and consider the element $2 \otimes_R x$. Then $2 \otimes_R x \in M \otimes_R N$ is zero since $2 \otimes_R x = 1 \otimes_R 2x = 1 \otimes_R 0 = 0$. However, $2 \otimes_R x \in M' \otimes_R N'$ is nonzero.

Proposition 4.9 Let $x_1, x_2, \dots, x_n \in M$ and $y_1, y_2, \dots, y_n \in N$ such that $\sum_{i=1}^n x_i \otimes_R y_i = 0$ (in $M \otimes_R N$). Then \exists finitely generated submodules M_0 and N_0 of M and N , respectively, such that $\sum_{i=1}^n x_i \otimes_R y_i = 0$ in $M_0 \otimes_R N_0$.

Proof Suppose that $\sum_{i=1}^n x_i \otimes_R y_i = 0$. Then (using the notation of the proof of Theorem 4.8) $\sum_{i=1}^n x_i \otimes y_i \in K \subseteq R^{(S)}$. Hence $\sum_{i=1}^n x_i \otimes y_i$ is a finite sum of generators of K . Let M_0 be the submodule of M generated by x_1, x_2, \dots, x_n and all elements of M which occur as “first coordinates” of these generators of K . Define N_0 similarly. Then $\sum_{i=1}^n x_i \otimes_R y_i = 0$ in $M_0 \otimes_R N_0$.

4.2 Restriction and Extension of Scalars

Definition 4.10 Let $f : R \rightarrow S$ be a ring homomorphism, and let N be an S -module. Then N has an R -module structure: If $r \in R, n \in N$, then $rn := f(r)n$. This R -module is said to be obtained

from N by **restriction of scalars**.

Proposition 4.11 Suppose that N is a finitely generated S -module and that S is a finitely generated R -module. Then N is a finitely generated R -module.

Proof Let y_1, y_2, \dots, y_n generate N over S , and let x_1, x_2, \dots, x_n generate S over R . Then $\{x_i y_j\}$ generate N over R . Now suppose that M is an R -module. Since S is an R -module, we may form the R -module $M_S := S \otimes_R M$. Now M_S carries an S -module structure such that $s(s' \otimes_R m) = ss' \otimes_R m \forall x, x' \in S, m \in M$. The S -module M_S is said to be obtained from M by **extension of scalars**.

Proposition 4.12 If M is finitely generated as an R -module, then M_S is finitely generated as an S -module.

Proof If x_1, x_2, \dots, x_n generates M over R , then $1 \otimes_R x_1, 1 \otimes_R x_2, \dots, 1 \otimes_R x_n$ generate M_S over S .

4.3 Exactness Properties of the Tensor Product

Product Suppose that M, N , and P are R -modules. Recall that we showed earlier that $B_R(M, N; P) \simeq \text{hom}_R(M, \text{hom}_R(N, P))$ (canonically). On the other hand, from the universal property of the tensor product, we have $B_R(M, N; P) \simeq \text{hom}_R(M \otimes_R N, P)$ (canonically). Hence we have a canonical isomorphism $\text{hom}_R(M \otimes_R N, P) \simeq \text{hom}_R(M, \text{hom}_R(N, P))$.

Proposition 4.13 Let $E^\bullet : 0 \rightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \rightarrow 0$ be an exact sequence of R -modules and homomorphisms, and suppose that N is any R -module. Then the sequence $E^\bullet \otimes_R N : M' \otimes_R N \xrightarrow{f \otimes_R 1} M \otimes_R N \xrightarrow{g \otimes_R 1} M'' \otimes_R N \rightarrow 0$ (where “1” denotes the identity mapping on N) is exact.

Proof Let P be any R -module. Since E^\bullet is exact, Proposition 2.17 implies that the sequence $\text{hom}_R(E^\bullet, \text{hom}_R(N, P))$ given by

$$0 \rightarrow \text{hom}_R(M'', \text{hom}_R(N, P)) \rightarrow \text{hom}_R(M, \text{hom}_R(N, P)) \rightarrow \text{hom}_R(M', \text{hom}_R(N, P))$$

is exact. So the sequence $\text{hom}_R(E^\bullet \otimes_R N, P)$ given by $0 \rightarrow \text{hom}_R(M'' \otimes_R N, P) \rightarrow \text{hom}_R(M \otimes_R N, P) \rightarrow \text{hom}_R(M' \otimes_R N, P)$ is exact. Now it follows from Proposition 2.17 that the sequence $M' \otimes_R N \rightarrow M \otimes_R N \rightarrow M'' \otimes_R N \rightarrow 0$ is exact, as asserted.

Remark It is *not* true in general that if $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$ is exact, then so is $M' \otimes_R N \rightarrow M \otimes_R N \rightarrow M'' \otimes_R N$ for an arbitrary R -module N , e.g. take $R = \mathbb{Z}$, and consider the exact sequence $0 \rightarrow \mathbb{Z} \xrightarrow{f} \mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow 0$, where $f(x) = 2x \forall x \in \mathbb{Z}$. Tensoring with

$N = \mathbb{Z}/2\mathbb{Z}$ gives a sequence $\mathbb{Z} \otimes_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z}) \xrightarrow{f \otimes_{\mathbb{Z}} 1} \mathbb{Z} \otimes_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z}) \rightarrow (\mathbb{Z}/2\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z}) \rightarrow 0$, and this is *not* exact because $f \otimes_{\mathbb{Z}} 1$ is not injective. $(f \otimes_{\mathbb{Z}} 1)(x \otimes_{\mathbb{Z}} y) = 2x \otimes_{\mathbb{Z}} y = x \otimes_{\mathbb{Z}} 2y = x \otimes_{\mathbb{Z}} 0 = 0$. But $\mathbb{Z} \otimes_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} \neq 0$.

Definition 4.14 Suppose that an R -module N satisfies the following property: Given any exact sequence

$$\cdots \rightarrow M_i \rightarrow M_{i+1} \rightarrow M_{i+2} \rightarrow \cdots$$

of R -modules, the sequence

$$\cdots \rightarrow M_i \otimes_R N \rightarrow M_{i+1} \otimes_R N \rightarrow M_{i+2} \otimes_R N \rightarrow \cdots$$

is also exact. Then N is said to be a **flat** R -module.

Proposition 4.15 Let N be an R -module. Then the following statements are equivalent:

1. N is flat.
2. If $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$ is any exact sequence of R -modules, the sequence $0 \rightarrow M' \otimes_R N \rightarrow M \otimes_R N \rightarrow M'' \otimes_R N \rightarrow 0$ is also exact.
3. If $f : M' \rightarrow M$ is injective, then $f \otimes_R 1 : M' \otimes_R N \rightarrow M \otimes_R N$ is also injective.
4. If $f : M' \rightarrow M$ is injective and M' and M are finitely generated, then $f \otimes_R 1 : M' \otimes_R N \rightarrow M \otimes_R N$ is injective.

Proof (1) and (2) are equivalent since any long exact sequence can be split into short exact sequences. (2) and (3) are equivalent by Proposition 4.13. It is clear that (3) implies (4). Thus we need to show that (4) implies (3). To do this, suppose that $f : M' \rightarrow M$ is injective, and let $u = \sum x_i \otimes_R y_i \in \ker(f \otimes_R 1)$. Then $\sum f(x_i) \otimes_R y_i = 0$ in $M \otimes_R N$. Let M'_0 be the submodule generated by the x_i s. Then $u_0 = \sum x_i \otimes_R y_i$ viewed as an element of $M'_0 \otimes_R N$. \exists a finitely generated submodule M_0 of M such that $f(M'_0) \subseteq M_0$ and $\sum f(x_i) \otimes_R y_i = 0$ as an element of $M_0 \otimes_R N$. So if $f_0 : M'_0 \rightarrow M_0$ is the restriction of f , then $(f_0 \otimes_R 1)(u_0) = 0$. M_0 and M'_0 are finitely generated, and so $f_0 \otimes_R 1$ is injective. This implies that $u_0 = 0$, and so $u = 0$.

