Goal: Structure theory for modules over PID, e.g. $\mathbb{Z}$, $\mathbb{R}[x]$

12.1 Noetherian rings and modules.

Let R be a ring with 1.

Definition. An R-module is *Noetherian* if it satisfies the *ascending chain condition (ACC)* on submodules: every strictly increasing chain of submodules is finite.

A ring R is *(left) Noetherian* if R is Noetherian as left R-module (ACC on left ideals).
regular R-mod

Typical **Example.** $\mathbb{Z}$ $\quad (16) \subseteq (8) \subseteq \dots$

$F[x_1, \dots, x_n]$ $\quad$ (Hilbert's Basis Thm)

not Noetherian $\quad \mathbb{R}[x_1, x_2, \dots]$ since $(x_1) \subsetneq (x_1, x_2) \subsetneq \dots$

Theorem. *TFAE:*

(1) *M is Noetherian.*
(2) *Every nonempty set S of submodules of M has a maximal member (with respect to $\subseteq$).*
(3) *Every $N \leq M$ is finitely generated.*

Proof. 1) $\Rightarrow$ 2) Let $M_1 \in S \neq \emptyset$.

If M_1 is not maximal, $\exists M_2 \in S$: $M_1 \subsetneq M_2$

Repeat. Since M is Noetherian, $M_1 \subseteq M_2 \subseteq \dots$ stabilizes in finitely many steps with a maximal $M_n \in S$.

2) $\Rightarrow$ 3) Let $S := \{N' \leq N : N' \text{ is fin generated}\}$ for $N \leq M$.

By 2) S has a max element $N'' \leq N$.

Suppose $N'' \neq N$. Then $\exists x \in N \setminus N''$ and $N'' + \langle x \rangle$ is fin generated contradicting the maximality of N''. Hence $N = N''$ is fin generated.

3) $\Rightarrow$ 1) Let $M_1 \leq M_2 \leq \dots \leq M$.

$N := \bigcup_{i \in \mathbb{N}} M_i \leq M$

By 3) N is fin generated, say $N = R\{a_1, \dots, a_m\}$

Then $\exists n \in \mathbb{N}$: $a_1, \dots, a_m \in M_n$.

So $M_n = N = \bigcup M_i = M_{n+1} = M_{n+2} = \dots$ $\square$

Cor. Every PID is Noetherian

Proof by 3) of the Thm above for the regular R-module.
Submodules of the regular R-mod are ideals of R, hence of the form Ra for some $a \in R$. $\square$

Recall. For any $n \geq 0$ there exists a free R-module $F_R(x_1, \dots, x_n)$ over the free generators $x_1, \dots, x_n$ satisfying

1. the Universal Property for Maps: for any R-module M and $m_1, \dots, m_n \in M$ there exists a unique R-module homomorphism $\Phi \colon F_R(x_1, \dots, x_n) \to M$ with $\Phi(x_i) = m_i$ for all $i \leq n$;
2. every n-generated module M is a homomorphic image of $F_R(x_1, \dots, x_n)$;
3. $F_R(x_1, \dots, x_n) = Rx_1 \oplus \cdots \oplus Rx_n \cong R^n$.

Lemma. *If the ring R is Noetherian, then the R-module R^n is Noetherian for all $n \geq 0$.*

Proof. Show that every $M \leq R^n$ is fin. generated by induction on n.

$n = 0, 1$ by assumption.

Consider $\pi : R^n \to R$, $(x_1, \dots, x_n) \mapsto x_n$

For $M \leq R^n$, then $\pi|_M : M \to R$ satisfies

- $K := \ker \pi|_M \cong$ submodule of R^{n-1}, fin. generated by induction assumption
- $M/K \cong \pi(M) \leq R$, also fin. generated

Combining these yields that M is fin. generated.

Let $K = R\{a_1, \dots, a_m\}$

$M/K = R\{b_1 + K, \dots, b_\ell + K\}$

Claim. $M = R\{a_1, \dots, a_m, b_1, \dots, b_\ell\}$ □

Theorem. *For a ring R TFAE:*

1. *R is a Noetherian ring.*
2. *Every finitely generated R-module is Noetherian.*

Proof. 2) $\Rightarrow$ 1) since R is generated by 1.

1) $\Rightarrow$ 2) Let M be a fin. generated R-mod.

Then $\exists n \in \mathbb{N}$ such that M is a hom image of R^n, $M \cong R^n/K$.

By the previous Lemma R^n is Noetherian

So M is Noetherian by the Correspondence Thm □

Presentations.

Definition. Let M be an R-module. If $M \cong F/K$ for some finitely generated free module $F := F_R(x_1, \ldots, x_n)$ and a finitely generated submodule $K := \langle w_1, \ldots, w_m \rangle$, we say M has the *finite presentation*

$$M = \langle \underbrace{x_1, \ldots, x_k}_{\text{generators}} \mid \underbrace{w_1 = 0, \ldots, w_m = 0}_{\text{relations}} \rangle$$

(M is *finitely presented* for short).

