Rings, Modules, and Linear Algebra

Sean Sather-Wagstaff

Department of Mathematics, NDSU Dept # 2750, PO Box 6050, Fargo, ND 58108-6050 USA

E-mail address: sean.sather-wagstaff@ndsu.edu

URL: http://www.ndsu.edu/pubweb/~ssatherw/

October 1, 2011.

Contents

Introduction

Two of the most fundamental objects in mathematics are (1) the set $\mathbb{Z}$ of all integers, and (2) the set $\mathbb{R}[x]$ of all polynomials in x with real number coefficients. These two sets share many common features. Each one comes equipped with two binary operations, addition and multiplication, that satisfy certain axioms essentially saying that these operations are "nice". A set satisfying with two operations satisfying these axioms is called a commutative ring with identity. Other examples include $\mathbb{Z}_n$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, so rings are fundamental.

What is not obvious is how important rings are. For instance, much of the world's internet security is based on Fermat's Little Theorem, which is essentially a statement about exponentiation in $\mathbb{Z}_n$. As a second example, the modern field of Algebraic Geometry studies geometric objects essentially by replacing them with rings; theorems about rings translate to theorems about geometric objects, and vice versa. The theory of rings will be our starting point in this course.

One way to study a ring R is to study the objects that it "acts on". This is like studying a group by studying the sets it acts on. (This is how one proves the Sylow theorems, for instance, and how one can prove that various groups cannot be simple.) The most interesting objects R acts on are called "modules". One uses modules like group actions to show that certain rings have certain desirable properties (or do not). If the ring comes from a geometric object, then this property may translate to information about the geometry of that object. The theory of modules is the second part of this course.

When R is a field, the R-modules are nothing more than vector spaces over R, so we recover much of the theory of linear algebra. In fact, we will use modules to prove some strong results about matrices. For instance, we will prove the familiar fact that the determinant of a square matrix can be computed by expanding along any row or column, and we will prove that a square matrix can be put in a certain "canonical form" which is much nicer for computations. The first of these facts follows from a uniqueness theorem for alternating forms. The second one follows from a version of the Fundamental Theorem of Finite Abelian Groups for modules over a polynomial ring. The third part of this course is linear algebra.

Notation

$\mathbb{Z}$ is the set of all integers.
$\mathbb{Z}_n$ is the set of integers modulo n.
$n\mathbb{Z}$ is the set of all integer multiples of n.
$\mathbb{N}$ is the set of all non-negative integers.
$\mathbb{Q}$ is the set of all rational numbers.
$\mathbb{R}$ is the set of all real numbers.
$\mathbb{C}$ is the set of all complex numbers.
S_n is the symmetric group on n letters.
$\mathbb{R}[x]$ is the set of all polynomials in x with real number coefficients.

CHAPTER 1

Foundations

1.1. Sets and Arithmetic

Definition 1.1.1. The *cartesian product* of two non-empty sets S and T is

$$S \times T = \{(s,t) \mid s \in S, t \in T\}.$$

More generally, let $\{S_\alpha\}_{\alpha \in A}$ be a set of non-empty sets. The *cartesian product* $\prod_{\alpha \in A} S_\alpha$ is

$$\textstyle\prod_{\alpha \in A} S_\alpha = \{\text{sequences } (s_\alpha) \text{ such that } s_\alpha \in S_\alpha \text{ for each } \alpha \in A\}.$$

Fact 1.1.2 (Division Algorithm)**.** For all $a, b \in \mathbb{Z}$, if $b \neq 0$, then there exist $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $|r| < |b|$.

Fact 1.1.3 (Fundamental Theorem of Arithmetic)**.** Every integer $n \geqslant 2$ can be written as a product of (positive) prime numbers. Moreover, this factorization is unique up to re-ordering.

1.2. Additive Abelian Groups

Definition 1.2.1. An *additive abelian group* is a non-empty set G equipped with a binary operation $+$ that is associative and commutative, and with an additive identity 0_G such that every element $g \in G$ has an additive inverse $-g$. A *subgroup* of G is a subset $H \subseteq G$ which is itself a group under the operation for G; we sometimes write $H \leqslant G$.

Let $n \in \mathbb{N}$ and $g \in G$. Define $0 \cdot g = 0_G$ and $1 \cdot g = g$. Inductively, when $n \geqslant 2$ define $ng = (n-1)g + g$. Set $(-n)g = -(ng)$.

Fact 1.2.2 (Subrgroup Test)**.** Let G be an additive abelian group and $H \subseteq G$ a subset. Then H is a subgroup of G if and only if it satisfies the following conditions:

(1) $H \neq \emptyset$; and
(2) H is closed under the subtraction from G.

Remark 1.2.3. In the subgroup test, item (2) can be replaced with the following:

(2′) H is closed under addition and additive inverses.

Example 1.2.4. Let G and H be additive abelian groups. The cartesian product $G \times H$ is a group under the "coordinatewise" operation

$$(g,h) + (g',h') = (g+g', h+h')$$

with $0_{G \times H} = (0_G, 0_H)$ and $-(g,h) = (-g,-h)$.

More generally, let $\{G_\alpha\}_{\alpha\in A}$ be a set of additive abelian groups. The cartesian product $\prod_{\alpha\in A} G_\alpha$ is a group under the "coordinatewise" operation

$$\begin{aligned}(g_\alpha)+(h_\alpha)&=(g_\alpha+h_\alpha)\\ -(g_\alpha)&=(-g_\alpha)\\ 0_{\prod_{\alpha\in A} G_\alpha}&=(0_{G_\alpha}).\end{aligned}$$

Sometimes, we call this the *direct product* of the G_α.

The *direct sum* of the G_α is the subgroup

$$\oplus_{\alpha\in A}G_\alpha=\{(g_\alpha)\in \textstyle\prod_{\alpha\in A} G_\alpha \mid g_\alpha=0 \text{ for all but finitely many } \alpha\in A\}$$
$$\oplus_{\alpha\in A}G_\alpha \leqslant \textstyle\prod_{\alpha\in A} G_\alpha.$$

Sometimes we write $\coprod_{\alpha\in A} G_\alpha$ instead of $\oplus_{\alpha\in A}G_\alpha$, and we call this the *coproduct.* If $A=\emptyset$, then $\prod_{\alpha\in\emptyset} G_\alpha=\oplus_{\alpha\in\emptyset}G_\alpha=\{0\}$. If A is finite, then $\prod_{\alpha\in A} G_\alpha=\oplus_{\alpha\in A}G_\alpha$.

Given any set A and any additive abelian group G, set $G^{(A)}=\oplus_{\alpha\in A}G$ the direct sum of A many copies of G, and $G^A=\prod_{\alpha\in A} G$ the direct product of A many copies of G.

Definition 1.2.5. A *homomorphism of additive abelian groups* (or *additive abelian group homomorphism*) is a function $f\colon G\to H$ where G and H are additive abelian groups and $f(g+g')=f(g)+f(g')$ for all $g,g'\in G$. The *kernel* of f is the subgroup

$$\operatorname{Ker}(f)=\{g\in G\mid f(g)=0_H\}\leqslant G.$$

The homomorphism f is a *monomorphism* if it is injective. The homomorphism f is an *epimorphism* if it is surjective. The homomorphism f is an *isomorphism* if it is bijective. If there is an isomorphism $g\colon G\to H$, then we say that G and H are *isomorphic* and write $G\cong H$.

Fact 1.2.6. If $f\colon G\to H$ is a homomorphism of additive abelian groups, then $f(0_G)=0_H$, and $f(-a)=-f(a)$ for all $a\in G$.

Definition 1.2.7. Let G be an additive abelian group and $H\leqslant G$ a subgroup. For an element $g\in G$, define the *left coset* $g+H$ to be

$$g+H:=\{g+h\in G\mid h\in H\}.$$

Let G/H denote the set of all left cosets

$$G/H=\{g+H\mid g\in G\}.$$

Fact 1.2.8. Let G be an additive abelian group and $H\leqslant G$ a subgroup. Define a relation on G as: $g\sim g'$ provided that $g-g'\in H$. Then $\sim$ is an equivalence relation, and for each $g\in G$ the equivalence class $[g]$ is the coset $g+H$. Thus G/H is the set of equivalence classes under $\sim$. Another notation for $[g]$ is $\overline{g}$.

The set G/H is an additive abelian group with

$$\begin{aligned}(g+H)+(g'+H)&=(g+g')+H\\ 0_{G/H}&=0_G+H\\ -(g+H)&=(-g)+H.\end{aligned}$$

Using the equivalence class notations, we have

$$\begin{aligned} [g]+[g'] &= [g+g'] & \overline{g}+\overline{g'} &= \overline{g+g'} \\ 0_{G/H} &= [0_G] & 0_{G/H} &= \overline{0_G} \\ -[g] &= [-g] & -\overline{g} &= \overline{-g}. \end{aligned}$$

Fact 1.2.9. Let G be an additive abelian group and $H \leqslant G$.

(a) The function $\pi\colon G \to G/H$ given by $g \mapsto \overline{g}$ is a well-defined epimorphism of groups with $\operatorname{Ker}(\pi) = H$. (E.g., $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$.)
(b) π is an isomorphism if and only if $H = \{0_G\}$.
(c) An example of a group G and a normal subgroup $\{0_G\} \neq H \leqslant G$ such that $G/H \cong G$: Let $G = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots$ and $H = \mathbb{Z} \oplus \{0\} \oplus \{0\} \oplus \cdots$. (Use the first isomorphism theorem below.)

Fact 1.2.10 (First Isomorphism Theorem)**.** Let $f\colon G \to H$ be an additive abelian group homomorphism.

(a) $\operatorname{Ker}(f) \leqslant G$ and $\operatorname{Im}(f) \leqslant H$.
(b) The function $\overline{f}\colon G/\operatorname{Ker}(f) \to \operatorname{Im}(f)$ given by $\overline{g} \mapsto f(g)$ is a well-defined group isomorphism and so $\operatorname{Im}(f) \cong G/\operatorname{Ker}(f)$.
(c) f is a monomorphism if and only if $\operatorname{Ker}(f) = \{0_G\}$.

Fact 1.2.11 (Second Isomorphism Theorem)**.** Let G be an additive abelian group and $H, K \leqslant G$ with $K \subseteq H$.

(a) $K \leqslant H$
(b) $H/K \leqslant G/K$
(c) The function $\tau\colon G/K \to G/H$ given by $\tau(g+H) = g+K$ is a well defined group epimorphism with $\operatorname{Ker}(\tau) = H/K$. In particular, $(G/K)/(H/K) \cong G/H$.

Definition 1.2.12. Let G be an additive abelian group and $H, K \leqslant G$. Set

$$H + K = \{h + k \in G \mid h \in H \text{ and } k \in K\}.$$

Fact 1.2.13 (Third Isomorphism Theorem)**.** Let G be an additive abelian group and $H, K \leqslant G$.

(a) $K \leqslant H + K \leqslant G$
(b) $H \cap K \leqslant H$
(c) The function $\phi\colon H/(H \cap K) \to (H+K)/K$ given by $\phi(h + (H \cap K)) = h + K$ is a well defined group isomorphism. In particular, $H/(H \cap K) \cong (H+K)/K$.

Fact 1.2.14. Let G be an additive abelian group and $H, K \leqslant G$ such that $H \cap K = \{0\}$ and $H + K = G$. Then the function $f\colon H \times K \to G$ given by $f(h,k) = h+k$ is an isomorphism,

Fact 1.2.15. Let G be an additive abelian group with $K \leqslant G$, and let $\pi\colon G \to G/K$ be the group epimorphism $\pi(g) = g + K$. There is a 1-1 correspondence

$$\{H \leqslant G \mid K \subseteq H\} \longleftrightarrow \{H' \leqslant G/K\}$$

given by

$$\begin{aligned} H &\longmapsto H/K \\ \pi^{-1}(H') &\longleftarrow H' \end{aligned}$$

CHAPTER 2

Ring Theory

2.1. Rings, Homomorphisms, Subrings, and Ideals

Definition 2.1.1. A *ring* is a non-empty set R with two binary operations "+" and "·" such that $(R, +)$ is an abelian group, $\cdot$ is associative, and $(R, +, \cdot)$ satisfies both distributive laws:

$$r(s+t) = rs + rt \qquad\qquad (r+s)t = rt + st.$$

A ring R is *commutative* if the multiplication $\cdot$ is commutative.

A ring R has *identity* if there is a (two-sided) multiplicative identity $1_R \in R$. (Note that we do not assume the existence of multiplicative inverses.)

Assuming that R has a multiplicative identity 1_R, a *multiplicative inverse* for an element $r \in R$ is another element $r' \in R$ such that $rr' = 1_R = r'r$.

A *field* is a commutative ring with identity $1_R \neq 0_R$ such that every non-zero element in R has a multiplicative inverse in R.

Example 2.1.2. Under the usual addition and multiplication of integers, $\mathbb{Z}$ is a commutative ring with identity; it is not a field.

Under the usual addition and multiplication, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields.

Under the usual addition and multiplication of matrices, $M_2(\mathbb{R})$ is a ring with identity that is not commutative. (More generally, this holds for $M_n(R)$ where $n \geqslant 2$ and R is any commutative ring with identity.)

Under the usual addition and multiplication of integers, $2\mathbb{Z}$ is a commutative ring without identity.

Example 2.1.3. Fix an integer $n \geqslant 2$. Define multiplication in $\mathbb{Z}_n$ by the formula $[a] \cdot [b] = [ab]$. (Note that this is well-defined.) Under the usual addition in $\mathbb{Z}_n$, this multiplication endows $\mathbb{Z}_n$ with the structure of a commutative ring with identity. Furthermore, $\mathbb{Z}_n$ is a field if and only if n is prime. (Exercise.)

Proposition 2.1.4. *Let R be a ring.*

(a) *The additive identity in R is unique.*
(b) *If R has (multiplicative) identity, then the multiplicative identity in R is unique.*
(c) *For each $r \in R$, we have $0_R r = 0_R = r0_R$.*
(d) *Assume that R has identity. Then $R = \{0_R\}$ if and only if $1_R = 0_R$.*

Proof. (a) and (b): Exercise.

(c) $0r = (0+0)r = 0r + 0r \implies 0 = 0r$. The other equality is verified similarly.

(d) The implication "$\implies$" is immediate. For "$\impliedby$" assume $1 = 0$. For each $r \in R$, we have $r = 1r = 0r = 0$. □

Proposition 2.1.5. *Let R be a ring and let $r, s, t \in R$.*

(a) *If $r+s=r+t$, then $s=t$.*
(b) *r has a unique additive inverse in R, denoted $-r$.*
(c) *If r has a multiplicative inverse in R, then the multiplicative inverse is unique, denoted r^{-1}.*
(d) $-(-r)=r$.
(e) $(-r)s=-(rs)=r(-s)$.
(f) *If R has identity, then $(-1_R)r=-r=r(-1_R)$.*
(g) $(-r)(-s)=rs$.
(h) *For all $a_1,\ldots,a_m,b_1,\ldots,b_n\in R$, we have*

$$(\textstyle\sum_{i=1}^m a_i)(\sum_{j=1}^n b_j)=\sum_{i=1}^m\sum_{j=1}^n a_ib_j.$$

Proof. (a)–(c): Exercise.

(d) $r+(-r)=0$, so r satisfies the defining property for $-(-r)$. Now use part (b).

(e) $rs+(-r)s=(r+(-r))s=0s=0$. This explains the first equality, and the second one is explained similarly.

(f) $-r=-(1r)=(-1)r$ by part (e). This explains the first equality, and the second one is explained similarly.

(g) $(-r)(-s)=r(-(-s))=rs$.

(h) First, we show $a(\sum_{j=1}^n b_j)=(\sum_{j=1}^n ab_j)$ by induction on n: For $n\geqslant 2$, we have

$$a(\textstyle\sum_{j=1}^n b_j)=a(b_1+\sum_{j=2}^n b_j)=ab_1+a\sum_{j=2}^n b_j)=ab_1+\sum_{j=2}^n ab_j)=(\sum_{j=1}^n ab_j).$$

Next, we show $(\sum_{i=1}^m a_i)(\sum_{j=1}^n b_j)=\sum_{i=1}^m\sum_{j=1}^n a_ib_j$ by induction on m. The base case $m=1$ is in the previous paragraph. For $m\geqslant 2$, we have

$$\begin{aligned}(\textstyle\sum_{i=1}^m a_i)(\sum_{j=1}^n b_j)&=(a_1+\textstyle\sum_{i=2}^m a_i)(\sum_{j=1}^n b_j)\\&=a_1(\textstyle\sum_{j=1}^n b_j)+(\sum_{i=2}^m a_i)(\sum_{j=1}^n b_j)\\&=\textstyle\sum_{j=1}^n a_1b_j+\sum_{i=2}^m\sum_{j=1}^n a_ib_j\\&=\textstyle\sum_{i=1}^m\sum_{j=1}^n a_ib_j.\end{aligned}$$

□

Definition 2.1.6. Let R be a ring. For $r,s\in R$, define $r-s=r+(-s)$.

A subset $S\subseteq R$ is a *subring* if it is a ring with respect to the addition, subtraction, and multiplication on R.

Example 2.1.7. $n\mathbb{Z}$ is a subring of $\mathbb{Z}$.

Example 2.1.8. Let $S=\{\left(\begin{smallmatrix}r&0\\0&r\end{smallmatrix}\right)\in M_2(\mathbb{R})\,|\,r\in\mathbb{R}\}\subset M_2(\mathbb{R})$. Then S is a subring of $M_2(\mathbb{R})$.

Remark 2.1.9. If S is a subring of R, then $0_S=0_R$ as follows: $s\in S\implies 0_R=s-s\in S$, and since 0_R is an additive identity on R it is also an additive identity on S.

Example 2.1.10. Let $S=\{\left(\begin{smallmatrix}r&0\\0&0\end{smallmatrix}\right)\in M_2(\mathbb{R})\,|\,r\in\mathbb{R}\}\subset M_2(\mathbb{R})$. Then S is a subring of $M_2(\mathbb{R})$. Note that S and $M_2(\mathbb{R})$ are both rings with identity, but they do not have the same identity.

Proposition 2.1.11 (Subring Test). *Let R be a ring and $S\subseteq R$ a subset. Then S is a subring of R if and only if it satisfies the following conditions:*

(1) *$S \neq \emptyset$;*
(2) *S is closed under the subtraction from R;*
(3) *S is closed under the multiplication from R.*

Proof. Exercise: the missing axioms for S are inherited from R. □

Remark 2.1.12. In the subring test, item (2) can be replaced with the following:

($2'$) S is closed under addition and additive inverses.

Example 2.1.13. When $f\colon R \to S$ is a ring homomorphism and the rings R and S both have identity, we may have $f(1_R) \neq 1_S$. For example, this is so for the ring homomorphism $f\colon \mathbb{R} \to M_2(\mathbb{R})$ given by $f(r) = \left(\begin{smallmatrix} r & 0 \\ 0 & 0 \end{smallmatrix}\right)$.

Example 2.1.14. Products/coproducts of rings; see Example 1.2.4. Let $\{R_\lambda\}_{\lambda\in\Lambda}$ be a non-empty set of non-zero rings.

The product $\prod_\lambda R_\lambda$ is a ring with addition and multiplication defined coordinatewise: $(r_\lambda) + (r'_\lambda) = (r_\lambda + r'_\lambda)$ and $(r_\lambda)(r'_\lambda) = (r_\lambda r'_\lambda)$.

The product $\prod_\lambda R_\lambda$ has identity if and only if each R_λ has identity. $\Longleftarrow$: If $1_{R_\lambda} \in R_\lambda$ is a multiplicative identity, then the sequence (1_{R_λ}) is a multiplicative identity for $\prod_\lambda R_\lambda$. $\Longrightarrow$: If (r_λ) is a multiplicative identity for $\prod_\lambda R_\lambda$, then r_λ is a multiplicative identity for R_λ.

Similarly, the product $\prod_\lambda R_\lambda$ is commutative if and only if each R_λ is commutative.

The coproduct $\coprod_\lambda R_\lambda$ is a ring with addition and multiplication defined coordinatewise: $(r_\lambda) + (r'_\lambda) = (r_\lambda + r'_\lambda)$ and $(r_\lambda)(r'_\lambda) = (r_\lambda r'_\lambda)$. The coproduct $\coprod_\lambda R_\lambda$ has identity if and only if Λ is finite and each R_λ has identity. The coproduct $\coprod_\lambda R_\lambda$ is commutative if and only if each R_λ is commutative. The coproduct $\coprod_\lambda R_\lambda$ is a subring of $\prod_\lambda R_\lambda$.

Definition 2.1.15. Let R and S be rings. A function $f\colon R \to S$ is a *homomorphism of rings* or *ring homomorphism* if it respects the addition and multiplication on the rings: for all $r, r' \in R$, we have $f(r + r') = f(r) + f(r')$ and $f(rr') = f(r)f(r')$.

If R and S are rings with identity, then f is a *homomorphism of rings with identity* if it is a ring homomorphism and $f(1_R) = 1_S$.

Proposition 2.1.16. *If $f\colon R \to T$ is a ring homomorphism, then* $\mathrm{Im}(f)$ *is a subring of T.*

Proof. Exercise: use the Subring Test. □

Definition 2.1.17. Let R be a ring. A subset $I \subseteq R$ is a *(two-sided) ideal* if $(I, +) \leqslant (R, +)$ and, for all $a \in I$ and all $r \in R$, we have $ar \in I$ and $ra \in I$. In particular, when I is a two-sided ideal of R, the quotient R/I is a well-defined additive abelian group.

Example 2.1.18. For each integer n, the set $n\mathbb{Z}$ is a two-sided ideal in $\mathbb{Z}$.

In $\mathbb{Q}$, the set $\mathbb{Z}$ is a subring; it is not an ideal.

Every ring has the trivial ideals: $0 = \{0_R\}$ and R.

The only ideals of $\mathbb{Q}$ are $\{0\}$ and $\mathbb{Q}$. More generally, if k is a field, then the only two-sided ideals of k are $\{0\}$ and k. (Exercise.)

Remark 2.1.19. If I is an ideal in R, then $0_R \in I$ because $s \in S \implies 0_R = s - s \in S$.

Proposition 2.1.20 (Ideal Test)**.** *Let R be a ring and $I \subseteq R$ a subset. Then I is an ideal of R if and only if it satisfies the following conditions:*

(1) *$I \neq \emptyset$;*
(2) *I is closed under the subtraction from R;*
(3) *For all $r \in R$ and all $a \in I$, we have $ra \in I$ and $ar \in I$.*

Proof. Like the Subring Test. □

Remark 2.1.21. In the ideal test, item (2) can be replaced with the following:

(2′) I is closed under addition and additive inverses.

Proposition 2.1.22. *If $f\colon R \to T$ is a ring homomorphism, then* $\mathrm{Ker}(f)$ *is an ideal of R.*

Proof. Exercise: use the Ideal Test. □

Proposition 2.1.23. *Let R be a ring and $I \subseteq R$ a two-sided ideal.*

(a) *Define a product on the quotient R/I by the formula $\overline{r} \cdot \overline{s} = \overline{rs}$. This is well-defined and makes R/I into a ring.*
(b) *If R is commutative, then so is R/I.*
(c) *If R has identity 1_R, then R/I has identity $1_{R/I} = \overline{1_R}$.*
(d) *The natural map $\pi\colon R \to R/I$ given by $r \mapsto \overline{r}$ is a surjective ring homomorphism with kernel I.*
(e) *If R has identity, then π is a homomorphism of rings with identity.*

Proof. (a) If $\overline{r} = \overline{r'}$ and $\overline{s} = \overline{s'}$, then $r - r', s - s' \in I$ and so

$$rs - r's' = rs - r's + r's - r's' = \underbrace{\underbrace{\underbrace{(r-r')}_{\in I} s}_{\in I} + \underbrace{r' \underbrace{(s-s')}_{\in I}}_{\in I}}_{\in I} \in I$$

which implies $\overline{rs} = \overline{r's'}$. The remaining properties of R/I follow from the corresponding properties for R. For instance, once half of distributivity:

$$\overline{r}(\overline{s} + \overline{t}) = \overline{r(s+t)} = \overline{rs + rt} = \overline{rs} + \overline{rt}.$$

(b) Exercise.

(c) $\overline{1}\overline{r} = \overline{1r} = \overline{r}$ etc.

(d) π is a well-defined surjective additive abelian group homomorphism by Example 1.1.2.9(a). And it is a ring homomorphism because $\pi(rs) = \overline{rs} = \overline{r} \cdot \overline{s} = \pi(r)\pi(s)$.

(e) $1_{R/I} = \overline{1_R} = \pi(1_R)$. □

Example 2.1.24. We have $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ and $R/0 \cong R$ and $R/R \cong 0$.

Proposition 2.1.25 (First Isomorphism Theorem)**.** *Let $f\colon R \to S$ be a ring homomorphism.*

(a) *The function $\overline{f}\colon R/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ given by $\overline{r} \mapsto f(r)$ is a well-defined isomorphism of rings and so $\mathrm{Im}(f) \cong R/\mathrm{Ker}(f)$.*
(b) *f is a monomorphism if and only if $\mathrm{Ker}(f) = \{0_R\}$.*

Proof. Exercise: $\overline{f}$ comes from Fact 1.2.10. Check that it is a ring homomorphism. □

Here is the ideal correspondence for quotients, and the third isomorphism theorem.

Theorem 2.1.26. *Let R be a ring and $I \subseteq R$ an ideal. Let $\pi\colon R \to R/I$ be the ring epimorphism $\pi(r) = \overline{r}$. There is a 1-1 correspondence*

$$\{\textit{ideals } J \subseteq R \mid I \subseteq J\} \longleftrightarrow \{\textit{ideals } J' \subseteq R/I\}$$

given by

$$J \longmapsto J/I$$
$$\pi^{-1}(J') \longleftarrow J'$$

If J is an ideal of R such that $I \subseteq J$, then the function $\tau\colon R/I \to R/J$ given by $\tau(r+I) = r+J$ is a well-defined ring epimorphism with $\operatorname{Ker}(\tau) = J/I$*; in particular, there is a (well-defined) ring isomorphism $(R/I)/(J/I) \xrightarrow{\cong} R/J$.*

Proof. Exercise: use Facts 1.2.11 and 1.2.15. □

Example 2.1.27. Let $n \geqslant 2$. The ideals of $\mathbb{Z}/n\mathbb{Z}$ are exactly the sets of the form $m\mathbb{Z}/n\mathbb{Z} = \{\overline{a} \mid m\big|a\}$ for some $m\big|n$. And $(\mathbb{Z}/n\mathbb{Z})/(m\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z}$.

2.2. Operations on Ideals

Here are three important ways to create ideals.

Proposition 2.2.1. *If $\{I_\lambda\}_{\lambda\in\Lambda}$ is a non-empty set of ideals in a ring R, then $\cap_{\lambda\in\Lambda} I_\lambda$ is an ideal in R. In particular, if I, J are ideals of R, then so is $I \cap J$.*

Proof. Exercise: use the ideal test. □

Example 2.2.2. If $m, n \in \mathbb{Z}$, then $m\mathbb{Z} \cap n\mathbb{Z} = \operatorname{lcm}(m,n)\mathbb{Z}$.

Definition 2.2.3. Let X be a subset of a ring R. The *ideal generated by X* is the intersection of all ideals of R containing X; it is denoted $(X)R$. If $X = \{x_1, \ldots, x_n\}$, then we write $(X)R = (x_1, \ldots, x_n)R$.

Proposition 2.2.4. *Let X be a subset of a ring R.*

(a) *The set $(X)R$ is an ideal of R that contains X.*
(b) *$(X)R$ is the smallest ideal of R containing X.*
(c) *Assume that R has identity. Then*

$$(X)R = \{\textit{finite sums of the form } \textstyle\sum_i a_i x_i b_i \mid a_i, b_i \in R \textit{ and } x_i \in X\}.$$

In particular, if $x \in R$, then

$$(x)R = \{\textit{finite sums of the form } \textstyle\sum_j a_j x b_j \mid a_j, b_j \in R\}.$$

(d) *Assume that R is commutative and has identity. Then*

$$(X)R = \{\textit{finite sums of the form } \textstyle\sum_i c_i x_i \mid c_i \in R \textit{ and } x_i \in X\}.$$

In particular, if $x \in R$, then

$$(x)R = \{cx \mid c \in R\}.$$

Proof. (a) The set of all ideals of R containing X is non-empty because R is an ideal of R containing X. Now apply Proposition 2.2.1.

(b) If J is an ideal of R containing X, then J is one of the ideals in the intersection defining $(X)R$. Hence $(X)R \subseteq J$.

(c) For the first equality, set

$$I = \{\text{finite sums of the form } \textstyle\sum_i \sum_j a_i x_i b_i \mid a_i, b_i \in R \text{ and } x_i \in X\}.$$

We need to show $(X)R = I$.

"$\supseteq$" For each ideal J containing X, the fact that J is an ideal implies that every finite sum of the form $\sum_i \sum_j a_i x_i b_i$ is in J. In particular, every such sum is in the intersection of all the ideals of R containing X. Hence, the containment.

"$\subseteq$" It is straightforward to show that I is an ideal of R. Because R has identity, we have $X \subseteq I$. Hence, I is one of the ideals in the intersection defining $(X)R$, and so $(X)R \subseteq I$.

The second equality is a special case of the first one.

(d) The first equality follows from part (c) and the following computation:

$$\textstyle\sum_i \sum_j a_{i,j} x_i b_{i,j} = \sum_i \sum_j (a_{i,j} b_{i,j} x_i) = \sum_i (\underbrace{\textstyle\sum_j a_{i,j} b_{i,j}}_{c_i}) x_i.$$

The first equality uses the commutativity of R, and the second one uses the generalized distributive law from Proposition 2.1.5(h).

The second equality is a special case of the first one. $\square$

Example 2.2.5. If $m, n \in \mathbb{Z}$, then $(m, n)\mathbb{Z} = \gcd(m, n)\mathbb{Z}$.

Definition 2.2.6. Let $I_1, \ldots, I_n$ be ideals of a ring R. Their *sum* is

$$\textstyle\sum_j I_j = I_1 + \cdots + I_n = \{\sum_j a_j \mid a_j \in I_j, j = 1, \ldots, n\}.$$

In particular, for ideals I and J, we set

$$I + J = \{a + b \mid a \in I, b \in J\}.$$

Proposition 2.2.7. *Let $I_1, \ldots, I_n$ be ideals of a ring R.*

(a) *The sum $\sum_j I_j$ is an ideal of R.*
(b) *The sum $\sum_j I_j$ contains I_k for each $k = 1, \ldots, n$*
(c) *We have $\sum_j I_j = (\cup_j I_j)R$. In particular, $\sum_j I_j$ is the smallest ideal of R containing $\cup_j I_j$.*
(d) *If $I_j = (S_j)R$ for $j = 1, \ldots, n$, then $\sum_j I_j = (\cup_j S_j)R$, so $\sum_j I_j$ is the smallest ideal of R containing $\cup_j S_j$.*
(e) *For ideals I, J, K in R, we have $(I + J) + K = I + J + K = I + (J + K)$.*
(f) *If $\sigma \in S_n$, then $\sum_j I_j = \sum_j I_{\sigma(j)}$.*

Proof. (a) Use the ideal test and the generalized distributive law.

(b) Use the fact that $0_R \in I_k$ for each k.

(c) Let $z \in \sum_j I_j$. Then there exist $a_j \in I_j$ such that $z = \sum_j a_j$. Each $a_j \in \cup_j I_j \subseteq (\cup_j I_j)R$, so the fact that $(\cup_j I_j)R$ is closed under sums implies $z = \sum_j a_j \in (\cup_j I_j)R$. Hence $\sum_j I_j \subseteq (\cup_j I_j)R$.

For the reverse containment, note that $\sum_j I_j \supseteq I_l$ for each l, and therefore $\sum_j I_j \subseteq \cup_j I_j$. Since $(\cup_j I_j)R$ is the smallest ideal containing $\cup_j I_j$, it follows that $\sum_j I_j \supseteq (\cup_j I_j)R$.

The second statement follows from the first one by Proposition 2.2.4(b).

(d)–(f) Exercise. □

Example 2.2.8. In $\mathbb{Z}$, we have $m\mathbb{Z} + n\mathbb{Z} = (m, n)\mathbb{Z} = \gcd(m, n)\mathbb{Z}$.

Definition 2.2.9. Let $I_1, \ldots, I_n$ be ideals of a ring R. Their *product* is

$$\begin{aligned}\textstyle\prod_j I_j &= I_1 \cdots I_n \\ &= \{\text{finite sums of elements of the form } a_1 \cdots a_n \mid a_j \in I_j, j = 1, \ldots, n\}.\end{aligned}$$

In particular, for ideals I and J, we set

$$IJ = \{\text{finite sums of elements of the form } ab \mid a \in I, b \in J\}.$$

Starting with $I^0 = R$ and $I^1 = I$ we define I^n inductively for $n \geqslant 2$ as $I^n = II^{n-1}$.

Remark 2.2.10. Note that $\prod_j I_j$ is not the cartesian product.

Proposition 2.2.11. *Let $I_1, \ldots, I_n$ be ideals of a ring R with $n \geqslant 2$.*

(a) *The product $\prod_j I_j$ is an ideal of R contained in $\bigcap_j I_j$.*

(b) *We have $\prod_j I_j = (\{a_1 \cdots a_n \mid a_j \in I_j, j = 1, \ldots, n\})R$. In particular, $\prod_j I_j$ is the smallest ideal of R containing the set $\{a_1 \cdots a_n \mid a_j \in I_j, j = 1, \ldots, n\}$.*

(c) *If R is commutative and $I_j = (S_j)R$ for $j = 1, \ldots, n$, then*

$$\prod_j I_j = (\{a_1 \cdots a_n \mid a_j \in S_j, j = 1, \ldots, n\})R.$$

In particular, $\prod_j I_j$ is the smallest ideal of R containing the set

$$\{a_1 \cdots a_n \mid a_j \in S_j, j = 1, \ldots, n\}.$$

(d) *For ideals I, J, K in R, we have $(IJ)K = I(JK) = IJK$.*

(e) *If J is an ideal of R, then $J(\sum_j I_j) = \sum_j (JI_j)$ and $(\sum_j I_j)J = \sum_j (I_j J)$.*

(f) *If R is commutative and $\sigma \in S_n$, then $\prod_j I_j = \prod_j I_{\sigma(j)}$.*

Proof. (a) Use the ideal test and the generalized distributive law.