Exercise Prove that if $f : R \rightarrow S$ is a ring homomorphism and M is a flat R -module, then $M_S := S \otimes_R M$ is a flat S -module.

4.4 Algebras

Suppose that $f : R \rightarrow S$ is a ring homomorphism. If $r \in R$ and $s \in S$, define a product $rs := f(r)s$. This makes S an R -module. Note that S also has a ring structure, and these two structures are compatible.

Definition 4.16 An R -algebra is a ring S together with a ring homomorphism $f : R \rightarrow S$.

Note

1. If R is a field K and $S \neq 0$, then f is injective. Hence K may be canonically identified with its image in S . So a K -algebra is a ring containing K as a subring.
2. Every ring (with identity) is a \mathbb{Z} -algebra.
3. Let $f : R \rightarrow S$, $g : R \rightarrow T$ be ring homomorphisms. An R -algebra homomorphism $h : S \rightarrow T$ is a ring homomorphism which is also an R -module homomorphism.

Definition 4.17 A ring homomorphism $f : R \rightarrow S$ is **finite** and S a **finite R -algebra** if S is finitely generated as an R -module.

Definition 4.18 We say that f is of **finite type** and that S is a **finitely generated R -algebra** if \exists a finite set $\{x_1, x_2, \dots, x_n\} \subseteq S$ such that every element of S can be written as a polynomial in x_1, x_2, \dots, x_n with coefficients in $f(R)$.

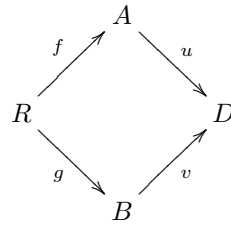
Aliter Thus if \exists an R -algebra homomorphism from $R[t_1, t_2, \dots, t_n]$ onto S .

Definition 4.19 A ring R is said to be **finitely generated** if it is finitely generated as a \mathbb{Z} -algebra. So $\exists x_1, x_2, \dots, x_n \in R$ such that every element of R can be written as a polynomial in the x_i s with coefficients in \mathbb{Z} .

4.5 Tensor Products of Algebras

Let A and B be two R -algebras, and let $f : R \rightarrow A$ and $g : R \rightarrow B$ be the corresponding homomorphisms. Consider the R -module $D := A \otimes_R B$. We define a multiplication on D as follows: Consider the mapping $A \times B \times A \times B \rightarrow D$, $(a, b, a', b') \mapsto aa' \otimes_R bb'$. This is R -linear in each factor, so it induces an R -homomorphism $A \otimes_R B \otimes_R A \otimes_R B \rightarrow D$, i.e. $D \otimes_R D \rightarrow D$. This in turn corresponds to an R -bilinear mapping $\mu : D \times D \rightarrow D$ such that $\mu(a \otimes_R b, a' \otimes_R b') = aa' \otimes_R bb'$. With this multiplication, D is a commutative ring with identity $1 \otimes_R 1$. Also, D is an R -algebra via

$r \mapsto f(r) \otimes_R g(r)$. \exists a commutative diagram



with $u(a) = a \otimes_R 1$ and $v(b) = 1 \otimes_R b$.

Proposition 4.20 Let M be a finitely generated R -module, and let I be an ideal of R . Suppose that $\phi : M \rightarrow M$ is an R -homomorphism such that $\phi(M) \subseteq IM$. Then ϕ satisfies an equation of the form $\phi^n + a_1\phi^{n-1} + \cdots + a_n = 0$, with $a_i \in I$.

Proof Let x_1, x_2, \dots, x_n be a set of generators of M . Then $\phi(x_i) \in IM$, so $\phi(x_i) = \sum_{j=1}^n a_{ij}x_j$ ($1 \leq i \leq n$, $a_{ij} \in I$), i.e. $\sum_{j=1}^n (\delta_{ij}\phi - a_{ij})x_j = 0$. Multiply the left-hand side by the adjoint of the matrix $(\delta_{ij}\phi - a_{ij})$. Then it follows that $\det(\delta_{ij}\phi - a_{ij})$ annihilates each x_{ij} . Thus $\det(\delta_{ij}\phi - a_{ij})$ is the zero endomorphism of n . Expand this to get the desired equation.

Corollary 4.21 Let M be a finitely generated R -module, and suppose that I is an ideal of R such that $IM = M$. Then $\exists x \in R$ such that $x \equiv 1 \pmod{I}$ with $xM = 0$.

Proof Take ϕ as the identity in Proposition 4.20. Then $x = 1 + a_1 + \cdots + a_n$.

Recall The Jacobson radical \mathcal{R} of R is the intersection of all maximal ideals in R .

Proposition 4.22 (Nakayama's Lemma) Let M be a finitely generated R -module and I an ideal of R contained in \mathcal{R} . Then if $IM = M$, then $M = 0$.

Proof

- 1st proof Corollary 4.21 implies that $xM = 0$ for some $x \equiv 1 \pmod{I}$. Proposition 1.24 implies that x is a unit in R since $1 - (1 - x) \in Rx$. So $M = x^{-1}xM = 0$.
- 2nd proof Suppose that $M \neq 0$, and let u_1, u_2, \dots, u_n be a minimal set of generators of M . Then $u_n \in IM$, so we have an equation of the form $u_n = a_1u_1 + a_2u_2 + \cdots + a_nu_n$, $a_i \in I \subseteq \mathcal{R}$. Thus $(1 - a_n)u_n = a_1u_1 + a_2u_2 + \cdots + a_{n-1}u_{n-1}$. But $a_n \in \mathcal{R}$, so $1 - a_n$ is a unit, which is a contradiction.

Corollary 4.23 Let M be a finitely generated R -module, N a submodule of M , and $I \subseteq \mathcal{R}$. Then $M = IM + N$ implies that $M = N$.

Proof Apply Proposition 4.22 to M/N . (Note that $I(M/N) = (IM + N)/N$).

Now suppose that R is a local ring with maximal ideal \mathfrak{m} and residue field $k = R/\mathfrak{m}$. Suppose that M is a finitely generated R -module. Then $M/\mathfrak{m}M$ is a finite dimensional k -vector space.

Proposition 4.24 Let x_i ($1 \leq i \leq n$) be elements of M whose images in $M/\mathfrak{m}M$ form a basis of this k -vector space. Then the x_i s generate M .

Proof Let N be the submodule of M generated by the x_i . The map $N \rightarrow M \rightarrow M/\mathfrak{m}M$ is surjective. Thus $M + \mathfrak{m}M = M$, whence $N = M$ by Corollary 4.23.

4.6 Exterior Powers

Suppose that R is a commutative ring and M is an R -module. Then $(M \otimes_R M) \otimes_R M \simeq M \otimes_R (M \otimes_R M)$, i.e. we can form “repeated tensor products.” Let K_n be the submodule of $M \otimes_R M \otimes_R \cdots \otimes_R M$ (n times) generated by the set $\{m_1 \otimes_R m_2 \otimes_R \cdots \otimes_R m_n \mid m_1, m_2, \dots, m_n \in M \text{ and } m_i = m_j \text{ for some } i \neq j\}$. Write $q_n : M \otimes_R M \otimes_R \cdots \otimes_R M \rightarrow (M \otimes_R M \otimes_R \cdots \otimes_R M)/K_n$ for the quotient map.