For each $i \leq m$ we have $a_{ij} \in R$ such that

$$w_i = \sum_{j=1}^{n} a_{ij} x_j.$$

Let $A = (a_{ij}) \in M_{m \times n}(R)$. Then we can rewrite the presentation of $M \cong F/K$ as

$$M = \langle x_1, \ldots, x_k \mid A \cdot (x_1, \ldots, x_n)^T = 0 \rangle.$$

Corollary. *Every finitely generated module M over a Noetherian ring R is finitely presented.*

Running example: $R = \mathbb{Z}$

$F = \mathbb{Z}x_1 \oplus \mathbb{Z}x_2 \cong \mathbb{Z}^2$

$K = \langle \underbrace{36x_2}_{w_1}, \underbrace{6x_1 + 6x_2}_{w_2}, \underbrace{4x_1 + 10x_2}_{w_3} \rangle$

$$M = F/K = \langle x_1, x_2 \mid \underbrace{\begin{array}{l} 36x_2 = 0 \\ 6x_1 + 6x_2 = 0 \\ 4x_1 + 10x_2 = 0 \end{array}}_{\text{relations}} \rangle$$

$$\underbrace{\begin{pmatrix} 0 & 36 \\ 6 & 6 \\ 4 & 10 \end{pmatrix}}_{= A} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Lemma (Changing presentations)**.** *Let* $A \in M_{m\times n}(R)$ *and*

$$M = \langle x_1, \dots, x_n \mid A \cdot (x_1, \dots, x_n)^T = 0\rangle$$

be a finitely presented R*-module. Let* $P \in M_{m\times m}(R)$ *and* $Q \in M_{n\times n}(R)$ *be invertible. Then*

$$M = \langle y_1, \dots, y_n \mid PAQ \cdot (y_1, \dots, y_n)^T = 0\rangle$$

is another presentation of M*.*

Proof. Note $M \cong F/K$ for

$$\begin{aligned}
&F := F_R(x_1, \dots, x_n)\\
&(w_1, \dots, w_m)^T := A \cdot (x_1, \dots, x_n)^T\\
&K := \langle w_1, \dots, w_m\rangle\\
&(y_1, \dots, y_n)^T := Q^{-1} \cdot (x_1, \dots, x_n)^T
\end{aligned}$$

Claim 1. F is free over $y_1, \dots, y_n$.

- $y_1, \dots, y_n$ generates F since $Q(y_1, \dots, y_n)^T = (x_1, \dots, x_n)^T$.
- To show the universal property, let N be an R-module and $v_1, \dots, v_n \in N$. Since F is free over $x_1, \dots, x_n$, there exists a homomorphism

  $$\varphi\colon F \to N \text{ with } (x_1, \dots, x_n)^T \mapsto Q(v_1, \dots, v_n)^T \quad \text{(componentwise).}$$

  Then

$$(y_1, \dots, y_n) = Q^{-1}(x_1, \dots, x_n)^T \overset{\varphi}{\to} Q^{-1}Q(v_1, \dots, v_n)^T = (v_1, \dots, v_n)^T.$$

We proved Claim 1 and that $(x_1, \dots, x_n)^T \to (y_1, \dots, y_n)^T$ extends to an automorphism of F.

Let

$$(v_1, \dots, v_m)^T := P(w_1, \dots, w_m)^T$$

Claim 2. $K = \langle v_1, \dots, v_m\rangle$.

- $\supseteq$ is clear.
- $\subseteq$ follows since $P^{-1}(v_1, \dots, v_m)^T = (w_1, \dots, w_m)^T$.

This proves Claim 2. Thus

$$M \cong F_R(y_1, \dots, y_n)/\langle v_1, \dots, v_m\rangle$$

and moreover

$$(v_1, \dots, v_m)^T = P(w_1, \dots, w_m)^T = PA(x_1, \dots, x_n)^T = PAQ(y_1, \dots, y_n)^T$$

□

Theorem. (Row reduction in PIDs) *Let R be a PID. For every $A \in M_{m\times n}(R)$ there exist invertible $P \in M_{m\times m}(R)$ and $Q \in M_{n\times n}(R)$ such that*

$$D = PAQ \text{ is a diagonal matrix with diagonal entries } a_1|a_2|\dots|a_l \quad , \text{ i.e. } (a_1) \supseteq (a_2) \supseteq \dots$$

for $l := \min(m,n)$.

$$E_{ij} := \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & 1 & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \leftarrow i, \quad \uparrow j$$

Proof. We find D using the following row operations on A that can be obtained by multiplication with invertible $m \times m$ matrices on the left.

