NOTES ON ALGEBRA

Marc Culler - Fall 2004

1. Rings

Definition 1.1. A *ring* R is a set together with two binary operations $+\colon R \times R \to R$, and $\cdot\colon R \times R \to R$ such that

R1 $(R, +)$ is an abelian group (whose identity element is denoted by 0);

R2 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$;

R3 $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ for all $a, b, c \in R$;

RU there exists an element $1 \in R$ such that $0 \neq 1$ and $1 \cdot a = a = a \cdot 1$ for all $a \in R$.

A *subring* of R is a subset which contains 1 and is closed under both operations.

The multiplication operator $\cdot$ will usually be omitted, and the usual rules for operator precedence will be assumed, so that $ab + cd \doteq (ab) + (cd)$.

Definition 1.2. A *homomorphism* from a ring R to a ring S is a function $\phi : R \to S$ such that

$$\phi(a + b) = \phi(a) + \phi(b)$$
$$\phi(ab) = \phi(a)\phi(b)$$

for all $a, b \in R$. The *kernel* of ϕ is $\ker \phi = \{a \in R \mid \phi(a) = 0\}$. A bijective homomorphism is an *isomorphism*.

2. Modules

Definition 2.1. Let R be a ring. A *left R-module* is an abelian group $(M, +)$ together with an *R-action* $\cdot\colon R \times M \to M$ which satisfies

M1 $1 \cdot m = m$ for all $m \in M$;

M2 $r(s \cdot m) = (rs) \cdot m$ for all $r, s \in R$ and $m \in M$;

M3 $r \cdot (m + n) = (r \cdot m) + (s \cdot n)$

A *submodule* N of M is a subset which is closed under $+$ and satisfies $r \cdot n \in N$ for all $r \in R$ and $n \in N$. A right R-module is defined similarly, but modules will be assumed to

Date: September 2, 2005.

be left modules when no side is specified. It is the readers job to translate definitions and theorems about left R-modules into definitions and theorems about right R-modules.

Exercise 2.1. Show that if M is an R-module then $0 \cdot m = 0$ for all m in M. (The 0 on the left is the additive identity of R, while the one on the right is the identity of M as an abelian group.)

2.2. Any ring R is an R-module, where the R-action is the multiplication operation in R. If S is a subring of R then R is an S-module.

Definition 2.3. A *homomorphism* from an R-module M to an R-module N is a function $\phi\colon M \to N$ such that $\phi(r_1 \cdot m_1 + r_2 \cdot m_2) = r_1 \cdot \phi(m_1) + r_2 \cdot \phi(m_2)$ for all $m_1, m_2 \in M$ and $r_1, r_2 \in R$. As usual, a bijective homomorphism is an *isomorphism*. We define $\ker \phi = \{m \in M \mid \phi(m) = 0\}$ and $\operatorname{im} \phi = \{\phi(m) \mid m \in M\}$.

If R is a ring and $\phi\colon M \to N$ is a homomorphism from an R-module M to an R-module N then $\ker \phi$ is a submodule of M and $\operatorname{im} \phi$ is a submodule of N.

Definition 2.4. Let R be a ring. A (finite or infinite) sequence of R-module homomorphisms

$$\cdots M_2 \xrightarrow[f_1]{} M_1 \xrightarrow[f_0]{} M_0 \cdots$$

is *exact* if $\ker f_i = \operatorname{im} f_{i+1}$ for $i = 0, 1, \ldots$. A *short exact sequence* of R-module homomorphisms is an exact sequence of the form

$$0 \longrightarrow K \longrightarrow M \longrightarrow Q \longrightarrow 0.$$

Exercise 2.2. Let R be a ring and let M be an R-module. Suppose that A is a submodule of M. Let $(M/A, +)$ be the quotient of the abelian groups $(M, +)$ and $(N, +)$. Show that the the R-action $r \cdot (m + A) \doteq (r \cdot m) + A$ is well-defined, and makes M/A into an R-module. Show that the function $\pi : M \to M/A$ defined by $\pi(m) = m + N$ is an R-module homomorphism.

Definition 2.5. Let R be a ring and let M be an R-module. Suppose that N is a submodule of M. The R-module M/N defined in Exercise 2.2 is the *quotient* of M by N and homomorphism $\pi : M \to M/N$ is the *natural surjection*.

3. Direct products and direct sums

In this section proofs will be omitted if they follow from, or are essentially the same as the proofs of corresponding statements about abelian groups.

Theorem 3.1. *(First Isomorphism Theorem) Let R be a ring and let $\phi : M \to N$ be a homomorphism of R-modules. Then the function $x + \ker\phi \mapsto \phi(x)$ is an isomorphism from $R/\ker\phi$ to $\phi(R)$.*

3.2. Let R be a ring and let M be an R-module. If A is a submodule of M then

$$0 \longrightarrow A \xrightarrow[\iota]{} M \xrightarrow[\pi]{} M/A \longrightarrow 0$$

is a short exact sequence, where ι is the inclusion homomorphism and π is the natural surjection. Conversely, if

$$0 \longrightarrow K \xrightarrow[f]{} M \xrightarrow[g]{} Q \longrightarrow 0.$$

is a short exact sequence, then $Q \cong M/f(K)$.

3.3. Let R be a ring. For any positive integer n, we denote by R^n the set of n-tuples of elements of R, with componentwise addition and left R-action:

$$(r_1, \ldots, r_n) + (s_1, \ldots, s_n) = (r_1 + s_1, \ldots, r_n + s_n)$$
$$r(s_1, \ldots, s_n) = (rs_1, \ldots, rs_n)$$

It is clear that R^n is a left R-module.

Definition 3.4. Let R be a ring. If $(M_\alpha)_{\alpha\in I}$ is an indexed family of left R-modules then the direct product $\prod_{\alpha\in I} M_\alpha$ is the abelian group $\prod_{\alpha\in I}(M_\alpha)$ with the left R-action given by $r\cdot(x_\alpha)_{\alpha\in I} = (r\cdot x_\alpha)_{\alpha\in R}$. For each $\beta \in I$ the *projection homomorphism* $\pi_\beta\colon \prod_{\alpha\in I} G_\alpha \to G_\beta$ is defined by $\pi_\beta((x_\alpha)_{\alpha\in I}) = x_\beta$.

It is easily checked that the direct product of any indexed family of R-modules is an R-module.

Proposition 3.5. *Let $(M_\alpha)_{\alpha\in I}$ be an indexed family of left R-modules. The direct product $\prod_{\alpha\in I} M_\alpha$ has the following universal mapping property: if N is an arbitrary R-module and if $\sigma_\alpha\colon N \to M_\alpha$ is a homomorphism for each $\alpha \in I$ then there exists a unique homomorphism $\phi\colon N \to \prod_{\alpha\in I} M_\alpha$ such that $\pi_\alpha \circ \phi = \sigma_\alpha$ for all $\alpha \in I$.*

Definition 3.6. Let R be a ring. If $(M_\alpha)_{\alpha\in I}$ is an indexed family of left R-modules then the direct sum $\bigoplus_{\alpha\in I} M_\alpha$ is the abelian group $\bigoplus_{\alpha\in I}(M_\alpha, +)$ with the R-action it inherits from the direct product. (It is clearly closed under the R-action.) For each $\beta \in I$ the *inclusion homomorphism* $\iota_\beta\colon M_\beta \to \bigoplus_{\alpha\in I} M_\alpha$ sends each element $x \in G_\beta$ to $(x_\alpha)_{\alpha\in I}$ where $x_\beta = x$ and $x_\alpha = 0$ for all $\alpha \neq \beta$.

Proposition 3.7. *Let $(M_\alpha)_{\alpha\in I}$ be an indexed family of left R-modules. The direct sum $\bigoplus_{\alpha\in I} M_\alpha$ has the following universal mapping property: if N is a left R-module and if*

$\nu_\alpha \colon M_\alpha \to N$ is a homomorphism for each $\alpha \in I$ then there exists a unique homomorphism $\phi \colon \bigoplus_{\alpha \in I} M_\alpha \to N$ such that $\phi \circ \iota_\alpha = \nu_\alpha$ for all $\alpha \in I$.

Definition 3.8. Let R be a ring and let M be a left R-module. If $A_1, \ldots, A_n$ are submodules of M then define

$$\sum_{i=1}^{n} A_i \doteq A_1 + \cdots + A_n = \{r_1 x_1 + \cdots + r_n x_n \mid r_i \in R \text{ and } x_i \in A_i \text{ for } i = 1, \ldots, n\}.$$

It is clear that $A_1 + \cdots + A_n$ is the smallest submodule of M containing $A_1, \ldots, A_n$.

Proposition 3.9. *Let R be a ring and let M be a left R-module. If $A_1, \ldots, A_n$ are submodules of M such that $M = A_1 + \ldots + A_n$. and $A_i \cap \sum_{j \neq i} A_j = \{0\}$ for $i = 1, \ldots, n$. Then $G \cong \bigoplus_{i=1}^{n} H_i$.*

Proposition 3.10. *Let R be a ring and let*

$$0 \longrightarrow A \xrightarrow[\alpha]{} M \xrightarrow[\beta]{} B \longrightarrow 0.$$

be a short exact sequence of R-modules. The following are equivalent:

- *there exists a homomorphism $\sigma \colon Q \to M$ such that $g \circ \sigma = \mathrm{id}_Q$;*
- *there exists a homomorphism $\tau \colon M \to K$ such that $\tau \circ f = \mathrm{id}_K$; and*
- *There is an isomorphism $\phi \colon M \to A \oplus B$ such that the following diagram is commutative:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow[\alpha]{} & M & \xrightarrow[\beta]{} & B & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle \phi} & & \| & & \\ 0 & \longrightarrow & A & \xrightarrow[\iota_A]{} & A \oplus B & \xrightarrow[\pi_B]{} & B & \longrightarrow & 0 \end{array}$$

Definition 3.11. Let R be a ring. A short exact sequence of R-modules *splits* if it satisfies the three equivalent conditions in Proposition 3.10.

Exercise 3.1. Prove Proposition 3.10.