(b) Set $J = (\{a_1 \cdots a_n \mid a_j \in I_j, j = 1, \ldots, n\})R$. Let $c_j \in I_j$ for $j = 1, \ldots, n$. Then

$$\begin{aligned}c_1 \cdots c_n &\in \{a_1 \cdots a_n \mid a_j \in I_j, j = 1, \ldots, n\} \\ &\subseteq (\{a_1 \cdots a_n \mid a_j \in I_j, j = 1, \ldots, n\})R = J.\end{aligned}$$

Since $(\{a_1 \cdots a_n \mid a_j \in I_j, j = 1, \ldots, n\})R$ is closed under finite sums, it follows that every finite sum of elements of the form $c_1 \cdots c_n$ is in J. From the definition of $\prod_j I_j$, we conclude $\prod_j I_j \subseteq J$.

On the other hand, $\prod_j I_j$ is an ideal that contains each product $c_1 \cdots c_n$ with $c_j \in I_j$. Since J is the smallest such ideal, it follows that $\prod_j I_j \supseteq J$.

The second statement follows from the first one by Proposition 2.2.4(b).

(c) Exercise.

(d) Check $(IJ)K \subseteq IJK$ directly from the definitions using associativity of multiplication. Check $(IJ)K \supseteq IJK$ by showing that every generator of IJK is in $(IJ)K$. The equality $I(JK) = IJK$ is verified similarly.

(e) To show $J(\sum_j I_j) \subseteq \sum_j (JI_j)$, show that every generator of $J(\sum_j I_j)$ is in $\sum_j (JI_j)$. For $J(\sum_j I_j) \supseteq \sum_j (JI_j)$, show directly that every element of $\sum_j (JI_j)$ is in $J(\sum_j I_j)$ using the (generalized) distributive law. The equality $(\sum_j I_j)J = \sum_j (I_j J)$ is verified similarly.

(f) This follows similarly from the (generalized) commutative law. □

Example 2.2.12. If $m, n \in \mathbb{Z}$, then $(m\mathbb{Z})(n\mathbb{Z}) = mn\mathbb{Z}$.

2.3. Prime Ideals and Maximal Ideals

Definition 2.3.1. Let R be a ring and $P \subseteq R$ an ideal. P is *prime* if $P \neq R$ and, for all ideals $I, J \subseteq R$, if $IJ \subseteq P$, then either $I \subseteq P$ or $J \subseteq P$.

Example 2.3.2. $0\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$. If $0 \neq m \in \mathbb{Z}$, then $m\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$ if and only if m is a prime number. (These are the prototypes.)

Proposition 2.3.3. *Let R be a ring and $P \subsetneq R$ an ideal.*

(a) *Assume that, for all $a, b \in R$, if $ab \in P$, then either $a \in P$ or $b \in P$. Then P is prime.*

(b) *If R is commutative and P is prime, then, for all $a, b \in R$, if $ab \in P$, then either $a \in P$ or $b \in P$.*

Proof. (a) Let $I, J \subseteq R$ be ideals such that $IJ \subseteq P$ and $I \not\subseteq P$. We need to show that $J \subseteq P$. Let $a \in I - P$. For all $b \in J$, we have $ab \in IJ \subseteq P$; since $a \notin P$, our hypothesis implies $b \in P$. Thus, $J \subseteq P$.

(b) Let $a, b \in R$ and assume that $ab \in P$. Since P is an ideal, we have $(ab)R \subseteq P$. Since R is commutative, we have $[(a)R][(b)R] = (ab)R \subseteq P$ by Proposition 2.2.11(c). Since P is prime, either $(a)R \subseteq P$ or $(b)R \subseteq P$, and so either $a \in P$ or $b \in P$. □

Definition 2.3.4. An *integral domain* is a non-zero commutative ring with identity such that, for all $0 \neq a, b \in R$ we have $ab \neq 0$.

Example 2.3.5. $\mathbb{Z}$ is an integral domain. Every field is an integral domain, e.g., $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$.

Proposition 2.3.6. *Let R be a non-zero commutative ring with identity. An ideal $I \subseteq R$ is prime if and only if R/I is an integral domain.*

Proof. "$\Longrightarrow$" Assume that I is prime. Then $I \subsetneq R$ and so $R/I \neq 0$. Also, because R is commutative with identity, so is R/I. Let $0 \neq a + I, b + i \in R/I$. Then $a, b \notin I$ and so $ab \notin I$ because I is prime. Hence $(a + I)(b + I) = ab + I \neq 0$ and so R/I is an integral domain.

"$\Longleftarrow$" Assume R/I is an integral domain. In particular, we have $R/I \neq 0$ and so $I \subsetneq R$. Let $a, b \in R - P$. Then $0 \neq a + I, b + I \in R/I$. Since R/I is an integral domain, we have $0 \neq (a + I)(b + I) = ab + I$ and so $ab \notin I$. Proposition 2.3.3(a) implies that I is prime. □

Definition 2.3.7. An ideal $\mathfrak{m} \subseteq R$ is *maximal* if $\mathfrak{m} \neq R$ and $\mathfrak{m}$ is a maximal element in the set of all proper ideals, partially ordered by inclusion. In other words, $\mathfrak{m}$ is maximal if and only if $\mathfrak{m} \neq R$ and, for all ideals $I \subseteq R$, if $\mathfrak{m} \subseteq I$, then either $I = \mathfrak{m}$ or $I = R$.

Example 2.3.8. $0\mathbb{Z}$ and $6\mathbb{Z}$ are not maximal ideals of $\mathbb{Z}$ because $0\mathbb{Z} \subsetneq 6\mathbb{Z} \subsetneq 3\mathbb{Z} \subsetneq \mathbb{Z}$. In fact, $m\mathbb{Z}$ is maximal if and only if m is prime.

Here's something important that does not follow from the "usual" axioms of set theory. See Hungerford pp. 12-15 for a discussion.

The Axiom of Choice. *The Cartesian product of a family of non-empty sets indexed over a non-empty set is non-empty.*

For an important reformulation, we need some terminology.

Definition 2.3.9. A *partially ordered set* is a non-empty set A with a relation $\leqslant$ (called a *partial ordering on* A) which is reflexive (for all $a \in A$, we have $a \leqslant a$), transitive (for all $a, b, c \in A$, if $a \leqslant b$ and $b \leqslant c$, then $a \leqslant c$) and antisymmetric (for all $a, b \in A$, if $a \leqslant b$ and $b \leqslant a$, then $a = b$).

Example 2.3.10. If $A \subseteq \mathbb{R}$, then A is a partially ordered set under the usually ordering $\leqslant$.

If S is a set and A is a set of subsets of S, then A is a partially ordered set under inclusion.

Definition 2.3.11. Assume that A is a partially ordered set. Two elements $a, b \in A$ are *comparable* if either $a \leqslant b$ or $b \leqslant a$. An element $c \in A$ is *maximal* in A if, for every $a \in A$ which is comparable to c, we have $a \leqslant c$. If $\emptyset \neq B \subseteq A$, then an *upper bound* of B in A is an element $a \in A$ such that, for all $b \in B$, we have $b \leqslant a$. B is a *chain* if every two elements in B are comparable.

Assuming the "usual" axioms of set theory, the following is equivalent to the Axiom of Choice. For a proof, consult a book on set theory.

Theorem 2.3.12 (Zorn's Lemma)**.** *Let A be a non-empty partially ordered set such that every chain in A has an upper bound in A. Then A contains a maximal element.*

Here is a useful application of Zorn's Lemma.

Proposition 2.3.13. *Let R be a non-zero ring with identity. For every ideal $I \subsetneq R$, there is a maximal ideal $\mathfrak{m} \subsetneq R$ such that $I \subseteq \mathfrak{m}$. In particular, R has at least one maximal ideal.*

Proof. Fix an ideal $I \subsetneq R$. We use Zorn's Lemma to show that I is contained in some maximal ideal $\mathfrak{m}$ of R. Let $\mathcal{A}$ denote the set of all ideals J such that $I \subseteq J \subsetneq R$. Partially order $\mathcal{A}$ by inclusion. Since $I \neq R$, we have $I \in \mathcal{A}$ and so $\mathcal{A} \neq \emptyset$. In order to be able to invoke Zorn's lemma, we need to show that every chain $\mathcal{C}$ in $\mathcal{A}$ has an upper bound in $\mathcal{A}$.

Let $K = \cup_{J \in \mathcal{C}} J$. We will be done once we show that K is an ideal of R such that $K \neq R$. Indeed, then $K \supseteq J \supseteq I$ for all $J \in \mathcal{C}$ and so $K \in \mathcal{A}$ and K is an upper bound for $\mathcal{C}$ in $\mathcal{A}$.

We use the ideal test to show that K is an ideal of R. Since $0 \in I \subseteq K$, we have $K \neq \emptyset$. Let $a, a' \in K = \cup_{J \in \mathcal{C}} J$. Then there are $J, J' \in \mathcal{C}$ such that $a \in J$ and $a' \in J'$. Since $\mathcal{C}$ is a chain, either $J \subseteq J'$ or $J' \subseteq J$. Assume without loss of generality that $J \subseteq J'$. Then $a, a' \in J'$ and so $a - a' \in J' \subseteq K$ since J' is an ideal.

Now let $r \in R$ and $b \in K$. There is an ideal $J'' \in \mathcal{C}$ such that $b \in J''$. Since J'' is an ideal, we have $rb \in J'' \subseteq K$. Similarly, we see that $br \in K$, and so K is an ideal.

Suppose $K = R$. Then $1_R \in K$. It follows that $1_R \in J'''$ for some $J''' \in \mathcal{C}$ and so $J''' = R$ by an exercise. This contradicts the fact that $J''' \in \mathcal{C}$.

Zorn's Lemma implies that $\mathcal{C}$ has a maximal element $\mathfrak{m}$. It is straightforward to check that $\mathfrak{m}$ is a maximal ideal of R that contains I.

For the final statement, note that $(0)R \neq R$ and so $(0)R$ is contained in some maximal ideal $\mathfrak{m}'$. Hence, R has at least one maximal ideal. □

Proposition 2.3.14. *Let R be a non-zero commutative ring with identity.*

(a) *An ideal I is maximal if and only if R/I is a field.*
(b) *Every maximal ideal of R is prime.*

Proof. (a) If I is maximal, then there are no ideals J such that $I \subsetneq J \subsetneq R$. The ideal correspondence shows that R/I has only two ideals, I/I and R/I. Hence, R/I is a field by an exercise.

Conversely, assume that R/I is a field and let J be an ideal such that $I \subseteq J \subseteq R$. Hence, J/I is an ideal of R/I. Since R/I is a field, the same exercise shows that R/I has only two ideals, I/I and R/I. Hence, either $J/I = I/I$ or $J/I = R/I$. That is, either $J = I$ or $J = R$, so I is maximal.

(b) If $\mathfrak{m} \subsetneq R$ is a maximal ideal, then $R/\mathfrak{m}$ is a field. Hence, $R/\mathfrak{m}$ is an integral domain and so $\mathfrak{m}$ is prime. □

Proposition 2.3.15. *Let R be a non-zero commutative ring with identity. Let $I \subsetneq R$ be an ideal and let $\pi\colon R \to R/I$ be the ring epimorphism $\pi(r) = \overline{r}$.*

(a) *There is a 1-1 correspondence*

$$\{\textit{prime ideals } P \subsetneq R \mid I \subseteq P\} \longleftrightarrow \{\textit{prime ideals } P' \subsetneq R/I\}$$

given by

$$\begin{aligned} P &\longmapsto P/I \\ \pi^{-1}(P') &\longleftarrow\!\shortmid P'. \end{aligned}$$

In other words, the ideal $J/I \subseteq R/I$ is prime if and only if J is a prime ideal of R.

(b) *There is a 1-1 correspondence*

$$\{\textit{maximal ideals } \mathfrak{m} \subsetneq R \mid I \subseteq \mathfrak{m}\} \longleftrightarrow \{\textit{maximal ideals } \mathfrak{m}' \subsetneq R/I\}$$

given by

$$\begin{aligned} \mathfrak{m} &\longmapsto \mathfrak{m}/I \\ \pi^{-1}(\mathfrak{m}') &\longleftarrow\!\shortmid \mathfrak{m}'. \end{aligned}$$

In other words, the ideal $J/I \subseteq R/I$ is maximal if and only if J is a maximal ideal of R.

Proof. (a) Using the ideal correspondence, it suffices to verify the last statement. The ideal $J/I \subseteq R/I$ is prime if and only if $(R/I)/(J/I) \cong R/J$ is an integral domain, and this is so if and only if J is prime. The isomorphism comes from the Third Isomorphism Theorem.

(b) As in part (a), changing "prime" to "maximal" and "integral domain" to "field". □

Example 2.3.16. The prime ideals of $\mathbb{Z}/42\mathbb{Z}$ are $2\mathbb{Z}/42\mathbb{Z}, 3\mathbb{Z}/42\mathbb{Z}, 7\mathbb{Z}/42\mathbb{Z}$ because $42 = (2)(3)(7)$. These are exactly the maximal ideals of $\mathbb{Z}/42\mathbb{Z}$ as well.

2.4. Quotient Fields

It is straightforward to show that if R is isomorphic to a non-zero subring of a field, then R is an integral domain. In this section, we prove the converse. To do this, we construct the field of quotients of an integral domain. It is modeled on the construction of $\mathbb{Q}$ from $\mathbb{Z}$. The elements of $\mathbb{Q}$ are of the form r/s where $r, s \in \mathbb{Z}$ and $s \neq 0$.

Construction 2.4.1. Let R be an integral domain and consider the Cartesian product $R \times (R - \{0\})$. Define a relation on $R \times (R - \{0\})$ as follows: $(r, s) \sim (r', s')$ if and only if $rs' = r's$. This is an equivalence relation on $R \times (R - \{0\})$, and the set of equivalence classes is denoted $\mathrm{Q}(R)$. The equivalence class of an element (r, s) in $\mathrm{Q}(R)$ is denoted r/s or $\frac{r}{s}$. If $0 \neq t \in R$, then the definition implies $(r, s) \sim (rt, st)$; this translates to the cancellation formula $\frac{rt}{st} = \frac{r}{s}$.

For elements $r/s, t/u \in \mathrm{Q}(R)$, set

$$\frac{r}{s} + \frac{t}{u} = \frac{ru + ts}{su} \qquad \text{and} \qquad \frac{r}{s}\frac{t}{u} = \frac{rt}{su}.$$

Proposition 2.4.2. *With notation as in Construction 2.4.1:*

(a) *In $\mathrm{Q}(R)$, we have $r/s = 0/t$ if and only if $r = 0$.*
(b) *In $\mathrm{Q}(R)$, we have $r/s = t/t$ if and only if $r = s$.*
(c) *$\mathrm{Q}(R)$ is a field with $0_{\mathrm{Q}(R)} = 0_R/1_R$ and $1_{\mathrm{Q}(R)} = 1_R/1_R = r/r$ and $(r/s)^{-1} = s/r$.*
(d) *The assignment $f\colon R \to \mathrm{Q}(R)$ given by $r \mapsto r/1$ is a monomorphism of rings with identity.*

Proof. (a) $r/s = 0/t$ if and only if $rt = s0$ if and only if $r = 0$; the last equivalence is from the fact that R is an integral domain.

(b) $r/s = t/t$ if and only if $rt = st$ if and only if $r = s$; the last equivalence is by cancellation.

(c) The main point is to show that the addition and multiplication on $\mathrm{Q}(R)$ are well-defined; the other field-axioms are then easily verified. Assume that $r/s = r'/s'$ and $t/u = t'/u'$, that is, $rs' = r's$ and $tu' = t'u$. Then

$$\begin{aligned} \frac{ru + ts}{su} &= \frac{(ru + ts)s'u'}{(su)s'u'} = \frac{rs'uu' + tu'ss'}{ss'uu'} = \frac{r'suu' + t'uss'}{ss'uu'} \\ &= \frac{(r'u' + t's)us}{(u's')us} = \frac{r'u' + t's}{u's'} \end{aligned}$$

so addition is well-defined. The equality $\frac{rt}{su} = \frac{r't'}{s'u'}$ is even easier to verify, showing that multiplication is well-defined.

We have the correct additive identity because

$$\frac{r}{s} + \frac{0}{1} = \frac{r1 + s0}{s1} = \frac{r}{s}$$

and the multiplicative identity is even easier. The other axioms showing that $\mathrm{Q}(R)$ is a commutative ring with identity are straightforward but tedious.

To see that $\mathrm{Q}(R)$ is non-zero, we need to show $0/1 \neq 1/1$: this follows from parts (a) and (c).

Finally, if $r/s \neq 0/1$ then $r \neq 0$ and so $s/r \in \mathrm{Q}(R)$. It is straightforward to check that $\frac{r}{s}\frac{s}{r} = \frac{1}{1}$, and so $(r/s)^{-1} = s/r$.

(d) The function is well-defined. It is straightforward to show that it is a homomorphism of rings with identity: for instance

$$\frac{r}{1}+\frac{r'}{1}=\frac{r1+1r'}{1\cdot 1}=\frac{r+r'}{1}.$$

The fact that f is a monomorphism, follows from part (a). □

We generally identify R with its image in $\mathrm{Q}(R)$.

Example 2.4.3. $\mathrm{Q}(\mathbb{Z})\cong\mathbb{Q}$.

2.5. Factorization

Here is one way that integral domains are like fields. Note that we are not assuming that a has a multiplicative inverse.

Proposition 2.5.1. *Let R be an integral domain. If $a,b,c\in R$ such that $ab=ac$, then either $a=0$ or $b=c$.*

Proof. $ab=ac$ implies $a(b-c)=0$. Since R is an integral domain, either $a=0$ or $b-c=0$. □

Definition 2.5.2. Let R be a non-zero commutative ring with identity. An element $u\in R$ is a *unit* if it has a multiplicative inverse in R. An element $p\in R$ is *prime* if it is a non-zero nonunit and $(p)R$ is a prime ideal in R. An element $q\in R$ is *irreducible* if it is a non-zero nonunit and, q has only trivial factors, that is, for all $a,b\in R$, if $q=ab$ then either a or b is a unit.

For elements $a,b\in R$, we say *a is a factor of b* or *a divides b* if there exists $c\in R$ such that $b=ac$; when a divides b, we write $a\big|b$.

An ideal I is *principal* if it can be generated by a single element, that is, if there exists an element $r\in R$ such that $I=(r)R$.

Example 2.5.3. The units in $\mathbb{Z}$ are ±1. The prime elements are exactly the prime numbers (positive and negative), and same for the irreducible elements.

In a field, every non-zero element is a unit. Hence, a field has no prime elements and no irreducible elements.

In $\mathbb{Z}/(6)\mathbb{Z}$, the units are $\overline{1},\overline{5}=-\overline{1}$; the prime elements are $\overline{2},\overline{3},\overline{4}=-\overline{2}$. The element $\overline{2}$ is not irreducible because $\overline{2}=\overline{2}\cdot\overline{4}$. The element $\overline{3}$ is not irreducible because $\overline{3}=\overline{3}\cdot\overline{3}$. The element $\overline{4}$ is not irreducible because $\overline{4}=\overline{2}\cdot\overline{2}$.

Exercise 2.5.4. Let R be a non-zero commutative ring with identity, and let $a,b\in R$. The following conditions are equivalent:

(a) $a\big|b$;
(b) $b\in(a)R$;
(c) $(b)R\subseteq(a)R$.

Proposition 2.5.5. *Let R be a non-zero commutative ring with identity. Let $p\in R$ be a non-zero nonunit. Then p is prime if and only if, for all $a,b\in R$, if $p\big|ab$, then $p\big|a$ or $p\big|b$.*

Proof. From the characterization of prime ideals from Proposition 2.3.3: $(p)R$ is prime if and only if for all $a,b\in R$, if $ab\in(p)R$, then either $a\in(p)R$ or $b\in(p)R$. Now use Exercise 2.5.4. □

Proposition 2.5.6. *Let R be an integral domain. If $p \in R$ is prime, then p is irreducible.*

PROOF. Assume that p is prime, and suppose $p = ab$ for some $a, b \in R$. Then $p \big| ab$, so the fact that p is prime implies $p \big| a$ or $p \big| b$. Assume $p \big| a$; we need to show that b is a unit. Since $p \big| a$ and $a \big| p$, we have $(a)R = (p)R = (ab)R$. Since R is an integral domain, an exercise implies that b is a unit. □

Remark 2.5.7. Example 2.5.3 shows that the assumption "R is an integral domain" is necessary: In $\mathbb{Z}/(6)\mathbb{Z}$, the element $\overline{2}$ is prime but not irreducible.

Example 2.5.8. Not every irreducible element is prime, even in an integral domain. To see this, let $\mathbb{R}[x^2, x^3]$ be the set of polynomials of the form $a_0 + a_2x^2 + a_3x^3 + a_4x^4 + \cdots$ with $a_0, a_2, a_3, a_4, \ldots \in \mathbb{R}$. That is, $\mathbb{R}[x^2, x^3]$ is the set of all polynomials with real-number coefficients and zero linear term. This is an integral domain. (Use the subring test to show that $\mathbb{R}[x^2, x^3]$ is a subring of the ring of polynomials $\mathbb{R}[x]$ with real number coefficients. Because $\mathbb{R}[x]$ is an integral domain, it follows readily that $\mathbb{R}[x^2, x^3]$ is also an integral domain. We will deal with polynomial rings more thoroughly below.) In $\mathbb{R}[x^2, x^3]$ the element x^2 is irreducible, but it is not prime. To see that x^2 is not prime, note that $x^2x^4 = x^6 = x^3x^3$ and so $x^2 \big| x^3x^3$; however, $x^2 \nmid x^3$ because $x \notin \mathbb{R}[x^2, x^3]$.

Definition 2.5.9. Let R be an integral domain. If every non-zero nonunit of R can be written as a (finite) product of prime elements, then R is a *unique factorization domain* or UFD for short.

Example 2.5.10. $\mathbb{Z}$ is a UFD. A field k is a UFD.

Proposition 2.5.11. *Let R be an integral domain. Prime factorization in R is unique up to order and multiplication by units: Let $p_1, \ldots, p_k, q_1, \ldots, q_m$ be primes elements of R such that $p_1 \cdots p_k = q_1 \cdots q_m$, then $m = k$ and there is a permutation $\sigma \in S_k$ and there are units $u_1, \ldots, u_k$ in R such that $p_i = u_i q_{\sigma(i)}$ for $i = 1, \ldots, k$.*

PROOF. We proceed by induction on k.

Base case: $k = 1$. We need to show $m = 1$, so suppose $m > 1$. Then $p_1 = q_1 \cdots q_m$ and so $p_1 \big| q_i$ for some i because p_1 is prime. Reorder the q_j to assume $p_1 \big| q_1$. Since $q_1 \big| q_1 \cdots q_m = p_1$, we also have $q_1 \big| p_1$. Hence, we have $(q_1)R = (p_1)R = (q_1q_2 \cdots q_m)R$ and so $q_2 \cdots q_m$ is a unit. This implies that each q_j is a unit, contradicting the fact that q_j is prime.

Induction step. Assuming that $p_1 \cdots p_k = q_1 \cdots q_m$ and $k \geqslant 2$, we have $p_1 \big| p_1 \cdots p_k$ and so $p_1 \big| q_1 \cdots q_m$. Since p_1 is prime, $p_1 \big| q_j$ for some j. As above, reorder the q_i to assume $p_1 \big| q_1$, and use the fact that q_1 is prime to conclude that $q_1 = u_1 p_1$ for some unit u_1. It follows that $p_2 \cdots p_k = u_1 q_2 \cdots q_m$, so the rest of the result follows by induction. □

Proposition 2.5.12. *If R is a UFD, then every irreducible element of R is prime.*

PROOF. Fix an irreducible element $x \in R$. Since R is a UFD, we can write $x = p_1 \cdots p_k$ where each $p_i \in R$ is prime. In particular, no p_i is a unit. Suppose $k > 1$. Then $x = p_1(p_2 \cdots p_k)$. Since x is irreducible, either p_1 is a unit or $p_2 \cdots p_k$ is a unit. This contradicts the fact that no p_i is a unit, so we must have $k = 1$. That is $x = p_1$ is prime. □

Here we reconcile our definition of UFD with Hungerford's definition, which is condition (iii).

Proposition 2.5.13. *Let R be an integral domain. TFAE.*

(i) *R is a UFD;*
(ii) *Every irreducible element of R is prime, and every non-zero nonunit of R can be written as a finite product of irreducible elements;*
(iii) *Every non-zero nonunit of R can be written as a finite product of irreducible elements and such a factorization is unique up to order and multiplication by units.*

Proof. (ii) $\Longrightarrow$ (i) Definition of UFD.

(i) $\Longrightarrow$ (iii) This follows from the definition of UFD and Propositions 2.5.6 and 2.5.11.

(iii) $\Longrightarrow$ (ii) It suffices to show that every irreducible element $x \in R$ is prime. Suppose that $a, b \in R$ and $x \big| ab$. We need to show that $x \big| a$ or $x \big| b$. There is an element $c \in R$ such that $ab = xc$. If $a = 0$, then $a = 0 = x0 \implies x \big| a$. So assume $a \neq 0$, and similarly assume $b \neq 0$. Note that this implies $c \neq 0$.

If a is a unit, then $b = x(a^{-1}c) \implies x \big| b$. So, assume that a is not a unit, and similarly assume that b is not a unit. If c is a unit, then $x = (c^{-1}a)b$; since x is irreducible, either $c^{-1}a$ is a unit or b is a unit. That is, either a is a unit or b is a unit, a contradiction.

Since a, b, c are non-zero nonunits, there are irreducible elements

$$a_1, \ldots, a_k, b_1, \ldots, b_l, c_1, \ldots, c_m \in R$$

such that $a = a_1 \cdots a_k$, $b = b_1 \cdots b_l$ and $c = c_1 \cdots c_m$. The equation $xc = ab$ implies

$$xc_1 \cdots c_m = a_1 \cdots a_k b_1 \cdots b_l.$$

The uniqueness condition for factorizations implies that x is a unit multiple of one of the elements $a_1, \ldots, a_k, b_1, \ldots, b_l$. If $x = ub_i$, then

$$b = b_1 \cdots b_l = u^{-1} b_1 \cdots b_{i-1}(ub_i)b_{i+1} \cdots b_l = u^{-1} b_1 \cdots b_{i-1} x b_{i+1} \cdots b_l$$

and so $x \big| b$. Similarly, if $x = ua_j$, then $x \big| a$. Hence x is prime. □

Example 2.5.14. Factorization into products of irreducibles is not unique if R is not a UFD. For example, in the ring $\mathbb{R}[x^2, x^3]$, the elements x^2, x^3 are irreducible and $x^2x^2x^2 = x^3x^3$. Hence, the number of irreducible factors need not be the same, and the factors need not be unit multiples of each other.

Definition 2.5.15. Let R be a UFD, and let $r_1, \ldots, r_n \in R$, not all zero. An element $r \in R$ is a *greatest common divisor (GCD)* of $\{r_1, \ldots, r_n\}$ if (a) $r \big| r_i$ for each i, and (b) if $s \in R$ and $s \big| r_i$ for each i, then $s \big| r$; we write $\gcd(r_1, \ldots, r_n) = [r]$. We say that $r_1, \ldots, r_n$ are *relatively prime* if $\gcd(r_1, \ldots, r_n) = [1]$.

An element $t \in R$ is a *least common multiple (LCM)* of $\{r_1, \ldots, r_n\}$ if (a) $r_i \big| t$ for each i, and (b) if $s \in R$ and $r_i \big| s$ for each i, then $t \big| s$; we write $\operatorname{lcm}(r_1, \ldots, r_n) = [t]$.

Remark 2.5.16. Let R be a commutative ring with identity, and let $R^\times$ denote the set of units of R. It is straightforward to show that $R^\times$ is an abelian group under multiplication. In particular, if k is a field, then $k^\times = k - \{0\}$.

Lemma 2.5.17. *Let R be a UFD, and let $r_0, \ldots, r_d \in R$, not all zero.*

(a) *There are prime elements* $p_1, \ldots, p_n \in R$ *and elements* $u_0, \ldots, u_d \in R^\times \cup \{0\}$ *and* $k_{i,j} \in \mathbb{N}$ *for* $i = 0, \ldots, d$ *and* $j = 1, \ldots, n$ *such that (1)* $[p_j] \neq [p_{j'}]$ *when* $j \neq j'$*, and (2)* $r_i = u_i p_1^{k_{i,1}} \cdots p_n^{k_{i,n}}$ *for each* i*. If* $r_i = 0$*, we may take* $u_i = 0$ *and* $k_{i,j} = 0$ *for each* j*.*

(b) *With notation as in part* (a)*, assume* $r_0, r_1 \neq 0$*. Then* $r_0 \big| r_1$ *if and only if* $k_{0,j} \leqslant k_{1,j}$ *for each* j*.*

(c) *With notation as in part* (a)*, assume* $r_0 \neq 0$*. Then* r_0 *is a unit if and only if* $k_{0,j} = 0$ *for each* j*.*

(d) *With notation as in part* (a)*, set* $m_j = \min_i\{k_{i,j} \mid r_i \neq 0\}$*. Then the element* $r = p_1^{m_1} \cdots p_n^{m_n} \in R$ *is a GCD for* $\{r_0, \ldots, r_d\}$*.*

(e) *With notation as in part* (a)*, set* $M_j = \max_i\{k_{i,j}\}$*. Then the element* $t = p_1^{M_1} \cdots p_n^{M_n} \in R$ *is an LCM for* $\{r_0, \ldots, r_d\}$*.*

Proof. (a) Bookkeeping nightmare: Use the existence of prime factorizations and the uniqueness of prime factorizations.

(b) "$\Longrightarrow$" Assume $r_0 \big| r_1$. We will show that $k_{0,1} \leqslant k_{1,1}$, by induction on $k_{0,1}$. (The other cases follow by commutativity of multiplication.)

The base case $k_{0,1} = 0$ is straightforward because $k_{1,1} \geqslant 0$.

So, assume that $k_{0,1} \geqslant 1$.

We will first show that $k_{1,1} \geqslant 1$. Our assumption implies $p_1 \big| r_0$, and since $r_0 \big| r_1$, this implies $p_1 \big| r_1$. Since p_1 is prime, this implies $p_1 \big| u_1$ or $p_1 \big| p_j^{k_{1,j}}$ for some j. Since u_1 is a unit, we have $p_1 \nmid u_1$, and so $p_1 \big| p_j^{k_{1,j}}$ for some j. Then $p_j^{k_{1,j}}$ is not a unit, and so $k_{1,j} \geqslant 1$. It follows that $p_1 \big| p_j$. Since p_j is prime, it is irreducible, so its only factors are the units and the unit multiples of p_j. Since p_1 is not a unit, we conclude that $[p_1] = [p_j]$ and so $1 = j$ by assumption. In particular, we have $k_{1,1} \geqslant 1$.

Let $r_0' = u_0 p_1^{k_{0,1}-1} \cdots p_n^{k_{0,n}}$ and $r_1' = u_0 p_1^{k_{1,1}-1} \cdots p_n^{k_{1,n}}$. Because $pr_0' = r_0 \big| r_1 = pr_1'$, the fact that R is an integral domain implies that $r_0' = r_1'$. By induction, we conclude $k_{0,1} - 1 \leqslant k_{1,1} - 1$, and so $k_{0,1} \leqslant k_{1,1}$.

"$\Longleftarrow$" Assuming that $k_{0,j} \leqslant k_{1,j}$ for each j, we have

$$r_1' = u_0^{-1} u_1 p_1^{k_{1,1}-k_{0,1}} \cdots p_n^{k_{1,n}-k_{0,n}} \in R$$

and

$$r_0 r_1' = u_0 p_1^{k_{0,1}} \cdots p_n^{k_{0,n}} u_0^{-1} u_1 p_1^{k_{1,1}-k_{0,1}} \cdots p_n^{k_{1,n}-k_{0,n}} = u_1 p_1^{k_{1,1}} \cdots p_n^{k_{1,n}} = r_1$$

and so $r_0 \big| r_1$.

(c) Write $1 = 1 \cdot p_1^0 \cdots p_n^0$. Then r_0 is a unit if and only if $r_0 \big| 1$ if and only if $k_{0,j} \leqslant 0$ for each j by part (b) if and only if $k_{0,j} = 0$.

(d) First, we need to show that $r \big| r_i$ for each i. If $r_i = 0$, then $r_i = 0 = r0 \implies t \big| r_i$. So, assume $r_i \neq 0$. By assumption, we have $k_{i,j} \geqslant m_j$ for each j, and so part (b) implies $r \big| r_i$.

Next, we need to assume that $s \in R$ and $s \big| r_i$ for each i, and show $s \big| r$. Since at least one $r_i \neq 0$, we know $s \neq 0$. If s is a unit, then $s \big| r$ easily. So, assume that s is a nonunit. Write $s = u q_1^{l_1} \cdots q_h^{l_h}$ where u is a unit, $q_1, \ldots, q_h \in R$ are prime and $l_1, \ldots, l_h \geqslant 1$ and $[q_j] \neq [q_{j'}]$ when $j \neq j'$.

