Course Commutative Algebra

Commutative Algebra studies

- the generalization of vector spaces, i.e. modules over commutative rings (they naturally come up in algebraic geometry, e.g. invariant theory, and in complex geometry, e.g. the theory of vector bundles over a complex manifolds.)

- the study of ring extensions and decomposition of ideals in commutative rings. (related to number theory when

there is no unique prime factorization anymore.)

<u>More concrete:</u>

Number theory related to Algebraic Geometry (CA is the algebraic part of AG)

Let k be a field. Number theoretical problems are related to algebraic varieties

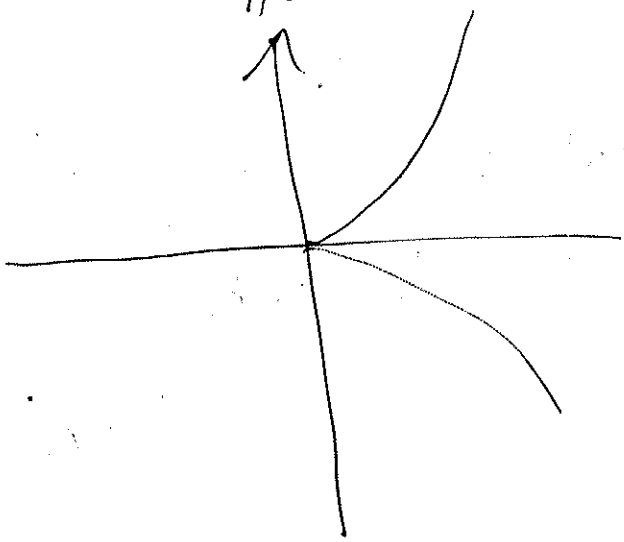
$$\{ \underline{x} \in k^n \mid P_1(\underline{X}) = \dots = P_m(\underline{X}) = 0 \} =: V_k(P_1, \dots, P_m)$$

$$P_1, \dots, P_m \in k[X_1, \dots, X_n]$$

Two 1st approaches to study them

① If there is a topology on it then use top. arguments to study it

Ex: $V = V_{\mathbb{R}}(Y^2 - X^3) = \{(t^2, t^3) \mid t \in \mathbb{R}\}$



"cuspidal cubic"

Here we have the Euclidian topology.

② Analyze its algebraic structure first

In our example we see that V is "algebraically irreducible", i.e. not a proper union of algebraic varieties, because $P = Y^2 - X^3$ is irreducible $/\mathbb{R}$

(in fact $/\mathbb{C}$ $\Rightarrow$ $V_{\mathbb{C}} = \{(x,y) \in \mathbb{C}^2 \mid P(x,y) = 0\}$ is connected in the Euclidian topology)

So its isomorphy class is related (up to density) to the isomorphy class of its function field:

$$Q\left(\mathbb{R}[X,Y]/(Y^2-X^3)\right) \simeq \mathbb{R}(T)$$

seen as polynomial functions.

$$X \longmapsto T^2$$
$$Y \longmapsto T^3$$

(This is not very informative, because it does not see the cusp at (0,0).)

In fact the "algebraic isomorphism ~~cat~~ class" is given by the $\mathbb{R}$-algebra isomorphism class of its "coordinate ring" $\mathbb{R}[X,Y]/(Y^2-X^3)$

$$\simeq \mathbb{R}[T^2, T^3] \subseteq \mathbb{R}[T].$$

<u>Proof of this iso:</u>

$$\mathbb{R}[X,Y]/(Y^2-X^3) \xrightarrow{\varphi} \mathbb{R}[T^2,T^3]$$

$$[X] \longmapsto T^2$$

$$[Y] \longmapsto T^3$$

$$[P] \longmapsto P(T^2,T^3)$$

- surjective ✓
- $\mathbb{R}$-algebra homomorphism ✓
- injective? <u>Show:</u> $\ker(\varphi) = \{[0]\}$

<u>Proof:</u> $\varphi([P]) = 0 \Rightarrow P(T^2,T^3) = 0$

As $P(X,Y) = Q_2(X,Y)(Y^2-X^3)$
$+ Q_1(X)Y + Q_2(X)$

(Q_i polynomials over $\mathbb{R}$)

we get $0 = Q_1(T^2)T^3 + Q_0(T^2)$.

Only possible if Q_1 and Q_0 are zero polynomials, because otherwise

$2 \nmid \deg Q_1(T^2)T^3$ and $2 \mid \deg Q_0(T^2)$ ↯.

This iso does sees the cusp!

Here is the point: ② can be generalized to fields without topology!

For example finite fields or $k(X)$ or extensions of them in particular their algebraic closure.

So to sum up:

The study of AG amounts to the study of their coordinate rings

i.e. the study

- of their modules
- of ring extensions of them
- of their ideal / prime ideal structure.

<u>Convention:</u> If we refer to a ring R we always mean in this course that R is <u>commutative</u> with $1_R \neq 0_R$.

Chapter I

Modules over commutative rings

I.1. 1st definitions

<u>Def 1:</u> Let R be a ring. A tuple $((M,+),\cdot)$ is called an R-module if
- $(M,+)$ is an abelian group
- $\cdot : R \times M \longrightarrow M$ satisfies

the distributivity laws:

$\forall_{r_1,r_2,r \in R,\ m_1,m_2,m \in M}$:

(D1) $(r_1+r_2)m = r_1 m + r_2 m$

(D2) $r(m_1+m_2) = r m_1 + r m_2$.

the associativity law

(A) $\forall_{r_1,r_2 \in R}\ \forall_{m \in M}$: $r_1(r_2 m) = (r_1 r_2) m$

and the identity law

(I) $\forall_{m \in M}: 1_R \cdot m = m$.

<u>Remark 2:</u> For non-commutative rings we can define left and right modules.

$R \times M \to M$ (see above) for <u>left</u>

$M \times R \to M$ for <u>right</u>

<u>Examples 3:</u>

(a) The ring $(\mathbb{Z}, +, \cdot)$ is a $\mathbb{Z}$-module, i.e. over itself a module.

$$\mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$
$$(z_1, z_2) \longmapsto z_1 \cdot z_2$$

- $(\mathbb{Z}, +)$ abelian group ✓
- $\mathbb{Z}$ satisfies (D1), (D2), (A), (I) as a ring.

(b) $R \subseteq S$ a ring extension.

S is an R-module

$$R \times S \longrightarrow S$$
$$(r, s) \longmapsto r \cdot s.$$

because S satisfies (D1), (D2), (A), (I)
as a ring, e.g.

$\mathbb{Q}$ is a $\mathbb{Z}$-module

$\mathbb{R}$ is a $\mathbb{Q}$-module ($\mathbb{Q}$ vector space)

(c) $\mathbb{R}^\times = \{r \in \mathbb{R} \mid \exists s \in \mathbb{R} : rs = sr = 1\} = \mathbb{R} \setminus \{0\}$

is a $\mathbb{Z}$-module via

$z * r := r^z$ on the abelian group

$(\mathbb{R}^\times, \odot)$: $r_1 \odot r_2 := r_1 r_2$.

(exercise assigned)

(d) $\mathbb{R}^{>0} = \{r \in \mathbb{R} \mid r > 0\}$ is a $\mathbb{Q}^\times$-module

via $\frac{a}{b} * r := \sqrt[b]{r^a}$ on

$(\mathbb{R}^{>0}, \odot)$. $(a \in \mathbb{Z}, b \in \mathbb{Z}^{>0})$

<u>Proof</u>: • $*$ is well-defined:

$$\frac{a}{b} = \frac{c}{d} \in \mathbb{Q}, \quad r \in \mathbb{R}^{>0}$$

$$\Rightarrow \quad ad = bc \Rightarrow r^{ad} = r^{bc}$$

$$\underset{r>0}{\Rightarrow} \quad \underbrace{\sqrt[b]{r^{ad}}}_{= \left(\sqrt[b]{r^a}\right)^d} = r^c \Rightarrow \sqrt[b]{r^a} = \sqrt[d]{r^c}$$

$$\Rightarrow \frac{a}{b} * r = \frac{c}{d} * r.$$

- (I) $\quad 1 * r = \sqrt[1]{r^1} = r$

- (D1) $\quad \left(\frac{a}{b} + \frac{c}{d}\right) * r = \sqrt[bd]{r^{ad+bc}} = \sqrt[bd]{r^{ad} r^{bc}}$

$$\underset{r>0}{=} \sqrt[bd]{r^{ad}} \sqrt[bd]{r^{bc}} = \sqrt[b]{r^a} \sqrt[d]{r^c}$$

(D2) $\quad \frac{a}{b} * (r_1 \odot r_2) = \sqrt[b]{(r_1 r_2)^a} = \sqrt[b]{r_1^a r_2^a}$

$$\overset{r_i>0}{=} \sqrt[b]{r_1^a} \sqrt[b]{r_2^a} = \left(\frac{a}{b} * r_1\right) \odot \left(\frac{a}{b} * r_2\right)$$

- (A) $\quad \left(\frac{a}{b} \cdot \frac{c}{d}\right) * r = \sqrt[bd]{r^{ac}}$

$$= \sqrt[b]{\left(\sqrt[d]{r^c}\right)^a} = \frac{a}{b} * \left(\frac{c}{d} * r\right)$$

$\square$

(e) R a ring $\quad R^n$ is an R module via $\quad r * \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} := \begin{pmatrix} r r_1 \\ \vdots \\ r r_n \end{pmatrix}$

- $(R^n, +)$ is an abelian group
  $\uparrow$ component-wise
- (I), (D*), (A) are inherited ~~by~~ from R, e.g.

(D1) $$(r_1 + r_2) * \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} (r_1 + r_2) x_1 \\ \vdots \\ (r_1 + r_2) x_n \end{pmatrix}$$

$$= \begin{pmatrix} r_1 x_1 + r_2 x_1 \\ \vdots \\ r_1 x_n + r_2 x_n \end{pmatrix} = \begin{pmatrix} r_1 x_1 \\ \vdots \\ r_1 x_n \end{pmatrix} + \begin{pmatrix} r_2 x_1 \\ \vdots \\ r_2 x_n \end{pmatrix}$$

$$= r_1 * \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + r_2 * \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

<u>end lecture 1, 14.09.21</u>

(f) Let V be an $\mathbb{R}$-vector space of finite dimension m. A $\mathbb{Z}$-lattice in V is a $\mathbb{Z}$-module $\Lambda \subseteq V$ s.t. $\exists$ $\mathbb{R}$-basis $v_1, \dots, v_m$: $\Lambda = \mathbb{Z} v_1 + \dots + \mathbb{Z} v_m$.

With these we can define ~~nice~~ nice simplicial geometric spaces.
(generalization of trees)

<u>Example:</u> $W = \mathbb{Q}^n \subseteq \mathbb{R}^n$.

Two lattices $\Lambda_1, \Lambda_2 \subseteq W$ are called equivalent if $\exists\, z_1, z_2 \in \mathbb{Z} \setminus \{0\}$: $z_1 \Lambda_1 = z_2 \Lambda_2$.

$\left(z\Lambda := \{ zx \mid x \in \Lambda \} \right)$

~~Ex: $\mathbb{Q}^2 \supseteq \Lambda_1 := \{ (x_1, x_2) \mid x_1 + x_2 = 0 \}$~~

~~and~~

<u>Ex:</u> $\mathbb{Q}^2 \supseteq \Lambda_1 = \{ (x_1, 2x_1) \mid x_1 \in \mathbb{Z} \}$

and $\Lambda_2 = \{ (\frac{7}{9} x_1, \frac{14}{9} x_1) \mid x_1 \in \mathbb{Z} \}$

are equivalent, because

$9\Lambda_2 = \Lambda_1$

$[\Lambda] = [\Lambda]_{\mathbb{Q}^\times} :=$ "equivalence class of Λ"
$=$ "homothety class of Λ".

$\mathrm{Latt}(W) := \{ [\Lambda] \mid \Lambda \text{ lattice in } W \}$

<u>Define a graph:</u>

Vertices: $[\Lambda] \in \mathrm{Latt}(W)$

Edges: $[\Lambda_1]$ and $[\Lambda_2]$ are incident (i.e. are ends of an edge) if $[\Lambda_1] \neq [\Lambda_2]$ and $\exists\ z_1, z_2 \in \mathbb{Z} \setminus \{0\}$: $z_1 \Lambda_1 \supseteq z_2 \Lambda_2$ and

$$z_1\Lambda_1 / z_2\Lambda_2 \simeq \text{simple non-trivial group.}$$

($\simeq \mathbb{Z}/p\mathbb{Z}$ for some prime p.)

<u>Exercise</u>: (assigned): The graph is connected.

<u>Proof</u> (Sketch): Take $[\Lambda_1], [\Lambda_2] \in \mathrm{Latt}(W)$.

<u>Step 1</u>: $\exists\ z_1, z_2 \in \mathbb{Z} \setminus \{0\}$:

$$z_1 \Lambda_1 \supseteq z_2 \Lambda_2$$

So without loss of generality:

$\Lambda_1 \supseteq \Lambda_2$

<u>Step 2:</u> Prove that $\left| \Lambda_1 / \Lambda_2 \right| < \infty$

<u>Step 3:</u> We need to show that

$\exists\ \Lambda_0', \Lambda_1', \Lambda_2', \dots, \Lambda_\ell' :$

$[\Lambda_0'] = [\Lambda_1]$ and $[\Lambda_\ell'] = [\Lambda_1]$

and $\forall_{i=0,\dots,\ell-1}$: $\{[\Lambda_i'], [\Lambda_{i+1}']\}$

is an edge.

Proof by induction on $\left| \Lambda_1 / \Lambda_2 \right|$.

<u>base case:</u> 1) $\left| \Lambda_1 / \Lambda_2 \right| = 1 \implies [\Lambda_1] = [\Lambda_2]$.

2) $\left| \Lambda_1 / \Lambda_2 \right| = 2 \implies$ By definition

$\{[\Lambda_1], [\Lambda_2]\}$ is a singleton

or an edge.

(Singleton if $m=1$, $W=\mathbb{Q}$, $\Lambda_2 = 2\Lambda_1$)

(IS) "induction step":

Suppose $|\Lambda_1/\Lambda_2| > 2$. If it is a prime then we are done.

If not $\exists$ $\underset{\substack{\shortparallel \\ [x]_{\Lambda_2}}}{x + \Lambda_2} \in \Lambda_1/\Lambda_2$:

$\operatorname{ord}([x]_{\Lambda_2})$ is a prime

$\tilde{\Lambda} := \mathbb{Z}x + \Lambda_2$.

$\Rightarrow \quad \Lambda_1 \supsetneq \tilde{\Lambda} \supsetneq \Lambda_2$

and $|\Lambda_1/\tilde{\Lambda}|$, $|\tilde{\Lambda}/\Lambda_2|$ both are $< |\Lambda_1/\Lambda_2|$.

(IH) $\Rightarrow$ $\exists$ $\Lambda'_0, \dots, \Lambda'_{\ell_1}$ for connecting $[\Lambda_1]$ with $[\tilde{\Lambda}]$ and

$\exists$ $\Lambda'_{\ell_1}, \dots, \Lambda'_{\ell_2}$ for connecting $[\tilde{\Lambda}]$ with $[\Lambda_2]$. $\square$

(g) Let R be a ring and $J_1, \dots, J_m$ be ideals of R. Then

$$M := R/J_1 \times R/J_2 \times \dots \times R/J_m$$

is an R module, via

$$r * ([r_1]_{J_1}, \dots, [r_m]_{J_m}) := ([r r_1]_{J_1}, \dots, [r r_m]_{J_m})$$

E.g. $R := \mathbb{Q}[X]$. $M := \mathbb{Q}[X]/(X^2+1) \oplus \mathbb{Q}[X]/(X^2-1)$

is a $\mathbb{Q}[X]$-module

This is a new module, because it cannot be embedded in any $\mathbb{Q}(X)$-vector space, because $P := (X^2+1)(X^2-1)$
$= X^4 - 1$
annihilates every element of M, i.e. $P \cdot m = 0_M \ \forall m \in M$, and $P \neq 0_{\mathbb{Q}[X]}$.

We call M a <u>torsion module</u>

Lots of notion for abelian groups and vector spaces carry over to modules (sum, direct sum (inner, outer), factor modules, submodules.)

<u>Def 4:</u> Let M be an R-module

1) A subset $N \subseteq M$ is called an R-submodule if $(N, +|_{N \times N})$ is a subgroup of M and $\forall_{r \in R} \forall_{n \in N}: rn \in N$.

2) Let N_i, $i \in I$, be R-submodules of M. ~~There~~ Their sum is defined as

$$\sum_{i \in I} N_i := \{ \sum_{i \in I} n_i \mid n_i \in N_i, \; n_i = 0 \text{ for almost all } i \in I \}$$

(meaning at most finitely many are non-zero.)

The sum is called an <u>(inner) direct</u> sum if $\forall (n_i)_{i \in I} \in \bigtimes_{i \in I} N_i$ s.t. $n_i = 0$ f.a.a. $i \in I$

$\left(\sum_{i \in I} n_i = 0 \implies \forall_{i \in I} : n_i = 0 \right)$

3) M/N, for $N \underbrace{\leq_R}_{\text{"R-submodule"}} M$, is

an R-module via

$r * [m]_N := [rm]_N$

(~~exercise~~ assignment: well-def., axioms.)

M/N is called <u>the factor module of M by N</u>

4) Let $S \subseteq M$ be a subset.

$\langle S \rangle_R := \bigcap_{S \subseteq N \leq_R M} N$ is called the

R-submodule of M generated by S.

<u>Def 5:</u> (outer direct sum)

Let M_i, $i \in I$, be a family of R-modules.

(a) The module

$$\bigoplus_{i \in I} M_i := \{ (m_i)_{i \in I} \mid m_i \in M_i \text{ and } m_i = 0 \text{ f.a.a. } i \in I \}$$

is an R-module called the (outer) direct sum of the M_i, $i \in I$.

(b) The ~~set~~ set

$$\prod_{i \in I} M_i := \{ (m_i)_{i \in I} \mid m_i \in M_i, i \in I \}$$

with the structure

$r.(m_i)_{i \in I} := (r m_i)_{i \in I}$ is an R-module called the <u>direct product</u> of the M_i, $i \in I$.

Examples 6:

(a) All $\mathbb{Z}$-~~subg~~ submodules of $\mathbb{Z}$ are the modules $m\mathbb{Z}$, $m \in \mathbb{Z}^{\geq 0}$;

because

"For an abelian group (which is a $\mathbb{Z}$-module) a sub-module is the same as a sub-group."

and $m\mathbb{Z}$, $m \in \mathbb{Z}^{\geq 0}$, ~~passes~~ are ~~the~~ all subgroups of $(\mathbb{Z}, +)$.

(b) $M := \mathbb{Z}/6\mathbb{Z}$ is a $\mathbb{Z}$-module

It is the inner direct sum of

$$N_1 := \frac{2\mathbb{Z}}{6\mathbb{Z}} \text{ and } \frac{3\mathbb{Z}}{6\mathbb{Z}} =: N_2$$

$$\begin{array}{cc} \| & \| \\ \{[2]_6, [4]_6, [0]_6\} & \{[0]_6, [3]_6\} \end{array}$$

<u>Proof:</u> N_1 and N_2 are $\mathbb{Z}$-sub-modules of M, because subgroups of M.

Take $[n_1]_6 \in N_1$, $[n_2]_6 \in N_2$

s.t. $[n_1]_6 + [n_2]_6 = [0]_6$, i.e.

$[n_1+n_2]_6 = [0]_6 \Rightarrow 6 \mid n_1+n_2$.

~~W.l.o.g.~~ ~~$0 \leq n_1$~~

Thus: $3 \mid n_1$, because $3 \mid n_2$ and $3 \mid n_1+n_2$,

and thus $2 \mid n_2$, " $2 \mid n_1$ " $2 \mid n_1+n_2$.

Thus 2 and 3 divide n_1 and n_2.

2 and 3 are coprime to each other
(or look at prime factorization of n_1 and n_2
(if non-zero)).

$\Rightarrow 6 \mid n_1$ and $6 \mid n_2$

$\Rightarrow [n_1]_6 = [0]_6$ and $[n_2]_6 = [0]_6$.

$\square$

Similar for the $\mathbb{R}[X]$-module

$$\mathbb{R}[X]/(X^2-1) = (X-1)\,\mathbb{R}[X]/(X^2-1) \oplus (X+1)\,\mathbb{R}[X]/(X^2-1)$$

(try it as an exercise.)

<u>Remark 7:</u> Def 4 and Def 5 generalize naturally to left- and right modules over non-commutative rings (including to have $1_R \neq 0_R$). This is true for almost all definitions that follow.

<u>Def 8:</u> Let M be an R-module. We call an R-submodule N a direct summand of M if $\exists\, U \leq_R M$: $N \oplus U = M$.

<u>Examples 9:</u>

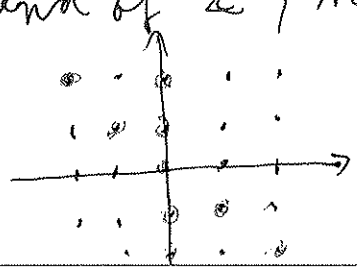
(a) V a vector space over a field k, then every k-submodule W of V is a direct summand.

(<u>Pf</u>: (from LA) $(w_i)_{i \in I}$ a basis of W, extend to a basis of V: $(v_j)_{j \in J}$, $I \subseteq J$ and $v_i = w_i$ for $i \in I$.

Then $U := \bigoplus_{j \in J \setminus I} k v_j$ ~~satisfied~~ satisfies $V = W \oplus U$.)

<u>End of lecture 2 16.09.21</u>

(b) (b-1) $N = \{(z_1, z_2) \in \mathbb{Z}^2 \mid z_1 + z_2 = 0\}$ is a direct summand of $\mathbb{Z}^2$, take $U = \{0\} \times \mathbb{Z}$.