Exercise 3.2. Suppose that $R$is a ring and

$$0 \longrightarrow A \xrightarrow[\alpha]{} M \xrightarrow[\beta]{} B \longrightarrow 0.$$

is a short exact sequence of R-modules. Show that if B is free then the sequence splits.

4. Ideals

Definition 4.1. A *left ideal* A in a ring R is a left R-submodule of R. That is, A is closed under addition and

- if $r \in R$ and $a \in A$ then $ra \in A$.

Right ideals are defined similarly, but ideals will be assumed to be left ideals when no side is specified. An ideal is *two-sided* if it is both a left and a right ideal.

4.2. If R is a ring then $\{0\}$ and R are two-sided ideals in R.

The kernel of a ring homomorphism is a two-sided ideal.

If A is an ideal in a ring R then $1 \in A$ if and only if $A = R$.

Exercise 4.1. If R is a ring and if A and B are left (right) ideals in R then

$$A + B \doteq \{a + b \,|\, a \in A \text{ and } b \in B\}$$

is a left (right) ideal in R.

Exercise 4.2. If R is a ring and if $A_1 \subseteq A_2 \subseteq \cdots$ is an ascending chain of left (right) ideals in R, then

$$A = \bigcup_{i=1}^{\infty} A_i$$

is a left (right) ideal in R.

4.3. The *cosets* of a two-sided ideal A in a ring R are the equivalence classes under the equivalence relation given by: $r \sim s$ if $r - s \in A$. (In other words, the cosets of the ideal A are the same as the cosets of A, regarded as a subgroup of the additive group of R.) The coset of A which contains an element r of R is $r + A = \{r + a \,|\, a \in A\}$.

Proposition 4.4. *Let A be a two-sided ideal in a ring R. The following operations on cosets of A are well defined.*

$$(x + A) + (y + A) = (x + y) + A$$
$$(x + A)(y + A) = (xy) + A.$$

Moreover, the set of cosets of A, under these operations, forms a ring.

Exercise 4.3. Prove Proposition 4.4

The ring formed by the cosets of a two-sided ideal A is denoted R/A, and is called the *factor ring* or *quotient ring* of R by A.

Theorem 4.5. *(First Isomorphism Theorem) Let $\phi : R \to S$ be a homomorphism of rings. Then $A = \ker \phi$ is an ideal, $\phi(R)$ is a ring, and the function $x + A \mapsto \phi(x)$ is an isomorphism from R/A to $\phi(R)$.*

Exercise 4.4. Prove the First Isomorphism Theorem for rings.

5. Commutative rings

Definition 5.1. A ring R is *commutative* if $rs = sr$ for all $r, s \in R$.

Exercise 5.1. Show that subrings and factor rings of a commutative ring are commutative, and that every ideal in a commutative ring is two-sided.

Definition 5.2. An element r of a ring R is said to be a *zero divisor* if $r \neq 0$ and if there exists $0 \neq s \in R$ so that $rs = 0$.

Definition 5.3. An *integral domain* is a commutative ring R such that, for any elements $r, s \in R$,

- $rs = 0$ implies $r = 0$ or $s = 0$.

That is, a commutative ring is an integral domain if and only if it contains no zero divisors.

Definition 5.4. If R is a commutative ring and $a \in R$ then $(a) = \{ra \mid s \in R\}$ is an ideal in R, called *the principal ideal generated by a*. We will say that *a divides b* if $b \in (a)$. We write $a|b$ to indicate that a divides b.

Definition 5.5. A *principal ideal domain (or PID)* is an integral domain R such that every ideal in R is a principal ideal.

Definition 5.6. A *field* is a commutative ring F such that every non-zero element of F has a multiplicative inverse.

5.7. A field is an integral domain: if $xy = 0$ and $x \neq 0$ then $y = x^{-1}xy = x^{-1}0 = 0$.

A field F has only two ideals: $(0) = \{0\}$ and $(1) = F$.

5.8. If R is a commutative ring and $a1, \ldots, a_n \in R$ then

$$(a_1, \ldots, a_n) \doteq \{r_1a_1 + \cdots + r_na_n \mid r_1, \ldots, r_n \in R\}$$

is an ideal in R, and equals the intersection of all ideals in R that contain $a_1, \ldots, a_n$.

5.9. If R is a commutative ring, we will denote by $R[x]$ the ring of polynomials in the indeterminant x with coefficients in R. The ring of polynomials with n indeterminants $x_1, \ldots, x_n$ and with coefficients in R will be denoted by $R[x_1, \ldots, x_n]$. Since these are just notes, I feel entitled to skip the formal definitions of these important rings, and refer the reader to the text.

6. Prime and maximal ideals

6.1. Let R be a commutative ring. An ideal $A \subseteq R$ is a *prime ideal* if

- $A \neq R$; and
- $xy \in A \Rightarrow x \in A$ or $y \in A$.

6.2. Let R be a commutative ring. An ideal $A \subseteq R$ is a *maximal ideal* if

- $A \neq R$; and
- if B is an ideal with $A \subseteq B \subsetneq R$ then $A = B$.

Theorem 6.3. *Let R be a commutative ring and let $A \subseteq R$ be an ideal. Then*

- *R/A is an integral domain if and only if A is a prime ideal; and*
- *R/A is a field if and only if A is a maximal ideal.*

Proof. First observe that $1+A$ is a multiplicative identity in R/A, so R/A is a commutative ring. Next observe that $0+A$ is the additive identity in R/A and that $(x+A)(y+A) = 0+A$ if and only if $xy \in A$.

Assume that R/A is an integral domain. Suppose that $(x + A)(y + A) = 0 + A$. Then $xy \in A$. Since R/A is an integral domain, either $x + A = 0 + A$ or $y + A = 0 + A$. Thus either $x \in A$ or $y \in A$. This shows that A is a prime ideal.

Assume that A is a prime ideal. Suppose that $(x + A)(y + A) = 0 + A$. Then $xy \in A$. Since A is a prime ideal, either $x \in A$ or $y \in A$. If $x \in A$ then $x + A = 0 + A$. If $y \in A$ then $y + A = 0 + A$. This shows that R/A is an integral domain.

Assume that R/A is a field. Let B be an ideal with $A \subseteq B \subsetneq R$. Suppose $A \neq B$. Then there is an element $x \in B - A$ and $x + A$ is a non-zero element of R/A. Let $y + A$ be the multiplicative inverse of $x + A$ in R/A. Then $(x + A)(y + A) = (xy) + A = 1 + A$, so $1 = xy + a$ for some $a \in A$. Since $x \in B$ and $a \in A \subseteq B$, we have $1 \in B$, a contradiction since $B \neq R$. This shows that A is maximal.

Assume that A is maximal. Let $x + A$ be a non-zero element of R/A, so $x \notin A$. Let $B = (x)$. Then $A+B$ is an ideal which contains x and A. Since A is maximal, $A+B = R$. Therefore $1 \in A + B$, so $1 = xy + a$ for some $y \in R$ and $a \in A$. This implies that

$1 + A = (xy) + A = (x + A)(y + A)$, so $y + A$ is a multiplicative inverse of $x + A$. This shows that R/A is a field. □

Corollary 6.4. *Suppose R is a commutative ring and A is an ideal in R. If A is maximal then A is prime.*

Proof. A field is an integral domain. (See 5.7.) □

Exercise 6.1. Show that every commutative ring has a maximal ideal. Give an example to show that this would be false without axiom **RU**.

7. Elements and their principal ideals

7.1. Let R be a commutative ring. An element $u \in R$ is a *unit* if u has a multiplicative inverse.

7.2. Let R be a commutative ring. Two elements x and y of R are *associates* if $x = uy$ for some unit $u \in R$. (NOTE: The relation $x \sim y$ *if x and y are associates* is an equivalence relation.)

7.3. Let R be a commutative ring. An element $x \in R$ is *prime* if

- x is not a unit; and
- $x|yz \Rightarrow x|y$ or $x|z$.

7.4. Let R be a commutative ring. An element $x \in R$ is *irreducible* if

- x is not a unit; and
- $x = yz \Rightarrow y$ is a unit or z is a unit.

Proposition 7.5. *Suppose that R is a commutative ring and that $x \in R$. Then*

(1) x is a unit if and only if $(x) = R$;

(2) x is prime if and only if (x) is a prime ideal.

Proof. (1)

$$x \text{ is a unit } \Leftrightarrow \exists y \in R \ni xy = 1 \Leftrightarrow 1 \in (x) \Leftrightarrow (x) = R.$$

(3) ($\Rightarrow$) Suppose x is prime, so $x|yz \Rightarrow x|y$ or $x|z$. We have

$$yz \in (x) \Leftrightarrow x|yz \Rightarrow x|y \text{ or } x|z \Leftrightarrow y \in (x) \text{ or } z \in (x).$$

Since x is not a unit, $(x) \neq R$. Thus (x) is a prime ideal.

($\Leftarrow$) Suppose (x) is a prime ideal, so $yz \in (x) \Rightarrow y \in (x)$ or $z \in (x)$. We have

$$x|yz \Leftrightarrow yz \in (x) \Rightarrow y \in (x) \text{ or } z \in (x) \Leftrightarrow x|y \text{ or } x|z.$$

Since $(x) \neq R$, we know x is not a unit. Thus x is prime. $\square$

8. Integral domains

8.1. Suppose that x, y and z are elements of an integral domain. Then

- $x \neq 0$ and $xy = xz \Rightarrow y = z$.