Note that each $q_j \big| s$ and $s \big| r_i = u_i p_1^{k_{i,1}} \cdots p_n^{k_{i,n}}$ and so $q_j \big| p_{j'}$ for some j'. Because $p_{j'}$ is irreducible and q_j is not a unit, we conclude that q_j is a unit multiple of $p_{j'}$. Thus, after reordering the q_j we may write $s = v p_1^{l_1} \cdots p_n^{l_n}$ where v is a unit. Now, the assumption

$$vp_1^{l_1}\cdots p_n^{l_n} = s\big|r_i = u_ip_1^{k_{i,1}}\cdots p_n^{k_{i,n}}$$

for each i such that $r_i \neq 0$ implies $l_j \leqslant k_{i,j}$ by part b, and so $l_j \leqslant m_j$. Another application of part (b) implies $s\big|r$.

(e) Similar to part (d). □

Lemma 2.5.18. *Let R be a UFD, and let $r_0, \ldots, r_d \in R$, not all zero.*

(a) *Let r be a GCD for $\{r_0, \ldots, r_d\}$. Then r' is a GCD for $\{r_0, \ldots, r_d\}$ if and only if $r' = ur$ for some $u \in R^\times$.*

(b) *Let t be a LCM for $\{r_0, \ldots, r_d\}$. Then t' is an LCM for $\{r_0, \ldots, r_d\}$ if and only if $t' = ut$ for some $u \in R^\times$.*

(c) *With notation as in Lemma 2.5.17*(d)*, the elements $r_0, \ldots, r_d$ are relatively prime if and only if $m_j = 0$ for each j.*

(d) *If* $\gcd(r_0, \ldots, r_d) = [r]$, *then $r_i/r \in R$ for all i and* $\gcd(r_0/r, \ldots, r_d/r) = [1]$.

Proof. (a) "$\Longrightarrow$" Assume that r' is a GCD for $\{r_0, \ldots, r_d\}$. Since r is also a GCD for $\{r_0, \ldots, r_d\}$, we have $r\big|r'$ and $r'\big|r$. Hence, $[r] = [r']$ because R is a domain.

"$\Longleftarrow$" Assume $r' = ur$ where u is a unit. Since $r\big|r_i$ for all i, we have $r' = ur\big|r_i$ for all i. Also, if $s\big|r_i$ for all i, then $s\big|r$ and $r\big|r'$, so $s\big|r'$. Thus r' is a GCD for $\{r_0, \ldots, r_d\}$.

(b) Similar to part (a).

(c) Let r be as in Lemma 2.5.17(d). Then $\gcd(r_0, \ldots, r_d) = [r]$. If $r_0, \ldots, r_d$ are relatively prime if and only if $\gcd(r_0, \ldots, r_d) = [1]$ if and only if $[r] = [1]$ if and only if r is a unit if and only if each $m_j = 0$ by Lemma 2.5.17(c).

(d) For each i, we have $r\big|r_i$, so we write $r_i = rr_i'$ for some $r_i' \in R$. The cancellation property shows that r_i' is the unique element of R with this property (in fact, it is the unique element of $\mathrm{Q}(R)$ with this property) and so we write $r_i/r = r_i'$.

In the notation of Lemma 2.5.17, write $r_i = u_ip_1^{k_{i,1}}\cdots p_n^{k_{i,n}}$ for each i and $r = up_1^{m_1}\cdots p_n^{m_n} \in R$. Then $r_i/r = u_iu^{-1}p_1^{k_{i,1}-m_1}\cdots p_n^{k_{i,n}-m_n}$ for each i. For each i and j where $r_i \neq 0$, we have $k_{i,j} \geqslant m_j$, and so $k_{i,j} - m_j \geqslant 0$. And for each j, there is an i such that $r_i \neq 0$ and $k_{i,j} = m_j$. It follows that $\min\{k_{i,j} - m_j \mid r_i/r \neq 0\} = 0$ for each j, and so $p_1^0\cdots p_n^0 = 1$ is a GDC for $\{r_0/r, \ldots, r_d/r\}$. □

Exercise 2.5.19. Let R be an integral domain with field of fractions $Q(R)$. For $a, b \in R$ with $b \neq 0$, we have $a/b \in R$ if and only if $b\big|a$.

Lemma 2.5.20. *Let R be a UFD and set $K = \mathrm{Q}(R)$.*

(a) *Each element of K can be written in the form a/b so that a and b are relatively prime.*

(b) *Let $0 \neq a/b \in K$ with $a, b \in R$. In the notation of Lemma 2.5.17 write $a = up_1^{k_1}\cdots p_n^{k_n}$ and $b = vp_1^{l_1}\cdots p_n^{l_n}$. Then $a/b \in R$ if and only if $k_j \geqslant l_j$ for all j.*

(c) *Given elements $\frac{a_0}{b_0}, \frac{a_1}{b_1}, \ldots, \frac{a_d}{b_d} \in K$, there exists an element $0 \neq b \in K$ such that $b\frac{a_i}{b_i} \in R$ for each i and* $\gcd(b\frac{a_0}{b_0}, b\frac{a_1}{b_1}, \ldots, b\frac{a_d}{b_d}) = [1]$.

(d) *Given elements $a_0, a_1, \ldots, a_d \in R$ such that* $\gcd(a_0, a_1, \ldots, a_d) = [1]$, *if $c \in K$ such that $ca_i \in R$ for each i, then $c \in R$.*

Proof. (a) Let $c/d \in K$ with $c, d \in R$. If $c/d = 0$ then $c/d = 0/1$ has the desired form. Assume that $c/d \neq 0$ and let $[r] = \gcd(c, d)$. (Essentially, we will "divide the top and bottom" of $\frac{c}{d}$ by $\gcd(c, d)$ in order to put the fraction in the desired form.) Then $a = c/r$ and $b = d/r$ are elements of R, and Lemma 2.5.18(d) implies $\gcd(a, b) = [1]$. Furthermore, $\frac{a}{b} = \frac{ar}{br} = \frac{c}{d}$.

(b) Write $c = a/b$ and note that our assumptions imply

$$c = \frac{a}{b} = vw^{-1}p_1^{k_1-l_1} \cdots p_n^{k_n-l_n}.$$

"$\Longleftarrow$" If $k_j \geqslant l_j$ for all j, then $k_j - l_j \geqslant 0$ and so the above display implies $a/b \in R$.

"$\Longrightarrow$" Assume $c = a/b \in R$, and suppose that $k_j < l_j$ for some j. Reorder the p_j to assume that $k_1 - l_1, \ldots, k_t - l_t < 0$ and $k_{t+1} - l_{t+1}, \ldots, k_n - l_n \geqslant 0$. The displayed equality implies

$$p_1^{l_1-k_1} \cdots p_t^{l_t-k_t}c = vw^{-1}p_{t+1}^{k_{t+1}-l_{t+1}} \cdots p_n^{k_n-l_n}.$$

Since p_1 divides the left-hand side, it divides the right-hand side. Thus, $p_1 \big| p_j$ for some $j > 1$, contradicting our assumption $[p_1] \neq [p_j]$.

(c) We use the notation of Lemma 2.5.17: There are prime elements $p_1, \ldots, p_n \in R$ and elements $u_0, \ldots, u_d, v_0, \ldots, v_d \in R^\times \cup \{0\}$ and $k_{i,j}, l_{i,j} \in \mathbb{N}$ for $i = 0, \ldots, d$ and $j = 1, \ldots, n$ such that (1) $[p_j] \neq [p_{j'}]$ when $j \neq j'$, and (2) $a_i = u_i p_1^{k_{i,1}} \cdots p_n^{k_{i,n}}$ and $b_i = v_i p_1^{l_{i,1}} \cdots p_n^{l_{i,n}}$ for each i. If $a_i = 0$, we may take $u_i = 0$, $v_i = 1$ and $k_{i,j} = 0 = l_{i,j}$ for each j. Furthermore,

$$\frac{a_i}{b_i} = u_i v_i^{-1} p_1^{k_{i,1}-l_{i,1}} \cdots p_n^{k_{i,n}-l_{i,n}} \in K.$$

Write $M_j = \max_i\{l_{i,j} - k_{i,j}\}$ and set

$$b = p_1^{M_1} \cdots p_n^{M_n}.$$

It follows that we have

$$b\frac{a_i}{b_i} = u_i v_i^{-1} p_1^{M_1+k_{i,1}-l_{i,1}} \cdots p_n^{M_n+k_{i,n}-l_{i,n}}.$$

To finish the proof we have two things to show.

$b\frac{a_i}{b_i} \in R$ for each i. For this, it suffices to show $M_j + k_{i,j} - l_{i,j} \geqslant 0$ for each j. This inequality follows from the fact that $M_j \geqslant l_{i,j} - k_{i,j}$.

$\gcd(b\frac{a_0}{b_0}, b\frac{a_1}{b_1}, \ldots, b\frac{a_d}{b_d}) = [1]$. For this, it suffices to show, for each j, there is an i such that $M_j + k_{i,j} - l_{i,j} = 0$; then apply Lemma 2.5.18(c). Fix j and choose i such that $M_j = l_{i,j} - k_{i,j}$. This i works.

(d) Write $c = r/s$ so that $\gcd(r, s) = [1]$. Assume without loss of generality that $r/s \neq 0$. There are prime elements $p_1, \ldots, p_n \in R$ and elements $u_0, \ldots, u_d, v, w \in R^\times \cup \{0\}$ and $k_{i,j}, l_j, m_j \in \mathbb{N}$ for $i = 0, \ldots, d$ and $j = 1, \ldots, n$ such that (1) $[p_j] \neq [p_{j'}]$ when $j \neq j'$, and (2) $a_i = u_i p_1^{k_{i,1}} \cdots p_n^{k_{i,n}}$ for each i and $r = vp_1^{l_1} \cdots p_n^{l_n}$ and $s = wp_1^{m_1} \cdots p_n^{m_n}$. If $a_i = 0$, we may take $u_i = 0$ and $k_{i,j} = 0$ for each j. Note that, for each j, either $l_j = 0$ or $m_j = 0$ or both. We have

$$c = \frac{r}{s} = vw^{-1}p_1^{l_1-m_1} \cdots p_n^{l_n-m_n}$$

and, for each i

$$ca_i = \frac{r}{s}a_i = vw^{-1}u_i p_1^{k_{i,1}+l_1-m_1} \cdots p_n^{k_{i,n}+l_n-m_n}$$

The proof will be complete once we show $l_j \geqslant m_j$ for each j. Our assumption $ca_i \in R$ implies $k_{i,j} + l_j - m_j \geqslant 0$ for each i, j by part (b); that is $l_j \geqslant m_j - k_{i,j}$. The assumption $\gcd(a_0, a_1, \ldots, a_d) = [1]$ implies that, for each j there is an i such that $k_{i,j} = 0$. This choice of i yields $l_j \geqslant m_j - 0 = m_j$. □

Exercise 2.5.21. Let R be a UFD. If $a, b, c \in R$ and $a \big| bc$ and $\gcd(a, b) = [1]$, then $a \big| c$.

Definition 2.5.22. Let R be an integral domain. If every ideal of R is principal, then R is a *principal ideal domain* or PID for short.

Example 2.5.23. $\mathbb{Z}$ is a PID. A field k is a PID. We will see below that every PID is a UFD, but not every UFD is a PID.

The next lemma says that every PID is noetherian. More on this later.

Lemma 2.5.24. *Let R be a PID. Given a chain of ideals $I_1 \subseteq I_2 \subseteq \cdots \subseteq R$, there exists an integer $N \geqslant 1$ such that, for every $n \geqslant N$ we have $I_n = I_N$.*

Proof. Each ideal I_j is principal, say $I_j = (a_j)R$. As in the proof of Proposition 2.3.13, since the ideals I_j form a chain, the union $I = \cup_{j \geqslant 1} I_j$ is an ideal of R. Hence $I = (a)R$ for some $a \in I = \cup_{j \geqslant 1} I_j$, say $a \in I_N$. For each $n \geqslant N$, we have

$$I_N \subseteq I_n \subseteq I = (a)R \subseteq I_N$$

and so $I_n = I_N$. □

We will see below that the converse to the next result fails: If k is a field, then the polynomial ring $k[x, y]$ is a UFD and not a PID.

Theorem 2.5.25. *Every PID is a UFD.*

Proof. Let R be a PID.

Step 1. Every irreducible element $x \in R$ is prime; moreover, the ideal (x) is maximal. Let I be an ideal such that $(x)R \subseteq I \subseteq R$. There is an element $a \in I$ such that $I = (a)R$, and so $(x)R \subseteq (a)R$. By an exercise, this means $a \big| x$, say $x = ab$. Since x is irreducible, either a or b is a unit. If a is a unit, then $I = (a)R = R$. If b is a unit, then $I = (a)R = (ab)R = (x)R$. Thus, $(x)R$ is maximal. Proposition 2.3.14(b) implies that $(x)R$ is prime, hence x is prime.

Step 2. Every non-zero nonunit $y \in R$ has an irreducible factor. If y is irreducible, then y is an irreducible factor of y and we are done. So, assume y is not irreducible. Then $y = y_1 z_1$ where y_1, z_1 are non-zero nonunits. If y_1 is irreducible, then it is an irreducible factor of y and we are done. So, assume y_1 is not irreducible. Then $y_1 = y_2 z_2$ where y_2, z_2 are non-zero nonunits. Continue this process, writing $y_n = y_{n+1} z_{n+1}$. Eventually, y_n will be irreducible, as follows.

Suppose $y_n = y_{n+1} z_{n+1}$ for $n = 1, 2, \ldots$ where y_i, z_i are non-zero nonunits for each i. Then $y_{n+1} \big| y_n$ for each n, and so we have

$$(y_1)R \subseteq (y_2)R \subseteq (y_3)R \subseteq \cdots .$$

By Lemma 2.5.24, we have $(y_N) = (y_{N+1})$ for some $N \geqslant 1$. Since $y_N = y_{N+1} z_{N+1}$, this implies z_{N+1} is a unit, a contradiction.

Step 3. Every non-zero nonunit $z \in R$ can be written as a finite product of irreducible elements. By Step 2, we know that z has an irreducible factor z_1, say $z = z_1 w_1$. If w_1 is a unit, then z is irreducible and we are done. So, assume that w_1 is a nonunit, necessarily non-zero because $z \neq 0$. Then w_1 has an irreducible factor

z_2, say $w_1 = z_2 w_2$. Continuing this process, we see that the argument of Step 2 implies that the process terminates in finitely many steps, yielding a factorization $z = z_1 \cdots z_N$ with each z_i irreducible.

Now apply Proposition 2.5.13 to conclude that R is a UFD. □

Definition 2.5.26. An integral domain R is a *Euclidean domain* or ED for short if there exists a function $\varphi\colon R - \{0\} \to \mathbb{N}$ satisfying the following property: for all $a, b \in R$, if $b \neq 0$, then there exist $q, r \in R$ such that $a = bq + r$ and either $r = 0$ or $\varphi(r) < \varphi(b)$.

Example 2.5.27. In $\mathbb{Z}$ let $\varphi(n) = |n|$. This is the division algorithm.

Theorem 2.5.28. *Every ED is a PID.*

Proof. Let R be an ED and fix an ideal $0 \neq I \subseteq R$. We need to find an element $b \in I$ such that $I = (b)R$. The set

$$\{\varphi(a) \mid 0 \neq a \in I\}$$

is a non-empty subset of $\mathbb{N}$ and hence has a minimal element. That is, there is an element $0 \neq b \in I$ such that $\varphi(b) \leqslant \varphi(c)$ for all $c \in I$.

Claim: $I = (b)R$. Since $b \in I$, we know $I \supseteq (b)R$. For the containment $I \subseteq (b)R$, fix an element $a \in I$. By assumption, there exist $q, r \in R$ such that $a = bq + r$ and either $r = 0$ or $\varphi(r) < \varphi(b)$. Notice that $a, bq \in I$ and so $r = a - bq \in I$. If $r \neq 0$, then $\varphi(r) < \varphi(b)$; however, the minimality of $\varphi(b)$ implies $\varphi(r) \geqslant \varphi(b)$, a contradiction. Hence $r = 0$ and so $a = bq \in (b)R$. □

Remark 2.5.29. In summary, we have the following: ED$\overset{(2.5.28)}{\Longrightarrow}PID\overset{(2.5.25)}{\Longrightarrow}$UFD and ED $\overset{\mathbb{Z}[\sqrt{-19}/2]}{\not\Longleftarrow}$ PID $\overset{k[x,y]}{\not\Longleftarrow}$ UFD. We will see below that, if R is a UFD, then the polynomial ring $R[x_1, \ldots, x_n]$ is a UFD. In particular, if k is a field, then $k[x_1, \ldots, x_n]$ is a UFD. However, if $n \geqslant 1$, then $R[x_1, \ldots, x_n]$ is a PID if and only if R is a field and $n = 1$ if and only if $R[x_1, \ldots, x_n]$ is an ED.

2.6. Polynomial rings

Definition 2.6.1. Let R be a ring. We define the polynomial ring in one indeterminate over R as follows: Let $R[x]$ denote the additive abelian group

$$R^{(\mathbb{N})} = \{(r_0, r_1, r_2, \ldots) \mid r_j \in R \text{ for all } j \geqslant 0 \text{ and } r_j = 0 \text{ for } j \gg 0\}.$$

Hence, addition and subtraction are defined coordinatewise

$$(r_0, r_1, r_2, \ldots) + (s_0, s_1, s_2, \ldots) = (r_0 + s_0, r_1 + s_1, r_2 + s_2, \ldots)$$
$$(r_0, r_1, r_2, \ldots) - (s_0, s_1, s_2, \ldots) = (r_0 - s_0, r_1 - s_1, r_2 - s_2, \ldots)$$
$$0_{R[x]} = (0_R, 0_R, 0_R, \ldots).$$

Define multiplication via the formula

$$(r_0, r_1, r_2, \ldots)(s_0, s_1, s_2, \ldots) = (c_0, c_1, c_2, \ldots)$$

where

$$c_j = \textstyle\sum_{i=0}^{j} r_i s_{j-i} = \sum_{m+n=j} r_m s_n.$$

Computations:

$$(0, \ldots, 0, r_i, r_{i+1}, r_{i+2}, \ldots, r_d, 0, \ldots)(0, \ldots, 0, s_j, s_{j+1}, s_{j+2}, \ldots, s_e, 0, \ldots)$$
$$= (0, \ldots, 0, r_i s_j, r_i s_{j+1} + r_{i+1} s_j, r_i s_{j+2} + r_{i+1} s_{j+1} + r_{i+2} s_j, \ldots, r_d s_e, 0, \ldots).$$

and

$$(r_0, r_1, r_2, \ldots)(s, 0, 0, \ldots) = (r_0 s, r_1 s, r_2 s, \ldots).$$

The *degree* of $(r_0, r_1, r_2, \ldots)$ is $\deg((r_0, r_1, r_2, \ldots)) = \sup\{i \geqslant 0 \mid r_i \neq 0\}$.

Proposition 2.6.2. *Let R be a commutative ring with identity and let $0 \neq f, g \in R[x]$.*

(a) *If $fg \neq 0$, then $\deg(fg) \leqslant \deg(f) + \deg(g)$.*
(b) *If the leading coefficient of f is not a zero-divisor (e.g., if the leading coefficient of f is a unit or if R is an integral domain), then $\deg(fg) = \deg(f) + \deg(g)$.*
(c) *If $f + g \neq 0$, then $\deg(f + g) \leqslant \max\{\deg(f), \deg(g)\}$.*
(d) *If $\deg(f) \neq \deg(g)$, then $f + g \neq 0$ and $\deg(f + g) = \max\{\deg(f), \deg(g)\}$.*

Proof. (a) and (b). Let $d = \deg(f)$ and $e = \deg(g)$. The computation of Definition 2.6.1 shows that $\deg(fg) \leqslant d + e = \deg(f) + \deg(g)$. Furthermore, the coefficient of x^{d+e} in fg is the product of the leading coefficients of f and g. So, equality holds if the product of the leading coefficients of f and g is non-zero.

(c) and (d) follow from similar computations. □

Theorem 2.6.3. *Let R be a ring.*

(a) *With the above operations, $R[x]$ is a ring.*
(b) *The function $f\colon R \to R[x]$ given by $f(r) = (r, 0, 0, \ldots)$ is a monomorphism of rings.*
(c) *R is commutative if and only if $R[x]$ is commutative.*
(d) *R has identity if and only if $R[x]$ has identity.*
(e) *R is an integral domain if and only if $R[x]$ is an integral domain.*
(f) *$R[X]$ is never a field.*

Proof. (a) We already know that $R[x]$ is an additive abelian group, so it remains to show that multiplication is well-defined, associative, and distributive. For well-definedness, we only need to check closure. Fix $(r_0, r_1, r_2, \ldots), (s_0, s_1, s_2, \ldots) \in R[x]$. The element $c_j = \sum_{i=0}^{j} r_i s_{j-i}$ is a finite sum of products of elements of R and, hence, is in R. And the above computation shows that $c_j = 0$ for $j \gg 0$. The proofs of associativity and distributivity are exercises.

(b) By definition, we have

$$f(r + s) = (r + s, 0, 0, \ldots) = (r, 0, 0, \ldots) + (s, 0, 0, \ldots) = f(r) + f(s)$$

$$f(rs) = (rs, 0, 0, \ldots) = (r, 0, 0, \ldots)(s, 0, 0, \ldots) = f(r)f(s).$$

To see that f is a monomorphism: $f(r) = 0$ if and only if $(r, 0, 0, \ldots) = (0, 0, 0, \ldots)$ if and only if $r = 0$.

(c) ($\Longrightarrow$) Assume that R is commutative. Then

$$\sum_{m+n=j} r_m s_n = \sum_{m+n=j} s_m r_n.$$

The left-hand side is the jth entry of the product $(r_0, r_1, r_2, \ldots)(s_0, s_1, s_2, \ldots)$, and the right-hand side is the jth entry of the product $(s_0, s_1, s_2, \ldots)(r_0, r_1, r_2, \ldots)$.

($\Longleftarrow$) Assume that $R[x]$ is commutative. For $r, s \in R$, we have $f(rs) = f(r)f(s) = f(s)f(r) = f(sr)$. Since f is 1-1, this implies $rs = sr$.

(d) ($\implies$) Assume that R has identity 1. Then $(1,0,0,\ldots)$ is a multiplicative identity for $R[x]$:

$$(1,0,0,\ldots)(r_0,r_1,r_2,\ldots) = (1r_0,1r_1,1r_2,\ldots) = (r_0,r_1,r_2,\ldots)$$

and similarly for $(r_0,r_1,r_2,\ldots)(1,0,0,\ldots)$.

($\impliedby$) Assume that $R[x]$ has identity $(e_0,e_1,e_2,\ldots)$. It follows that, for all $r \in R$, we have

$$(r,0,0,\ldots) = (r,0,0,\ldots)(e_0,e_1,e_2,\ldots) = (re_0,re_1,re_2,\ldots)$$

and so $re_0 = r$. Similarly, we have $e_0r = r$ and so e_0 is a multiplicative identity for R.

(e) ($\implies$) Assume that R is an integral domain. Then R is a non-zero commutative ring with identity, and so the same is true of $R[x]$. Fix elements $0 \neq (r_0,r_1,r_2,\ldots),(s_0,s_1,s_2,\ldots) \in R$. Then there exist $i,j \geqslant 0$ such that $r_i \neq 0$ and $r_m = 0$ for all $m < i$ and $s_j \neq 0$ and $s_n = 0$ for all $n < j$. Then, we have $r_is_j \neq 0$ and so

$$\begin{aligned}
&(r_0,r_1,r_2,\ldots)(s_0,s_1,s_2,\ldots)\\
&\quad= (0,\ldots,0,r_i,r_{i+1},r_{i+2},\ldots)(0,\ldots,0,s_j,s_{j+1},s_{j+2},\ldots)\\
&\quad= (0,\ldots,0,r_is_j,r_is_{j+1}+r_{i+1}s_j,r_is_{j+2}+r_{i+1}s_{j+1}+r_{i+2}s_j,\ldots,r_ds_e,0,\ldots)\\
&\quad\neq 0
\end{aligned}$$

($\impliedby$) Assume that $R[x]$ is an integral domain. Then $R[x]$ is a non-zero commutative ring with identity, and so the same is true of R. Suppose $0 \neq r,s \in R$. Then $f(r), f(s) \neq 0$ and so

$$f(rs) = f(r)f(s) \neq 0$$

and so $rs \neq 0$.

(f) Suppose that $R[X]$ is a field. Part (e) implies that R is an integral domain. Proposition 2.6.2(b) implies that no polynomial of positive degree has a multiplicative inverse in $R[X]$, contradiction. □

Remark 2.6.4. We frequently identify R with its image in $R[x]$. This yields formulas like:

$$r(r_0,r_1,r_2,\ldots) = (rr_0,rr_1,rr_2,\ldots).$$

Here is a more familiar presentation:

Proposition 2.6.5. *Let R be a ring with identity and set $x = (0,1,0,0,\ldots)$ in $R[x]$.*

(a) *For each $n \geqslant 1$, we have $x^n = (\underbrace{0,0,\ldots,0}_{n},1,0,0,\ldots)$.*

(b) *For each $r \in R$ and each $n \geqslant 1$, we have*

$$rx^n = (\underbrace{0,0,\ldots,0}_{n},r,0,0,\ldots) = x^nr.$$

(c) *For each $f \in R[x]$ there is an integer $d \geqslant 0$ and elements $r_0,r_1,\ldots,r_d \in R$ such that*

$$f = \textstyle\sum_{i=0}^{d} r_ix^i = r_0 + r_1x + r_2x^2 + \cdots + r_dx^d.$$

Proof. (a) Exercise. By induction on n.

(b) From part (a).

(c) We have

$$\begin{aligned} f &= (r_0, r_1, r_2, \ldots, r_d, 0, 0, \ldots) \\ &= r_0(1, 0, 0, \ldots) + r_1(0, 1, 0, \ldots) + \cdots + r_d(0, 0, \ldots, 0, 1, 0, \ldots) \\ &= r_0 + r_1 x + r_2 x^2 + \cdots + r_d x^d. \end{aligned}$$

□

Remark 2.6.6. Proposition 2.6.5(c) says that the monomials $1, x, x^2, \ldots$ span $R[x]$ over R. The uniqueness of representation of polynomials ($f = 0$ if and only if all the coefficients of f are 0) says that these monomials are linear independent over R, so they form a basis of $R[x]$ over R.

Definition 2.6.7. Let R be a ring. The polynomial ring in two indeterminates over R is the ring

$$R[x, y] = R[x][y] \qquad \text{or} \qquad R[x_1, x_2] = R[x_1][x_2].$$

Inductively, the polynomial ring in n indeterminates over R is the ring

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

The next result follows from the previous ones using induction on n. See also Hungerford pp. 151-152.

Proposition 2.6.8. *Let R be a ring and $n \geqslant 1$.*

(a) *$R[x_1, \ldots, x_n]$ is a ring.*

(b) *Assume that R has identity. Let $f \in R[x_1, \ldots, x_n]$. For each element $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{N}^n$ there is an element $r_{\mathbf{a}} \in R$ such that $r_{\mathbf{a}} = 0$ for all but finitely many $\mathbf{a} \in \mathbb{N}^n$ and*

$$f = \textstyle\sum_{\mathbf{a} \in \mathbb{N}^n} r_{\mathbf{a}} x_1^{a_1} \cdots x_n^{a_n}.$$

(c) *Assume that R has identity. The function $f \colon R \to R[x_1, \ldots, x_n]$ given by $f(r) = r x_1^0 \cdots x_n^0$ is a monomorphism of rings.*

(d) *R is commutative if and only if $R[x_1, \ldots, x_n]$ is commutative.*

(e) *R has identity if and only if $R[x_1, \ldots, x_n]$ has identity.*

(f) *R is an integral domain if and only if $R[x_1, \ldots, x_n]$ is an integral domain.*

(g) *For each k such that $1 < k < n$, there is an isomorphism $R[x_1, \ldots, x_n] \cong R[x_1, \ldots, x_k][x_{k+1}, \ldots, x_n]$.*

(h) *For each $\sigma \in S_n$ there is an isomorphism $R[x_1, \ldots, x_n] \cong R[x_{\sigma(1)}, \ldots, x_{\sigma(n)}]$.*

(i) *Assume that R has identity. For all $r, s \in R$ and all $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{N}$, we have*

$$(r x_1^{a_1} \cdots x_n^{a_n})(s x_1^{b_1} \cdots x_n^{b_n}) = rs x_1^{a_1+b_1} \cdots x_n^{a_n+b_n}.$$

□

Definition 2.6.9. If S is a ring, then the *center* of S is

$$Z(S) = \{s \in S \mid ss' = s's \text{ for all } s' \in S\}.$$

Using the subring test, we see that the center $Z(S)$ is a subring of S.

Let R be a commutative ring with identity. For each $r \in R$, set $r^0 = 1$.

An *R-algebra* is a ring S with identity equipped with a homomorphism of rings with identity $f\colon R \to S$ such that $\operatorname{Im}(f) \subseteq Z(S)$.

Let S and T be R-algebras via the maps $f\colon R \to S$ and $g\colon R \to T$. A *homomorphism of R-algebras* from S to T is a ring homomorphism $h\colon S \to T$ making the following diagram commute.

$$\begin{tikzcd}
R \arrow[r, "f"] \arrow[dr, "g"'] & S \arrow[d, dashed, "\exists! h"] \\
& T
\end{tikzcd}$$

Note that, because $f(1) = 1$ and $g(1) = 1$, we have $h(1) = 1$.

Example 2.6.10. Let R be a commutative ring with identity.

R is an R-algebra via the identity map $R \to R$.

The polynomial ring $R[x_1, \ldots, x_n]$ is an R-algebra via the natural map $R \to R[x_1, \ldots, x_n]$.

The ring $M_n(R)$ of $n \times n$ matrices with entries from R is an R-algebra via the map $R \to M_n(R)$ given by

$$r \mapsto rI_n = \begin{pmatrix} r & 0 & \cdots & 0 \\ 0 & r & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & r \end{pmatrix}.$$

Here is the universal property for polynomial rings. It includes the prototype for R-algebra homomorphisms. The maps h are often called evaluation homomorphisms: they are given by $P(x_1, \ldots, x_n) \mapsto P(s_1, \ldots, s_n)$.

Proposition 2.6.11. *Let R be a commutative ring with identity, and let $f\colon R \to R[x_1, \ldots, x_n]$ be the natural map. Let S be an R-algebra via the homomorphism $g\colon R \to S$. For each list $s_1, \ldots, s_n \in Z(S)$ there exists a unique homomorphism of R-algebras $h\colon R[x_1, \ldots, x_n] \to S$ such that $h(x_i) = s_i$ for each i. In particular, the following diagrams commute*

$$\begin{tikzcd}
R \arrow[r, "f"] \arrow[dr, "g"'] & R[x_1, \ldots, x_n] \arrow[d, dashed, "\exists! h"] \\
& S
\end{tikzcd}
\qquad
\begin{tikzcd}
\{x_1, \ldots, x_n\} \arrow[r] \arrow[dr] & R[x_1, \ldots, x_n] \arrow[d] \\
& S
\end{tikzcd}$$

and S is an $R[x_1, \ldots, x_n]$-algebra.

Proof. Define h by the following formula:

$$h(\textstyle\sum_{\mathbf{a} \in \mathbb{N}^n} r_{\mathbf{a}} x_1^{a_1} \cdots x_n^{a_n}) = \sum_{\mathbf{a} \in \mathbb{N}^n} g(r_{\mathbf{a}}) s_1^{a_1} \cdots s_n^{a_n}$$

where $\mathbf{a} = (a_1, \ldots, a_n)$. The uniqueness of representation of polynomials shows that this is well-defined. It is routine to check that h is a ring homomorphism with the desired properties. For instance, the first diagram commutes because

$$h(f(r)) = h(rx_1^0 \cdots x_n^0) = g(r)s_1^0 \cdots s_n^0 = g(r)1_s = g(r).$$

For the uniqueness of h, suppose that $H\colon R[x_1, \ldots, x_n] \to S$ is another homomorphism of R-algebras such that $H(x_i) = s_i$ for each i. For each $\mathbf{a} \in \mathbb{N}^n$ and each

$r_{\mathbf{a}} \in R$, we then have

$$\begin{aligned} H(r_{\mathbf{a}} x_1^{a_1} \cdots x_n^{a_n}) &= H(f(r_{\mathbf{a}}))H(x_1)^{a_1} \cdots H(x_n)^{a_n} \\ &= g(r_{\mathbf{a}}) s_1^{a_1} \cdots s_n^{a_n} \\ &= h(r_{\mathbf{a}} x_1^{a_1} \cdots x_n^{a_n}). \end{aligned}$$

Since H preserves finite sums, it follows that

$$h(\textstyle\sum_{\mathbf{a}\in\mathbb{N}^n} r_{\mathbf{a}} x_1^{a_1} \cdots x_n^{a_n}) = \sum_{\mathbf{a}\in\mathbb{N}^n} g(r_{\mathbf{a}}) s_1^{a_1} \cdots s_n^{a_n} = H(\sum_{\mathbf{a}\in\mathbb{N}^n} r_{\mathbf{a}} x_1^{a_1} \cdots x_n^{a_n})$$

and so $H = h$. □

Corollary 2.6.12. *Let R be a commutative ring with identity, and let $f\colon R \to R[x_1, \ldots, x_n]$ be the natural map. For each list $r_1, \ldots, r_n \in R$ there exists a unique homomorphism of R-algebras $h\colon R[x_1, \ldots, x_n] \to r$ such that $h(x_i) = r_i$ for each i. In particular, the following diagrams commute:*

$$\begin{tikzcd} R \arrow[r, "f"] \arrow[dr, "\mathrm{id}"'] & R[x_1, \ldots, x_n] \arrow[d, dashed, "\exists! h"] \\ & R \end{tikzcd} \qquad \begin{tikzcd} \{x_1, \ldots, x_n\} \arrow[r] \arrow[dr] & R[x_1, \ldots, x_n] \arrow[d] \\ & R. \end{tikzcd}$$

Given a polynomial $P = P(x_1, \ldots, x_n)$ we write $h(P) = P(r_1, \ldots, r_n)$. □

Here is the division algorithm for polynomial rings. As with the division algorithm in $\mathbb{Z}$, this is the key to all the factorization properties in $R[x]$.