<u>Proof:</u> • $N + U = \mathbb{Z}^2$, because

$$(z_1, z_2) = (z_1, -z_1) + (0, z_2 - z_1)$$

• $N \cap U = \{(0,0)\}$. $\square$

(b-2) $N' = \{(2z_1, 2z_2) \in \mathbb{Z}^2 \mid z_1, z_2 \in \mathbb{Z}\}$

is not a direct summand in $\mathbb{Z}^2$.

<u>Proof:</u> Assume $\exists\, U' \leq_{\mathbb{Z}} \mathbb{Z}^2 : N' \oplus U' = \mathbb{Z}^2$.

$N' \neq \mathbb{Z}^2 \Rightarrow U' \neq \{0\} \Rightarrow \exists\, (z_1, z_2) \in U' \setminus \{(0,0)\}$.

$\Rightarrow (2z_1, 2z_2) \in U' \cap N' \underset{\oplus}{=} \{(0,0)\}$ $\square$

$\Rightarrow z_1 = z_2 = 0$ ↯

So we need to generalize direct summands: exact sequences.

<u>Def 10:</u> ~~A form~~ (morphism / ~~[illegible]~~)

<u>Morphisms:</u> (1) A map $f: M_1 \longrightarrow M_2$ between R-modules is called an <u>R-module homomorphism</u> if

- f is a group homomorphism $(M_1, +) \to (M_2, +)$ such that
- f is R-~~lin~~ homogenous:

$$\forall r \in R\ \forall m_1 \in M_1 : f(r m_1) = r f(m_1).$$

We say f is <u>R-linear</u> or <u>R-homomorphism</u>.

(ii) An R- homomorphism $f: M_1 \longrightarrow M_2$ is called

(ii)(a) <u>epimorphism</u>, if f is surjective "$\twoheadrightarrow$"

(b) <u>monomorphism</u>, if f is injective "$\hookrightarrow$"

(c) <u>isomorphism</u>, if f is bijective. "$\simeq$"

~~Examples 11:~~

<u>Notation 11:</u> $\mathrm{Hom}_R(M_1, M_2)$, $\mathrm{Epi}_R(M_1, M_2)$, $\mathrm{Mono}_R(M_1, M_2)$, $\mathrm{Iso}_R(M_1, M_2)$.

<u>Examples 12:</u>

(a) There are only 4 $R = \mathbb{Z}/6\mathbb{Z}$ - modules generated by one element. (up to isomorphism.)

<u>Proof:</u> $\{0\}$, $\mathbb{Z}/2\mathbb{Z} \simeq 3\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \simeq 2\mathbb{Z}/6\mathbb{Z}$

and R are R- modules.

Let $M = \langle m_0 \rangle_R$ be an R- module just generated by $m_0 \in M$. $(M = \langle m \rangle_R = Rm)$

$\varphi: R \longrightarrow M$ $\quad \varphi(r) := r m_0$ is an

R- epimorphism.

$$\Longrightarrow \quad R/\mathrm{ker}(\varphi) \overset{\bar{\varphi}}{\simeq} M. \qquad \bar{\varphi}([r]) = \varphi(r) = r m_0.$$

$\ker(\varphi) \leq_R R$ (an ideal of R)

The only ideals of R are $\{[0]_6\}$, $2\mathbb{Z}/6\mathbb{Z}$, $3\mathbb{Z}/6\mathbb{Z}$, R.

Then we get $R/\ker(\varphi)$:

$\frac{\mathbb{Z}/6\mathbb{Z}}{6\mathbb{Z}/6\mathbb{Z}}$ is $\mathbb{Z}/6\mathbb{Z}$ is R	$\frac{\mathbb{Z}/6\mathbb{Z}}{2\mathbb{Z}/6\mathbb{Z}}$ is $\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/3\mathbb{Z}$	R/R is $\{[0]_6\}$.

$\square$

<u>Claim:</u> (a1) $\mathrm{Hom}_R(2\mathbb{Z}/6\mathbb{Z}, 2\mathbb{Z}/6\mathbb{Z}) \simeq 2\mathbb{Z}/6\mathbb{Z}$.

(a2) $\mathrm{Hom}_R(2\mathbb{Z}/6\mathbb{Z}, 3\mathbb{Z}/6\mathbb{Z}) = \{0\}$

zero map (everything send to $[0]_6$)

<u>Proof:</u> (a1)

$$\varphi \xmapsto{F} \varphi([2]_6)$$

$$\psi_k \xleftarrow{G} [2k]_6$$

$$\psi_k([2\ell]_6) := [2k\ell]_6$$

<u>To show:</u>
- $\forall_k : \psi_k \in \mathrm{Hom}_R(2\mathbb{Z}/6\mathbb{Z}, 2\mathbb{Z}/6\mathbb{Z})$ ✓
- $G \circ F(\varphi) = \varphi$ ✓
- $F \circ G([2k]_6) = [2k]_6$ ✓ $\square$ (a1)

(a2) $\varphi \in \mathrm{Hom}_{\mathbb{Z}}(2\mathbb{Z}/6\mathbb{Z}, 3\mathbb{Z}/6\mathbb{Z})$.

Then $[2]_6\, \varphi([2]_6) \underset{\uparrow}{=} \varphi([4]_6)$

$\mathrm{im}\,\varphi \subseteq 3\mathbb{Z}/6\mathbb{Z} \longrightarrow \| \qquad$ $\mathbb{Z}$- homo.

$[0]_6$.

Thus $\varphi([2]_6) = \varphi([4]_6 + [4]_6)$

$= \varphi([4]_6) + \varphi([4]_6)$

$= [0]_6 + [0]_6 = [0]_6$. $\square$

(b) For vector spaces $V/_k$ we have that every k- subspace $W \leq_k V$ can be realized as a quotient of V:

<u>Pf:</u> Take $U \leq_k V$: $U \oplus W = V$.

Then $V/_U \simeq W$. $\square$

This is false for modules.

$\mathbb{Q}$ is a $\mathbb{Z}$ - module. and $\mathbb{Z} \leq_{\mathbb{Z}} \mathbb{Q}$.

But $\mathbb{Z}$ is not isomorph to a quotient of $\mathbb{Q}$.

<u>Pf:</u> Assume $\exists\, U \leq_{\mathbb{Z}} \mathbb{Q}$: $\mathbb{Q}/_U \xrightarrow[\sim]{\overline{\varphi}} \mathbb{Z}$.

Then $U \neq \{0\}$, because $\mathbb{Q} \not\subset \mathbb{Z}$ because $\mathbb{Q}$ is not generated by one element over $\mathbb{Z}$

(If $\mathbb{Q} = \langle \frac{a}{b} \rangle_{\mathbb{Z}}$, $a \in \mathbb{Z}$, $b \in \mathbb{Z}^{>0}$, $\gcd(a,b)=1$, then

for p a prime number $p \nmid b$ we have:

$\exists z \in \mathbb{Z}: \frac{za}{b} = \frac{1}{p} \Rightarrow b = zap \underset{\gcd(a,b)=1}{\Rightarrow} b \mid pz$

$\Rightarrow \exists t \in \mathbb{Z}: tb = pz$

$\Rightarrow atb = apz = bz \Rightarrow (1-at)b = 0 \Rightarrow 1 = at$

$\underset{a,t \in \mathbb{Z}}{\Rightarrow} |a| = |t| = 1$. W.l.o.g. $a = 1$

$\Rightarrow b = zp \Rightarrow p \mid b$ ↯.)

Take $u \in U \setminus \{0\}$ $u = \frac{c}{d}$ $c \in \mathbb{Z}, d \in \mathbb{Z}^{>0}$, $\gcd(c,d)=1$.

For $q \in \mathbb{Q}$ $\exists z \in \mathbb{Z} \setminus \{0\}: zq \in c\mathbb{Z} \subseteq U$.

$\Rightarrow \bar{\varphi}([zq]_U) = \bar{\varphi}([0]_U) = 0_{\mathbb{Z}}$

$\|$

$z\bar{\varphi}([q]_U) \underset{\mathbb{Z} \text{ has no zero-divisors (it is an integral domain)}}{\Rightarrow} \bar{\varphi}([q]_U) = 0$.

↯ $\ker \bar{\varphi} = \mathbb{Z} \neq \{0\}$ $\square$

(c) Another new phenomena:

For vector spaces we know:

"If $V/_K$ is finitely generated and $f \in \mathrm{Hom}_K(V,V)$. Then are equivalent

1° $f \in \mathrm{Iso}_K(V,V)$

2° $f \in \mathrm{Mono}_K(V,V)$

3° $f \in \mathrm{Epi}_K(V,V)$

For modules this goes wrong:

- $f \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z},\mathbb{Z})$ $f(z) := 2z$ is injective but not surjective.
- ~~$\mathrm{Hom}(\mathbb{Q},\mathbb{Q})$~~
- but we still have $3° \Rightarrow 2°$ for finitely generated R-modules.

<u>Notation 13:</u> $\mathrm{End}_R(M)$, $\mathrm{Epi}_R(M)$, $\mathrm{Mono}_R(M)$.

<u>Def 14:</u> Let M be an R-Module and I be an ideal of R.
We write $I \cdot M$ for the submodule generated by the set $\{r \cdot m \mid r \in I \text{ and } m \in M\}$,

i.e. $$I \cdot M \overset{\text{ex.}}{=} \left\{ \sum_{j=1}^{l} r_j m_j \;\middle|\; l \in \underset{\{1,2,3,\dots\}}{\underset{\shortparallel}{\mathbb{N}}} \text{ and } r_j \in R, m_j \in M \right\}$$

Theorem ~~Lemma~~ 15: Let M/R be finitely generated by n elements, $\varphi \in \mathrm{End}_R(M)$ and $I \leq_R R$ s.t. $\varphi(M) \subseteq I \cdot M$.

Then there exist a polynomial

$$P = X^n + b_{n-1} X^{n-1} + \dots + b_1 X + b_0 \in R[X]$$

such that

(i) $P(\varphi)(m) = 0 \quad \forall m \in M$ and

(ii) $b_j \in I^{n-j} = \underbrace{I \cdot \dots \cdot I}_{n-j} \quad \forall j = 0, \dots, n-1$.

<u>Proof</u>: We consider M as an $R[X]$-module via $Q(X) \cdot m := Q(\varphi)(m)$, $Q \in R[X]$ and $m \in M$.

$M = Rm_1 + \dots + Rm_n$ (generated by n-elements)

$\Rightarrow \exists B \in R^{n \times n}$:

$$\begin{pmatrix} \varphi(m_1) \\ \vdots \\ \varphi(m_n) \end{pmatrix} = B \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}$$

$$\Rightarrow \quad (X \cdot \underbrace{I_n}_{\begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}} - B) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \underbrace{\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}}_{0 \text{ in } M}$$

multiply with the cofactor matrix from the left:

$$\begin{pmatrix} \det(X \cdot I_n - B) & & \\ & \ddots & \\ & & \det(X I_n - B) \end{pmatrix} \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \mathrm{Adj}(X I_n - B) \cdot (X \cdot I_n - B) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

$$\det(X \cdot I_n - B) \cdot m = 0_M \quad \forall m \in M.$$

$\Longrightarrow$

$m_1, \dots, m_n$ generate M

Take $P(X) := \det(X \cdot I_n - B)$.

By $\varphi(M) \subseteq I \cdot M$ we could have taken $B \in I^{n \times n}$. $\square$

<u>Remark 16:</u> The statement is called Cayley - Hamilton's theorem and the trick using the cofactor matrix is called ~~the~~ Noether's determinant trick.

<u>Corollary 17</u> (Nakayama's lemma)

Let M be a f.g. R-module and $I \leq_R R$ such that $M = I \cdot M$.

Then there exists $r \in I$ s.t. for all $m \in M$:

$$(1 - r)\, m = 0.$$

<u>Proof:</u> Take $\varphi = id_M$ in Theorem 15. $\square$

<u>Corollary 18:</u> Let M be a finitely generated R-module. Then $\mathrm{Epi}_R(M) \subseteq \mathrm{Iso}_R(M)$.

<u>end of 3rd lecture 23.09.21</u> (Next lecture Sunday the 26th say a few words about 1.4.)

<u>Proof:</u> Consider M as an $R[X]$-module via $Q \cdot m := Q(\varphi)(m)$.

Then we have for $I := (X) \leq_{R[X]} R[X]$ the equality $I \cdot M = M$, because $XM = M$, because $\varphi(M) = M$.

Nakayama's Lemma

$\Longrightarrow \exists\, Q \in R[X] : (1 - XQ) . M = \{0_M\}$,

i.e. $(id_M - \varphi \circ Q(\varphi))(m) = 0_M \quad \forall m \in M$.

$$\Longrightarrow \quad m = id_M(m) = (\varphi \circ Q(\varphi))(m)$$
$$= (Q(\varphi) \circ \varphi)(m)$$

$\Longrightarrow$ $Q(\varphi)$ is an inverse of φ $\square$

<u>Def 19:</u> A family of maps of R-homomorphisms

$$\cdots \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} M_{i+2} \xrightarrow{f_{i+2}} M_{i+2} \xrightarrow{f_{i+3}} \cdots$$

is called

(a) a <u>sequence</u>

(b) a <u>chain complex</u>, if it is a sequence and $\forall_i$: $\operatorname{im} f_i \subseteq \ker f_{i+1}$

(i.e. $f_{i+1} \circ f_i = 0$-map)

(c) an exact sequence, if

$\forall_i$: $\operatorname{im} f_i = \ker f_{i+1}$.

<u>Def 20:</u> An exact sequence

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

of R-modules is called a short exact sequence.

<u>Examples 21:</u>

(a) $$0 \longrightarrow M_1 \xrightarrow{\alpha} M_1 \oplus M_2 \xrightarrow{\beta} M_2 \longrightarrow 0$$

$\alpha(m_1) := (m_1, 0)$, $\beta(m_1, m_2) := m_2$.

is exact.

at $M_1 \oplus M_2$: • $\beta \circ \alpha(m_1) = \beta((m_1, 0)) = 0$

• let $(m_1, m_2) \in \ker \beta \Rightarrow \beta((m_1, \underset{\substack{\shortparallel \\ m_2}}{m_2})) = 0$

$\Rightarrow m_2 = 0$.

$\Rightarrow (m_1, m_2) = (\underset{\substack{\shortparallel \\ \alpha(m_1)}}{m_1}, 0) \in \operatorname{im}(\alpha)$

at M_1 ✓

at M_2 ✓

(b) These are more kinds of exact sequences:

$$0 \longrightarrow \mathbb{Z} \xrightarrow[\alpha]{\cdot 2} \mathbb{Z} \xrightarrow{\beta} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

$\alpha(z) := 2z$, $\beta(z) := [z]_2$.

It is exact, but $2\mathbb{Z} = \operatorname{im}(\alpha)$ is not a direct summand of $\mathbb{Z}$.

(because every subgroup $U \leq_{\mathbb{Z}} \mathbb{Z}$ with $2\mathbb{Z} + U = \mathbb{Z}$ satisfies $U \cap 2\mathbb{Z} \neq \{0\}$.)

The analogue to direct summands for vector spaces are split exact sequences.

<u>Def 22:</u> A short exact sequence is called <u>split</u>

$$0 \to M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3 \to 0$$

if there exists an $s \in \mathrm{Hom}_R(M_3, M_2)$ such that $\beta \circ s = id_{M_3}$.

<u>Prop 23:</u> Let $0 \to M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3 \to 0$ be a short exact sequence of R-modules. Then are equivalent:

1° The sequence is split.

2° $\exists\, t \in \mathrm{Hom}_R(M_2, M_1) : \quad t \circ \alpha = id_{M_1}$

3° ~~$M_2 \cong \alpha(M_1) \oplus M_1 \oplus M_3$~~

$\alpha(M_1)$ is a direct summand of M_2.

<u>Proof:</u> We show that 1° is equivalent to 3° (2° $\Leftrightarrow$ 3° is an exercise.)

1° $\Rightarrow$ 3° $\quad M_2 = \alpha(M_1) \oplus \mathrm{im}(s)$

because $m_2 = \underbrace{s(\beta(m_2))}_{s(M_3)} + \underbrace{m_2 - s(\beta(m_2))}_{\in \alpha(M_1) = \ker(\beta)}$

and $\alpha(M_1) \cap s(M_3) = \{0\}$

because from $\alpha(m_1) = s(m_3)$
follows $m_3 = \beta(s(m_3)) = \beta(\alpha(m_1)) = 0_{M_3}$.

$3^\circ \Rightarrow 1^\circ$ $\quad \beta|_U$ for $\alpha(M_1) \oplus U = M_2$

is an isomorphism $U \xrightarrow{\sim} M_3$
(surj ✓, injective because $\ker(\beta) \cap U$
$= \alpha(M_1) \cap U = \{0\}$.)
Take $s = (\beta|_U)^{-1}$ $\square$

<u>Notation 24:</u> $N \overset{\oplus}{\underset{R}{|}} M$ "N is a direct summand of M".

<u>Remark 25:</u> $M_1 \oplus M_3 \simeq M_2$ is not enough to force the sequence to split.

<u>Ex:</u> $M_2 = \bigoplus_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Q}/\mathbb{Z}$

$M_1 = \frac{1}{2}\mathbb{Z}/\mathbb{Z}$, α inclusion, β quotient map

$$0 \to M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3 \to 0$$

M_1 is not a $\oplus$ summand and
$M_1 \oplus M_3 \simeq M_2$
$(M_1 \simeq \mathbb{Z}/2\mathbb{Z},\ M_3 \simeq M_2)$.

<u>Proof</u>: $M_3 := M_2 / M_1 \simeq \left(\bigoplus_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}\right) \oplus \left(\mathbb{Q}/\mathbb{Z} \Big/ \left(\tfrac{1}{2}\mathbb{Z}/\mathbb{Z}\right)\right)$

$$\simeq \left(\bigoplus_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}\right) \oplus \underbrace{\left(\mathbb{Q}/\tfrac{1}{2}\mathbb{Z}\right)}_{\substack{\simeq\, \mathbb{Q}/\mathbb{Z} \\ [q]_{\frac{1}{2}\mathbb{Z}} \mapsto [2q]_{\mathbb{Z}}}} \simeq M_2$$

(as $\mathbb{Z}$-modules)

and $M_1 \oplus M_3 \simeq \tfrac{1}{2}\mathbb{Z}/\mathbb{Z} \oplus M_2$

$$\simeq \mathbb{Z}/2\mathbb{Z} \oplus M_2 \simeq M_2$$

But M_1 is not a $\oplus$-summand of M_2, because, since $M_1 \subseteq \tfrac{1}{2}\mathbb{Z}/\mathbb{Z} \subseteq \mathbb{Q}/\mathbb{Z}$ we have by the following exercise that

$$M_1 \mid^{\oplus} M_2 \iff M_1 \mid^{\oplus} \tfrac{1}{4}\mathbb{Z}/\mathbb{Z}$$

But $M_1 \mid^{\oplus} \tfrac{1}{4}\mathbb{Z}/\mathbb{Z}$ is not possible, because

$$\mathbb{Z}/4\mathbb{Z} \simeq \tfrac{1}{4}\mathbb{Z}/\mathbb{Z} \not\simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \simeq \left(\tfrac{1}{4}\mathbb{Z}/\mathbb{Z}\right)/M_1 \oplus M_1,$$

because $\exists$ an element of order 4 in $\mathbb{Z}/4\mathbb{Z}$. $\square$

<u>Exercise 26:</u> Let M be an R-module, $U \leq_R N \leq_R M$ and $U \mid_R^{\oplus} M$. Then $U \mid_R^{\oplus} N$.

<u>Proof:</u> <u>Hint:</u> $U \oplus V = M \overset{\text{Show}}{\Longrightarrow} U \oplus (V \cap N) = N$. $\square$

I.2. ~~Noeth~~ Noetherian modules

<u>Def 27:</u> Let M be an R-module. M is called <u>noetherian</u> if every R-submodule of M is finitely generated. (in particular M is f.g.)

<u>Prop. 28:</u> Let M be an R-module. Then are equivalent

1° M is ~~noetherian~~ noetherian.

2° Every chain of submodules of M

$$N_1 \subseteq N_2 \subseteq N_3 \subseteq \dots$$

is stabilizing eventually, i.e.

$$\exists_{k \in \mathbb{N}} \forall_{l \in \mathbb{N}} : N_k = N_{k+l}$$

3° Every non-$\emptyset$ set of R-submodules has a maximal element w.r.t. "$\subseteq$".

<u>Remark 29:</u> Def 27 and Prop. 28 also work over non-commutative rings.

<u>Proof of Prop 28:</u> (known from Abstract Algebra)

$1^\circ \Rightarrow 2^\circ$ Take $N_1 \leq_R N_2 \leq_R N_3 \leq_R \cdots$

$N := \bigcup_{i=1}^{\infty} N_i$ is an R-submodule of M.

($n, m \in N$, say $n, m \in N_{i_0}$
$\Rightarrow n + m \in N_{i_0} \subseteq N$.
$r \in R$ and $n \in N$, say $n \in N_{i_0}$,
$\Rightarrow rn \in N_{i_0} \subseteq N$)

So N is f.g., say by $x_1, \ldots, x_\ell$.

$\Rightarrow \exists\, i_0 \in \mathbb{N}: \quad x_1, \ldots, x_\ell \in N_{i_0}$

$\Rightarrow \quad N \subseteq N_{i_0} \quad \Rightarrow \forall_{j \geq i_0}: N_j \subseteq N \subseteq N_{i_0} \subseteq N_j$

$2^\circ \Rightarrow 3^\circ$ Let S be a non-empty set of R-submodules of M.

Assume that S has no "$\subseteq$"-maximal element, i.e. $\forall N \in S \; \exists N' \in S : N \subsetneq_R N'$

Take $N_1 \in S$, then $N_1 \subsetneq N_2 \in S$

$\cdots \quad N_1 \subsetneq N_2 \subsetneq N_3 \subsetneq$ $\lightning$ to 2°.

