Chapter 2

Rings and Modules

2.1 Rings

Definition 2.1.1. *A **ring** consists of a set R together with binary operations $+$ and $\cdot$ satisfying:*

1. $(R, +)$ *forms an abelian group,*
2. $(a \cdot b) \cdot c = a \cdot (b \cdot c)\ \forall a, b, c \in R$,
3. $\exists 1 \neq 0 \in R$ *such that* $a \cdot 1 = 1 \cdot a = a\ \forall a \in R$, *and*
4. $a \cdot (b + c) = a \cdot b + a \cdot c$ *and* $(a + b) \cdot c = a \cdot c + b \cdot c\ \forall a, b, c \in R$.

Note:

1. Some people (e.g. Dummit + Foote) do not require condition 3, and refer to a "ring with identity" if they want to assume $\cdot$ has an identity element.
2. People who include existence of a unit in their defn. of a ring refer to a "ring without identity" for an object satisfying the other three axioms. Some people (e.g. Jacobson) call this a "rng".
3. Some people (e.g. Lang) do not require $1 \neq 0$ in condition 3.

Definition 2.1.2. *R is called **commutative** if its multiplication is commutative, ie.*

$$ab = ba \quad \forall a, b \in R.$$

Definition 2.1.3. *A **ring homomorphism** from R to S is a function $f : R \mapsto S$ such that $\forall a, b \in R$:*

1. $f(a + b) = f(a) + f(b)$,

2. $f(ab) = f(a)f(b)$, and

3. $f(1) = 1$.

A bijective ring homomorphism is called an ***isomorphism****.*

Definition 2.1.4. *A* ***subring*** *of R is a subset A which forms a ring such that the inclusion $A \hookrightarrow R$ is a ring homomorphism. A subgroup I of the abelian group $(R, +)$ is called a (two -sided)* ***ideal*** *if*

$$x \in I, r \in R \Rightarrow \ rx \in I \text{ and } xr \in I.$$

Similarly if a subgroup I satisfies

$$x \in I, r \in R \Rightarrow \ rx \in I,$$

I is called a ***left ideal****, and if it satisfies*

$$x \in I, r \in R \Rightarrow \ xr \in I,$$

it is called a ***right ideal****.*

Example 2.1.5. *If $f : R \mapsto S$ is a homomorphism then* $\ker f := \{x \in R \mid f(x) = 0\}$ *is an ideal in R. (An ideal is always a subrng but never a subring, unless it is all of R.)*

Theorem 2.1.6. *Let $I \subsetneq R$ be a proper ideal. Then $\exists$ a ring R/I and a surjective ring homomorphism $f : R \mapsto\!\!\!\!\twoheadrightarrow R/I$ such that* $\ker f = I$.

Proof. Define an equivalence relation on R by $x \sim y \iff x - y \in I$. Let

$$R/I := \{\text{equiv. classes}\}.$$

Define operations on R/I by

$$[x] + [y] := [x + y],$$
$$[x] \cdot [y] := [xy].$$

Check that these are well-defined and produce a ring structure on R/I.

Define $f : R \mapsto R/I$ by $f(x) = [x]$. f is a ring homomorphism. Moreover, $f(x) = 0$ iff $[x] = 0$ iff $x = x - 0 \in I$. $\square$

Definition 2.1.7. *The ring R is called a* ***division ring*** *if $(R - \{0\}, \cdot)$ forms a group. A commutative division ring is called a* ***field****.*

An element $u \in R$ for which $\exists v \in R$ such that $uv = vu = 1$ is called a **unit**.

Notation: $R^\times = \{\text{units of R}\}$. This forms a group under multiplication.

A non-zero element $x \in R$ is called a **zero divisor** if $\exists y \neq 0$ such that either $xy = 0$ or $yx = 0$. A commutative ring with no zero divisors is called an **integral domain**.

Proposition 2.1.8. *If $x \neq 0$ is not a zero divisor and $xy = xz$ then $y = z$.*

Proof. $x(y - z) = 0$ and x is not a zero divisor so either $x = 0$ or $y - z = 0$. But $x \neq 0$ so $y = z$. □

Theorem 2.1.9 (First Isomorphism Theorem)**.** *Let $f : R \mapsto S$ be a ring homomorphism. Then $R/\ker f \cong \operatorname{Im} f$.*

Theorem 2.1.10 (Second Isomorphism Theorem)**.** *Let $A \subset R$ be a subring and let $I \subsetneq R$ be a proper ideal. Then $A + I := \{a + x \mid a \in A, x \in I\}$ is a subring of R, $A \cap I$ is a proper ideal in A, and*

$$(A + I)/I \cong A/(A \cap I).$$

Theorem 2.1.11 (Third Isomorphism Theorem)**.** *Let $I \subset J$ be proper ideals of R. Then $J/I := \{[x] \in R/I \mid x \in J\}$ is an ideal in R/I, and*

$$\frac{R/I}{J/I} \cong R/J.$$

Theorem 2.1.12 (Fourth Isomorphism Theorem)**.** *Let I be a proper ideal of R. Then the correspondence $J \mapsto J/I$ is a bijection between the ideals of J containing I and the ideals of R/I.*

Let I, J be ideals in R. Define ideals

$$\begin{aligned} &I + J := \{x + y \mid x \in I, y \in J\}, \\ &I \cap J, \\ &IJ := \left\{ \sum_{i=1}^{n} x_i y_y \mid n \in \mathbb{N}, x_i \in I, y_i \in J \right\} \end{aligned}$$

Then

$$IJ \subset I \cap J \subset I \cup J \subset I + J.$$

(Note that $I \cup J$ may not be an ideal.) $I + J$ is the smallest ideal containing both I and J.

2.2 Maximal and Prime Ideals

Definition 2.2.1. *An ideal $M \subsetneq R$ is called a* **maximal ideal** *if $\nexists$ an ideal I s.t. $M \subsetneq I \subsetneq R$.*

Lemma 2.2.2. *Given an ideal $I \subsetneq R$, $\exists$ a maximal ideal M s.t. $I \subset M$.*

Proof. Let
$$\mathcal{S} = \{\text{ideals } J \mid I \subset J \subsetneq R\}.$$
Then $\mathcal{S}$ is a partially ordered set (ordered by inclusion). If $C \subset \mathcal{S}$ is a chain (ie. a totally ordered subset) then
$$J = \bigcup_{C \in \mathcal{C}} C$$
is an ideal which forms an upper bound for $\mathcal{C}$ in $\mathcal{S}$ (it is indeed a proper ideal since $1 \notin J$).
$\therefore$ Zorn's Lemma $\Rightarrow \mathcal{S}$ has a maximal element M. □

For the rest of this section, suppose that R is commutative.

Proposition 2.2.3. *R is a field $\iff$ the only ideals of R are $\{0\}$ and R.*

Proof.

$\Rightarrow$: Let R be a field and let $I \subset R$ be an ideal. If $I \neq \{0\}$ then $\exists x \neq 0 \in I$.
R a field $\Rightarrow \exists y \in R$ such that $xy = yx = 1$. Since I is an ideal, $1 \in I$, so $r \in I$ $\forall r \in R$. Thus $I = R$.

$\Leftarrow$: Suppose the only ideals in R are $\{0\}$ and R. Let $x \neq 0 \in R$. Let
$$I = Rx := \{rx \mid r \in R\}.$$
I is an ideal and $x = 1x \in R$, so $I \neq 0$. Hence $I = R$, so $1 \in I$. ie. $1 = yz$ for some $y \in R$.

$\therefore$ Every $x \neq 0 \in R$ has an inverse, so R is a field.

□

Corollary 2.2.4. *Let $f : F \mapsto S$ be a ring homomorphism where F is a field. Then f is injective.*

Proof. $\ker f$ is a proper ideal in F, so $\ker f = 0$. □

Theorem 2.2.5. *M is a maximal ideal $\iff R/M$ is a field.*

Proof. The 4$^{\text{th}}$ iso. thm. says $\exists$ a bijection between the ideals of R containing M and the ideals of R/M.
$\therefore \exists I$ s.t. $M \subsetneq I \subsetneq R \iff \exists J$ s.t. $\{0\} \subsetneq J \subsetneq R/M$. ie. M is not maximal $\iff R/M$ is not a field. □

Definition 2.2.6. *An ideal $\mathcal{P} \subsetneq R$ is called a **prime ideal** if $ab \in \mathcal{P}$ implies $a \in \mathcal{P}$ or $b \in \mathcal{P}$.*

Theorem 2.2.7. *$\mathcal{P}$ is a prime ideal $\iff R/\mathcal{P}$ is an integral domain.*

Proof.

$\Rightarrow$: Suppose $\mathcal{P}$ is a prime ideal. If $[xy] = [x][y] = 0$ in $R/\mathcal{P}$ then $xy \in \mathcal{P}$, so either $x \in \mathcal{P}$ or $y \in \mathcal{P}$. ie. either $[x] = 0$ or $[y] = 0$. Thus $R/\mathcal{P}$ has no zero divisors.

$\Leftarrow$: Suppose $R/\mathcal{P}$ is an integral domain. If $xy \in \mathcal{P}$ then $[x][y] = 0$ in $R/\mathcal{P}$, so $[x] = 0$ or $[y] = 0$. ie. either $x \in \mathcal{P}$ or $y \in \mathcal{P}$.

□

Corollary 2.2.8. *A maximal ideal is a prime ideal.*

Proof. A field is an integral domain. □

Notation: $a \mid b$ means $\exists c$ s.t. $b = ac$ (say a **divides** b).

Proposition 2.2.9. *In an integral domain, if $a \mid b$ and $b \mid a$ then $b = ua$ for some unit u.*

Proof. $a \mid b \Rightarrow\ b = ua$ for some $u \in R$. $b \mid a \Rightarrow\ a = vb$ for some $v \in R$.
$\therefore b = ua = uvb$, and since b is not a zero divisor, $1 = uv$. Thus, u is a unit. □

Definition 2.2.10. *q is called a **greatest common divisor** of a and b if:*

1. *$q \mid a$ and $q \mid b$, and*
2. *If c also satisfies $c \mid a, c \mid b$ then $c \mid q$.*

Notation: $q = \gcd(a, b)$ means q is the greatest common divisor of a and b.
We say a and b are **relatively prime** if $\gcd(a, b) = 1$.

Proposition 2.2.11. *Let R be an integral domain. If $q = \gcd(a, b)$ and $q' = \gcd(a, b)$ then $q' = uq$ for some unit u. Conversely, if $q = \gcd(a, b)$ and $q' = uq$ where u is a unit then $q' = \gcd(a, b)$.*

Proof. Let $q = \gcd(a, b)$. If $q' = \gcd(a, b)$ then $q' \mid q$ and $q \mid q'$ so $q' = uq$ for some unit u.
Conversely, if $q' = uq$ for some unit u then $q' \mid q$ so $q' \mid a$ and $q' \mid b$. Also $q \mid q'$ so whenever $c \mid a$ and $c \mid b$, $c \mid q$ so $c \mid q'$. □

Definition 2.2.12. *A non-unit $p \neq 0 \in R$ is called a **prime** if $p \mid ab \Rightarrow\ p \mid a$ or $p \mid b$.*

Notation: Let $x \in R$. $(x) := Rx = \{rx \mid r \in R\}$ is called the **principal ideal** generated by x. Thus $y \in (x)$ iff $x \mid y$.

Likewise, for $x_1, \ldots, x_n \in R$, let $(x_1, \ldots, x_n)$ denote the following ideal:

$$\{r_1 x_1 + \cdots + r_n x_n \mid r_1, \ldots, r_n \in R\},$$

ie. the ideal generated by $x_1, \ldots, x_n$.

Proposition 2.2.13. *If $p \neq 0$ then p is prime $\iff (p)$ is a prime ideal.*

Proof.

$\Rightarrow$: Suppose p is prime. If $ab \in (p)$ then $ab = rp$ for some r, so $p \mid ab$. So $p \mid a$ or $p \mid b$. ie. $a \in (p)$ or $b \in (p)$.

$\Leftarrow$: Suppose (p) is a prime ideal. If $p \mid ab$ then $ab \in (p)$ so $a \in (p)$ or $b \in (p)$.

$\therefore p \mid a$ or $p \mid b$.

□

Nonzero elements x and y are called **associates** if $\exists$ a unit u s.t. $x = uy, y = u^{-1}x$. Thus, x, y are associate $\iff (x) = (y)$. ie. For associates x and y, $x \mid a$ iff $y \mid a$.

$x \sim y$ iff x, y are associate forms an equivalence relation on $R - \{0\}$.