Theorem 2.6.13. *Let R be a commutative ring with identity, and fix a polynomial $f = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$ such that a_n is a unit in R. For each polynomial $g \in R[x]$ there exist unique $q, r \in R[x]$ such that $g = qf + r$ and either $r = 0$ or* $\deg(r) < \deg(f)$.

Proof. First, we deal with existence.

Because a_n is a unit in R, we may assume without loss of generality that $a_n = 1$. We may also assume without loss of generality that f is not a constant polynomial. In particular, we have $\deg(f) \geqslant 1$.

If $g = 0$ or $\deg(g) < \deg(f)$, then the polynomials $q = 0$ and $r = g$ satisfy the desired conclusions.

We assume that $g \neq 0$ and proceed by induction on $d = \deg(g)$. The base case $d = 0$ follows from the previous paragraph, as do the cases $d < \deg(f)$. Therefore, assume that $d \geqslant \deg(f)$ and that the result holds for all polynomials $h \in R[x]$ such that $\deg(h) < d$. Let b_d be the leading coefficient of g. Then the polynomial $h = g - b_d x^{d-n} f$ is either 0 or has $\deg(h) < d$. Hence, the induction hypothesis provides polynomials $q_1, r \in R[x]$ such that

$$q_1 f + r = h = g - b_d x^{d-n} f$$

and either $r = 0$ or $\deg(r) < \deg(f)$. It follows that

$$g = [q_1 + b_d x^{d-n}] f + r$$

so the polynomials $q = q_1 + b_d x^{d-n}$ and r satisfy the desired properties.

Now for uniqueness. Assume $qf + r = g = q_2 f + r_2$ where (1) either $r = 0$ or $\deg(r) < \deg(f)$, and (2) either $r_2 = 0$ or $\deg(r_2) < \deg(f)$. Then $r - r_2 = (q_2 - q)f$.

The leading coefficient of f is a unit. If $q \neq q_2$, then $r - r_2 = (q_2 - q)f \neq 0$. In particular, either $r \neq 0$ or $r_2 \neq 0$. If $r, r_2 \neq 0$, then Proposition 2.6.2 implies

$$\begin{aligned}\deg(f) &\leqslant \deg(f) + \deg(q_2 - q) = \deg((q_2 - q)f)\\ &= \deg(r - r_2) \leqslant \max\{\deg(r), \deg(r_2)\} < \deg(f)\end{aligned}$$

a contradiction. The cases where $r = 0$ or $r_2 = 0$ similarly yield contradictions. Thus, we have $q = q_2$ and $r - r_2 = (q_2 - q)f = 0$ and so $r = r_2$. □

Corollary 2.6.14 (Remainder Theorem)**.** *Let R be a commutative ring with identity, and fix $s \in R$. For each polynomial $g \in R[x]$ there exist unique $q \in R[x]$ such that $g = q \cdot (x - s) + g(s)$.*

PROOF. Apply the division algorithm. It suffices to show that $r = g(s)$. Because either $r = 0$ or $\deg(r) < \deg(x - s) = 1$, we know that r is constant. The evaluation homomorphism yields

$$g(s) = q(s)(s - s) + r(s) = 0 + r = r$$

as desired. □

Definition 2.6.15. Let R be a commutative ring with identity and $P \in R[x]$. An element $r \in R$ is a *root* of P if $P(r) = 0$.

Proposition 2.6.16. *Let S be an integral domain and $R \subseteq S$ a non-zero subring such that R has identity.*

(a) *Then R is an integral domain and $1_S = 1_R$.*
(b) *If $0 \neq f \in R[x]$ and* $\deg(f) = n$, *then f has at most n roots in S; in particular, f has at most n roots in R.*

The conclusions in this result fail if S is not an integral domain.

PROOF. (a) It is straightforward to show that R is an integral domain. To see that $1_R = 1_S$, note that $1_S 1_R = 1_R = 1_R 1_R$, so that cancellation implies $1_S = 1_R$.

(b) Proceed by induction on $n = \deg(f)$. If $n = 0$, then f is a non-zero constant and therefore has no roots.

Inductively, assume that the result holds for polynomials of degree $< n$. If f has no roots in S, then we are done. So assume that $s \in S$ is a root of f. The Remainder Theorem implies that there is a unique $q \in S[x]$ such that $f = (x - s)q$. By Proposition 2.6.2(b) we have $\deg(q) = \deg(f) - 1 = n - 1 < n$, and so the induction hypothesis implies that q has at most $n - 1$ roots in S.

Let $t \in S$ be a root of f. Since the map $S[x] \to S$ given by $P \mapsto P(t)$ is a ring homomorphism, it implies that $0 = f(t) = (t - s)q(t)$. Since S is an integral domain, either $t - s = 0$ or $q(t) = 0$. That is, either $t = s$ or t is a root of q. Since q has at most $n - 1$ roots, this implies that f has at most n roots. □

Example 2.6.17. Let $R = \mathbb{R}[x]/(x^2)$ and set $\overline{x} = x + (x^2) \in R$. Then the polynomial $y^2 \in R[y]$ has infinitely many roots, namely, every element of the form $\lambda\overline{x}$ for some $\lambda \in \mathbb{R}$.

Remark 2.6.18. Here is a word of warning. Let $P \in \mathbb{R}[x]$. From calculus/college algebra we know that $P = 0$ if and only if $P(r) = 0$ for all $r \in \mathbb{R}$. This can fail if $\mathbb{R}$ is replaced with an arbitrary ring R, even when R is a field.

For example, let p be a positive prime integer and set $R = \mathbb{Z}/p\mathbb{Z}$. It is a fact that, for each $\overline{n} \in R$, we have $\overline{n}^p = \overline{n}$. (This is called Fermat's Little Theorem.) In particular, every element of R is a root of the polynomial $x^p - x$, even though this polynomial is non-zero. This shows the importance of distinguishing between the polynomial P and the function $R \to R$ given by evaluating the polynomial P.

Note, however, that this is only a problem with finite fields as the following can by shown relatively easily using Proposition 2.6.16(b): If k is an *infinite* field and $P \in k[x]$ has infinitely many roots in k, then $P = 0$.

2.7. Factorization in Polynomial Rings

Definition 2.7.1. Let R be a UFD and $0 \neq f = a_0 + a_1x + \cdots + a_dx^d \in R[x]$. A *content* of f is a greatest common divisor of $\{a_0, a_1, \ldots, a_d\}$ in R. The polynomial f is *primitive* if 1 is a content for f, that is, if the coefficients of f are relatively prime.

Remark 2.7.2. Let R be a UFD and $0 \neq f = a_0 + a_1x + \cdots + a_dx^d \in R[x]$.

Recall that greatest common divisors are not uniquely defined. Specifically, if r and s are greatest common divisors of $\{a_0, a_1, \ldots, a_d\}$ in R, then there is a unit $u \in R$ such that $s = ur$. Conversely, if r is a greatest common divisor of $\{a_0, a_1, \ldots, a_d\}$ in R and $u \in R$ is a unit, then ur is a greatest common divisor of $\{a_0, a_1, \ldots, a_d\}$ in R.

We say that $r, s \in R$ are *associates* if there is a unit $u \in R$ such that $s = ur$. Write $r \approx s$ when r and s are associates in R. The relation $\approx$ is an equivalence relation, and the equivalence class of r under this relation is denoted $[r]$. By definition, $[r]$ is the set of all unit multiples of r in R. Note that $[r] = [1]$ if and only if r is a unit in R.

If r, s are contents of f, then the above discussion implies $[r] = [s]$, and we write $C(f) = [r]$. (This notation is not standard. However, most books write $C(f) = r$ or $C(f) \approx r$, which is not well defined.) Conversely, if r is a content for f and $[r] = [s]$, then s is a content for f. Also, if f is constant $f = a_0$, then $C(f) = [a_0]$.

If $r \approx r_1$ and $s \approx s_1$, then $rs \approx r_1s_1$. Hence, the assignment $[r][s] = [rs]$ is well-defined.

Exercise 2.7.3. Let R be a UFD and $0 \neq f = a_0 + a_1x + \cdots + a_dx^d \in R[x]$.

(a) Show that $C(tf) = [t]C(f)$ for each $t \in R$.
(b) Show that, if $C(f) = [r]$, then there is a primitive polynomial g such that $f = rg$.

The following few results are due to Gauss.

Lemma 2.7.4. *Let R be a UFD and let $0 \neq f, g \in R[x]$.*

(a) *If f and g are primitive, then so is fg.*
(b) *$C(fg) = C(f)C(g)$.*

Proof. (a) Assume that f and g are primitive and let $C(fg) = [r]$. We want $[r] = [1]$, that is, we want to show that r is a unit. Note that $r \neq 0$: since R is an integral domain, so is $R[x]$ and so $fg \neq 0$.

Suppose that r is not a unit. Since R is a UFD, this implies that r has a prime factor p. The function $\tau\colon R[x] \to (R/(p))[x]$ given by $\tau(\sum_i a_ix^i) = \sum_i \overline{a_i}x^i$ is a well-defined epimorphism of rings with identity. Check this using the universal property for polynomial rings with the following diagram as your guide:

$$\begin{tikzcd}
R \arrow[r] \arrow[d] & R[x] \arrow[d, dashed, "\tau"] \\
R/(p) \arrow[r] & (R/(p))[x].
\end{tikzcd}$$

Since $p\big|r$ and $C(fg) = [r]$, we see that p divides each coefficient of fg and so $\tau(fg) = 0$. On the other hand, since f is primitive, we know that p does not divide at least one coefficient of f, and so $\tau(f) \neq 0$. Similarly, we have $\tau(g) \neq 0$. Since p is prime, the ring $R/(p)$ is an integral domain, and hence so is $(R/(p))[x]$. It follows that $0 \neq \tau(f)\tau(g) = \tau(fg)$, a contradiction.

(b) Write $C(f) = [r]$ and $C(g) = [s]$. Use Exercise 2.7.3(b) to find primitive polynomials $f_1, g_1 \in R[x]$ such that $f = rf_1$ and $g = sg_1$. Note that part (a) implies $C(f_1g_1) = [1]$. This explains the third equality in the next sequence:

$$C(fg) = C((rs)(f_1g_1)) = [rs]C(f_1g_1) = [rs] = [r][s] = C(f)C(g).$$

The first equality is by our choice of f_1 and g_1; the second equality is by Exercise 2.7.3(a); the remaining equalities are by definition. □

Lemma 2.7.5. *Let R be a UFD and let $0 \neq f, g \in R[x]$ and $0 \neq r \in R$.*

(a) *fg is primitive if and only if f and g are primitive.*
(b) *rf is primitive if and only if f is primitive and r is a unit.*
(c) *If f is irreducible in $R[x]$, then f is either constant or primitive.*

Proof. (a) ($\Longleftarrow$) Lemma 2.7.4(a).

($\Longrightarrow$) Assume that fg is primitive. With $C(f) = [r]$ and $C(g) = [s]$, we have

$$[1] = C(fg) = C(f)C(g) = [r][s] = [rs].$$

It follows that rs is a unit in R, and so r and s are units in R. Hence f and g are primitive.

(b) This is the special case of part (a) where $g = r$.

(c) Assume that f is irreducible and not constant. Suppose $C(f) = [r]$ where r is not a unit in R. Then there exists a nonconstant primitive polynomial $f_1 \in R[x]$ such that $f = rf_1$. This gives a factorization of f as a product of two nonunits, contradicting the assumption that f is irreducible. □

Lemma 2.7.6. *Let R be a UFD and set $K = \mathrm{Q}(R)$. Let $0 \neq f \in K[x]$.*

(a) *There exists an element $0 \neq b \in \mathrm{Q}(R)$ such that $bf \in R[x]$ and $C(bf) = [1]$.*
(b) *If $c \in K$ and $0 \neq F \in R[x]$ is primitive such that $cF \in R[x]$, then $c \in R$.*
(c) *If $h \in R[x]$ is primitive and $fh \in R[x]$, then $f \in R[x]$.*

Proof. (a) Write $f = \frac{a_0}{b_0} + \frac{a_1}{b_1}x + \cdots + \frac{a_d}{b_d}x^d$ with each $a_i, b_i \in R$ and $b_i \neq 0$. Lemma 2.5.20(c) shows that there exists an element $b \in K$ such that $b\frac{a_i}{b_i} \in R$ for each i and $\gcd(b\frac{a_0}{b_0}, b\frac{a_1}{b_1}, \ldots, b\frac{a_d}{b_d}) = [1]$. In particular, we have $bf \in R[x]$ and $C(bf) = [1]$.

(b) Write $F = a_0 + a_1x + \cdots + a_dx^d$. Since $\gcd(a_0, a_1, \ldots, a_d) = [1]$ and $ca_i \in R$ for each i, Lemma 2.5.20(d) implies that $c \in R$.

(c) Write $g = fh \in R[x]$ and set $[r] = C(g)$. Let $g_1 \in R[x]$ be primitive such that $g = rg_1$. Use part (a) to find an element $0 \neq c \in \mathrm{Q}(R)$ such that $cf \in R[x]$

and $C(cf) = [1]$. Then $(cr)g_1 = cg = (cf)h \in R[x]$ and the fact that g_1 is primitive implies $cr \in R$. Hence

$$[cr] = [cr]C(g_1) = C(crg_1) = C((cf)h) = C(cf)C(h) = [1][1] = [1]$$

and it follows that cr is a unit in R. Write $cr = u$. In K, it follows that $c^{-1} = ru^{-1} \in R$ and so

$$f = \underbrace{c^{-1}}_{\in R}\underbrace{(cf)}_{\in R[x]} \in R[x]$$

as desired. □

Theorem 2.7.7. *Let R be a UFD with quotient field $K = \mathrm{Q}(R)$. Let $f \in R[x]$ be primitive. Then f is irreducible in $R[x]$ if and only if it is irreducible in $K[x]$.*

Proof. ($\Longleftarrow$) Assume that f is irreducible in $K[x]$, and suppose that $f = gh$ with $g, h \in R[x] \subseteq K[x]$. Since f is irreducible in $K[x]$, either g or h is a unit in $K[x]$. Using a degree argument, we conclude that either g or h is a constant. By symmetry, assume that g is constant, say $g = r \in R$. By Lemma 2.7.5(b), since $rh = f$ which is primitive, we know that r is a unit in R, and so g is a unit in $R[x]$.

($\Longrightarrow$) Assume that f is not irreducible in $K[x]$. We will show that f is not irreducible in $R[x]$.

If f is a unit in $K[x]$, then it is constant say $f = r$. Since f is primitive in $R[x]$, we have $[1] = C(f) = [r]$. Hence r is a unit in R and so $f = r$ is a unit in $R[x]$. Thus, in this case, f is not irreducible in $R[x]$.

Assume that f is not a unit in $K[x]$. Since f is non-zero and is not irreducible, there exist nonconstant polynomials $g, h \in K[x]$ such that $f = gh$.

Lemma 2.7.6(a) implies that there is an element $0 \neq b \in K$ such that $bh \in R[x]$ and $C(bh) = [1]$, that is, $h_1 = bh$ is primitive. Write $g_1 = \frac{1}{b}g \in K[x]$ so that we have $f = gh = (\frac{1}{b}g)(bh) = g_1h_1$. Lemma 2.7.6(c) implies $g_1 \in R[x]$. That is, we have written $f = g_1h_1$ where g_1, h_1 are nonconstant polynomials in $R[x]$. Hence f is not irreducible in $R[x]$. □

Theorem 2.7.8. *If R is a UFD, then $R[x]$ is a UFD.*

Proof. Set $K = \mathrm{Q}(R)$.

We first show that every non-zero nonunit $f \in R[x]$ can be written as a product of irreducible polynomials in $R[x]$. Since f is a non-zero nonunit, set $C(f) = [c]$ and find a primitive polynomial $f_1 \in R[x]$ such that $f = cf_1$.

Since $K[x]$ is a UFD, we can write $f_1 = p_1 \cdots p_m$ where each $p_i \in K[x]$ is irreducible. Arguing as in Lemma 2.7.6(c), we can use Lemma 2.7.6(a) find elements $0 \neq b_1, \ldots, b_m \in K$ such that each $q_i = b_ip_i$ is a primitive polynomial in $R[x]$ and $f_1 = q_1 \cdots q_m$. Notice that b_i is a unit in $K[x]$, so each q_i is irreducible in $K[x]$. Hence, Theorem 2.7.7 implies that each q_i is irreducible in $R[x]$.

Since R is a UFD, either c is a unit or a product of irreducible elements of R. If c is a unit, then $f = cf_1 = (cq_1)q_2 \cdots q_m$ is a factorization of f in $R[x]$ into a product of irreducibles. If c is not a unit, then there are irreducible elements $r_1, \ldots, r_k \in R$ such that $c = r_1 \cdots r_k$. It is straightforward to show that each r_i is irreducible in $R[x]$: the only way factor a constant polynomial over an integral domain is with constant factors. Hence $f = cf_1 = r_1 \cdots r_kq_1 \cdots q_m$ is a factorization of f in $R[x]$ into a product of irreducibles.

Next we show that an irreducible element $f \in R[x]$ is prime. Lemma 2.7.5(c), implies that f is either primitive or constant. If f is constant, then the fact that it is irreducible in $R[x]$ implies that it is irreducible in R. Since R is a UFD, f is then prime in R. It is straightforward to show that this implies that f is prime in $R[x]$: since f is prime in R, the ring R/fR is an integral domain, and hence so is $(R/fR)[x] \cong R[x]/(fR[x])$.

Assume that f is primitive. Note that f is irreducible in $K[x]$ by Theorem 2.7.7. Hence, the fact that $K[x]$ is a UFD implies that f is prime in $K[x]$. Let $g, h \in R[x]$ such that $f\big|gh$ in $R[x]$. It follows that $f\big|gh$ in $K[x]$, and so either $f\big|g$ or $f\big|h$ in $K[x]$ because f is prime in $K[x]$. Assume that $f\big|g$ in $K[x]$ and write $g = fg_1$ for some $g_1 \in K[x]$. Arguing as in Theorem 2.7.7, we see that g_1 is in $R[x]$, and so $f\big|g$ in $R[x]$, as desired. □

Corollary 2.7.9. *If R is a UFD, then $R[x_1, \dots, x_n]$ is a UFD.*

PROOF. Induction on n. □

CHAPTER 3

Module Theory

3.1. Modules

Definition 3.1.1. Let R be a ring. A *(left) R-module* is an additive abelian group M equipped with a map $R \times M \to M$ (denoted $(r, m) \mapsto rm$) such that $(r + s)m = rm + sm$, $r(m + n) = rm + rn$, and $(rs)m = r(sm)$ for all $r, s \in R$ and all $m, n \in M$.

If R has identity, then a left R-module M is *unital* if $1m = m$ for all $m \in M$.

If k is a field, then a *k-vector space* is a unital left k-module.

Example 3.1.2. An abelian group is the same as a unital $\mathbb{Z}$-module.

Example 3.1.3. Let R be a ring. The additive abelian group R^n, consisting of all column vectors of size n with entries in R, is an R-module via the following action

$$r\begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} = \begin{pmatrix} rs_1 \\ \vdots \\ rs_n \end{pmatrix}$$

The set of $m \times n$ matrices with entries in R is denoted $M_{m,n}(R)$. It is also an R-module, with similar coordinate-wise action.

Assume that R has identity. For $j = 1, \ldots, n$ let $e_j \in R^n$ be the vector with ith entry $\delta_{i,j}$. (We call e_j the jth *standard basis vector* of R^n.) In this case the R-modules R^n and $M_{m,n}(R)$ are unital.

Example 3.1.4. Let R be a ring, and let $I \subseteq R$ be an ideal. Then I is an R-module via the multiplication from R. In particular, R is an R-module. Also, the quotient R/I is an R-module via the action $r\overline{s} := \overline{rs}$. (Check that this is well-defined. The other properties are straightforward.) If R has identity, then I and R/I are unital R-modules. Note that I does not need to be a two-sided ideal here.

Remark 3.1.5. The previous examples motivate module theory, in that it gives a unification of the theory of abelian groups, the theory of vector spaces, the theory of ideals and the theory of quotients by ideals.

Example 3.1.6. Let R be a ring, and let $\{M_\lambda\}_{\lambda\in\Lambda}$ be a set of R-modules. Then the abelian groups $\prod_\lambda M_\lambda$ and $\oplus_\lambda M_\lambda$ are R-modules via the coordinate-wise action $r(m_\lambda) = (rm_\lambda)$. (See Remark 3.1.8 to see why $\oplus_\lambda M_\lambda$ is closed under this action.) In particular, $R^{(\Lambda)}$ and R^Λ are R-modules.

Assume that R has identity and each M_λ is unital. Then $\prod_\lambda M_\lambda$ and $\oplus_\lambda M_\lambda$ are unital. In particular, $R^{(\Lambda)}$ and R^Λ are unital. In this case, for each $\mu \in \Lambda$, let $e_\mu \in R^{(\Lambda)}$ be defined as $e_\mu = (e_{\mu,\lambda})$ where

$$e_{\mu,\lambda} = \begin{cases} 1_R & \text{if } \lambda = \mu \\ 0_R & \text{if } \lambda \neq \mu. \end{cases}$$

Example 3.1.7. Let $\varphi\colon R \to S$ be a ring homomorphism. Then S is an R-module via the following action: $rs := \varphi(r)s$. If φ is a homomorphism of rings with identity, then this action makes S into a unital R-module. (Note that this subsumes part of Example 3.1.4.)

More generally, if M is an S-module, then M has a well-defined R-module structure defined by $rm := \varphi(r)m$. If φ is a homomorphism of rings with identity and M is a unital S-module, then this action makes M into a unital R-module.

In particular, if $I \subset R$ is a two-sided ideal and M is an R/I-module, then M is an R-module via the action $rm := \overline{r}m$. In particular $(R/I)^n$ is an R-module; it is unital when R has identity.

Other examples include:

$(R[x_1, \ldots, x_m])^n$ is an R-module. It is unital when R has identity.

If R is an integral domain with quotient field $K = \mathrm{Q}(R)$, then K^n is a unital R-module.

Remark 3.1.8. Let R be a ring and M an R-module. The following properties are straightforward to show:

$r0_M = 0_M$ for all $r \in R$;

$0_R m = 0_M$ for all $m \in M$;

$(-r)m = -(rm) = r(-m)$ for all $r \in R$ and all $m \in M$;

$n(rm) = (nr)m = r(nm)$ for all $n \in \mathbb{Z}$, all $r \in R$ and all $m \in M$.

3.2. Module Homomorphisms

Definition 3.2.1. Let R be a ring and let M and N be R-modules. An additive group homomorphism $f\colon M \to N$ is an *R-module homomorphism* if $f(rm) = rf(m)$ for all $r \in R$ and all $m \in M$. (We also say that the function f is "R-linear".) An R-module homomorphism is a *monomorphism* if it is 1-1; it is an *epimorphism* if it is onto; and it is an *isomorphism* if it is 1-1 and onto.

The set of all R-module homomorphisms $M \to N$ is denoted $\mathrm{Hom}_R(M, N)$.

If R is a field and M and N are R-vector spaces, then $f\colon M \to N$ is a *linear transformation* if it is an R-module homomorphism.

Example 3.2.2. Let G and H be abelian groups with the natural $\mathbb{Z}$-module structure. A function $f\colon G \to H$ is a $\mathbb{Z}$-module homomorphism if and only if it is a group homomorphism.

Example 3.2.3. Let R be a ring, and let M and N be R-modules. The zero map $M \to N$ given by $m \mapsto 0$ is an R-module homomorphism. The identity map $\mathrm{id}_M\colon M \to M$ given by $m \mapsto m$ is an R-module homomorphism. When R is commutative, for each $r \in R$, the multiplication map $\mu_r\colon M \to M$ given by $m \mapsto rm$ is an R-module homomorphism. The map μ_r is called a *homothety*.

Example 3.2.4. Let R be a commutative ring with identity. Let R^n and R^m have the natural R-module structure. There is a bijection $\Phi\colon \mathrm{Hom}_R(R^n, R^m) \to M_{m,n}(R)$. Given an R-module homomorphism $f\colon R^n \to R^m$, the associated matrix $\Phi(f)$ is the matrix whose jth column is $f(e_j)$. To see that this is a bijection, we define an inverse $\Psi\colon M_{m,n}(R) \to \mathrm{Hom}_R(R^n, R^m)$. Given an $m \times n$ matrix $(a_{i,j})$ with entries in R, the corresponding R-module homomorphism $\Psi(a_{i,j})$ is the function $f\colon R^n \to R^m$ given by matrix multiplication $f(v) = (a_{i,j})v$.

In particular, the set $\operatorname{Hom}_R(R,R)$ is in bijection with R. That is, the R-module homomorphisms $f\colon R \to R$ are exactly the homotheties $\mu_r\colon R \to R$ given by $s \mapsto rs$.

Example 3.2.5. Let R be a ring and $I \subset R$ a two-sided ideal. Let M and N be R/I-modules, and consider them as R-modules via φ. Then $\operatorname{Hom}_R(M,N) = \operatorname{Hom}_{R/I}(M,N)$. In other words $f\colon M \to N$ is an R-module homomorphism if and only if it is an R/I-module homomorphism.

Assume that R/I is commutative with identity. Then there is an equality $\operatorname{Hom}_R(R/I,R/I) = \operatorname{Hom}_{R/I}(R/I,R/I)$ which is naturally identified with R/I. That is, the R-module homomorphisms $f\colon R/I \to R/I$ are exactly the homotheties $\mu_r\colon R/I \to R/I$ given by $\overline{s} \mapsto r\overline{s} = \overline{rs}$.

Example 3.2.6. Let $\varphi\colon R \to S$ be a ring homomorphism. If we give S the R-module structure induced by φ, then this makes φ into an R-module homomorphism.

Let M and N be S-modules and consider them as R-modules via φ. Then $\operatorname{Hom}_S(M,N) \subseteq \operatorname{Hom}_R(M,N)$, but we may not have equality; that is, every S-module homomorphism $M \to N$ is also an R-module homomorphism, but not necessarily vice versa.

For instance, let $S = R[x]$ and let $\varphi\colon R \to R[x]$ be the natural inclusion. The function $f\colon R[x] \to R[x]$ given by $\sum_i a_i x^i \mapsto a_0$ is an R-module homomorphism but is not an $R[x]$-module homomorphism.

Proposition 3.2.7. *Let R be a ring, M an R-module and Λ a set. Given a subset $\{m_\lambda\}_{\lambda\in\Lambda}$, the map $f\colon R^{(\Lambda)} \to M$ given by $(r_\lambda) \mapsto \sum_\lambda r_\lambda m_\lambda$ is a well-defined R-module homomorphism.*

Proof. It is straightforward to show that f is a well-defined additive group homomorphism. It is an R-module homomorphism because

$$f(r(r_\lambda)) = f((rr_\lambda)) = \textstyle\sum_\lambda (rr_\lambda)m_\lambda = \sum_\lambda r(r_\lambda m_\lambda) = r(\sum_\lambda r_\lambda m_\lambda) = rf(r_\lambda)$$

□

3.3. Submodules

Definition 3.3.1. Let R be a ring and let M be an R-module. A *R-submodule* of M is an additive subgroup $N \subseteq M$ such that, for all $r \in R$ and all $n \in N$, we have $rn \in N$. If k is a field and M is a k-vector space, then a k-submodule of M is called a *k-subspace.*

Example 3.3.2. Let G be an abelian group considered as a unital $\mathbb{Z}$-module. A subset $H \subseteq G$ is a $\mathbb{Z}$-submodule of G if and only if it is a subgroup.

Example 3.3.3. Let R be a ring and let M and N be R-modules. The subsets $\{0\} \subseteq M$ and $M \subseteq M$ are R-submodules. If $f \in \operatorname{Hom}_R(M,N)$, then $\operatorname{Ker}(f) \subseteq M$ and $\operatorname{Im}(f) \subseteq N$ are R-submodules. If $N' \subseteq N$ is an R-submodule, then $f^{-1}(N') \subseteq M$ is an R-submodule. If $M' \subseteq M$ is an R-submodule, then $f(M') \subseteq N$ is an R-submodule.

Assume that R is commutative. If $r \in R$, then $(0 :_M r) = \{m \in M \mid rm = 0\} \subseteq M$ is an R-submodule, and $rM = \{rm \mid m \in M\} \subseteq M$ is an R-submodule. This follows from the previous paragraph because the homothety $\mu_r\colon M \to M$ is an R-module homomorphism.

Example 3.3.4. Let R be a ring considered as an R-module via its internal multiplication. A subset $I \subseteq R$ is an R-submodule if and only if it is a left ideal.

Example 3.3.5. Let R be a ring, and let $\{M_\lambda\}_{\lambda\in\Lambda}$ be a set of R-modules. Then $\oplus_\lambda M_\lambda \subseteq \prod_\lambda M_\lambda$ is an R-submodule.

Example 3.3.6. Let R be a ring and $I \subset R$ a two-sided ideal. Let M be an R/I-module, and consider M as an R-module via the natural surjection $R \to R/I$. Then the R/I-submodules of M are exactly the R-submodules of M. In particular, the R-submodules of R/I are exactly the left ideals of R/I, that is, the set of all quotients J/I where J is a left ideal of R such that $I \subseteq J$.

Example 3.3.7. Let $\varphi\colon R \to S$ be a ring homomorphism, and let M be an S-module. Consider M as an R-module via φ. Then every S-submodule of M is an R-submodule, but not vice versa.

For instance, let $S = R[x]$ and let $\varphi\colon R \to R[x]$ be the natural inclusion. Then $R \cong \mathrm{Im}(\varphi) \subset R[x]$ is an R-submodule but is not an $R[x]$-submodule.

Remark 3.3.8. Let R be a ring and M an R-module. If R has identity and M is unital, then every submodule of M is unital.

Example 3.3.9. Let R be a ring and M an R-module. If $\{M_\lambda\}_{\lambda\in\Lambda}$ is a set of R-submodules of M, then $\cap_\lambda M_\lambda$ is an R-submodule of M; it is also an R-submodule of M_μ for each $\mu \in \Lambda$.

Proposition 3.3.10. *Let R be a ring, M an R-module and $N \subseteq M$ a submodule. The quotient group M/N has a well-defined R-module structure via the action*

$$r(m+N) := (rm) + N.$$

If M is unital, then M/N is unital. The natural surjection $\pi\colon M \to M/N$ is an R-module homomorphism with $\mathrm{Ker}(\pi) = N$.

Proof. First, show that the action is well-defined: Let $r \in R$ and $m, m' \in M$ such that $m + N = m' + N$. Then $m - m' \in N$ and so $rm - rm' = r(m - m') \in N$ which implies $rm + N = rm' + N$.

The R-module axioms for M/N now follow from the R-module axioms for M. For instance, associativity:

$$r(s(m+N)) = r(sm+N) = r(sm) + N = (rs)m + N = (rs)(m+N).$$

The distributive laws are verified similarly. When R has identity and M is unital, it follows similarly that M/N is unital.

The fact that π is an R-module homomorphism is proved next:

$$\pi(rm) = (rm) + N = r(m+N) = r\pi(n).$$

The equality $\mathrm{Ker}(\pi) = N$ was shown in Chapter 1. □

Here is the Universal mapping property for quotients.

Proposition 3.3.11. *Let R be a ring, $f\colon M \to N$ an R-module homomorphism, and $M' \subseteq \mathrm{Ker}(f)$ an R-submodule.*

(a) *There is a unique R-module homomorphism $\overline{f}\colon M/M' \to N$ making the following diagram commute*

$$\begin{tikzcd}
M \arrow[r, "\pi"] \arrow[rd, "f"'] & M/M' \arrow[d, dashed, "\exists!\overline{f}"] \\
& N
\end{tikzcd}$$

that is, such that $\overline{f}(m+M') = f(m)$.

(b) *We have $\operatorname{Im}(\overline{f}) = \operatorname{Im}(f)$ and $\operatorname{Ker}(\overline{f}) = \operatorname{Ker}(f)/M'$.*

(c) *$\overline{f}$ is onto if and only if f is onto.*

(d) *$\overline{f}$ is 1-1 if and only if $M' = \operatorname{Ker}(f)$.*

(e) *$\overline{f}$ is an isomorphism if and only if f is onto and $M' = \operatorname{Ker}(f)$. In particular, $\operatorname{Im}(f) \cong M/\operatorname{Ker}(f)$.*

Proof. (a) If $\overline{g} = \overline{g'}$, then $g - g' \in K \subseteq \operatorname{Ker}(f)$ and so

$$0_H = f(g-g') = f(g) - f(g')$$

which implies $f(g) = f(g')$.

It is straightforward to show that $\overline{f}$ is a group homomorphism. For the uniqueness, suppose that $f'\colon G/K \to H$ is a homomorphism of additive abelian group making the following diagram commute

$$\begin{tikzcd}
G \arrow[r, "\pi"] \arrow[rd, "f"'] & G/K \arrow[d, "f'"] \\
& H.
\end{tikzcd}$$

Then we have $f'(\overline{g}) = f'(\pi(g)) = f(g) = \overline{f}(\overline{g})$ for all $\overline{g} \in G/K$, so $f' = \overline{f}$. We need only show that $\overline{f}$ is an R-module homomorphism:

$$\overline{f}(r(m+M')) = \overline{f}(rm+M') = f(rm) = rf(m) = r\overline{f}(m+M').$$

(b)–(e) These follow from Chapter 1 because they do not depend on the R-module structure. □

The next proposition follows from Chapter 1 material like Proposition 3.3.11.