$3^\circ \Rightarrow 1^\circ$ Assume $\exists N \leq_R M$ s.t. N is not f.g. Take $n_1 \in N$.

then $n_2 \in N \setminus Rn_1$

$n_3 \in N \setminus (Rn_1 + Rn_2)$

$\vdots$

$\Rightarrow \quad Rn_1 \subsetneq Rn_2 + Rn_1 \subsetneq Rn_1 + Rn_2 + Rn_3 \subsetneq \cdots$

So $S = \{ Rn_1 + \cdots + Rn_k \mid k \in \mathbb{N} \}$

has no "$\subseteq$"-maximal element $\lightning$ to 3° $\square$

end of lecture 4 26.09.21.

<u>Prop 30:</u> Let $0 \to M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3 \to 0$ be exact. Then are equivalent

1° M_2 is ~~noetherian~~ noetherian

2° M_1 and M_3 are ~~noetherian~~ noetherian.

<u>Proof:</u> $1^\circ \Rightarrow 2^\circ$ $M_1 \leq_R M_2$, so every R-submodule of M_1 is an R-submodule of M_2, so f.g. because M_2 is noetherian.

So M_1 is noetherian.

Take $N \leq_R M_3 \Rightarrow \beta^{-1}(N) \leq_R M$

$$\beta^{-1}(N) = \{ m_2 \in M_2 \mid \beta(m_2) \in N \}$$

So $\beta^{-1}(N) = Rx_1 + Rx_2 + \dots + Rx_k$

for some $x_1, \dots, x_k \in \beta^{-1}(N)$, because 1°

$$\Rightarrow \quad N \underset{\substack{\uparrow \\ \beta \text{ surjective}}}{=} \beta(\beta^{-1}(N)) = R\beta(x_1) + R\beta(x_2) + \dots + R\beta(x_k)$$

is f.g.

So M_3 is noetherian.

$2^\circ \Rightarrow 1^\circ$ Show this in an exercise.

<u>hint:</u> $N \leq_R M_2 \Rightarrow \beta(N) \leq_R M_3$
and $N \cap \alpha(M_1) \leq_R \alpha(M_1) \simeq M_1$

so $\beta(N)$ and $N \cap \alpha(M_1)$ are f.g.

Now find finitely many generators for N. $\square$

<u>Corollary 31:</u> Let G be a f.g. abelian group and $\underbrace{H \leq_{\mathbb{Z}} G}_{\text{(remember: means subgroup)}}$. Then H is f.g..

<u>Proof:</u> Take $\langle g_1, \dots, g_\ell \rangle = G$.

$$\langle g_1, \dots, g_\ell \rangle = \mathbb{Z} g_1 + \dots + \mathbb{Z} g_\ell$$

Then

$$0 \longrightarrow \ker \varphi \longrightarrow \underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_{\ell} \xrightarrow{\varphi} G \to 0$$

with

$$\varphi(z_1, \dots, z_\ell) := \sum_{i=1}^{\ell} z_i g_i$$

is exact as a sequence of $\mathbb{Z}$-modules.

We show that $\underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_{\ell}$ is a noetherian $\mathbb{Z}$-module (Then G is noetherian

and it is finitely generated.)

- $\mathbb{Z}$ is noetherian, because the sub-modules are $m\mathbb{Z}$, $m \geq 0$. They are all generated by one element.

- $$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z} & \longrightarrow & \mathbb{Z} \oplus \mathbb{Z} & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \\ & & z & \longmapsto & (z,0) & \longmapsto & & & \\ & & & & (z_1, z_2) & & z_2 & & \end{array}$$ is exact.

Thus by Prop 30: $\mathbb{Z} \oplus \mathbb{Z}$ is ~~not~~ noetherian.

- $$0 \longrightarrow \mathbb{Z} \longrightarrow \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{k+1} \longrightarrow \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{k} \to 0$$

exact.

$\Longrightarrow$ $\mathbb{Z}^{\oplus k+1}$ is noetherian if $\mathbb{Z}^{\oplus k}$ is.

By induction we get $\mathbb{Z}^{\oplus l}$ is noetherian. $\square$

Before giving examples let us state what the proof in fact gives:

<u>Def 32:</u> Recall that a ring R is called noetherian if it is noetherian as an R-module.

(non-commutative world: notion of left and right noetherian.)

<u>Prop. 33:</u> Let M be a f.g. R-module. Suppose R is noetherian. Then M is noetherian as an R-module.

<u>Proof:</u> Same as the one of Cor. 31. Replace $\mathbb{Z}$ by R $\square$

Recall:

<u>Theorem 34:</u> (Hilbert's basis theorem) (AA)
Let R be a noetherian ring. Then $R[X]$ is noetherian.

<u>Examples 35:</u>

1) A field k, e.g. $\mathbb{R}$, is a noetherian ring: because it has only two ideals, so (Apply Prop 28.3°) every non-$\emptyset$ set of ideals of k has a maximal element w.r.t. "$\subseteq$".

2) $\mathbb{R}[X]$ is a noetherian ring by Hilbert's basis theorem.
But $\mathbb{R}[X]$ is <u>not</u> a noetherian $\mathbb{R}$-module:

$$\mathbb{R}\cdot 1 \subsetneq \mathbb{R} + \mathbb{R}X \subsetneq \mathbb{R} + \mathbb{R}X + \mathbb{R}X^2 \subsetneq \dots$$

(see Prop 28.2°)

3) Modules and rings are closely related.
Let M be an R-module. Then we obtain the following ring:

$$R_M := R \oplus M \text{ with the multiplication}$$

$$(r_1, m_1)(r_2, m_2) := (r_1 r_2, r_1 m_2 + r_2 m_1).$$

(associativity: $((r_1, m_1)(r_2, m_2))(r_3, m_3)$
$= (r_1 r_2, r_1 m_2 + r_2 m_1)(r_3, m_3)$
$= (r_1 r_2 r_3, r_3 r_1 m_2 + r_3 r_2 m_1 + r_1 r_2 m_3)$
$= (r_1, m_1)((r_2, m_2)(r_3, m_3))$)

Every R-module N is an R_M-module:

$$(r, m) \cdot n := rn.$$

and we have
(a) N is f.g. as an R-module $\Leftrightarrow$ N is f.g. as an R_M-module
(b) N is R-noetherian $\Leftrightarrow$ N is R_M-noetherian.

We get the following proposition.

<u>Prop. 36:</u> Let M be an R-module. T.a.e.:
1° M and R are noetherian R-modules
2° R_M is a noetherian ring.

<u>Proof:</u> $1^\circ \Leftrightarrow 2^\circ$ will follow from Prop. 30 after some preparation.

$$(*)\quad 0 \longrightarrow M \xrightarrow{\alpha} \underset{\substack{\| \\ R \oplus M}}{R_M} \xrightarrow{\beta} R \longrightarrow 0 \qquad \begin{array}{l}\alpha(m) := (0,m)\\ \beta(r,m) := r\end{array}$$

is an exact sequence of $\mathbb{Z}$-modules.
But in fact α and β are R_M-module homomorphisms.

$$\alpha((r',m').m) = \alpha(r'm) = (0, r'm) = (r',m')(0,m)$$
$$= (r',m')\alpha(m)$$
$$\beta((r',m')(r,m)) = r'r = (r',m').r = (r',m')\beta(r,m).$$

Thus $(*)$ is an ex. seq of R_M-modules.

By Prop 30 we have

R_M is R_M-noetherian

$\Leftrightarrow$ M and R are R_M-noetherian.

$\overset{\text{Ex 35.3 (b)}}{\Longleftrightarrow}$ M and R are R-noetherian. $\square$

<u>Example 37:</u> $\mathbb{R}^{1\times 2}$ is an $\mathbb{R}$-module (component-wise)

Then $\mathbb{R}_{\mathbb{R}^{1\times 2}} \xrightarrow[\sim]{\varphi} \mathbb{R}[X,Y] / (X^2, XY, Y^2)$

$$(r_1,(r_2,r_3)) \longmapsto [r_1 + r_2 X + r_3 Y]_{(X^2, XY, Y^2)}$$

(check)

Noetherian modules can be decomposed into a direct sum of indecomposable modules.

<u>Def 38:</u> Let R be a ring and M be an R-module.

(a) M is called indecomposable if M is not the inner direct sum of two non-zero submodules.

(b) R is called an indecomposable ring if R is not ~~the~~ isomorphic to a product of two rings. (they are automatically non-zero by our convention)

<u>Example 39:</u>

(a) Let p be a prime number. Then $\mathbb{Z}/p^2\mathbb{Z}$ is indecomposable as a $\mathbb{Z}$-module (i.e. as an abelian group), because the only subgroups are $\{[0]_{p^2}\}$, $p\mathbb{Z}/p^2\mathbb{Z}$ and $\mathbb{Z}/p^2\mathbb{Z}$, and therefore $p\mathbb{Z}/p^2\mathbb{Z}$ is not a direct summand.

(b) Show that $\mathbb{Q}/\mathbb{Z}$ is indecomposable as a $\mathbb{Z}$-module and as a ring.
(The second follows directly from the first.)

(c) $\mathbb{Z}/42\mathbb{Z}$ is decomposable, because

$$\mathbb{Z}/42\mathbb{Z} = 6\mathbb{Z}/42\mathbb{Z} \oplus 7\mathbb{Z}/42\mathbb{Z} \quad \text{(by Bézout)}$$
$$= 6\mathbb{Z}/42\mathbb{Z} \oplus 14\mathbb{Z}/42\mathbb{Z} \oplus 21\mathbb{Z}/42\mathbb{Z}.$$

<u>Prop 40:</u> Let M be a noetherian R-module. Then $\exists\, \exists_{\ell \in \mathbb{N}}\, M_1, \dots, M_\ell$ all $\leq_R M$ and indecomposable and non-zero:

$$M = M_1 \oplus M_2 \oplus \dots \oplus M_\ell.$$

<u>Proof:</u> Assume that the assertion does <u>not</u> hold.

$\Rightarrow \exists\, M_1', N_1' \leq_R M$: $M_1' \oplus N_1' = M$ s.t. M_1' is not a direct sum of indecomp. modules.

$\Rightarrow \exists\, M_2' \leq_R M_1'$, $N_2' \leq_R M_1'$:
$M_1' = M_2' \oplus N_2'$ and M_2' is <u>not</u> ...

We proceed to get a sequence of modules.

$M_1' \gneqq M_2' \gneqq M_3' \gneqq \dots$ and

$N_1' \lneqq N_1' + N_2' \lneqq N_1' + N_2' + N_3' \lneqq \dots$

The ~~seq~~ second sequence does not stabilize eventually, so $\lightning$ $\square$

We have a similar statement for rings.

<u>Theorem 41:</u> Let R be a noetherian ring.

Then $\exists_{\ell \in \mathbb{N}}$ $\exists$ indecomposable rings $R_1, \dots, R_\ell$:

$R \simeq R_1 \times \dots \times R_\ell$ as rings.

For this we need some preparation.

<u>Def 42:</u> (a) Let $(M, *)$ be a magma.
$x \in M$ is called <u>idempotent</u> if $x * x = x$.

(b) Let A be a possible non-commutative ring. An idempotent $x \in A$ is called <u>primitive</u> if $x \neq 0$ and $\nexists$ y, z non-zero idempotents s.t.

$x = y + z$ and $\underbrace{yz = zy = 0}$, "pairwise orthogonal"

end of lect. 5.

~~Remark: In the commutative setting $(xy)z$ is automatically fulfilled.~~

~~$x = y + z \Rightarrow x^2 = (y+z)^2 = y^2 + yz + zy + z^2 = y^2 + z^2$~~

<u>Lemma 43:</u> There is a canonical bijection between the following two sets:

$$S_1 := \{ T \subseteq R \mid T \text{ consists of finitely many pairwise orthogonal non-zero idempotents such that } \sum_{t \in T} t = 1 \}$$

and

$$S_2 := \left\{ \{R_1, \dots, R_\ell\} \;\middle|\; \ell \in \mathbb{N},\ R_i \subseteq R \text{ is a subring},\ i = 1, \dots, \ell \text{ such that } \begin{array}{l} R_1 \times \dots \times R_\ell \longrightarrow R \\ (x_1, \dots, x_\ell) \longmapsto x_1 + \dots + x_\ell \end{array} \text{ is a ring isomorphism} \right\}$$

<u>Proof:</u>

$$S_1 \underset{G}{\overset{\mathcal{F}}{\rightleftarrows}} S_2$$

$$\mathcal{F}(T) := \{ Rt \mid t \in T \}$$

$$G(\{R_1, \dots, R_\ell\}) := \{1_{R_1}, \dots, 1_{R_\ell}\}$$

<u>Step 1:</u> To show $\mathcal{F}$ is well-defined.

$T \in S_1$. $T = \{t_1, \dots, t_\ell\}$

Put $R_i := Rt_i$. $\Rightarrow \forall_{i \neq j}\ R_i R_j \subseteq t_i t_j R = \{0\}$.

R_i is a subring of R, i.e.

$(R_i, +, \cdot)$ is a ring. (including comm., unitary, non-zero)

<u>Note:</u> R_i has unit element t_i.

The map $R_1 \times \cdots \times R_\ell \xrightarrow{\varphi} R$

$$(x_1, \ldots, x_\ell) \longmapsto \sum_{i=1}^{\ell} x_i$$

is surjective, because $x = \varphi(xt_1, \ldots, xt_\ell)$ $\forall x \in R$, and injective because from $\sum_{i=1}^{\ell} x_i = 0$ follows for $j \in \{1, \ldots, \ell\}$:

$$x_j = t_j \sum_{i=1}^{\ell} x_i = 0.$$

φ is a ring homomorphism (exercise).

<u>Step 2:</u> G is well-defined (exercise)

<u>Step 3:</u> $((G \circ F)(T) = \{1_{R_t} \mid t \in T\} = \{t \mid t \in T\}$

<u>Step 4:</u> $(F' \circ G_1)(\{R_1, \ldots, R_\ell\}) = \{R 1_{R_1}, \ldots, R 1_{R_\ell}\}$

$= \{R_1, \dots, R_\ell\}$, because

$$R \cdot 1_{R_1} = (R_1 + R_2 + \dots + R_\ell) \cdot 1_{R_1}$$
$$= R_1 \cdot 1_{R_1} + \underbrace{R_2 1_{R_1} + \dots + R_\ell 1_{R_1}}_{\{0_R\}}$$
$$= R_1 \qquad \square$$

<u>Proof of Theorem 41:</u> The proof is analogous to the proof of Prop. 40.

<u>Hint:</u> Assume that R is not $\simeq$ to a finite product of indecomposable rings.

Then find a idempotents

$1 = e_1 + f_1 \qquad e_1 f_1 = 0 \qquad e_1 \neq 0 \neq f_1$

$e_1 = e_2 + f_2 \qquad e_2 f_2 = 0 \qquad e_2 \neq 0 \neq f_2$

$\vdots \qquad\qquad \vdots$

$e_i = e_{i+1} + f_{i+1}$

Then $(f_1) \subsetneq (f_1 + f_2) \subsetneq (f_1 + f_2 + f_3) \subsetneq \dots$

$\Rightarrow$ ξ because R is noetherian. $\square$

Another property of noetherian rings is the existence of finite prime decompositions of radical ideals.

<u>Def 44:</u> Let $\mathfrak{a}$ be an ideal of R.

$$\sqrt{\mathfrak{a}} := \{ a \in R \mid \exists n \in \mathbb{N} : a^n \in \mathfrak{a} \}$$

"the radical of $\mathfrak{a}$". $\mathfrak{a}$ is called <u>radical</u> if $\mathfrak{a} = \sqrt{\mathfrak{a}}$

<u>Prop. 45:</u> $\mathfrak{a}, \mathfrak{b} \leq_R R$. Then

(1) $\sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}} = \sqrt{\mathfrak{a}\mathfrak{b}} = \sqrt{\mathfrak{a} \cap \mathfrak{b}}$

(2) $\sqrt{\sqrt{\mathfrak{a}}} = \sqrt{\mathfrak{a}}$

(3) $\sqrt{\mathfrak{a} + \mathfrak{b}} = \sqrt{\sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}}$

(4) A prime ideal is radical

(5) A maximal ideal is radical

(6) If $\{\mathfrak{a}_i \mid i \in I\}$ is a non-empty set of radical ideals of R and suppose it is totally ordered. Then $\mathfrak{a} := \bigcup_{i \in I} \mathfrak{a}_i$ is a radical ideal.

Proof (2) $a \in \sqrt{\sqrt{\mathfrak{a}}} \Rightarrow \exists_{n \in \mathbb{N}}: a^n \in \sqrt{\mathfrak{a}}$

$\Rightarrow \exists m \in \mathbb{N}: \underbrace{(a^n)^m}_{= a^{nm}} \in \mathfrak{a} \Rightarrow a \in \sqrt{\mathfrak{a}}$

And $\sqrt{\mathfrak{a}} \subseteq \sqrt{\sqrt{\mathfrak{a}}}$.

So $\sqrt{\mathfrak{a}} = \sqrt{\sqrt{\mathfrak{a}}}$.

(1) exercise.

(3) • $\mathfrak{a} + \mathfrak{b} \subseteq \sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}$

$\Rightarrow \sqrt{\mathfrak{a}+\mathfrak{b}} \subseteq \sqrt{\sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}}$

• $\mathfrak{a} \subseteq \mathfrak{a} + \mathfrak{b}$

$\Rightarrow \sqrt{\mathfrak{a}} \subseteq \sqrt{\mathfrak{a}+\mathfrak{b}}$

and similarly $\sqrt{\mathfrak{b}} \subseteq \sqrt{\mathfrak{a}+\mathfrak{b}}$

$\Rightarrow \sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}} \subseteq \sqrt{\mathfrak{a}+\mathfrak{b}}$

$\Rightarrow \sqrt{\sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}} \subseteq \sqrt{\mathfrak{a}+\mathfrak{b}}$

(4) $a \in \sqrt{\mathfrak{p}} \Rightarrow \exists_{n \in \mathbb{N}}: a^n \in \mathfrak{p}$ (take n smallest)

$\underset{\mathfrak{p} \text{ is prime}}{\Rightarrow} a^{n-1} \in \mathfrak{p}$ or $a \in \mathfrak{p}$

$\underset{n \text{ smallest}}{\Rightarrow} a \in \mathfrak{p}$. So $\sqrt{\mathfrak{p}} \subseteq \mathfrak{p} \subseteq \sqrt{\mathfrak{p}}$.

(5) maximal ideals are prime, so
— " — are radical.

(6) exercise. $\square$

<u>Example 46:</u>

(a) $m\mathbb{Z} \subseteq \mathbb{Z}$ $\quad m = p_1^{\nu_1} \cdots p_\ell^{\nu_\ell} \in \mathbb{N}^{\geq 2}$ $\quad p_1, \dots, p_\ell$ pairwise different primes

$$\sqrt{m\mathbb{Z}} = p_1 \cdots p_\ell \mathbb{Z}$$

(We also call $p_1 \cdots p_\ell$ the radical of m.)

<u>Proof:</u> <u>"$\subseteq$"</u>: $m \in p_1 \cdots p_\ell \mathbb{Z} \Rightarrow m\mathbb{Z} \subseteq p_1 \cdots p_\ell \mathbb{Z}$
$$\| $$
$$p_1\mathbb{Z} \cap \dots \cap p_\ell \mathbb{Z}$$

The last equation, because $p_1, \dots, p_\ell$ are pairwise different.

$p_i \mathbb{Z}$ is prime so radical. (Prop 45 (4))
Thus $p_1\mathbb{Z} \cap \dots \cap p_\ell \mathbb{Z}$ is radical by Prop 45 (1). So $\sqrt{m\mathbb{Z}} \subseteq p_1\mathbb{Z} \cap \dots \cap p_\ell \mathbb{Z} = p_1 \cdots p_\ell \mathbb{Z}$.

$\Rightarrow$ We have "$\subseteq$".

<u>"$\supseteq$":</u> $(p_1 \cdot \ldots \cdot p_\ell)^{\max\{\nu_1, \dots, \nu_\ell\}} \in m\mathbb{Z}$

$\Rightarrow$ $p_1 \cdots p_\ell \in \sqrt{m\mathbb{Z}}$

$\Rightarrow$ $p_1 \cdots p_\ell \mathbb{Z} \subseteq \sqrt{m\mathbb{Z}}$. $\square$

(b) $\cancel{\mathbb{R}[X] \supseteq (X}$

$R := \mathbb{R}[X,Y]$. $\supseteq \mathfrak{a} = (X^2, Y)_{\mathbb{R}[X,Y]}$

$= RX^2 + RY$.

$$\sqrt{\mathfrak{a}} = \sqrt{RX^2+RY} \overset{\text{Prop. 45 (3)}}{=} \sqrt{\sqrt{RX^2}+\sqrt{RY}}$$

$$= \sqrt{RX+RY}$$

$$= RX+RY = (X,Y)_{\mathbb{R}[X,Y]},$$

because $RX+RY$ is prime, because

$$\mathbb{R}[X,Y]/RX+RY \xrightarrow{\sim} \mathbb{R} \quad \text{as rings}$$

$$[P] \longmapsto P(0,0)$$

and $\mathbb{R}$ is an integral domain.

(c) We have a special radical ideal
The "nil-radical" of R.

$$\mathrm{nil}(R) := \{ r \in R \mid \exists_{n \in \mathbb{N}} r^n = 0_R \} = \sqrt{(0)_R}.$$

<u>Def 47:</u> A ring R is called reduced if $\mathrm{nil}(R) = \{0\}$

<u>Example 48:</u> (a) $\mathbb{Z}$ is reduced because $\mathbb{Z}$ has no zerodivisors

(b) Let $R_1, \dots, R_\ell$ be integral domains

Then $R_1 \times R_2 \times \dots \times R_\ell$ is reduced,
because $\mathrm{nil}(R_1 \times \dots \times R_\ell)$
$= \mathrm{nil}(R_1) \times \mathrm{nil}(R_2) \times \dots \times \mathrm{nil}(R_\ell)$.