Definition 2.2.14. *$x \in R$ is **irreducible** if $x \neq 0$, x is not a unit, and whenever $x = ab$, either a is a unit or b is a unit.*

Definition 2.2.15. *Ideals I and J are called **comaximal** or **relatively prime** if $I + J = R$.*

Theorem 2.2.16 (Chinese Remainder Theorem)**.** *Let R be a commutative ring. Let*

$$I_1, \ldots, I_k \subset R$$

be ideals. Suppose I_i and I_j are comaximal whenever $i \neq j$. Let

$$\begin{aligned} \phi : R &\mapsto R/I_1 \times R/I_2 \times \cdots \times R/I_k \\ r &\mapsto (r + I_1, r + I_2, \ldots, r + I_k). \end{aligned}$$

Then ϕ is surjective and

$$\ker \phi = I_1 \cap I_2 \cap \cdots \cap I_k = I_1 \cdots I_k.$$

Proof. Consider first the case when $k = 2$. Suppose I, J are comaximal. Then $\exists x \in I, y \in J$ s.t. $x+y = 1$. So $\phi(x) = (0, 1)$ and $\phi(y) = (1, 0)$. Since $(0, 1)$ and $(1, 0)$ generate $R/I \times R/J$, ϕ is surjective.

Clearly $\ker \phi = I \cap J$, and in general, $IJ \subset I \cap J$. For any $c \in I \cap J$,

$$c = c1 = cx + cy \in IJ.$$

$\therefore IJ = I \cap J$.

General case: set $I = I_1$, $J = I_2 \cdots I_k$. For each $i = 2, \ldots, k$, $\exists x_i \in I$ and $y_i \in I_i$ s.t. $x_i + y_i = 1$. Since $x_i + y_i \equiv y_i \mod I$,

$$1 = 1 \cdots 1 = (x_2 + y_2)(x_3 + y_3) \cdots (x_k + y_k) \equiv y_2 \cdots y_k \mod I$$

So $1 \in I + J$.
$\therefore R \twoheadrightarrow R/I \times R/J$ and by induction,

$$R/I \times R/J \twoheadrightarrow R/I_1 \times R/I_2 \times R/I_3 \times \cdots \times R/I_k$$

and

$$I_1 I_2 \cdots I_k = IJ = I \cap J = I_1 \cap I_2 \cap \cdots I_k.$$

□

2.3 Polynomial Rings

Let R be a ring.

$$R[x] := \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \mid n \geq 0 \in \mathbb{Z} \text{ and } a_j \in R \text{ for } j = 0, \cdots, n\}$$

(modulo $0x^n + a_{n-1}x^{n-1} + \cdots + a_0 \sim a_{n-1}x^{n-1} + \cdots + a_0$). Operations are

$$\sum_{i=1}^{n} a_i x^i + \sum_{i=1}^{n} b_i x^i := \sum_{i=1}^{n} (a_i + b_i) x^i, \quad \text{and}$$
$$\left(\sum_{i=1}^{n} a_i x^i\right)\left(\sum_{i=1}^{m} b_i x^i\right) := \sum_{k=0}^{n+m} \left(\sum_{i=0}^{k} a_i b_{k-i}\right) x^k.$$

More formally,

$$(R[x], +) = \bigoplus_{n=0}^{\infty} R,$$

with multiplication defined by

$$(a_i)_{i\geq 0}(b_j)_{j\geq 0} = (c_k)_{k\geq 0} \quad \text{where } c_k = \sum_{i=0}^{k} a_i b_{k-i}.$$

Inductively, set

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

(called the **polynomial ring in n variables**). For an arbitrary set S, set

$$R[S] := \bigcup_{T = \text{finite subset of } S} R[T].$$

If $q(x) = \sum_{i=0}^{n} a_i x^i$ and $a_n \neq 0$ then n is called the **degree** of q. Embed $R \hookrightarrow R[x]$ via

$$r \mapsto r \quad \text{(polynomial of degree 0)}.$$

Some properties:

1. $R[x]$ is commutative $\iff R$ is commutative.
2. $R[x]$ is an integral domain $\iff R$ is an integral domain.
3. If R is an integral domain then $q(x) \in R[x]$ is invertible $\iff q(x) \in R$ and is invertible in R.

Proposition 2.3.1. *Let $I \subset R$ be an ideal. Let $I[x]$ denote the ideal of $R[x]$ generated by I. Then $R[x]/I[x] \cong (R/I)[x]$.*

Proof. Define $\phi : R[x] \mapsto (R/I)[x]$ by

$$\phi(\sum a_i x^i) := \sum \overline{a_i} x^i.$$

Then ϕ is onto and $\ker \phi = I[x]$, so

$$R[x]/I[x] \cong (R/I)[x].$$

$\square$

Corollary 2.3.2. *$I[x]$ is a prime ideal $\iff$ I is a prime ideal.*

2.4 Modules

Definition 2.4.1. *Let R be a ring. A (left) R-**module** consists of an abelian group $(M,+)$, together with a function $\cdot : R \times M \mapsto M$ s.t.*

1. $(r+s)m = rm + sm\ \forall r,s \in R, m \in M$,
2. $r(m+n) = rm + rn\ \forall r \in R, m,n \in M$,
3. $(rs)m = r(sm)\ \forall r,s \in R, m \in M$, *and*
4. $1m = m\ \forall m \in M$.

*If R is a field, an R-module is also called a **vector space** over R.*

Definition 2.4.2. *An R-**module homomorphism** $f : M \mapsto N$ is a function satisfying*

1. $f(a+b) = f(a) + f(b)\ \forall a,b \in M$ *and*
2. $f(ra) = rf(a)\ \forall r \in R, a \in M$.

*If R is a field, an R-module homomorphism is also called a **linear transformation**. A bijective homomorphism is called an **isomorphism**.*

Definition 2.4.3. *A **submodule** of M is a subset A which forms an R-module s.t. the inclusion $A \hookrightarrow M$ is an R-module homomorphism. The R-module M is **simple** if its only submodules are M and $\{0\}$.*

Example 2.4.4.

1. *$M = R$ with $R \times M \mapsto M$ given by mult. in R. Submodules of R are left ideals.*
2. *$R = \mathbb{Z}$ and $M =$ abelian grp., with*

$$n \cdot x := x + \cdots + x, \quad \text{for } n \geq 0, \text{ and}$$
$$(-n) \cdot x := -(n \cdot x), \quad \text{for } n \geq 0.$$

   Conversely, any $\mathbb{Z}$-module is just an abelian group.

3. *F a field, V a vector space over F, $T : V \mapsto V$ a linear transformation. Let $R = F[x]$ and $M = V$. Define*

$$x^n \cdot v := T^n(v) = T(T^{n-1}v) \quad \forall v \in V$$

   and extend linearly to an action of $F[x]$ on V.

If $f : M \mapsto N$ is an R-module homomorphism then $\ker f$ is a submodule of M and $\mathrm{Im} f$ is a submodule of R. If M, N are R-modules, set

$$\hom_R(M,N) := \{R\text{-module homomorphisms from } M \text{ to } N\}.$$

$\hom_R(M,N)$ is an abelian group in general, and if R is commutative, it becomes an R-module via

$$(rf)(m) = f(rm).$$

Let N be a submodule of M. On the abelian group M/N, define the action of R by $r \cdot \overline{m} := \overline{r \cdot m}$. This is well-defined and produces an R-module structure on M/N.

Theorem 2.4.5.

1. *First Isomorphism Theorem*
   Let $f : M \mapsto N$ be an R-module homomorphism. Then $M/\ker f \cong \mathrm{Im} f$.

2. *Second Isomorphism Theorem Let A, B be submodules of M. Then*

$$(A+B)/B \cong A/(A \cap B)$$

   where $A + B = \{a + b \mid a \in A, b \in B\}$, which itself forms a submodule.

3. *Third Isomorphism Theorem Let $A \subset B \subset M$ be R-modules. Then*

$$\frac{M/A}{B/A} \cong M/B.$$

4. *Fourth Isomorphism Theorem Let $N \subset M$ be R-modules. Then $A \leftrightarrow A/N$ sets up a bijection between the submodules of M containing N and the submodules of M/N.*

A sequence

$$0 \longrightarrow A \xrightarrow{j} B \xrightarrow{f} C \longrightarrow 0$$

of R-module homomorphisms s.t. j is injective, f is surjective, and $\ker f = \mathrm{Im} j$ is called a **short exact sequence** of R-modules. 1^{st} iso. thm. $\Rightarrow C \cong B/\mathrm{Im} j$.

Proposition 2.4.6. *Let*

$$0 \longrightarrow A \xrightarrow{j} B \xrightarrow{f} C \longrightarrow 0$$

be a short exact sequence of R-modules. Then TFAE:

1. $\exists s : C \mapsto B$ *s.t.* $fs : C \mapsto C$ *is an isomorphism.*

2. $\exists r : B \mapsto A$ *s.t.* $rj : A \mapsto A$ *is an isomorphism.*

3. $B \cong A \oplus C$.

Remarks:

1. The fact that the above are isomorphic as abelian groups was discussed in the section on semidirect products, since for abelian groups, all subgroups are normal and semidirect products become products.

2. As discussed in semidirect product section, $2 \iff 3$, even for nonabelian groups, but in that situation, $1 \not\Rightarrow 2$ or 3.

Given a set S, $\exists$ an R-module M having the property that for any R-module M,

$$\hom_R(M, N) = \text{morphisms}_{\text{sets}}(S, N).$$

ie. An R-module homomorphism from M is uniquely determined by the images of the elts. of S. Explicitly,

$$M \cong R^S \equiv \bigoplus_S R.$$

M is called the **free R-module** with basis S. An R-module which possesses a basis is called a free R-module. An arbitrary elt. of a free R-module can be uniquely written as a finite linear combination

$$x = \sum r_i s_i$$

where $r_i \in R$ and $s_i \in S$. When $R = \mathbb{Z}$, the free $\mathbb{Z}$-module on S is also called the **free abelian group** on S, denoted $F_{ab}(S)$.

Let M be a right R-mod. and let N be a left R-mod. Define an abelian group $M \otimes_R N$ (tensor product of M, N over R) by

$$M \otimes_R N = F_{ab}(M \times N)/\sim$$

where

1. $(m, n_1 + n_2) \sim (m, n_1) + (m, n_2)\ \forall m \in M, n_1, n_2 \in N$,

2. $(m_1 + m_2, n) \sim (m_1, n) + (m_2, n)\ \forall m_1, m_2 \in M, n \in N$, and

3. $(m \cdot r, n) \sim (m, r \cdot n)\ \forall r \in R, m \in M, n \in N$.

Write $m \otimes n$ for the equiv. class of (m, n) in $M \otimes_R N$. So an arbitrary elt. of $M \otimes_R N$ has the form

$$\sum_{i=1}^{k} c_i(m_i \otimes n_i)$$

where $m_i \in M, n_i \in N, c_i \in \mathbb{Z}$.

Note that $R \otimes_R N \cong N$ and $M \otimes_R R \cong M$.

$M \otimes_R N$ has the universal property: q is R-bilinear and given bilinear $f : M \times N \mapsto A$,

$$\begin{tikzcd} M \times N \arrow[r, two heads, "q"] \arrow[dr, "f"'] & M \otimes_R N \arrow[d, dashed, "\exists ! \overline{f}"] \\ & A \end{tikzcd}$$

f bilinear means:

$$\begin{aligned} f(m_1 + m_2, n) &= f(m_1, n) + f(m_2, n), \\ f(m, n_1 + n_2) &= f(m, n_1) + f(m, n_2), \quad \text{and} \\ f(mr, n) &= f(m, rn) \end{aligned}$$

If R is commutative then $M \otimes_R N$ becomes an R-module via

$$r \cdot (m \otimes n) := m \otimes (r \cdot n).$$

More generally, if M is an R-bimodule (ie. has both a left and a right R-module action which commute with each other) then $M \otimes_R N$ becomes a left R-module via

$$r \cdot (m \otimes n) := (r \cdot m) \otimes n.$$

Notice that R is an R-bimodule even if R is not commutative. (ie. Left multiplication commutes with right multiplication – R is associative.)

More generally, let $f : R \mapsto S$ be a ring homomorphism. Then S becomes an R-bimodule via

$$\begin{aligned} r \cdot s &:= f(r)s \\ s \cdot r &:= sf(r) \end{aligned}$$

This induces a map from R-modules to S-modules given by $N \mapsto S \otimes_R N$.

Example 2.4.7 (Extension of Coefficients)**.** *Let N be a vector space over a field F. Let $F \hookrightarrow K$ be an extension field. Elts. of N are finite sums*

$$\sum a_i e_i$$

where $\{e_i\}_{i\in T}$ forms a basis for N. Then elts. of $K \otimes_F N$ are finite sums

$$\sum a_i e_i$$

where $a_i \in K, i \in T$. (So $\{e_i\}$ forms a basis for $K \otimes_F N$ as a vector space over K.)

In general,

$$M \otimes_R (\bigoplus_{i\in T} N_i) \cong \bigoplus_{i\in T}(M \otimes_R N_i),$$

so

$$S \otimes_R (\bigoplus_{i\in T} R) \cong \bigoplus_{i\in T}(S \otimes_R R) \cong \bigoplus_{i\in T} S.$$

Thus if N is a free R-module with basis T then $S \otimes_R N$ forms a free S-module with basis T.

Theorem 2.4.8 (Steinitz Exchange Theorem)**.** *Let R be a commutative ring. Let B and T be bases for a free R-module N. Then* $\mathrm{Card} B = \mathrm{Card} T$.