Proposition 3.3.12. *Let R be a ring, M an R-module and $M', M'' \subseteq M$ submodules.*

(a) *There is an R-module isomorphism $M'/(M' \cap M'') \cong (M'+M'')/M''$.*

(b) *If $M'' \subseteq M'$, then $M'/M'' \subseteq M/M''$ is a submodule, and there is an R-module isomorphism $(M/M'')/(M'/M'') \cong M/M'$.*

(c) *Let $\pi\colon M \to M/M''$ be the R-module epimorphism $\pi(m) = m + M''$. There is a 1-1 correspondence*

$$\{\textit{submodules } N \subseteq M \mid M'' \subseteq N\} \longleftrightarrow \{N' \subseteq M/M''\}$$

given by

$$N \longmapsto N/M''$$
$$\pi^{-1}(N') \longleftarrow N'.$$

(d) *If $M = M' + M''$ and $M' \cap M'' = 0$, then $M \cong M' \oplus M''$.* □

3.4. Generators

Definition 3.4.1. Let R be a ring, M an R-module and $X \subseteq M$ a subset. The *submodule of* M *generated by* X or *spanned by* X, denoted $(X)R$, is the intersection of all submodules of M containing X. If $X = \{x_1, \ldots, x_n\}$, then we write $(X)R = (x_1, \ldots, x_n)R$. If $(X)R = M$, then we say that X *generates* or *spans* M as an R-module.

If M has a finite generating set, then it is *finitely generated.* If M can be generated by a single element, then it is *cyclic.*

If $\{M_\lambda\}_{\lambda\in\Lambda}$ is a set of submodules of M, then $(\cup_\lambda M_\lambda)R$ is denoted $\sum_\lambda M_\lambda$.

Remark 3.4.2. Let R be a ring, M an R-module, and $X \subseteq M$ a subset. Then $(X)R$ is the smallest submodule of M containing X. The R-module M has a generating set, namely M itself.

Example 3.4.3. Let G be an abelian group with the natural unital $\mathbb{Z}$-module structure. The $\mathbb{Z}$-submodule of G generated by a subset X is equal to the subgroup generated by X. In particular G is generated by X as an $\mathbb{Z}$-module if and only if it is generated by X as an abelian group.

Example 3.4.4. If R is a ring and M is an R-module, then $(\emptyset)R = \{0\}$.

Example 3.4.5. If R is a ring with identity, then $R^n = (e_1, \ldots, e_n)R$ and $R^{(\Lambda)} = (\{e_\mu \mid \mu \in \Lambda\})R$.

Example 3.4.6. Let R be a ring and $I \subset R$ a two-sided ideal. Let M be an R/I-module with the R-module structure coming from the natural surjection $R \to R/I$. For each subset $X \subseteq M$, the R-submodule of M generated by X equals the R/I-submodule of M generated by X. In particular M is generated by X as an R-module if and only if it is generated by X as an R/I-module.

Proposition 3.4.7. *Let R be a ring with identity and M a unital R-module.*

(a) *Let $X \subseteq M$. There is an equality*

$$(X)R = \{\textstyle\sum_{x\in X}^{\textit{finite}} r_x x \mid r_x \in R, x \in X\}.$$

(b) *The function $f\colon R^{(X)} \to M$ given by $(r_x) \mapsto \sum_x^{\textit{finite}} r_x x$ is a well-defined R-module homomorphism such that* $\operatorname{Im}(f) = (X)R$*. Moreover, f is the unique R-module homomorphism $R^{(X)} \to M$ such that $e_x \mapsto m_x$ for each $x \in X$.*

(c) *The function $f\colon R^{(X)} \to (X)R$ given by $(r_x) \mapsto \sum_x^{\textit{finite}} r_x x$ is a well-defined R-module epimorphism.*

(d) *For each $m_1, \ldots, m_n \in M$, we have*

$$(m_1, \ldots, m_n)R = \{\textstyle\sum_{i=1}^n r_i m_i \mid r_1, \ldots, r_n \in R\}$$

and the function $f\colon R^n \to (m_1, \ldots, m_n)R$ given by $\begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} \mapsto \sum_{i=1}^n r_i m_i$ is a well-defined R-module epimorphism.

(e) *Given a set $\{M_\lambda\}_{\lambda\in\Lambda}$ of submodules of M, there is an equality*

$$\textstyle\sum_\lambda M_\lambda = \{\sum_\lambda^{\textit{finite}} m_\lambda \mid m_\lambda \in M_\lambda\}$$

and the function $f\colon \oplus_\lambda M_\lambda \to \sum_\lambda M_\lambda$ given by $(m_\lambda) \mapsto \sum_\lambda m_\lambda$ is a well-defined R-module epimorphism.

PROOF. (a) Set $N = \{\sum_x^{\text{finite}} r_x x \mid r_x \in R, x \in X\}$. It is straightforward to show that N is an R-submodule of M containing X, and so $(X)R \subseteq N$. For the reverse containment, we have $x \in X \subseteq (X)R$ for each i; since $(X)R$ is an R-module, we have $r_x x \in (X)R$ for each $r_x \in R$ and furthermore $\sum_x^{\text{finite}} r_x x \in (X)R$. This shows $(X)R \supseteq N$ and so $(X)R = N$.

(b) The function f is a well-defined R-module homomorphism by Proposition 3.2.7. The image of f is $(X)R$ by part (a). And

$$f(e_x) = 1_R m_x + \sum_{y \neq x} 0_R m_y = m_x.$$

For the uniqueness of f, let $g\colon R^{(X)} \to M$ be an R-module homomorphism such that $e_x \mapsto m_x$ for each $x \in X$. Let $(r_x) \in R^{(X)}$ and write $(r_x) = \sum_{x \in X} r_x e_x$. Then

$$g((r_x)) = g(\textstyle\sum_{x \in X} r_x e_x) = \sum_{x \in X} r_x g(e_x) = \sum_{x \in X} r_x m_x = f((r_x)).$$

It follows that $g = f$, as desired.

Part (c) follows from part (b). Part (d) is a special case of part (c) using $X = \{m_1, \ldots, m_n\}$. Part (e) is proved like (b). □

Example 3.4.8. Let R be a ring with identity and let $f\colon M \to N$ be a homomorphism of unital R-modules. If $M = (X)R$, then $f(M) = (f(X))R$. More generally, for each subset $X \subseteq M$, we have $f((X)R) = (f(X))R$.

Example 3.4.9. Let $\varphi\colon R \to S$ be a ring homomorphism. Let M be an S-module with the R-module structure coming from φ. For each subset $X \subseteq M$, the R-submodule of M generated by X is contained in the S-submodule of M generated by X, however they may not be equal.

For instance, let R be a commutative ring with identity. The R-submodule of $R[x]$ generated by 1 is R, and the $R[x]$-submodule of $R[x]$ generated by 1 is $R[x]$.

Proposition 3.3.10 gives one of the best ways to construct R-modules.

Example 3.4.10. Let R be a commutative ring with identity, and let $(a_{i,j}) \in M_{m,n}(R)$. The matrix $(a_{i,j})$ determines an R-module homomorphism $f\colon R^n \to R^m$. It follows that $\operatorname{Im}(f) \subseteq R^m$ is an R-submodule, namely the submodule generated by the columns of $(a_{i,j})$, and so $R^m/\operatorname{Im}(f)$ is an R-module. Proposition 3.4.11 shows that, in a sense, this is the only way to construct R-modules.

Proposition 3.4.11. *Let R be a ring with identity and M a unital R-module.*

(a) *There is a set Λ and an R-module epimorphism $\pi\colon R^{(\Lambda)} \to M$. If M is finitely generated, then Λ can be chosen to be finite.*

(b) *There are sets Λ and Γ and an R-module homomorphism $f\colon R^{(\Gamma)} \to R^{(\Lambda)}$ such that $M \cong R^{(\Lambda)}/\operatorname{Im}(f)$. If M is finitely generated, then Λ can be chosen to be finite.*

PROOF. (a) Let Λ be a generating set for R, which exists by Remark 3.4.2. Note that, if M is finitely generated, then Λ can be chosen to be finite. Proposition 3.4.7 (c) provides an R-module epimorphism $\pi\colon R^{(\Lambda)} \to (\Lambda)R = M$.

(b) Let Λ and π be as in part (a). Then $\operatorname{Ker}(\pi)$ is an R-module, so part (a) implies that there is a set Γ and an R-module epimorphism $\tau\colon R^{(\Gamma)} \to \operatorname{Ker}(\pi)$. Let $\iota\colon \operatorname{Ker}(\pi) \to R^{(\Lambda)}$ be the natural inclusion. Then ι is an R-module homomorphism because $\operatorname{Ker}(\pi) \subseteq R^{(\Lambda)}$ is an R-submodule. It follows that the composition $f =$

$\iota\tau\colon R^{(\Gamma)} \to R^{(\Lambda)}$ is an R-module homomorphism and $\operatorname{Im}(f) = \operatorname{Ker}(\pi)$. This gives the equality in the next sequence

$$M \cong R^{(\Lambda)}/\operatorname{Ker}(\pi) = R^{(\Lambda)}/\operatorname{Im}(f)$$

while the isomorphism is from Proposition 3.3.11(e). □

3.5. Bases, Free Modules, and Vector Spaces

Definition 3.5.1. Let R be a ring and M an R-module. A subset $X \subseteq M$ is *linear independent* over R if, for every $n \in \mathbb{N}$ and every list of distinct elements $x_1, \ldots, x_n \in X$, given $r_1, \ldots, r_n \in R$ such that $\sum_i r_i x_i = 0$, we have $r_i = 0$ for $i = 1, \ldots, n$.

Assume that R has identity. A subset of $X \subseteq M$ is an *R-basis* for M if it spans M as an R-module and is linearly independent over R. If M has a basis, then it is *free.*

Example 3.5.2. Let G be an abelian group with the natural unital $\mathbb{Z}$-module structure. A subset $X \subseteq G$ is a $\mathbb{Z}$-basis for G if and only if it is a basis for G as an abelian group. In particular G is free as a $\mathbb{Z}$-module if and only if it is free as an abelian group.

Example 3.5.3. If R is a ring with identity and M is a unital R-module, then $\emptyset$ is an R-basis for $\{0\}$.

Example 3.5.4. If R is a ring with identity, then $\{e_1, \ldots, e_n\} \subseteq R^n$ is an R-basis. Hence R^n is a free R-module. More generally, if Λ is a set, then $\{e_\lambda\}_{\lambda\in\Lambda} \subseteq R^{(\Lambda)}$ is an R-basis. Hence $R^{(\Lambda)}$ is a free R-module. We shall see below that, up to isomorphism, these are the only free R-modules.

Most R-modules are not free:

Example 3.5.5. The unital $\mathbb{Z}$-module $\mathbb{Z}/2\mathbb{Z}$ is not free. Indeed, a generating set $X \subseteq \mathbb{Z}/2\mathbb{Z}$ must be non-empty because $\mathbb{Z}/2\mathbb{Z} \neq 0$. However, for each $x \in X$, we have $2x = 0$ in $\mathbb{Z}/2\mathbb{Z}$ even though $2 \neq 0$ in $\mathbb{Z}$; hence X is not linearly independent over $\mathbb{Z}$.

More generally, if R is a ring with identity and $0 \neq I \subsetneq R$ is an ideal, then R/I is not a free R-module. In particular, this shows that quotients of free R-modules need not be free.

Submodules of free R-modules need not be free.

Example 3.5.6. Every subgroup of $\mathbb{Z}^n$ is free as an abelian group; see Proposition 3.9.1. In other words, every $\mathbb{Z}$-submodule of $\mathbb{Z}^n$ is free as a $\mathbb{Z}$-module.

Over different rings, though, the analogous result need not be true. Indeed, the $\mathbb{Z}/6\mathbb{Z}$-module $M = \mathbb{Z}/6\mathbb{Z}$ is free as a $\mathbb{Z}/6\mathbb{Z}$-module. However, the $\mathbb{Z}/6\mathbb{Z}$-submodule $3\mathbb{Z}/6\mathbb{Z} \subseteq \mathbb{Z}/6\mathbb{Z}$ is not free as a $\mathbb{Z}/6\mathbb{Z}$-module. (Argue as in Example 3.5.5.)

For another example, let k be a field and consider the polynomial ring $R = k[x, y]$. Then R is a free R-module, and the ideal $(x, y)R \subset R$ is a submodule. The submodule $(x, y)R$ is generated by the set $\{x, y\}$ but this set is not a basis over R because $yx - xy = 0$ and $y \neq 0$. (We will see below that this shows that $(x, y)R$ is not free as an R-module.)

Example 3.5.7. Let R be a ring with identity. The polynomial ring $R[x]$, considered as an R-module via the natural inclusion $R \to R[x]$ is a free R-module with basis $\{1, x, x^2, \ldots\}$.

Here is the Universal Mapping Property for free modules. Compare it to Proposition 3.4.7(b).

Proposition 3.5.8. *Let R be a ring with identity and M a unital R-module. Let F be a free R-module with basis E, and let $X = \{m_e \in M \mid e \in E\}$ be a subset of M. The function $f\colon F \to M$ given by $\sum_{e\in E} r_e e \mapsto \sum_{e\in E} r_e m_e$ is a well-defined R-module homomorphism such that $\operatorname{Im}(f) = (X)R$. Moreover, f is the unique R-module homomorphism $F \to M$ such that $e \mapsto m_e$ for each $e \in E$.*

Proof. The function f is a well-defined, as follows. Each element of F has a unique expression of the form $\sum_{e\in E} r_e e$ since E is a basis for F. This sum is finite, so the sum $\sum_{e\in E} r_e m_e$ is finite and describes an element of M; thus, the output of f is in M. The uniqueness of representation of $\sum_{e\in E} r_e e$ shows that this is independent of representative of the input.

Now that f is well-defined, it is straightforward to show that it is an R-module homomorphism. by Proposition 3.2.7. For each $e \in E$ we have

$$f(e) = 1_R m_e + \sum_{e' \neq e} 0_R m_{e'} = m_e.$$

The image of f is $(X)R$ by Proposition 3.4.7(a). For the uniqueness of f, argue as in the proof of Proposition 3.4.7(b). □

Proposition 3.5.9. *Let R be a ring with identity and M a unital R-module. Then M is free if and only if there is a set Λ and an isomorphism $M \cong R^{(\Lambda)}$. When M is free with basis X, then one has $M \cong R^{(X)}$.*

Proof. If $M \cong R^{(\Lambda)}$, then Example 3.5.4 shows that M is free. Thus, it remains to assume that M is free with basis X and prove that $M \cong R^{(X)}$. Proposition 3.4.7(b) implies that there is a unique R-module homomorphism $f\colon R^{(X)} \to M$ such that $f(e_x) = x$ for all $x \in X$. Proposition 3.5.8 implies that there is a unique R-module homomorphism $g\colon M \to R^{(X)}$ such that $f(x) = e_x$ for all $x \in X$.

The composition $g \circ f\colon R^{(X)} \to R^{(X)}$ is an R-module homomorphism $R^{(X)} \to R^{(X)}$ such that $e_x \mapsto e_x$ for all $x \in X$. The identity map $\mathrm{id}_{R^{(X)}}\colon R^{(X)} \to R^{(X)}$ is another R-module homomorphism $R^{(X)} \to R^{(X)}$ such that $e_x \mapsto e_x$ for all $x \in X$. Hence, the uniqueness statement in Proposition 3.4.7(b) implies that $g \circ f = \mathrm{id}_{R^{(X)}}$. Similarly, the uniqueness statement in Proposition 3.5.8 implies that $f \circ g = \mathrm{id}_M$. Thus, f and g are inverse isomorphisms, implying that $M \cong R^{(X)}$, as desired. □

Lemma 3.5.10. *Let k be a field and V a k-vector space.*

(a) *Let $X \subseteq V$, and let $Y \subseteq X$ be a linearly independent subset that is maximal among all linearly independent subsets of V contained in X, with respect to inclusion. Then Y is a basis for $(X)R$.*

(b) *Let $Y \subseteq V$ be a linearly independent subset that is maximal among all linearly independent subsets of V, with respect to inclusion. Then Y spans V and so Y is a basis for V.*

Proof. (a) The condition $Y \subseteq X$ implies $(Y)R \subseteq (X)R$. The desired conclusion will follow once we show $(Y)R = (X)R$, because then Y will be a linearly independent spanning set for $(X)R$. So, suppose $(Y)R \subset (X)R$.

Claim: $X \not\subseteq (Y)R$. If not, then $X \subseteq (Y)R$ and so $(X)R \subseteq (Y)R \subseteq (X)R$ which implies $(X)R = (Y)R$, a contradiction.

Fix an element $v \in X \smallsetminus (Y)R$, and set $Y' = Y \cup \{v\}$. We will show that Y' is linearly independent, and this will contradict the maximality of X. Let $r, r_1, \ldots, r_n \in k$ and $y_1, \ldots, y_n \in Y$ such that $rv + \sum_i r_i y_i = 0$. If $r \neq 0$, then $v = \sum_i (-r^{-1} r_i) y_i \in (Y)R \subseteq (X)R$, a contradiction. It follows that $r = 0$ and so $\sum_i r_i y_i = 0$. Since Y is linearly independent, it follows that $r_i = 0$ for each i. Hence Y' is linearly independent.

(b) This is the special case $X = V$ of part (a). □

Theorem 3.5.11. *Let k be a field and V a k-vector space. Every linearly independent subset of V is contained in a basis for V. In particular V has a basis and is therefore free.*

Proof. The second statement is the special case $X = \emptyset$ of the first statement, so we prove the first statement.

Let $X \subseteq V$ be a linearly independent subset. Set

$$\Sigma = \{\text{linearly independent } Z \subseteq V \mid X \subseteq Z\}$$

and partially order Σ by inclusion. Since $X \in \Sigma$, we have $\Sigma \neq \emptyset$. We will apply Zorn's Lemma to show that Σ contains a maximal element Y. This will be a linearly independent subset of V that is maximal among all linearly independent subsets of V, with respect to inclusion, that contains X. Then Lemma 3.5.10(b) will imply that Y is a basis for V containing X.

Let $\mathcal{C}$ be a chain in Σ. That is $\mathcal{C} \subseteq \Sigma$ such that, for all $Z, Z' \in \mathcal{C}$, either $Z \subseteq Z'$ or $Z' \subseteq Z$. It is straightforward to show that the set $\cup_{Z \in \mathcal{C}} Z$ is a linearly independent subset of V such that $X \subseteq \cup_{Z \in \mathcal{C}} Z$, that is, we have $\cup_{Z \in \mathcal{C}} Z \in \Sigma$. It follows immediately that $\cup_{Z \in \mathcal{C}} Z$ is an upper bound for $\mathcal{C}$ in Σ. Thus Σ satisfies the hypotheses of Zorn's Lemma. □

Theorem 3.5.12. *Let k be a field and V a k-vector space. Every spanning set for V contains a basis for V.*

Proof. Let $X \subseteq V$ be a spanning set for V. Set

$$\Sigma = \{\text{linearly independent } Z \subseteq X\}$$

and partially order Σ by inclusion. Since $\emptyset \in \Sigma$, we have $\Sigma \neq \emptyset$. As in the proof of Theorem 3.5.11, the set Σ contains a maximal element Y. This is a linearly independent subset of V that is maximal among all linearly independent subsets of V contained in X, with respect to inclusion. Lemma 3.5.10(a) implies that Y is a basis for $(X)R = V$ contained in X. □

Example 3.5.13. Let $m, n \geqslant 1$. It is a fact that, if $\mathbb{Z}^m \cong \mathbb{Z}^n$, then $m = n$; see Theorem 3.5.29. If we replace $\mathbb{Z}$ with an arbitrary ring R with identity, though, the analogous statement can be false. (See Hungerford Exercise IV.2.13.) We will see, however, that when R is commutative with identity, this is OK.

First we show that free modules with infinite bases are always OK.

Lemma 3.5.14. *Let R be a ring with identity and F a free R-module. If X is a basis for F and $X' \subset X$, then X' does not span F.*

PROOF. Let $x \in X \smallsetminus X'$. We claim that $x \notin (X')R$. (Then $x \in F \smallsetminus (X')R$ and so X' does not span F.) Suppose $x \in (X')R$ and write $x = \sum_{i=1}^{m} r_i x_i'$ with the $r_i \in R$ and $x_i' \in X$. Then the nontrivial linear dependence relation $-x + \sum_{i=1}^{m} r_i x_i' = 0$ contradicts the linear independence of X. □

Lemma 3.5.15. *Let R be a ring with identity and F a free R-module. If X spans F and Y is a finite subset of F, then there is a finite subset $X' \subseteq X$ such that $(Y)R \subseteq (X')R$.*

PROOF. Write $Y = \{y_1, \ldots, y_m\} \subseteq F = (X)R$. For each $i = 1, \ldots, m$ there exists $n_i \in \mathbb{N}$ and $x_{i,1}, \ldots, x_{i,n_i} \in X$ and $r_{i,1}, \ldots, r_{i,n_i} \in R$ such that $y_i = \sum_{j=1}^{n_i} r_{i,j} x_{i,j}$. Consider the finite set $X' = \{x_{i,j} \mid i = 1, \ldots, n; j = 1, \ldots, n_i\} \subseteq X$. It follows that $Y \subseteq (X')R$ and so $(Y)R \subseteq (X')R$. □

Lemma 3.5.16. *Let R be a ring with identity and F a free R-module. If F has an infinite basis, then every spanning set (and hence every basis) for F is infinite.*

PROOF. Let X be an infinite basis for F, and let Y be a spanning set for F. By way of contradiction, suppose that Y is a finite set. By Lemma 3.5.15 there is a finite subset $X' \subseteq X$ such that $F = (Y)R \subseteq (X')R \subseteq F$. Hence $(X')R = F$ and so X' spans F. On the other hand, X is infinite and X' is a finite subset. Hence $X' \subset X$, and so Lemma 3.5.14 says that X' cannot span F, a contradiction. □

Lemma 3.5.17. *Let R be a ring with identity and F an R-module. Let X be a linearly independent subset of F and let $X', X'' \subseteq X$. If $(X')R \subseteq (X'')R$, then $X' \subseteq X''$.*

PROOF. Suppose that $x' \in X' \smallsetminus X''$. Since $x' \in X' \subseteq (X')R \subseteq (X'')R$ we have $x' = \sum_i r_i x_i''$ for some $r_i \in R$ and distinct $x_i'' \in X''$. Since x' is distinct from the x_i'', this yields a nontrivial linear dependence relation in X, a contradiction. □

Remark 3.5.18. Let R be a ring with identity and F a free R-module. Let Y be a basis for F, and let $K(Y)$ denote the set of all finite subsets of Y. Let $X \subseteq F$, and define a function $f\colon X \to K(Y)$ as follows: for each $x \in X$ let $f(x) = \{y_1, \ldots, y_n\}$ where there exist $r_1, \ldots, r_n \in R$ such that each $r_i \neq 0$ and $x = \sum_{i=1}^{n} r_i y_i$. Since Y is a basis for F, the y_i are uniquely determined by x, so this function is well-defined.

Lemma 3.5.19. *Let R be a ring with identity and F a free R-module. Assume that X and Y are infinite bases for F, and let $K(Y)$ denote the set of all finite subsets of Y. Let $f\colon X \to K(Y)$ be the function from Remark 3.5.18.*

(a) *The set $\cup_{S\in\mathrm{Im}(f)} S \subseteq Y$ spans F, and so $\cup_{S\in\mathrm{Im}(f)} S = Y$.*
(b) *The set $\mathrm{Im}(f)$ is infinite.*
(c) *For each $T \in K(Y)$, the set $f^{-1}(T)$ is finite.*

PROOF. (a) For each $x \in X$, we have $x \in (f(x))R$ by the definition of f. Hence $X \subseteq (\cup_{S\in\mathrm{Im}(f)} S)R$ and so $F = (X)R \subseteq (\cup_{S\in\mathrm{Im}(f)} S)R \subseteq F$ which implies $(\cup_{S\in\mathrm{Im}(f)} S) = F$. Since Y is a basis for F and $\cup_{S\in\mathrm{Im}(f)} S$ is a spanning set for F contained in Y, Lemma 3.5.14 implies $\cup_{S\in\mathrm{Im}(f)} S = Y$.

(b) Suppose that $\mathrm{Im}(f)$ is finite. Since each element of $\mathrm{Im}(f)$ is a finite subset of Y, it follows that $Y' = \cup_{S\in\mathrm{Im}(f)} S$ is a finite subset of Y. Part (a) says that Y' spans F. On the other hand, Y is infinite and Y' is a finite subset. Hence $Y' \subset Y$, and so Lemma 3.5.14 says that Y' cannot span F, a contradiction.

(c) Note that $f^{-1}(T) \subseteq X$. If $T \notin \operatorname{Im}(f)$, then $f^{-1}(T) = \emptyset$ which is a finite set. Assume that $T \in \operatorname{Im}(f)$. If $x \in f^{-1}(T)$, then $x \in (T)R$ by definition of f. It follows that $f^{-1}(T) \subseteq (T)R$. On the other hand, Lemma 3.5.15 implies that there is a finite subset $X' \subset X$ such that $(T)R \subseteq (X')R$ and so $(f^{-1}(T)) \subseteq (T)R \subseteq (X')R$. Since $f^{-1}(T)$ and X' are subsets of X, Lemma 3.5.17 implies $f^{-1}(T) \subseteq X'$. Since X' is finite, the same is true of $f^{-1}(T)$. □

Here are some highlights of Hungerford section 0.8.

Definition 3.5.20. Let X and Y be sets. If there is a 1-1 function $X \to Y$, then we write $|X| \leqslant |Y|$. If there is a bijection $X \to Y$, then we say that X and Y have *the same cardinality* and write $|X| = |Y|$. A set X is countable if $|X| = |\mathbb{N}|$.

Example 3.5.21. When X and Y are finite sets, they have the same cardinality if and only if they contain the same number of elements.

Fact 3.5.22. (Schroeder-Bernstein Theorem) Let X and Y be sets. If $|X| \leqslant |Y|$ and $|Y| \leqslant |X|$, then $|X| = |Y|$. In other words, if there are 1-1 functions $X \to Y$ and $Y \to X$, then there is a bijection $X \to Y$.

Fact 3.5.23. Let X be an infinite set. Then $|X \times \mathbb{N}| = |X|$. If $K(X)$ denotes the set of all finite subsets of X, then $|K(X)| = |X|$.

Theorem 3.5.24. *Let R be a ring with identity and F a free R-module with an infinite basis X. Then every basis for F has the same cardinality as X. Specifically, if Y is another basis for F, then there is a bijection $X \to Y$.*

Proof. Let Y be another basis for F. Lemma 3.5.16 implies that Y is infinite. Let $K(Y)$ denote the set of all finite subsets of Y. Let $f\colon X \to K(Y)$ be the function from Remark 3.5.18. Note that X is the disjoint union $X = \cup_{T \in \operatorname{Im}(f)} f^{-1}(T)$.

For each $T \in \operatorname{Im}(f)$ order the elements of $f^{-1}(T)$, say $x_1, \ldots, x_n$ are the distinct elements of $f^{-1}(T)$. Define a function $g_T\colon f^{-1}(T) \to \mathbb{N}$ by setting $g_T(x_i) = i$.

Define $h\colon X \to K(Y) \times \mathbb{N}$ by the assignment $h(x) = (f(x), g_{f(x)}(x))$. One checks readily that h is well-defined and 1-1. Using Fact 3.5.23 this implies

$$|X| \leqslant |K(Y) \times \mathbb{N}| = |K(Y)| = |Y|.$$

By symmetry we have $|Y| \leqslant |X|$, so the Schroeder-Bernstein Theorem implies $|X| = |Y|$, as desired. □

Lemma 3.5.25. *Let k be a field and let F be a k-vector space. Fix elements $x_1, \ldots, x_j, y_j, \ldots, y_n \in F$ where $1 \leqslant j < n$, and assume that F is spanned by $\{x_1, \ldots, x_{j-1}, y_j, \ldots, y_n\}$. If $\{x_1, \ldots, x_j\}$ is linearly independent, then the y_i's can be reindexed so that $F = (x_1, \ldots, x_{j-1}, x_j, y_{j+1}, \ldots, y_n)R$.*

Proof. Case 1: $j = 1$. Our assumptions translate as: $F = (y_1, \ldots, y_n)R$ and $x_1 \neq 0$. Since $x_1 \in F = (y_1, \ldots, y_n)R$ we have $x_1 = r_1 y_1 + \cdots r_n y_n$ for some $r_i \in R$. Since $x_1 \neq 0$, we have $r_k \neq 0$ for some k. Reorder the y_i's to assume that $r_1 \neq 0$. Since k is a field, we have

$$y_1 = r_1^{-1} x_1 + \textstyle\sum_{i=2}^n (-r_1^{-1} r_i) y_i$$

and so $y_1 \in (x_1, y_2, \ldots, y_n)R$. Since we also have $y_i \in (x_1, y_2, \ldots, y_n)R$ for each $i = 2, \ldots, n$, we have

$$F = (y_1, y_2, \ldots, y_n)R \subseteq (x_1, y_2, \ldots, y_n)R \subseteq F$$

and so $F = (x_1, y_2, \dots, y_n)R$.

Case 2: $j \geqslant 2$. We have $F = (x_1, \dots, x_{j-1}, y_j, \dots, y_n)R$, and $\{x_1, \dots, x_j\}$ is linearly independent. Since $x_j \in F = (x_1, \dots, x_{j-1}, y_j, \dots, y_n)R$ we have $x_j = \sum_{i=1}^{j-1} r_i x_i + \sum_{i=j}^{n} r_i y_i$ for some $r_i \in R$.

Suppose that $r_i = 0$ for $i = j, \dots, n$, then $x_j = \sum_{i=1}^{j-1} r_i x_i \in (x_1, \dots, x_{j-1})R$, which is impossible since $\{x_1, \dots, x_{j-1}, x_j\}$ is linearly independent. This implies that $r_i \neq 0$ for some $i = j, \dots, n$. Reorder the y_i's to assume that $r_j \neq 0$. Since k is a field, the argument of Case 1 shows that $y_j \in (x_1, \dots, x_{j-1}, x_j, y_{j+1}, \dots, y_n)R$ and further that $F = (x_1, \dots, x_{j-1}, x_j, y_{j+1}, \dots, y_n)R$ as desired. □

Theorem 3.5.26. *Let k be a field and let F be a k-vector space. If X and Y are two bases for F, then $|X| = |Y|$.*

Proof. If either X or Y is infinite, then this follows from Theorem 3.5.24. Hence we assume that X and Y are both finite. If X is empty, then it is straightforward to show that Y is empty, and conversely. so we assume that $X, Y \neq \emptyset$. Let $x_1, \dots, x_m$ be the distinct elements of X and let $y_1, \dots, y_n$ be the distinct elements of Y.

Claim: $n \geqslant m$. (Once this is shown, a symmetric argument will imply $m \geqslant n$ and so $m = n$ and we are done.) Suppose $n < m$. Lemma 3.5.25 implies that the y_i's can be reordered so that $F = (x_1, y_2, \dots, y_n)R$. By induction on j, Lemma 3.5.25 implies that the remaining y_i's can be reordered so that $F = (x_1, \dots, x_j, y_{j+1}, \dots, y_n)R$ for each $j = 1, \dots, n$. The case $j = n$ says that $F = (x_1, \dots, x_n)R$. In particular, we have $(x_1, \dots, x_n, x_{n+1}, \dots, x_m)R \subseteq (x_1, \dots, x_n)R$. Lemma 3.5.25 implies that $\{x_1, \dots, x_n, x_{n+1}, \dots, x_m\} \subseteq \{x_1, \dots, x_n\}$ and so $x_m \in \{x_1, \dots, x_n\}$. Since $m > n$ and $\{x_1, \dots, x_m\}$ is linearly independent, this is impossible. □

Lemma 3.5.27. *Let R be a ring with identity and $I \subset R$ a two-sided ideal. Let F be a free R-module with basis X, and let $\pi \colon F \to F/IF$ be the canonical epimorphism. Then F/IF is a free R/I-module with basis $\pi(X)$, and $|\pi(X)| = |X|$.*

Proof. Step 1: $\pi(X)$ generates F/IF. This follows from Example 3.4.8 since π is an R-module epimorphism.

Step 2: Fix distinct elements $x_1, \dots, x_n \in X$ and suppose that $r_1, \dots, r_n \in R$ such that $\sum_{i=1}^{n}(r_i + I)\pi(x_i) = 0$. We show that each $r_i \in I$. We have

$$IF = \textstyle\sum_{i=1}^{n}(r_i + I)(x_i + IF) = \sum_{i=1}^{n}(r_i x_i + IF) = (\sum_{i=1}^{n} r_i x_i) + IF$$

and so $\sum_{i=1}^{n} r_i x_i \in IF$. Write $\sum_{i=1}^{n} r_i x_i = \sum_j a_j f_j$ for some $a_j \in I$ and $f_j \in F$. Write each $f_j = \sum_k r_{j,k} x_{j,k}$ for some $r_{j,k} \in R$ and $x_{j,k} \in X$. Then

$$\textstyle\sum_{i=1}^{n} r_i x_i = \sum_j a_j f_j = \sum_j a_j(\sum_k r_{j,k} x_{j,k}) = \sum_{j,k}(a_j r_{j,k}) x_{j,k}.$$

Thus, we have written the element $\sum_{i=1}^{n} r_i x_i$ in the form $\sum_l s_l x'_l$ for some $s_l \in I$ and $x'_l \in X$. Re-index if necessary and add terms of the form $0x_i$ and $0x'_l$ if necessary to write

$$\textstyle\sum_{i=1}^{n} r_i x_i = \sum_{i=1}^{n} s_i x_i$$

with the $s_i \in I$. This implies

$$0 = \textstyle\sum_{i=1}^{n}(r_i - s_i)x_i$$

so the fact that X is linearly independent implies $r_i = s_i \in I$ for each i.