Proposition 8.2. *Suppose that R is an integral domain and that $x \in R$. If x is prime then x is irreducible.*

Proof. Suppose that x is prime and $x = yz$. Then $x|y$ or $x|z$. If $x|y$ then $y = ux = uyz$ for some element u of R. Canceling y, we have $1 = uz$, so z is a unit. Similarly if $x|z$ then y is a unit. We know that x is not a unit since it is prime. Therefore x is irreducible. $\square$

Proposition 8.3. *Suppose that R is an integral domain and that x and y are elements of R. Then*

(1) x and y are associates if and only if $(x) = (y)$; and

(2) x is irreducible if and only if

$$(x) \subseteq (y) \subsetneq R \Rightarrow (y) = (x).$$

Proof. (1)($\Rightarrow$)

$$\begin{aligned} x \text{ and } y \text{ are associates} &\Leftrightarrow x = uy \text{ and } y = u^{-1}x \text{ for some unit } u \in R \\ &\Rightarrow x \in (y) \text{ and } y \in (x) \\ &\Rightarrow (x) \subseteq (y) \text{ and } (y) \subseteq (x) \\ &\Leftrightarrow (x) = (y). \end{aligned}$$

($\Leftarrow$)

$$\begin{aligned} (y) = (x) &\Rightarrow x = ay \text{ and } y = bx \text{ for some } a \text{ and } b \text{ in } R \\ &\Rightarrow x = abx \\ &\Rightarrow ab = 1 \text{ (since } R \text{ is an integral domain)} \\ &\Rightarrow a \text{ and } b \text{ are units} \end{aligned}$$

(2) ($\Rightarrow$) Suppose x is irreducible, so $x = yz \Rightarrow y$ is a unit or z is a unit. Then

$$\begin{aligned} (x) \subseteq (y) \subsetneq R &\Rightarrow x \in (y) \text{ and } (y) \neq R \\ &\Rightarrow x = yz \text{ and } y \text{ is not a unit} \\ &\Rightarrow x = yz \text{ and } z \text{ is a unit (since } x \text{ is irreducible)} \\ &\Rightarrow x \text{ and } y \text{ are associates} \\ &\Leftrightarrow (y) = (x). \end{aligned}$$

Since x is not a unit, we also have $(x) \neq R$.

($\Leftarrow$) Assume x is not a unit, and $(x) \subseteq (y) \subsetneq R \Rightarrow (x) = (y)$. Then

$$\begin{aligned} x = yz \text{ and } y \text{ is not a unit} &\Rightarrow (x) \subseteq (y) \neq R \\ &\Rightarrow (x) = (y) \text{ (by our assumption)} \\ &\Rightarrow yz = x = yu \text{ for some unit } u \\ &\Rightarrow z = u \text{ (since } R \text{ is an integral domain)} \end{aligned}$$

This shows that if $x = yz$ then y is a unit or z is a unit. Since x is not a unit, x is irreducible. □

9. Principal ideal domains

Proposition 9.1. *If R is a principal ideal domain and if $x \in R$ then x is irreducible if and only if (x) is maximal.*

Proof. Proposition 8.3 says that x is irreducible if and only if (x) is maximal *among all proper principal ideals*. But all ideals are principal in R. Thus x is irreducible if and only if (x) is maximal. □

Proposition 9.2. *If R is a principal ideal domain and if $x \in R$ then x is prime if and only if x is irreducible.*

Proof. ($\Rightarrow$) Assume x is irreducible. Then (x) is a maximal ideal by Corollary 9.1 and hence is a prime ideal by Corollary 6.4. Thus x is prime by part (3) of Proposition 7.5.

($\Leftarrow$) If x is prime then x is irreducible by Proposition 8.2. □

Proposition 9.3. *If R is a principal ideal domain and A is an ideal in R then A is a prime ideal if and only if A is a maximal ideal.*

Proof. Since R is a principal ideal domain, $A = (x)$ for some element $x \in R$.

$$\begin{aligned} A = (x) \text{ is a prime ideal} &\Leftrightarrow x \text{ is prime (by Proposition 8.3)} \\ &\Leftrightarrow x \text{ is irreducible (by Corollary 8.2)} \\ &\Leftrightarrow (x) = A \text{ is maximal (by Corollary9.1).} \end{aligned}$$

□

Example 9.4. $\mathbb{Z}$ is a principal ideal domain.

Let A be any ideal in $\mathbb{Z}$. If $n \in A$ then $-n \in A$. Thus if $A \neq \{0\}$ then A contains a positive integer. Let a be the smallest positive integer in A. Obviously $(a) \subseteq A$. Take any element b of A and write $b = aq + r$ where $0 \leq r < a$. Notice that $r = b - aq \in A$. Since $r < a$ it must not be a positive integer, so $r = 0$ and $b = aq$. This shows that $b \in (a)$ and, since b was an arbitrary element of A, we conclude that $A \subseteq (a) \subseteq A$. Thus $A = (a)$, so A is a principal ideal. □

Example 9.5. If F is a field then the polynomial ring $F[x]$ is a principal ideal domain.

Let A be any ideal in $F[x]$. If $A = (0)$ Then A is a principal ideal. If $A \neq (0)$ then A contains a nonzero polynomial. Let $a(x) \in A$ be a nonzero polynomial of smallest degree among all of the elements of A. Obviously $(a(x)) \subseteq A$. Take any element $b(x)$ of A and write $b(x) = a(x)q(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg a(x)$. Notice that $r(x) = b(x) - a(x)q(x) \in A$. Since $a(x)$ had the smallest possible degree, we must have $r(x) = 0$ and hence $b(x) = a(x)q(x)$. This shows that $b(x) \in (a(x))$ and, since $b(x)$ was an arbitrary element of A, we conclude that $A \subseteq (a(x)) \subseteq A$. Thus $A = (a(x))$, so A is a principal ideal. □

Definition 9.6. An integral domain R is a *Euclidean domain (or ED)* if there exists a function $N : R - \{0\} \to \mathbb{N} = \{n \in \mathbb{Z} \mid n \geq 0\}$ such that

- for any $y \in R$ and $x \in R - \{0\}$ there exist $q, r \in R$ such that $y = xq + r$ and either $r = 0$ or $N(r) < N(x)$.

9.7. The function N is called a *norm*. For $\mathbb{Z}$ the function $N(n) = |n|$ is a norm and for $F[x]$ the function $N(p(x)) = \deg p(x)$ is a norm.

The condition $N(x) \leq N(xy)$ for all $x, y \in R - \{0\}$ may seem mysterious since it is not used in showing that $\mathbb{Z}$ and $F[x]$ are principal ideal domains. It is a convenient property, though, because of the following.

Proposition 9.8. *If R is a Euclidean domain with norm N and if $N(x) \leq N(xy)$ for all $x, y \in R - \{0\}$, then $N(x) \geq N(1)$ for all $x \in R - \{0\}$, and $N(x) = N(1)$ if and only if x is a unit.*

Proof. First, we have $N(1) \leq N(1x) = N(x)$ for any non-zero element x. If x is a unit, with $xy = 1$, then we also have $N(x) \leq N(xy) = N(1)$. Thus $N(x) = N(1)$ if x is a unit.

Suppose that x is not a unit. Write $1 = xq + r$ where either $r = 0$ or $N(r) < N(x)$. Since x is not a unit, $r \neq 0$. Therefore $N(x) > N(r) \geq N(1)$.

Thus $N(x) > N(1)$ if x is not a unit, and $N(x) = N(1)$ if x is a unit. □

Proposition 9.9. *Every Euclidean domain is a principal ideal domain.*

Exercise 9.1. Prove Proposition 9.9.

Example 9.10. The ring $\mathbb{Z}[i]$ of Gaussian integers is a Euclidean domain, and hence is a principal ideal domain.

A norm for $\mathbb{Z}[i]$ is $N(a+bi) = a^2+b^2$. Note that if we think of elements of $\mathbb{Z}[i]$ as complex numbers, then $N(z) = |z|^2$ for any $z \in \mathbb{Z}[i]-\{0\}$. Thus for all $z, w \in \mathbb{Z}[i]-\{0\}$ we have $N(w) \geq 1$ and $N(zw) = N(z)N(w) \geq N(z)$.

For the proof that $\mathbb{Z}[i]$ has a division algorithm it is useful to think of elements of $\mathbb{Z}[i]$ as complex numbers. Suppose z and w are elements of $\mathbb{Z}[i]$ with $w \neq 0$. Consider the complex number z/w. The complex plane is covered by squares of side 1 having vertices at elements of $\mathbb{Z}[i]$. One of these squares contains z/w. For every point p in a square of side 1 there is at least one vertex v such that the distance from p to v is less than 1. Thus we can take $q \in \mathbb{Z}[i]$ to be one of the vertices of the square containing z/w, and we will have $|z/w - q| < 1$. Multiplying by $|w|$ we get $|z - wq| < |w|$ and hence $N(z-wq) = |z-wq|^2 < |w|^2 = N(w)$. If we set $r = z - wq$ then we have $z = wq + r$, where either $r = 0$ or $N(r) < N(w)$.

□

Example 9.11. The ring $\mathbb{Z}\left[\sqrt{-3}\right] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$ is **not** a principal ideal domain.

We can use the function $N(a+b\sqrt{-3}) = |a+b\sqrt{-3}|^2 = a+3b^2$ to understand factorization in this ring, even though it will not turn out to be a norm. The only elements $z \in \mathbb{Z}\left[\sqrt{-3}\right]$ with $N(z) = 1$ are $z = 1$ and $z = -1$, which are units, of course. For all other non-zero elements z of $\mathbb{Z}\left[\sqrt{-3}\right]$ we have $N(z) \geq 4$. We also have $N(zw) = N(z)N(w)$ for any $z, w \in \mathbb{Z}\left[\sqrt{-3}\right]$. A consequence of these two facts is that 2, $1+\sqrt{-3}$ and $1-\sqrt{-3}$ are all irreducible in $\mathbb{Z}\left[\sqrt{-3}\right]$. But we have

$$(2)(2) = (1+\sqrt{-3})(1-\sqrt{-3}),$$

even though neither of $1 \pm \sqrt{-3}$ is a multiple of 2. In other words, irreducible elements are not prime in this ring, so it cannot be a principal ideal domain.

It is interesting to see what goes wrong if we try to show that N is a norm using the same idea that we used for $\mathbb{Z}[i]$. The complex plane is covered by rectangles of width 1 and height $\sqrt{3}$ with vertices at elements of $\mathbb{Z}\left[\sqrt{-3}\right]$. But the center point of such a rectangle has distance exactly 1 from every vertex. In fact, the complex number $(1+\sqrt{-3})/2$ is the center point of such a rectangle. □

Example 9.12. The ring $\mathbb{Q}[x, y]$ of polynomials in two indeterminates with rational coefficients is **not** a principal ideal domain.