Proof. If $g : R \mapsto S$ is any ring homomorphism then $S \otimes_R N$ is a free S-module with both B and T as bases. Letting $g : R \mapsto\!\!\!\rightarrow R/M$ where M is a maximal ideal in R, we may reduce to the case where R is a field.

Case I: At least one of $\mathrm{Card} B, \mathrm{Card} T$ is finite. Say $\mathrm{Card} B \le \mathrm{Card} T$ and suppose $\mathrm{Card} B < \infty$. Write $B = \{b_1, \dots, b_n\}$. $\exists t_1 \in T$ s.t. when t_i is written in the basis B, the coeff. of b_1 is nonzero (or else $b_2, \dots, b_n$ would span N). Then $\{t_1, b_2, \dots, b_n\}$ forms a basis for N. Inductively, $\forall j = 1, \dots, n$, find t_j s.t. $\{t_1, \dots, t_j, b_{j+1}, \dots, b_n\}$ forms a basis for N. Then $\{t_1, \dots, t_n\}$ forms a basis for N, so

$$T = \{t_1, \dots, t_n\}$$

and $|T| = |B|$.

Case II: Both $\mathrm{Card} B$ and $\mathrm{Card} T$ are infinite. For each $b \in B$, set

$$T_b = \{\text{elts. of } T \text{ occuring in the expression for } b \text{ in basis } T\} \in 2^T.$$

Then T_b is finite $\forall b$. Define $f : B \mapsto 2^T$ by $f(b) = T_b$. If $X \subset T$ is finite with say $|X| = n$, at most n elts. of B lie in the span of X. So $|f^{-1}(X)| \le |X|$.

$$B = \bigcup_{\substack{X \subset T \\ X \text{ finite}}} f^{-1}(X) = \bigcup_{n=1}^{\infty} \bigcup_{\substack{X \subset T \\ |X| = n}} f^{-1}(X).$$

Since T is infinite, the cardinality of

$$\{X \subset T \mid |X| = n\}$$

is equal to the cardinality of $|T|$. Since $|f^{-1}(X)| \leq |X|$,

$$\begin{aligned}
\mathrm{Card} B &= \mathrm{Card} \bigcup_{n=1}^{\infty} \bigcup_{\substack{X \subset T \\ |X| = n}} f^{-1}(X) \\
&\leq \mathrm{Card}(\bigcup_{n=1}^{\infty} \mathrm{Card} T) \\
&= \mathrm{Card} T.
\end{aligned}$$

Similarly, $\mathrm{Card} T \leq \mathrm{Card} B$.

□

Note: Once we reduced to the case of a division ring, we no longer needed the commutativity of R, so the thm. also holds whenever R is a division ring, or indeed when R admits a homomorphism to a division ring. However, we used commutativity of R to produce our map $R \mapsto$ (division ring), since

$$R/\text{2-sided max. ideal}$$

need not be a division ring if R is not commutative.

If R is a commutative ring and N is a free R-module, the cardinality of any basis for N is called the **rank** of N. If R is a field then every R-module is free and its rank is called its **dimension**.

Proposition 2.4.9. *If $\phi : M \twoheadrightarrow N$ is a surjective R-module homomorphism and N is a free R-module then $\exists$ an R-module homomorphism $s : N \mapsto M$ s.t. $\phi s = 1_N$. In particular, $M \cong N \oplus \ker \phi$.*

Proof. Let S be a basis for N. For each $x \in S$, choose $m \in M$ s.t. $\phi(m) = x$ and set $s(x) = m$. Since N is free, this extends (uniquely) to an R-module map. □

An R-module P is called **projective** if given a surjective R-mod. homom. $\phi : M \mapsto P$, $\exists$ an R-mod. homom. $s : P \mapsto M$ s.t. $\phi s = 1_P$. Equivalently, P is surjective iff $\exists Q$ s.t. $P \oplus Q \cong R^N$ for some N. Equivalently, P is projective iff

$$\begin{tikzcd} P \arrow[d, dashed, "\exists s"'] \arrow[dr, "\theta"] & & \\ M \arrow[r, two heads, "f"] & N \arrow[r] & 0 \end{tikzcd}$$

$\exists$ a lift s (not necessarily unique).
$\therefore$ Free $\Rightarrow$ Projective.

Example 2.4.10 (A projective module which is not free)**.** *Let $R = M_{n\times n}(F)$ ($n\times n$ matrices with entries in a field F), with $n > 1$. Let*

$$P = \begin{pmatrix} * & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ * & 0 & \cdots & 0 \end{pmatrix}$$

(matrices which are 0 beyond the first column). Then P forms a left ideal in R, ie. P is a left R-module.

Let

$$Q = \begin{pmatrix} 0 & * & \cdots & * \\ \vdots & \vdots & & \vdots \\ 0 & * & \cdots & * \end{pmatrix}$$

(matrices which are 0 in the first column). Then $P \oplus Q = R$, so P is projective. But P is not free, because if $P \cong R^s$ then, regarded as vector spaces over F, we would have

$$n = \dim P = \dim R^s = sn^2.$$

This is a contradiction since $n > 1$.

Definition 2.4.11. *Let R be an integral domain. An elt. x in an R-module M is called a **torsion element** if $\exists r \neq 0 \in R$ s.t. $rx = 0$. M is called a **torsion module** if x is a torsion elt. $\forall x \in M$. M is called **torsion-free** if it has no torsion elements.*

x, y torsion elts. $\Rightarrow$ $x + y$ is a torsion elt. If x is a torsion elt. and $r \in R$ then rx is a torsion elt. Hence,

$$\mathrm{Tor} M := \{x \in M \mid x \text{ is a torsion elt.}\}$$

forms a submodule of M.

The **annihilator** of $x \in M$ is the left ideal

$$\mathrm{Ann}(x) := \{r \in R \mid rx = 0\}.$$

The **annihilator** of M is the 2-sided ideal

$$\mathrm{Ann}M := \{r \in R \mid rx = 0 \ \forall x \in M\}.$$

2.5 Localization and Field of Fractions

From the 4th isomorphism theorem we get:

Proposition 2.5.1. *A left ideal I is maximal if and only if the quotient module R/I is a simple (left) R-module.*

Note: It is important to remember that R/I (when I is a left ideal) is a quotient module and not (necessarily) a quotient ring.

Definition 2.5.2. *A ring with a unique maximal left ideal is called a* ***local ring****.*

While it appears initially that replacing "left ideal" by "right ideal" might give a different concept, as we shall see, "left local" equals "right local". That is, a ring has a unique maximal left ideal if and only if it has a unique maximal right ideal. Note however that while, as we shall see, a unique maximal left ideal must in fact be a 2-sided ideal, the existence of a unique maximal 2-sided ideal is not sufficient to guarantee that a ring be local. For example, when $n > 1$, $\{0\}$ forms a unique maximal ideal for matrix rings $M_{n\times n}(F)$ over a field F, but these rings are not local since they contain nontrivial left ideals, as we saw in the previous section.

Theorem 2.5.3. *Let R be a local ring with max. left ideal M. Then M is a 2-sided ideal.*

Proof. Suppose $y \in R$. Must show $My \subset M$. If $y \in M$ this is trivial since M is a left ideal, so assume $y \notin M$. Let $I_y := \{x \in R \mid xy \in M\}$. To finish the proof, we must show that $M \subset I_y$.

For $r \in R$ and $x \in I_y$, $(rx)y = r(xy) \in rM \subset M$, using that M is a left ideal. Therefore I_y is a left ideal. Note that $1 \notin I_y$, since $y \notin M$. Thus I_y is a proper left ideal so $I_y \subset M$. Let $\bar{y}$ denote the equivalence class of y in the quotient module R/M. Define $\phi : R \to R/M$ by $\phi(r) = r\bar{y}$. Then $\ker\phi = I_y$ by definition of I_y. Since M is maximal, R/M is a simple module, so $\mathrm{Im}\phi = R/M$. Therefore as left R-modules we have $R/I_y \cong \mathrm{Im}\phi = R/M$, which is simple and so I_y is a maximal left R-module. Thus $I_y = M$. □

Corollary 2.5.4. *Let R be a local ring with max. left ideal M. Then*

1. *$x \in R - M$ iff x is a unit.*

2. *R has a unique maximal right ideal.*

3. *The unique maximal right ideal of R is M.*

4. *R/M is a division ring.*

Conversely, if R is a ring with an ideal M s.t. x is a unit $\forall x \in R - M$ then R is a local ring.

Proof. Since no proper ideal can contain a unit, parts (2), (3), and (4) are immediate consequences of part (1).

Given $x \in R - M$, maximality of M shows that $Rx = R$ so $\exists\, y \in R$ such that $yx = 1$. Since M is a 2-sided ideal and $x \in R - M$ it follows that y cannot lie in M. Therefore the same argument applies to y and shows that $\exists\, z \in R$ such that $zy = 1$. But then $z = z(yx) = (zy)x = x$, so y forms a 2-sided inverse to x, establishing (1).

Conversely if every element of $R - M$ is a unit, then the fact that no proper ideal can contain a unit shows that R is a local ring. □

For the rest of this section, suppose that R is commutative.

A subset $S \subset R$ containing 1 and s.t. $0 \notin S$, which is closed under the multiplication of R is called a **multiplicative subset**. For example, let $\mathcal{P} \subset R$ be a prime ideal. Then $R - \mathcal{P}$ is a multiplicative subset. Form a ring called the **localization of** R w.r.t. S, denoted $S^{-1}R$. As a set,

$$S^{-1}R := R \times S/\sim,$$

where $(r, s) \sim (r', s')$ if $\exists t \in S$ s.t. $t(rs' - r's) = 0$. Think of (r, s) as $\frac{r}{s}$. Check $\sim$ is an equiv. reln.:

If $(r, s) \sim (r', s')$ and $(r', s') \sim (r'', s'')$ then

$$\exists t \in S \text{ s.t. } t(rs' - r's) = 0$$
$$\text{and } \exists t' \in S \text{ s.t. } t'(r's'' - r''s') = 0$$

Then

$$s'tt'rs'' = tt'r'ss'' = tt'r''s's$$

ie. $s'tt'(rs'' - r''s) = 0$, (and $s'tt' \in S$) so $(r, s) \sim (r'', s'')$.

Define addition by $(r, s) + (r', s') = (rs' + r's, ss')$. Check + is well-defined: suppose

$$(r', s') \sim (r'', s''), \quad \text{so } tr's'' = tr''s'.$$

Is $(rs' + r's, ss') \sim (rs'' + r''s, ss'')$?

Formally, $s^2tr's'' = s^2tr''s'$ so

$$t\,(ss''(rs' + r's) - ss'(rs'' + r''s) = t(s^2r's'' - s^2r''s) = 0.$$

Define $\cdot$ by $(r, s) \cdot (r', s') = (rr', ss')$ (easy to check $\cdot$ is well-defined). $(S^{-1}R, +, \cdot)$ becomes a commutative ring ring with identity $(1, 1)$.

Define the ring homomorphism

$$\psi : R \mapsto S^{-1}R$$
$$r \mapsto (r, 1)$$

Note that $\psi(s)$ is a unit in $S^{-1}R$ $\forall s \in S$. ie. $(1,s)\psi(s) = (1,s)(s,1) = (s,s) \sim (1,1)$.

$\psi : R \mapsto S^{-1}R$ has the universal property: If $f : R \mapsto A$ is a ring homomorphism s.t. $f(s)$ is a unit in A $\forall s \in S$ then

$$\begin{tikzcd} R \arrow[r, "\psi"] \arrow[dr, "f"'] & S^{-1}R \arrow[d, dashed, "\exists!"] \\ & A \end{tikzcd}$$

Proposition 2.5.5. *If R is an integral domain then $\psi : R \mapsto S^{-1}R$ is injective.*

Proof. Suppose $(r,1) = \psi(r) = 0 = (0,1)$. Then $t(r-0) = 0$ for some $t \in S$, so $r = 0$. $\square$

Note: if R is an integral domain, we can define the equiv. reln. simply by

$$(r,s) \sim (r',s') \text{ iff } rs' = r's$$

Special cases:

1. R an integral domain, $S = R - \{0\}$. Then $S^{-1}R$ is a field called the **field of fractions** of R.

2. $S = R - \mathcal{P}$ where $\mathcal{P}$ is a prime ideal. Then $\psi(\mathcal{P})$ forms an ideal in $S^{-1}R$ and every element of $S^{-1}R$ outside of $\psi(\mathcal{P})$ is invertible (quotient of images of elts. in S).

   $\therefore S^{-1}R$ is a local ring with max. ideal $\psi(\mathcal{P})$. $S^{-1}R$, also written $R_{\mathcal{P}}$, is called the **localization of R at the prime $\mathcal{P}$**.

3. $S = I - \{0\}$, where I is an ideal without 0-divisors. $S^{-1}R$ is sometimes called R with I inverted.

   e.g. $R = \mathbb{Z}$, $I = \mathbb{Z}p$. Then
   $$S^{-1}R = \mathbb{Z}[\frac{1}{p}] = \{\frac{m}{p^t} \in \mathbb{Q}\}$$
   is "$\mathbb{Z}$ with p inverted" or "$\mathbb{Z}$ with $\frac{1}{p}$ adjoined". Sometimes called the localization of $\mathbb{Z}$ **away** from p.