Step 3: $\pi(X)$ is linearly independent over R/I. (This will show that F/IF is a free R/I-module with basis $\pi(X)$.) Fix distinct elements $x_1, \ldots, x_n \in X$ and suppose that $r_1, \ldots, r_n \in R$ such that $\sum_{i=1}^n (r_i + I)\pi(x_i) = 0$. Step 2 shows that each $r_i \in I$, and so each coefficient $r_i + I = I = 0_{R/I}$.

Step 4: $|\pi(X)| = |X|$. The map $\pi\colon X \to \pi(X)$ is surjective by design. We need to show that it is 1-1. Suppose that $x, x' \in X$ such that $x \neq x'$ and $\pi(x) = \pi(x')$. Then

$$(1 + I)\pi(x) + (-1 + I)\pi(x') = 0$$

and so Step 2 implies that $1, -1 \in I$. This implies $I = R$, contradicting our assumption $I \subset R$. □

Definition 3.5.28. Let R be a ring with identity. R satisfies the *invariant basis property* if: for every free R-module F, any two bases of F have the same cardinality. If R has the invariant basis property and F is a free R-module, the *rank* of F is

$$\operatorname{rank}_R(F) = \begin{cases} n & \text{if } F \text{ has a finite basis with exactly } n \text{ elements} \\ \infty & \text{if } F \text{ has an infinite basis.} \end{cases}$$

Every field k has the invariant basis property by Theorem 3.5.26. The rank of a k-vector space V is often called the *dimension* of V, denoted $\dim_k(V) = \operatorname{rank}_k(V)$. Note that this definition differs from Hungerford's definition.

Theorem 3.5.29. *If R is a commutative ring with identity, then R has the invariant basis property.*

Proof. Let F be a free R-module with bases X and Y. Let $\mathfrak{m} \subset R$ be a maximal ideal. Let $\pi\colon F \to F/\mathfrak{m}F$ be the canonical epimorphism. Lemma 3.5.27 implies that $F/\mathfrak{m}F$ is a vector space over $R/\mathfrak{m}$ with bases $\pi(X)$ and $\pi(Y)$. Theorem 3.5.26 then provides the second inequality in the following sequence

$$|X| = |\pi(X)| = |\pi(Y)| = |Y|$$

while the first and third equalities are from Lemma 3.5.27. □

Now we focus on the basic properties of dimension.

Theorem 3.5.30. *Let k be a field. Let V be a k-vector space and let $W \subseteq V$ be a k-subspace.*

(a) $\dim_k(W) \leqslant \dim_k(V)$.
(b) *If* $\dim_k(W) = \dim_k(V)$ *and* $\dim_k(V) < \infty$*, then* $W = V$.
(c) $\dim_k(V) = \dim_k(W) + \dim_k(V/W)$.

Proof. Let Y be a k-basis for W. Theorem 3.5.11 provides a basis X for V such that $Y \subseteq X$.

(a) If $\dim_k(V) = \infty$, then we are done, so assume that $\dim_k(V) < \infty$. Then X is finite, and it follows that Y is finite and

$$\dim_k(W) = |Y| \leqslant |X| = \dim_k(V).$$

(b) Since $\dim_k(V) < \infty$, we know that X is finite, and so Y is finite. Since $\dim_k(W) = \dim_k(V)$, we see that Y is a subset of the finite set X with the same number of elements of X, and so $Y = X$. Thus $W = (Y)R = (X)R = V$.

(c) Claim: The set $Z = \{x + W \in V/W \mid x \in X \smallsetminus Y\}$ is a k-basis for V/W. To see that Z spans V/W, let $v + W \in V/W$. Since $v \in V$, we write

$v = \sum_i r_i x_i + \sum_j s_j y_j$ with $r_i, s_j \in R$, $x_i \in X \smallsetminus Y$ and $y_j \in Y$. Then $\sum_j s_j y_j \in W$ and so

$$v + W = (\textstyle\sum_i r_i x_i + \sum_j s_j y_j)R + W = (\sum_i r_i x_i)R + W \in (\{x_i + W\})R \subseteq (Z)R.$$

This shows that $V/W \subseteq (Z)R$. Since $Z \subseteq V/W$, we have $(Z)R \subseteq V/W$ and so $(Z)R = V/W$.

Note that, for $x, x' \in X \smallsetminus Y$ we have $x = x'$ if and only if $x + W = x' + W$. The forward implication is straightforward. For the reverse implication, assume $x+W = x'+W$. This implies $x - x' \in W = (Y)R$ and so $x - x' = \sum_i r_i y_i$ for some $r_i \in k$ and $y_i \in Y$. Since the set X is linearly independent, this linearly dependence relation implies $x = x'$.

To see that Z is linearly independent over k, let $x_1 + W, \ldots, x_n + W$ be distinct elements of V/W and let $r_1, \ldots, r_n \in k$ such that $\sum_i r_i(x_i + W) = 0$. Then $\sum_i r_i x_i \in W$, so there are distinct elements $y_1, \ldots, y_m \in Y$ and $s_1, \ldots, s_m \in k$ such that

$$\textstyle\sum_i r_i x_i = \sum_j s_j y_j.$$

The elements $x_1, \ldots, x_n, y_1, \ldots, y_m \in X$ are distinct since $Y \cap (X \smallsetminus Y) = \emptyset$, using the previous paragraph. Hence, the displayed linearly dependence relation implies that each $r_i, s_j = 0$. This establishes the claim.

If $\dim_k(V) = \infty$, then X is infinite, and so either Y or $X \smallsetminus Y$ is infinite; in this case, the formula $\dim_k(V) = \dim_k(W) + \dim_k(V/W)$ is satisfied. If $\dim_k(V) < \infty$, then

$$\dim_k(V) = |X| = |Y| + |X \smallsetminus Y| = \dim_k(W) + \dim_k(V/W)$$

as desired. □

Corollary 3.5.31. *Let k be a field and let $f\colon V \to W$ be a linear transformation of k-vector spaces. Then*

$$\dim_k(V) = \dim_k(\operatorname{Im}(f)) + \dim_k(\operatorname{Ker}(f)).$$

PROOF. We have an isomorphism $\operatorname{Im}(f) \cong V/\operatorname{Ker}(f)$ and so Theorem 3.5.30(c) yields the desired equality. □

3.6. Hom

Remark 3.6.1. Let R be a ring and let M and N be left R-modules. Recall that the set $\operatorname{Hom}_R(M, N)$ of all R-module homomorphisms $M \to N$ is an additive abelian group under pointwise addition $(f + g)(m) = f(m) + g(m)$. If R is commutative, then $\operatorname{Hom}_R(M, N)$ is a left R-module via the action $(rf)(m) = rf(m) = f(rm)$.

Definition 3.6.2. Let R be a ring and let $\phi\colon M \to M'$ and $\psi\colon N \to N'$ be homomorphisms of left R-modules. Define the function

$$\operatorname{Hom}_R(M, \psi)\colon \operatorname{Hom}_R(M, N) \to \operatorname{Hom}_R(M, N') \qquad \text{as} \qquad f \mapsto \psi \circ f.$$

Define the function

$$\operatorname{Hom}_R(\phi, N)\colon \operatorname{Hom}_R(M', N) \to \operatorname{Hom}_R(M, N) \qquad \text{as} \qquad g \mapsto g \circ \phi.$$

A common notation for $\operatorname{Hom}_R(M, \psi)$ is ψ_*. A common notation for $\operatorname{Hom}_R(\phi, N)$ is ϕ^*. The module $\operatorname{Hom}_R(M, R)$ is sometimes called the "dual" of M.

Here is the functoriality of Hom.

Proposition 3.6.3. *Let R be a ring and let M be an R-module. Let $\phi\colon N \to N'$ and $\phi'\colon N' \to N''$ be R-module homomorphisms.*

(a) *The maps* $\operatorname{Hom}_R(\phi, M)$ *and* $\operatorname{Hom}_R(M, \phi)$ *are group homomorphisms.*
(b) *We have* $\operatorname{Hom}_R(\mathrm{id}_N, M) = \mathrm{id}_{\operatorname{Hom}_R(N,M)}$ *and* $\operatorname{Hom}_R(M, \mathrm{id}_N) = \mathrm{id}_{\operatorname{Hom}_R(M,N)}$.
(c) *We have equalities* $\operatorname{Hom}_R(\phi' \circ \phi, M) = \operatorname{Hom}_R(\phi, M) \circ \operatorname{Hom}_R(\phi', M)$ *and* $\operatorname{Hom}_R(M, \phi' \circ \phi) = \operatorname{Hom}_R(M, \phi') \circ \operatorname{Hom}_R(M, \phi)$.
(d) *Assuming that R is commutative,* $\operatorname{Hom}_R(\phi, M)$ *and* $\operatorname{Hom}_R(M, \phi)$ *are R-module homomorphisms.*

Proof. We verify the properties for $\operatorname{Hom}_R(-, M)$. For $\operatorname{Hom}_R(M, -)$, the properties are verified similarly.

(a) For $\operatorname{Hom}_R(\phi, M)$, we need to show that

$$\operatorname{Hom}_R(\phi, M)(f + g) = \operatorname{Hom}_R(\phi, M)(f) + \operatorname{Hom}_R(\phi, M)(g)$$

for each $f, g \in \operatorname{Hom}_R(N', M)$. In other words, we need to show that

$$(f + g) \circ \phi = (f \circ \phi) + (g \circ \phi).$$

These are functions $N \to M$, so we check this on elements $n \in N$:

$$((f + g) \circ \phi)(n) = (f + g)(\phi(n)) = f(\phi(n)) + g(\phi(n)) = (f \circ \phi + g \circ \phi)(n)$$

The verification for $\operatorname{Hom}_R(M, \phi)$ is similar.

(b) For each $g \in \operatorname{Hom}_R(N, M)$, we have $\operatorname{Hom}_R(\mathrm{id}_N, M)(g) = g \circ \mathrm{id}_N = g$.

(c) For each $g \in \operatorname{Hom}_R(N'', M)$, we have

$$\begin{aligned}\operatorname{Hom}_R(\phi' \circ \phi, M)(g) &= g \circ (\phi' \circ \phi) = (g \circ \phi') \circ \phi = \operatorname{Hom}_R(\phi, M)(g \circ \phi') \\ &= \operatorname{Hom}_R(\phi, M)(\operatorname{Hom}_R(\phi', M)(g)) \\ &= (\operatorname{Hom}_R(\phi, M) \circ \operatorname{Hom}_R(\phi', M))(g).\end{aligned}$$

(d) Assume that R is commutative. We need to show that

$$\operatorname{Hom}_R(\phi, M)(rg) = r(\operatorname{Hom}_R(\phi, M)(g))$$

for each $r \in R$ and each $g \in \operatorname{Hom}_R(N', M)$. In other words, we need

$$(rg) \circ \phi = r(g \circ \phi).$$

As in part (a), we check this on elements $n \in N$:

$$((rg) \circ \phi)(n) = (rg)(\phi(n)) = r(g(\phi(n))) = (r(g \circ \phi))(n).$$

□

Remark 3.6.4. It is worth noting that Proposition 3.6.3(c) says that the following diagrams commute:

$$\begin{tikzcd}
\operatorname{Hom}_R(N'', M) \arrow[r, "\operatorname{Hom}_R(\phi', M)"] \arrow[dr, "\operatorname{Hom}_R(\phi' \circ \phi, M)"'] & \operatorname{Hom}_R(N', M) \arrow[d, "\operatorname{Hom}_R(\phi, M)"] \\
& \operatorname{Hom}_R(N, M)
\end{tikzcd}$$

$$\begin{tikzcd}
\operatorname{Hom}_R(M, N) \arrow[r, "\operatorname{Hom}_R(M, \phi)"] \arrow[dr, "\operatorname{Hom}_R(M, \phi' \circ \phi)"'] & \operatorname{Hom}_R(M, N') \arrow[d, "\operatorname{Hom}_R(M, \phi')"] \\
& \operatorname{Hom}_R(M, N'')
\end{tikzcd}$$

Proposition 3.6.5. *Let R be a ring and let $\phi\colon M \to M'$ be a homomorphism of left R-modules. Let $n \in \mathbb{N}$.*

(a) $\operatorname{Hom}_R(R^n, M)$ *is a left R-module by the action $(rf)(v) = f(vr)$. If R has identity, then this action is unital.*

(b) *The map* $\operatorname{Hom}_R(R^n, \phi)\colon \operatorname{Hom}_R(R^n, M) \to \operatorname{Hom}_R(R^n, M')$ *is a left R-module homomorphism.*

(c) $\operatorname{Hom}_R(M, R^n)$ *is a right R-module by the action $(\psi r)(v) = \phi(v)r$. If R has identity, then this action is unital.*

(d) *The map* $\operatorname{Hom}_R(\phi, R^n)\colon \operatorname{Hom}_R(M', R^n) \to \operatorname{Hom}_R(M, R^n)$ *is a right R-module homomorphism.*

Proof. Exercise. □

Proposition 3.6.6. *Let R be a ring with identity and let $\phi\colon M \to N$ be a homomorphism of unitary left R-modules. Let $n \in \mathbb{N}$ and let $e_1, \ldots, e_n \in R^n$ be a basis. Define $\Phi_M\colon \operatorname{Hom}_R(R^n, M) \to M^n$ by the formula $\Phi_M(f) = (f(e_1), \ldots, f(e_n))$.*

(a) *The map Φ_M is an isomorphism of left R-modules.*

(b) *There is a commutative diagram*

$$\begin{tikzcd}
\operatorname{Hom}_R(R^n, M) \arrow[r, "\operatorname{Hom}_R(R^n,\phi)"] \arrow[d, "\Phi_M"', "\cong"] & \operatorname{Hom}_R(R^n, N) \arrow[d, "\Phi_N"', "\cong"] \\
M^n \arrow[r, "\phi^n"] & N^n
\end{tikzcd}$$

where $\phi^n(m_1, \ldots, m_n) = (\phi(m_1), \ldots, \phi(m_n))$.

Proof. (a) It is straightforward to show that Φ_M is an R-module homomorphism. To see that it is onto, let $(m_1, \ldots, m_n) \in M^n$. Proposition 3.3.2.7 says that the map $f\colon R^n \to M$ given by $f(r_1, \ldots, r_n) = \sum_i r_i m_i$ is a well-defined R-module homomorphism. By definition, we have $f(e_i) = m_i$ for each i, and so $\Phi_M(f) = (m_1, \ldots, m_n)$.

To see that Φ_M is 1-1, assume that $\Phi_M(f) = 0$. That is, $f(e_i) = 0$ for each i. It follows that for each $\sum_i r_i e_i \in R^n$, we have $f(\sum_i r_i e_i) = \sum_i r_i 0 = 0$. Thus $f = 0$ and Φ_M is bijective.

(b) For $f \in \operatorname{Hom}_R(R^n, M)$, we compute:

$$\begin{aligned}
\Phi_N(\operatorname{Hom}_R(R^n, \phi)(f)) &= \Phi_N(\phi \circ f) = (\phi(f(e_1)), \ldots, \phi(f(e_n))) \\
\phi^n(\Phi_M(f)) &= \phi^n(f(e_1), \ldots, f(e_n)) = (\phi(f(e_1)), \ldots, \phi(f(e_n)))
\end{aligned}$$

as desired. □

3.7. Exact Sequences

Definition 3.7.1. Let R be a ring. A sequence of left R-module homomorphisms

$$M_2 \xrightarrow{f_2} M_1 \xrightarrow{f_1} M_0$$

is *exact* if $\operatorname{Ker}(f_1) = \operatorname{Im}(f_2)$. More generally, a A sequence of left R-module homomorphisms

$$\cdots \xrightarrow{f_{i+1}} M_i \xrightarrow{f_i} M_{i-1} \xrightarrow{f_{i-1}} \cdots$$

is *exact* if $\operatorname{Ker}(f_i) = \operatorname{Im}(f_{i+1})$ for all i. A *short exact sequence* is an exact sequence of the form

$$0 \to M' \to M \to M'' \to 0.$$

Remark 3.7.2. Given an sequence of left R-module homomorphisms

$$\cdots \xrightarrow{f_{i+1}} M_i \xrightarrow{f_i} M_{i-1} \xrightarrow{f_{i-1}} \cdots$$

we have $\operatorname{Ker}(f_i) \supseteq \operatorname{Im}(f_{i+1})$ if and only if $f_i f_{i+1} = 0$.

Example 3.7.3. Let M', M'' be left R-modules. Then the sequence

$$0 \to M' \xrightarrow{f} M' \oplus M'' \xrightarrow{g} M'' \to 0$$

is exact. Here $f(m') = (m', 0)$ and $g(m', m'') = m''$.

Example 3.7.4. Let R be a ring and let $I \subseteq R$ be an ideal. Then the sequence

$$0 \to I \xrightarrow{f} R \xrightarrow{g} R/I \to 0$$

is exact. Here f is the inclusion and g is the natural surjection.

More generally, let M be a left R-module, and let $M' \subseteq M$ be submodule. Then the sequence

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M/M' \to 0$$

is exact. Here f is the inclusion and g is the natural surjection.

Proposition 3.7.5. *Let R be a ring.*

(a) *The sequence $0 \to M' \xrightarrow{f} M$ is exact if and only if f is 1-1.*

(b) *The sequence $M \xrightarrow{g} M'' \to 0$ is exact if and only if g is onto.*

PROOF. f is 1-1 if and only if $\operatorname{Ker}(f) = 0 = \operatorname{Im}(0 \to M')$. g is onto if and only if $\operatorname{Im}(g) = M'' = \operatorname{Ker}(M'' \to 0)$. □

Definition 3.7.6. Let R be a ring, and consider two exact sequence of left R-module homomorphisms

$$M_\bullet = \cdots \xrightarrow{f_{i+1}} M_i \xrightarrow{f_i} M_{i-1} \xrightarrow{f_{i-1}} \cdots$$

and

$$N_\bullet = \cdots \xrightarrow{g_{i+1}} N_i \xrightarrow{g_i} N_{i-1} \xrightarrow{g_{i-1}} \cdots .$$

A *homomorphism* from $M_\bullet$ to $N_\bullet$ is a sequence of maps $h_\bullet = \{h_n \colon M_n \to N_n\}_{n\in\mathbb{Z}}$ such that $h_{n-1}f_n = g_n h_n$ for all $n \in \mathbb{Z}$. In other words, the maps h_n make the following "ladder diagram" commute.

$$\begin{tikzcd}
M_\bullet \arrow[d, "h_\bullet"'] & \cdots \arrow[r, "f_{i+1}"] & M_i \arrow[r, "f_i"] \arrow[d, "h_i"'] & M_{i-1} \arrow[r, "f_{i-1}"] \arrow[d, "h_{i-1}"'] & \cdots \\
N_\bullet & \cdots \arrow[r, "g_{i+1}"] & N_i \arrow[r, "g_i"] & N_{i-1} \arrow[r, "g_{i-1}"] & \cdots .
\end{tikzcd}$$

The homomorphism $h_\bullet$ is an *isomorphism* from $M_\bullet$ to $N_\bullet$ if it has a two-sided inverse, that is, if there exists a homomorphism $k_\bullet \colon N_\bullet \to M_\bullet$ such that $h_n k_n = \mathrm{id}_{N_n}$ and $k_n h_n = \mathrm{id}_{M_n}$ for all n.

Remark 3.7.7. Let R be a ring, and consider two exact sequence of left R-module homomorphisms

$$M_\bullet = \cdots \xrightarrow{f_{i+1}} M_i \xrightarrow{f_i} M_{i-1} \xrightarrow{f_{i-1}} \cdots$$

$$N_\bullet = \cdots \xrightarrow{g_{i+1}} N_i \xrightarrow{g_i} N_{i-1} \xrightarrow{g_{i-1}} \cdots .$$

Let $h_\bullet \colon M_\bullet \to N_\bullet$ be a homomorphism of exact sequences. Then $h_\bullet$ is an isomorphism if and only if each h_n is an isomorphism.

Example 3.7.8. Given two integers m and n with $n \neq 0$, here is a homomorphism of short exact sequences of abelian groups:

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z} \arrow[r, "n"] \arrow[d, "n"'] & \mathbb{Z} \arrow[r] \arrow[d] & \mathbb{Z}/n\mathbb{Z} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & n\mathbb{Z}/mn\mathbb{Z} \arrow[r] & \mathbb{Z}/mn\mathbb{Z} \arrow[r] & \mathbb{Z}/n\mathbb{Z} \arrow[r] & 0.
\end{tikzcd}$$

Here the unlabeled maps are the natural inclusions and surjections. This homomorphism is an isomorphism if and only if $m = 0$.

Proposition 3.7.9 (Short Five Lemma)**.** *Let R be a ring, and consider a homomorphism of exact sequences*

$$\begin{tikzcd}
 & M' \arrow[r, "f"] \arrow[d, "h"'] & M \arrow[r, "g"] \arrow[d, "k"'] & M'' \arrow[r] \arrow[d, "l"'] & 0 \\
0 \arrow[r] & N' \arrow[r, "F"] & N \arrow[r, "G"] & N''. &
\end{tikzcd}$$

(a) *If h and l are 1-1, then k is 1-1.*
(b) *If h and l are onto, then k is onto.*

Proof. (a) Assume that h and l are 1-1. Let $m \in \operatorname{Ker}(k) \subseteq M$. Commutativity of the diagram implies that

$$l(g(m)) = G(k(m)) = G(0) = 0.$$

Since l is 1-1, we have $g(m) = 0$. The exactness of the top row of the diagram implies that $m \in \operatorname{Ker}(g) = \operatorname{Im}(f)$ and so $m = f(m')$ for some $m' \in M'$. It follows that

$$0 = k(m) = k(f(m')) = F(h(m')).$$

Since F and h are 1-1, it follows that $m' = 0$ and so $m = f(m') = f(0) = 0$.

(b) Assume that h and l are onto. Let $n \in N$. Since l is onto, there exists $m'' \in M''$ such that $l(m'') = G(n)$. Since g is onto, there exists $m \in M$ such that $g(m) = m''$, and so

$$G(k(m)) = l(g(m)) = l(m'') = G(n).$$

(We would like to conclude that $k(m) = n$, but this may not be true.) Instead, the displayed equation implies that $G(k(m) - n) = G(k(m)) - G(n) = 0$ and so $k(m) - n \in \operatorname{Ker}(G) = \operatorname{Im}(F)$. Write $k(m) - n = F(n')$ for some $n' \in N'$. Since h is onto, there exists $m' \in M'$ such that $h(m') = n'$. It follows that

$$k(f(m')) = F(h(m')) = F(n') = k(m) - n$$

and so$k(m - f(m')) = n$. Thus, $n \in \operatorname{Im}(k)$ and so k is onto. □

Definition 3.7.10. Let R be a ring. An exact sequence

$$0 \to M' \to M \to M'' \to 0$$

is *split* if it is isomorphic to the sequence

$$0 \to M' \xrightarrow{f} M' \oplus M'' \xrightarrow{g} M'' \to 0$$

where $f(m') = (m', 0)$ and $g(m', m'') = m''$. In particular, if the given sequence is split, then $M \cong M' \oplus M''$.

Here is a classification of split exact sequences.

Proposition 3.7.11. *Let R be a ring, and consider an exact sequence*

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0.$$

TFAE.

(i) *The exact sequence is split;*
(ii) *There is an R-module homomorphism $f_1\colon M \to M'$ such that $f_1 \circ f = \mathrm{id}_{M'}$;*
(iii) *There is an R-module homomorphism $g_1\colon M'' \to M$ such that $g \circ g_1 = \mathrm{id}_{M''}$.*

Proof. We will prove (i) $\iff$ (ii). The proof of (i) $\iff$ (iii) is similar.

(i) $\implies$ (ii) Assume that the given sequence is split. Then there is a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r, "f"] \arrow[d, "h"', "\cong"] & M \arrow[r, "g"] \arrow[d, "k"', "\cong"] & M'' \arrow[r] \arrow[d, "l"', "\cong"] & 0 \\
0 \arrow[r] & M' \arrow[r, "i"] & M' \oplus M'' \arrow[r, "t"] & M'' \arrow[r] & 0
\end{tikzcd}$$

where $i(m') = (m', 0)$ and $t(m', m'') = m''$. Let $i_1\colon M' \oplus M'' \to M'$ be given by $i_1(m', m'') = m'$. We will show that the map $f_1 = h^{-1} \circ i_1 \circ k\colon M \to M'$ satisfies the desired property.

We first compute:

$$i \circ h \circ f_1 \circ f = i \circ h \circ h^{-1} \circ i_1 \circ k \circ f = i \circ i_1 \circ k \circ f = i \circ i_1 \circ i \circ h = i \circ \mathrm{id}_{M'} \circ h = i \circ h.$$

The third equality follows from the commutativity of the diagram. The remaining equalities are by definition. Thus, we have

$$(i \circ h) \circ (f_1 \circ f) = i \circ h = (i \circ h) \circ \mathrm{id}_{M'}.$$

Since i and h are 1-1, it follows that $f_1 \circ f = \mathrm{id}_{M'}$ as desired.

(i) $\impliedby$ (ii) Assume that there is an R-module homomorphism $f_1\colon M \to M'$ such that $f_1 \circ f = \mathrm{id}_{M'}$. Let $F\colon M \to M' \oplus M''$ be given by $F(m) = (f_1(m), g(m))$. We will show that the following diagram commutes

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r, "f"] \arrow[d, "\mathrm{id}_{M'}"', "\cong"] & M \arrow[r, "g"] \arrow[d, "F"', "\cong"] & M'' \arrow[r] \arrow[d, "\mathrm{id}_{M''}"', "\cong"] & 0 \\
0 \arrow[r] & M' \arrow[r, "i"] & M' \oplus M'' \arrow[r, "t"] & M'' \arrow[r] & 0
\end{tikzcd}$$

where $i(m') = (m', 0)$ and $t(m', m'') = m''$. The Short Five Lemma will then imply that F is an isomorphism, so that the displayed diagram is an isomorphism of exact sequences; by definition, it then follows that the original sequence is split.

We compute: for $m' \in M'$ and $m \in M$ we have

$$F(f(m')) = (f_1(f(m')), g(f(m'))) = (m', 0) = i(m').$$
$$t(F(m)) = t(f_1(m), g(m)) = g(m).$$

□

Corollary 3.7.12. *Let R be a ring with identity, and consider an exact sequence*

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

of unitary R-modules. If M'' is free, then this sequence is split.

Proof. It suffices to find an R-module homomorphism $g_1\colon M'' \to M$ such that $gg_1 = \mathrm{id}_{M''}$. Since M'' is free, it has a basis $B \subseteq M''$. g is surjective, so for each $b \in B$, there exists $m_b \in M$ such that $g(m_b) = b$. Define $g_1\colon M'' \to M$ by the formula $g_1(\sum_b a_b b) = \sum_b a_b m_b$. Proposition 3.3.2.7 says that f_1 is a well-defined R-module homomorphism. We compute:

$$g(g_1(\textstyle\sum_b a_b b)) = g(\sum_b a_b m_b) = \sum_b a_b g(m_b) = \sum_b a_b b$$

which shows that $g \circ g_1 = \mathrm{id}_{M''}$, as desired. □

Corollary 3.7.13. *Let R be a commutative ring with identity, and consider an exact sequence*

$$0 \to R^m \xrightarrow{f} R^n \xrightarrow{g} R^p \to 0.$$

Then $n = m + p$.

Proof. Corollary 3.7.12 implies that the given sequence splits. In particular, we have $R^n \cong R^m \oplus R^p \cong R^{m+p}$. The invariant basis property implies that $n = m + p$. □

Remark 3.7.14. The invariant basis property actually holds, more generally, for any ring with identity, whether it is commutative or not. It follows that the conclusion of Corollary 3.7.13 also holds when R is any ring with identity.

3.8. Noetherian Rings and Modules

Definition 3.8.1. Let R be a ring. A left R-module M is *noetherian* if it satisfies the *ascending chain condition (ACC) on submodules*: For every ascending chain of submodules $M_1 \subseteq M_2 \subseteq \cdots \subseteq M$, we have $M_n = M_{n+1} = M_{n+2} = \cdots$ for some $n \geqslant 1$.

Slogan: every ascending chain of submodules stabilizes.

The ring R is *(left) noetherian* if it is noetherian as an R-module, that is, if it satisfies ACC on left ideals.

Example 3.8.2. Every field k is a noetherian ring because the only ideals are $(0)k$ and k. More generally, every PID is noetherian by Lemma 2.5.24.

Theorem 3.8.3. *Let R be a ring and M an R-module. The following conditions are equivalent:*

(i) *M is noetherian as an R-module;*
(ii) *every submodule of M is finitely generated;*
(iii) *every non-empty set of submodules of M has a maximal element.*

Proof. (i) $\implies$ (ii). Assume that M is noetherian and let $N \subseteq M$ be a left submodule. Suppose that N is not finitely generated. In particular, we have $N \neq 0$. Let $0 \neq x_1 \in N$. Since N is not finitely generated, we have $(x_1)R \subsetneq N$, so we have $x_2 \in N - (x_1)R$. It follows that $(x_1)R \subsetneq (x_1, x_2)R$ because $x_2 \in (x_1, x_2)R - (x_1)R$. Since N is not finitely generated, we have $(x_1, x_2)R \subsetneq N$, so we have $x_3 \in N - (x_1, x_2)R$. It follows that $(x_1)R \subsetneq (x_1, x_2)R \subsetneq (x_1, x_2, x_3)R$ because $x_3 \in (x_1, x_2, x_3)R - (x_1, x_2)R$. Continue inductively to find construct an ascending chain of left submodules

$$(x_1)R \subsetneq (x_1, x_2)R \subsetneq \cdots \subsetneq (x_1, x_2, \ldots, x_n)R \subsetneq (x_1, x_2, \ldots, x_n, x_{n+1})R \subsetneq \cdots$$

This chain never stabilizes, contradicting our noetherian assumption. Thus, N is finitely generated.

(ii) $\implies$ (iii). Assume that every left submodule of M is finitely generated, and let S be a non-empty set of left submodules of M. We need to show that S has a maximal element N, that is, a submodule N in S with the following property: If P is a submodule in S such that $N \subseteq P$, then $N = P$.

We employ Zorn's Lemma.[1] For this, we need to show that every chain in S has an upper bound in S. Let C be a chain of submodules in S. As usual the union $N = \cup_{P \in C} P$ is a left submodule of R. We need to show that N is in S. By assumption, the submodule N is finitely generated, say $N = (a_1, \ldots, a_n)R$. Since each $a_i \in N = \cup_{P \in C} P$, we have $a_i \in P_i$ for some $P_i \in C$. Since C is a chain, there is an index j such that $P_i \subseteq P_j$ for each i. Hence, we have $a_i \in P_j$ for each i, and so

$$N = (a_1, \ldots, a_n)R \subseteq P_j \subseteq N.$$

It follows that $N = P_j \in S$, as desired.

(iii) $\implies$ (i). Assume every non-empty set of left submodules of M has a maximal element, and consider a chain of left submodules $M_1 \subseteq M_2 \subseteq \cdots \subseteq M$. We need to show that the chain stabilizes. By assumption, the set $S = \{M_1, M_2, \ldots\}$ has a maximal element, say it is M_n. For each $i \geqslant 1$ we have $M_n \subseteq M_{n+i}$, so the maximality of M_n implies $M_n = M_{n+i}$. Thus, the chain stabilizes and M is noetherian. □

Corollary 3.8.4. *Let R be a ring. The following conditions are equivalent:*

(i) *R is noetherian;*
(ii) *every left ideal of R is finitely generated;*
(iii) *every non-empty set of left ideals of R has a maximal element.*

Proof. This is the special case $M = R$ of Theorem 3.8.3. □

This characterization shows how to construct a ring that is not noetherian.

Example 3.8.5. Let k be a field and let $R = k[x_1, x_2, \ldots]$ be a polynomial ring in infinitely many variables. The ideal $(x_1, x_2, \ldots)R \subset R$ is not finitely generated and so R is not noetherian.

Here is the Hilbert Basis Theorem.

Theorem 3.8.6 (Hilbert). *Let R be a commutative ring with identity. The polynomial ring $R[x]$ is noetherian.*

Proof. Let $I \subseteq R[x]$ be an ideal. We will show that I is finitely generated.

For each $r = 0, 1, 2, \ldots$ let

$$I_r = \{a \in R \mid \exists a_0 + a_1 x + \ldots + a_{r-1}x^{r-1} + ax^r \in I\}.$$

Since I is an ideal in $R[x]$, it follows readily that I_r is an ideal in R. Furthermore, we have $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots \subseteq R$: If $a \in I_r$ then there exists a polynomial $f = a_0 + a_1 x + \ldots + a_{r-1}x^{r-1} + ax^r \in I$; since I is an ideal the polynomial $xf = a_0 x + a_1 x^2 + \ldots + a_{r-1}x^r + ax^{r+1} \in I$, and so $a \in I_{r+1}$.

Since R is noetherian, there exists $J \geqslant 0$ such that, for every $j \geqslant J$ we have $I_j = I_J$. Furthermore, every I_r is finitely generated, say, $I_r = (a_{r,1}, \ldots, a_{r,k_r})R$. Thus,

[1] Q. What is yellow and equivalent to the Axiom of Choice?

there exist $f_{r,1},\ldots,f_{r,k_r}\in I$ such that $f_{r,i}=a_{r,i,0}+a_{r,i,1}x+\ldots+a_{r,i,r-1}x^{r-1}+a_{r,i}x^r$.

Claim: $I=(\{f_{r,i}\mid r=0,\ldots,J;\ i=1,\ldots,k_r\})R$. (Once this is proved, we are done.) Set $I'=(\{f_{r,i}\mid r=0,\ldots,J;\ i=1,\ldots,k_r\})R$. The containment $I\supseteq I'$ holds because each $f_{r,i}\in I$. for the containment $I\subseteq I'$, let $f\in I$. Since $0\in I'$, we assume that $f\neq 0$ and set $s=\deg(f)$. We show that $f\in I'$ by induction on s.