(c) $\mathrm{nil}\left(\mathbb{Q}[X]/(X^2)\right) = (X)/(X^2)$

(d) $\mathrm{nil}\left(\mathbb{Z}/p_1^{\nu_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_\ell^{\nu_\ell}\mathbb{Z}\right)$
$= p_1\mathbb{Z}/p_1^{\nu_1}\mathbb{Z} \times \dots \times p_\ell\mathbb{Z}/p_\ell^{\nu_\ell}\mathbb{Z}$.

(e) Let M be an R-module. Consider R_M.
$\mathrm{nil}(R_M) = \mathrm{nil}(R) \oplus M$.

<u>Proof</u>: "$\supseteq$" $(r,m) \in \mathrm{nil}(R) \oplus M \Rightarrow \exists\, n \in \mathbb{N}: r^n = 0$
$\Rightarrow (r,m)^{n+1} = (r^{n+1}, (n+1) r^n m) = (0_R, 0_M)$
$\Rightarrow (r,m) \in \mathrm{nil}(R_M)$

"$\subseteq$" $(r,m) \in \mathrm{nil}(R_M) \Rightarrow \exists\, n \in \mathbb{N}: (r,m)^n = (0_R, 0_M)$
$\Rightarrow (r^n, n r^{n-1} m) = (0_R, 0_M)$
$\Rightarrow r \in \mathrm{nil}(R)$ $\square$

<u>Theorem 49:</u> (Noether) Let R be a noetherian ring and $\mathfrak{a} \leq_R R$. We denote
$$V(\mathfrak{a}) := \{\mathfrak{p} \leq_R R \mid \mathfrak{p} \text{ prime ideal } \mathfrak{p} \supseteq \mathfrak{a}\}$$
and
$$V_{\min}(\mathfrak{a}) := \{\mathfrak{q} \in V(\mathfrak{a}) \mid \mathfrak{q} \text{ is minimal w.r.t. "}\subseteq\text{" in } V(\mathfrak{a})\}$$

($V_{min}(\mathfrak{a})$ is called the set of minimal primes of $\mathfrak{a}$)

Then (a) $\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{p} \in V_{min}(\mathfrak{a})} \mathfrak{p}$

(b) Let $\{\mathfrak{p}_i \mid i \in I\} \subseteq V(\mathfrak{a})$ be a finite set of prime ideals which satisfies

(b1) $\sqrt{\mathfrak{a}} = \bigcap_{i \in I} \mathfrak{p}_i$ and

(b2) $\forall i_0 \in I: \mathfrak{p}_{i_0} \not\supseteq \bigcap_{i \in I \setminus \{i_0\}} \mathfrak{p}_i$.

$\left(\text{i.e. } \bigcap_{i \in I \setminus \{i_0\}} \mathfrak{p}_i \supsetneq \sqrt{\mathfrak{a}} \right)$

Then $\{\mathfrak{p}_i \mid i \in I\} = V_{min}(\mathfrak{a})$.

end of lecture 6, 30.9.21 (Go also to Example 50)

<u>Proof:</u> We prove (a) and (b) on the way.

The steps look different.

<u>Step 1:</u> $\sqrt{\mathfrak{a}}$ is the intersection of finitely many prime ideals.

<u>Pf:</u> Assume not.

$S := \{\mathfrak{b} \trianglelefteq_R R \mid \sqrt{\mathfrak{b}}$ is not such an intersection$\}$ has a maximal element I. (R is noetherian)

Then $\mathfrak{t}$ is not prime, so $\exists\, c, b \in R : cb \in \mathfrak{t}$ and $c, b \notin \mathfrak{t}$.

$$\mathfrak{t}_c := \sqrt{Rc + \mathfrak{t}} \supsetneq \mathfrak{t}$$

$$\mathfrak{t}_b := \sqrt{Rb + \mathfrak{t}} \supsetneq \mathfrak{t}$$

$\Rightarrow$ $\mathfrak{t}_c$ and $\mathfrak{t}_b$ are finite intersections of prime ideals.

$$\Rightarrow \quad \mathfrak{t} \subseteq \mathfrak{t}_b \cap \mathfrak{t}_c = \sqrt{(Rb + \mathfrak{t})(Rc + \mathfrak{t})}$$

$$\subseteq \sqrt{\mathfrak{t}} = \mathfrak{t}$$ is also such an intersection $\lightning$

<u>Step 2:</u> We can find a set $\{\mathfrak{p}_i \mid i \in I\} \subseteq V(\mathfrak{a})$ satisfying (b1) and (b2)

<u>Pf:</u> Take $\mathfrak{q}_1, \dots, \mathfrak{q}_\ell$ from Step 1 s.t.

$$\sqrt{\mathfrak{a}} = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_\ell.$$

and if $\mathfrak{q}_{i_0} \supseteq \bigcap_{i \neq i_0} \mathfrak{q}_i$ then remove $\mathfrak{q}_{i_0}$. $\square$

<u>Step 3:</u> We prove (b). (With Step 2 we obtain (a))

Consider $\{\mathfrak{p}_i \mid i \in I\}$ satisfying (b1) and (b2)

Take $i_0 \in I$ and $\mathfrak{p}$ a prime such that $\mathfrak{p} \subseteq \mathfrak{p}_{i_0}$

Take $x \in \mathfrak{p}_{i_0}$ and $y \in \left(\bigcap_{i \neq i_0} \mathfrak{p}_i\right) \setminus \mathfrak{p}_{i_0}$.

Then $xy \in \mathfrak{p}_{i_0} \cdot \left(\bigcap_{i \neq i_0} \mathfrak{p}_i\right) \subseteq \mathfrak{p}_{i_0} \cap \left(\bigcap_{i \neq i_0} \mathfrak{p}_i\right) = \sqrt{\mathfrak{a}}$

$\subseteq \mathfrak{p}$.

$y \notin \mathfrak{p}_{i_0} \supseteq \mathfrak{p} \Rightarrow x \in \mathfrak{p}$.

$\Rightarrow \mathfrak{p}_{i_0} = \mathfrak{p}$. So all the $\mathfrak{p}_i$ are $\in V_{min}(\mathfrak{a})$

Take $\mathfrak{p} \in V_{min}(\mathfrak{a})$. $\Rightarrow \mathfrak{p} \supseteq \sqrt{\mathfrak{a}} \supseteq \prod_{i \in I} \mathfrak{p}_i$

$\Rightarrow \exists_{i_0 \in I} : \mathfrak{p} \supseteq \mathfrak{p}_{i_0} \supseteq \mathfrak{a}$.

Minimality of $\mathfrak{p} \Rightarrow \mathfrak{p} = \mathfrak{p}_{i_0}$ $\square$

<u>Example 50:</u> $R = \mathbb{Z}[\sqrt{-5}] = \mathbb{Z} \oplus \mathbb{Z}\sqrt{-5}$

$\mathfrak{a} = (6)_R = 6\mathbb{Z}[\sqrt{-5}] = 6\mathbb{Z} \oplus 6\mathbb{Z}\sqrt{-5}$.

Then $\sqrt{(6)_R} = \sqrt{(2)_R (3)_R} = \sqrt{(2)_R} \cap \sqrt{(3)_R}$

Find $V_{min}((6)_R)$.

<u>Claim:</u> $V_{min}((6)_R) = \{(2, 1+\sqrt{-5})_R, (3, 1+\sqrt{-5})_R, (3, 1-\sqrt{-5})_R\}$

We just show: $\sqrt{(2)}$ is prime and

$\sqrt{(2)} = (2, 1+\sqrt{-5})$.

~~$\sqrt{(2)}$ prime~~

<u>Pf:</u> We have $(2)_R \subseteq (2, 1+\sqrt{-5})_R \subseteq \sqrt{(2)_R}$

because $(1+\sqrt{-5})^2 = -4 + 2\sqrt{-5} \in (2)_R$.

So we only have to show that $(2, 1+\sqrt{-5})$ is prime, because then $\sqrt{(2)_R} \subseteq (2, 1+\sqrt{-5}) \subseteq \sqrt{(2)_R}$.

prime ideals are radical.

$$(2, 1+\sqrt{-5})_R = 2\mathbb{Z}[\sqrt{-5}] + (1+\sqrt{-5})\mathbb{Z}[\sqrt{-5}]$$
$$= 2\mathbb{Z}[\sqrt{-5}] + (1+\sqrt{-5})\underbrace{\mathbb{Z}[1-\sqrt{-5}]}_{\mathbb{Z} + \mathbb{Z}\cdot(1-\sqrt{-5})}$$

$$= 2\mathbb{Z}[\sqrt{-5}] + \mathbb{Z}\cdot(1+\sqrt{-5})$$
$$= \left\{ a + b\sqrt{-5} \;\middle|\; \begin{array}{l} a, b \in \mathbb{Z} \\ a \equiv_2 b \end{array} \right\}$$

Take $a+b\sqrt{-5}$, $c+d\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ s.t.

$$(a+b\sqrt{-5})(c+d\sqrt{-5}) \in (2, 1+\sqrt{-5})_R$$

$$\Rightarrow \quad ac - 5bd \equiv_2 ad + bc$$
$$\Leftrightarrow \quad a(c-d) \equiv_2 b(c-d)$$
$$\Leftrightarrow \quad (a-b)(c-d) \equiv_2 0$$
$$\Leftrightarrow \quad 2 \mid a-b \text{ or } 2 \mid c-d.$$
$$\Leftrightarrow \quad a+b\sqrt{-5} \in (2, 1+\sqrt{-5})_R \text{ or}$$
$$c+d\sqrt{-5} \in \text{— " —}.$$

So $(2, 1+\sqrt{-5})_R$ is prime. $\square$

The claim and Thm 49 imply $\sqrt{(6)_R} = (2, 1+\sqrt{-5})_R \cap (3, 1+\sqrt{-5})_R \cap (3, 1-\sqrt{-5})_R$.

There is a decomposition for radical ideals in non-noetherian rings.

<u>Theorem 51:</u> Let R be a ring and $\mathfrak{a} \leq_R R$.
Suppose $\mathfrak{a} \neq R$.
Then $\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{p} \in V(\mathfrak{a})} \mathfrak{p}$.

<u>Proof:</u> "$\subseteq$" ✓
"$\supseteq$" Take $x \in R \setminus \sqrt{\mathfrak{a}}$.

$\mathfrak{M} := \{ \mathfrak{b} \leq_R R \mid \mathfrak{b} \text{ radical and } x \notin \mathfrak{b} \}$

$\sqrt{\mathfrak{a}} \in \mathfrak{M}$, so $\mathfrak{M} \neq \emptyset$

$\mathfrak{M}$ is inductively ordered, because for $\emptyset \neq \mathfrak{N} \subseteq \mathfrak{M}$ with $(\mathfrak{N}, \text{"}\subseteq\text{"})$ totally ordered the ideal $\mathfrak{t} := \bigcup_{\mathfrak{b} \in \mathfrak{N}} \mathfrak{b}$

is radical: $a^n \in \mathfrak{t} \Rightarrow \exists \mathfrak{b} \in \mathfrak{N} : a^n \in \mathfrak{b}$
$\Rightarrow a \in \mathfrak{b}$ because $\mathfrak{b}$ is radical.
$\Rightarrow a \in \mathfrak{t}$. Further $x \notin \mathfrak{t}$.
So $\mathfrak{t} \in \mathfrak{M}$.

Zorn's Lemma $\Rightarrow$ $\exists\, \hat{\mathfrak{b}} \in \mathcal{M}$ a "$\subseteq$"-maximal element.

Claim $\hat{\mathfrak{b}}$ is prime.

$ab \in \hat{\mathfrak{b}}$. Assume $a, b \notin \hat{\mathfrak{b}}$.

$\Rightarrow$ $x \in \sqrt{aR + \hat{\mathfrak{b}}}$ and $x \in \sqrt{bR + \hat{\mathfrak{b}}}$

$$\Rightarrow \quad x^2 \in \sqrt{} \cdot \sqrt{}$$

$$\subseteq \sqrt{} \cap \sqrt{}$$

$$= \sqrt{(aR + \hat{\mathfrak{b}})(bR + \hat{\mathfrak{b}})}$$

$$= \sqrt{\hat{\mathfrak{b}}} = \hat{\mathfrak{b}}.$$

$\hat{\mathfrak{b}}$ radical.

$\Rightarrow$ $x \in \hat{\mathfrak{b}}$ $\lightning$. So $a \in \hat{\mathfrak{b}}$ or $b \in \hat{\mathfrak{b}}$.

Thus $\hat{\mathfrak{b}}$ is a prime ideal satisfying

$$x \notin \hat{\mathfrak{b}} \supseteq \mathfrak{a}$$

Therefore $x \notin \bigcap_{\mathfrak{p} \in V(\mathfrak{a})} \mathfrak{p}$ $\square$

<u>Example 52:</u> Consider the non-noetherian ring $R := k[X_1, X_2, X_3, \dots]$ where k is a field. Then we have

(a) $\underbrace{(X_i X_j \mid i \neq j)_R}_{=: \mathfrak{a}} = \bigcap_{i=1}^{\infty} \underbrace{(X_1, X_2, \dots, \hat{X}_i, X_{i+1}, X_{i+2}, \dots)_R}_{\mathfrak{q}_i}$

(b) ~~Then~~ $V_{\min}(\mathfrak{a}) = \{\mathfrak{q}_i \mid i \in \mathbb{N}\}$

(c) $\forall i_0 \in \mathbb{N}: \quad \mathfrak{q}_{i_0} \not\supseteq \bigcap_{i \neq i_0} \mathfrak{q}_i$.

<u>Proof:</u> (a) "$\subseteq$" ✓ "$\supseteq$" $p \in \bigcap_{i=1}^{\infty} \mathfrak{q}_i$

$\Rightarrow \forall i \in \mathbb{N} \ \forall j \in \mathbb{N}\ j \neq i:$

$p \in \mathfrak{q}_i \cap \mathfrak{q}_j$

$\|$

$Q_1(X_i, X_j) + Q_2(X_{i_1}, X_{i_2}, \dots, X_{i_e})$

$\{i_1, \dots, i_e\} \not\ni i, j.$

$\overset{\text{exercise}}{\Longrightarrow} Q_1(X_i, X_j) \in (X_i)_R \cap (X_j)_R$

$\|$

$(X_i X_j)_R$

For an element Q of $\mathfrak{q}_i$ we have that all monomials occurring in Q have the form $X_{j_1} X_{j_2} \cdots X_{j_\ell}$ with $\ell > 0$ and some $j_i \neq i$.

Thus $\forall_{i \in \mathbb{N}}$ there does not exists $n \in \mathbb{N}_0$ such that X_i^n occurs in P.

$\Longrightarrow P \in \mathfrak{M}$.

(c) Take $i_0 \in \mathbb{N}$. Then $X_{i_0} \in \bigcap_{i \neq i_0} \mathfrak{q}_i$,

and therefore $\mathfrak{q}_{i_0} \not\supseteq \bigcap_{i \neq i_0} \mathfrak{q}_i$.

(e) Exercise! $\square$

If there is time, then we will later study primary decompositions of f.g. modules ~~of~~ over noetherian rings.

I.3. projective and injective modules

For vector spaces, if $V \overset{\varphi}{\twoheadrightarrow} W$ then one can realize this map as $V = U \oplus \tilde{W} \to W$, $u + \tilde{w} \mapsto \varphi(\tilde{w})$

where $U = \ker(\varphi)$, i.e. $\ker(\varphi)$ has a direct complement $\simeq W$.

Similar $W \overset{\psi}{\hookrightarrow} V$ can be realized

as $W \longrightarrow \tilde{W} \oplus U$, $w \mapsto \varphi(w)$

where $\tilde{W} = \operatorname{im} \varphi$ and U is a direct complement of $\tilde{W}$.

For modules this goes wrong.

Example 53:

① $\mathbb{Z}$ as a $\mathbb{Z}$ module. $\mathbb{Z} \xrightarrow{\varphi} \mathbb{Z}/2\mathbb{Z}$, $z \mapsto [z]_2$

$\ker \varphi = 2\mathbb{Z}$ is not a direct summand of $\mathbb{Z}$.

② $\mathbb{Z} \overset{\psi}{\hookrightarrow} \mathbb{Z}$ $\quad \psi(z) = 2z$.

We look for modules M_3 which force any short exact sequence $0 \to M_1 \to M_2 \to M_3 \to 0$ to split.

<u>Def 54:</u> An R-module M_3 is called <u>projective</u> if any short exact sequence $0 \to M_1 \to M_2 \to M_3 \to 0$ of R-module splits "$(\text{proj})_R$"

An R-module M_1 is called injective if every exact sequence of R-modules $0 \to M_1 \to M_2 \to M_3 \to 0$ splits. "$(\text{inj})_R$"

<u>Lecture 7. 9.10.2021</u>

<u>Example 55:</u>

(a) $\mathbb{Z}/2\mathbb{Z}$ is not a projective $\mathbb{Z}$-module, but it is a projective $(\mathbb{Z}/2\mathbb{Z}, +, \cdot)$-module, because $(\mathbb{Z}/2\mathbb{Z}, +, \cdot)$ is a field.

$\mathbb{Z}/2\mathbb{Z}$ is not an injective $\mathbb{Z}$-module because

$$0 \to \mathbb{Z}/2\mathbb{Z} \xrightarrow{[z]_2 \mapsto [2z]_4} \mathbb{Z}/4\mathbb{Z} \xrightarrow{[z]_4 \mapsto [z]_2} \mathbb{Z}/2\mathbb{Z} \to 0$$

does not split.

(If it would split then $\mathbb{Z}/4\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ ↯)

(b) R^n is projective

$$0 \longrightarrow M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} R^n \longrightarrow 0$$

Let $\{e_1, \dots, e_n\}$ be the standard basis of R^n.

Take $v_1, \dots, v_n \in M_2$ s.t. $\beta(v_i) = e_i$ and

define $s : R^n \longrightarrow M_2$ via $s(e_i) := v_i$

and linearly extension.

$$\left(s\left(\sum_{i=1}^{n} \lambda_i e_i\right) := \sum_{i=1}^{n} \lambda_i v_i \right)$$

Then $\beta \circ s\left(\sum \lambda_i e_i\right) = \sum \lambda_i \beta(v_i) = \sum \lambda_i e_i$.

$\Longrightarrow \beta \circ s = id_{R^n}$.

So the sequence is split.

(c) $\mathbb{Q}/\mathbb{Z}$ is an injective $\mathbb{Z}$-module.

<u>Proof:</u> Let $0 \longrightarrow \mathbb{Q}/\mathbb{Z} \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3 \longrightarrow 0$

be an ex. sequence of $\mathbb{Z}$-modules.

Define $\mathcal{M} := \{ U \leq_{\mathbb{Z}} M_2 \mid \alpha(\mathbb{Q}/\mathbb{Z}) \cap U = \{0\} \}$

Then $\{0\} \in \mathcal{M}$ and $\mathcal{M}$ is inductively ordered w.r.t. "$\subseteq$".

($(N_i)_{i \in I}$ a "$\subseteq$"-chain

$\Rightarrow \bigcup_{i \in I} N_i \in \mathcal{M}$.)

Zorn's Lemma $\Rightarrow \exists\ \hat{U} \leq_{\mathbb{Z}} M_2$ "$\subseteq$"-maximal in $\mathcal{M}$.

<u>Claim:</u> $\alpha(\mathbb{Q}/\mathbb{Z}) \oplus \hat{U} = M_2$.

<u>Pf:</u> Assume $M_2 \supsetneq \alpha(\mathbb{Q}/\mathbb{Z}) \oplus \hat{U}$.

Then take $m \in M_2 \setminus$ — " — and put $z_0 := \min \{ z \in \mathbb{N} \mid zm \in \alpha(\mathbb{Q}/\mathbb{Z}) \oplus \hat{U} \}$

(Note: z_0 exists, because otherwise $\mathbb{Z}m + \hat{U} \in \mathcal{M}$ ↯)

$$z_0 m = \alpha([\tilde{q}]_{\mathbb{Z}}) + \hat{u}_0$$
$$= z_0\, \alpha([\tilde{q} \cdot \tfrac{1}{z_0}]_{\mathbb{Z}}) + \hat{u}_0$$

$$\Rightarrow \quad m_0 := m - \alpha([\tilde{q}\, \tfrac{1}{z_0}]_{\mathbb{Z}}) \in M_2 \setminus (\alpha(\mathbb{Q}/\mathbb{Z}) + \hat{U})$$

and $z_0 m_0 \in \hat{U}$.

We show $\tilde{U} \cap \alpha(\mathbb{Q}/\mathbb{Z}) = \{0\}$ for

$\tilde{U} := \mathbb{Z} m_0 + \hat{U}$.

<u>Pf:</u> If $z m_0 + \hat{u} \in \tilde{U} \cap \alpha(\mathbb{Q}/\mathbb{Z})$

$$\Rightarrow \quad z m_0 \in \alpha(\mathbb{Q}/\mathbb{Z}) + \hat{U}$$

$$\Rightarrow \quad z m \in \quad — \text{ " } —$$

$$\Rightarrow \quad z_0 \mid |z| \Rightarrow z m_0 \in \hat{U}$$

$$\Rightarrow \quad z m_0 + \hat{u} \in \hat{U} \cap \alpha(\mathbb{Q}/\mathbb{Z}) = \{0\} \quad \square$$

Thus $\tilde{U} \in \mathcal{M}$ with $\tilde{U} \supsetneq \hat{U}$ ↯.

$\square$

Def 56: An R-module M is called <u>divisible</u>

if $\forall m \in M \ \forall r \in R$ $r \neq 0$ not a zero divisor:

$\exists m' \in M$: $rm' = m$.

Example 57: (1) $\mathbb{Q}/\mathbb{Z}$ and $\mathbb{Q}$ are divisible

$\mathbb{Z}$-modules.

Vector spaces are divisible.