2.6 Noetherian Rings and Modules

Definition 2.6.1. *An R-module M is called **Noetherian** if, given any increasing chain of submodules*

$$M_1 \subset M_2 \subset \cdots \subset M_n \subset \cdots$$

*$\exists N$ s.t. $M_n = M_N$ $\forall n \geq N$. The ring R is called a **Noetherian ring** if it is Noetherian when regarded as an R-module.*

If R is not commutative, notions of Noetherian, "right Noetherian", and "2-sided Noetherian" do not necessarily coincide.

Theorem 2.6.2. *Let R be a ring and let M be a left R-module. Then TFAE:*

1. *M is a Noetherian R-module.*
2. *Every non-empty set of submodules of M contains a maximal element.*
3. *Every submodule of M is finitely generated (and in particular, M is finitely generated).*

Proof.

$1 \Rightarrow 2$: Let Σ be a nonempty collection of submodules of M. Choose $M_1 \in \Sigma$. If M_1 is not maximal in Σ then $\exists M_2 \in \Sigma$ s.t. $M_1 \subsetneq M_2$. Having chosen $M_1, \ldots, M_{n-1}$, if M_{n-1} is not maximal in Σ then $\exists M_n \in \Sigma$ s.t.

$$M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_{n-1} \subsetneq M_n.$$

By hypothesis, no infinite chain of this sort exists, so eventually reach a max. elt.

$2 \Rightarrow 3$: Let N be a submodule of M. Let Σ be the collection of all finitely generated submodules of N. By the hypothesis, Σ contains a maximal element N'. If $N' \neq N$ then pick $x \in N - N'$. Then $\langle N', x\rangle$ is f.g. and properly contains N', which is a contradiction.

$\therefore N' = N$, so N is f.g.

$3 \Rightarrow 1$: Suppose every submod. of M is f.g. Let

$$M_1 \subset M_2 \subset M_3 \subset \cdots$$

be a chain of submodules. Let $N = \bigcup_{i=1}^{\infty} M_i$. Then $N \subset M$ is a submodule, so

$$N = \langle a_1, a_2, \ldots, a_n \rangle$$

for some finite set $a_1, \ldots, a_n \in N$.

Since $a_i \in N$, each $a_i \in M_k$ for some k. So $\exists K$ s.t. M_K contains all of $a_1, \ldots, a_n$. But then $N \subset M_K$, so

$$M_K = M_{K+1} = \cdots = M_{K+m} = \cdots = N.$$

ie. $M_n = M_K \; \forall n \geq K$.

$\square$

Corollary 2.6.3. *Let $f : M \mapsto N$ be an R-module homomorphism. Then M is Noetherian iff* $\ker f$ *and* $\operatorname{Im} f$ *are Noetherian.*

Proof.

⇒: Suppose M is Noetherian. Every submodule of $\ker f$ is a submodule of M, and thus is f.g., so $\ker f$ is Noetherian.

If $A \subset \operatorname{Im} f$ then $f^{-1}(A)$ is a submodule of M, thus f.g. But then the images of the generators of $f^{-1}(A)$ generate A, so A is f.g.

⇐: Suppose $\ker f$ and $\operatorname{Im} f$ are f.g. Let $B \subset M$ be a submodule of M. Let

$$\Delta = f(B) \subset \operatorname{Im} f.$$

Pick a set $\overline{x_1}, \ldots, \overline{x_k}$ of generators for Δ and let $x_1, \ldots, x_k$ be pre-images in B.
Claim. $B = \langle \ker f \cap B, x_1, \ldots, x_k \rangle$.

Proof. Given $b \in B$, $f(b) \in f(B)$ so

$$f(b) = \sum_{i=1}^{n} r_i \overline{x_i}, \quad \text{for some } r_1, \ldots, r_k \in R.$$

Then $f(b - \sum_{i=1}^{n} r_i x_i) = 0$ so

$$b - \sum_{i=1}^{n} r_i x_i \in \ker f \cap B.$$

ie. $b \in \langle \ker f \cap B, x_1, \ldots, x_k \rangle$.

But $\ker f \cap B \subset \ker f$ is f.g., so B is f.g.

$\square$

Corollary 2.6.4. *Let R be Noetherian. Then R/I is Noetherian.*

Proof. It follows from the preceding corollary that R/I is Noetherian when regarded as an R-module. However an increasing chain of R/I-submodules of R/I is also a increasing chain of R-submodules of R/I and so the corollary follows. $\square$

Theorem 2.6.5 (Hilbert Basis Theorem)**.** *Let R be a commutative Noetherian ring. Then $R[x]$ is Noetherian.*

Note: The converse is trivial, since $R \cong R[x]/R[x]x$.

Proof. Let $I \subset R[x]$ be an ideal. Let $L \subset R$ be the set of leading coefficients of elts. in I. That is,

$$L = \{a \in R \mid ax^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 \in I, \text{ for some } c_{n-1}, \ldots, c_0\}.$$

Then L is an ideal in R, so

$$L = (a_1, \ldots, a_n), \quad \text{for some } a_1, \ldots, a_n.$$

For each $i = 1, \ldots, n$, choose $f_i \in I$ s.t. leading coeff. of f_i is a_i. Let $N := \max\{N_1, \ldots, N_n\}$ where $N_i = \deg f_i$. For each $d = 0, \ldots, N-1$, let

$$L_d := \{0\} \cup \{\text{leading coefficients of elts. of } I \text{ of degree } d\}.$$

Then $L_d \subset R$ is an ideal, so

$$L_d = (b_1^{(d)}, \ldots, b_{n_d}^{(d)}), \quad \text{some } b_1^{(d)}, \ldots, b_{n_d}^{(d)} \in I.$$

Let $f_i^{(d)}$ be a polynomial of degree d with leading coeff. $b_i^{(d)}$. To finish the proof, it suffices to show:
Claim. I is generated by

$$\{f_1, \ldots, f_n\} \cup \bigcup_{d=0}^{N-1} \{f_i^{(d)}\}_{i=1,\ldots,n_d}.$$

Proof. Let I' be the ideal generated by this set. If $I' \subsetneq I$ then $\exists f \in I$ of minimal degree s.t. $f \notin I'$. Let $e = \deg f$ and let a be the leading coeff. of f.

Suppose $e \geq N$. $a \in L$ so

$$a = \sum_{i=1}^{n} r_i a_i, \quad \text{for some } r_1, \ldots, r_n \in R.$$

Then

$$\sum_{i=1}^{n} r_i x^{e-N_i} f_i \in I'$$

has degree e and leading coeff. a. So $f - \sum r_i x^{e-N_i} f_i \in I - I'$ has degree less than e, which is a contradiction.

$\therefore e < N$. Hence $a \in L_e$, so

$$a = \sum_{i=1}^{n_e} r_i b_i^{(e)}, \quad \text{for some } r_1, \ldots, r_{n_e} \in R.$$

Then $\sum r_i f_i^{(e)}$ has degree e and leading coeff. a, so $f - \sum r_i f_i^{(e)} \in I - I'$ and has degree less than e. This is a contradiction, so $I = I'$ and I is f.g. $\square$

2.7 Unique Factorization Domains

Note: For the remainder of this chapter, all the rings considered are integral domains, and in particular, are commutative.

$x \in R$ is called **irreducible** if $x \neq 0$, x is not a unit, and whenever $x = ab$, either a is a unit or b is a unit.

Proposition 2.7.1. *In an integral domain, prime $\Rightarrow$ irreducible.*

Proof. Let R be an integral domain. Let $p \in R$ be a prime and suppose $p = ab$. Then $p \mid a$ or $p \mid b$. Say $p \mid a$, so $a = zp$ for some $z \in R$. Thus $p = ab = zpb$ so $1 = zb$.
$\therefore$ b is a unit. Similarly, if $p \mid b$ then a is a unit. Hence p is irreducible. □

Example 2.7.2. *Let*

$$R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \cong \mathbb{Z}[x]/(x^2 + 5).$$

Claim. *2 is irreducible but not prime in R. To see 2 is irreducible, consider $N : R \mapsto \mathbb{Z}$ given by*

$$N(a + b\sqrt{-5}) = |a + b\sqrt{-5}|^2 = a^2 + 5b^2,$$

(the "norm" map). N is not a ring homorphism but $N(yz) = N(y)N(z)$.
$\therefore$ *If $2 = \alpha\beta$ then $4 = N(\alpha)N(\beta)$, so $N(\alpha) \leq 4$ and $N(\beta) \leq 4$. The only elements with norm ≤ 4 are $1, -1, 2, -2$, so*

$$\alpha, \beta \in \{1, -1, 2, -2\}.$$

Since $\alpha\beta = 2$, either $\alpha = \pm 1$ or $\beta = \pm 1$, so 2 is irreducible.

However, in $R/(2)$,

$$(1 + \sqrt{5})^2 = 6 + 2\sqrt{5} \equiv 0$$

so $R/(2)$ has zero divisors.
$\therefore$ *$R/(2)$ is not an integral domain, so 2 is not prime. What are the primes in R?*

Consider first $y \in \mathbb{Z}^+ \subset R$. If y is not prime in $\mathbb{Z}$ then y is reducible so it is not prime in R. We already saw that 2 is not prime in R and since $5 = (-\sqrt{-5})(\sqrt{-5})$ is reducible, 5 is not prime in R. Therefore suppose y is a prime $p \in \mathbb{Z}^+$ with $p \neq 2$ or 5. $R/(y)$ fails to be an integral domain iff $\exists$ nonzero $s = a + b\sqrt{-5}$ and $t = c + d\sqrt{-5}$ such that

$$st = (ac - 5bd) + (ad + bc)\sqrt{-5}$$

is zero in $R/(y) = (\mathbb{Z}/p)[\sqrt{-5}]$. That is, $ac = 5bd$ and $ad = -bc$ in $\mathbb{Z}/p$. None of a, b, c, d can be 0 in $\mathbb{Z}/p$ since otherwise these equations would imply either $s = 0$ or $= 0$ in $R/(y)$. But then the equations yield

$$\frac{a^2}{b^2} = \frac{c^2}{d^2} = -5,$$

so if $R(y)$ fails to be an integral doman than -5 is a square modulo p.

Conversely, if $\exists$ z such that $z^2 \cong -5 \pmod{p}$, then

$$(z+\sqrt{-5})(z-\sqrt{-5}) = z^2+5 = 0$$

in $R/(y)$ so $R/(y)$ is not an integral domain. Thus $y \in \mathbb{Z}$ is a prime in R iff $|y|$ is a prime $p \neq 5$ in $\mathbb{Z}$ such that -5 is not a square modulo p.

Now consider $y = a + b\sqrt{-5}$ with $b \neq 0$.

$$a^2+5b^2 = (a-b\sqrt{-5})y \in (y)$$

so $R \mapsto\!\!\!\!\twoheadrightarrow R/(a^2+5b^2) \xrightarrow{q} R/(y)$. q is not injective since $y \notin (a^2+5b^2)$.

If a^2+5b^2 is not a prime in $\mathbb{Z}$ then we can see that y is not prime in R as follows. Suppose that $a^2+5b^2 = cd$ $(c, d \neq \pm 1)$ and suppose that y is prime in R. Then $y \mid cd$ so either $y \mid c$ or $y \mid d$. Say $y \mid c$. Write $c = \lambda y$ for some $\lambda \in R$. λ is not a unit since application of the norm map shows that the only units in R are ± 1, and $c \neq \pm y$ because $c \in \mathbb{Z}$, $y \notin \mathbb{Z}$. Letting $\overline{x}$ denote the complex conjugate of x, we have

$$y\overline{y} = N(y) = cd = \lambda y d$$

so $\overline{y} = \lambda d$. Thus $y = \overline{\lambda}\overline{d}$ and since $\overline{\lambda}$ and $\overline{d} = d$ are not units, this shows that y is reducible and therefore not prime.

If a^2+5b^2 is a prime p in $\mathbb{Z}$ then

$$x^2+5 \equiv 0 \mod p$$

has a solution $x = a/b$, so -5 is a square mod p. Set $c := a/b \in \mathbb{Z}/p$.

Define $\phi : R/(y) \mapsto \mathbb{Z}/p \cong \mathbb{F}_p$ by $\phi(\sqrt{-5}) = c$ and extending linearly. Then

$$\phi(y) = a + bc \equiv 0 \mod p$$

so ϕ is well-defined. $\left|R/(a^2+5b^2)\right| = p^2$ and q is not injective so $|R/(y)| = p$ and ϕ is an isomorphism. $\therefore$ $y = a + b\sqrt{-5}$ is prime in R whenever a^2+5b^2 is prime in $\mathbb{Z}$.