Base case: $s=0$. Here we see that f is constant, and so $f=a_0\in R$. Since $f\in I$, we conclude that $f\in I_0=(a_{0,1},\ldots,a_{0,k_0})R=(f_{0,1},\ldots,f_{0,k_0})R\subseteq I'$.

Inductive step: Assume that $s\geqslant 1$ and that, for every polynomial $g\in I$ with $\deg(g)<s$, we have $g\in I'$. Write $f=b_0+\cdots+b_sx^s$.

Case 1: $s\leqslant J$. Then $b_s\in I_s=(a_{s,1},\ldots,a_{s,k_s})R$. Write $b_s=\sum_{i=1}^{k_s}c_ia_{s,i}$ with each $c_i\in R$. The polynomial $g=f-\sum_{i=1}^{k_s}c_if_{s,i}x^{r-s}\in I$ is either 0 or has $\deg(g)<s$. Furthermore, we have $f-g=\sum_{i=1}^{k_s}c_if_{s,i}x^{r-s}\in(f_{s,1},\ldots,f_{s,k_s})R\subseteq I'$, and so $f\in I'$ if and only if $g\in I'$. By our induction hypothesis, we have $g\in I'$, and so $f\in I'$, as desired.

Case 2: $s>J$. Then $b_s\in I_s=I_J=(a_{J,1},\ldots,a_{J,k_J})R$. Write $b_s=\sum_{i=1}^{k_J}c_ia_{J,i}$ with each $c_i\in R$. The polynomial $g=f-\sum_{i=1}^{k_J}c_if_{J,i}x^{r-J}\in I$ is either 0 or has $\deg(g)<s$. Furthermore, we have $f-g=\sum_{i=1}^{k_J}c_if_{J,i}x^{r-J}\in I'$, and so $f\in I'$ if and only if $g\in I'$. By our induction hypothesis, we have $g\in I'$, and so $f\in I'$, as desired. □

The Hilbert Basis Theorem gives a lot of examples of noetherian rings.

Definition 3.8.7. Let S be a commutative ring with identity, and let $R\subseteq S$ be a subring such that $1_R=1_S$. Given a subset $T\subset S$, let $R[T]$ denote the intersection of all subrings of S that contain $R\cup T$. This is the *subring of S generated over R by T*. It is the smallest subring of S containing R and T. In other words, it is the smallest R-subalgebra of S containing T.

The R-algebra S is said to be a *finitely generated R-algebra* if there are elements $s_1,\ldots,s_n\in S$ such that $S=R[\{s_1,\ldots,s_n\}]=R[s_1,\ldots,s_n]$.

Corollary 3.8.8. *Let R be a commutative ring with identity. Every finitely generated R-algebra is noetherian. In particular, each polynomial ring in finitely many variables $R[x_1,\ldots,x_n]$ is noetherian.*

Proof. For polynomial rings, the result follows from the Hilbert Basis Theorem by induction on the number of variables. In general, each finitely generated R-algebra is (isomorphic to a ring) of the form $R[x_1,\ldots,x_n]/J$. Since R is noetherian, the same is true of the polynomial ring $R[x_1,\ldots,x_n]$, and an exercise shows that the same is true for the quotient $R[x_1,\ldots,x_n]/J$. □

3.9. Modules over Principal Ideal Domains

Proposition 3.9.1. *Let R be a PID. Every submodule of R^n is free of rank $\leqslant n$.*

Proof. By induction on n. If $n=1$, then every submodule $M\subseteq R$ is $M=rR$ for some $r\in R$. Therefore,

$$M=\begin{cases}\{0\}\cong R^0 & \text{if } r=0\\ rR\cong R^1 & \text{if } r\neq 0.\end{cases}$$

Assume $n > 1$ and assume that every submodule of R^{n-1} is free of rank $\leqslant n-1$. Let $K \subseteq R^n$ be a submodule, and define $t\colon R^n \to R$ by the formula $t(a_1, \ldots, a_n) = a_n$. Check that t is a homomorphism with $\mathrm{Ker}(t) = R^{n-1} \oplus \{0\} \cong R^{n-1}$. It follows that $t(K) \subseteq R$, so $t(K) = rR$ for some $r \in R$. If $r = 0$, then $K \subseteq \mathrm{Ker}(t) = R^{n-1}$, so our induction hypothesis implies that K is free of rank $\leqslant n-1$. So, we assume that $r \neq 0$.

Define $g\colon K \to t(K)$ by the formula $g(k) = t(k)$. Then g is an R-module epimorphism. It is straightforward to verify that

$$\mathrm{Ker}(g) = \mathrm{Ker}(t) \cap K = R^{n-1} \cap K \subseteq R^{n-1}.$$

By our induction hypothesis, we have $\mathrm{Ker}(g) \cong R^m$ for some $m \leqslant n-1$.

There is an exact sequence

$$0 \to \mathrm{Ker}(g) \to K \xrightarrow{g} t(K) \to 0.$$

Since $t(K)$ is free, this sequence splits, so we have

$$K \cong \mathrm{Ker}(g) \oplus t(K) \cong R^m \oplus R \cong R^{m+1}.$$

Since $m+1 \leqslant n$, this is the desired result. □

Remark 3.9.2. Let R be a commutative ring with identity, and fix integers $n, k \geqslant 1$. Recall that we have $\mathrm{Hom}_R(R^k, R^n) \cong \mathcal{M}_{n\times k}(R)$. Specifically, let $h\colon R^k \to R^n$ be an R-module homomorphism. Write elements of R^k and R^n as column vectors with entries in R. Let $\mathbf{e}_1, \ldots, \mathbf{e}_k \in R^k$ be the standard basis. For $j = 1, \ldots, k$ write

$$h(\mathbf{e}_j) = \begin{pmatrix} a_{1,j} \\ \vdots \\ a_{i,j} \\ \vdots \\ a_{n,j} \end{pmatrix}.$$

Then h is represented by the $n \times k$ matrix

$$[f] = (a_{i,j}) = \begin{pmatrix} a_{1,1} & \cdots & a_{1,j} & \cdots & a_{1,k} \\ \vdots & & \vdots & & \vdots \\ a_{i,1} & \cdots & a_{i,j} & \cdots & a_{i,k} \\ \vdots & & \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,j} & \cdots & a_{n,k} \end{pmatrix}$$

in the following sense: For each vector

$$\begin{pmatrix} r_1 \\ \vdots \\ r_k \end{pmatrix} \in R^k$$

we have

$$h\begin{pmatrix} r_1 \\ \vdots \\ r_k \end{pmatrix} = \begin{pmatrix} a_{1,1} & \cdots & a_{1,k} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,k} \end{pmatrix} \begin{pmatrix} r_1 \\ \vdots \\ r_k \end{pmatrix}.$$

We have elementary basis operations on the $\mathbf{e}_j$:

(1) Replace $\mathbf{e}_j$ with $u\mathbf{e}_j$ where $u \in R$ is a unit;
(2) Interchange $\mathbf{e}_j$ and $\mathbf{e}_l$;
(3) Replace $\mathbf{e}_j$ with $\mathbf{e}_j + r\mathbf{e}_l$ for some $r \in R$ and $l \neq j$.

These correspond to the appropriate elementary column operations on the matrix $(a_{i,j})$, in the following sense. Applying one of the elementary basis operations to the $\mathbf{e}_j$ yields an isomorphism $\Phi\colon R^k \to R^k$ such that the following diagram commutes

$$\begin{tikzcd}
R^k \arrow[r, "(a_{i,j})"] \arrow[d, "\Phi"', "\cong"] & R^n \arrow[d, "="] \\
R^k \arrow[r, "(b_{i,j})"] & R^n
\end{tikzcd}$$

where $(b_{i,j})$ is the matrix obtained by applying the corresponding elementary column operation to the matrix $(a_{i,j})$. And, conversely, if $(b_{i,j})$ is obtained from $(a_{i,j})$ by an elementary column operation, then the corresponding elementary basis operations on the $\mathbf{e}_j$ yields a commutative diagram as above.

Let $\mathbf{f}_1, \ldots, \mathbf{f}_n \in R^n$ be the standard basis. The elementary basis operations on the $\mathbf{f}_j$ correspond similarly to the elementary row operations on the matrix $(a_{i,j})$.

Furthermore, if we repeatedly apply elementary row and column operations to the matrix $(a_{i,j})$ to obtain the matrix $(c_{i,j})$, then this yields a commutative diagram

$$\begin{tikzcd}
R^k \arrow[r, "(a_{i,j})"] \arrow[d, "\Phi"', "\cong"] & R^n \arrow[d, "\Psi"', "\cong"] \\
R^k \arrow[r, "(c_{i,j})"] & R^n.
\end{tikzcd}$$

We say that an $n \times k$ matrix $(d_{i,j})$ with entries in R is *equivalent* to $(a_{i,j})$ if it can be obtained from $(a_{i,j})$ using a (finite) sequence of elementary row and column operations.

Proposition 3.9.3. *Let R be a PID. Fix integers $n \geqslant k \geqslant 1$ and let $h\colon R^k \to R^n$ be an R-module monomorphism. There exists a commutative diagram of group homomorphisms*

$$\begin{tikzcd}
R^k \arrow[r, "h"] \arrow[d, "\Phi"', "\cong"] & R^n \arrow[d, "\Psi"', "\cong"] \\
R^k \arrow[r, "h'"] & R^n
\end{tikzcd}$$

such that the matrix representing h' is "diagonal", that is, $[h'] = (d_{i,j})$ where $d_{i,j} = 0$ when $i \neq j$.

Proof. Let $[h] = (a_{i,j})$, and let A denote the set of all $s \in R$ such that a finite number of elementary row and column operations applied to $(a_{i,j})$ yields a matrix with s in the upper left corner. The set $S = \{sR \mid s \in A\}$ is a non-empty set of ideals of R. Since R is a PID, it is noetherian, and so S has a maximal element. Apply the necessary row and column operations to yield a new matrix $(b_{i,j})$ such that $b_{1,1}R$ is a maximal element of S.

Note that $b_{1,1} \neq 0$. Indeed, since h is a monomorphism, the matrix $(b_{i,j})$ is non-zero. It follows that a finite number of row and column operations will yield a matrix with a non-zero element $s \neq 0$ in the upper left corner. If $b_{1,1} = 0$, then $b_{1,1}R = (0) \subsetneq sR$, contradicting the maximality of $b_{1,1}$ in S.

Claim: $b_{1,1} \big| b_{1,2}$. Suppose not. Then $b_{1,2} \notin b_{1,1}R$. It follows that $b_{1,1}R \subsetneq (b_{1,1}, b_{1,2})R$. Since R is a PID, there is an element $d \in R$ such that $(b_{1,1}, b_{1,2})R =$

dR. Thus, we have
$$(0) \subsetneq b_{1,1}R \subsetneq (b_{1,1}, b_{1,2})R = dR.$$
In particular, we have $d \neq 0$. We will derive a contradiction by showing that $d \in A$; the relation $b_{1,1}R \subsetneq dR$ will then contradict the maximality of $b_{1,1}R$ in S.

Since $d \in dR = (b_{1,1}, b_{1,2})R$, there are elements $u, v \in R$ such that $d = ub_{1,1} + vb_{1,2}$. On the other hand, we have $b_{1,1}, b_{1,2} \in (b_{1,1}, b_{1,2})R = dR$ and so there are elements $x, y \in R$ such that $b_{1,1} = xd$ and $b_{1,2} = yd$. This yields
$$1d = d = ub_{1,1} + vb_{1,2} = uxd + vyd = (ux + vy)d$$
and so $ux + vy = 1$ because $d \neq 0$.

Consider the following matrix multiplication:
$$\begin{pmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,k} \\ b_{2,1} & b_{2,2} & \cdots & b_{2,k} \\ \vdots & \vdots & & \vdots \\ b_{n,1} & b_{n,2} & \cdots & b_{n,k} \end{pmatrix} \begin{pmatrix} u & -y & 0 & \cdots & 0 \\ v & x & 0 & \cdots & 0 \\ 0 & 1 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} = \begin{pmatrix} d & * & \cdots & * \\ * & * & \cdots & * \\ \vdots & \vdots & & \vdots \\ * & * & \cdots & * \end{pmatrix}$$
Because $ux + vy = 1$, it can be shown that the second matrix corresponds to a change of basis. It follows that $d \in A$, as desired.

A similar argument shows that $b_{1,1} \big| b_{1,i}$ for $i = 2, \ldots, k$ and $b_{1,1} \big| b_{j,1}$ for $j = 2, \ldots, n$. Thus, we may use elementary row and column operations to find an matrix $(c_{i,j})$ equivalent to $(b_{i,j})$ and hence equivalent to $(a_{i,j})$ such that $r \neq 1$ implies $c_{1,r} = 0$ and $c_{r,1} = 0$:
$$\begin{pmatrix} c_{1,1} & 0 & 0 & \cdots & 0 \\ 0 & c_{2,2} & c_{2,3} & \cdots & c_{2,k} \\ 0 & c_{3,2} & c_{3,3} & \cdots & c_{3,k} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & c_{n,2} & c_{n,3} & \cdots & c_{n,k} \end{pmatrix}$$

Repeating this process to appropriate "submatrices" of $(c_{i,j})$ yields the desired matrix, and Remark 3.9.2 yields the desired commutative diagram. □

Note that, in the next result, we have $\operatorname{Coker}(h) = N/\operatorname{Im}(h)$ and $\operatorname{Coker}(h') = N'/\operatorname{Im}(h')$.

Proposition 3.9.4. *Let R be a ring, and consider the following commutative diagram of R-module homomorphisms*
$$\begin{tikzcd} K \arrow[r, "h"] \arrow[d, "\Phi"'] & N \arrow[d, "\Psi"'] \\ K' \arrow[r, "h'"] & N'. \end{tikzcd}$$

(a) *There is a unique R-module homomorphism $\alpha\colon N/\operatorname{Im}(h) \to N'/\operatorname{Im}(h')$ making the following diagram commute*
$$\begin{tikzcd} K \arrow[r, "h"] \arrow[d, "\Phi"'] & N \arrow[r, "\pi"] \arrow[d, "\Psi"'] & N/\operatorname{Im}(h) \arrow[r] \arrow[d, dashed, "\exists!\alpha"'] & 0 \\ K' \arrow[r, "h'"] & N' \arrow[r, "\pi'"] & N'/\operatorname{Im}(h') \arrow[r] & 0 \end{tikzcd}$$
where π and π' are the natural epimorphisms.

(b) *If Ψ is surjective, then so is α.*

(c) *If Φ is surjective and Ψ is injective, then α is injective.*

Proof. Let $\alpha\colon N/\operatorname{Im}(h) \to N'/\operatorname{Im}(h')$ be given by $\alpha(\overline{x}) = \overline{\Psi(x)}$. It is straightforward to show that α satisfies the given properties. □

Here is the Fundamental Theorem for Finitely Generated Modules over a PID. Compare to the Fundamental Theorem for Finite Abelian Groups.

Theorem 3.9.5. *Let R be a PID and let M be a finitely generated R-modle. Then G is a direct sum of cyclic R-modules:*

$$M \cong R/d_1R \oplus \cdots \oplus R/d_kR \oplus R^{n-k}.$$

Proof. Let $\{m_1, \ldots, m_n\} \subseteq M$ be a generating set for M. The map $f\colon R^n \to M$ given by $f(r_1, \ldots, r_n) = \sum_i r_i m_i$ is a well-defined group epimorphism. We have $\operatorname{Ker}(f) \subseteq R^n$, so Proposition 3.9.1 yields an isomorphism $h_1\colon R^k \xrightarrow{\cong} \operatorname{Ker}(f)$ for some $k \leqslant n$. Let $\varepsilon\colon \operatorname{Ker}(f) \to R^n$ be the natural inclusion, and set $h = \varepsilon h_1\colon R^k \to R^n$. Since h_1 is an isomorphism and ε is a monomorphism, we know that h is a monomorphism.

Proposition 3.9.3 yields a commutative diagram of group homomorphisms

$$\begin{tikzcd}
R^k \arrow[r, "h"] \arrow[d, "\Phi"', "\cong"] & R^n \arrow[d, "\Psi"', "\cong"] \\
R^k \arrow[r, "h'"] & R^n
\end{tikzcd}$$

such that $[h'] = (d_{i,j})$ where $d_{i,j} = 0$ when $i \neq j$. Let $\mathbf{f}_1, \ldots, \mathbf{f}_n \in \mathbb{Z}^n$ be the standard basis. Then we have

$$\begin{aligned}
M &\cong R^n/\operatorname{Ker}(f) && \text{first isomorphism theorem}\\
&= R^n/\operatorname{Im}(h) && \text{construction of } h\\
&\cong R^n/\operatorname{Im}(h') && \text{Proposition 3.9.4}\\
&= R^n/(d_{1,1}\mathbf{f}_1, \ldots, d_{k,k}\mathbf{f}_k)R && \text{assumptions on } h'\\
&\cong R/d_{1,1}R \oplus \cdots \oplus R/d_{k,k}R \oplus \mathbb{Z}^{n-k} && \text{Exercise.}
\end{aligned}$$

This is the desired conclusion. □

3.10. Left Exactness of Hom

The next results says that $\operatorname{Hom}_R(N, -)$ and $\operatorname{Hom}_R(-, N)$ are left exact.

Theorem 3.10.1. *Let R be a ring and let N be an R-module.*

(a) *Given an exact sequence*

$$0 \to M' \xrightarrow{f'} M \xrightarrow{f} M''$$

of R-module homomorphisms, the induced sequence

$$0 \to \operatorname{Hom}_R(N, M') \xrightarrow{f'_*} \operatorname{Hom}_R(N, M) \xrightarrow{f_*} \operatorname{Hom}_R(N, M'')$$

of homomorphisms of abelian groups is exact.

(b) *Given an exact sequence*

$$M' \xrightarrow{f'} M \xrightarrow{f} M'' \to 0$$

of R-module homomorphisms, the induced sequence

$$0 \to \mathrm{Hom}_R(M'', N) \xrightarrow{f^*} \mathrm{Hom}_R(M, N) \xrightarrow{(f')^*} \mathrm{Hom}_R(M', N)$$

of homomorphisms of abelian groups is exact.

Proof. We will verify part (a). The verification of part (b) is similar.

1. f'_* is 1-1. Let $\phi \in \mathrm{Ker}(f'_*) \subseteq \mathrm{Hom}_R(N, M')$. Then $0 = f'_*(\phi) = f' \circ \phi$. Since f' is 1-1, it follows that $\phi = 0$.

2. $\mathrm{Ker}(f_*) \supseteq \mathrm{Im}(f'_*)$. Proposition 3.6.3(c) provides the first equality in the following sequence

$$f_* \circ f'_* = \mathrm{Hom}_R(N, f \circ f') = \mathrm{Hom}_R(N, 0) = 0.$$

The second equality follows from the exactness of the original sequence. The third equality is straightforward.

3. $\mathrm{Ker}(f_*) \subseteq \mathrm{Im}(f'_*)$. Let $\phi \in \mathrm{Ker}(f_*) \subseteq \mathrm{Hom}_R(N, M)$. Then $0 = f_*(\phi) = f \circ \phi$ and it follows that $\mathrm{Im}(\phi) \subseteq \mathrm{Ker}(f) = \mathrm{Im}(f')$. For every $n \in N$, this implies that $\phi(n) = f'(m'_n)$ for some $m'_n \in M'$. Furthermore, since f' is 1-1, the element m'_n is the unique element $m' \in M'$ such that $\phi(n) = f'(m')$.

Define $\psi \colon N \to M'$ by the rule $\psi(n) = m'_n$. This is well-defined by the previous paragraph.

Claim: ψ is an R-module homomorpism. By definition, $m'_{n_1+n_2}$ is the unique element $m' \in M'$ such that $\phi(n_1 + n_2) = f'(m')$. By assumption, we have

$$f'(m_{n_1} + m_{n_2}) = f'(m_{n_1}) + f'(m_{n_2}) = \phi(n_1) + \phi(n_2) = \phi(n_1 + n_2).$$

Hence, the uniqueness of $m'_{n_1+n_2}$ implies that

$$\psi(n_1 + n_2) = m'_{n_1+n_2} = m_{n_1} + m_{n_2} = \psi(n_1) + \psi(n_2).$$

A similar argument shows that $\psi(rn) = r\psi(n)$.

Thus, we have $\psi \in \mathrm{Hom}_R(N, M')$. Now we show that $f'_*(\psi) = \phi$:

$$(f'_*(\psi))(n) = f'(\psi(n)) = f'(m'_n) = \phi(n).$$

Hence, we have $\phi \in \mathrm{Im}(f'_*)$, and we are done. □

The next result says that $\mathrm{Hom}_R(R^n, -)$ is exact.

Proposition 3.10.2. *Let R be a ring with identity, and let $n \geqslant 0$. Given an exact sequence*

$$M' \xrightarrow{f'} M \xrightarrow{f} M''$$

of R-module homomorphisms, the induced sequence

$$\mathrm{Hom}_R(R^n, M') \xrightarrow{f'_*} \mathrm{Hom}_R(R^n, M) \xrightarrow{f_*} \mathrm{Hom}_R(R^n, M'')$$

of homomorphisms of abelian groups is exact.

Proof. It is straightforward to show that the bottom row of the following commutative diagram

$$\begin{tikzcd}
\mathrm{Hom}_R(R^n, M)' \arrow[r, "f'_*"] \arrow[d, "\Phi_{M'}"', "\cong"] & \mathrm{Hom}_R(R^n, M) \arrow[r, "f_*"] \arrow[d, "\Phi_M"', "\cong"] & \mathrm{Hom}_R(R^n, M'') \arrow[d, "\Phi_{M''}"', "\cong"] \\
(M')^n \arrow[r, "(f')^n"] & M^n \arrow[r, "f^n"] & (M'')^n
\end{tikzcd}$$

is exact; see Proposition 3.6.6. A diagram chase shows that the top row is exact. □

The next example says that $\mathrm{Hom}_R(N, -)$ and $\mathrm{Hom}_R(-, N)$ are not usually exact:

Example 3.10.3. Consider the sequence of $\mathbb{Z}$-modules

$$0 \to \mathbb{Z} \xrightarrow{\mu_2} \mathbb{Z} \xrightarrow{\tau} \mathbb{Z}/2\mathbb{Z} \to 0 \qquad (*)$$

where $\mu_2(n) = 2n$ and $\tau(m) = \overline{m}$. This sequence is exact. However, the sequences $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, (*))$ and $\mathrm{Hom}_{\mathbb{Z}}((*), \mathbb{Z}/2\mathbb{Z})$ are not exact, as follows.

To see that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, (*))$ is not exact, we need to show that the map

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \xrightarrow{\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \tau)} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$$

is not onto. We show that $\mathrm{id}_{\mathbb{Z}/2\mathbb{Z}} \colon \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ is not in $\mathrm{Im}(\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \tau))$. By definition, it suffices to show that there does not exist a $\mathbb{Z}$-module homomorphism $\phi \colon \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}$ making the following diagram commute.

$$\begin{tikzcd}
 & \mathbb{Z}/2\mathbb{Z} \arrow[ld, dashed, "\nexists\phi"'] \arrow[d, "="] \\
\mathbb{Z} \arrow[r, "\tau"] & \mathbb{Z}/2\mathbb{Z}.
\end{tikzcd}$$

Note that the only $\mathbb{Z}$-module homomorphism $\phi \colon \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}$ is the zero map $\phi = 0$, and this map does not make the diagram commute. (Another way to see this: The map ϕ would give a splitting of the sequence $(*)$, which would imply that $\mathbb{Z} \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, which is impossible.)

To see that the sequence $\mathrm{Hom}_{\mathbb{Z}}((*), \mathbb{Z}/2\mathbb{Z})$ is not exact, we need to show that the map

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \xrightarrow{\mathrm{Hom}_{\mathbb{Z}}(\mu_2, \mathbb{Z}/2\mathbb{Z})} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$$

is not onto. We show that $\tau \colon \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ is not in $\mathrm{Im}(\mathrm{Hom}_{\mathbb{Z}}(\mu_2, \mathbb{Z}/2\mathbb{Z}))$. By definition, it suffices to show that there does not exist a $\mathbb{Z}$-module homomorphism $\psi \colon \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ making the following diagram commute.

$$\begin{tikzcd}
\mathbb{Z} \arrow[r, "\mu_2"] \arrow[d, "\tau"'] & \mathbb{Z} \arrow[ld, dashed, "\nexists\psi"] \\
\mathbb{Z}/2\mathbb{Z} &
\end{tikzcd}$$

Let $\psi \colon \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}$. Then $\psi(\mu_2(1)) = \psi(2) = 2\psi(1) = 0 \neq \tau(1)$, so ψ does not make the diagram commute.

3.11. Projective Modules and Injective Modules

Definition 3.11.1. Let R be a ring. An R-module P is *projective* if $\mathrm{Hom}_R(P, -)$ transforms arbitrary exact sequences into exact sequences.

Remark 3.11.2. Since $\mathrm{Hom}_R(M, -)$ is always left exact, a module P is projective if and only if, for every R-module epimorphism $f \colon M \twoheadrightarrow M''$ the induced map $\mathrm{Hom}_R(P, f) \colon \mathrm{Hom}_R(P, M) \to \mathrm{Hom}_R(P, M'')$ is surjective.

Proposition 3.10.2 says that, when R has identity, the module R^n is projective. The next result generalizes this.

Proposition 3.11.3. *Let R be a ring with identity, and let F be a free R-module. Then F is projective.*

Proof. It suffices to consider an exact sequence

$$M \xrightarrow{g} M'' \to 0$$

and show that the resulting sequence

$$\operatorname{Hom}_R(F,M) \xrightarrow{\operatorname{Hom}_R(F,g)} \operatorname{Hom}_R(F,M'') \to 0$$

is exact. Fix an R-module homomorphism $f \in \operatorname{Hom}_R(F,M'')$ and consider the diagram

$$\begin{tikzcd} & F \arrow[ld, dashed, "\exists h"'] \arrow[d, "f"] & \\ M \arrow[r, "g"] & M'' \arrow[r] & 0. \end{tikzcd}$$

It suffices to find h making the diagram commute.

Let $B \subseteq F$ be a basis for F as an R-module. The map g is surjective. For each $b \in B$, choose an element $m_b \in M$ such that $g(m_b) = f(b)$. Define $h\colon F \to M$ by the formula $h(\sum_{b\in B} r_b b) = \sum_{b\in B} r_b m_b$. Proposition 3.3.2.7 shows that h is a well-defined R-module homomorphism. Also, we have

$$g(h(\textstyle\sum_{b\in B} r_b b)) = g(\sum_{b\in B} r_b m_b) = \sum_{b\in B} r_b g(m_b) = \sum_{b\in B} r_b f(b) = f(\sum_{b\in B} r_b b)$$

and so

$$f = gh = \operatorname{Hom}_R(F,g)(h).$$

It follows that $\operatorname{Hom}_R(F,g)$ is surjective, as desired. □

The implication (iv) $\implies$ (i) in the next result generalizes the previous result. Note that the map h in condition (ii) need not be unique.

Proposition 3.11.4. *Let R be a ring with identity, and let P be a unitary R-module. TFAE.*

(i) *P is a projective R-module;*

(ii) *For every diagram of unitary R-module homomorphisms with exact bottom row*

$$\begin{tikzcd} & P \arrow[d, "f"] & \\ M \arrow[r, "g"] & M'' \arrow[r] & 0 \end{tikzcd}$$

there is an R-module homomorphism $h\colon P \to M$ making the next diagram commute

$$\begin{tikzcd} & P \arrow[ld, dashed, "\exists h"'] \arrow[d, "f"] & \\ M \arrow[r, "g"] & M'' \arrow[r] & 0. \end{tikzcd}$$

(iii) *Every exact sequence of the form $0 \to M' \to M \to P \to 0$ splits;*

(iv) *There is a unitary R-module M' such that $P \oplus M'$ is free.*

Proof. (i) $\implies$ (ii). Assume that P is projective and consider a diagram

$$\begin{tikzcd} & P \arrow[d, "f"] & \\ M \arrow[r, "g"] & M'' \arrow[r] & 0 \end{tikzcd}$$

with exact bottom row. The fact that P is projective implies that the following sequence is exact:

$$\mathrm{Hom}_R(P,M) \xrightarrow{\mathrm{Hom}_R(P,g)} \mathrm{Hom}_R(P,M'') \to 0.$$

The given map f is in $\mathrm{Hom}_R(P,M'')$, so there exists $h \in \mathrm{Hom}_R(P,M)$ such that

$$f = \mathrm{Hom}_R(P,g)(h) = g \circ h.$$

Hence h makes the desired diagram commute.

(ii) $\implies$ (iii). Assume condition (ii) holds and consider an exact sequence $0 \to M' \to M \to P \to 0$. This gives a commutative diagram

$$\begin{tikzcd} & P \arrow[dl, dashed, "\exists g_1"'] \arrow[d, "\mathrm{id}_P"] & \\ M \arrow[r, "g"] & P \arrow[r] & 0. \end{tikzcd}$$

The map h satisfies $gg_1 = \mathrm{id}_P$, so the sequence splits by Proposition 3.7.11.

(iii) $\implies$ (iv). Proposition 3.3.4.11(a) a free R-module F and a surjection $\tau\colon F \to M$. Condition (iii) implies that the exact sequence

$$0 \to \mathrm{Ker}(\tau) \to F \xrightarrow{\tau} P \to 0$$

splits, and so $F \cong \mathrm{Ker}(\tau) \oplus P$.

(iv) $\implies$ (i). Write $F = P \oplus M'$. Proposition 3.11.3 shows that F is projective. By an exercise, we know that

$$\mathrm{Hom}_R(F,-) \cong \mathrm{Hom}_R(P \oplus M',-) \cong \mathrm{Hom}_R(P,-) \oplus \mathrm{Hom}_R(M',-).$$

Since $\mathrm{Hom}_R(F,-)$ transforms arbitrary exact sequences into exact sequences, another exercise implies that the the same is true of $\mathrm{Hom}_R(P,-)$ and $\mathrm{Hom}_R(M',-)$. In particular, P is projective. □

Here is an example of a ring with a non-free projective module.

Example 3.11.5. Let R_1 and R_2 be rings with identity and set $R = R_1 \times R_2$. The modules $P_1 = R_1 \times 0$ and $P_2 = 0 \times R_2$ are both projective because $P_1 \oplus P_2 \cong R$. Note that P_1 is not free because the element $(0,1) \in R$ is non-zero and $(0,1)P_1 = 0$.

Definition 3.11.6. Let R be a ring. An R-module I is *injective* if $\mathrm{Hom}_R(-,I)$ transforms arbitrary exact sequences into exact sequences.

Remark 3.11.7. Since $\mathrm{Hom}_R(-,N)$ is always left exact, the module I is injective if and only if, for every R-module monomorphism $f\colon M' \hookrightarrow M$ the induced map $\mathrm{Hom}_R(f,I)\colon \mathrm{Hom}_R(M,I) \to \mathrm{Hom}_R(M',I)$ is surjective.

Proposition 3.11.8. *Let R be a ring with identity, and let I be a unitary R-module. TFAE.*

(i) *I is an injective R-module;*

(ii) *For every diagram of unitary R-module homomorphisms with exact top row*

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r, "f"] \arrow[d, "g"'] & M \\
& I &
\end{tikzcd}$$

there is an R-module homomorphism $h\colon M \to I$ making the next diagram commute

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r, "f"] \arrow[d, "g"'] & M \arrow[dl, dashed, "\exists h"] \\
& I. &
\end{tikzcd}$$

□

Remark 3.11.9. Note that the map h in condition (ii) need not be unique.

Also, note the absence of a condition corresponding to Proposition 3.11.4(iii) and (iv). There is an analogue of (iii), but we do not have time to prove it. There is no version of (iv).

Examples of injective modules are more difficult to construct. However, it can be shown that the quotient field of a PID R is injective over R.

3.12. Tensor Product

Remark 3.12.1. Let R be a ring. The function $\mu\colon R \times R$ given by $\mu(r, s) = rs$ is not as well-behaved as one might like. For instance, it is not an R-module homomorphism:

$$\mu((1,0) + (0,1)) = \mu(1,1) = 1 \neq 0 = \mu(1,0) + \mu(0,1).$$

In a sense, the tensor product fixes this problem.

Definition 3.12.2. Let R be a ring. Let M be a right R-module and let N be a left R-module. Let G be an abelian group. A function $f\colon M \times N \to G$ is *R-biadditive* if

$$\begin{aligned}
f(m + m', n) &= f(m, n) + f(m', n) \\
f(m, n + n') &= f(m, n) + f(m, n') \\
f(mr, n) &= f(m, rn)
\end{aligned}$$

for all $m, m' \in M$ all $n, n' \in N$ and all $r \in R$.

Example 3.12.3. Let R be a ring. The function $\mu\colon R \times R$ given by $\mu(r, s) = rs$ is the prototype of an R-biadditive function.