Definition 4.25 The n^{th} exterior power $\Lambda^n M$ is defined by $\Lambda^n M = (M \otimes_R M \otimes_R \cdots \otimes_R M)/K_n$. We write $t_1 \wedge t_2 \wedge \cdots \wedge t_n$ for $q_n(t_1 \otimes_R t_2 \otimes_R \cdots \otimes_R t_n)$ ($t_i \in M$).

Remark Observe that we have $0 = m_1 \wedge m_2 \wedge \cdots \wedge (a+b) \wedge \cdots \wedge (a+b) \wedge \cdots \wedge m_n = m_1 \wedge m_2 \wedge \cdots \wedge a \wedge \cdots \wedge b \wedge \cdots \wedge m_n + m_1 \wedge m_2 \wedge \cdots \wedge b \wedge \cdots \wedge a \wedge \cdots \wedge m_n$, where the specially marked terms are in the i^{th} and j^{th} positions, respectively. (All the other terms cancel.) So $m_1 \wedge m_2 \wedge \cdots \wedge a \wedge \cdots \wedge b \wedge \cdots \wedge m_n = -m_1 \wedge m_2 \wedge \cdots \wedge b \wedge \cdots \wedge a \wedge \cdots \wedge m_n$, i.e. $m_1 \wedge m_2 \wedge \cdots \wedge m_n = -m_{\tau(1)} \wedge m_{\tau(2)} \wedge \cdots \wedge m_{\tau(n)}$, where τ is any transposition in S_n . Hence if $\sigma \in S_n$ and $\epsilon(\sigma)$ is the signature of σ , then we have $m_1 \wedge m_2 \wedge \cdots \wedge m_n = \epsilon(\sigma) m_{\sigma(1)} \wedge m_{\sigma(2)} \wedge \cdots \wedge m_{\sigma(n)}$.

Examples

1. For any M $\Lambda^1 M = M$.
2. $\Lambda^2(\mathbb{Z}/2\mathbb{Z}) = 0$. This is because a generator of $\mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_2$ is $1 \otimes_{\mathbb{Z}} 1$. But $\langle 1 \otimes_{\mathbb{Z}} 1 \rangle$ is the submodule factored out to get $\Lambda^2(\mathbb{Z}/2\mathbb{Z})$.

3. Similarly, $\Lambda^r V = 0$ if V is an F -vector space of dimension $n < r$, for if e_1, e_2, \dots, e_n is a basis of V , then $\Lambda^r(V)$ is spanned by elements of the form $e_{i_1} \wedge e_{i_2} \wedge \dots \wedge e_{i_r}$. Since $r > n$, at least two of the e_i s are equal, and so $e_{i_1} \wedge e_{i_2} \wedge \dots \wedge e_{i_r} = 0$. (Similarly, $\Lambda^r M = 0$ for any R -module M which is generated by a set of order less than r .)
4. Let V be an \mathbb{R} -vector space of dimension 3. Then $\Lambda^2 V$ has dimension 3, for let e_1, e_2, e_3 be a basis of V . Then $V \otimes_{\mathbb{R}} V$ has a basis of V . Then $V \otimes_{\mathbb{R}} V$ has dimension 9 with basis $\{e_1 \otimes_{\mathbb{R}} e_j \mid 1 \leq i, j \leq 3\}$. To get $\Lambda^2 V$, factor out the submodule generated by all elements of the form $u \otimes_{\mathbb{R}} u$. So $e_i \wedge e_j = 0$, and also $e_i \wedge e_j = -e_j \wedge e_i$ if $i \neq j$. So a basis of $\Lambda^2 V$ is $e_1 \wedge e_2, e_1 \wedge e_3, e_2 \wedge e_3$.

Theorem 4.26 Let M be a finitely generated free R -module with basis a_1, a_2, \dots, a_n . Then

$$\Lambda^r M \begin{cases} 0 & \text{if } r > n \\ \text{is free with basis } B = \{a_{i_1} \wedge a_{i_2} \wedge \dots \wedge a_{i_r} \mid 1 \leq i_1 < i_2 < \dots < i_r \leq n\} & \text{if } 1 \leq r \leq n. \end{cases}$$

Proof The result is trivial for $r > n$. Suppose that $1 \leq r \leq n$. It is clear that the set of all $a_{i_1} \wedge a_{i_2} \wedge \dots \wedge a_{i_r}$ (any choice of integers i_1, i_2, \dots, i_r) span $\Lambda^r M$. Hence such an element is zero if two indices are equal and otherwise can be written in the form $a_{j_1} \wedge a_{j_2} \wedge \dots \wedge a_{j_r}$, where $j_1 < j_2 < \dots < j_r$ by permuting and multiplying by the signature of the permutation. To show linear independence, suppose if possible that $\lambda_1 b_1 + \lambda_2 b_2 + \dots + \lambda_t b_t = 0$, where each $\lambda_i \in R$, $\lambda_i \neq 0$, and each $b_i \in B$. Suppose that $b_i = a_{i_1} \wedge a_{i_2} \wedge \dots \wedge a_{i_r}$, $i_1 < i_2 < \dots < i_r$. Define a homomorphism $\phi : \underbrace{M \otimes_R M \otimes_R \dots \otimes_R M}_{r \text{ times}} \rightarrow R$ by

$$\phi(a_{j_1} \otimes_R a_{j_2} \otimes_R \dots \otimes_R a_{j_r}) = \begin{cases} \epsilon(\sigma) & \text{if } (j_1, j_2, \dots, j_r) = \sigma(i_1, i_2, \dots, i_r), \sigma \in S_r, \\ 0 & \text{otherwise.} \end{cases}$$

extended linearly. Then $\phi(m_1 \otimes_R m_2 \otimes_R \dots \otimes_R m_r) = 0$ if any two of the m_i s are equal. So ϕ induces a homomorphism $\bar{\phi} : \Lambda^r M \rightarrow R$ such that $\bar{\phi}(a_{i_1} \wedge a_{i_2} \wedge \dots \wedge a_{i_r}) = 1$. Then $0 = \bar{\phi}(\lambda_1 b_1 + \lambda_2 b_2 + \dots + \lambda_t b_t)$, i.e. $0 = \lambda_1$ since $\bar{\phi}(b_2) = \bar{\phi}(b_3) = \dots = \bar{\phi}(b_t) = 0$ by construction, which is a contradiction. So the elements of B are linearly independent.

Proposition 4.27 (c.f. Theorem 4.4) Let M and N be R -modules, and let $f : M \rightarrow N$ be a homomorphism. Then \exists homomorphisms $\Lambda^r f : \Lambda^r M \rightarrow \Lambda^r N \forall r$ such that

1. Given also a homomorphism $g : N \rightarrow P$, we have that $\Lambda^r(g \circ f) = (\Lambda^r g) \circ (\Lambda^r f)$.
2. If f is an isomorphism, then $\Lambda^r f$ is an isomorphism $\forall r$.

Proof

1. Theorem 4.4 implies that for each $r \geq 1$, f induces a homomorphism $\bar{f} : M \otimes_R M \otimes_R \dots \otimes_R M \rightarrow N \otimes_R N \otimes_R \dots \otimes_R N$ (r times) such that $\bar{f}(m_1 \otimes_R m_2 \otimes_R \dots \otimes_R m_r) = f(m_1) \otimes_R f(m_2) \otimes_R \dots \otimes_R f(m_r)$. Clearly \bar{f} maps $K_r(M)$ to $K_r(N)$. Hence \bar{f} induces a map $\Lambda^r f : \Lambda^r M \rightarrow \Lambda^r N$, where $(\Lambda^r f)(m_1 \wedge m_2 \wedge \dots \wedge m_r) = f(m_1) \wedge f(m_2) \wedge \dots \wedge f(m_r)$.