In fact, the ideal $(x, y) = \{p(x, y) \mid p(0, 0) = 0\}$ is proper, and hence does not contain any units. But it does contain x and y, and the only elements of $\mathbb{Q}[x, y]$ that divide both x and y are units. □

Example 9.13. The ring $\mathbb{Z}[x]$ is **not** a principal ideal domain.

The ideal $(2, x) = \{p(x) \mid p(0) \text{ is even } \}$ is not principal. It contains 2 and x but the only common divisors of 2 and x are the units ± 1. Morevoer the ideal $(2, x)$ does not contain 1 or -1. (Notice that the division algorithm for polynomials requires that the coefficients have multiplicative inverses.) □

10. Unique factorization

Definition 10.1. An integral domain R is a *unique factorization domain (or UFD)* if

- every non-zero element r of R can be factored as $r = up_1 \cdots p_n$, where u is a unit and p_i is irreducible for $i = 1, \ldots n$; and
- this factorization is unique in the following sense: if

$$up_1 \cdots p_n = vq_1 \cdots q_m$$

where u and v are units and $p_1, \ldots, p_n$ and $q_1, \ldots, q_m$ are irreducible, then $m = n$ and there is a permutation $\sigma \in S_n$ such that p_i is an associate of $q_{\sigma(i)}$ for each $i = 1, \ldots, n$.

Exercise 10.1. Show that if R is a unique factorization domain then an element $r \in R$ is prime if and only if it is irreducible.

Lemma 10.2. *Suppose that R is a principal ideal domain and that $A_1 \subseteq A_2 \subseteq \cdots$ is an ascending chain of ideals in R. Then there exists some integer k such that $A_n = A_k$ for all $n \geq k$.*

Proof. By Exercise 4.2, $A = \bigcup_{i=1}^{\infty} A_i$ is an ideal in R. Since R is a PID, $A = (a)$ for some element $a \in A$. Thus $a \in A_k$ for some integer k. Since the A_i are nested, we must have $a \in A_n$ for all $n \geq k$. Thus we have $(a) \subseteq A_k \subseteq A = (a)$ for all $n \geq k$, so $A_n = A_k$ for all $n \geq k$. □

Theorem 10.3. *Every principal ideal domain is a unique factorization domain.*

Exercise 10.2. Use the lemma to prove Theorem 10.3.

Definition 10.4. Suppose that $r_1, \ldots, r_n$ are elements of an integral domain R. An element $d \in R$ is a *greatest common divisor* of $r_1, \ldots, r_n$ if

- $d | r_i$ for $i = 1, \ldots, n$; and

- if $c|r_i$ for $i = 1, \ldots, n$ then $c|d$.

Exercise 10.3. Suppose that $r_1, \ldots, r_n$ are elements of an integral domain R. Show that if d_1 and d_2 are greatest common divisors of $r_1, \ldots, r_n$ then d_1 and d_2 are associates.

Even though greatest common divisors are not unique, we may write $r = \gcd(r_1, \ldots, r_n)$ when we mean that r is a greatest common divisor of $r_1, \ldots, r_n$.

Exercise 10.4. Let R be an integral domain. Show that if any pair of non-zero elements of r has a greatest common divisor, then every finite collection of non-zero elements of R has a greatest common divisor.

Exercise 10.5. Suppose that R is a UFD and that r and s are non-zero elements of R. Show that r and s have a greatest common divisor.

Exercise 10.6. Suppose that R is a PID and that r and s are non-zero elements of R. Show that d is a greatest common divisor of r and s if and only if $(r, s) = (d)$. In particular, r and s have a greatest common divisor, and it can be written as $ar + bs$ for some $a, b \in R$.

10.5. It may be helpful to compare the properties of greatest common divisors in Euclidean domains, principal ideal domains and unique factorization domains.

Let R be an integral domain and let r and s be non-zero elements of R.

- If R is a Euclidean domain, then r and s have a greatest common divisor d, there exist elements a and b of R such that $d = ar + bs$, and the elements d, a and b can be computed by Euclid's algorithm.
- If R is a principal ideal domain, then r and s have a greatest common divisor d, and there exist elements a and b of R such that $d = ar + bs$. But there may not be an algorithm for computing d, or a and b.
- If R is a unique factorization domain then r and s have a greatest common divisor d. But there may not exist elements a and b of R such that $d = ar + bs$. For example, in $\mathbb{Z}[x]$ a greatest common divisor of 2 and x is 1 but there do not exist integer polynomials a and b such that $1 = 2a + xb$.

Theorem 10.6. *If R is a unique factorization domain then $R[x]$ is a unique factorization domain.*

Corollary 10.7. *If R is a unique factorization domain then $R[x_1, \ldots, x_n]$ is a unique factorization domain for any positive integer n.*

The corollary follows by induction on n from the following:

Exercise 10.7. Prove that $R[x_1 \ldots, x_n] \cong (R[x_1])[x_2, \ldots, x_n]$ for any integer $n \geq 2$.

The proof of Theorem 10.6 requires two lemmas.

Lemma 10.8. *Let R be a commutative ring, regarded as a subring of $R[x]$. If p is a prime element of R then p is also prime as an element of $R[x]$.*

Proof. Let Q denote the quotient ring $R/(p)$, and let $\pi : R \to Q$ be the natural surjection. Since p is prime, Q is an integral domain and so is $Q[x]$.

Let $\Pi : R[x] \to Q[x]$ be the reduction map defined by

$$\Pi(a_0 + a_1 x + \cdots a_n x^n) = \pi(a_0) + \pi(a_1)x + \cdots \pi(a_n)x^n.$$

It is easy to check that Π is a homomorphism and that

$$\ker \Pi = \{a_0 + a_1 x + \cdots a_n x^n \mid a_i \in (p) \text{ for } i = 0, \ldots, n\},$$

which is just the principal ideal in $R[x]$ generated by p. Since $Q[x]$ is an integral domain, $\ker \Pi$ is a prime ideal, and hence p is prime in $R[x]$. □

Lemma 10.9 (Gauss' Lemma)**.** *Let R be a unique factorization domain and let F be the field of fractions of R. Regard R as a subring of F and $R[x]$ as a subring of $F[x]$. Suppose that $f(x) \in R[x] \subseteq F[x]$ factors as $f(x) = a(x)b(x)$, where $a(x)$ and $b(x)$ are polynomials in $F[x]$. Then there exists ξ in F such that $\xi a(x) \in R[x]$ and $(1/\xi)b(x) \in R[x]$.*

Proof. Consider all pairs (ξ, η) of elements of F such that $\xi a(x)$ and $\eta b(x)$ are in $R[x]$ and $\xi a(x)\eta b(x) = r f(x)$ for some $r \in R$. Pairs with this property do exist; for example, we could take ξ to be the product of the denominators of the coefficients of a, and η to be the product of the denominators of the coefficients of b. We may assume that (ξ, η) has been chosen among all such pairs so that the number of irreducible factors in the factorization of r is as small as possible. We claim that r must then be a unit.

If r were not a unit we could write $r = p_1 \cdots p_n$, where p_i is irreducible (and hence prime) in R for $i = 1, \ldots n$. Since p_1 is also prime in $R[x]$, by the lemma, we know that p_1 divides either $\xi a(x)$ or $\eta b(x)$ in $R[x]$. In the first case define $(\xi', \eta') = (\xi/p_1, \eta)$ and in the second case define $(\xi', \eta') = (\xi, \eta/p_1)$. Then $\xi' a(x)\eta' b(x) = r' f(x)$, where $r = p_1 r'$. But then r' has fewer irreducible factors then r by the uniqueness of factorization. This contradiction shows that r is a unit in R. Thus $\eta/r \in R$, so $(\eta/r)b(x) \in R[x]$. But, since $\xi a(x)(\eta/r)b(x) = f(x) = a(x)b(x)$, it follows that $\eta/r = 1/\xi$. □

Corollary 10.10. *Let R be a unique factorization domain and let F be the field of fractions of R. Regard R as a subring of F and $R[x]$ as a subring of $F[x]$. Let $f(x) \in R[x]$.*

- *If $f(x)$ is irreducible in $R[x]$ then $f(x)$ is irreducible in $F[x]$.*

- *If $f(x)$ is irreducible in $F[x]$ and $f(x)$ is not divisible by any prime element of R, then $f(x)$ is irreducible in $R[x]$.*

Proof of Theorem 10.6. Let F be the field of fractions of R and let $f(x) \in R[x]$. Let d be a greatest common divisor of the coefficients of $f(x)$. Then $f(x) = dg(x)$ where $g(x) \in R[x]$ is not divisible by any prime in R. Factor d in R as $d = up_1 \cdots p_n$ where u is a unit and each p_i is irreducible. Factor $g(x)$ in $F[x]$ as $g(x) = q_1(x) \cdots q_m(x)$ where each $q_j(x)$ is an irreducible polynomial of positive degree in $F[x]$. By Gauss' Lemma, we may also write $g(x) = P_1(x) \cdots P_m(x)$ where each $P_j(x) \in R[x]$ and $P_j(x) = \xi_j q(x)$ for some $\xi_j \in F$. Since $g(x)$ is not divisible by any prime in R, it follows that $P_j(x)$ is not divisible by any prime in R for $j = 1, \ldots, m$. Thus, by Corollary 10.10, we have factored $f(x)$ as

$$f(x) = up_1 \cdots p_n P_1(x) \cdots P_m(x)$$

where u is a unit in R, each p_i is irreducible in R and hence in $R[x]$, and each $P_j(x)$ is an irreducible polynomial of positive degree in $R[x]$.