Remark 2.7.3. *The question of which primes p have the property that -5 is a square modulo p can be solved with the aid of Gauss' Law of Quadratic Reciprocity, which says that for odd primes p and q,*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})}$$

where $\left(\begin{matrix} p \\ - \\ q \end{matrix}\right)$ *is the Legendre symbol, defined by*

$$\left(\begin{matrix} x \\ - \\ p \end{matrix}\right) = \begin{cases} 1 & \text{if } x \text{ is a square modulo } p; \\ -1 & \text{if } x \text{ is a not square modulo } p. \end{cases}$$

Therefore

$$\left(\begin{matrix} -5 \\ - \\ p \end{matrix}\right) = \left(\begin{matrix} -1 \\ - \\ p \end{matrix}\right)\left(\begin{matrix} 5 \\ - \\ p \end{matrix}\right) = \left(\begin{matrix} -1 \\ - \\ p \end{matrix}\right)(-1)^{4(\frac{p-1}{2})}\left(\begin{matrix} p \\ - \\ 5 \end{matrix}\right) = \left(\begin{matrix} -1 \\ - \\ p \end{matrix}\right)\left(\begin{matrix} p \\ - \\ 5 \end{matrix}\right).$$

Since $\left(\begin{matrix} -1 \\ - \\ p \end{matrix}\right) = \begin{cases} 1 & p \cong 1 \mod 4; \\ -1 & p \cong 3 \mod 4, \end{cases}$ *and* $\left(\begin{matrix} p \\ - \\ 5 \end{matrix}\right) = \begin{cases} 1 & p \cong 1 \text{ or } 4 \mod 5; \\ -1 & p \cong 2 \text{ or } 3 \mod 5, \end{cases}$*, we get* $\left(\begin{matrix} -5 \\ - \\ p \end{matrix}\right) = 1$ *iff one of the following* 4 *pairs of congruences holds:*

$$\begin{matrix} p \cong 1 \mod 4 \\ p \cong 1 \mod 5 \end{matrix} \quad \text{or} \quad \begin{matrix} p \cong 1 \mod 4 \\ p \cong 4 \mod 5 \end{matrix} \quad \text{or} \quad \begin{matrix} p \cong 3 \mod 4 \\ p \cong 2 \mod 5 \end{matrix} \quad \text{or} \quad \begin{matrix} p \cong 3 \mod 4 \\ p \cong 3 \mod 5. \end{matrix}$$

By the Chinese Remainder Theorem, this is equivalent to saying that -5 *is a square modulo the prime* p *iff* $p \cong 1, 3, 7,$ *or* $9 \mod (20)$.

Definition 2.7.4. *An integral domain R is called a* ***unique factorization domain*** *(UFD) if every nonzero element can be factored into primes.*

Lemma 2.7.5. *In an integral domain, a factorization into primes (should one exist) is always unique up to associates. ie. If* $x = p_1 \cdots p_n$ *and* $x = q_1 \cdots q_k$ *then* $k = n$ *and* $\exists$ *some renumbering* σ *of the q's such that* p_j *and* $q_{\sigma(j)}$ *are associate primes* $\forall j$.

Proof. Suppose

$$p_1 \cdots p_n = q_1 \cdots q_k$$

and say $n \leq k$. Then $p_1 \mid q_1 \cdots q_k$ so $p_1 \mid q_j$ for some j. Renumber so that q_j is q_1.
$\therefore q_1 = ap_1$ for some a. But q_1 is a prime and thus irreducible, so either a or p_1 is a unit. Since p_1 is prime, it is not a unit, so a is a unit. ie. p_1 and q_1 are associates.
$\therefore p_1 \cdots p_n = q_1 \cdots q_k = ap_1q_2 \cdots q_k$,
$\therefore p_2 \cdots p_n = q_2'q_3 \cdots q_k$ where $q_2' = aq_2$ is associate to q_2. Continuing, $\forall i = 1, \ldots, n$, after renumbering q_j associate to p_i, eventually reach

$$1 = q_{n+1}' \cdots q_k$$

where q_{n+1}' is associate to q_{n+1}. If $k > n$ this is a contradiction since prime q_{n+1} is not invertible. Hence $k = n$. ◻

Proposition 2.7.6. *In a UFD, prime $\iff$ irreducible.*

Proof. Prime $\Rightarrow$ irreducible in any integral domain, so must show irreducible $\Rightarrow$ prime. Let $x \in R$ be irreducible. Write $x = p_1 \cdots p_n$ be a product of primes and suppose $n > 1$. Since x is irreducible, p_1 is a unit or $p_2 \cdots p_n$ is a unit. But p_1 is not a unit since p_1 is prime and $p_2 \cdots p_n$ is not a unit since $p_2, \ldots, p_n$ are primes. So this is a contradiction and thus $n = 1$ and $x = p_1$ is prime. □

Theorem 2.7.7. *An integral domain is a UFD iff every nonzero elt. can be factored uniquely (up to associates) into irreducibles.*

Proof.

$\Rightarrow$: Suppose R is a UFD. Then prime $\iff$ irreducible and every nonzero elt. has a unique factorization into primes.

$\Leftarrow$: Suppose every nonzero elt. has a unique factorization (up to associates) into irreducibles. It suffices to show that x is prime iff x is irreducible. ie. Show irreducible $\Rightarrow$ prime.

Let $x \neq 0$ be irreducible. Suppose $x \mid ab$. Then $ab = zx$ for some z. Let

$$a = a_1 \cdots a_n \quad \text{and} \quad b = b_1 \cdots b_k$$

be the factorizations of a, b into irreducibles. So

$$zx = a_1 \cdots a_n b_1 \cdots b_k$$

is the factorization of zx into irreducibles, so by uniqueness, x is associate to some factor on the RHS.

$\therefore$ x is assoc. to a_j for some j, in which case $x \mid a$, or x is assoc. to b_j for some j, in which case $x \mid b$. Thus x is prime.

□

Proposition 2.7.8. *In a UFD, every pair of elts. has a g.c.d.*

Proof. Let R be a UFD and suppose $x \neq 0, y \neq 0 \in R$. Factor x into primes and, replacing primes by associate ones when necessary, write

$$x = up_1^{r_1} \cdots p_n^{r_n}$$

where u is a unit and $p_1, \ldots, p_n$ are primes with p_i not associate to p_j for $i \neq j$. Similarly, write

$$y = vq_1^{s_1} \cdots q_k^{s_k}$$

where, replacing by associate if necessary, we may assume that if q_j is associate to p_i for some i then $q_j = p_i$. Letting $z_1, \ldots, z_m$ be the union $\{p_1, \ldots, p_n, q_1, \ldots, q_k\}$ of all primes occurring, we can write

$$x = uz_1^{e_1} \cdots z_m^{e_m} \quad \text{and} \quad y = vz_1^{f_1} \cdots z_m^{f_m}$$

for some exponents $e_1, \ldots, e_m, f_1, \ldots, f_m \geq 0$. Let

$$d = \prod z_j^{\min\{e_j, f_j\}}.$$

Then $d = (x, y)$. $\square$

2.8 Principal Ideal Domains

Definition 2.8.1. *A* ***principal ideal domain*** *(PID) is an integral domain in which every ideal is principal.*

Proposition 2.8.2. *In a PID, every nonzero prime ideal is maximal.*

Proof. Let $I \neq 0$ be a prime ideal. Suppose $I \subsetneq J \subsetneq R$. Write $I = (x), J = (y)$. Since I is a prime ideal, x is prime. Since $I \subset J$, $x \in J$ so $x = ay$ for some $a \in R$. Thus $x \mid a$ or $x \mid y$.

If $x \mid a$ then $a = bx$ for some $b \in R$. Then $x = ay = abxy \Rightarrow 1 = by$, so y is a unit and $J = R$.

If $x \mid y$ then $y \in (x) = I$, so $J \subset I$, contradiction $I \subsetneq J$. Hence I is maximal. □

Example 2.8.3. *Let* $R = \mathbb{Z}[x]$. $R/(x) \cong \mathbb{Z}$ *is an integral domain but not a field. So* (x) *is a prime ideal which is not maximal.*
$\therefore \mathbb{Z}[x]$ *is not a PID. In fact,* $I = (2, x)$ *is an example of a non-principal ideal in R.*

Theorem 2.8.4. *Every PID is Noetherian*

Proof. Every ideal in R is generated by a single element, so in particular, every ideal is finitely generated. By Theorem 2.6.2, this means that R is Noetherian. □

Theorem 2.8.5. *Every PID is a unique factorization domain.*

Proof. Let R be a PID and let $x \neq 0 \in R$ be a non-unit. Must show that x can be factored into primes. $(x) \subsetneq R$ so $\exists$ a maximal ideal M_1 s.t.

$$(x) \subset M_1 \subsetneq R.$$

Write $M_1 = (p_1)$. M_1 is maximal and thus prime, so p_1 is prime. $x \in (p_1)$ says $x = p_1 x_1$ for some $x_1 \in R$. If x_1 is a unit then $p_1 x_1$ is a prime associate to p_1 and we are done, so suppose not. Continuing, we get

$$x_n = p_n x_{n+1} \quad \forall n.$$

$\therefore x_n \in (x_{n+1})$ so $(x_n) \subset (x_{n+1})$. If x_n is a unit for some n then we have a factorization of x into primes. If not, we get a chain of ideals

$$(x) \subset (x_1) \subset \cdots \subset (x_n) \subset \cdots$$

Since R is Noetherian, $\exists N$ s.t. $(x_n) = (x_N)\ \forall n \geq N$. So $x_{N+1} \in (x_N)$ so $x_{N+1} = \lambda x_N = \lambda p_{N+1} x_{N+1}$ so that $1 = \lambda p_{N+1}$ showing that p_{N+1} is a unit, which is a contradiction.

So the infinite chain does not exist, so the procedure terminated giving a factorization of x. □

Proposition 2.8.6. *Let R be a PID. Let* $a, b \in R$ *and let* $q = \gcd(a, b)$. *Then* $\exists s, t \in R$ *s.t.* $q = sa + tb$.

Proof. Let $I = \langle a, b\rangle = \{xa + yb \mid x, y \in R\}$. Then I is an ideal so $I = (c)$ for some $c \in R$. $c \in I$ so $c = xa + yb$ for some x, y. $a \in I$ so $c \mid a$ and $b \in I$ so $c \mid b$. Moreover, if $z \mid a$ and $z \mid b$ then let $a = \alpha z$ and $b = \beta z$ for some α, β. Then

$$c = xa + yb = x\alpha z + y\beta z = (x\alpha + y\beta)z$$

and thus $z \mid c$. So $c = \gcd(a, b)$.

If q is another g.c.d. of a, b then $q = uc$ for some unit u, so

$$q = (ux)a + (uy)b.$$

$\square$

2.9 Norms and Euclidean Domains

Definition 2.9.1. *A **Euclidean domain** is an integral domain R together with a function $d : R - \{0\} \mapsto \mathbb{Z}^+ = \{n \in \mathbb{Z} \mid n \geq 0\}$ s.t.*

1. *$d(a) \leq d(ab)\ \forall a, b \neq 0$, and*

2. *Given $a, b \neq 0 \in R$, $\exists t, r$ s.t. $a = tb + r$ where either $r = 0$ or $d(r) < d(b)$.*

Example 2.9.2.

1. *$R = \mathbb{Z}$, $d(n) = |n|$.*

2. *$R = F[x]$ where F is a field. $d(p(x))$ = polynomial degree of p.*

Notice that if (R, d) is a Euclidean domain then so is (R, d') where

$$d'(x) = d(x) + c, \quad \text{for some constant } c \in \mathbb{Z}^+.$$

$\therefore$ May assume that d takes values in $\mathbb{N} = \{n \in \mathbb{Z} \mid n \geq 1\}$. Then extend d by defining $d(0) = 0$.

Definition 2.9.3. *A **Dedekind-Hasse norm** on an integral domain R is a function $N : R \mapsto \mathbb{Z}^+$ s.t.*

1. *$N(x) = 0$ iff $x = 0$, and*

2. *For $a, b \neq 0 \in R$ either $a \in (b)$ or $\exists$ a nonzero $x \in (a, b)$ s.t. $N(x) < N(b)$.*

If (R, d) is a Euclidean domain then d (modified s.t. $d(0) = 0$) is a Dedekind-Hasse norm: given $a, b \neq 0$,

$$a = tb + r$$

for some t and r, so either $b \mid a$ (ie. $r = 0$) or $r = a - tb \in (a, b)$ with $d(r) < d(b)$.

Theorem 2.9.4. *Let R be an integral domain.*

1. *R is a PID iff R has a Dedekind-Hasse norm. In particular, a Euclidean domain is a PID.*

2. *If R has a Dedekind-Hasse norm then it is has a multiplicative Dedekind-Hasse norm (ie. one satisfying $N(ab) = N(a)N(b)$.)*

Proof.

1. $\Rightarrow$: Suppose R has a Dedekind-Hasse norm. Let $I \subset R$ be a nonzero ideal. Choose $0 \neq b \in I$ s.t. $N(b)$ is minimum. Let $a \in I$. Then $(a, b) \subset I$ so $\nexists$ nonzero $x \in (a, b)$ s.t. $N(x) < N(b)$. Hence $a \in (b)$. Thus $I = (b)$.

$\Leftarrow$: Suppose R is a PID. Define $N : R \mapsto \mathbb{Z}^+$ as follows: $N(0) := 0$. If $u \in R$ is a unit, set $N(u) = 1$. If $x \neq 0 \in R$ is a nonunit, write $x = p_1 \cdots p_n$ where each p_j is prime and set $N(x) = 2^n$. Notice that N is multiplicative.