2. Let $g : N \rightarrow M$ be the inverse isomorphism of f . Then $\Lambda^r(f) \circ \Lambda^r(g) = \Lambda^r(gf)$ (from (1))
 $= \Lambda^r(id) = id$. Similarly, $\Lambda^r(g) \circ \Lambda^r(f) = \Lambda^r(fg) = \Lambda^r(id) = id$, and hence $\Lambda^r(f)$ is an isomorphism $\forall r$.

Theorem 4.28 Let M and N be free, finitely generated R -modules ($R \neq 0$) with $M \simeq N$. Suppose that a_1, a_2, \dots, a_m is a basis of M and that b_1, b_2, \dots, b_n is a basis of N . Then $m = n$.

Proof Clearly $M \simeq R^m$ and $N \simeq R^n$. Hence $R^m \simeq R^n$. Suppose if possible that $m > n$. Then $R \simeq \Lambda^m(R^m)$ (via Theorem 4.26) $\simeq \Lambda^m(R^n)$ (via Proposition 4.27) $= 0$, which is a contradiction. Hence $m = n$. Hence *every* basis of M has m elements in it. This number m is called the **rank** of M . (This generalizes the notion of **dimension** of a vector space.)

Remark It follows from Theorem 4.26 that the rank of $\Lambda^r M$ is $\binom{n}{r}$ ($1 \leq r \leq n$) if M is free of rank n .

Definition 4.29 Let M and N be R -modules. A function $f : \underbrace{M \times M \times \dots \times M}_{r \text{ times}} \rightarrow N$ is an **alternating map** if

1. It is a homomorphism in each variable separately (i.e. “ f is r -linear”).
2. $f(m_1, m_2, \dots, m_r) = 0$ if any two m_i s are equal

Theorem 4.30 \exists a one-to-one correspondence between alternating maps $\underbrace{M \times M \times \dots \times M}_{r \text{ times}} \rightarrow N$ and R -homomorphisms $\Lambda^r M \rightarrow N$.

Proof Suppose that $f : M \times M \times \dots \times M \rightarrow N$ is an alternating map. Then $\exists!$ map $\tilde{f} : M \otimes_R M \otimes_R \dots \otimes_R M \rightarrow N$ such that the following diagram commutes:

$$\begin{array}{ccc} M \times M \times \dots \times M & \xrightarrow{f} & N \\ \downarrow \otimes_R & \searrow \tilde{f} & \\ M \otimes_R M \otimes_R \dots \otimes_R M & & \end{array}$$

Since f is alternating, $\tilde{f}(K_r(M)) = 0$. Hence \tilde{f} induces an R -homomorphism $\bar{f} : \Lambda^r M \rightarrow N$. Conversely, given $g : \Lambda^r M \rightarrow N$, define $\tilde{g} : M \times M \times \dots \times M \rightarrow N$ by $\tilde{g}(m_1, m_2, \dots, m_r) = g(m_1 \wedge m_2 \wedge \dots \wedge m_r)$. Then \tilde{g} is alternating.

Definition 4.31 Let M be a free R -module of rank n , say, and let $f : M \rightarrow N$ be a homomorphism. Then $\Lambda^n M$ is free of rank 1, and so $\Lambda^n f : \Lambda^n M \rightarrow \Lambda^n M$ is multiplication by an element of R . This element is called the **determinant** of f , i.e. if $x \in \Lambda^n M$, then $(\Lambda^n f)(x) = (\det f)x$ or for $m_1, m_2, \dots, m_n \in M$, we have that $f(m_1) \wedge f(m_2) \wedge \dots \wedge f(m_n) = (\det f)(m_1 \wedge m_2 \wedge \dots \wedge m_n)$.

Proposition 4.32

1. If f is the identity morphism, then $\det(f) = 1$.
2. If $g : M \rightarrow M$ is another homomorphism, then $\det(fg) = (\det f)(\det g)$.
3. If f is an isomorphism, then $\det(f)$ is in the group of units of R .

Proof

1. $\Lambda^n(id)$ is the identity map on $\Lambda^n(M)$.
2. This follows from the fact that $\Lambda^n(fg)\Lambda^n(f)\Lambda^n(g)$.
3. Let g be the inverse of f . Then $(\det g)(\det f) = \det(gf) = \det(id) = 1$.

Proposition 4.33 Let a_1, a_2, \dots, a_n be a basis of a finitely generated free R -module M . Let $f : M \rightarrow M$ be a homomorphism, and let $f(a_j) = \sum_i r_{ij}a_i$ ($r_i \in R$) (i.e. (r_{ij}) is the matrix of f with respect to this basis). Then $\det f = \sum_{\sigma \in S_n} \epsilon(\sigma)r_{\sigma(1)1}r_{\sigma(2)2} \cdots r_{\sigma(n)n}$.

Proof $\Lambda^n f(a_1 \wedge a_2 \wedge \cdots \wedge a_n) = f(a_1) \wedge f(a_2) \wedge \cdots \wedge f(a_n) = (\sum_{i_1} r_{i_1 1} a_{i_1}) \wedge (\sum_{i_2} r_{i_2 2} a_{i_2}) \wedge \cdots \wedge (\sum_{i_n} r_{i_n n} a_{i_n}) = \sum_{i_1, i_2, \dots, i_n} r_{i_1 1} r_{i_2 2} \cdots r_{i_n n} (a_{i_1} \wedge a_{i_2} \wedge \cdots \wedge a_{i_n}) = \sum_{\sigma \in S_n} \epsilon(\sigma) r_{\sigma(1)1} r_{\sigma(2)2} \cdots r_{\sigma(n)n} (a_1 \wedge a_2 \wedge \cdots \wedge a_n)$ because if i_1, i_2, \dots, i_n is not a permutation of $1, 2, \dots, n$, then $a_{i_1} \wedge a_{i_2} \wedge \cdots \wedge a_{i_n} = 0$, but if $\{i_1, i_2, \dots, i_n\} = \sigma\{1, 2, \dots, n\}$ ($\sigma \in S_n$), then $a_{i_1} \wedge a_{i_2} \wedge \cdots \wedge a_{i_n} = \epsilon(\sigma) a_1 \wedge a_2 \wedge \cdots \wedge a_n$.

Notation Suppose that M is a finitely generated free R -module of rank n and that $x \in \Lambda^r M$ and $y \in \Lambda^{n-r} M$. Then $x = \sum_i x_i$, where each x_i is of the form $m_1 \wedge m_2 \wedge \cdots \wedge m_r$, and $y = \sum_i y_i$, where each y_i is of the form $m_{r+1} \wedge m_{r+2} \wedge \cdots \wedge m_n$. We write $x \wedge y$ for $\sum_{i,j} x_i \wedge y_j$ in $\Lambda^n M$, where $(m_1 \wedge m_2 \wedge \cdots \wedge m_r) \wedge (m_{r+1} \wedge m_{r+2} \wedge \cdots \wedge m_n) = m_1 \wedge m_2 \wedge \cdots \wedge m_n$.

Observe that if $f : M \rightarrow M$ is an R -homomorphism, then $[(\Lambda^r f)(x)] \wedge [(\Lambda^{n-r} f)(y)] = \Lambda^n(f)(x \wedge y)$.