Suppose that we have another factorization $f(x) = vq_1 \cdots q_r Q_1(x) \cdots Q_s(x)$ where v is a unit in R, $q_1, \ldots, q_r$ are irreducible elements of R and $Q_1(x), \ldots Q_s(x)$ are irreducible elements of positive degree in $R[x]$. Then $p_1 \cdots p_n$ and $q_1, \ldots, q_r$ are both associates of d, so we have that $r = n$ and, for some $\sigma \in S_n$, we have that p_i is an associate of $q_{\sigma(i)}$ for $i = 1, \ldots, n$. According to Corollary 10.10, $P_1(s), \ldots, P_m(s)$ and $Q_1(x), \ldots, Q_s(x)$ are all irreducible in $F[x]$. Moreover, $P_1(x) \cdots P_m(x)$ and $Q_1(x) \cdots Q_s(x)$ are associates in $F[x]$. Thus it follows from the fact that $F[x]$ is a PID, and hence a UFD that $m = s$ and, for some $\tau \in S_m$, we have that P_j is an associate of $Q_{\tau(j)}$ for $j = 1, \ldots m$. This proves the uniqueness of the factorization of $f(x)$. □

11. Finitely generated modules

Definition 11.1. Let R be a ring and M a left R-module. If X is a set of elements of M then the *submodule generated by* X is the smallest submodule of M containing X.

Exercise 11.1. Let R be a ring, M a left R-module, and $X \subseteq M$. Show that the sumbodule of M generated by X consists of all elements of the form $a_1x_1 + \cdots + a_nx_n$, where $x_1, \ldots, x_n \in X$.

Definition 11.2. An R-module is *finitely generated* if it is generated by a finite set of elements.

It not true in general that submodules of finitely generated modules are finitely generated. In fact, it is possible for R itself, a module generated by a single element, to have submodules, i.e. ideals, which are not finitely generated.

Definition 11.3. A left R-module is *Noetherian* if it satisfies the following ascending chain condition:

- If $M_1 \subseteq M_2 \subseteq \cdots$ is an ascending chain of submodules of M then there exists an integer k such that $M_n = M_k$ for all $n \geq k$.

A ring R is *left Noetherian* if it is a Noetherian left module over itself, i.e. if every ascending chain of left ideals in R is eventually constant.

A ring is *Noetherian* if it is commutative and left Noetherian.

11.4. Any principal ideal domain is Noetherian, by Lemma 10.2.

Proposition 11.5. *Let M be an R-module. The following conditions are equivalent:*

- *M is Noetherian.*
- *Every collection of submodules of M has a maximal element.*
- *Every submodule of M is finitely generated.*

Exercise 11.2. Prove Proposition 11.5. The second statement means that if $\mathcal{S}$ is any collection of submodules of M, then there exists $N \in \mathcal{S}$ such that N is not properly contained in any other submodule in $\mathcal{S}$.

11.6. A ring R is Noetherian if and only if every ideal in R is generated by finitely many elements of R. (That is, every ideal in R has the form $(r_1, \ldots, r_n)$.)

Proposition 11.7. *If R is a Noetherian ring, then R^n is a Noetherian module for any positive integer n.*

Proof. To avoid confusion with ideals, elements of R^n will be denoted with square brackets:

$$R^n = \{[r_1, \ldots, r_n] \mid r_i \in R \text{ for } i = 1, \ldots n\}.$$

Let M be a submodule of R^n. For $j = 1, \ldots, n$ let M_j denote the submodule of M consisting of n-tuples for which the first $j-1$ entries are 0, and let A_j denote the set of elements of R which arise as the j^{th} entry of some element of M_j. It is easy to check that A_j is an ideal for each $j = 1, \ldots, n$.

Since R is Noetherian, for each $j = 1, \ldots, n$ there exist elements $r_{j,1}, \ldots r_{j,n_j}$ of R which generate the ideal A_j, and we can choose elements $x_{j,1}, \ldots x_{j,n_j}$ of M_j such that the j^{th} entry of $x_{j,i}$ is $r_{j,i}$ for $i = 1, \ldots, n_j$. We will show that

$$X = \bigcup_{i=1}^{n} \{x_{j,1}, \ldots, x_{j,n_j}\}$$

is a generating set for M. Let $M' \subseteq M$ denote the submodule of R^n generated by X.

Suppose that $y \in M = M_1$ and that the first entry of y is $a \in R$. Since $a \in A_1$ there exist elements $a_1, \ldots, a_{n_1}$ such that $a = a_1 r_{1,1} + \cdots + a_{n_1} r_{1,n_1}$. If we set $u_1 = a_1 x_{1,1} + \cdots + a_{n_1} x_{1,n_1}$ then $u_1 \in M'$ and $y - u_1 \in M_2$. The same argument, applied to $y - u_1$ shows that there exists an element $u_2 \in M'$ such that $y - u_1 - u_2 \in M_3$. Continuing inductively we find elements $u_1, u_2, \ldots, u_n \in M'$ such that $y - u_1 - \cdots - u_n \in M_n = \{0\}$. Thus $y \in M'$. Since y was arbitrary we have shown that $M = M'$, so M is generated by the finite set X. □

Exercise 11.3. Prove that a quotient of a Noetherian R-module is Noetherian.

Theorem 11.8 (Hilbert's Basis Theorem)**.** *If R is a Noetherian ring then $R[x_1, \ldots, x_n]$ is Noetherian for any positive integer n.*

Proof. It suffices to show that $R[x]$ is Noetherian. The general statement follows by induction, using the fact that $R[x_1, \ldots, x_n] \cong (R[x_1])[x_2 \ldots, x_n]$.

Let A be any ideal in $R[x]$. Let $L \subseteq R$ be the collection of all leading coefficients of polynomials in A. We will show that L is an ideal. Suppose that $a \in L$ is the leading coefficient of a polynomial $f(x) \in A$ of degree n, and $b \in L$ is the leading coefficient of $g(x) \in A$ of degree m. Then $a + b$ is the leading coefficient of $x^m f(x) + x^n g(x) \in A$. This shows that L is closed under addition. If $r \in R$ then ra is the leading coefficient of $rf(x) \in A$. This shows that L is an ideal in R.

Since R is Noetherian we can find finitely many polynomials $f_1(x), \ldots, f_k(x)$ whose leading coefficients generate L. Suppose that the leading term of f_i is $a_i x^{n_i}$, and let N be the maximum degree of any of the polynomials f_i for $i = 1, \ldots, k$. Suppose that $g(x) \in A$ has degree $m \geq N$. Then the leading coefficient of g can be written as $r_1 a_1 + \cdots + r_n a_n$, and hence the polynomial $g(x) - (r_1 x^{m-n_1} f_1(x) + \cdots + r_n x^{m-n_k} f_k(x)) \in A$ has lower degree than g. Thus any polynomial in A which has degree at least N is congruent, modulo the ideal $(f_1, \ldots, f_n)$ to a polynomial in A of degree less than N.

For each $j = 1, \ldots, N-1$ let L_j be the set of leading coefficients of elements of degree j in A. Each L_j is an ideal, by an argument similar to the one used above to show that L is an ideal. For each $j = 1, \ldots N-1$ choose polynomials $f_{1,j}, \ldots, f_{n_j,j}$ whose leading coefficients generate L_j. Then, as above, each element of degree $N-1$ in A is congruent modulo $(f_{N-1,1}, \ldots f_{N-1,n_{-1}})$ to an element of lower degree in A. It now follows by induction that A is generated by $f_1, \ldots, f_n$ together with the $f_{j,k}$. □

12. Free modules

Definition 12.1. Let R be a ring and M a left R-module. A subset $\mathcal{B} \subseteq M$ is a *basis* for M if

- M is generated by $\mathcal{B}$ (i.e. for each $m \in M$ there exist $r_1, \ldots, r_n \in R$ and $b_1, \ldots, b_n \in B$ such that $m = r_1 b_1 + \cdots r_n b_n$); and
- the expression of $m \in M$ as an R-linear combination of elements of $\mathcal{B}$ is unique (i.e. if $b_1, \ldots, b_n \in B$ and $r_1, \ldots, r_n, s_1, \ldots, s_n \in R$, then $r_1 b_1 + \cdots r_n b_n = s_1 b_1 + \cdots s_n b_n$ if and only if $r_i = s_i$ for all $i = 1, \ldots, n$).

A left R-module is *free* if it has a basis.

Proposition 12.2. *Let R be a ring and M a left R-module. A subset $\mathcal{B}$ of M is a basis if and only if it satisfies the following universal property:*

- *If N is an R-module and $f : \mathcal{B} \to N$ is an arbitrary function then there exists a unique R-module homomorphism $\phi : M \to N$ such that $\phi(b) = f(b)$ for all $b \in \mathcal{B}$.*

Exercise 12.1. Prove Proposition 12.2

Exercise 12.2. Let R be a ring. Let $e_i \in R^n$ be the n-tuple $(r_1, \ldots, r_n)$ where $r_i = 1$ and $r_j = 0$ if $j \neq i$. Prove that $\{e_1, \ldots, e_n\}$ is a basis of R^n.

Exercise 12.3. Prove that a finitely-generated free left R-module is isomorphic to R^n for some integer n.

Exercise 12.4. Show that the direct sum of an arbitrary family of free R-modules is a free R-module.

Exercise 12.5. Let R be a ring. Prove that every R-module is a quotient of a free R-module. Prove that every finitely generated R-module is a quotient of a finitely generated free R-module.

Exercise 12.6. Suppose that R is a Noetherian ring. Prove that any finitely generated R-module is Noetherian.

Definition 12.3. Let R be a ring and M be a left R-module. A finite set $\{x_1, \ldots, x_k\}$ of elements of M is *dependent* if there exist elements $r_1, \ldots, r_k$ of R, not all equal to 0, such that $r_1 x_1 + \cdots r_k x_k = 0$. A k-tuple of elements of M is *independent* if it is not dependent.

Exercise 12.7. Let M be a finitely generated left R-module. Show that a finite set of generators of M is a basis if and only if it is independent.