Suppose $a, b \neq 0 \in R$. R is a PID so $(a, b) = (r)$ for some $r \in R$, so $b = xr$ for some $x \in R$. If $a \notin (b)$ then $r \notin (b)$ so x is not a unit, and thus

$$N(b) = N(x)N(r) > N(r),$$

ie. $\exists r \in (a, b)$ s.t. $N(r) < N(b)$.

2. If R has a Dedekind-Hasse norm then by part 1, it is a PID, in which case it has a multiplicative Dedekind-Hasse norm as constructed above.

□

2.9.1 Euclidean Algorithm

Let (R, d) be a Euclidean domain. Then R is a PID, so given $a, b \in R$, $\exists s, t \in R$ s.t.

$$as + bt = \gcd(a, b).$$

The Euclidean algorithm is an algorithm for finding s and t (and thus $\gcd(a, b)$).
Procedure:
Say $d(b) \geq d(a)$. Set $r_{-1} := b$, $r_0 := a$. Write

$$\begin{aligned} r_{-1} &= q_1 r_0 + r_1, \quad \text{some } q_1, r_1 \text{ with } d(r_1) < d(r_0), \\ &\vdots \\ r_{j-1} &= q_{j+1} r_j + r_{j+1}, \quad \text{some } q_{j+1}, r_{j+1} \text{ with } d(r_{j+1}) < d(r_j) \end{aligned}$$

$\therefore d(r_{-1}) \geq d(r_0) > d(r_1) > \cdots > d(r_j) > \cdots$. Continue until $r_{k+1} = 0$, some k. Set

$$\begin{aligned} s_0 &:= 0 \\ s_1 &:= 1 \\ s_j &:= -q_{j-1} s_{j-1} + s_{j-2} \\ t_0 &:= 1 \\ t_1 &:= 0 \\ t_j &:= -q_{j-1} t_{j-1} + t_{j-2} \end{aligned}$$

Claim. $r_k = \gcd(a, b)$ and $r_k = sa + tb$ where $s = s_{k+1}$ and $t = t_{k+1}$.

Proof. $r_{k+1} = 0$ so $r_{k-1} = q_{k+1}r_k + 0$. Suppose by induction that $r_k \mid r_i$ for $i \geq j$. Then $r_{j-1} = q_{j+1}r_j + r_{j+1}$ so $r_k \mid r_{j-1}$, concluding induction step.
$\therefore r_k \mid r_j\ \forall j$ and in particular, $r_k \mid r_0 = a$ and $r_k \mid r_{-1} = b$.

Conversely, suppose z divides both a and b. Since $r_{j+1} = r_{j-1} - q_{j+1}r_j$, induction (going the other way) shows $z \mid r_j\ \forall j$. In particular, $z \mid r_k$. So $r_k = \gcd(a, b)$. □

Also,

$$\begin{aligned}
as_0 + bt_0 &= a \cdot 0 + b \cdot 1 = b = r_{-1} \\
as_1 + bt_1 &= a \cdot a + b \cdot 0 = a = r_0 \\
as_2 + bt_2 &= a(-q_1 s_1 + s_0) + b(-q_1 t_1 + t_0) = -q_1(as_1 + bt_1) + (as_0 + bt_0) \\
&= -q_1 r_0 + r_{-1} = r_1 \\
&\vdots \\
as_j + bt_j &= a(-q_{j-1}s_{j-1} + s_{j-2}) + b(-q_{j-1}t_{j-1} + t_{j-2}) = -q_{j-1}(as_{j-1} + bt_{j-1}) + (as_{j-2} + bt_{j-2}) \\
&= -q_{j-1}r_{j-2} + r_{j-3} = r_{j-1}
\end{aligned}$$

By induction, $as_j + bt_j = r_{j-1}\ \forall j$. In particular, $as + bt = as_{k+1} + bt_{k+1} = r_k = \gcd(a, b)$.

Remark: In Computer Science, the speed of the Euclidean Algorithm over $\mathbb{Z}$ is important. Estimate of the number of steps required: The faster the r's go down, the quicker the algorithm goes, so the worst case scenario is when all the q's are only 1. In this case,

$$r_{j-1} = r_j + r_{j+1}.$$

ie. Worst case scenario occurs when a, b are consecutive terms of the Fibonacci Sequence. The smallest possible numbers requiring N steps would be when:

$$r_N = 1 \quad r_{N-1} = 2 \quad r_{N-2} = 3 \quad r_{N-3} = 4 \cdots r_{N-j} = j^{\text{th}} \text{ Fibonacci Number}$$

$\therefore r_0 = N^{\text{th}}$ Fibonacci Number F_N. ie. N steps can handle all numbers up to F_N.

$F_{n+1} = F_n + F_{n-1} \Rightarrow \frac{F_{n+1}}{F_n} = 1 + \frac{F_{n-1}}{F_n}$. So if $L = \lim_{n\to\infty} \frac{F_{n+1}}{F_n}$ then $L = 1 + \frac{1}{L}$. So

$$\begin{aligned}
L^2 - L - 1 &= 0 \\
L &= \frac{1 \pm \sqrt{5}}{2} \\
L &= \frac{1 + \sqrt{5}}{2} = G
\end{aligned}$$

So $F_n \approx G^N$, ie. for large N, the number of steps required is no worse than around $\log_G(r_0)$.

Lemma 2.9.5 (Gauss)**.** *Let R be a UFD and let F be its field of fractions. Let $q(x) \in R[x]$. If $q(x)$ is reducible in $F[x]$ then $q(x)$ is reducible in $R[x]$. Futhermore, if $q(x) = A(x)B(x)$ in $F[x]$ then in $R[x]$, $q(x) = a(x)b(x)$ where $A(x) = \frac{a(x)}{r}$ and $B(x) = \frac{b(x)}{s}$ for some nonzero $r, s \in F$.*

Proof. Suppose $q(x) = A(x)B(x)$ where the coefficients of A, B lie in F. Multiplying by a common denominator we get

$$dq(x) = a'(x)b'(x)$$

for some $d \in R$ and polynomials $a'(x), b'(x) \in R[x]$. If $d \in R$ is a unit, we can divide by d to get $q(x) = \frac{a'(x)}{d}b'(x)$.
$\therefore$ Suppose d is not a unit. Write $d = p_1 \cdots p_n$ as a product of primes in R. Let

$$\begin{aligned} R[x] &\twoheadrightarrow \frac{R[x]}{p_1R[x]} \cong (\frac{R}{p_1R})[x] \\ f(x) &\mapsto \overline{f(x)} \end{aligned}$$

Reducing modulo $(p_1R)[x]$ gives $0 = \overline{a'(x)}\,\overline{b'(x)}$ in the integral domain $(\frac{R}{p_1R})[x]$. Hence $\overline{a'(x)} = 0$ or $\overline{b'(x)} = 0$. Say $\overline{a'(x)} = 0$. Then all the coeffs. of $a'(x)$ are divisible by p_1, so can divide $dq(x) = a'(x)b'(x)$ by p_1 to get

$$p_2 \cdots p_n g(x) = \frac{a'(x)}{p_1}b'(x) = a''(x)b'(x)$$

with $a'', b' \in R[x]$. Continuing, eventually reach $q(x) = a(x)b(x)$ with $a(x), b(x) \in R[x]$ and $a(x), b(x)$ obtained from $a'(x), b'(x)$ by multiplying by nonzero elements of F. □

A polynomial whose leading coefficient is 1 is called **monic**.

Corollary 2.9.6. *Let R be a UFD with field of fractions F. Let $p(x) \in R[x]$. Suppose*

$$gcd\{coeffs.\ of\ p\} = 1.$$

Then $p(x)$ is irreducible in $R[x]$ iff it is irreducible in $F[x]$. In particular, if $p(x)$ is monic and irreducible in $F[x]$ then it is irreducible in $R[x]$.

Proof. If $p(x)$ is reducible in $F[x]$ then Gauss implies $p(x)$ is reducible in $R[x]$.

Conversely, if $p(x)$ is reducible in $R[x]$ then the hypothesis on gcd $\Rightarrow$ $p(x) = a(x)b(x)$ where neither $a(x)$ nor $b(x)$ is constant. Hence, $a(x), b(x)$ are not units in $F[x]$ so this factorization shows $p(x)$ is reducible in $F[x]$. □

Lemma 2.9.7. *Let R be a UFD and let $p(x) \in R[x]$ be irreducible. Then $p(x)$ is prime.*

Proof. Let F be the field of fractions of R.

$$\frac{R[x]}{(p(x))} \hookrightarrow \frac{F[x]}{(p(x))}.$$

$\therefore$ To show $p(x)$ $R[x]/(p(x))$ is an integral domain, it suffices to show that $F[x]/(p(x))$ is an integral domain.

$p(x)$ irreducible in $R[x] \Rightarrow p(x)$ irreducible in $F[x]$. However, $F[x]$ is a UFD (being a Euclidean Domain). So $p(x)$ is prime in $F[x]$ and thus $F[x]/(p(x))$ is an integral domain. □

Theorem 2.9.8. *R is a UFD $\iff R[x]$ is a UFD.*

Proof.

$\Leftarrow$: Suppose $R[x]$ is a UFD. Let $r \in R$. Write $r = p_1(x) \cdots p_n(x)$ as a product of primes in $R[x]$. Since $\deg r = 0$ and R is an integral domain, $\deg p_j(x) = 0\ \forall j$, ie. $p_j(x) = p_j \in R$.

$$R[x]/(p_j) = \left(\frac{R}{(p_j)}\right)[x]$$

$\therefore R/(p_j)$ is an integral domain, so p_j is prime in R.

Thus $r = p_1 \cdots p_n$ is a factorization of r into primes in R.

$\Rightarrow$: Suppose R is a UFD and let $0 \neq q(x) \in R[x]$. Let F be the field of fractions of R. Since $F[x]$ is a UFD, in $F[x]$ we can factor $q(x)$

$$q(x) = p_1(x) \cdots p_r(x)$$

where $p_j(x)$ is a prime in $F[x]$. By Gauss' lemma, in $R[x]$ we can write

$$q(x) = p_1'(x) \cdots p_n'(x)$$

where $\forall j \exists s_j \neq 0 \in F$ such that $p_j'(x) = s_j p_j(x)$.

$\therefore$ It suffices to show that $p_j'(x)$ can be factored uniquely into primes in $R[x]$, as in the following claim:

Claim. If $p(x)$ is prime in $F[x]$ and $sp(x) = p'(x) \in R[x]$ for some $0 \neq s \in F$ then $p'(x)$ can be factored uniquely into primes in $R[x]$.

Proof. Let

$$d = \gcd\{\text{coeffs. of } p'(x)\}.$$

Then $p'(x) = dp''(x)$ where

$$\gcd\{\text{coeffs. of } p''(x)\} = 1.$$

In $F[x]$, have $p''(x) = \frac{p'(x)}{d} = \frac{s}{d}p(x)$, which is prime in $F[x]$ since $p(x)$ is prime and $\frac{s}{d}$ is a unit. $\therefore$ Cor. 2.9.6$\Rightarrow$ $p''(x)$ is irreducible in $R[x]$ and thus prime in $R[x]$ by the previous lemma. Since d can be factored into primes in R and a prime in R is also a prime in $R[x]$, $p'(x) = dp''(x)$ can be factored into primes in $R[x]$.Uniqueness is easy to show. This concludes the proof of the claim and thus concludes the proof of the theorem.

$\square$

2.10 Modules over PID's

Note: In this section, and elsewhere, we will sometimes abuse notation and write R/p in place of $R/(p)$. (The notation $\mathbb{Z}/n$ is generally quite common).

Theorem 2.10.1. *Over a PID, a submodule of a free module is free.*

Proof. Let R be a PID. Let $P = \bigoplus_{j \in J} R_j$ be a free R-module with basis J ($R_j \cong R\ \forall j$), and suppose $M \subset P$ is a submodule.

Choose a well-ordering of the set J. For each $j \in J$, set $P_j = \bigoplus_{i \leq j} R_i$ and $\overline{P}_j = \bigoplus_{i<j} R_i$, so $P_j = \overline{P}_j \oplus R$.

Let f_j be the composite

$$P_j \cap M \hookrightarrow P_j = \overline{P}_j \oplus R \mapsto\!\!\!\!\twoheadrightarrow R.$$

Then $\ker f_j = \overline{P}_j \cap M$. $\operatorname{Im} f_j \subset R$ is an ideal, so let $\operatorname{Im} f_j = (\lambda_j)$, some $\lambda_j \in R$. Pick $c_j \in P_j \cap M$ such that $f(c_j) = \lambda_j$. Let

$$J' = \{j \in J \mid \lambda_j \neq 0\}.$$

To finish the proof we show:
Claim: $\{c_j\}_{j \in J'}$ is a basis for M.
Proof. Check $\{c_j\}_{j \in J'}$ is linearly independent:
Suppose

$$\sum_{k=1}^{n} a_k c_{j_k} = 0, \quad \text{where } j_1 < j_2 < \cdots < j_n \tag{$*$}$$

Since $j_k < j_n$ for $k < n$, $c_{j_k} \in \overline{P}_{j_n}$ for $k < n$.