Proposition 4.34 Suppose that $x \in \Lambda^r M$. Then the values of $x \wedge y \in \Lambda^n M$ for all $y \in \Lambda^{n-r} M$ determine x .

Proof Let a_1, a_2, \dots, a_n be a basis of M . Let $x = \sum_i r_i x_i$, where $r_i \in R_i$ and each x_i is of the form $a_{i_1} \wedge a_{i_2} \wedge \cdots \wedge a_{i_r}$, where $1 \leq i_1 < i_2 < \cdots < i_r \leq n$. Consider the coefficient r_k of $x_k = a_{k_1} \wedge a_{k_2} \wedge \cdots \wedge a_{k_r}$. Let $y = a_{j_1} \wedge a_{j_2} \wedge \cdots \wedge a_{j_{n-r}}$, where $1 \leq j_1 < j_2 < \cdots < j_{n-r} \leq n$ and no k is equal to a j . Then $x \wedge y = \sum_i r_i (x_i \wedge y) = r_k (x_k \wedge y) = \pm (a_1 \wedge a_2 \wedge \cdots \wedge a_n)$. This determines $r_k \forall k$ and hence also x .

Corollary 4.35 \exists a one-to-one correspondence between homomorphisms $\Lambda^r M \rightarrow \Lambda^r M$ and $\Lambda^{n-r} M \rightarrow \Lambda^{n-r} M$.

Proof Given $f : \Lambda^r M \rightarrow \Lambda^r M$, define $\bar{f} : \Lambda^{n-r} M \rightarrow \Lambda^{n-r} M$ by $x \wedge \bar{f}(y) = f(x) \wedge y$, $x \in \Lambda^r M$ ($y \in \Lambda^{n-r} M$). By the proof of Proposition 4.34, this determines $\bar{f}(y)$. Now \bar{f} is a homomorphism since e.g. $x \wedge \bar{f}(y_1 + y_2) = f(x) \wedge (y_1 + y_2) = f(x) \wedge y_1 + f(x) \wedge y_2 = x \wedge \bar{f}(y_1) + x \wedge \bar{f}(y_2) = x \wedge (\bar{f}(y_1) + \bar{f}(y_2))$. Since this is true $\forall x \in \Lambda^r M$, it follows that $\bar{f}(y_1 + y_2) = \bar{f}(y_1) + \bar{f}(y_2)$. Similarly, $\bar{f}(sy) = s\bar{f}(y) \forall s \in R, y \in \Lambda^{n-r} M$. Since the process $f \mapsto \bar{f}$ is clearly reversible, it is a one-to-one correspondence.

Proposition 4.36 Let $f : M \rightarrow M$ be an R -homomorphism. Let $\Lambda_*^r f : \Lambda^r M \rightarrow \Lambda^r M$ be the homomorphism corresponding to $\Lambda^{n-r} f : \Lambda^{n-r} M \rightarrow \Lambda^{n-r} M$ via Corollary 4.35 (i.e. if $x \in \Lambda^r M$ and $y \in \Lambda^{n-r} M$, then $[\Lambda_*^r f(x)] \wedge y = x \wedge (\Lambda^{n-r} f(y))$). Then $(\Lambda_*^r f)(\Lambda^r f) = (\det f) \cdot id$.

Proof Suppose that $x \in \Lambda^r M$ and $y \in \Lambda^{n-r} M$. Then $[(\Lambda_*^r f \cdot \Lambda^r f)x] \wedge y = (\Lambda^r f)(x) \wedge (\Lambda^{n-r} f)(y) = (\Lambda^n f)(x \wedge y) = (\det f)(x \wedge y) = [(\det f)x] \wedge y$. This is true $\forall y \in \Lambda^{n-r} M$. Hence, by Proposition 4.34, we have $(\Lambda_*^r f \cdot \Lambda^r f)x = (\det f)x$. This is true $\forall x \in \Lambda^r M$, and so $\Lambda_*^r f \cdot \Lambda^r f = (\det f)id$.

Corollary 4.37 If $\det f \in$ group of units of R , then f is an isomorphism.

Proof Let $g : (\det f)^{-1} \Lambda_*^1 f : M \rightarrow M$. Then $g \cdot f = id$ by Proposition 4.36. Hence f is one-to-one, and g is onto. Since $g \cdot f = id$, we have that $(\det g)(\det f) = 1$, and so $\det g \in$ group of units of R . A similar argument shows that g is one-to-one. Therefore g is an isomorphism, and so f is an isomorphism.

Chapter 5

Finitely Generated Modules Over a Euclidean Domain

Definition 5.1 An integral domain R is **Euclidean** if \exists a function $d : R \rightarrow \mathbb{Z}$ such that

1. $d(x) > d(0) \forall x \neq 0$;
2. If $x \neq 0$ and $y \in R$, then $y = xq + r$, with $d(r) < d(x)$.

If R is a Euclidean domain, then R is a principal ideal domain.

Definition 5.2 Let A and A' be $m \times n$ matrices over a Euclidean domain R . Then A and A' are said to be **equivalent** if \exists an $m \times n$ matrix B and an $m \times n$ matrix C , both invertible, such that $A' = BAC$. (This is plainly an equivalence relation.)

Observe that B is invertible iff B represents a homomorphism $R^m \rightarrow R^m$ which is an isomorphism iff $\det B \in$ group of units of R .

Lemma 5.3 Let A be an $m \times n$ matrix over R . Then A is equivalent to a matrix of the form

$$\begin{bmatrix} r_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & r_2 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 0 & \ddots & 0 & 0 & \ddots & 0 \\ 0 & 0 & \cdots & r_s & 0 & \cdots & 0 \\ 0 & 0 & \ddots & 0 & 0 & \ddots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{bmatrix},$$

where r_1, r_2, \dots, r_s are nonzero elements in R and $s \geq 0$.

Proof First note that we have elementary row and column operations of the following forms:

1. Exchange the i^{th} and j^{th} rows or columns.
2. Replace the i^{th} row or column by $(i^{\text{th}} \text{ row or column}) + r(j^{\text{th}} \text{ row or column})$ for some $r \in R$.

Each of these corresponds to pre-multiplying or post-multiplying A by invertible matrices and so gives an invertible matrix.

Replace A by an equivalent matrix with the property that $\min_{a_{ij}=0} d(a_{ij})$ is as small as possible. Then arrange for this minimum to be attained by a_{11} using operations of type (1). Now consider a_{ij} ($j > 1$). Write $a_{ij} = a_{11}q + r$, where $d(r) < d(a_{11})$. If we were to replace the j^{th} column by $(j^{\text{th}} \text{ column}) - q(1^{\text{st}} \text{ column})$, we'd get an equivalent matrix with a_{1j} replaced by r . Since $d(r) < d(a_{11}) = \text{minimum possible}$, we must have $r = 0$, i.e. $a_{11} \mid a_{1j}$. Similarly, $a_{11} \mid a_{i1}$ for each $i > 1$. Now use row and column operators to make $a_{1j} = 0$ and $a_{i1} = 0 \forall i, j > 1$. Then consider the matrix B which is A without the first row and column. Repeat the process on B .