(R1) *Switching rows i and j of A.* For a permutation matrix $S := E_{ij} + E_{ji} + \sum_{k\neq i,j} E_{kk}$ compute SA.

$$\begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 0 & & 1 & \\ & & & \ddots & & \\ & & 1 & & 0 & \\ & & & & & \ddots \end{pmatrix} \cdot \begin{pmatrix} - & a_i & - \\ - & a_j & - \end{pmatrix} = \begin{pmatrix} - & a_j & - \\ - & a_i & - \end{pmatrix}$$

(R2) *Add c times row i to row j of A.* For $T := I_m + cE_{ji}$ compute TA.

$$j \rightarrow \begin{pmatrix} 1 & & \\ & \ddots & \\ c & & 1 \end{pmatrix} \cdot \begin{pmatrix} - & a_i & - \\ - & a_j & - \end{pmatrix} = \begin{pmatrix} - & a_i & - \\ - & ca_i + a_j & - \end{pmatrix}$$

(R3) *Scale row i and add a multiple of row j to replace a_{ik} by $d := \gcd(a_{ik}, a_{jk})$ if $d \neq 0$.*

Let $\begin{pmatrix} u_{ii} & u_{ij} \\ u_{ji} & u_{jj} \end{pmatrix}$ such that (a) $d = u_{ii}a_{ik} + u_{ij}a_{jk}$ and (b) $u_{ii}u_{jj} - u_{ij}u_{ji} = 1$.
Since R is a PID, we have $u_{ii}, u_{ij} \in R$ satisfying (a); moreover $\gcd(u_{ii}, u_{ij}) = 1$ since $d \neq 0$. Hence we find u_{jj}, u_{ji} satisfying (b).

For $U := u_{ii}E_ii + u_{ij}E_{ij} + u_{ji}E_{ji} + u_{jj}E_{jj} + \sum_{k\neq i,j} E_{kk}$ compute UA.

$$\begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & u_{ii} & u_{ij} & \\ & & u_{ji} & u_{jj} & \\ & & & & \ddots \end{pmatrix} \cdot \begin{pmatrix} - & a_i & - \\ - & a_j & - \end{pmatrix} = \begin{pmatrix} - & u_{ii}a_i + u_{ij}a_j & - \\ - & & - \end{pmatrix}$$

Claim. Applying row operations (R1)-(R3) and corresponding column operations (C1)-(C3) (via multiplications with invertible $n \times n$ matrices on the right) A can be transformed into a diagonal matrix D with diagonal entries $a_1|a_2|\dots|a_l$.

Switching rows and columns if necessary we may assume that $a_{11} \neq 0$. First transform A until a_{11} has as few prime factors as possible:

(1) For $k \leq m$, if a_{11} does not divide a_{k1}, let $d := \gcd(a_{11}, a_{k1}) \neq 0$ and use (R3) to get a new matrix B with $b_{11} = d$. Note that b_{11} has fewer prime factors than a_{11}.
(2) Similar for a_{1k}.

After finitely many step we have a new matrix A such that $a_{11} \mid a_{i1}, a_{1j}$ for all i, j.

Ex continued:

$$A = \begin{pmatrix} \boxed{0} & 36 \\ 6 & 6 \\ \boxed{4} & 10 \end{pmatrix} \xrightarrow{R1} \begin{pmatrix} \boxed{4} & 10 \\ \boxed{6} & 6 \\ 0 & 36 \end{pmatrix} \xrightarrow{R3} \begin{pmatrix} 2 & -4 \\ 6 & 6 \\ 0 & 36 \end{pmatrix}$$

$$\gcd(4,6) = 2 = (-1)4 + 1\cdot 6$$

(3) Using (R2) and (C2) we can now transform A into a block diagonal matrix
$$\begin{pmatrix} a_{11} & 0 \\ 0 & A' \end{pmatrix}.$$

(4) If a_{11} does not divide a_{ij} for some i, j, add row i to row 1 by (R2) and go to step (2) to further reduce the number of prime factors of a_{11}.

Since a_{11} only has finitely many factors, after finitely many steps we have a matrix $A = \begin{pmatrix} a_{11} & 0 \\ 0 & A' \end{pmatrix}$ such that $a_{11}|a_{ij}$ for all i, j.

Repeat the process for the $(m-1) \times (n-1)$-matrix A' to get the Claim. Since the row and column operations were obtained by multiplication with invertible matrices, we have $D = PAQ$ as required. □

Corollary. *Let R be a PID. Every submodule of the free module R^n of rank n is a free module of rank $\leq n$.*

Proof. Let $K \leq R^n$. Then K is finitely generated, say $K = \langle w_1, \ldots, w_m \rangle$ where
$$(w_1, \ldots, w_m)^T = A \cdot (x_1, \ldots, x_n)^T$$
for some $A \in M_{m \times n}(R)$.