$\therefore$ Applying f_{j_n} to $(*)$ gives

$$\sum_{k=1}^{n} a_k \cdot 0 + a_n \lambda_{j_n} = 0,$$

whence $a_n = 0$, since $\lambda_{j_k} \neq 0$. Inductively, $c_{j_k} = 0\ \forall k = n, n-1, \ldots, 1$.

$\therefore \{c_{j_k}\}_{j \in J'}$ is linearly independent.
Check that $\{c_j\}_{j \in J'}$ spans M:
Suppose not. Then $\exists$ a least $i \in J$ such that $P_i \cap M$ contains an element a not in $\operatorname{span}\{c_j\}_{j \in J'}$. Must have $i \in J'$, since if not, $f_i(a) = 0$, so $a \in \overline{P}_i$, and thus $a \in P_k$ for some $k < i$, contradicting minimality of i.

$\therefore i \in J'$. $f_i(a) \in (\lambda_i)$, so $f_i a = r\lambda_i$, for some $r \in R$. Set $b := a - rc_i$. Since $a = b + rc_i$ cannot be written as a linear combination of $\{c_i\}$, neither can b. But

$$f_i b = f(a) - r f(c_i) = r\lambda_i - r\lambda_i = 0$$

so $b \in P_k \cap M$ for some $k < i$, contradicting the minimality of i.

$\therefore \{c_j\}_{j \in J'}$ spans M. $\square$

Theorem 2.10.2. *Over a PID, a finitely generated torsion-free module is free.*

Proof. Let R be a PID and let M be a finitely generated torsion-free R-module. Let $R \hookrightarrow K$ be the inclusion of R into its field of fractions, and let

$$\tilde{M} := K \otimes_R M$$

be the extension of M to a K-vector space.

Let $x_1, \ldots, x_m \in M$ be a generating set for M. The images of $x_1, \ldots, x_m$ generate $\tilde{M}$, so $\exists$ a subset $y_1 \ldots, y_n$ whose images in $\tilde{M}$ form a basis for $\tilde{M}$. Each x_j can be written in $\tilde{M}$ as a K-linear combination of $y_1, \ldots, y_n$, so clearing denominators gives that $b_j x_j$ is an R-linear combination of $y_1, \ldots, y_n$ $\forall j$.

Set $b = b_1 \cdots b_m$, so that bx_j is an R-linear combination of $y_1, \ldots, y_n$ $\forall j$.

$\therefore bz$ is an R-linear combination of $y_1, \ldots y_n$ $\forall z \in M$, since $x_1, \ldots, x_m$ span M. Since M is torsion-free,

$$\begin{aligned} b : M &\mapsto M \\ z &\mapsto bz \end{aligned}$$

is injective. Hence,

$$M \cong M/\ker\phi \cong \mathrm{Im} b = bM.$$

However,

$$\begin{aligned} \bigoplus_{j=1}^{n} y_j &\overset{\phi}{\longmapsto} bM \\ y_j &\mapsto y_j \end{aligned}$$

is an isomorphism (onto since bz is a linear combination of $y_1, \ldots, y_n$ $\forall z \in M$, (1-1) since $y_1, \ldots y_n$ are linearly independent in $\tilde{M}$).

$\therefore M \cong bM \cong$ a free R-module. $\square$

Corollary 2.10.3. *If M is a finitely generated module over a PID then $R \cong \mathrm{Tor}(M) \oplus R^n$ for some $n \in \mathbb{N}$.*

Proof. $M/\mathrm{Tor}(M)$ is finitely generated and torsion-free. Hence,

$$M/\mathrm{Tor}(M) \cong R^n, \quad \text{for some } n.$$

R^n free $\Rightarrow M \mapsto\!\!\!\!\twoheadrightarrow M/\mathrm{Tor}(M) \cong R^n$ splits, so

$$M \cong \mathrm{Tor}(M) \oplus R^n.$$

$\square$

A torsion-free module over a PID which is not finitely generated need not be free:

Example 2.10.4. *Let $R = \mathbb{Z}$, $M = \mathbb{Q}$. Clearly $\mathbb{Q}$ is torsion-free as a $\mathbb{Z}$-module. Suppose $M \cong R^s$. Then as a vector space $/\mathbb{Q}$ we get*

$$\begin{aligned}\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} &\cong M \otimes \mathbb{Q} \\ &\cong R^s \otimes \mathbb{Q} \\ &\cong (R \otimes \mathbb{Q})^s \\ &\cong \mathbb{Q}^s\end{aligned}$$

Let

$$\begin{gathered}\phi : \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \mapsto \mathbb{Q} \\ x \otimes y \mapsto xy, \\ \psi : \mathbb{Q} \mapsto \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \\ x \mapsto x \otimes 1.\end{gathered}$$

Clearly $xy = 1_{\mathbb{Q}}$. $\psi\phi(x \otimes y) = (xy) \otimes 1$. Write $x = \frac{p}{q}, y = \frac{p'}{q'}$. Then in $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$,

$$\begin{aligned}x \otimes y &= \frac{p}{q} \otimes \frac{p'}{q'} \\ &= q' \frac{p}{qq'} \otimes p' \frac{1}{q'} \\ &= p' \frac{p}{qq'} \otimes q' \frac{1}{q'} \\ &= \frac{pp'}{qq'} \otimes 1 \\ &= (xy) \otimes 1.\end{aligned}$$

$\therefore \psi\phi = 1_{\mathbb{Q}\otimes\mathbb{Q}}$. Hence $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}$, and thus $\mathbb{Q} \cong \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}^s$. So counting dimensions gives $\mathrm{Card} S = 1$.

ie. If $\mathbb{Q}$ is a free R-module then its rank as a $\mathbb{Z}$-module is 1. So $\mathbb{Q} \cong \mathbb{Z}$ as a $\mathbb{Z}$-module. ie. $\exists q \in \mathbb{Q}$ s.t. $\mathbb{Q} = \mathbb{Z}q$; that is to say, $\forall x \in \mathbb{Q}\ \exists n \in \mathbb{Z}$ s.t. $x = nq$. This is a contradiction.

So $\mathbb{Q}$ is not a free $\mathbb{Z}$-module.

We now consider decompositions of finitely generated torsion modules over a PID. Let R be a PID (throughout this section). We will show that every finitely generated R-module decomposes as a direct sum of finitely many R-modules with a single generator (called cyclic modules).

First consider torsion modules.

Notation: For $r \in R$, let $\mu_r : M \mapsto M$ be multiplication by r.

Lemma 2.10.5. *Let M be a torsion R-module. Write* $\mathrm{Ann}(M) = (a)$ *and suppose $b \in R$ such that* $(a, b) = 1$. *Then multiplication by b,*

$$M \overset{\mu_b}{\longmapsto} M$$

is an isomorphism.

Proof. Since R is a PID, $\exists s, t \in R$ such that $sa + tb = 1$. Hence, for $x \in M$,

$$x = sax + tbx = tbx,$$

$\therefore bx = 0 \implies x = 0$, so μ_b is injective. Moreover,

$$x = b(tx) = \mu_b(tx)$$

so μ_b is surjective. □

Let $M \neq 0$ be a torsion module. Let $\mathrm{Ann}(M) = (a)$. Suppose $a \neq 0$. (Note: if M is torsion and f.g. then $a \neq 0$ automatically.)

$M \neq 0 \implies a$ is not a unit. Write

$$a = up_1^{e_1} \cdots p_k^{e_k}$$

where u is a unit and $p_1, \dots, p_k$ are distinct primes. Replacing a by $u^{-1}a$, may assume

$$a = p_1^{e_1} \cdots p_k^{e_k}.$$

Let

$$M_{p_j} := \{x \in M \mid p_j^e x = 0 \text{ for some } e\}.$$

Lemma 2.10.6. $M \cong M_{p_1} \oplus \cdots \oplus M_{p_k}$.

Proof. $\forall x \in M$,

$$p_1^{e_1} \mu_{p_2^{e_2} \cdots p_k^{e_k}}(x) = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} x = 0$$

so $\mathrm{Im}\mu_{p_2^{e_2} \cdots p_k^{e_k}} \subset M_{p_1}$.

Since $p_2^{e_2} \cdots p_k^{e_k}$ is coprime to $\mathrm{Ann}(M_{p_1})$, by the preceding lemma,

$$\mu_{p_2^{e_2} \cdots p_k^{e_k}}|_{M_{p_1}}$$

is an isomorphism, so it splits the inclusion $M_{p_1} \hookrightarrow M$. Hence,

$$M \cong M_{p_1} \oplus \ker \mu_{p_2^{e_2} \cdots p_k^{e_k}}.$$

$\operatorname{Ann}(\ker \mu_{p_2^{e_2}\cdots p_k^{e_k}}) = p_2^{e_2} \cdots p_k^{e_k}$. By induction,

$$\ker \mu_{p_2^{e_2}\cdots p_k^{e_k}} \cong M'_{p_2} \oplus \cdots \oplus M'_{p_k}$$

where

$$\begin{aligned} M'_{p_j} &= \{x \in \ker \mu_{p_2^{e_2}\cdots p_k^{e_k}} \mid p_j^e x = 0 \text{ for some } e\} \\ &\subset M_{p_j} = \{x \in M \mid p_j^e x = 0 \text{ for some } e\}. \end{aligned}$$

However, $M_{p_j} \subset \ker \mu_{p_2^{e_2}\cdots p_k^{e_k}}$ so $M_{p_j} \subset M'_{p_j}$ and thus $M_{p_j} = M'_{p_j}$.

Hence $M \cong M_{p_1} \oplus \cdots \oplus M_{p_k}$. □

In the finitely generated case, we now decompose M_{p_j} into cyclic summands for each p_j. ie. We have reduced to the case where $\operatorname{Ann}(M) = (p^e)$ for some prime p.

Suppose M is a f.g. R-module with $\operatorname{Ann}(M) = (p^e)$. $\exists x \in M$ such that $p^{e-1}x \neq 0$ (or else $\operatorname{Ann}(M) = p^{e-1}$ rather than p^e). Let $x, m_1, \ldots, m_k$ be a generating set for M. Let M_j be the submodule

$$M_j := \langle x, m_1, \ldots, m_j \rangle.$$

Beginning with the identity map $r_0 : M_0 \mapsto Rx$, we inductively construct $r_j : M_j \mapsto Rx$ extending $r_{j-1} : M_{j-1} \mapsto Rx$ to produce a splitting $r : M \mapsto Rx$ of the inclusion $Rx \hookrightarrow M$.

Suppose by induction that $r_{j-1} : M_{j-1} \mapsto Rx$ has been defined such that $r_{j-1}|_{Rx} = 1_{Rx}$. M_j is generated by M_{j-1} and m_j. So to define r_j extending r_{j-1}, must define $r_j(m_j) \in Rx$, ie. $r_j(m_j) = \lambda x$ for the correct λ.

Let $(p^s) = \operatorname{Ann}(M_j/M_{j-1})$, so $p^s m_j \in M_{j-1}$. $r_{j-1}(p^s m_j) \in Rx$, so $r_{j-1}(p^s m_j) = \alpha x$ for some $\alpha \in R$.

$$p^{e-s}\alpha x = p^{e-s}(r_{j-1}p^s m_j) = r_{j-1}(p^e m_j) = r_{j-1}(0) = 0$$

so $p^{e-s}\alpha = \lambda p^e$ for some $\lambda \in R \implies \alpha = \lambda p^s$.

Define $r_j(m_j) = \lambda x$ and $r_j(y) = r_{j-1}(y) \forall y \in M_{j-1}$. Then

$$r_j(p^s m_j) = p^s \lambda x = \alpha x = r_{j-1}(p^s m_j)$$

so r_j is well-defined. Thus $M \cong Rx \oplus M'$.

Applying the procedure to M' gives

$$M \cong Rx \oplus Rx' \oplus M''.$$

Continuing, the procedure eventually terminates since M is Noetherian.

$\therefore M \cong Rx_1 \oplus Rx_2 \oplus \cdots \oplus Rx_n$ for some $x_1, \ldots, x_n$ with $\mathrm{Ann} x_j = (p^j)$ for some j. Notice that

$$\begin{aligned} R &\overset{\psi_j}{\longmapsto} Rx_j \\ r &\mapsto rx_j \end{aligned}$$

is surjective with $\ker \psi_j = \mathrm{Ann} x_j$. Thus $Rx_j \cong R/(p^j)$.

Putting it all together, we get:

Theorem 2.10.7 (Structure Theorem for Finitely Generated Modules over a PID)**.** *Let M be a finitely generated module over a PID R. Then*

$$M \cong R/(p_1^{s_1}) \oplus R/(p_2^{s_2}) \oplus \cdots \oplus R/(p_n^{s_n}) \oplus R^k,$$

where $p_1, \ldots, p_n \in R$ are primes (not necessarily distinct), $s_1, \ldots, s_n \in \mathbb{N}$ and $k \geq 0$.