Definition 12.4. A *vector space* over a field F is an F-module V. Elements of V are called *vectors* and, in this context, elements of F are called *scalars*. A vector space is

finite dimensional if it is finitely generated. As set of vectors that generate V is called a *spanning set*

Proposition 12.5. *Let V be a finite dimensional vector space and let $\{e_1, \ldots, e_n\}$ be a spanning set for V. If $m > n$ then any set of m elements of V is dependent.*

Proof. Let $v_1, \ldots, v_m$ be elements of V, where $m > n$. For each $j = 1, \ldots, m$ write v_i as a linear combination of elements of $\mathcal{B}$:

$$v_j = a_{1j}e_1 + \cdots a_{nj}e_n.$$

Then $b_1v_1 + \cdots b_mv_m = 0$ if and only if, for each $i = 1, \ldots, n$ we have

$$a_{i1}b_1 + \cdots + a_{im}b_m = 0.$$

In other words, the vectors $v_1, \ldots, v_m$ are dependent if and only if the $n \times m$ linear system

$$a_{i1}x_1 + \cdots + a_{im}x_m = 0; \quad i = 1, \ldots, n$$

has a non-zero solution. But, as is taught in undergraduate linear algebra, any linear system with more variables than equations has a non-zero solution. (Gaussian elimination works over any field.) □

Another proof. Another popular way to prove this is with the "exchange argument."

First we need an observation: Suppose that $r_1x_1 + \cdots + r_kx_k = 0$ where $r_1, \ldots, r_k \in F$ and $x_1, \ldots, x_k \in V$. Suppose, in addition, that $r_j \neq 0$ for some j. Then x_j can be written as a linear combination of the x_i for $i \neq j$.

Start with the set $\{e_1, \ldots, e_n\}$. Write v_1 as a linear combination of $e_1, \ldots, e_n$. One of the e_i must have a non-zero coefficient; we may reorder so that the coefficient of e_1 is non-zero. Replace e_1 by v_1 to get a new set $\{v_1, e_2, \ldots, e_n\}$. By the observation above, e_1 can be written as a linear combination of $v_1, e_2, \ldots, e_n$, so we have a new spanning set.

We attempt to repeat this process. At the i^{th} step we know that $\{v_1, \ldots, v_i, e_{i+1}, \ldots e_n\}$ is a spanning set (although the e_j have been reordered). We write v_{i+1} as a linear combination of $v_1, \ldots, v_i, e_{i+1}, \ldots e_n$. If all of the coefficients of the e_j are zero then we have shown that $\{v_1, \ldots, v_{i+1}\}$ is dependent, which implies that $\{v_1, \ldots, v_m\}$ is dependent. Otherwise we can go one more step, exchanging v_{i+1} for one of the e_j and reordering to conclude that $\{v_1, \ldots, v_{i+1}, e_{i+2}, \ldots, e_n\}$ is a spanning set.

If this process continues for n steps, we will have shown that $\{v_1, \ldots, v_n\}$ is a spanning set. Since $m > n$, we have that $v_{n+1}, \ldots, v_m$ can all be expressed as linear combinations of $v_1, \ldots, v_n$, so $\{v_1, \ldots, v_m\}$ is dependent. □

Corollary 12.6. *Any two bases of a finite dimensional vector space have the same cardinality. In particular, if F is a field then F^n is isomorphic to F^m if and only if $m = n$.*

Exercise 12.8. Let V be a finite dimensional vector space over a field F. Show that every independent set of vectors can be extended to a basis, and that every spanning set contains a basis. (In particular, V is a free F-module.)

The *dimension* of a finite dimensional vector space is the cardinality of any of its bases.

Proposition 12.7. *Let R be a commutative ring and let M be a finitely generated free R-module. Then any two bases of M have the same cardinality.*

Proof. Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be two bases of M. By Exercise 6.1 we know that R has a maximal ideal A. Consider the field $F = R/A$ and let $\pi : R \to F$ be the natural surjection. For $i = 1, 2$, let V_i be the vector space which is the direct sum of copies of F indexed by $\mathcal{B}_i$. For $b \in B_i$ let $e_b \in V_i$ denote the vector with b-coordinate 1 and all other coordinates 0. The set $\{e_b \mid b \in \mathcal{B}_i\}$ is a basis of V_i.

Define $\phi_i : M \to V_i$ by

$$\phi_i(a_1 b_1 + \cdots a_k b_k) = \pi(a_1) e_{b_1} + \cdots \pi(a_k) e_{b_k}$$

for any $b_1, \ldots, b_k \in \mathcal{B}_i$ and $a_1, \ldots, a_k \in R$.

It is easy to check that these are both surjective homomorphisms, and that $\ker \phi_i = AM = \{am \mid a \in A \text{ and } m \in M\}$. Since the two homomorphisms have the same kernel, we have $V_1 \cong V_2$. But by Corollary 12.6 this implies that $\mathcal{B}_1$ and $\mathcal{B}_2$ have the same cardinality. □

Definition 12.8. Let R be a commutative ring and M a finitely generated free R-module. The *rank* of M is the cardinality of any of its bases.

Exercise 12.9. Let R be an integral domain, and let F be its field of fractions. Let M be a finitely generated free R-module having a basis consisting of n elements of M. By embedding M as a subset of F^n, show that if $m > n$ then any set of m elements of M is dependent.

13. Presentations and syzygies

Exercise 13.1. Let R be a ring. Define matrix multiplication of R-matrices. Show that the $n \times n$ R-matrices form a ring under componentwise addition and matrix multiplication. This ring is denoted $M_n(R)$.

13.1. Let R be a ring and let M and N be free left R-modules with ordered bases $\mathcal{B} = (x_1, \ldots, x_m)$ and $\mathcal{C} = (y_1, \ldots, y_n)$ respectively. A homomorphism $\phi : M \to N$ is determined by the elements $\phi(x_i) = a_{i1} y_1 + \cdots + a_{in} y_n$ for $i = 1, \ldots, m$. The $m \times n$ R-matrix (a_{ij}) is said to represent ϕ with respect to the ordered bases $\mathcal{B}$ and $\mathcal{C}$.

Exercise 13.2. Let R be a ring. Suppose that M and N are finitely generated free left R-modules with fixed ordered bases $\mathcal{B}$ and $\mathcal{C}$ respectively. Describe how to use $\mathcal{B}$ and $\mathcal{C}$ to represent each element of M or N as a column of the appropriate size. Let $\phi : M \to N$ be a homomorphism represented by a matrix (aij) with respect to $\mathcal{B}$ and $\mathcal{C}$. Show that the column which represents $\phi(x) \in N$ is the product of the matrix (a_{ij}) and the column which represents $x \in M$. Show that the composition of two homomorphisms between free R-modules (with given ordered bases) is represented by the product of their matrix representations.

Exercise 13.3. Let R be a commutative ring. Define the determinant of a matrix in $M_n(R)$. If $A \in M_n(R)$, show that there exists $B \in M_n(R)$ with $AB = BA = 1$ if and only if the determinant of A is a unit.

Exercise 13.4. Let R be an integral domain. Show that a matrix $A \in M_n(R)$ represents an injective homomorphism from R^n to R^n if and only if it has non-zero determinant.

13.2. Let R be a Noetherian ring and suppose that M is a finitely generated R-module with generators $g_1, \ldots, g_n$. Let M_1 be a free R-module with basis $\{e_1, \ldots, e_n\}$. (Thus, in particular, $M_1 \cong R^n$.) It follows from Proposition 12.2 that there is a unique homomorphism $f_1 \colon M_1 \to M$ such that $f_1(e_i) = g_i$. Since M is generated by $g_1, \ldots, g_n$ the homomorphism f_1 is surjective. Since $M_1 \cong R^n$ is Noetherian, the kernel of f_0 is finitely generated, and hence there is a finitely generated free R-module M_2 and a homomorphism $f_2 : M_2 \to M_1$ such that $\operatorname{im} f_2 = \ker f_1$. This process can be iterated to produce an exact sequence

$$\cdots \longrightarrow M_2 \xrightarrow[f_2]{} M_1 \xrightarrow[f_1]{} M \longrightarrow 0$$

in which M_i is a finitely generated free R-module for $i = 1, 2, \ldots$. Such an exact sequence is called a *free resolution* of M. The modules M_i are sometimes called *syzygies* of M.

We will see later that if R is a PID then every submodule of a free R-module is free. In particular the homomorphism f_2 can be taken to be injective, so a finitely generated module over a PID has a free resolution of length at most 2. (That is, we have $M_i = 0$ for $i > 2$.) Hilbert's Syzygy Theorem says that if $R = \mathbb{C}[x_1, \ldots, x_n]$ then any finitely generated R-module has a free resolution of length at most $n + 1$.

Definition 13.3. Let R be a Noetherian ring and M a finitely generated R-module. A *presentation* of M is an exact sequence

$$M_2 \xrightarrow[f_2]{} M_1 \xrightarrow[f_1]{} M \longrightarrow 0$$

where M_1 and M_2 are finitely generated free R-modules. If $\mathcal{B}_1 = (a_1, \ldots, a_n)$ and $\mathcal{B}_2 = (b_1, \ldots, b_m)$ are ordered bases of M_1 and M_2 respectively then the homomorphism f_2 is represented by an $n \times m$ matrix. This matrix is called a *presentation matrix* for M.

If R is Noetherian then every finitely generated R-module M is isomorphic to R^n/K for some integer $n > 0$ and some submodule K of R^n. The submodule K is finitely generated by Proposition 11.7. It follows that M can be described by a presentation matrix A. We just choose elements $c_1, \ldots, c_m \in R^n$ which generate K, and use these "R-vectors" as the columns of A.

Definition 13.4. An *elementary row operation* on an $m \times n$ R-matrix consists of

- interchanging two rows; or
- replacing row i by the sum of row i and r times row j, where $r \in R$ and $j \neq i$;

An *elementary column operation* is defined similarly. If A and A' are $m \times n$ R-matrices then we will write $A \underset{E}{\simeq} A'$ if there is a finite sequence $A = A_0, \ldots, A_n = A'$ of $m \times n$ R-matrices such that A_i is obtained from A_{i-1} by an elementary row or column operation for $i = 1, \ldots, n$.

Exercise 13.5. Show that the relation $\underset{E}{\simeq}$ is an equivalence relation on $m \times n$ R-matrices.

Proposition 13.5. *Let R be a Noetherian ring and let M be a finitely generated R-module. Assume that*

$$M_2 \xrightarrow[f_2]{} M_1 \xrightarrow[f_1]{} M \longrightarrow 0$$

is a presentation of M, and that the homomorphism f_2 is represented by the R-matrix A with respect to ordered bases $\mathcal{B}_1$ of M_1 and $\mathcal{B}_2$ of M_2. Suppose that $A \underset{E}{\simeq} A'$. Then there are ordered bases $\mathcal{B}'_1$ of M_1 and $\mathcal{B}'_2$ of M_2 such that the homomorphism f_2 is represented by A' with respect to $\mathcal{B}'_1$ and $\mathcal{B}'_2$.

