Setup

Ring $(R, +, \cdot)$

① $(R,+)$ abelian group

- $a+(b+c) = (a+b)+c$ for all $a,b,c \in R$
- $a+b = b+a$ for all $a,b \in R$
- $\exists 0 \in R$ $a+0 = a$ for all $a \in R$
- for all $a \in R$ there exists $-a \in R$ st $a+(-a)=0$

② $(R, \cdot)$ is a commutative monoid

- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a,b,c \in R$
- $a \cdot b = b \cdot a$ for all $a,b \in R$
- $\exists 1 \in R$ such that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$

③ $a \cdot (b+c) = a \cdot b + a \cdot c$ for all $a,b,c \in R$

④ $1 \neq 0$

Examples

1) $\mathbb{Z}$
2) $\mathbb{Z}/n$
3) polynomial rings $R = k[x_1, \dots, x_n]$ (k field)
4) Quotients of polynomial rings: $\dfrac{k[x_1, \dots, x_n]}{I}$
5) Power series rings: $R = k[[x_1, \dots, x_n]]$

Elements are (formal) power series $\sum_{a_i \geq 0} c_{a_1, \dots, a_n} x_1^{a_1} \cdots x_n^{a_n}$

6) Polynomial rings in infinitely many variables $k[x_1, \dots]$

Ring Homomorphism $f: R \to S$ map of rings satisfying

① $f(a+b) = f(a) + f(b)$

② $f(ab) = f(a) f(b)$

③ $f(1) = 1$

Subring $R \subseteq S$ rings. R is a subring of S if the operations on R are restrictions of the operations on S, and $1_R = 1_S$.

Ideal $I \subseteq R$ is an ideal of the ring R if

- I is closed for $+$: $a+b \in I$ $\quad a, b \in I \Rightarrow$
- I is closed for products by elements in R: $R \cdot I \subseteq I$
- $I \neq \emptyset$ $\quad (\Rightarrow 0 \in I)$

Def the ideal generated by $f_1, \dots, f_n \in R$ is the smallest ideal of R containing $f_1, \dots, f_n$:

$$(f_1, \dots, f_n) = \{ r_1 f_1 + \dots + r_n f_n : r_i \in R \}$$

Note Any ring has at least 2 ideals: $(1) = R$ and (0).

Convention When we say ideal, we usually mean $I \neq R$

Example the ideals in $\mathbb{Z}$ are all principal, so of the form (n)

<u>Module</u> An R-module M is an abelian group $(M, \circ)$ with an R-multiplication

$$R \times M \xrightarrow{\cdot} M$$
$$(r, m) \longmapsto r \cdot m = rm$$

satisfying

- $r(a+b) = ra + rb$ for all $r \in R$, $a, b \in M$
- $(r+s)a = ra + sa$ for all $r, s \in R$, $a \in M$
- $(rs)a = r(sa)$ for all $r, s \in R$, $a \in M$
- $1a = a$ for all $a \in M$

<u>Note</u> For us, all modules are 2-sided (no left/right modules)

<u>Submodule</u> $M \subseteq N$ modules, R-module structure on M is reduction from N

<u>Homomorphism of R-modules</u> $f: M \to N$ map of R-modules

- $f(a+b) = f(a) + f(b)$ for all $a, b \in M$
- $f(rb) = r f(b)$ for all $r \in R$, $a \in M$

1^{st} <u>Isomorphism Theorem</u> $f: M \to N$ R-module homomorphism

$$\operatorname{im} f \cong M/\ker f$$

<u>Example</u> Submodules of R = ideals of R

<u>Example</u> $R = k$ a field $\Rightarrow$ R-modules = k-vector spaces

R-module homomorphisms = linear maps

<u>Warning!</u> vector spaces are a <u>lot</u> simpler than R-modules

An R-module M is *generated* by $\Gamma \subseteq M$ if every element in M is an R-linear combination of elements in Γ (with finitely many $\neq 0$ coefficients)

We also say Γ is a *generating set* for M

M is finitely generated if there is a *finite* generating set for M

fg R-mod $\equiv$ finitely generated R-module

$\Gamma \subseteq M$ is a *basis* for M if

- Γ generates M
- Γ is linearly independent $\left(\sum_i \underbrace{x_i}_{\in R} \underbrace{\gamma_i}_{\in \Gamma} = 0 \Rightarrow \text{all } x_i = 0 \right)$

Most R-modules **do not** have a basis

A *free R-module* is an R-module with a basis.

In general, given a generating set $\Lambda = \{\lambda_i\}_{i \in I}$ for an R-mod M,

$$\bigoplus_I R \xrightarrow{\pi} M$$
$$(x_i)_{i \in I} \longmapsto \sum_i x_i \lambda_i$$

(this works even if M is not fg
the elements in $\bigoplus_I R$ are tuples
with only finitely many $\neq 0$ entries)

$$\begin{cases} \cdot\ \Lambda = \{\lambda_i\}_{i\in I} \text{ generates } M \Rightarrow \pi \text{ is surjective} \\ \cdot\ \Lambda = \{\lambda_i\}_{i\in I} \text{ is a linearly independent} \Rightarrow \pi \text{ is injective} \end{cases}$$

M is free $\Leftrightarrow$ $M \cong \oplus R$ some direct sum of copies of R

Most modules are <u>not</u> free. Usually, $\ker \pi$ nontrivial

(even when we take a "minimal generating set", when that's a thing)

<u>Ex</u> $R = k[x,y]$ $\qquad M = I = (x^2, xy, y^2)$ is <u>not</u> free

$\Lambda = \{x^2, xy, y^2\}$ is a generating set, but linearly dependent

$$\text{eg, } y \cdot x^2 - x \cdot xy = 0$$

$$\begin{aligned} R^3 &\xrightarrow{\pi} M \\ (a, b, c) &\longmapsto a x^2 + b xy + c y^2 \end{aligned}$$

$$(y, -x, 0) \in \ker \pi$$

$$\left(\text{actually } \ker \pi = R \cdot (y, -x, 0) + R \cdot (0, y, -x)\right)$$

Noetherian Rings

A ring R is **noetherian** if every ascending chain

$$I_0 \subseteq I_1 \subseteq \cdots$$

of ideals in R stabilizes, meaning $I_n = I_N$ for all $n \geq N$

Proposition 1.2 R ring TFAE:

1. R is noetherian
2. Every nonempty family of ideals has a maximal element
3. Every ascending chain of fg ideals of R stabilizes
4. Given any generating set S for any ideal I, I is generated by some finite subset of S
5. Every ideal in R is finitely generated

Proof

1 ⇒ 2 Suppose Λ is a family of ideals with no max. this means we can inductively construct an infinite chain:

$$I_0 \subsetneq I_1 \subsetneq \cdots$$

② ⇒ ① Given an ascending chain

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$$

the family $\{I_i\}_{i\geq 0}$ has a maximal element $I_N \Rightarrow I_n = I_N$ for $n \geq N$

① ⇒ ③ obvious

③ ⇒ ④ Suppose there is an ideal I and a generating set S such that no finite subset of S generates I.
Start with a finite subset $S' \subseteq S$. Since $(S') \neq I$, there exists $s_1 \in S$ st $s \notin (S')$. Then

$$(S') \subsetneq (S' \cup \{s_1\}) \neq I, \text{ so find } s_2 \in S,\ s_2 \notin (S' \cup \{s_1\})$$

$\Rightarrow$ construct an infinite ascending chain