(2) $\mathbb{Z}[\sqrt{d}]$, d square free $d \in \mathbb{N}^{\geq 2}$

is not a divisible $\mathbb{Z}$-module.

$r = 2$. $\quad m' = a + b\sqrt{d}$.

$2 \cdot m' = 2a + 2b\sqrt{d} \neq 1$.

The concept related to projective modules is free modules.

Def 58: ① An R-module M is called free

if $\exists$ set I: $\quad M \simeq \bigoplus_{i \in I} R$

② A set $\{m_i \mid i \in I\} \subseteq M$ is called

(a) R-linearly independent if

$\forall_{(r_i)_{i\in I},\, r_i\in R} : \left(\sum r_i m_i = 0 \implies \text{all } r_i \text{ are zero} \right)$

$r_i = 0$ f.a.a. i

("The only linear combination of 0_M is by 0_R-coefficients.")

(b) R-generating set for M if the homomorphism

$$\bigoplus_{i\in I} R \xrightarrow{\varphi} M \qquad \varphi((r_i)_{i\in I}) := \sum_{i\in I} r_i m_i$$

is surjective.

(c) an R-basis of ~~of~~ M if it is an R-generating set of M and R-linearly independent.

<u>Remark 59:</u> An R-module M is free if and only if it contains an R-basis.

<u>Proof:</u> "$\Rightarrow$" $M \overset{\varphi}{\simeq} \bigoplus_I R$. $m_i := \varphi^{-1}(e_i)$, $e_i := (x_j)_{j\in I}$

$$x_j = \begin{cases} 1, & j = i \\ 0, & j \neq i \end{cases}$$

$\{e_i \mid i\in I\}$ is an R-basis of $\bigoplus_I R$, so

$\{m_i \mid i \in I\}$ — " — M.

"$\Leftarrow$" Given an R-basis $\{m_i \mid i\in I\}$ of M

define $\bigoplus_I R \xleftrightarrow{\sim} M$

$$\varphi((r_i)_{i\in I}) := \sum r_i m_i$$

α R-linear ✓

surjective (by definition of R-generating set)

injective, because $\{m_i \mid i \in I\}$ is R-linearly independent. $\square$

<u>Remark 60:</u> Free R-modules are projective.

See Example 55(b) for the idea for the proof.

We have a property which looks stronger than $(\text{proj})_R$, but we will show it isn't.

<u>Def 61:</u> Let M be an R-module. We say that

(a) M satisfies $(\text{proj}+)_R$, if for all diagrams of R-modules

$$\begin{tikzcd} & M \arrow[d, "\gamma"] \\ N_2 \arrow[r, two heads, "\beta"] & N_3 \end{tikzcd}$$

$\exists\ \delta : M \longrightarrow N_2$:

$$\begin{tikzcd} & M \arrow[dl, "\delta"'] \arrow[d, "\gamma"] \arrow[dl, phantom, shift right=3ex, "\circlearrowleft"] \\ N_2 \arrow[r, two heads, "\beta"] & N_3 \end{tikzcd}$$

i.e. $\beta \circ \delta = \gamma$.

"We can lift γ from N_3 to N_2 using β".

(b) M satisfies $(\text{inj}+)_R$ if

for all diagrams of R-modules

$$\begin{tikzcd} N_1 \arrow[r, hook, "\alpha"] \arrow[d, "\varepsilon"'] & N_2 \\ M & \end{tikzcd}$$

$\exists\ \iota : N_2 \longrightarrow M$:

$$\begin{tikzcd} N_1 \arrow[r, hook, "\alpha"] \arrow[d, "\varepsilon"'] \arrow[dr, phantom, "\circlearrowleft"] & N_2 \arrow[dl, "\iota"] \\ M & \end{tikzcd},$$

i.e. $\iota \circ \alpha = \varepsilon$

"We can ε from N_1 to N_2 along α."

<u>Remark 62</u>: We will see later that

$(\text{proj})_R \Leftrightarrow (\text{proj}+)_R$ and

$(\text{inj})_R \Leftrightarrow (\text{inj}+)_R$.

The second equivalence is very difficult.

At first we have.

<u>Prop 63</u>: (a) $(\text{proj}+)_R \Rightarrow (\text{proj})_R$

(b) $(\text{inj}+)_R \Rightarrow (\text{inj})_R$.

<u>Proof</u>: (a) Let M be an R-module which satisfies $(\text{proj}+)_R$.

let $0 \to M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M \to 0$

be exact. Consider

$$\begin{tikzcd} M_2 \arrow[r, two heads, "\beta"] & M \\ M \arrow[u, "s"] \arrow[ur, "id_M =: \gamma"'] & \end{tikzcd}$$

$(proj+)_R \Rightarrow \exists\, \delta : M \to M_2 : \quad \beta \circ \delta = \gamma = id_M$

$\Rightarrow$ The sequence splits.

(b) exercise. $\square$

<u>Lemma 64'</u> (1) Free R-modules satisfy $(proj+)_R$

(2) Let M be an R-module satisfying $(proj+)_R$ and $N \mid M$. Then N satisfies $(proj+)_R$.

<u>Proof:</u> (1)

$$\begin{tikzcd} & \bigoplus_{i\in I} R \arrow[dl, dashed, "\delta"'] \arrow[d, "\gamma"] \\ M_2 \arrow[r, two heads, "\beta"] & M_3 \end{tikzcd}$$

Take $v_i \in \beta^{-1}(\gamma(e_i))$, $i \in I$.

Define $\delta\left(\sum_{i\in I} r_i e_i\right) := \sum_{i \in I} r_i v_i$.

$\Rightarrow \beta \circ \delta = \gamma$.

(2) Take $U \leq_R M$ s.t. $N \oplus U = M$.

Consider a diagram

$$\begin{tikzcd}
 & N \oplus U \arrow[d, "\pi"] \arrow[dr, bend left, "\tilde{\gamma} := \gamma \circ \pi"] & n+u \arrow[d, mapsto] \\
M_2 \arrow[r, two heads, "\beta"] & U \arrow[r, "\gamma"] & u
\end{tikzcd}$$

$\exists \tilde{\delta}$

$\Rightarrow \exists \tilde{\delta} : M \to M_2 : \quad \beta \circ \tilde{\delta} = \tilde{\gamma}$

Put $\delta(u) := \tilde{\delta}(u), u \in U$.

$$\Rightarrow \beta(\delta(u)) = \beta(\tilde{\delta}(u)) = \tilde{\gamma}(u) = \gamma(\pi(u))$$

$$\underset{\pi(u)=u}{=} \gamma(u) \quad , u \in U. \qquad \square$$

end lecture 8.12.10.2021

Now we collect equivalent conditions for $(proj)_R$.

<u>Theorem 65:</u> Let M be an R-module. T.a.e.:

1° M satisfies $(proj)_R$

2° — " — $(proj^+)_R$

3° $\forall M_2 \xrightarrow{\beta} M_3$ R-hom.:

$$\mathrm{Hom}_R(M, M_2) \xrightarrow{\beta_*} \mathrm{Hom}_R(M, M_3)$$
$$\varphi \longmapsto \beta \circ \varphi$$

is surjective.

4° $\forall\ 0 \to M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3 \to 0$ exact:

$$0 \to \mathrm{Hom}_R(M, M_1) \xrightarrow{\alpha_*} \mathrm{Hom}_R(M, M_2) \xrightarrow{\beta_*} \mathrm{Hom}_R(M, M_3) \to 0$$

is exact

5° M is isomorphic to a direct summand of a free R-module.

For 4° we need the following Lemma:

<u>Lemma 66:</u> Let $0 \to M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3$ be an exact sequence of R-modules. Then for every R-module M the sequence

$$0 \to \mathrm{Hom}_R(M, M_1) \xrightarrow{\alpha_*} \mathrm{Hom}_R(M, M_2) \xrightarrow{\beta_*} \mathrm{Hom}_R(M, M_3)$$

is exact.

<u>Proof:</u> (Note: we do not require β to be surjective)

- α_* is injective: $\alpha_*(\varphi) = 0_{hom} \Rightarrow \alpha \circ \varphi = 0_{hom}$

$$\Rightarrow \forall m \in M: \alpha(\varphi(m)) = 0 \underset{\alpha \text{ inj}}{\Rightarrow} \forall m \in M\ \varphi(m) = 0$$

$$\Rightarrow \varphi = 0_{hom}.$$

- $\beta_* \circ \alpha_* = (\beta \circ \alpha)_* = (0_{hom})_* = 0_{\mathrm{Hom}_R(\mathrm{Hom}_R(M, M_1), \mathrm{Hom}_R(M, M_3))}$

- Take $\psi \in \underset{\substack{\cap \\ \mathrm{Hom}_R(M,M_2)}}{\ker \beta_*} \Rightarrow \beta \circ \psi = 0_{\mathrm{Hom}_R(M,M_3)}$

$\Rightarrow \operatorname{im}\psi \subseteq \ker\beta = \operatorname{im}\alpha$

Let α^{-1} be the inverse of $M_1 \xrightarrow{\alpha}_{\sim} \operatorname{im}\alpha$

Then $\alpha^{-1}\circ\psi \in \mathrm{Hom}_R(M, M_1)$

and $\alpha_*(\alpha^{-1}\circ\psi) = \alpha\circ\alpha^{-1}\circ\psi = \psi$.

$\Rightarrow \psi \in \operatorname{im}\alpha_*$. $\square$

Now we can prove Theorem 65:

<u>Proof</u> (Theorem 65)

<u>$2^\circ \Leftrightarrow 3^\circ$</u>: 3° is just a reformulation of M satisfying $(\mathrm{proj}^+)_R$.

<u>$3^\circ \Leftrightarrow 4^\circ$</u>: follows from Lemma 66.

<u>$2^\circ \Rightarrow 1^\circ$</u>: is Prop. 63 (a)

<u>$1^\circ \Rightarrow 5^\circ$</u>: Take a generating set $\{m_i \mid i \in I\}$ for M and consider

$$\beta : \bigoplus_{i\in I} R \twoheadrightarrow M \qquad \beta\left(\sum r_i e_i\right) := \sum_{i\in I} r_i m_i$$

$$0 \longrightarrow \ker(\beta) \xhookrightarrow{\text{incl}} \bigoplus_{i\in I} R \xrightarrow{\beta} M \to 0$$

is exact.

$1^\circ \Rightarrow \exists\, s \in \mathrm{Hom}_R(M, \bigoplus_I R) : \beta \circ s = \mathrm{id}_M.$

$\Rightarrow \quad M \xrightarrow[\sim]{s} s(M) \,\Big|\, \bigoplus_I R.$

<u>$5^\circ \Rightarrow 2^\circ$:</u> Every free R-module satisfies $(\text{proj}+)_R$. by Lemma 64 (1).
5° and Lemma 64(2) imply 2°. $\square$

<u>Remark 67:</u> All of § I.3. upto here did <u>not</u> need the commutativity of $(R, \cdot)$.

We want to give an example, but need the following definition.

<u>Def 68:</u> An element m of an R-module M is called R-torsion element if $\exists\, r \in R \setminus \{0\}$: $rm = 0_M$ and r is a nonzerodivisor in R.
A module M consisting only of R-torsion elements is called torsion module.

$T_R(M) := \{ m \in M \mid m \text{ is } R\text{-torsion} \}$

M is called <u>R-torsion free</u> if $T_R(M) = \{0_M\}$.

<u>Example 69</u>: (1) Let R be an integral domain. If $T_R(M) \neq \{0_M\}$ then M is not projective.

<u>Proof</u>: Assume M is projective.

Theorem 65.5° $\Rightarrow$ $\exists$ F a free R-module and ~~$\alpha: M \to F$~~ $\alpha \in \mathrm{Mono}_R(M, F)$.

$F \simeq \bigoplus_I R$ and R is an integral domain

$\Rightarrow$ F has no non-zero R-torsion elements.

(<u>Pf</u>: $r(r_i)_{i\in I} = (0_R)_{i\in I}$ with $r \neq 0$

$\qquad\qquad \| $

$\qquad (r r_i)_{i\in I}$

$\Rightarrow$ $r r_i = 0_R$ $\forall i \in I$ $\underset{\substack{\text{integral domain} \\ \text{and } r\neq 0}}{\Rightarrow}$ $\forall i \in I: r_i = 0_R$ $\square$)

$\Rightarrow$ $\alpha(M) \leq_R F$ has no R-torsion

$\Rightarrow$ $M \simeq \alpha(M)$ — " — . $\lightning$ $\square$

(2) $\mathbb{Q}$ is not $\mathbb{Z}$-projective.

<u>Proof</u>: $\mathbb{Q}$ is $\mathbb{Z}$-divisible, so if we have $\mathbb{Q} \xhookrightarrow{\varphi} \bigoplus_{i\in I} \mathbb{Z}$, then $\varphi(1)$

is $\mathbb{Z}$-divisible.

$\varphi(1) = (r_i)_{i \in I}$ let $r_{i_1}, \dots, r_{i_\ell} \in \mathbb{Z} \setminus \{0\}$ be

the non-zero coordinates.

Then r_{i_1} is not divisible by $|r_{i_1}|+1$.

$\Rightarrow$ $\varphi(1)$ is — " —

$\Rightarrow$ $1 \in \mathbb{Q}$ — " — $\lightning$

because $1 = (|r_{i_1}|+1) \dfrac{1}{|r_{i_1}|+1}$ in $\mathbb{Q}$.

(c) $R := \mathbb{R} \times \mathbb{R}$. $M_1 = \mathbb{R} \times \{0\}$

$M_2 = \{0\} \times \mathbb{R}$.

Then M_1 and M_2 are projective R-modules, because $M_1 \oplus M_2 = R$.

But M_1 is not free, because M_1 is a torsion module, in fact

$(0,1) \cdot (r,0) = (0,0) \in M_1 \quad \forall (r,0) \in M_1$.

(A basis element ~~would not be R-torsion~~ has a zero annihilator.)

Over a principal ideal domain the situation is beautiful: $(\mathrm{proj})_R$ is not needed.

<u>Theorem 70:</u> Let R be a PID.

(1) Every R-submodule of a free R-module is free.

(2) Every R-projective module is R-free.

<u>Remark 71:</u> Thm 70 (2) implies that $\mathbb{Q}$ is not $\mathbb{Z}$-free. (but there are easier ways to show it.)

Before we prove Thm 70. we give an interesting example.

<u>Example 72:</u> $R = \mathbb{Z}[\sqrt{-5}]$ $\quad \mathfrak{U} := \mathfrak{U}_1 = (2, 1+\sqrt{-5})_R$.

Then $\mathfrak{U}$ is a non-R-free, but ~~and~~ R-projective, module.

<u>Proof:</u> <u>Non-freeness:</u> $\mathfrak{U} = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}, a \equiv_2 b\}$

Two non-zero elements of $\mathfrak{U}$ are linearly dependent:

$$z_1, z_2 \in \mathfrak{U} \setminus \{0\} \Rightarrow (z_2 \bar{z}_2 \cdot \bar{z}_1) \cdot z_1 - (z_1 \bar{z}_1 \bar{z}_2) \cdot z_2 = 0.$$

(Here $\bar{z} = \overline{a+b\sqrt{-5}} = a - b\sqrt{-5}$).

Note that $z_2 \bar{z}_2 \bar{z}_1$ and $z_1 \bar{z}_1 z_1$ are non-zero, because R is an integral domain, because $R \subseteq \mathbb{C}$.

Assume now that $\mathfrak{a}$ is R-free.

Then, by the above, $\mathfrak{a} = (z)_R$ for some $z \in \mathbb{Z}[\sqrt{-5}]$.

Ex. 50 $\Rightarrow$ $\mathfrak{a}$ is prime. Also $z \notin R^\times \cup \{0\}$.

So z is a prime element of R.

Now $z \mid 2 \in \mathfrak{a}$ $\Rightarrow$ $\exists u \in R^\times$: $uz = 2$.

2 is irreducible $\Rightarrow$ $u \in R^\times$. $\Rightarrow$ 2 is a prime element $\lightning$.

Thus $\mathfrak{a}$ is not R-free.

<u>R-projectiveness:</u>

We have

$$\Big(\underbrace{\overset{b_1}{\left(\tfrac{1}{2} + \tfrac{1}{2}\sqrt{-5}\right)}\overset{a_1}{\left(1+\sqrt{-5}\right)}}_{-2+\sqrt{-5}} + \underbrace{\overset{b_2}{3}\overset{a_2}{\left(1+\sqrt{-5}\right)}}_{3+3\sqrt{-5}} + \underbrace{\overset{b_3}{\left(\sqrt{-5}(-2)\right)}\cdot\overset{a_3}{2}}_{-4\sqrt{-5}}\Big) = 1$$

Note: $b_1\mathfrak{a} + b_2\mathfrak{a} + b_3\mathfrak{a} \subseteq R$

and

$$(a_1, a_2, a_3)_R = \mathfrak{a}.$$

Consider the maps:

$$R^3 \underset{s}{\overset{\beta}{\rightleftarrows}} \mathfrak{A}$$

$\beta(r_1, r_2, r_3) := r_1 a_1 + r_2 a_2 + r_3 a_3$

$s(a) := (b_1 a, b_2 a, b_3 a)$

β, s are R-homos. and $\beta \circ s(a) = b_1 a a_1 + b_2 a a_2 + b_3 a a_3$

$= a$

$= id_{\mathfrak{A}}(a)$.

$\Rightarrow \mathfrak{A} \mid R^3 \Rightarrow \mathfrak{A}$ is R-projective. $\square$

<u>Exercise:</u> Think about the hidden property of $\mathfrak{A}$ forcing the argument to work.

(Answer: Next lecture.)

end of lecture 9:

<u>Proof of Theorem 70:</u>

(2) follows from (1) because an R-projective module is R-isomorphic to a direct summand of an R-free module, in particular to an R-submodule of an R-free module.

So we prove (1):

Let $0 \neq N \leq_R \bigoplus_I R =: \mathcal{M}$.

Write $\mathcal{M}_J := \bigoplus_J R$ for $J \subseteq I$

$\bigoplus_J R = \sum_{i \in J} R e_i$

and $N_J := N \cap M_J$.

Put $\mathcal{M} := \{ (J, B) \mid \emptyset \neq J \subseteq I$ and

B is an R-basis of N_J

(B is empty if $N_J = \{0\}$) $\}$

We have an order on $\mathcal{M}$.

$(J_1, B_1) \leq (J_2, B_2) \Leftrightarrow_{\text{def.}} J_1 \subseteq J_2$ and $B_1 \subseteq B_2$.

We want to use Zorn's Lemma

So we have to show:

(i) $\mathcal{M} \neq \emptyset$

(ii) $(\mathcal{M}, \leq)$ is inductively ordered.

<u>(i)</u>: Take $i_0 \in I$. If $N_{\{i_0\}} = 0$

then $(\{i_0\}, \emptyset) \in \mathcal{M}$.

Otherwise $0 \neq N_{\{i_0\}} \leq_R R e_{i_0} \simeq R$

R (PID) $\Rightarrow \exists\, a \in R \setminus \{0\} : N_{\{i_0\}} = R a e_{i_0}$.

M is torsion free, because M is free.

$\Rightarrow$ N is torsion free. $\Rightarrow$ $a e_{i_0}$ is an R-basis.

of $N_{\{i_0\}}$. $\Rightarrow$ $(\{i_0\}, \{a e_{i_0}\}) \in \mathcal{M}$.

(ii) Let $\emptyset \neq \mathcal{N} \subseteq \mathcal{M}$ be a chain.

Define $\mathcal{J}' := \bigcup_{\substack{(\mathcal{J},B) \in \mathcal{M} \\ \text{for some } B}} \mathcal{J}$ $\qquad$ $B' := \bigcup_{\substack{(\mathcal{J},B) \in \mathcal{N} \\ \text{for some } \mathcal{J}.}} B$

Exercise $(\mathcal{J}', B') \in \mathcal{M}$.

Further $(\mathcal{J}, B) \leq (\mathcal{J}', B') \; \forall (\mathcal{J}, B) \in \mathcal{N}$,

so we have an upper bound.

Zorn's Lemma $\Rightarrow$ $\exists$ "$\leq$"-maximal element $(\hat{\mathcal{J}}, \hat{B})$ in $\mathcal{M}$.

Assume $\hat{\mathcal{J}} \neq I$. Take $i_0 \in I \setminus \hat{\mathcal{J}}$.

Consider the ideal

$$\{r \in R \mid (r e_{i_0} + M_{\hat{\mathcal{J}}}) \cap N \neq \emptyset\}$$

$= (a)_R$ (because R is a PID.)

Take $\hat{w} \in M_{\hat{\mathcal{J}}}$, s.t. $a e_{i_0} + \hat{w} \in N$ and

put $b_{i_0} := a e_{i_0} + \hat{w}$

<u>Claim:</u>

① If $a = 0$ then $(\hat{\mathcal{J}} \cup \{i_0\}, B\hat{\mathcal{J}}) \in \mathcal{M}$.

② If $a \neq 0$ then

$$N_{\hat{\mathcal{J}} \cup \{i_0\}} = N_{\mathcal{J}} + R e_{i_0} \quad \text{(inner direct sum)}$$

(exercise!)

So $(\hat{\mathcal{J}} \cup \{i_0\}, B\hat{\mathcal{J}} \cup \{e_{i_0}\}) \in \mathcal{M}$. ↯

□

For page 77. Examples for ~~exte~~ lifting and extending:

1) $\mathbb{Z}/16\mathbb{Z}$ is not a projective $\mathbb{Z}$-module (why?), but some lifting exist.

$$\begin{tikzcd}
 & \mathbb{Z}/16\mathbb{Z} \arrow[d, "\gamma"] & {[z]_{16}} \arrow[d, mapsto] \\
\mathbb{Z}/6\mathbb{Z} \arrow[ur, dashed, "\delta"] \arrow[r, two heads, "\beta"] & \mathbb{Z}/2\mathbb{Z} & {[z]_2} \\
{[z]_6} \arrow[r, mapsto] & {[z]_2} &
\end{tikzcd}$$

$\delta([z]_{16}) := [3z]_6$

2) $\begin{tikzcd} \mathbb{Z} \arrow[r, hook] \arrow[d, "id"'] & \mathbb{Q} \\ \mathbb{Z} & \end{tikzcd}$ $\mathbb{Z}$ is not $(\text{inj}+)_R$, because we cannot extend $id_{\mathbb{Z}}$ to $\mathbb{Q}$.