Definition 3.12.4. Let R be a ring. Let M be a right R-module and let N be a left R-module. A *tensor product* of M and N over R is an abelian group $M \otimes_R N$ equipped with an R-biadditive function $h\colon M \times N \to M \otimes_R N$ satisfying the following universal property: For every abelian group G and every R-biadditive function $f\colon M \times N \to G$, there exists a unique abelian group homomorphism

$F\colon M \otimes_R N \to G$ making the following diagram commute

$$\begin{tikzcd}
M \times N \arrow[r, "h"] \arrow[dr, "f"'] & M \otimes_R N \arrow[d, dashed, "\exists! F"] \\
& G.
\end{tikzcd}$$

Theorem 3.12.5. *Let R be a ring. Let M be a right R-module and let N be a left R-module. Then $M \otimes_R N$ exists.*

Proof. Existence. Consider $\mathbb{Z}^{(M\times N)}$, the free abelian group with basis $M\times N$. For $m \in M$ and $n \in N$, let $(m,n) \in \mathbb{Z}^{(M\times N)}$ denote the corresponding basis vector. Let $\epsilon\colon M \times N \to \mathbb{Z}^{(M\times N)}$ be the function $\epsilon(m,n) = (m,n)$. Set

$$H = \left(\begin{array}{c|c} (m+m',n)-(m,n)-(m',n) & m,m' \in M \\ (m,n+n')-(m,n)-(m,n') & n,n' \in N \\ (mr,n)-(m,rn) & r \in R \end{array} \right) \mathbb{Z} \subseteq \mathbb{Z}^{(M\times N)}.$$

Set $M \otimes_R N = \mathbb{Z}^{(M\times N)}/H$ and, for $m \in M$ and $n \in N$ write

$$m \otimes n = [(m,n)] = (m,n) + H \in \mathbb{Z}^{(M\times N)}/H = M \otimes_R N.$$

Define $h\colon M \times N \to M \otimes_R N$ to be the composition

$$M \times N \xrightarrow{\varepsilon} \mathbb{Z}^{(M\times N)} \xrightarrow{\pi} \mathbb{Z}^{(M\times N)}/H = M \otimes_R N$$

that is, by the rule $h(m,n) = m \otimes n$.

It is straightforward to show that h is well-defined and R-biadditive. For example, we have

$$\begin{aligned} h(m+m',n) &= (m+m') \otimes n \\ &= [(m+m',n)] \\ &= [(m,n)] + [(m',n)] \\ &= m \otimes n + m' \otimes n \\ &= h(m,n) + h(m',n). \end{aligned}$$

In terms of tensors, the R-biadditivity of h reads as

$$\begin{gathered} (m+m') \otimes n = m \otimes n + m' \otimes n \\ m \otimes (n+n') = m \otimes n + m \otimes n' \\ (mr) \otimes n = m \otimes (rn) \end{gathered}$$

Note also that elements of $M \otimes_R N$ are of the form

$$[\textstyle\sum_i l_i(m_i,n_i)] = \sum_i l_i[(m_i,n_i)] = \sum_i l_i(m_i \otimes n_i).$$

We'll see later that, usually, there are elements of $M \otimes_R N$ that cannot be written as "simple tensors", that is, are not of the form $m \otimes n$.

To see that $M \otimes_R N$ satisfies the desired universal property, let G be an abelian group and $f\colon M \times N \to G$ an R-biadditive function. Use the universal property for free modules Proposition 3.5.9 to see that there is a unique abelian group homomorphism $F_1\colon \mathbb{Z}^{(M\times N)} \to G$ such that $F_1(m,n) = f(m,n)$.

$$\begin{tikzcd}
M \times N \arrow[r, "\varepsilon"] \arrow[dr, "f"'] & \mathbb{Z}^{(M\times N)} \arrow[d, dashed, "\exists! F_1"] \\
& G.
\end{tikzcd}$$

From the proof of Proposition 3.5.9, we have

$$F_1(\textstyle\sum_i l_i(m_i,n_i)) = \sum_i l_i f(m_i,n_i)).$$

Use this formula to check that each generator of H is in $\operatorname{Ker}(F_1)$; this will use the R-biadditivity of f. It follows that $H \subseteq \operatorname{Ker}(F_1)$ and so the universal property for quotients Proposition 3.3.11 implies that there exists a unique abelian group homomorphism $F\colon \mathbb{Z}^{(M\times N)}/H \to G$ making the right-hand triangle in the next diagram commute

$$\begin{tikzcd}
M \times N \arrow[r, "\varepsilon"] \arrow[dr, "f"'] & \mathbb{Z}^{(M\times N)} \arrow[r, "\pi"] \arrow[d, dashed, "\exists! F_1"] & \mathbb{Z}^{(M\times N)}/H \arrow[r, equal] \arrow[dl, dashed, "\exists! F"] & M \otimes_R N \\
& G. & &
\end{tikzcd}$$

Thus, we see that the desired homomorphism F exists and is unique.

The above construction shows that F is given by the formula

$$F(\textstyle\sum_i l_i(m_i\otimes n_i)) = F([\sum_i l_i(m_i,n_i)]) = F_1(\sum_i l_i(m_i,n_i)) = \sum_i l_i f(m_i,n_i)).$$

□

Example 3.12.6. Let R be a ring. Let M be a right R-module and let N be a left R-module. The computations in the proof of Theorem 3.12.5 show

$$(\textstyle\sum_i m_i r_i)\otimes n = \sum_i (m_i r_i)\otimes n = \sum_i m_i \otimes (r_i n)$$

for all $m_i \in M$, all $r_i \in R$ and all $n \in N$. Other formulas hold similarly. In particular, for $l_i \in \mathbb{Z}$, we have

$$\textstyle\sum_i l_i(m_i\otimes n_i) = \sum_i ((l_i m_i)\otimes n_i) = \sum_i m_i' \otimes n_i$$

where $m_i' = l_i m_i$.

The additive identity in $M \otimes_R N$ is $0_{M\otimes N} = 0_M \otimes 0_N$. This can be written several (seemingly) different ways. For instance, for each $n \in N$, we have

$$0_M \otimes n = (0_M 0_R)\otimes n = 0_M \otimes (0_R n) = 0_M \otimes 0_N.$$

Similarly, for all $m \in M$, we have $m \otimes 0_N = 0_M \otimes 0_N$.

Remark 3.12.7. Let R be a ring. Let M be a right R-module and let N be a left R-module. It should be reiterated that there are more elements in $M \otimes_R N$ than the simple tensors $m\otimes n$. General elements of $M\otimes_R N$ are of the form $\sum_i m_i \otimes n_i$, as was shown in Example 3.12.6. However, certain properties of $M \otimes_R N$ are determined by their restrictions to the simple tensors, as we see in Lemma 3.12.8.

Lemma 3.12.8. *Let R be a ring. Let M be a right R-module and let N be a left R-module. Let $\gamma, \delta\colon M \otimes_R N \to G$ be a abelian group homomorphisms.*

(a) *$M \otimes_R N = 0$ if and only if $m \otimes n = 0$ for all $m \in M$ and all $n \in N$.*
(b) *$\gamma = \delta$ if and only if $\gamma(m\otimes n) = \delta(m\otimes n)$ for all $m \in M$ and all $n \in N$.*

(c) *If* $G = M \otimes_R N$*, then* $\gamma = \mathrm{id}_{M\otimes_R N}$ *if and only if* $\gamma(m \otimes n) = m \otimes n$ *for all* $m \in M$ *and all* $n \in N$*.*
(d) $\gamma = 0$ *if and only if* $\gamma(m \otimes n) = 0$ *for all* $m \in M$ *and all* $n \in N$*.*

Proof. Part (a) follows from the fact that every element of $M \otimes_R N$ is of the form $\sum_i m_i \otimes n_i = \sum_i 0 = 0$.

Part (b) can be proved similarly, or by using the uniqueness statement in the universal property.

Part (c) can be proved similarly, or by using the uniqueness statement in the universal property, or as the special case $\delta = \mathrm{id}_{M\otimes_R N}$ of part (b).

Part (d) can be proved similarly, or by using the uniqueness statement in the universal property, or as the special case $\delta = 0$ of part (b). □

When proving properties about tensor products, we very rarely use the construction. Usually, we use the universal property, as in the following result.

Theorem 3.12.9. *Let* R *be a ring. Let* M *be a right* R*-module and let* N *be a left* R*-module. Then* $M \otimes_R N$ *is unique up to abelian group isomorphism.*

Proof. Assume that $h\colon M \times N \to M \otimes_R N$ and $k\colon M \times N \to M \odot_R N$ both satisfy the defining property for the tensor product, that is: $M \otimes_R N$ and $M \odot_R N$ are abelian groups, the functions h and k are R-biadditive, and for every abelian group G and every R-biadditive function $f\colon M \times N \to G$, there exists a unique abelian group homomorphism $F\colon M \otimes_R N \to G$ and $H\colon M \odot_R N \to G$ making the following diagrams commute

$$\begin{tikzcd}
M \times N \arrow[r, "h"] \arrow[dr, "f"'] & M \otimes_R N \arrow[d, dashed, "\exists! F"] & & M \times N \arrow[r, "k"] \arrow[dr, "f"'] & M \odot_R N \arrow[d, dashed, "\exists! H"] \\
& G & & & G.
\end{tikzcd}$$

Apply the universal property for $M \otimes_R N$ to the map $k\colon M \times N \to M \odot_R N$ to find an abelian group homomorphism $\phi\colon M \otimes N \to M \odot_R N$ making the following diagram commute

$$\begin{tikzcd}
M \times N \arrow[r, "h"] \arrow[dr, "k"'] & M \otimes_R N \arrow[d, dashed, "\exists! \phi"] \\
& M \odot_R N.
\end{tikzcd}$$

Apply the universal property for $M \odot_R N$ to the map $h\colon M \times N \to M \otimes_R N$ to find an abelian group homomorphism $\psi\colon M \otimes N \to M \odot_R N$ making the following diagram commute

$$\begin{tikzcd}
M \times N \arrow[r, "k"] \arrow[dr, "h"'] & M \odot_R N \arrow[d, dashed, "\exists! \psi"] \\
& M \otimes_R N.
\end{tikzcd}$$

It follows that the next diagrams commute

$$\begin{tikzcd}
M \times N \arrow[r, "h"] \arrow[dr, "h"'] & M \otimes_R N \arrow[d, "\psi\phi"] \\
& M \otimes_R N
\end{tikzcd}
\qquad
\begin{tikzcd}
M \times N \arrow[r, "h"] \arrow[dr, "h"'] & M \otimes_R N \arrow[d, "\mathrm{id}_{M \otimes_R N}"] \\
& M \otimes_R N.
\end{tikzcd}$$

Hence, the uniqueness statement in the universal property implies that $\psi\phi = \mathrm{id}_{M\otimes_R N}$. A similar argument shows that $\phi\psi = \mathrm{id}_{M\odot_R N}$ and so ϕ and ψ are inverse isomorphisms, as desired. □

Proposition 3.12.10. *Let R be a ring with identity. Let M be a unital right R-module and let N be a unital left R-module. There are abelian group isomorphisms*

$$F\colon M \otimes_R R \xrightarrow{\cong} M \qquad \textit{and} \qquad G\colon R \otimes_R N \xrightarrow{\cong} N$$

such that $F(m \otimes r) = mr$ and $G(r \otimes n) = rn$. In particular, we have $M \otimes_R R \cong M$ and $R \otimes_R N \cong N$ and $R \otimes_R R \cong R$.

Proof. We will verify the claim for $M \otimes_R R$. The map $f\colon M \times R \to M$ given by $f(m, r) = mr$ is R-biadditive. Hence, the universal property yields a unique R-module homomorphism $F\colon M \otimes_R R \to M$ such that $F(m \otimes r) = mr$ for all $m \in M$ and $r \in R$. We will show that F is bijective. The main point is the following computation in $M \otimes_R R$

$$\textstyle\sum_i (m_i \otimes r_i) = \sum_i ((m_i r_i) \otimes 1) = (\sum_i m_i r_i) \otimes 1$$

which shows that every element of $M \otimes_R R$ is of the form $m \otimes 1$.

F is surjective: $m = F(m \otimes 1)$.

F is injective: $0 = F(m \otimes 1)$ implies $0 = F(m \otimes 1) = m \cdot 1 = m$ implies $0 = 0 \otimes 1 = m \otimes 1$. □

Remark 3.12.11. Note that we have not shown that the isomorphisms in Proposition 3.12.10 are R-module isomorphisms. This is because we have not shown, for instance, that $M \otimes_R R$ has an R-module structure. However, because R is also a right R-module (technically, it is an "RR-bimodule") it follows that $M \otimes_R R$ has a right R-module structure given by $(m \otimes r)r' = m \otimes (rr')$. Furthermore, this structure makes the isomorphism F into a homomorphism of right R-modules.

We will address this in the case when R is commutative in the exercises.

Remark 3.12.12. It should be noted that other tensor products of R with itself, like $R \otimes_{\mathbb{Z}} R$ are not usually so simple. In fact, even when R is noetherian, the ring $R \otimes_{\mathbb{Z}} R$ is often not noetherian.

Here is the functoriality of tensor product.

Proposition 3.12.13. *Let R be a ring. Let $\alpha\colon M \to M'$ and $\alpha'\colon M' \to M''$ be homomorphisms of right R-modules. Let $\beta\colon N \to N'$ and $\beta'\colon N' \to N''$ be homomorphisms of left R-modules.*

(a) *There exists a unique abelian group homomorphism $\alpha \otimes_R \beta\colon M \otimes_R N \to M' \otimes_R N'$ such that $(\alpha \otimes_R \beta)(m \otimes n) = \alpha(m) \otimes_R \beta(n)$ for all $m \in M$ and all $n \in N$.*

(b) *The following diagram commutes*

$$\begin{tikzcd}
M \otimes_R N \arrow[r, "\alpha\otimes_R\beta"] \arrow[dr, "(\alpha'\alpha)\otimes_R(\beta'\beta)"'] & M' \otimes_R N' \arrow[d, "\alpha'\otimes_R\beta'"] \\
& M'' \otimes_R N''
\end{tikzcd}$$

In other words, we have $(\alpha' \otimes_R \beta')(\alpha \otimes_R \beta) = (\alpha'\alpha) \otimes_R (\beta'\beta)$.

Proof. (a) We use the universal property. Define $f\colon M \times N \to M' \otimes_R N'$ by the formula $f(m,n) = \alpha(m) \otimes \beta(n)$. In other words, f is the composition $M \times N \xrightarrow{\alpha\times\beta} M' \times N' \xrightarrow{h'} M' \otimes_R N'$ where h' is the appropriate universal biadditive map. Since α and β are R-module homomorphisms, it is straightforward to show that f is R-biadditive. The universal property yields a unique abelian group homomorphism $\alpha \otimes_R \beta\colon M \otimes_R N \to M' \otimes_R N'$ such that

$$(\alpha \otimes_R \beta)(m \otimes n) = f(m,n) = \alpha(m) \otimes_R \beta(n)$$

for all $m \in M$ and all $n \in N$.

(b) By definition, we have

$$\begin{aligned}
(\alpha' \otimes_R \beta')((\alpha \otimes_R \beta)(m \otimes n)) &= (\alpha' \otimes_R \beta')(\alpha(m) \otimes_R \beta(n)) \\
&= \alpha'(\alpha(m)) \otimes_R \beta'(\beta(n)) \\
&= (\alpha'\alpha) \otimes_R (\beta'\beta)(m \otimes n).
\end{aligned}$$

Now apply Lemma 3.12.8(b). □

Notation 3.12.14. Continue with the notation of Proposition 3.12.13. We write

$$M \otimes_R \beta = \mathrm{id}_M \otimes_R \beta\colon M \otimes_R N \to M \otimes_R N'$$
$$\alpha \otimes_R N = \alpha \otimes_R \mathrm{id}_N\colon M \otimes_R N \to M' \otimes_R N.$$

Remark 3.12.15. Let R be a ring. Let M be a right R-module and let N be a left R-module. It is straightforward to show that $\mathrm{id}_M \otimes_R N = \mathrm{id}_{M\otimes_R N}\colon M \otimes_R N \to M \otimes_R N$. Proposition 3.12.13(b) then shows that $M \otimes_R -$ and $- \otimes_R N$ respect compositions.

Next, we go for exactness properties.

Proposition 3.12.16. *Let* $f\colon M \to M'$ *be an epimorphism of right* R*-modules, and let* $g\colon N \to N'$ *be an epimorphism of left* R*-modules*

(a) *The map* $f \otimes_R g\colon M \otimes_R N \to M' \otimes_R N'$ *is surjective.*

(b) $\mathrm{Ker}(f \otimes_R g)$ *is generated as an abelian group by the set*

$$L = \{m \otimes n \in M \otimes_R N \mid f(m) = 0 \text{ or } g(n) = 0\} \subseteq M \otimes_R N.$$

Proof. (a) We compute directly: For an arbitrary element $\sum_i m_i' \otimes n_i' \in M' \otimes_R N'$, we have

$$\textstyle\sum_i m_i' \otimes n_i' = \sum_i f(m_i) \otimes g(n_i) = (f \otimes_R g)(\sum_i m_i \otimes n_i).$$

(b) Let K denote the subgroup of $M \otimes_R N$ generated by the set L. Each generator of K is in $\mathrm{Ker}(f \otimes_R g)$, and so $K \subseteq \mathrm{Ker}(f \otimes_R g)$. Hence, we have a well-defined abelian group epimorphism $\phi\colon (M \otimes_R N)/K \to M' \otimes_R N'$ such that $\phi(\overline{m \otimes n}) = f(m) \otimes g(n)$. To show that $K = \mathrm{Ker}(f \otimes_R g)$, it suffices to show that ϕ is injective.

Define a map $h\colon M'\times_R N'\to(M\otimes_R N)/K$ as follows: for $(m',n')\in M'\times_R N'$, fix $m\in M$ and $n\in N$ such that $f(m)=m'$ and $g(n)=n'$, and set $h(m',n')=\overline{m\otimes n}$. We need to show this is well-defined. Assume $f(m_1)=m'=f(m)$ and $g(n_1)=n'=g(n)$. Then $m_1-m\in\operatorname{Ker}(f)$ and $n_1-n\in\operatorname{Ker}(g)$ and so in $M\otimes_R N$ we have

$$\begin{aligned} m_1\otimes n_1 &= (m_1-m)\otimes(n_1-n)\\ &= \underbrace{(m_1-m)\otimes(n_1-n)+(m_1-m)\otimes n+m\otimes(n_1-n)}_{\in K}+m\otimes n. \end{aligned}$$

It follows that, in $(M\otimes_R N)/K$, we have $\overline{m_1\otimes n_1}=\overline{m\otimes n}$ and so h is well-defined.

We check that h is R-biadditive. For instance, we want $h(m_1'+m_2',n')=h(m_1',n')+h(m_2',n')$. Fix $m_1,m_2\in M$ and $n\in N$ such that $f(m_1)=m_1'$, $f(m_2)=m_2'$ and $g(n)=n'$. Then $f(m_1+m_2)=m_1'+m_2'$ and so

$$h(m_1'+m_2',n')=\overline{(m_1+m_2)\otimes n}=\overline{m_1\otimes n}+\overline{m_2\otimes n}=h(m_1',n')+h(m_2',n').$$

The other conditions are verified similarly.

Since h is R-biadditive, the universal property for tensor products yields a well-defined abelian group homomorphism $H\colon M'\otimes_R N'\to(M\otimes_R N)/K$ such that $H(m'\otimes n')=h(m',n')$ for all $m'\in M'$ and all $n'\in N'$. In other words,

$$H(m'\otimes n')=\overline{m\otimes n}$$

where $m\in M$ and $n\in N$ are such that $f(m)=m'$ and $g(n)=n'$. It follows readily that the composition $H\phi\colon(M\otimes_R N)/K\to(M\otimes_R N)/K$ is $\mathrm{id}_{(M\otimes_R N)/K}$, and so ϕ is injective as desired. □

Here is the right-exactness of the tensor product.

Proposition 3.12.17. *Let R be a ring, M a right R-module and N a left R-module.*

(a) *For each an exact sequence of left R-modules $N'\xrightarrow{g'}N\xrightarrow{g}N''\to 0$ the associated sequence of abelian groups*

$$M\otimes_R N'\xrightarrow{M\otimes_R g'}M\otimes_R N\xrightarrow{M\otimes_R g}M\otimes_R N''\to 0$$

is exact.

(b) *For each an exact sequence of right R-modules $M'\xrightarrow{f'}M\xrightarrow{f}M''\to 0$ the associated sequence of abelian groups*

$$M'\otimes_R N\xrightarrow{f'\otimes_R N}M\otimes_R N\xrightarrow{f\otimes_R N}M''\otimes_R N\to 0$$

is exact.

Proof. (a) Because g is surjective, Proposition 3.12.16(a) implies that $M\otimes_R g$ is surjective. Also, we have

$$(M\otimes_R g)(M\otimes_R g')=M\otimes_R(gg')=M\otimes_R 0=0$$

and so $\operatorname{Im}(M\otimes_R g')\subseteq\operatorname{Ker}(M\otimes_R g)$. To show $\operatorname{Im}(M\otimes_R g')\supseteq\operatorname{Ker}(M\otimes_R g)$, it suffices to show that every generator of $\operatorname{Ker}(M\otimes_R g)$ is in $\operatorname{Im}(M\otimes_R g')$. By Proposition 3.12.16(b), $\operatorname{Ker}(M\otimes_R g)$ is generated by $\{m\otimes n\mid g(n)=0\}$. For each $m\otimes n\in M\otimes_R N$ such that $g(n)=0$, there exists $n'\in N'$ such that $g'(n')=n$ and so $m\otimes n=(M\otimes_R g')(m\otimes n')\in\operatorname{Im}(M\otimes_R g')$.

Part (b) is similar. □

In general, the tensor product is not left exact.

Example 3.12.18. Let $\mu\colon \mathbb{Z} \to \mathbb{Z}$ be the monomorphism given by $n \mapsto 2n$. It is straightforward to show that the following diagram commutes

$$\begin{tikzcd}
(\mathbb{Z}/2\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z} \arrow[r, "F", "\cong"'] \arrow[d, "(\mathbb{Z}/2\mathbb{Z})\otimes\mu"'] & \mathbb{Z}/2\mathbb{Z} \arrow[d, "\overline{\mu}"] \\
(\mathbb{Z}/2\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z} \arrow[r, "F", "\cong"'] & \mathbb{Z}/2\mathbb{Z}
\end{tikzcd}$$

where $\overline{\mu}(\overline{n}) = \overline{\mu(n)} = \overline{2n} = 0$. It follows that $\mu_2^{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathrm{id}_{\mathbb{Z}/2\mathbb{Z}} = 0$. This map is not injective because $(\mathbb{Z}/2\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$.

Definition 3.12.19. Let R be a ring. A right R-module M is *flat* if the functor $M \otimes_R -$ is exact. A left R-module N is *flat* if $- \otimes_R N$ transforms arbitrary exact sequences into exact sequences.

Example 3.12.20. Let R be a ring with identity. Then R is flat as a left R-module and as a right R-module. More generally any projective R-module is flat.

3.13. Localization

Localization generalizes the construction of the field of fractions of an integral domain. It will also give us examples of flat R-modules that are not projective.

Definition 3.13.1. Let R be a commutative ring with identity. A subset $S \subseteq R$ is *multiplicatively closed* if $1 \in S$ and $ss' \in S$ for all $s, s' \in S$.

Here are the prototypical examples of multiplicatively closed subsets.

Example 3.13.2. Let R be a commutative ring with identity. For each $s \in R$, the set $\{1, s, s^2, \ldots\} \subseteq R$ is multiplicatively closed. For each prime ideal $\mathfrak{p} \subset R$, the set $R \smallsetminus \mathfrak{p} \subset R$ is multiplicatively closed. For instance, if R is an integral domain, then the set of non-zero elements of R is multiplicatively closed.

Construction 3.13.3. Let R be a commutative ring with identity, and let $S \subseteq R$ be multiplicatively closed. Define a relation $\sim$ on $R \times S$ as follows: $(r, s) \sim (r', s')$ if there exists $s'' \in S$ such that $s''(rs' - r's) = 0$. Check that this is an equivalence relation on $R \times S$.

The *localization* $S^{-1}R$ is then the set of all equivalence classes under this relation $S^{-1}R = (R \times S)/\sim$ where the equivalence class of (r, s) in $S^{-1}R$ is denoted r/s or $\frac{r}{s}$. If $t \in S$, then the definition implies $(r, s) \sim (rt, st)$; this translates to the cancellation formula $\frac{rt}{st} = \frac{r}{s}$.

For elements $r/s, t/u \in S^{-1}R$, set

$$\frac{r}{s} + \frac{t}{u} = \frac{ru + ts}{su} \qquad \text{and} \qquad \frac{r}{s}\frac{t}{u} = \frac{rt}{su}.$$

When $\mathfrak{p} \subset R$ is a prime ideal and $S = R \smallsetminus \mathfrak{p}$, we write $R_{\mathfrak{p}}$ in lieu of $S^{-1}R$.

Example 3.13.4. Let R be an integral domain, and set $S = \{r \in R \mid r \neq 0\}$. Then $S^{-1}R$ is the quotient field of R.

Proposition 3.13.5. *Let R be a commutative ring with identity, and let $S \subseteq R$ be multiplicatively closed.*

(a) *$S^{-1}R$ is a commutative ring with identity, with $0_{S^{-1}R} = 0_R/1_R = 0/s$ and $1_{S^{-1}R} = 1_R/1_R = s/s$ for all $s \in S$.*

(b) *The assignment $f\colon R \to S^{-1}R$ given by $r \mapsto r/1$ is a homomorphism of rings with identity.*

Proof. Argue as in the proof of Proposition 2.4.2. The main point is to show that the addition and multiplication on $S^{-1}R$ are well-defined; the other ring-axioms are then easily verified. Assume that $r/s = r'/s'$ and $t/u = t'/u'$, that is, $s''(rs' - r's) = 0 = u''(tu' - t'u)$ for some $s'', u'' \in S$. Then

$$\begin{aligned}\frac{ru+ts}{su} &= \frac{(ru+ts)s's''u'u''}{(su)s's''u'u''} = \frac{rs's''uu'u'' + tu'u''ss's''}{ss's''uu'u''}\\ &= \frac{r'ss''uu'u'' + t'uu''ss's''}{ss's''uu'u''} = \frac{(r'u'+t's)ss''uu''}{(s'u')ss''uu''} = \frac{r'u'+t's}{s'u'}\end{aligned}$$

so addition is well-defined. The equality $\frac{rt}{su} = \frac{r't'}{s'u'}$ is even easier to verify, showing that multiplication is well-defined. □

Construction 3.13.6. Let R be a commutative ring with identity, and let $S \subseteq R$ be multiplicatively closed. Let M be a unital R-module. Define a relation $\sim$ on $M \times S$ as follows: $(m, s) \sim (m', s')$ if there exists $s'' \in S$ such that $s''(ms' - m's) = 0$. Check that this is an equivalence relation on $M \times S$.

The *localization* $S^{-1}M$ is then the set of all equivalence classes under this relation $S^{-1}M = (M \times S)/\sim$ where the equivalence class of (m, s) in $S^{-1}M$ is denoted m/s or $\frac{m}{s}$. If $t \in S$, then the definition implies $(m, s) \sim (tm, ts)$; this translates to the cancellation formula $\frac{tm}{ts} = \frac{m}{s}$.

For elements $m/s, n/u \in S^{-1}M$ and $r/v \in S^{-1}R$, set

$$\frac{m}{s} + \frac{n}{u} = \frac{um+sn}{su} \qquad \text{and} \qquad \frac{r}{v}\frac{m}{s} = \frac{rm}{vs}.$$

When $\mathfrak{p} \subset R$ is a prime ideal and $S = R \smallsetminus \mathfrak{p}$, we write $M_{\mathfrak{p}}$ in lieu of $S^{-1}M$.

Proposition 3.13.7. *Let R be a commutative ring with identity, and let $S \subseteq R$ be multiplicatively closed. Let $f\colon M \to N$ be a homomorphism of unital R-modules.*

(a) *$S^{-1}M$ is a unital $S^{-1}R$-module, with $0_{S^{-1}M} = 0_M/1_R = 0_M/s$ for all $s \in S$.*

(b) *$S^{-1}M$ is a unital R-module, with action $r(m/s) = (rm)/s$.*

(c) *The assignment $g_M\colon M \to S^{-1}M$ given by $m \mapsto m/1$ is a homomorphism of unital R-modules.*

(d) *The assignment $S^{-1}f\colon S^{-1}M \to S^{-1}N$ given by $m/s \mapsto f(m)/s$ is a homomorphism of unital $S^{-1}R$-modules making the following diagram commute*

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "g_M"'] & N \arrow[d, "g_N"] \\ S^{-1}M \arrow[r, "S^{-1}f"] & S^{-1}N. \end{tikzcd}$$

(e) *The operator $S^{-1}(-)$ respects compositions and transforms arbitrary exact sequences of R-module homomorphisms into exact sequences of $S^{-1}R$-module homomorphisms.*

Proof. Parts (a) and (b) are proved as in Proposition 3.13.5. Most of the remaining parts are exercises in applying the definitions. We explain the well-definedness of $S^{-1}f$ and the exactness of $S^{-1}(-)$.

To see that $S^{-1}f$ is well-defined, let $m/s = n/t \in S^{-1}M$. Then there exists $u \in S$ such that $utm = usn$, and so

$$utf(m) = f(utm) = f(usn) = usf(n).$$

It follows that

$$\frac{f(m)}{s} = \frac{utf(m)}{uts} = \frac{usf(n)}{ust} = \frac{f(n)}{t}$$

in $S^{-1}N$, as desired.

To see that $S^{-1}(-)$ is exact, consider an exact sequence of R-modules

$$M \xrightarrow{f} N \xrightarrow{g} L.$$

We need to show that the sequence

$$S^{-1}M \xrightarrow{S^{-1}f} S^{-1}N \xrightarrow{S^{-1}g} S^{-1}L$$

is exact. The functoriality of $S^{-1}(-)$ implies

$$(S^{-1}g) \circ (S^{-1}f) = S^{-1}(g \circ f) = S^{-1}(0) = 0$$

and so $\operatorname{Im}(S^{-1}f) \subseteq \operatorname{Ker}(S^{-1}g)$. For the reverse containment, let $n/s \in \operatorname{Ker}(S^{-1}g)$. Then

$$0/1 = 0 = (S^{-1}g)(n/s) = g(n)/s$$

so there exists $t \in S$ such that

$$g(tn) = tg(n) = ts0 = 0.$$

The exactness of the original sequence yields an element $m \in M$ such that $f(m) = tn$. It follows that

$$n/s = tn/ts = f(m)/ts = (S^{-1}f)(m/ts) \in \operatorname{Im}(S^{-1}f)$$

as desired. □

Proposition 3.13.8. *Let R be a commutative ring with identity, and let $S \subseteq R$ be multiplicatively closed. Let M be a unital R-modules.*

(a) *Every element of $(S^{-1}R) \otimes_R M$ is of the form $\frac{r}{s} \otimes m$ for some $r \in R$ and $s \in S$ and $m \in M$.*

(b) *Given an R-module homomorphism $g \colon M \to M'$ there is a commutative diagram of abelian group homomorphisms*

$$\begin{tikzcd}
(S^{-1}R) \otimes_R M \arrow[r, "(S^{-1}R)\otimes g"] \arrow[d, "F", "\cong"'] & (S^{-1}R) \otimes_R M' \arrow[d, "F'", "\cong"'] \\
S^{-1}M \arrow[r, "S^{-1}g"] & S^{-1}M'
\end{tikzcd}$$

where $F((r/s) \otimes m) = (rm)/s$ and $F'((r/s) \otimes m') = (rm')/s$.

(c) *$S^{-1}R$ is a flat R-module.*

Proof. (a) Fix an element $\sum_i \frac{r_i}{u_i} \otimes m_i \in (S^{-1}R) \otimes_R M$. Set $u = \prod_i u_i$ and $u_i' = \prod_{j \neq i} u_j$. Then $u = u_i' u_i$ and so

$$\textstyle\sum_i \frac{r_i}{u_i} \otimes m_i = \sum_i \frac{u_i' r_i}{u_i' u_i} \otimes m_i = \sum_i \frac{1}{u} \otimes (u_i' r_i m_i) = \frac{1}{u} \otimes \left(\sum_i u_i' r_i m_i\right).$$

(b) The universal mapping property for tensor products shows that the map $F \colon S^{-1}R \otimes_R M \to S^{-1}M$ given by $F\bigl(\frac{r}{u} \otimes m\bigr) = \frac{rm}{u}$ is a well-defined abelian group homomorphism. The map F is surjective: $\frac{m}{u} = F\big(\frac{1}{u} \otimes m\big)$. To see that F is injective, fix $\xi \in \operatorname{Ker}(F)$. Part (a) implies that $\xi = \frac{r}{u} \otimes m$ for some $r \in R$ and $u \in S$ and $m \in M$. Then $0 = F\big(\frac{r}{u} \otimes m\big) = \frac{rm}{u}$ implies that there exists an element $u' \in S$ such that $u'rm = 0$. Hence, we have

$$\tfrac{r}{u} \otimes m = \tfrac{ru'}{uu'} \otimes m = \tfrac{1}{uu'} \otimes (ru'm) = \tfrac{1}{uu'} \otimes (0) = 0.$$

To show that the isomorphism is natural, let $g\colon M \to M'$ be an R-module homomorphism. We need to show that the following diagram commutes:

$$\begin{tikzcd}
(S^{-1}R) \otimes_R M \arrow[r, "(S^{-1}R)\otimes g"] \arrow[d, "\cong"', "F"] & (S^{-1}R) \otimes_R M' \arrow[d, "\cong"', "F'"] \\
S^{-1}M \arrow[r, "S^{-1}g"] & S^{-1}M'
\end{tikzcd}$$

where the vertical maps are the isomorphisms from the previous paragraph. We have $S^{-1}g\big(\frac{m}{u}\big) = \frac{g(m)}{u}$, and so

$$\begin{aligned}
F'(((S^{-1}R) \otimes_R g)(\tfrac{r}{u} \otimes m)) &= F'(\tfrac{r}{u} \otimes g(m)) \\
&= \tfrac{rg(m)}{u} \\
&= \tfrac{g(rm)}{u} \\
&= (S^{-1}g)(\tfrac{rm}{u}) \\
&= (S^{-1}g)(F(\tfrac{r}{u} \otimes m)).
\end{aligned}$$

(c) The functor $S^{-1}(-) \cong (S^{-1}R) \otimes_R -$ is exact by Proposition 3.13.7(e), and so $S^{-1}R$ is flat by definition. □