By the previous Theorem (row reduction) and Lemma (changing presentation) we obtain free generators $y_1, \ldots, y_n$ for R^n and generators $v_1, \ldots, v_m$ for K such that
$$(v_1, \ldots, v_m)^T = PAQ(y_1, \ldots, y_n)^T = D(y_1, \ldots, y_n)^T = (a_1 y_1, \ldots, a_l y_l, 0, \ldots, 0)^T$$
Then $K = Ra_1 y_1 \oplus \cdots \oplus Ra_l y_l \cong Ra_1 \oplus \cdots \oplus Ra_l$ since $y_1, \ldots, y_n$ is a basis. Since $Ra_i \cong R$ if $a_i \neq 0$ the result follows. □

The Structure Theorem for finitely generated modules over PIDs.

Let R be a PID.

Structure Theorem (Invariant Factor Form). *Let M be a finitely generated R-module for a PID R. Then*

$$M \cong R/(a_1) \oplus \cdots \oplus R/(a_k) \oplus R^r$$

where $k, r \geq 0$, $a_1, \ldots, a_k \in R$ are neither 0 nor a unit and $a_1|a_2|\ldots|a_k$.
$a_1, \ldots, a_k$ are the invariant factors *of M.*
r is the free rank *of M.*

Note. This decomposition of M is unique up to isomorphism (see below), i.e., if also

$$M \cong R/(b_1) \oplus \cdots \oplus R/(b_l) \oplus R^s$$

for $l, s \geq 0$, $b_1, \ldots, b_l \in R$ neither 0 nor a unit and $b_1|b_2|\ldots|b_l$, then $r = s, k = l$ and $(a_i) = (b_i)$ for all $i \leq k$.

Hence the invariant factors are unique up to multiplication with units.

Proof. Since R is Noetherian, M has a finite presentation. Apply a change of presentation with invertible matrices P, Q and diagonal D as in the previous Theorem to get

$$M = \langle y_1, \ldots, y_n \mid a_1 y_1 = 0, \ldots, a_l y_l = 0 \rangle$$

with $a_1|a_2|\ldots|a_l$.

Set $a_{l+1} := \ldots a_n := 0$ if $n > l$ to get

$$M = \langle y_1, \ldots, y_n \mid a_1 y_1 = 0, \ldots, a_n y_n = 0 \rangle = Ry_1 \oplus \ldots Ry_n \cong R/(a_1) \oplus \cdots \oplus R/(a_n).$$

If a_i is a unit, then $Ry_i \cong R/(a_i) \cong 0$ can be omitted.
If $a_i = 0$, then $Ry_i \cong R/(a_i) \cong R$. $\square$

Primary Decomposition Theorem. *Let M be a torsion R-module for a PID R with annihilator (a) where*

$$a = p_1^{\alpha_1} \dots p_n^{\alpha_n}$$

for distinct primes $p_1, \dots, p_n \in R$ and $\alpha_1, \dots, \alpha_n \in \mathbb{N}$. Then

$$M \cong M_1 \oplus \cdots \oplus M_n$$

*where $M_i := \{m \in M \mid p_i^{\alpha_i} m = 0\}$ is the p_i-*primary component *of M.*

Proof. Exercise 10.3.18. □

Decomposing $R/(a_i)$ into its primary components yields

Structure Theorem (Elementary Divisor Form). *Let M be a finitely generated R-module for a PID R. Then*

$$M \cong R/(p_1^{\alpha_1}) \oplus \cdots \oplus R/(p_n^{\alpha_n}) \oplus R^r$$

where $p_1, \dots, p_n \in R$ are (not necessarily distinct) primes, $\alpha_1, \dots, \alpha_n, r \in \mathbb{N}$. $p_1^{\alpha_1}, \dots, p_n^{\alpha_n}$ are the elementary divisors *of M.*

Structure Theorem (Uniqueness). *Let M, N be a finitely generated R-modules for a PID R. TFAE:*

(1) *$M \cong N$*
(2) *M, N have the same free rank and invariant factors.*
(3) *M, N have the same free rank and elementary divisors.*

Proof Sketch.
For (1)⇒(3) we need

Lemma. *For a prime $p \in R$, let $F := R/(p)$. Then*

(1) *$R^n/(p)R^n \cong F^n$*
(2) *$R/(p^\alpha) \,/\, pR/(p^\alpha) \cong F$*

Assume $M \cong N$. Then

- Their torsion parts and their complements are isomorphic. Hence their free ranks are equal by (1) of the Lemma.
- Their p-primary components are isomorphic for every prime p, say with annihilator (p^α). Induct on α and use (2) of the Lemma to obtain that their elementary divisors are the same.