Let's summarize:

In general: projective modules are direct summands of free modules

hereditary rings: projective modules are precisely the submodules of free modules.

For PID: projective modules are free

<u>Def 73:</u> A ring R is called hereditary if every ideal of R is R-projective.

<u>Examples 74:</u> (a) PID's are hereditary ($(a)_R = Ra \cong R$)

(b) $R = \mathbb{Z}[\sqrt{-5}]$ is hereditary.

The reason is the following fact:

$$\forall \mathfrak{a} \leq_R R \ \exists\, \mathfrak{b} \leq_R R : \mathfrak{a}\mathfrak{b} \text{ is non-zero principal,}$$

i.e. $\exists\, \pi \in R \setminus \{0\} : \mathfrak{a}\mathfrak{b} = (\pi)_R$

(You can see $\frac{1}{\pi}\mathfrak{b}$ as an R-submodule of $Q(R) = \mathbb{Q}[\sqrt{-5}]$)

So for $\mathfrak{a} = (a_1, \dots, a_m)_R$ ~~and~~ we find

~~for~~ $b_1, \dots, b_m \in \mathfrak{b}$: $\sum_{i=1}^{m} \frac{b_i}{\pi} \cdot a_i = 1$.

Then consider $R^m \xrightarrow{\varphi} \mathfrak{a}$ $\quad \varphi(r_1, \dots, r_m) = \sum_{i=1}^{m} r_i a_i$

$\quad \rightsquigarrow s$

$$s(a) := \left(a\frac{b_1}{\pi}, \dots, a\frac{b_m}{\pi}\right) \in R^m.$$

Topic for this: Dedekind rings.

We have an analogue to Theorem 70 for hereditary rings

<u>Theorem 75:</u> Let R be a hereditary ring. Then every submodule of a free module is isomorphic to a direct sum of ideals.

$$\left(M \leq_R \bigoplus_I R \Rightarrow \exists (\mathfrak{a}_\lambda)_{\lambda \in \Lambda} \ \mathfrak{a}_\lambda \leq_R R : \right.$$
$$\left. M \simeq \bigoplus_{\lambda \in \Lambda} \mathfrak{a}_\lambda \right)$$

<u>Proof:</u> Like the proof of Theorem 70. Exercise! $\square$

<u>Remark 76:</u> Thm 70 and 75 are true in the non-commutative setting. Exercise! (right projective and right hereditary)

<u>Corollary 77:</u> A finitely generated torsion-free module over a PID is free.

<u>Proof:</u> $M = Rm_1 + \dots + Rm_\ell$. $\quad m_i \neq 0$

Let $S = \{v_1, \dots, v_t\}$ be maximal linearly independent set in M.

$$\Rightarrow \quad \mathbb{Z}^\ell \simeq F := Rv_1 + \dots + Rv_t \leq_R M$$

$\forall i = 1, \dots, \ell$: $Rm_i \cap F \neq \{0_M\}$,

by the maximality of S and torsion-free-ness, in particular $(am_i = 0 \underset{\substack{m_i \neq 0 \\ M \text{ torsion-free}}}{\Rightarrow} a = 0)$

Thus $\forall i = 1, \dots, \ell \; \exists a_i \in R \setminus \{0\}$: $a_i m_i \in F$

$\Rightarrow$ $a := a_1 \cdots a_\ell$ $\quad \varphi : M \hookrightarrow F \quad \varphi(m) := am$.

(M torsion-free $\Rightarrow$ φ is injective)

$\Rightarrow$ $\varphi(M)$ is free by Theorem 70.

<u>Example 78:</u> (a) $\begin{pmatrix} \mathbb{Z} & \mathbb{Z} \\ 0 & \mathbb{Z} \end{pmatrix} = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| \, a, b, c \in \mathbb{Z} \right\} \subseteq \mathbb{Z}^{2 \times 2}$

is not a left-hereditary ring

(Exercise!)

(b) $\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$

We will see that $\begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ p\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$

is right and left-hereditary.

<u>end of lecture 10.</u>

Now we look at injective modules.
Remember we have to prove $(inj)_R \Rightarrow (inj^+)_R$.

<u>Theorem 79:</u> (Baer) Let M be an R-module
Then are equivalent:
1° M is R-injective
2° $\forall J \leq_R R \ \forall \varepsilon : J \longrightarrow M \ \exists \iota : R \to M \mid_J = \varepsilon$.

<u>Proof:</u> We only need to prove $2° \Rightarrow 1°$.
Consider
$$\begin{tikzcd} M_1 \arrow[r, hook, "\alpha"] \arrow[d, "\varepsilon"'] & M_2 \\ M & \end{tikzcd}$$
(α w.l.o.g. an inclusion.)

$$\mathfrak{M} := \{ (N, \iota) \mid M_1 \leq_R N \leq_R M_2, \ \iota \in \mathrm{Hom}_R(N, M) \text{ such that } \iota|_{M_1} = \varepsilon \} \ni (M_1, \varepsilon)$$

$\mathfrak{M}$ is inductively ordered w.r.t.
$$(N_1, \iota_1) \leq (N_2, \iota_2) \Leftrightarrow_{Def.} N_1 \subseteq N_2 \text{ and } \iota_2|_{N_1} = \iota_1.$$
Let $(\hat{N}, \hat{\iota})$ be a maximale element of $\mathfrak{M}$ (Zorn's Lemma) and assume $\hat{N} \subsetneq M_2$.

Take $m \in M_2 \setminus \hat{N}$.

$J := \{ r \in R \mid rm \in \hat{N} \}$ is an ideal of R.

$$\begin{tikzcd} J \arrow[r, hook] \arrow[d, "\tilde{\xi}"'] \arrow[dr, phantom, "\circlearrowleft"] & R \arrow[dl, dashed, "\exists \tilde{L}"] \\ M & \end{tikzcd}$$

$\tilde{\xi}(i) := \hat{L}(i \cdot m)$

$\tilde{L} \circ \mathrm{ind}_{J \hookrightarrow R} = \tilde{\xi} \quad (\tilde{L}|_J = \tilde{\xi})$ by 2°.

Define $N' := \hat{N} + Rm$

$L'(\hat{n} + rm) := \hat{L}(\hat{n}) + \tilde{L}(r)$.

Well-defined ?! $\hat{n}_1 + r_1 m = \hat{n}_2 + r_2 m$

$\Rightarrow \quad \hat{L}(\hat{n}_1) - \hat{L}(\hat{n}_2) = \hat{L}(\hat{n}_1 - \hat{n}_2) = \tilde{\xi}(r_2 - r_1)$

$= \tilde{L}(r_2 - r_1) = \tilde{L}(r_2) - \tilde{L}(r_1)$.

$L' \in \mathrm{Hom}_R(N', M)$ ✓ (Exercise!)

Thus $(N', L') \in \mathcal{M}$ ↯. $\square$

<u>Corollary 80:</u> Let M be an R-module.

(1) If M is $(\mathrm{inj}+)_R$ then M is R-divisible.

(2) Suppose $R = \mathbb{Z}$ or a PID.

Then, if M is ~~(inj+)$_R$, then~~ R-divisible, then M satisfies $(\text{inj}+)_R$.

<u>Proof:</u> (1) Take $r \in R$ not a zero-divisor. $m \in M$.

$$\begin{tikzcd} (r) = J \arrow[r, hook] \arrow[d, "\varepsilon"'] & R \arrow[dl, dashed, "L"] \\ M & \end{tikzcd}$$

$\varepsilon(\lambda r) := \lambda . m$.

$(\text{inj}+)_R \Rightarrow \exists\, L : R \to M : L|_J = \varepsilon$.

$\Rightarrow \quad rL(1) = L(r) = \varepsilon(r) = m$.

(2) Consider

$$\begin{tikzcd} (r) \overset{PID}{=} J \arrow[r, hook] \arrow[d, "\varepsilon"'] & R \\ M & \end{tikzcd}$$

If $J = \{0\}$, then we extend ε by 0, i.e. $L(x) = 0 \ \forall x \in R$.

Suppose $J \supsetneq \{0\}$.

M is R-divisible and r is not zero.

$\Rightarrow$ r is not a zero-divisor (R is an integral domain) and for $m := \varepsilon(r)$ $\exists\, m' \in M : rm' = m$.

Define $L : R \to M$ via: $L(x) := xm'$

Then $L(\lambda r) = \lambda r m' = \lambda m = \lambda \varepsilon(r) = \varepsilon(\lambda r)$.

So by Baer's criterion M satisfies $(\text{inj}+)_R$

$\square$

<u>Corollary 81:</u> $(\text{inj})_{\mathbb{Z}} \Leftrightarrow (\text{inj}+)_{\mathbb{Z}} \Leftrightarrow \mathbb{Z}$-divisible.

<u>Proof:</u> Let M be a $\mathbb{Z}$-module satisfying $(\text{inj})_{\mathbb{Z}}$, $r_0 \in \mathbb{Z} \setminus \{0\}$, $m_0 \in M$.

Consider
$$M \xhookrightarrow{\alpha} M \oplus R \big/ \{(\lambda m_0, -\lambda r_0) \mid \lambda \in R\} =: M_2$$
$$m \longmapsto [(m, 0)]$$

$(\text{inj})_{\mathbb{Z}} \Rightarrow \exists\, s \in \mathrm{Hom}_{\mathbb{Z}}(M_2, M)$: $s \circ \alpha = id_M$.

$$\Rightarrow s(\alpha(m_0)) = s([(m_0, 0)]) = s([(0, r_0)])$$
$$= r_0\, s([(0_M, 1_R)]).$$

$\Rightarrow M$ is $\mathbb{Z}$-divisible. The rest follows from Cor. 80. $\square$

<u>Lemma 82:</u> Let Q be an injective $\mathbb{Z}$-module and R be a ring. Then

(1) $\mathrm{Hom}_{\mathbb{Z}}(R, Q)$ is an R-module via
$$(r.\varphi)(t) := \varphi(tr), \quad \varphi \in \mathrm{Hom}_{\mathbb{Z}}(R, Q),\ r, t \in R.$$
$$\left(\begin{array}{ccc} R \times \mathrm{Hom}_{\mathbb{Z}}(R, Q) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(R, Q) \\ (r, \varphi) & \longmapsto & r.\varphi \end{array} \right)$$

(2) $\mathrm{Hom}_{\mathbb{Z}}(R, Q)$ is satisfying $(\mathrm{inj}+)_R$.

<u>Proof:</u> (1) Exercise.

(2) Given a diagramm

$$\begin{tikzcd} M_1 \arrow[r, hook, "\alpha"] \arrow[d, "\varepsilon"'] \arrow[dd, bend right=60, "\tilde{\varepsilon}"] & M_2 \arrow[dd, dashed, bend left=60, "\tilde{L}"] \\ \mathrm{Hom}_{\mathbb{Z}}(R, Q) \arrow[d] & \\ Q & \end{tikzcd}$$

of R-modules we define

$\tilde{\varepsilon} : M \longrightarrow Q$ via $\tilde{\varepsilon}(m_1) = \varepsilon(m_1)(1)$

So, by Q satisfying $(\mathrm{inj}+)_{\mathbb{Z}}$ (see Cor. 8.1),

there exists an extension $\tilde{L}$ of $\tilde{\varepsilon}$.

Now we put $L(m_2)(r) := \tilde{L}(r m_2)$.

Then
- $L(m_2) \in \mathrm{Hom}_{\mathbb{Z}}(R, Q)$ (exercise)
- L is additive: $L(m_2 + m_2')(r) = \tilde{L}(r(m_2 + m_2'))$
  $= \tilde{L}(r m_2) + \tilde{L}(r m_2') = L(m_2)(r) + L(m_2')(r)$
  $= (L(m_2) + L(m_2'))(r)$.
- L is R-homogeneous:
  $(L(s m_2))(r) = \tilde{L}(r s m_2) = L(m_2)(rs)$
  $= (s . L(m_2))(r)$
- $L \circ \alpha = \varepsilon$: $L(\alpha(m_1))(r) = \tilde{L}(r \alpha(m_1)) = \tilde{\varepsilon}(r m_1)$

$$= \varepsilon(r m_1)(1) = (r \circ \varepsilon(m_1))(1) = \varepsilon(m_1)(r).$$

i.e. $\psi(\alpha(m_1)) = \varepsilon(m_1)$. $\square$

<u>Theorem 83:</u> Let R be a ring and M be an R-module. Then there exists an R-module $\tilde{M}$ which satisfies $(\text{inj}+)_R$ and an R-monomorphism $\alpha : M \hookrightarrow \tilde{M}$.

<u>Proof:</u> Part 1 ~~(Baer)~~ (Baer '40) Consider the case $R = \mathbb{Z}$. Let $\{m_i \mid i \in I\}$ be a $\mathbb{Z}$-generating set for M.

Then we get

$$\bigoplus_I \mathbb{Q} \supseteq \bigoplus_I \mathbb{Z} \xrightarrow{\beta} M. \qquad \beta((z_i)_{i\in I}) = \sum_{i \in I} z_i m_i.$$

$$\Rightarrow \underbrace{\bigoplus_I \mathbb{Q} / \ker\beta}_{Q'} \hookleftarrow \bigoplus_I \mathbb{Z} / \ker\beta \simeq M.$$

$\bigoplus_I \mathbb{Q}$ is $\mathbb{Z}$-divisible $\Rightarrow$ Q' is $\mathbb{Z}$-divisible.

Cor 81 $\Rightarrow$ Q' satisfies $(\text{inj}+)_{\mathbb{Z}}$.

Part 2: R general (Eckmann and Schöpf 53)

By Part 1 $\exists\ \alpha \in \mathrm{Mono}_{\mathbb{Z}}(M, Q')$.
Q' $\mathbb{Z}$-inj.

Now consider the R-monomorphisms:

$$M \xhookrightarrow{\varphi} \mathrm{Hom}_{\mathbb{Z}}(R, M) \xhookrightarrow{\alpha_*} \mathrm{Hom}_{\mathbb{Z}}(R, Q)$$

$m \longmapsto \varphi(m)$

$\varphi(m)(r) := rm$

Lemma 82 $\Rightarrow$ $\mathrm{Hom}_{\mathbb{Z}}(R, Q)$ satisfies $(\mathrm{inj}+)_R$.

$\square$

end of lecture 11

<u>Theorem 84:</u> Let M be an R-module. Then are equivalent:

1° M is injective, i.e. satisfies $(\mathrm{inj})_R$

2° M satisfies $(\mathrm{inj}+)_R$.

3° $\forall\ \alpha \in \mathrm{Mono}_R(M_1, M_2)$: The map

$$\alpha^* : \mathrm{Hom}_R(M_2, M) \longrightarrow \mathrm{Hom}_R(M_1, M)$$
$$\alpha^*(f) := f \circ \alpha.$$

is surjective.

4° $\forall$ exact sequence of R-modules:

$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$ the

sequence:

$$0 \longrightarrow \mathrm{Hom}_R(M_3, M) \xrightarrow{\beta^*} \mathrm{Hom}_R(M_2, M) \xrightarrow{\alpha^*} \mathrm{Hom}_R(M_1, M) \to 0$$

is exact.

~~Proof:~~

For the proof we need the following Lemma:

<u>Lemma 85:</u> Let $M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3 \to 0$ be an exact sequence of R-modules.

Then the sequence

$$0 \to \mathrm{Hom}_R(M_3, M) \xrightarrow{\beta^*} \mathrm{Hom}_R(M_2, M) \xrightarrow{\alpha^*} \mathrm{Hom}_R(M_1, M)$$

of R-modules is exact.

<u>Proof:</u> exercise. $\square$

<u>Proof of Theorem 84:</u>

<u>$2^\circ \Leftrightarrow 3^\circ$:</u> 3° is a reformulation of $(\mathrm{inj}+)_R$ which is 2°

So we have $3^\circ \Leftrightarrow 2^\circ$

<u>$3^\circ \Leftrightarrow 4^\circ$:</u> This follows from Lemma 85.

<u>$2^\circ \Rightarrow 1^\circ$:</u> — " — Prop 63 (b).

<u>$1^\circ \Rightarrow 2^\circ$:</u> By Theorem 83 $\exists$ R-module $\tilde{M}$: $\tilde{M}$ satis-

fies $(\text{inj}+)_R$ and $\exists\, \alpha \in \text{Mono}_R(M, \tilde{M})$.

We have the exact sequence

$$0 \to M \xrightarrow{\alpha} \tilde{M} \longrightarrow \tilde{M}/\text{im}\,\alpha \longrightarrow 0$$

M is R-injective $\Rightarrow$ $\alpha(M)$ is a direct summand of $\tilde{M}$.

Exercise $\Rightarrow$ $\alpha(M)$ satisfies $(\text{inj}+)_R$

$\Rightarrow$ M satisfies $(\text{inj}+)_R$ $\Rightarrow$ 2° $\square$

At the end we given an example of ~~xxx~~ ~~xxx~~ divisible R-module which is not injective.

<u>Example 86:</u> $R := \mathbb{Z}[X]$.

$M := \mathbb{Q}(X)/(X)_{\mathbb{Z}[X]}$ is R-divisible, because $\mathbb{Q}(X)$ is.

We consider the diagram

$$\begin{tikzcd}
(2, X)_{\mathbb{Z}[X]} \arrow[r, hook] \arrow[d, "\varepsilon"'] & R \arrow[dl, dashed, "G"] \\
M & \text{Assume } \exists\, V
\end{tikzcd}$$

~~$X\nu(1) = [0]_{\mathbb{Z}[X]}$.~~

<u>Example 86:</u> Consider the $R = \mathbb{Z}[X]$ module $M := \mathbb{Q}(X) / (X)_{\mathbb{Z}[X]}$ and the map

$$\begin{tikzcd} \mathfrak{U} = (2, X)_{\mathbb{Z}[X]} \arrow[r, hook] \arrow[d, "\varepsilon"'] & R \arrow[dl, dashed, "\text{Assume } \exists \nu"] \\ M & \end{tikzcd}$$

$\varepsilon(2P_1 + XP_2) := [P_1]_{(X)}$

ε is well-defined: $2P_1 + XP_2 = 2Q_1 + XQ_2$

$\Rightarrow \quad X \mid P_1 - Q_1 \quad \Rightarrow \quad [P_1]_{(X)} = [Q_1]_{(X)}$.

Assume $\exists\, \nu : R \to M$ an R-morphism: $\nu|_{\mathfrak{U}} = \varepsilon$.

Then for $\nu(1) = [a]_{(X)}$ we have

$[2a]_{(X)} = [1]_{(X)}$ and $[Xa]_{(X)} = [0]_{(X)}$

$\Rightarrow \quad a \in \mathbb{Z}[X]$ and $X \mid 2a - 1$

$\Rightarrow \quad 2a(0) = 1 \quad \lightning$.

Further reading / studying:
- injective hull
- essential extension.

I.4. Tensor product

We start with a definition.

Def 87: Let R be a ring and $M_1, \dots, M_n, U$ be R-modules. A map $b: M_1 \times \dots \times M_n \to U$ is called <u>R-n-linear</u> (R-multilinear, if $n=2$: R-bilinear) if for every $i_0 \in \{1, \dots, n\}$ $\forall m_1 \in M_1, \dots, \hat{m}_{i_0} \in M_{i_0}, \dots, m_n \in M_n$

the map $x \in M_{i_0} \longmapsto b(m_1, \dots, \hat{m}_{i_0}, \dots, m_n)$

is an R-morphism, i.e. $\in \operatorname{Hom}_R(M_{i_0}, U)$.

If $U = R$, then we say that b is a <u>multi-linear form</u>.

Example 88:

1) $\langle , \rangle : \mathbb{R}^n \times \mathbb{R}^n \longrightarrow \mathbb{R}$, $\langle \underline{v}, \underline{w} \rangle := \underline{v} \cdot \underline{w}$

dot-product ~~(or scalar~~

Under $\mathbb{R}^n \simeq \mathbb{R}^{n \times 1}$: $\langle \underline{v}, \underline{w} \rangle = {}^t\underline{v}\, \underline{w}$.

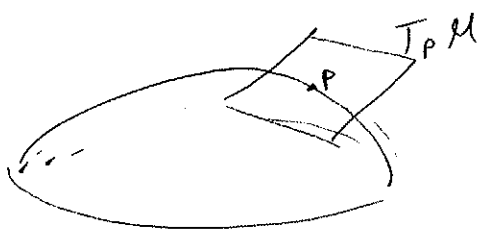
2) More general, $A \in \mathbb{R}^{n \times n}$, $\langle , \rangle_A : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$

$\langle \underline{v}, \underline{w} \rangle_A := {}^t\underline{v}\, A\, \underline{w}$.

All $\mathbb{R}$-bilinear forms on $\mathbb{R}^n$ are of the form $\langle , \rangle_A$, because we only need to know the Gram matrix w.r.t. the standard basis:

$$A = \left(b(e_i, e_j)\right)_{(i,j)\in\{1,\dots,n\}^2} =: \mathrm{Gram}_{\{e_1,\dots,e_n\}}(b)$$

3) Let M be a ~~ds~~ ~~smooth~~ differentiable manifold (means C^∞ transition maps), $P \in M$ and T_pM the tangent space of M at P.



$$D_p : T_pM \times C^\infty(M) \longrightarrow \mathbb{R}$$

$$D_p(v, f) := D_v(f)(p) = \left.\frac{\partial\, f\circ c(t)}{\partial t}\right|_{t=0}$$

c a curve through x at 0 with $c'(0) = v$.

is a bilinear form.