Exercise 13.6. Prove Proposition 13.5.

Proposition 13.6. *Let R be a Euclidean domain and let A be an $m \times n$ R-matrix. Then $A \underset{E}{\simeq} D$ where $D = (d_{ij})$ is an n $m \times n$ R-matrix such that, for some $k \leq n$, the only non-zero entries of D are $d_{11}, \ldots, d_{kk}$. Moreover we have $d_{11} | d_{22} | \cdots | d_{kk}$, and the greatest common divisor of the determinants of the $i \times i$ submatrices of A is equal to $d_{11} \cdots d_{ii}$ for $i = 1, \ldots, \min(m, n)$.*

Proof. Let $N : R \to Z$ be the norm on the Euclidean domain R. We will give a effective procedure, which generalizes Euclid's algorithm, for constructing the matrix D.

Define SUBPROCEDURE 1 as follows. Given an $m \times n$ R-matrix, interchange two rows and two columns, if necessary, to obtain a matrix (a_{ij}) such that $N(a_{11}) \leq N(a_{ij})$ for any non-zero entry a_{ij}. If there exists $1 < i \leq m$ such that $a_{i1} \neq 0$ then, by the division algorithm, there is $r \in R$ so that $N(a_{i1} - ra_{11}) < N(a_{11})$. In this case, subtract r times the first row from the i^{th} row. The resulting matrix has an entry with strictly smaller

norm than any entry of A. If $a_{i1} = 0$ for all $i = 1, \ldots, m$, but there exists $1 < j \leq n$ such that $a_{1j} \neq 0$ then a similar column operation will produce a matrix which has an entry of strictly smaller norm than a_{11}.

Repeat SUBPROCEDURE 1 as many times as possible. Each application will reduce the minimum norm of the non-zero matrix entries unless the minimal entry is in the upper left corner, and all other entries in the first row or column are 0, or the entire matrix is 0. Thus we obtain such a matrix after finitely many applications.

Define SUBPROCEDURE 2 as follows. We are given an $m \times n$ R-matrix $(a_i j)$ such that the entry a_{11} is the non-zero entry of minimal norm and all other entries in the first row or column are 0. If there exists a non-zero entry a_{ij} which is not divisible by a_{11} then add row i to the first row. There exists $r \in R$ such that $a_{ij} - r a_{11}$ is a non-zero element of smaller norm than a_{11}. Subtract r times the first column from column j. This produces a matrix which has an entry of smaller norm than a_{11}.

By alternately applying SUBPROCEDURE 1 as many times as possible and then applying SUBPROCEDURE 2 we obtain, after finitely many steps, either the 0 matrix or a matrix (a_{ij}) whose non-zero entry of smallest norm is a_{11}, such that a_{11} is the only non-zero entry in the first row or column, and such that a_{11} divides all other non-zero entries.

We now repeat this entire process on the lower right $m - 1 \times n - 1$ submatrix, using elementary row and column operations that do not involve the first row or column. These operations preserve the property that all non-zero entries are divisible by a_{11}. Continuing inductively we produce the desired matrix D. Elementary row or column operations preserve the greatest common divisor of the determinants of all $i \times i$ submatrices. This implies the last statement, since $d_{11} \cdots d_{ii}$ is the greatest common divisor of the determinants of all $i \times i$ submatrices of D. □

Proposition 13.7. *Let R be a Euclidean domain and let M be a finitely generated R-module. Suppose that N is a submodule of M. Then there exists a basis $\{e_1, \ldots, e_n\}$ of M, and $k \leq n$ elements $a_1, \ldots, a_k$ of R with $a_1 | a_2 \cdots | a_k$, such that $\{a_1 e_1, \ldots, a_k e_k\}$ is a basis of N. In particular N is a free module and the rank of N is no larger than the rank of M.*

Proof. We apply Proposition 13.6 to a presentation matrix for M, and then use Proposition 13.5 to conclude that there exists a basis $\{e_1, \ldots, e_n\}$ of M such that N is generated by $\{d_1 e_1, \ldots, d_m e_m\}$, where $m \leq n$, $d_1, \ldots, d_m$ are non-zero and $d_1 | d_2 \cdots | d_m$. Some of the d_i may be units, but the divisibility condition implies that these must precede the non-units. Suppose the first j of the d_i are units. Let $k = m - j$. Set $u_i = d_i$ for $i = 1, \ldots, j$ and set $a_i = d_{j+i}$ for $i = 1, \ldots, k$.

It remains to show that this generating set is a basis for N. According to Exercise 12.7 it suffices to check that they are independent. Suppose, to the contrary, that $r_1, \ldots, r_m$

are elements of R, not all zero, so that $r_1d_1e_1 + \cdots + r_md_me_m = 0$. Since R is an integral domain, the elements $r_1d_1, \ldots, r_kd_k$ are not all zero. This contradicts the independence of $e_1, \ldots, e_n$. □

Theorem 13.8. *Let R be a Euclidean domain and let M be a finitely generated R-module. Then there exist non-negative integers b and k and non-zero non-unit elements $a_1, \ldots, a_k \in R$ so that $a_1|a_2|\cdots a_k$ and*

$$M \cong R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_k) \oplus R^b.$$

Proof. Let

$$M_2 \xrightarrow[f_2]{} M_1 \xrightarrow[f_1]{} M \longrightarrow 0$$

be a presentation of M. Set $N = \ker f_1 = \operatorname{im} f_2$, so M is isomorphic to M_1/N. Proposition 13.7 implies that there is a basis $\{e_1, \ldots, e_n\}$ of M_1, some units $u_1, \ldots, u_j \in R$ and some non-zero non-units $a_1, \ldots, a_k \in R$ so that $a_1|a_2|\cdots|a_k$ and

$$\{u_1e_1, \ldots, u_je_j, a_1e_{j+1}, \ldots, a_ke_{j+k}\}$$

is a basis of N. Set $b = n - k - j$ and choose a basis $\{f_1, \ldots, f_b\}$ of R^b. Set

$$P = R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_k) \oplus R^b.$$

Let $\iota_i : R/(a_{i-j}) \to P$, for $i = j+1, \ldots, j+k$, and $\iota_{j+k+1} : R^m \to P$ denote the inclusion homomorphisms.

Consider the homomorphism $\phi : M_1 \to P$ which satisfies

$$\phi(e_i) = \begin{cases} 0, & \text{if } 0 < i \leq j; \\ \iota_i(1 + (a_{i-j})), & \text{if } j < i \leq j+k; \\ \iota_{j+k+1}(f_{i-k-j}), & \text{if } j+k < i \leq n. \end{cases}.$$

It is straightforward to check that ϕ is surjective and $\ker \phi = N$. Thus $M \cong M/N \cong P$. □

13.9. Any abelian group is a $\mathbb{Z}$ module where the $\mathbb{Z}$-action is defined by

$$ng = \begin{cases} g + \cdots + g \ (n \text{ terms}) & \text{if } n > 0; \\ 0 & \text{if } n = 0; \\ -g - \cdots - g \ (|n| \text{ terms}) & \text{if } n < 0. \end{cases}$$

Theorem 13.8 implies the structure theorem for finite abelian groups which was proved earlier. However, the statements are slightly different. For example, the group $\mathbb{Z}/6\mathbb{Z}$ is in standard form as far as Theorem 13.8 is concerned, whereas the structure theorem for finite abelian groups would decompose it as a direct sum of cyclic groups of prime power order: $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. The result that links these two standard forms is the Chinese Remainder Theorem.

Definition 13.10. Let R be a commutative ring and let $A_1, \ldots, A_n$ be ideals of R. Then

$$A_1 \cdots A_n = \{a_1 \cdots a_n \mid a_i \in A_i \text{ for } i = 1, \ldots, n\}.$$

Exercise 13.7. Show that if $A_1, \ldots, A_n$ are ideals in a commutative ring R then $A_1 \cdots A_n$ is an ideal in R.

13.11. Given ideals A and B in a commutative ring R, we have three ways to construct new ideals from A and B:

- $A + B = \{a + b \mid a \in A \text{ and } b \in B\}$;
- $A \cap B$;
- $AB = \{ab \mid a \in A \text{ and } b \in B\}$.

Note that $A+B \supset A \cap B \supset AB$. In a principal ideal domain these three ideals correspond, respectively, to the greatest common divisor, least common multiple, and product of the generators. For example, in $\mathbb{Z}$ we have

$$(4) + (6) = (2)$$
$$(4) \cap (6) = (12)$$
$$(4)(6) = (24)$$

Of course the product of two integers is equal to their least common multiple when their greatest common divisor is 1. That is, if $(m) + (n) = (1) = \mathbb{Z}$ then $(m)(n) = (m) \cap (n)$.

Theorem 13.12 (Chinese Remainder Theorem)**.** *Let $A_1, \ldots, A_n$ be ideals in a commutative ring R. If $A_1 + \cdots + A_n = R$ then $A_1 \cdots A_n = A_1 \cap \cdots \cap A_n$. As a consequence, $R/A_1 \cdots A_n \cong R/A_1 \oplus \cdots \oplus R/A_n$.*

Proof. We will give the proof for two ideals A and B. The general result follows by induction.

Since it is always true that $AB \subseteq A \cap B$, it suffices to show that $A \cap B \subseteq AB$. Suppose $x \in A \cap B$. Since $A + B = R$ we have $1 = a + b$ for some $a \in A$ and $b \in B$. Multiplying by x we have $x = ax + xb$. Since $x \in B$, we have $ax \in AB$. Since $x \in A$ we have $xb \in AB$. Thus $x \in AB$.