Remarks

1. It is possible to arrange for $r_1 \mid r_2, r_2 \mid r_3, \dots$. To prove this, assume that, amongst equivalent diagonal forms, $d(r_1)$ is minimal. If, say, r_1 and r_2 , then write $r_2 = r_1q + r$, with $d(r) < d(r_1)$. Now use operations of type (2) above to replace r_2 by r . But now the matrix is no longer diagonal. Now diagonalize the matrix as before: $d(\text{new } r_1) \leq d(r) < d(r_1)$. This is a contradiction unless $r = 0$.
2. In fact, the same results hold if R is just a principal ideal domain. (Replace $d(r)$ be the **length** $l(r) = \text{the number of irreducibles (primes) in the unique factorization of } r$.)

Definition 5.4 An R -module M is **cyclic** if it is generated by a single element, m , say.

Note Suppose that $I = \{r \in R : rm = 0\}$. Let $\theta : R \rightarrow M$ be given by $\theta(r) = rm$. Then θ is onto, and $\ker \theta = I$. So I is an ideal, and $M \simeq R/I$. Since R is a principal ideal domain, $\exists r \in R$ such that $I = (r)$, and so in fact $M \simeq R/(r)$ and $M \simeq R$ if $r = 0$.

Theorem 5.5 If R is a Euclidean domain and M is a finitely generated R -module, then \exists cyclic R -modules M_1, M_2, \dots, M_n such that $M \simeq M_1 \oplus M_2 \oplus \dots \oplus M_n$.

Proof By Proposition 2.15, we can write $M \simeq L/K$, where L is a free R -module of rank n , say. By Proposition 3.7, since R is a principal ideal domain, L is noetherian, and so K is finitely generated. Let l_1, l_2, \dots, l_n be a basis of L and let k_1, k_2, \dots, k_m be a generating set for K (the k s don't necessarily form a basis for K). Write $b_i = \sum_{j=1}^n a_{ij}l_j$ (some $a_{ij} \in R$), i.e. $\tilde{k} = A\tilde{l}$, where

$$\tilde{k} = \begin{pmatrix} k_1 \\ k_2 \\ \vdots \\ k_m \end{pmatrix}, \quad \tilde{l} = \begin{pmatrix} l_1 \\ l_2 \\ \vdots \\ l_n \end{pmatrix}, \quad A = (a_{ij}).$$

By Lemma 5.3, \exists invertible matrices B and C such that

$$BAC = \begin{bmatrix} r_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & r_2 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 0 & \ddots & 0 & 0 & \ddots & 0 \\ 0 & 0 & \cdots & r_s & 0 & \cdots & 0 \\ 0 & 0 & \ddots & 0 & 0 & \ddots & 0 \end{bmatrix}$$

($s \geq 0$, r_s nonzero). Let $\tilde{k}' = B\tilde{k}$, $\tilde{l}' = C^{-1}\tilde{l}$. Then $\tilde{k}' = BA\tilde{l} = (BAC)\tilde{l}'$. Since B and C are invertible, we have that \tilde{k}' generates K and \tilde{l}' is a basis of L . We have $k'_1 = r_1l'_1$, $k'_2 = r_2l'_2$, \dots , $k'_s = r_sl'_s$, $k'_{s+1} = k'_{s+2} = \dots = k'_m = 0$. Now define $\theta : L \rightarrow R/(r_1) \oplus R/(r_2) \oplus \dots \oplus R/(r_s) \oplus R \oplus R \oplus \dots \oplus R$ (total of n factors) by $\theta(a_1l'_1 + a_2l'_2 + \dots + a_nl'_n) = ([a_1], \dots, [a_s], a_{s+1}, \dots, a_n)$. Then θ is an R -homomorphism and is onto, and $\ker \theta = K$. Hence $M \simeq L/K \simeq R/(r_1) \oplus R/(r_2) \oplus \dots \oplus R/(r_s) \oplus R \oplus R \oplus \dots \oplus R$.

Remarks

1. By the first remark after Lemma 5.3, we may assume that $r_1 \mid r_2$, $r_2 \mid r_3$, \dots . (In this case, the above decomposition is unique.) (Note that the number of copies of R is unique. If F is the field of fractions of R , then $M \otimes_R F = F \oplus F \oplus \dots \oplus F$ ($(n-s)$ times). Thus $M \otimes -rF$ is an F -vector space of dimension $n-s$. So $n-s$ is determined by M .)
2. We may assume that each r_i is a power of an irreducible (prime).
3. Everything works over a principal ideal domain R , not merely a Euclidean Domain.

Examples

1. Take $R = \mathbb{Z}$. Given a finitely generated abelian group G , we can write $G \simeq \mathbb{Z}/r_1\mathbb{Z} \oplus \mathbb{Z}/r_2\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/r_s\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \dots \oplus \mathbb{Z}$, where *either*
 - (a) $r_1 \mid r_2, r_2 \mid r_3, \dots$ or
 - (b) Each r_i is a prime power.
2. Vector spaces with endomorphism. Let V be a finite dimensional F -vector space. Let $\theta : V \rightarrow V$ be an endomorphism. Then V is an $F[x]$ -module, where $(a_0 + a_1x + \dots + a_nx^n)v = a_0v + a_1\theta(v) + \dots + a_n\theta^n(v)$. Now V is a finitely generated $F[x]$ -module, so by Theorem 5.5, we get $V \simeq F[x]/(f_1(x)) \oplus F[x]/(f_2(x)) \oplus \dots \oplus F[x]/(f_m(x))$. Hence we may assume that $\deg f_i(x) \geq 1$ (for if $f_i(x) = 0$, then $F[x]/(f_i(x)) = 0$, and we can ignore it). Also assume that each polynomial $f_i(x)$ has leading coefficient 1. Further we can arrange that *either*
 - (a) $f_1(x) \mid f_2(x), f_2(x) \mid f_3(x), \dots$ or
 - (b) Each $f_i(x)$ is a power of an irreducible polynomial (i.e. a linear polynomial if F is algebraically closed).

How do we find such polynomials given θ ?

Given V of dimension n , choose a basis e_1, e_2, \dots, e_n and let $\theta(e_i) = \sum_j a_{ij}e_j$ (so the matrix of θ is $A := (a_{ij})$). As in Theorem 5.5, we get a corresponding $F[x]$ -module L with basis l_1, l_2, \dots, l_n and an $F[x]$ -homomorphism $\phi : L \rightarrow V$ given by $\phi(l_i) = e_i$. Then $V \simeq L/K$, where $K = \ker \phi$. Let $k_i = xl_i - \sum_j a_{ij}l_j \in L$. Then $\phi(k_i) = 0$, i.e. $k_i \in \ker \phi$. In fact, k_1, k_2, \dots, k_n generate K (for if K' is a submodule of K generated by k_1, k_2, \dots, k_n , then L/K' is an F -vector space of dimension $\leq n$. But $K' \subset K$, and L/K has dimension n . Hence $K = K'$). So, in the proof of Theorem 5.5, we have to diagonalize $xI - A$. When diagonalized, the diagonal elements are $f_1(x), f_2(x), \dots, f_m(x)$ (plus $(n - m)$ 1s). Observe that $f_1(x)f_2(x) \cdots f_m(x) = \det(xI - A)$ since $\forall v \in V$ we have $[f_1(\theta)f_2(\theta) \cdots f_m(\theta)]v = (xI - A)v = 0$.

We can read off the Cayley–Hamilton Theorem.

Theorem 5.6 If we also arrange for $f_1 \mid f_2, f_2 \mid f_3, \dots$, then $f_m(x)$ (the last polynomial) is the minimum polynomial for θ . (We have $f_m(\theta)v = 0 \forall v$ since each $f_i(x) \mid f_m(x)$ and 1 in $F[x]/(f_m(x))$ is not killed by a polynomial of smaller degree.)