4) The map $f : \mathbb{R}\times\mathbb{R} \to \mathbb{R}$ $\quad f(r_1, r_2) := r_1 + r_2$

is NOT bilinear: $f(-1,1) + f(1,1) = 2 \neq 1 = f(0,1)$.

5) Bilinear forms are important to define classical groups:

<u>Example:</u> Take $A \in GL_n(\mathbb{R})$ s.t. ${}^tA = \pm A$.

$$U(A) := \{ B \in \mathbb{R}^{n\times n} \mid \langle B\underline{v}, B\underline{w}\rangle_A = \langle \underline{v}, \underline{w}\rangle_A \ \forall \underline{v}, \underline{w} \in \mathbb{R}^n \}$$

We get:

the symplectic group in dimension $2n$:

$$Sp_{2n}(\mathbb{R}) := U\left(\underbrace{\begin{pmatrix} & & & 1 \\ & & -1 & \\ & \iddots & & \\ -1 & & & \end{pmatrix}}_{2n}\right),$$

the ~~orthogonal~~ orthogonal group in dimension n:

$$O_n(\mathbb{R}) := U\left(\underbrace{\begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}}_{n}\right).$$

The idea of "tensor product" is to interprete bilinear maps as homomorphisms.

<u>Def. 89:</u> Let M, N, U be R-modules.

$$\mathrm{Bil}_R(M,N,U) := \{ b : M \times N \to U \mid b \ R\text{-bilinear} \}$$

An R-module T together with a bilinear map $t \in \mathrm{Bil}_R(M,N,T)$ is called a tensor product of M with N over R if

$\forall$ R-modules U: the map $\mathrm{Hom}_R(T,U) \to \mathrm{Bil}_R(M,N,U)$, $f \mapsto f \circ t$

is a bijection

<u>Remark 90:</u> Def. 89 can be illustrated as follows:

$$\begin{tikzcd} M \times N \arrow[r, "t"] \arrow[rr, bend left, "b"] & T \arrow[r, dotted, "\exists f \ R\text{-morph.}"'] & U \end{tikzcd}$$

<u>Proposition 91:</u> (a) For every pair of R-modules M, N there exists a tensor product.

(b) The tensor product is unique upto R-isomorphism.

<u>Proof:</u> (a) We consider a bijection $M \times N \xrightarrow{\varphi} S$ to a set S and we write $s_{m,n}$ for $\varphi(m,n)$.

The ~~formal~~ outer direct sum $\bigoplus_{s \in S} \mathbb{Z} s =: F$ (free $\mathbb{Z}$-module with basis S) has a submodule

$$F_0 := \langle \{ s_{\lambda m, n} - s_{m, \lambda n} \mid m \in M, n \in N, \lambda \in R \} \rangle_{\mathbb{Z}}$$

Put $T := F / F_0$ and take $t : M \times N \longrightarrow T$

$$t(m,n) := [s_{m,n}]_{F_0}.$$

<u>(a1):</u> F is an R-module via

$$\lambda(z_1 s_{m_1,n_1} + \dots + z_\ell s_{m_\ell,n_\ell}) := z_1 s_{\lambda m_1, n_1} + \dots + z_\ell s_{\lambda m_\ell, n_\ell}$$

<u>Proof:</u> (b) Let (T_1, t_1) and (T_2, t_2) be tensor products of M and N.

(T_1, t_1) is a tensor product and $t_2 \in \mathrm{Bil}_R(M, N, T_2)$

$$\Rightarrow \exists! f_1 \in \mathrm{Hom}_R(T_1, T_2) : f_1 \circ t_1 = t_2$$

(T_2, t_2) is a ...

$$\Rightarrow \exists! f_2 \in \mathrm{Hom}_R(T_2, T_1) : f_2 \circ t_2 = t_1$$

$\Rightarrow \quad f_1 \circ f_2 \circ t_2 = t_2$ and $f_2 \circ f_1 \circ t_1 = t_1$.

We also have $id_{T_2} \circ t_2 = t_2$ and $id_{T_1} \circ t_1 = t_1$.

Def of tensor product (~~uniqueness~~ injectivity of

$\mathrm{Hom}_R(T, U) \longrightarrow \mathrm{Bil}_R(M, N, U)$)

$\Rightarrow f_1 \circ f_2 = id_{T_2}$ and $f_2 \circ f_1 = id_{T_1}$.

end of lecture 12.

(a) We consider a bijection $M \times N \xrightarrow{\varphi} S$ to a set S and we write $s_{m,n}$ for $\varphi(m,n)$.

The direct sum $\bigoplus_{s \in S} R s =: F$

(free R-module with basis S) has a submodule

$$F_0 := \Big\langle \{ \lambda s_{m,n} - s_{\lambda m, n},\ \lambda s_{m,n} - s_{m, \lambda n},\ s_{m_1+m_2, n} - s_{m_1, n} - s_{m_2, n},\ s_{m, n_1+n_2} - s_{m, n_1} - s_{m, n_2} \mid \lambda \in R,\ m, m_1, m_2 \in M,\ n, n_1, n_2 \in N \} \Big\rangle_R$$

Put $T := F/F_0$ and take $t : M \times N \longrightarrow T$

$$t(m,n) := [s_{m,n}]_{F_0}.$$

<u>Claim:</u> (T, t) is a tensor product of M and N.

To show: $\forall U$ R-module:

$$\mathrm{Hom}_R(T, U) \xrightarrow{t^*} \mathrm{Bil}_R(M \times N, U)$$
$$f \longmapsto f \circ t.$$

<u>surjectivity:</u> Given $b \in \mathrm{Bil}_R(M \times N, U)$, define

$f_b : T \longrightarrow U$ via $f_b\left(\left[\sum_{(m,n)} \lambda_{m,n} s_{m,n}\right]\right) := \underbrace{\sum_{(m,n)} \lambda_{m,n}\, b(m,n)}_{(*)}$

f_b is well-defined, because for the ~~elements in F_0~~ generators of F_0

$(*)$ is zero.

$$\lambda b(m,n) - b(\lambda m, n) \underset{\substack{\uparrow \\ b \text{ is bilinear}}}{=} \lambda b(m,n) - \lambda b(m,n) = 0_U$$

etc.

Further $f_b \circ t(m,n) = f_b([s_{m,n}]) = b(m,n)$.

<u>injectivity:</u> t^* is an R-morphism, so we just compute the kernel.

$t^*(f) = 0$ (zero bilinear map)

$\Rightarrow f([s_{m,n}]_{F_0}) = 0_U \quad \forall (m,n) \in M \times N$

$\langle [s_{m,n}]_{F_0} \rangle_R = T \Rightarrow f$ is the zero-map.

$\square$

<u>Notation 92:</u> We write $(M \otimes_R N, \otimes_R)$ for the tensor product (T, t) constructed in Proposition 91(a). We write $m \otimes_R n$ for $t(m,n)$.

Example 93:

1) $\mathbb{R}[X] \otimes_{\mathbb{R}} \mathbb{R}[Y] \simeq \mathbb{R}[X,Y]$

Proof: The map $\varphi : \mathbb{R}[X] \times \mathbb{R}[Y] \to \mathbb{R}[X,Y]$
$\varphi(P,Q) := P \cdot Q$

is $\mathbb{R}$-bilinear.

$$\begin{tikzcd} \mathbb{R}[X] \times \mathbb{R}[Y] \arrow[r, "\varphi"] \arrow[d, "\otimes_{\mathbb{R}}"'] \arrow[dr, phantom, "\circlearrowleft"] & \mathbb{R}[X,Y] \\ \mathbb{R}[X] \otimes_{\mathbb{R}} \mathbb{R}[Y] \arrow[ur, dotted, "\exists f_\varphi \in \mathrm{Hom}_{\mathbb{R}}(\mathbb{R}[X] \otimes_{\mathbb{R}} \mathbb{R}[Y], \mathbb{R}[X,Y])"'] & \end{tikzcd}$$

f_φ is surjective because $\forall i,j \in \mathbb{N}_0$:
$X^i Y^j \in \operatorname{im} \varphi \subseteq \operatorname{im} f_\varphi$.

For proving injectivity we construct the candidate for the inverse.

$g : \mathbb{R}[X,Y] \longrightarrow \mathbb{R}[X] \otimes_{\mathbb{R}} \mathbb{R}[Y]$

$$g\Big(\sum_{i,j \geq 0} \lambda_{ij} X^i Y^j\Big) := \sum_{i,j \geq 0} \lambda_{ij} (X^i \otimes_{\mathbb{R}} Y^j)$$

Then $g(f_\varphi(\sum_{i,j \geq 0} \lambda_{i,j} (X^i \otimes_{\mathbb{R}} Y^j))) = g\Big(\sum_{i,j \geq 0} \lambda_{ij} f_\varphi(X^i \otimes_{\mathbb{R}} Y^j)\Big)$

$= g\Big(\sum_{i,j \geq 0} \lambda_{ij} \varphi(X^i, Y^j)\Big) = g\Big(\sum_{i,j \geq 0} \lambda_{ij} X^i Y^j\Big)$

$= \sum_{i,j \geq 0} \lambda_{ij} (X^i \otimes_{\mathbb{R}} Y^j)$. So $g \circ f_\varphi = id_{\mathbb{R}[X] \otimes_{\mathbb{R}} \mathbb{R}[Y]}$ $\Rightarrow f_\varphi$ is injective.

2) $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} = 0$ the zero module.

<u>Proof:</u> Write $M := \mathbb{Q} \otimes_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z})$.

Then $q \otimes_{\mathbb{Z}} [z]_2 = 2\frac{q}{2} \otimes_{\mathbb{Z}} [z]_2 = \frac{q}{2} \otimes_{\mathbb{Z}} [2z]_2$

$= \frac{q}{2} \otimes_{\mathbb{Z}} [0]_2 = 0_M$.

The elements $q \otimes_{\mathbb{Z}} [z]_2$, $q \in \mathbb{Q}$, $z \in \mathbb{Z}$ generate M. $\Rightarrow M = \{0_M\}$ $\square$

3) $\mathbb{Z}/3\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} = \{0\}$

<u>Proof:</u> $[z_1]_3 \in \mathbb{Z}/3\mathbb{Z}$, $[z_2]_2 \in \mathbb{Z}/2\mathbb{Z}$.

$\Rightarrow z_1 = 2q + r$ for some $q \in \mathbb{Z}$ and $r \in \{0,1\}$

$\Rightarrow [z_1]_3 \otimes_{\mathbb{Z}} [z_2]_2 = [r]_3 \otimes_{\mathbb{Z}} [z_2]_2 = [0]_3 \otimes_{\mathbb{Z}} [z_2]_2$

$= 0$. $\square$

4) $m, n \in \mathbb{N}$. Then

$\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/\gcd(m,n)\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/\gcd(m,n)\mathbb{Z}$.

Exercise!

5) $\mathfrak{a} = (2, X)_{\mathbb{Z}[X]}$, $\mathbb{Q}(X) = Q(\mathbb{Z}[X])$ field of fractions.

Then $\mathfrak{a} \otimes_{\mathbb{Z}[X]} \mathbb{Q}(X)$

$\simeq \mathbb{Q}(X)$.

This is a general fact:

R an integral domain with $F := Q(R)$.

Then $J \otimes_R F \simeq F$ for all $F \geq_R J \gneqq \{0\}$

$$i \otimes_R \frac{a}{b} \longmapsto \frac{ia}{b}$$

The map is well-defined because $(i, q) \longmapsto iq$ is R-bilinear and the map is an isomorphism, because for $i_0 \in J \setminus \{0\}$ fixed it has the inverse $\frac{a}{b} \longmapsto i_0 \otimes_R \frac{a}{i_0 b}$.

(Check!)

<u>Proposition 94:</u> Let M, N, P be R-modules.

Then:

(1) $M \otimes_R N \simeq N \otimes_R M$

(2) $M \otimes_R (N \otimes_R P) \simeq (M \otimes_R N) \otimes_R P$

(3) $M \otimes_R (N \oplus P) \simeq (M \otimes_R N) \oplus (M \otimes_R P)$

(4) $M \otimes_R R \simeq M$

(5) If M, N are vectorspaces over a field K, then

$$\dim_K (M \otimes_R N) = (\dim_R M) \cdot (\dim_R N)$$

~~(0/0 = 0)~~

if M and N are finite dimensional.

(6) $\mathrm{Hom}_R(M, \mathrm{Hom}_R(N,P)) \simeq \mathrm{Hom}_R(M \otimes_R N, P)$

<u>Proof:</u> (1) $(m,n) \xmapsto{b} m \otimes_R n$ is R-bilinear.

$$b(m_1+m_2, n) = n \otimes_R (m_1+m_2)$$
$$= n \otimes_R m_1 + n \otimes_R m_2$$
$$= b(m_1, n) + b(m_2, n)$$

$$b(m, n_1+n_2) = b(m,n_1) + b(m,n_2)$$

$$b(\lambda m, n) = n \otimes (\lambda m) = \lambda (n \otimes m)$$
$$= \lambda\, b(m,n)$$
$$b(m, \lambda n) = \lambda\, b(m,n)$$

Universal property of $\otimes_R$: $\exists\, f_b : M \otimes_R N \longrightarrow N \otimes_R M$
R-linear

such that $f_b(m \otimes_R n) = b(m,n) \;\forall_{(m,n) \in M \times N}$
$$\overset{\shortparallel}{n \otimes_R m}.$$

Analogously $\exists\, g \in \mathrm{Hom}_R(N \otimes_R M, M \otimes_R N)$:

$$g(n \otimes_R m) = m \otimes_R n.$$

$\Rightarrow$ $g \circ f(m \otimes n) = g(n \otimes m) = m \otimes n$.

and $f \circ g(n \otimes_R m) = n \otimes_R m$.

$\{m \otimes_R n \mid m \in M, n \in N\}$ <u>generates</u> $M \otimes_R N$

$\{n \otimes_R m \mid \cdots \}$ — " — $N \otimes_R M$.

$\Rightarrow f \circ g = id_{N \otimes M}$ and $g \circ f = id_{M \otimes_R N}$

(2) Exercise!

(3) $M \otimes (N \oplus P) \xrightarrow{b} M \otimes_R N$ and $M \times (N \oplus P) \xrightarrow{c} M \otimes_R P$

$(m \otimes (n+p)) \longmapsto m \otimes_R n$ $\qquad (m, n+p) \longmapsto m \otimes p$

are R-bilinear.

$\Rightarrow \exists\ M \otimes (N+P) \xrightarrow{\varphi} M \otimes_R N$ and

$M \otimes (N+P) \xrightarrow{\psi} M \otimes_R P$

R-linear s.t. $\varphi \circ \otimes_R = b$ and $\psi \circ \otimes_R = c$.

Define $F : M \otimes (N+P) \longrightarrow M \otimes_R N \oplus M \otimes_R P$

via $\cancel{F(m \otimes p)}$ $F(v) := \varphi(v) + \psi(v)$.

$\forall v \in M \otimes (N \oplus P)$.

Then $F \in Epi_R(M \otimes (N \oplus P), M \otimes N \oplus M \otimes P)$

Exercise: Show that F is injective.

(4) $(m, r) \in M \times R \longmapsto r \cdot m \in M$ is

R-bilinear.

$\Rightarrow \exists\ f : M \otimes_R R \longrightarrow M$ R-linear:

$f(m \otimes_R r) = rm.\ \forall r \in R\ \forall m \in M.$

f has an inverse, namely:

$m \in M \longmapsto m \otimes_R 1.$

$$m \longmapsto m \otimes_R 1 \longmapsto 1 \cdot m = m$$

$$m \otimes_R r \longmapsto rm \longmapsto (rm) \otimes_R 1 = m \otimes_R (r \cdot 1)$$

(5) $M \simeq R^m$, $N \simeq R^n = \underbrace{R \oplus R \oplus \cdots \oplus R}_{n}$

$$\Rightarrow M \otimes_R N \simeq M \otimes_R (R^n)$$

$$\simeq M \otimes_R \left(\bigoplus_{i=1}^{n} R\right) \underset{(3)}{\simeq} \bigoplus_{i=1}^{n} (M \otimes_R R)$$

$$\simeq \bigoplus_{i=1}^{n} M$$

$$\Rightarrow \dim_R (M \otimes_R N) = n \dim_R M$$

(6) $\mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P))$

$$\simeq \overset{\mathrm{Bil}}{\cancel{\mathrm{Hom}}}_R(M, N, P) \simeq \mathrm{Hom}_R(M \otimes_R N, P).$$

$\square$

The first application of the tensor product is the uniqueness of the cardinality of a basis of a free R-module.

<u>Lemma 95:</u> Let $\mathfrak{a} \leq_R R$ and M be an R-module. Then

$$M \otimes_R R/\mathfrak{a} \simeq M/\mathfrak{a}M.$$

$$\left(\mathfrak{a}M = \langle \{ am \mid a \in \mathfrak{a}, m \in N \} \rangle_R \right)$$

<u>Proof:</u> We have the following two maps:

$$M \otimes_R R/\mathfrak{a} \xrightarrow{\psi} M/\mathfrak{a}M$$

given by $m \otimes_R [r]_{\mathfrak{a}} \longmapsto [rm]_{\mathfrak{a}M}$

on ~~gen~~ elementary tensors.

$$\begin{aligned} M &\xrightarrow{\varphi} M \otimes_R R/\mathfrak{a} \\ m &\longmapsto m \otimes_R [1]_{\mathfrak{a}} \end{aligned}$$

$\ker \varphi \supseteq \mathfrak{a}M$, because for $\sum_{i=1}^{n} a_i m_i \in \mathfrak{a}M$

we have $\varphi\left(\sum_{i=1}^{n} a_i m_i\right) = \left(\sum_{i=1}^{m} a_i m_i\right) \otimes_R [1]$

$$= \sum_{i=1}^{n} (a_i m_i \otimes_R [1]) = \sum_{i=1}^{n} \underbrace{(m_i \otimes_R [a_i])}_{m_i \otimes_R [0]_{\mathfrak{a}}} = \sum_{i=1}^{n} 0_{M \otimes_R R/\mathfrak{a}}$$

$$= 0.$$

$$\Rightarrow \exists\ \bar{\varphi} : M/\mathfrak{a}M \longrightarrow M \otimes_R R/\mathfrak{a}$$

such that $\bar{\varphi}([m]_{\mathfrak{a}M}) = \varphi(m)$

$= m \otimes_R [1]_{\mathfrak{a}}$

· On generators we have:

$(\psi \circ \bar{\varphi})([m]_{\mathfrak{a}M}) = \psi(m \otimes_R [1]_{\mathfrak{a}})$

$= [m]_{\mathfrak{a}M}$ and $(\bar{\varphi} \circ \psi)(m \otimes_R [r]_{\mathfrak{a}})$

$$= \bar{\varphi}([rm]_{\mathcal{M}M}) = rm \otimes_R [1]_{\mathcal{M}} = m \otimes_R (r[1])_{\mathcal{M}}$$

$$= m \otimes_R [r]_{\mathcal{M}}. \qquad \square$$

<u>end lecture 13</u>

<u>Theorem 96:</u> Let M be a free R-module and let B and C be two R-basis of M. Then $|B| = |C|$.

<u>Proof:</u> $B = \{v_i \mid i \in I\}$

$C = \{u_j \mid j \in J\}$

$$\Rightarrow \quad M \simeq \bigoplus_{i \in I} R \quad \text{and} \quad M \simeq \bigoplus_{j \in J} R$$

Take a maximal ideal $\mathfrak{m}$ of R.

$$\Rightarrow \bigoplus_{i \in I} R/\mathfrak{m} \simeq \bigoplus_{i \in I} (R \otimes_R R/\mathfrak{m}) \simeq \left(\bigoplus_{i \in I} R\right) \otimes_R R/\mathfrak{m}$$

$$\underset{\text{Lemma 96}}{\simeq} M/\mathfrak{m}M \simeq \bigoplus_{j \in J} R/\mathfrak{m}$$

as R modules, thus as $R/\mathfrak{m}$ - ~~vect~~ vector spaces.

$$\Rightarrow \quad |I| = |J| \qquad \square$$

<u>Def 97:</u> Let M be a fgr R-module and B be a basis of M. We call $|B|$ the <u>rank of M</u> (R-rank) and we write $\mathrm{rk}_R(M)$.

<u>Example 98:</u> Tensor product can be used for extension of scalars: $R \overset{\mathrm{ind}}{\subseteq} S$ a ring extension (we usually assume $1_R = 1_S$)

Let M be an R-module.

$$\Rightarrow M \simeq M \otimes_R R \xrightarrow[\mathrm{id}_M \otimes \mathrm{ind}_{R \subseteq S}]{} M \otimes_R S$$

The map $\mathrm{id}_M \otimes \mathrm{ind}$ does not need to be injective: $M := \mathbb{Q}/\mathbb{Z}$. $R = \mathbb{Z} \subseteq S = \mathbb{Q}$

$$\mathbb{Q}/\mathbb{Z} \simeq \mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z} \longrightarrow \mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} = \{0\}$$

$$\left(\left[\frac{a}{b}\right]_{\mathbb{Z}} \otimes_{\mathbb{Z}} \frac{c}{d} = \left[\frac{a}{b}\right]_{\mathbb{Z}} \otimes_{\mathbb{Z}} \frac{bc}{bd} = \left[\frac{ab}{b}\right]_{\mathbb{Z}} \otimes_{\mathbb{Z}} \frac{c}{bd} = 0 . \right)$$

Normally it works well:

$$\mathbb{R}^2 \otimes_{\mathbb{R}} \mathbb{C} \simeq (\mathbb{R} \oplus \mathbb{R}) \otimes_{\mathbb{R}} \mathbb{C}$$

$$\simeq (\mathbb{R} \otimes_{\mathbb{R}} \mathbb{C}) \oplus (\mathbb{R} \otimes_{\mathbb{R}} \mathbb{C}) \simeq \mathbb{C} \oplus \mathbb{C} \simeq \mathbb{C}^2.$$

as $\mathbb{C}$-vector spaces.