Note that the generator of $\mathrm{Ann}(M)$ is $\mathrm{lcm}\{p_1^{s_1}, \ldots, p_n^{s_n}\}$.

We now show that this decomposition is unique. k is the dimension of $M \otimes_R K$, where K is the field of fractions, so k is unique, and we need only be concerned with the torsion part of the module.

Theorem 2.10.8. *Suppose*

$$R/(p_1^{s_1}) \oplus R/(p_2^{s_2}) \oplus \cdots \oplus R/(p_n^{s_n}) \cong R/(q_1^{t_1}) \oplus R/(q_2^{t_2}) \oplus \cdots \oplus R/(q_k^{t_k}),$$

with $p_1, \ldots, p_n, q_1, \ldots q_k$ primes in R and $s_1, \ldots s_n, t_1, \ldots t_k \in \mathbb{N}$. Then $n = k$ and $\{q_1^{t_1}, \ldots, q_k^{t_k}\}$ is a permutation of (associates of) $\{p_1^{s_1}, \ldots, p_n^{s_n}\}$.

Proof. Let

$$\begin{aligned} M &= R/(p_1^{s_1}) \oplus R/(p_2^{s_2}) \oplus \cdots \oplus R/(p_n^{s_n}) \quad \text{and} \\ N &= R/(q_1^{t_1}) \oplus R/(q_2^{t_2}) \oplus \cdots \oplus R/(q_k^{t_k}). \end{aligned}$$

For any prime p, let

$$\begin{aligned} M_p &= \{x \in M \mid p^e x = 0, \text{ for some } e\}, \\ N_p &= \{x \in N \mid p^e x = 0, \text{ for some } e\}. \end{aligned}$$

If $M \cong N$ then $M_p \cong N_p$. Moreover,

$$\begin{aligned} M_p &\cong \bigoplus_{p_j \text{ assoc. to } p} R/(p_j^{s_j}), \\ N_p &\cong \bigoplus_{q_j \text{ assoc. to } p} R/(q_j^{t_j}). \end{aligned}$$

$\therefore$ It suffices to consider one prime at a time. ie. We are reduced to the case where $p_j = q_j = p \ \forall j$.

Suppose

$$M = R/(p^{s_1}) \oplus \cdots \oplus R/(p^{s_n}) \quad \text{and} \quad N = R/(p^{q_1}) \oplus \cdots \oplus R/(p^{q_k}).$$

For $Z = R/(p^s)$, $\exists$ a short exact sequence

$$0 \mapsto pZ \mapsto Z \mapsto R/p \mapsto 0,$$

ie. $Z/pZ \cong R/p$, a field.

Since $M \cong N$,

$$\bigoplus_n R/p \cong M/pM \cong N/pN \cong \bigoplus_k R/p.$$

Since the dimension of a vector space is an invariant of the isomorphism class of the vector space, $n = k$.

Also, $M \cong N \Rightarrow pM \cong pN$; that is:

$$R/p^{s_1-1} \oplus \cdots \oplus R/p^{s_n-1} \cong R/p^{t_1-1} \oplus \cdots \oplus R/p^{t_k-1}.$$

Ann(pM) has one less power of p than Ann$M$. So by induction on the size of Ann(M), the positive elts. in the list $\{t_1 - 1, \dots, t_k - 1\}$ is a permutation of those in $\{s_1 - 1, \dots, s_n - 1\}$. ie. Information about summands R/p has been lost, since $p(R/p) = 0$, so pM and pN have no record of how many summands R/p there were in M and N. But they see all the remaining summands, showing that entries in $\{t_1, \dots, t_k\}$ which are at least 2 are the same (up to a permutation) as those in $\{s_1, \dots, s_n\}$. The remaining entries on each list are 1, and there are the same number of them on each list since $n = k$ and the entries greater than 1 correspond.

$\therefore \{t_1, \dots, t_k\}$ is a permutation of $\{s_1, \dots, s_n\}$. $\square$

Thus, $\{p_j^{s_j}\}$ is uniquely determined by (and uniquely determines) M. It is called the set of **elementary divisors** of M.

Example 2.10.9.

1. *$R = \mathbb{Z}$. List all non-isomorphic abelian groups of order* 16*:*

$$\mathbb{Z}/16, \quad \mathbb{Z}/8 \oplus \mathbb{Z}/2, \quad \mathbb{Z}/4 \oplus \mathbb{Z}/4 \quad \mathbb{Z}/4 \oplus \mathbb{Z}/2, \oplus \mathbb{Z}/2 \quad \mathbb{Z}/2 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/2$$

(all non-isomorphic by the theorem).

2. *Let F be a field, V a f.d. vector space $/F$, $T : V \mapsto V$ a linear transformation. Let $R = F[x]$ (a PID) and $M = V$ with R-action*

$$f(x)(v) = f(T)(v) = \sum_{j=0}^{n} a_j T^j(v).$$

Let

$$\mathrm{Ch}(\lambda) = \det(T - \lambda I),$$

the ***characteristic polynomial*** *of* T*. Then* $\mathrm{Ch}(T) = 0$ *(Cayley-Hamilton Theorem).*

$\therefore\ \mathrm{Ch}(x)v = 0\ \forall v \in V$*. ie.* M *is a torsion* R*-module and* $\mathrm{Ch}(x) \in \mathrm{Ann}(M)$*. Hence*

$$M \cong F[x]/p_1(x)^{r_1} \oplus \cdots \oplus F[x]/p_k(x)^{r_k}$$

for some primes $p_1(x), \ldots, p_k(x) \in F[x]$*.*

Suppose F *is algebraically closed so that every poly. in* $F[x]$ *factors completely as a product of linear factors. Then the primes in* $F[x]$ *are the degree* 1 *polynomials. So mult. by a scalar to make* p_j *monic:*

$$p_j(x) = x - \lambda_j$$

for some $\lambda_j \in F$*. Then*

$$M \cong \cdots \oplus F[x]/(x - \lambda_j)^{r_j} \oplus \cdots$$

implies that $\exists v \in V$ *s.t.* $(x - \lambda_j) \in \mathrm{Ann}V$*. ie.* $(T - \lambda_j)v = 0$*. (And conversely, if* $(T - \lambda)v = 0$ *for some* v *then* $x - \lambda = p_j(x)$ *for some* j*.)*

$\therefore \{\lambda_1, \ldots, \lambda_k\}$ *= eigenvalues of* T*.*

Examine $F[x]/(x-\lambda_j)^{r_j}$ *more closely. Write* λ *for* λ_j *and* r *for* r_j*. As an* $F[x]$*-module,* $F[x]/(x-\lambda)^r$ *is gen. by* $(x - \lambda)$*. Elts. can be written uniquely as*

$$\sum_{k=0}^{r-1} a_k (x - \lambda)^k$$

where $a_k \in F$*. ie. Over* F*,* $F[x]/(x - \lambda)^r$ *has dimension* r *with basis*

$$1, x - \lambda, (x - \lambda)^2, \ldots, (x - \lambda)^{r-1}.$$

Let $B = B_j \subset V = M$ *be the image of* $F[x] = (x - \lambda_j)^{r_j}$ *under the iso.*

$$\psi : \bigoplus_i F[x]/(x - \lambda_i)^{r_i} \xrightarrow{\cong} M$$

and let $v_j = \psi((x - \lambda)^{j-1})$ *for* $j = 1, \ldots, r$ *be the* F*-basis for* B *corresponding to the basis* $\{(x - \lambda)^i\}$*.*

B *is a* $F[x]$*-submodule of* V *so it is closed under the action of any* $f(x) \in F[x]$*. For* $f(x) = x - \lambda$*, by construction,*

$$\begin{aligned} f(x) \cdot v_j &= v_{j+1} \quad j < r \\ f(x) \cdot v_r &= 0. \end{aligned}$$

ie. when written in the basis $v_1, \ldots, v_r$, the matrix $T - \lambda$ is

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

ie. T looks like

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

Therefore:

Theorem 2.10.10 (Jordan Canonical Form)**.** *Let $T : V \mapsto V$ be a linear transformation where V is a f.d. vector space over an algebraically closed field F. Then $\exists$ a basis for V in which T has the form*

$$\begin{pmatrix} B_1 & 0 & \cdots & 0 \\ 0 & B_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & B_k \end{pmatrix}$$

where

$$B_j = \begin{pmatrix} \lambda_j & 0 & \cdots & & 0 \\ 1 & \lambda_j & \ddots & & \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \lambda_j & 0 \\ 0 & \cdots & 0 & 1 & \lambda_j \end{pmatrix}.$$

Note: While $\mathrm{Ch}(\lambda) \in \mathrm{Ann}(V)$, it does not necessarily generate the ideal $\mathrm{Ann}(V)$. Letting $\mathrm{Ann}(V) = (M(\lambda))$, $M(\lambda)$ is called the **minimum polynomial** of T. ie.

$$\mathrm{Ch}(x) = \prod_j (x - \lambda_j)^{r_j} \quad \text{but} \quad M(x) = \mathrm{lcm}\{(x - \lambda_j)^{r_j}\}.$$

Reformulation of the Structure Theorem for f.g. torsion modules.
Let R be a PID and let $a, b \in R$ be relatively prime. Then $Ra + Rb = 1$ so the Chinese Remainder Thm. applies:

$$R \overset{\phi}{\longmapsto\!\!\!\!\to} R/(a) \times R/(b)$$

and $\ker \phi = (a) \cap (b) = (a)(b)$.
Claim. R a PID and $\gcd(a, b) = 1 \Rightarrow (a)(b) = (ab)$.

Proof. $(a)(b) = (c)$ for some c. Since $ab \in (a)(b) = (c)$, $c \mid ab$.

Conversely, $(c) = (a) \cap (b) \subset (a)$ so $a \mid c$ and similarly $b \mid c$. Write $c = \lambda a$ and $c = \mu b$. $\gcd(a, b) = 1 \Rightarrow \exists s, t$ s.t. $sa + tb = 1$. So

$$\begin{aligned} \lambda &= \lambda sa + \lambda bt \\ &= sc + \lambda bt \\ &= s\mu b + \lambda bt \\ &= (s\mu + \lambda t)b \end{aligned}$$

$\therefore (ab) = (c)$. □

Thus

$$R/(ab) \cong R/(a) \times R/(b).$$

By continual application of this iso. we can rewrite our decomposition thm. as follows:

Theorem 2.10.11. *Let M be a f.g. R-module (R a PID). Then*

$$M \cong R^k \oplus R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_n)$$

where $a_n \mid a_{n-1} \mid \cdots \mid a_1 \neq 0$.

$a_1, \ldots, a_n$ are called the **invariant factors** of M.

Example 2.10.12. *Suppose*

$$M \cong \mathbb{Z}/8 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/9 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}/5.$$

Then

$$M \cong \mathbb{Z}/360 \oplus \mathbb{Z}/6 \oplus \mathbb{Z}/2$$

The number of summands required is

$$\max\{r \mid \text{some prime } p \text{ occurs } r \text{ times among the elementary divisors}\}.$$

Reformulation of Chinese Remainder Thm. over a PID. Suppose $m_1, \ldots, m_k$ satisfy $\gcd(m_i, m_j) = 1$ for $i \neq j$. Given $a_1, \ldots, a_k$, $\exists x \in R/(m_1 \cdots m_k)$ s.t. $x \equiv a_j \mod m_j \forall j = 1, \ldots, k$.

Example 2.10.13. *Find x s.t.* $x \equiv 2 \mod 9, x \equiv 3 \mod 5, x \equiv 3 \mod 7.$

Solution. $m_1 = 9, m_2 = 5, m_3 = 7$, $a_1 = 2, a_2 = 3, a_3 = 3$. Set $z_1 := m_2 m_3 = 35$. Then

$$\begin{aligned} y_1 &:= z_1^{-1} \mod 9 \\ &= 8^{-1} \mod 9 \\ &= 8. \end{aligned}$$

Likewise,

$$\begin{aligned} z_2 &:= m_1 m_2 = 60 \\ y_2 &:= z_2^{-1} \mod 5 \\ &= 3^{-1} \mod 5 \\ &= 2, \\ z_3 &:= m_1 m_2 = 45 \\ y_3 &:= z_3^{-1} \mod 7 \\ &= 3^{-1} \mod 7 \\ &= 5. \end{aligned}$$

Set $x := a_1 y_1 z_1 + a_2 y_2 z_2 + a_3 y_3 z_3 \mod (m_1 m_2 m_3)$. Then modulo m_1, $z_2 \equiv 0, z_3 \equiv 0, y_1 z_1 \equiv 1$, so $x \equiv a_1 \mod m_1$, etc. In our example,

$$\begin{aligned} x &= 2 \cdot 8 \cdot 35 + 3 \cdot 2 \cdot 63 + 5 \cdot 3 \cdot 45 \mod (9 \cdot 5 \cdot 7) \\ &= 1613 \mod 315 \\ &= 38 \mod 315. \end{aligned}$$

In general, $x = \sum_j a_j y_j z_j$ where $z_j = m_1 \cdots m_{j-1} m_{j+1} \cdots m_n$ and $y_j = z_j^{-1} \mod m_j$.