5.1 Jordan Canonical Form

Consider $F[x]/(f_i(x))$. Suppose $\deg f_i(x) = n_i \geq 1$. As an F -vector space, take basis $1, x, x^2, \dots, x^{n_i-1}$. So if we string together these bases for each i , we get a basis of V , and the matrix of θ is the

$$\begin{bmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & \cdots & A_m \end{bmatrix},$$

where

$$A_i = \begin{bmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ 0 & 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 0 & \cdots & 1 \\ a_0 & a_{n_1} & a_{n_2} & a_{n_3} & \cdots & a_{n_{i-1}} \end{bmatrix},$$

where $f_i(x) = a_0 + a_{n_1}x + \cdots + a_{n_{i-1}}x^i + 1x^n$.

5.2 Classical Canonical Form

($F = \mathbb{C}$). Take each $f_i(x)$ to be a power of a *linear* polynomial. Then, as an F -vector space, $F[x]/(x - \lambda)^s$ has basis $1, x - \lambda, (x - \lambda)^2, \dots, (x - \lambda)^{s-1}$. We have $x(x - \lambda)^i = (x - \lambda)^{i+1} - \lambda(x - \lambda)^i$

(and $x(x - \lambda)^{s-1} = \lambda(x - \lambda)$). The matrix now becomes

$$\begin{bmatrix} \lambda & 1 & 0 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & 0 & \cdots & 0 \\ 0 & 0 & \lambda & 1 & \cdots & 0 \\ 0 & 0 & 0 & \lambda & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & \lambda \end{bmatrix}.$$

5.3 Linear Maps Over Non-Commutative Rings

Now we shall no longer assume that R is commutative.

The goal is to analyze the structure of R , where R is a finite dimensional algebra over a field k , say.

Suppose that $M = M_1 \oplus M_2 \oplus \cdots \oplus M_m$ and $N = N_1 \oplus N_2 \oplus \cdots \oplus N_n$ are R -modules. Consider an R -homomorphism $\varphi : M_1 \oplus M_2 \oplus \cdots \oplus M_m \rightarrow N_1 \oplus N_2 \oplus \cdots \oplus N_n$. Then each $x \in M$ may be written uniquely in the form $X = x_1 + x_2 + \cdots + x_m$ ($x_i \in M_i$). We may represent $\varphi(x)$ by

$$\begin{pmatrix} \varphi_{11} & \varphi_{12} & \cdots & \varphi_{1n} \\ \varphi_{21} & \varphi_{22} & \cdots & \varphi_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \varphi_{m1} & \varphi_{m2} & \cdots & \varphi_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix},$$

where $\varphi_{ij} \in \text{hom}_R(M_i, N_j)$ is the map $M_i \xrightarrow{\varphi|_{M_i}} N \xrightarrow{\text{proj}} N_j$. In particular, if M is a fixed R -module and $K = \text{end}_R(M)$, then we have a ring homomorphism $\text{end}_R(M^n) \xrightarrow{\sim} M_n(K)$.

Definition 5.7 We say that an R -module $M \neq 0$ is **simple** if it has no proper nontrivial submodules.

Lemma 5.8 (Schur) Suppose that M and N are simple R -modules, and suppose that $f \in \text{hom}_R(M, N)$ is nonzero. Then f is an isomorphism. Furthermore, $\text{end}_R(M)$ is a division ring.

Proof Since M and N are simple and $f \neq 0$, we have $\ker f = \{0\}$ and $\text{Im}(f) = N$, and so f is an isomorphism. If $M = N$, then f is invertible in $\text{end}_R(M)$.

Definition 5.9 We say that an R -module M is **semisimple** if it is a direct sum of simple modules.

Lemma 5.10 Let $M = \sum_{i \in I} M_i$ be a (not necessarily direct) sum of simple modules. Then \exists a subset J of I such that $M = \bigoplus_{j \in J} M_j$.

Proof Let $J \subset I$ be maximal such that $\sum_{j \in J} M_j$ is a direct sum. Then for any i , we have that $(\sum_{j \in J} M_j) \cap M_i = M_i$ since J is maximal and M_i is simple. Hence $M = \sum_{j \in J} M_j = \bigoplus_{j \in J} M_j$.

Proposition 5.11 Suppose that M is an R -module. The following conditions are equivalent:

1. M is the sum of a family of simple modules.
2. M is the direct sum of a family of simple modules.
3. Every submodule N of M is a direct summand, i.e. \exists a submodule N' of M such that $M = N \oplus N'$.

Proof (1) implies (2) follows from Lemma 5.10. To show that (2) implies (3), suppose that $M = \sum_{i \in I} M_i$, where each M_i is a simple submodule of M . Let $J \subset I$ be maximal such that the sum $N + \bigoplus_{j \in J} M_j$ is direct. Then $M_i \cap (N + \bigoplus_{j \in J} M_j) = M_i$ for all i (arguing as in the proof of Lemma 5.10), and so $N + \bigoplus_{j \in J} M_j = N \oplus \bigoplus_{j \in J} M_j = M$.

To show that (3) implies (1), we claim that every nonzero submodule of M contains a simple submodule. To see why this is true, suppose that $m \in M$ with $m \neq 0$. Then Rm is a submodule of M . Consider the map $p : R \rightarrow Rm$, $r \mapsto rm$. Then $\ker p$ is contained in a maximal left ideal \mathfrak{m} of R . Then $\mathfrak{m}/\ker p$ is a maximal submodule of $R/\ker p$, and so $\mathfrak{m}m$ is a maximal submodule of Rm . Using (3), we may write $M = \mathfrak{m}m \oplus M'$, where M' is a submodule of M . Then $Rm = \mathfrak{m}m \oplus (M' \cap Rm)$ (since every $x \in Rm$ can be written uniquely in the form $x = am + x'$ ($a \in \mathfrak{m}$, $x' \in M'$), and $x' = x - am \in M' \cap Rm$). Now if $\mathfrak{m}m$ is maximal in Rm , then $M' \cap Rm$ is a simple R -module, as required. Now let M_0 be the sum of all simple submodules of M . If $M_0 \neq M$, then (3) implies that $M = M_0 \oplus M_1$, with $M_1 \neq 0$. Then M_1 has a simple submodule, and this contradicts the definition of M_0 . Hence $M_0 = M$, and so (3) implies (1).

Proposition 5.12 Every submodule and quotient module of a semisimple module M are semisimple.

Proof Let N be a submodule of M , and let N_0 be the sum of all simple submodules of N . Since M is semisimple, we may write $M = N_0 \oplus N'_0$ by Proposition 5.11(3). If $x \in N$, then x may be written uniquely in the form $x = x_0 + x'_0$ ($x_0 \in N_0$, $x'_0 \in N'_0$). Since $x'_0 = x - x_0 \in N$, we have $x'_0 \in N \cap N'_0$. Hence $N = N_0 \oplus (N \cap N'_0)$. This implies that $N = N_0$, i.e. N is semisimple.

To show this is true for quotient modules, since M is semisimple, we may write $M = N \oplus N'$. Then $M/N \simeq (N \oplus N')/N \simeq N'$, which is semisimple.

Definition 5.13 Suppose that M is a semisimple R -module and set $R' = R'(M) := \text{end}_R(M)$. Then M is an R' -module via $\varphi \cdot x = \varphi(x) \forall \varphi \in R', \forall x \in M$. Each $\alpha \in R$ induces an R' -homomorphism

$f_\alpha : M \rightarrow M$ given by $f_\alpha(x) = \alpha x$. Note that we have $\varphi(\alpha x) = \alpha \varphi(x) \forall \varphi \in R', \alpha \in R, x \in M$. The ring R' is called the **commutant** of R . Set $R'' = R''(M) = \text{end}_{R'}(M)$. Then R'' is called the **bicommutant** of R .