To prove the last part of the statement, consider the homomorphism $\phi\colon R \to R/A \oplus R/B$ given by $\phi(x) = (x + A, x + B)$. Since $a + b = 1$, we have $\phi(a) = (a + A, a + B) = (0, 1)$ and $\phi(b) = (b + A, b + B) = (1, 0)$. Thus $\phi(ya + xb) = (x + A, y + B)$, which shows that ϕ is surjective. The kernel of ϕ is $A \cap B$. Since $A \cap B = AB$, we have $R/AB \cong R/A \oplus R/B$ by the first isomorphism theorem. $\square$

Corollary 13.13. *Suppose that R is a principal ideal domain and that $a \in R$ factors as $a = p_1^{n_1} \cdots p_k^{n_k}$ where $p_1, \ldots, p_k$ are distinct primes (and hence irreducible). Then*

$$R/(a) \cong R/(p_1^{n_1}) \oplus \cdots \oplus R/(p_k^{n_k}).$$

Corollary 13.14. *Let R be a Euclidean domain and let M be a finitely generated R-module. Then there exist a non-negative integer b, prime elements $p_1, \ldots, p_m$ of R (not necessarily distinct) and non-negative integers $n_1, \ldots, n_m$ such that*

$$M \cong R/(p_1^{n_1}) \oplus \cdots \oplus R/(p_m^{n_m}) \oplus R^b.$$

13.15. The prime powers in Corollary 13.14 are obtained by taking all prime power factors of the elements $a_1, \ldots, a_k$ in the statement of Theorem 13.8. Conversely, given the prime powers, there is a unique sequence of elements $a_1, \ldots, a_k$ which are products of these prime powers and satisfy a_1
$cdots|a_n$. One takes a_n to be the product of the maximal power of each prime, etc. For example, taking $R = \mathbb{Z}$, the prime powers $\{2, 2, 2^2, 2^3, 3, 3^3, 5\}$ would produce $a_4 = 2^3 3^3 5$; $a_3 = 2^2 3$; $a_2 = 2$; $a_1 = 2$;

14. Finitely generated modules over a principal ideal domain

Definition 14.1. Let R be a ring and let M be an R-module. An element $m \in M$ is a *torsion element* if there exists $0 \neq r \in R$ such that $rm = 0$. The R-module M is *torsion-free* if it contains no non-zero torsion elements.

14.2. If R is an integral domain then any free R-module is torsion-free.

Exercise 14.1. Let R be an integral domain and M be an R-module. Show that the sum of two torsion elements of M is a torsion element.

Definition 14.3. Let R be an integral domain and let M be an R-module. Define $\operatorname{Tor} M \doteq \{m \in M \mid rm = 0 \text{ for some } r \in R - \{0\}\}$. This is a sumodule of M by the previous exercise, and is called the *torsion submodule* of M.

Suppose that R is a PID and that M is a finitely generated free R-module. Since R is Noetherian, any submodule of M is finitely generated. By Exercise 12.9 an independent set of elements of M can contain at most n elements. Thus the following definition makes sense.

Definition 14.4. If R is a PID and M is a finitely generated free R-module then the *rank* of a submodule N of M is the maximum number of independent elements of M.

Lemma 14.5. *Let R be a PID. Suppose that M is a finitely generated free R-module. If $M \cong A \oplus B$ then* $\operatorname{rank} A + \operatorname{rank} B \leq \operatorname{rank} M$.

Exercise 14.2. Prove Lemma 14.5.

14.6. If R is a PID and A is an ideal in R then A is isomorphic to R as an R-module. In fact, if $A = (a)$ then $x \mapsto ax$ is an R-module isomorphism from R to A.

Lemma 14.7. *Let R be a principal ideal domain and let M be an R-module. Suppose that $\phi : M \to R$ is a non-zero homomorphism of R-modules. Then $M \cong R \oplus \ker \phi$. If the ideal $\phi(M)$ is generated by $a \in R$ and if $x \in M$ is such that $\phi(x) = a$, then $M = Rx \oplus \ker \phi$, where Rx denotes the submodule generated by x.*

Proof. The image of ϕ is a submodule of R, and hence an ideal. Since R is a PID the observation above shows that $\operatorname{im} R$ is isomorphic to R, as an R-module, and hence that $\operatorname{im} R$ is a free R-module of rank 1. Exercise 3.2 shows that $M \operatorname{im} \phi \oplus \ker \phi \cong R \oplus \ker \phi$.

If we have $\phi(x) = a$, where $\phi(M) = (a)$, then we can define a section $\sigma : (a) \to M$ by $\sigma(r) = rx$. Thus

$$M = \ker \phi \oplus \operatorname{im} \sigma = Rx \oplus \ker \phi.$$

□

Theorem 14.8. *Let R be a PID and let M be a finitely generated free R-module of rank n. Then any submodule of M is free of rank at most n,*

Proof. The proof is by induction on n. If M has rank 1 then $M \cong R$ and a submodule of M is isomorphic to an ideal in R. As we have observed above, since R is a PID, any non-zero ideal in R is a free R-module of rank 1.

For the induction step, assume that every submodule of a free R-module of rank less than n is free. Let N be a submodule of M. Choose a basis $\{e_1, \ldots, e_n\}$ of M. Let $\pi : M \to R$ be the projection homomorphism defined by $\pi_n(r_1 e_1 + \cdots r_n e_n) = r_n$. By Lemma 14.7 we have $M \cong \ker \pi \oplus Re_n$, where $\ker \pi$ is generated by $e_1, \ldots, e_{n-1}$ and Re_n is the submodule generated by e_n. The elements $e_1, \ldots, e_{n-1}$ are independent, so $\ker \pi$ is a free R-module of rank $n-1$.

If $N \subseteq \ker \pi$ then N is a submodule of a free R-module of rank $n-1$ and hence is free of rank at most $n-1$ by the induction hypothesis. Otherwise, the homomorphism $\phi = \pi | N$ is non-zero. Thus, by Lemma 14.7

$$N \cong \ker \phi \oplus R = (N \cap \ker \pi) \oplus R.$$

By induction, $N \cap \ker \pi$ is free of rank at most $n-1$. Since a direct sum of two free modules is free, with rank equal to the sum of the ranks of the summands, we have shown that N is free of rank at most n. □

Corollary 14.9. *Let R be a principal ideal domain and let M be a finitely generated free R-module. If $M \cong A \oplus B$ then A and B are free R-modules and* $\operatorname{rank} A + \operatorname{rank} B = \operatorname{rank} M$.

Lemma 14.10. *Let R be a principal ideal domain and let M be a finitely generated free R-module with basis $e_1, \ldots, e_n$. Let $r_1, \ldots, r_n$ be elements of R and set $x = r_1 e_1 + \cdots + r_n e_n$. There exists a homomorphism $\psi : M \to R$ such that $\psi(x)$ is the greatest common divisor of $r_1, \ldots, r_n$.*

Proof. Let d be the greatest common divisor of $r_1, \ldots, r_n$. Write $d = s_1 r_1 + \cdots + s_n r_n$. Define ψ to be the unique homomorphism from M to R such that $\psi(e_i) = s_i$ for $i = 1, \ldots, n$. □

Proposition 14.11. *Let R be a principal ideal domain and let M be a finitely generated R-module of rank n. Suppose that N is a submodule of M. Then there exists a basis $\{e_1, \ldots, e_n\}$ of M, and $k \leq n$ elements $a_1, \ldots, a_k$ of R with $a_1 | a_2 \cdots | a_k$, such that $\{a_1 e_1, \ldots, a_k e_k\}$ is a basis of N.*

Proof. The proof is by induction on n. Start by fixing some arbitrary basis $f_1, \ldots, f_n$ of M.

Consider the following collection of ideals in R:

$$\{\phi(N) \mid \phi : M \to R \text{ is a homomorphism}\}.$$

(By definition, an ideal in R is a submodule of R as an R-module, so $\phi(N)$ is an ideal for any R-module homomorphism $\phi : M \to R$.) Since any PID is Noetherian, this collection has a maximal element (a_1). Choose $x \in N$ so that $\phi(x) = a_1$ and write $x = r_1 f_1 + \ldots + r_n f_n$.

Next we will show that a_1 is a greatest common divisor of $r_1, \ldots, r_n$. According to Lemma 14.10 there is a homomorphism $\psi : M \to R$ so that $\psi(x)$ is a greatest common divisor of $r_1, \ldots, r_n$. But $a_1 = \phi(x) = r_1 \phi(f_1) + \cdots + r_n \phi(f_n)$, so we have $a_1 \in (r_1, \ldots, r_n)$. Thus

$$\phi(N) = (a_1) \subseteq (r_1, \ldots, r_n) = (\psi(x)) \subseteq \psi(N).$$

Thus, by the maximality of $\phi(N)$, we have $(a_1) = (r_1, \ldots, r_n)$.

Since we have shown that a_1 divides r_i for all i, we may now write $x = a_1 y$ for some $y \in M$. This implies that $\phi(y) = 1$. According to Lemma 14.7 we have $M \cong Ry \oplus \ker \phi$.

By induction, there is a basis $e_2, \ldots, e_n$ of $\ker \phi$ and elements $a_2, \ldots, a_n \in R$ such that $N \cap \ker \phi$ is generated by $a_2 e_2, \ldots, a_n e_n$. Set $e_1 = y$. Since $M = \ker \phi \oplus Ry$, we have that $e_1, \ldots, e_n$ is a basis of M. If we apply Lemma 14.7 to the restriction of ϕ to N, we have $N \cong \ker(\phi|_N) \oplus Rx = (N \cap \ker \phi) \oplus Rx$. Since $x = a_1 e_1$, this implies that $a_1 e_1, \ldots, a_n e_n$ is a basis of N.

To complete the proof we must show that $a_1 | a_2$. The element $z = a_1 e_1 + a_2 e_2$ is contained in the submodule N. Another application of Lemma 14.10 shows that there is a

homomorphism $\psi' : M \to R$ such that $\psi'(z)$ is the greatest common divisor of a_1 and a_2. Once again we have

$$\phi(N) = (a_1) \subseteq (a_1, a_2) = (\psi(z)) \subseteq \psi(N),$$

so the maximality of $\phi(N)$ implies that $(a_1) = (a_1, a_2)$. Thus $a_1 | a_2$. $\square$

Index of Definitions