We have a homomorphism $R \rightarrow \text{end}_{R'}(M) = R''(M) = R'', \alpha \mapsto f_\alpha$.

Observe If $\alpha \in R$, then α induces an R' -endomorphism $f_\alpha : M \rightarrow M, m \mapsto \alpha m$ of M . So $f_\alpha \in \text{end}_{R'}(M) = R'' = R''(M)$. $R \rightarrow \text{end}_{R'}(M), \alpha \mapsto f_\alpha$.

Question How large is the image of this map?

Lemma 5.14 Suppose that M is a semisimple R -module. Let $R' = \text{end}_R(M)$. Suppose that $f \in \text{end}_{R'}(M)$ and $x \in M$. Then $\exists \alpha \in R$ such that $\alpha x = f(x)$.

Proof Since M is semisimple, we have $M = Rx \oplus N$ by Proposition 5.11 for some submodule N of M . Let $p : M \rightarrow Rx$ be the projection map. Then $p \in R'$ and so $f(x) = f(px) = pf(x)$. Hence $f(x) \in Rx$, as claimed.

Theorem 5.15 (Jacobson Density Theorem) Suppose that M is a semisimple R -module, and let $R' = \text{end}_R(M)$. Let $f \in \text{end}_{R'}(M)$ and $x_1, x_2, \dots, x_n \in M$. Then $\exists \alpha \in R$ such that $\alpha x_i = f(x_i)$ ($i = 1, 2, \dots, n$). If M is finitely generated over R' , then the natural map $R \rightarrow \text{end}_{R'}(M)$ is surjective.

Proof Suppose first that M is simple and define $f^{(n)} : M^n \rightarrow M^n$ by $(y_1, y_2, \dots, y_n) \mapsto (f(y_1), f(y_2), \dots, f(y_n))$. Set $R'_n = \text{end}_R(M^n)$. Then R'_n is the ring of $n \times n$ matrices over R' . Since f commutes with R' when acting on M , it follows that $f^{(n)} \in \text{end}_{R'_n}(M^n)$. Thus Lemma 5.14 implies that $\exists \alpha \in R$ such that $(\alpha x_1, \alpha x_2, \dots, \alpha x_n) = (f(x_1), f(x_2), \dots, f(x_n))$, as required.

If M is not simple, then M is a finite direct sum of nonisomorphic simple modules M_i with multiplicities n_i . $M = M'_1 \oplus M'_2 \oplus \dots \oplus M'_r$ (with $M_i \not\cong M_j$ if $i \neq j$). Now argue as before, using the fact that the matrices representing $\text{end}_R(M)$ split according to blocks corresponding to nonisomorphic simple components in the direct sum decomposition. If M is finitely generated over R' by y_1, y_2, \dots, y_m say, then any $f \in \text{end}_{R'}(M)$ is determined by the values $f(y_1), f(y_2), \dots, f(y_m)$, and so the map $R \rightarrow \text{end}_{R'}(M)$ is surjective.

Theorem 5.16 (Burnside) Let V be a finite dimensional vector space over an algebraically closed field k , and suppose that R is a subalgebra of $\text{end}_k(V)$. If V is a simple R -module, then $R = \text{end}_{R'}(V)$.

Proof We claim that $R' = \text{end}_R(V) = k$. To prove the claim, we note that certainly R' is a division ring (by Lemma 5.8) containing k as a subring and every element of k commutes with every element of R' . Suppose that $\alpha \in R'$. Then $k(\alpha)$ is a field. Also $R' \subseteq \text{end}_k(V)$ is a k -vector space, and so R' is a finite dimensional k -vector space. Hence $[k(\alpha) : k] < \infty$ implies that $k(\alpha) = k$ since k is algebraically closed. This proves the claim. Now suppose that v_1, v_2, \dots, v_n is a k -basis of V , and let $A \in \text{end}_{R'}(V) = \text{end}_k(V)$. The Jacobson Density Theorem implies that $\exists \alpha \in R$ such that $\alpha v_i = A v_i, i = 1, 2, \dots, n$. Hence $R = \text{end}_k(V) = \text{end}_{R'}(V)$, as claimed.

Example We shall use the notation of Theorem 5.16. Suppose that $G \leq GL(V)$. A G -invariant subspace W of V is a subspace such that $gW \subseteq W \forall g \in G$. Say V is G -simple if it has no proper nontrivial G -invariant subspace. So if $R = k[G]$ then V is G -simple iff V is a simple R -module. Hence Theorem 5.16 implies that if V is G -simple, then $k[G] = \text{end}_k(V)$.

Definition 5.17 Let M be any R -module. We say that M is **faithful** if given $\alpha \in R$ such that $\alpha x = 0 \forall x \in M$, we have $\alpha = 0$.

Theorem 5.18 Let R be a ring, and suppose that M is a simple, faithful R -module. Let $D = \text{end}_R(M)$ (so D is a division ring), and assume that M is finite dimensional over D . Then $R = \text{end}_D(M)$.

Proof Let $\{v_1, v_2, \dots, v_n\}$ be a basis of M over D , and suppose that $A \in \text{end}_D(M)$. The Jacobson Density Theorem implies that $\exists \alpha \in R$ such that $\alpha v_i = A v_i \forall i = 1, 2, \dots, n$. Thus the natural map $R \rightarrow \text{end}_D(M)$ is surjective. Since M is a faithful R -module, this homomorphism is also injective, and this proves the result.

Example Suppose that R is a finite dimensional algebra over a field k . If a ring R has no non-trivial proper 2-sided ideals, then any nonzero R -module M is faithful since the kernel of the map $R \rightarrow \text{end}_k(M)$ is a proper 2-sided ideal of R . If M is simple, then M is finite dimensional over k , and $D = \text{end}_R(M)$ is a finite dimensional division algebra over k . To obtain a faithful R -module, take e.g. M to be a minimal nontrivial left ideal of R (get this e.g. by taking a left ideal of minimal nonzero dimension over k).

Corollary 5.19 Suppose that R is a finite dimensional algebra over an algebraically closed field k . Let V be a finite dimensional k -vector space with a simple, faithful representation $p : R \rightarrow \text{end}_k(V)$. Then p is an isomorphism, and so $R \simeq M_n(k)$, where $n = \dim_k(V)$.

Proof Wedderburn's Theorem implies that $R = \text{end}_D(V)$, where $D = \text{end}_R(V)$, is finite dimensional over k . If $\alpha \in D$, then $k(\alpha)$ is a commutative subfield of D . Since k is algebraically closed (and D is finite dimensional over k), this implies that $k(\alpha) = k$. Hence $D = k$, as claimed.

Example

1. Let G be a cyclic group of prime order p . Then $\mathbb{Q}G \simeq \mathbb{Q} \oplus \mathbb{Q}(\zeta_p)$, where $\zeta_p \in \mathbb{C}$, $\zeta_p \neq 1$, and $\zeta_p^p = 1$. Also, $\mathbb{C}G \simeq \bigoplus_{i=1}^p \mathbb{C}$.
2. Let $G = H_8 = \langle \sigma, \tau \mid \sigma^4 = 1, \sigma^2 = \tau^2, \sigma^{-1}\tau\sigma = \tau^{-1} \rangle$. Then $\mathbb{C}G \simeq \bigoplus_{i=1}^4 \mathbb{C} \oplus M_2(\mathbb{C})$.