So we need to study those modules which, when tensored with them, preserve ~~injective morphisms~~ injectivity.

<u>Def 99:</u> Let M be an R-module. M is called <u>flat</u> (<u>R-flat</u>) if

$\forall_{N,P}$ R-module $\forall \alpha \in \mathrm{Mono}(N,P)$:

$\mathrm{id}_M \otimes \alpha : M \otimes_R N \longrightarrow M \otimes_R P$ is injective.

<u>Example 101:</u> (a) $\mathbb{Q}/\mathbb{Z}$ is not a flat $\mathbb{Z}$-module.

(b) Every free module is flat.

$$\begin{tikzcd}
M \otimes_R N \arrow[r] \arrow[d, phantom, "\cong"] & M \otimes_R P \arrow[d, phantom, "\cong"] \\
\bigoplus_I (R \otimes_R N) \arrow[r, phantom, "\circlearrowleft"] \arrow[d, phantom, "\cong"] & \bigoplus_I (R \otimes_R P) \arrow[d, phantom, "\cong"] \\
\bigoplus_I N \arrow[r, hook, "\bigoplus_I \alpha"] & \bigoplus_I P
\end{tikzcd}$$

$\Rightarrow$ $id_M \otimes_R \alpha$ is injective.

(c) $\mathbb{Q}$ is a flat $\mathbb{Z}$-module.

Assume $\exists$ $\alpha \in \mathrm{Mono}_R(N, P)$:

$\mathbb{Q} \otimes_R N \Longrightarrow \mathbb{Q} \otimes_R P$ is not inj.

$\Rightarrow$ $\exists$ $q_1, \dots, q_\ell \in \mathbb{Q}$: For $M := \langle q_1, \dots, q_\ell \rangle_{\mathbb{Z}}$

$M \otimes_R N \longrightarrow M \otimes_R P$ is not injective.

(Look at Prop 91 (a). For an element in the kernel of $id_{\mathbb{Q}} \otimes \alpha$ you only need finitely many relations!)

M is torsion free and $\mathbb{Z}$ is a PID $\Rightarrow$ M is free $\Rightarrow$ M is flat.

$\Rightarrow$ $id_M \otimes \alpha$ is injective $\lightning$.

<u>Prop. 102:</u> Let M be an R-module.

(1) If M is flat then M is torsion-free.

(2) Let R be a PID and M be torsion free. Then M is flat.

<u>Proof:</u> (2) As in Example 101(c) using Cor. 77.

(1) Suppose M has torsion, i.e. $\exists\, m_0 \in M \setminus \{0\}$ $\exists\, r_0 \in R \setminus \{0\}$ r_0 is not a zerodivisor and $r_0 m_0 = 0$, then for $\alpha : R \hookrightarrow R$, $\alpha(r) := r_0 r$, we have

$$id_M \otimes_R \alpha : \underset{\substack{\cong \\ M}}{M \otimes_R R} \longrightarrow \underset{\substack{\cong \\ M}}{M \otimes_R R}$$

is not injective, because

$$\alpha(m_0 \otimes_R 1) = m_0 \otimes_R r_0 = r_0 m_0 \otimes_R 1 = 0_M \otimes_R 1$$

$\square$

<u>Example (D):</u> $R = \mathbb{Z}[X]$

$M := (X, Z)_R$ is torsion free but not flat.

Consider $\alpha : (2, X) \hookrightarrow \mathbb{Z}[X]$.

$$\mathrm{id}_M \otimes \alpha : M \otimes_{\mathbb{Z}[X]} (2, X) \longrightarrow M \otimes_{\mathbb{Z}[X]} \mathbb{Z}[X]$$

$$\cup$$

$$c := X \otimes 2 - 2 \otimes X \longmapsto 0.$$

To show: c is not zero in $M \otimes_R (2, X)_R$.

Consider the map

$$M \otimes_R M \xrightarrow{\varphi} \mathbb{Z}[Y, Z] / \mathfrak{a}$$

$$\mathfrak{a} = (8, 4Z, 4Y, 2Y^2, 2Z^2, 2YZ, Y^3, Y^2Z, YZ^2, Z^3)$$

$$\varphi(P \otimes Q) := P(Y)\, Q(Z).$$

- φ is well-defined
- $\varphi((X \otimes 2) - (2 \otimes X)) = 2Y - 2Z.$

Assume $\varphi(c) = [0]_{\mathfrak{a}} \Rightarrow 2Y - 2Z \equiv P_1 8 + P_2 4Z + P_3 4Y$

mod (Y^2, Z^2, YZ). with

$\deg P_2, \deg P_3 \leq 0$ and $\deg P_1 \leq 1$.

$\Rightarrow$ ~~The coefficients~~

$\Rightarrow$ The coefficients on the RHS are divisible by 4. $\lightning$.

<u>Prop 104:</u> Projective modules are flat.

<u>Proof:</u> Exercise. $\square$

<u>Lemma 105:</u> Let $0 \to M_1 \to M_2 \to M_3 \to 0$ be a sequence of R-modules.

(1) If a.e.:

1° $0 \to M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3$ is exact

2° $\forall U$ R-modules

$$0 \to \mathrm{Hom}_R(U, M_1) \xrightarrow{\alpha_*} \mathrm{Hom}_R(U, M_2) \xrightarrow{\beta_*} \mathrm{Hom}_R(U, M_3)$$

is exact

(2) If a.e.:

1° $M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3 \longrightarrow 0$ is exact

2° $\forall U$ - R-module

$$0 \to \mathrm{Hom}(M_3, U) \xrightarrow{\beta^*} \mathrm{Hom}(M_2, U) \xrightarrow{\alpha^*} \mathrm{Hom}(M_1, U)$$

is exact.

<u>Proof:</u> (1) $1^\circ \Rightarrow 2^\circ$ is already known.

<u>$2^\circ \Rightarrow 1^\circ$:</u> α injective: Take $U = \ker(\alpha)$, $f := \mathrm{incl}_{U \subseteq M_1}$

$$\alpha_*(f) = \alpha \circ f = 0 \underset{2^\circ}{\Rightarrow} f = 0 \Rightarrow U = \{0\}.$$

- $\beta\alpha = 0$: $U = M_1$ $f = \mathrm{id}_{M_1}$

$$\Rightarrow 0 = \beta_*(\alpha_*(f)) = \beta \circ \alpha \circ f = \beta \circ \alpha.$$

- $\mathrm{im}\,\alpha \supseteq \ker \beta$: Take $v \in \ker(\beta)$. $U := Rv$.

$$\Rightarrow \mathrm{incl}_{Rv \subseteq M_2} \in \ker(\beta_*) = \mathrm{im}(\alpha_*)$$

$$\Rightarrow \exists f \in \mathrm{Hom}_R(U, M_1): \alpha \circ f = \mathrm{incl}_{Rv \subseteq M_2}$$

$$\Rightarrow \alpha(f(v)) = v \Rightarrow v \in \mathrm{im}\,\alpha.$$

(2) Exercise! $\square$

<u>Prop. 10:</u> Let M be an R-module. T.a.e.:

1° M is flat

2° $\forall\ 0 \to M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3 \to 0$ exact:

$$0 \to M_1 \otimes M \xrightarrow{\alpha \otimes id} M_2 \otimes M \xrightarrow{\beta \otimes id} M_3 \otimes M \to 0$$

is exact.

<u>End lecture 14</u>

<u>Proof:</u> $2^\circ \Rightarrow 1^\circ$ by the definition of flatness.

$1^\circ \Rightarrow 2^\circ$: From the exactness of $M_1 \to M_2 \to M_3 \to 0$

follows the exactness of

$$0 \to \mathrm{Hom}_R(M_3, U) \to \mathrm{Hom}_R(M_2, U) \to \mathrm{Hom}_R(M_1, U) \quad \forall U$$

So take for U: $U = \mathrm{Hom}_R(M, V)$

for an R-module V.

$$\Rightarrow 0 \to \mathrm{Hom}_R(M_3 \otimes_R M, V) \to \mathrm{Hom}_R(M_2 \otimes_R M, V)$$

$$\to \mathrm{Hom}_R(M_1 \otimes_R M, V) \text{ is exact.}$$

V arbitrary + Lemma 105

$$\Longrightarrow \quad M_1 \otimes M \to M_2 \otimes M \to M_3 \otimes M \to 0$$

is exact.

The injectivity of $\alpha \otimes id$ is implied by the flatness of M. $\square$

II Local - global principle.

II.1. Localization

Given a manifold M it is one approach to study M in studying its local behaviour.

For example in looking at the functions defined around a point.

There is a "sheaf" defined on M.

$U \mapsto \Gamma(M,U) := \mathcal{C}^\infty(U)$, $U \subseteq M$ open.

Around a point $x \in M$ we get the "stalk" as follows.

$\{(f,U) \mid U \subseteq M \text{ open}, x \in U, f \in \Gamma(M,U)\}$

$(f,U) \sim (g,V) \underset{\text{def.}}{\Longleftrightarrow} f|_{U\cap V} = g|_{U\cap V}$.

$\Gamma(M)_x := \{ [f,U]_\sim \mid \cancel{(f,U)} \; x \in U \subseteq M \text{ open}, f \in \Gamma(M,U)\}$

If we replace M by a complex manifold and consider the sheaf $\Gamma(M,U) := \mathcal{C}^{an}(U)$, then

$\Gamma(M)_x \hat{=}$ "Taylor series around x (after fixing a chart $\varphi : U \subseteq M \longrightarrow \mathbb{C}^n$ around x".

The algebraic analogue of a ~~Rea~~ real or complex manifold is an algebraic variety. Let k be a field

$$V \subseteq k^m \quad , \quad P_1, \dots, P_n \in k[X_1, \dots X_m]$$

$$V = \{(x_1, \dots, x_m) \in k^m \mid P_1(x_1, \dots, x_m) = \dots = P_n(x_1, \dots, x_m) = 0\}$$

$$=: V(P_1, \dots, P_n).$$

regular functions on V:

$$\mathcal{O}_V(V) := k[X_1, \dots, X_m] / I(V) \quad .$$

coordinate ring of V.

$I(V) := \{P \in k[X_1, \dots, X_m] \mid P(V) = \{0\}\}$ vanishing ideal.

Now take $U \subseteq V$ open (in V)

(The open sets of V are of the form $V \setminus W$
W an algebraic ~~set~~ subset of V, i.e. $W = V(Q_1, \dots, Q_e)$
for some ~~po~~ $Q_1, \dots, Q_e \in k[X_1, \dots, X_m]$)

"Zariski - topology". Now let k be infinite

$$\mathcal{O}_V(U) = \{ f : U \to k \mid \exists (U_i)_{i \in I} \text{ an open covering of } U: \text{ s.t. } f|_{U_i} = \frac{g_i}{h_i} \text{ for some } g_i, h_i \in \mathcal{O}_V(V). \}$$

How can we compute $\mathcal{O}_{V,x}$ ~~[illegible]~~ for $x \in V$?

<u>Def 1.07:</u> Let $S \neq \emptyset$ be a multiplicatively closed subset of a ring R. ($\forall x,y \in S: xy \in S$ and $1 \in S$)
Let M be an R-module.
The localization of M at S is the following module: $M_S := \{(m,s) \mid m \in M, s \in S\}/\sim$ via

$$(m_1,s_1) \sim (m_2,s_2) \iff \exists t \in S: t(s_2 m_1 - s_1 m_2) = 0$$

We denote the class $[(m,s)]_\sim$ by $\frac{m}{s}$.

<u>Example 1.08:</u>

(1) R_S is a ring and we have the map

$$R \to R_S, \quad r \longmapsto \frac{r}{1}.$$

This map is injective $\iff$ $0 \notin S$ and S does not contain a zero divisor.

<u>Proof:</u> "$\Rightarrow$" Assume $\exists s \in S\ \exists r \in R \setminus \{0\}: sr = 0$.

$\Rightarrow (r,1) \sim (0,1)$ $\quad (s(r \cdot 1 - 0 \cdot 1) = 0)$

$\Rightarrow \frac{r}{1} = \frac{0}{1} = 0_{R_S}$. $\lightning$ injectivity.

"$\Leftarrow$" Take $r \in R$ s.t. $\frac{r}{1} = \frac{0}{1}$.

$\Rightarrow \exists s \in S: s(r \cdot 1 - 0 \cdot 1) = 0 \Rightarrow \exists s \in S: s \cdot r = 0 \overset{s \neq 0 \text{ and not a zero divisor}}{\Longrightarrow} r = 0$. $\square$

(2) $S := \mathbb{Z} \setminus \{0\}$, $R = \mathbb{Z}$.

$\Rightarrow R_S \simeq \mathbb{Q}$. via $[(r,s)]_\sim \overset{\varphi}{\longmapsto} \frac{r}{s} \in \mathbb{Q}$.

surjective ✓, ring homomorphism ✓

$$\left([(r_1,s_1)]_\sim + [(r_2,s_2)]_\sim := [(r_1 s_2 + r_2 s_1, s_1 s_2)]_\sim \right.$$
$$\left. [(r_1,s_1)]_\sim \cdot [(r_2,s_2)]_\sim := [(r_1 r_2, s_1 s_2)]_\sim \right)$$

injectivity: $\varphi([(r,s)]_\sim) = 0 \Rightarrow \frac{r}{s} = 0$ in $\mathbb{Q}$

$\Rightarrow r \underset{=0}{=} 0 \cdot s$ in $\mathbb{Z} \subseteq \mathbb{Q}$. $\Rightarrow [(r,s)]_\sim = [(0,s)]_\sim$ = zero element in R_S.

(3) $S \ni \{0\}$. $\subseteq R$. Then $R_S = \{0\}$.

"If you can divide by zero, then you get the zero module.

(4) $R_S = \{0\} \Leftrightarrow 0 \in S$ (exercise)

(5) Let $(\mathfrak{p}_i)_{i \in I}$ be a family of prime ideals of R.

$S := R \setminus (\bigcup_{i \in I} \mathfrak{p}_i)$ is multiplicatively closed.

We will see that if $|I| < \infty$ then the prime ideals of R_S are exactly those ideals $\mathfrak{q}_S \subseteq R_S$ such that $\mathfrak{q}$ is a prime ideal of R with $\mathfrak{q} \subseteq \mathfrak{p}_i$ for some i.

<u>Notation 109:</u> $\mathrm{Spec}(R) := \{\mathfrak{p} \subseteq R \mid \mathfrak{p} \text{ a prime ideal of } R\}$, $\mathrm{Specm}(R) = \{\mathfrak{m} \mid \mathfrak{m} \leq_R R \text{ max.}\}$

<u>Prop 110:</u> Let R be a ring and $S \subseteq R$ be non-empty and mult. closed.

(1) $\forall$ ideal $\mathfrak{a}$ of R: $\mathfrak{a}_S \leq_{R_S} R_S$.

(2) The map $\mathfrak{p} \longmapsto \mathfrak{p}_S$ from

$\{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p} \cap S = \emptyset\}$ to $\operatorname{Spec}(R_S)$

is bijective.

end lecture 15

<u>Proof:</u> (1) The assertion of (1) is that the set (*)

$\{\frac{a}{s} \in R_S \mid a \in \mathfrak{a}, s \in S\}$ is an ideal of R_S.

- $\frac{a_1}{s_1} - \frac{a_2}{s_2} = \frac{a_1 s_2 - a_2 s_1}{s_1 s_2}$ and $a_1 s_2 - a_2 s_1 \in \mathfrak{a}$
- $\frac{r}{t} \cdot \frac{a}{s} = \frac{ra}{ts}$ and $ra \in \mathfrak{a}$.
- the above set is not empty.

We identify $\mathfrak{a}_S$ (localization of $\mathfrak{a}$ at S) with the set (*).

(2) · <u>$\mathfrak{p}_S$ is a prime ideal of R_S</u>: Take $\mathfrak{p} \in \operatorname{Spec}(R)$ with $S \cap \mathfrak{p} = \emptyset$.

$\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} \in \mathfrak{p}_S \Longrightarrow \exists\, p \in \mathfrak{p},\ s \in S: \frac{r_1 \cdot r_2}{s_1 s_2} = \frac{p}{s}$

$\Longrightarrow \exists\, t \in S: \ t(s_1 s_2 p - s r_1 r_2) = 0$

$\Longrightarrow \ t s r_1 r_2 \in \mathfrak{p} \underset{t, s \notin \mathfrak{p}, \text{ because } \mathfrak{p} \cap S = \emptyset}{\Longrightarrow} r_1 \in \mathfrak{p}$ or $r_2 \in \mathfrak{p}$

$\Rightarrow \quad \frac{r_1}{s_1} \in \mathfrak{p}_S$ or $\frac{r_2}{s_2} \in \mathfrak{p}_S$.

Also $\mathfrak{p}_S \neq R_S$ because $\frac{1}{1} \notin \mathfrak{p}_S$

($\frac{1}{1} \in \mathfrak{p}_S \Rightarrow \exists\, p \in \mathfrak{p}, s \in S : \frac{1}{1} = \frac{p}{s} \Rightarrow \exists_{t \in S}\, t(s-p) = 0$

$\Rightarrow ts \in \mathfrak{p} \Rightarrow t \in \mathfrak{p}$ or $s \in \mathfrak{p}$ ↯ $\mathfrak{p} \cap S = \emptyset$)

Thus using (1): $\mathfrak{p}_S$ is a prime ideal of R_S.

- $\underset{\substack{\uparrow \\ \mathrm{Spec}(R)}}{\mathfrak{p}}$ with $\mathfrak{p} \cap S = \emptyset \longmapsto \underset{\substack{\uparrow \\ \mathrm{Spec}(R_S)}}{\mathfrak{p}_S}$ is <u>injective</u>:

Consider $\varphi : R \to R_S$. $\varphi(r) = \frac{r}{1}$. Take

$\mathfrak{p} \in \mathrm{Spec}(R)$ with $\mathfrak{p} \cap S = \emptyset$.

Then $\varphi^{-1}(\mathfrak{p}_S) = \{ r \in R \mid \frac{r}{1} \in \mathfrak{p}_S \}$

$= \{ r \in R \mid \exists\, p \in \mathfrak{p}, s \in S : \frac{r}{1} = \frac{p}{s} \}$

$\underset{\substack{\uparrow \\ \mathfrak{p} \text{ prime ideal} \\ \mathfrak{p} \cap S = \emptyset}}{=} \{ r \in R \mid r \in \mathfrak{p} \} = \mathfrak{p}$

So ~~for~~ φ^{-1} on $\mathrm{Spec}(R_S)$ is a left inverse

of $\underset{S \cap \mathfrak{p} = \emptyset}{\mathfrak{p}} \longmapsto \mathfrak{p}_S$.

· <u>surjectivity</u>: Let $\mathfrak{q}$ be a prime ideal of R_S

$\mathfrak{p} := \varphi^{-1}(\mathfrak{q})$. Then $S \cap \mathfrak{p} = \emptyset$, because otherwise $\mathfrak{q} \cap (R_S)^\times \neq \emptyset$ ↯. Note: $\{\frac{s}{1} \mid s \in S\} \subseteq (R_S)^\times$.

Further $\mathfrak{p}_S \subseteq \mathfrak{q}$.

"$\supseteq$"? Take $\frac{r}{s} \in \mathfrak{q} \Rightarrow \frac{r}{1} = \frac{sr}{s} \in \mathfrak{q} \Rightarrow r \in \mathfrak{p}$

$\Rightarrow \frac{r}{s} \in \mathfrak{p}_S$. $\square$

<u>Examples III:</u>

(1) p a prime: $\mathbb{Z}_{(p)} := \{\frac{a}{b} \mid a \in \mathbb{Z},\ b \in \mathbb{Z} \setminus p\mathbb{Z}\} = \mathbb{Z}_S$ for

$S = \mathbb{Z} \setminus p\mathbb{Z}$.

$\mathbb{Z}_{(p)}$ has two prime ideals: $p\mathbb{Z}_S$ and $\{0\}$, because there are only two prime ideals of $\mathbb{Z}$ contained in $p\mathbb{Z}$.

(2) We come back to Ex 108 (5).

$S = R \setminus (\mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_e)$

$\mathrm{Spec}(R_S)$ 1-1 $\{\mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{p} \cap S = \emptyset\}$

1-1 $\{$ " $\mid \mathfrak{p} \subseteq \mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_e\}$

1-1 $\{$ " $\mid \exists_{i \in \{1, \ldots, e\}}: \mathfrak{p} \subseteq \mathfrak{p}_i\}$

(The last 1-1 by the prime avoidance ~~theorem~~ theorem.)

(3) We can generalize (1). $\mathfrak{p} \in \operatorname{Spec}(R)$.

$\Rightarrow S := R \setminus \mathfrak{p}$.

Then $\operatorname{Spec}(R_S) = \{ \mathfrak{q}_S \mid \mathfrak{q} \in \operatorname{Spec}(R), \mathfrak{q} \subseteq \mathfrak{p} \}$

In particular $\operatorname{Specm}(R_S) = \{ \mathfrak{p}_S \}$,

i.e. R_S has only one maximal ideal.

<u>Notation 112:</u> Let $\mathfrak{p} \in \operatorname{Spec}(R)$

We write $R_{\mathfrak{p}}$ for the localization of R at $R \setminus \mathfrak{p}$. (So here $S = R \setminus \mathfrak{p}$!)

<u>Prop 113:</u> Let S_1 and S_2 be multiplicatively closed subsets of R. Then $S_1 S_2 = \{ s_1 s_2 \mid s_1 \in S_1 \text{ and } s_2 \in S_2 \}$ is also multiplicatively closed and

$$R_{S_1 S_2} \simeq (R_{S_1})_{\varphi(S_2)}$$ ~~and~~ using

$\varphi : R \longrightarrow R_{S_1}$, $\varphi(r) := \frac{r}{1}$.

<u>Proof:</u> Exercise. $\square$

<u>Prop 114:</u> Let M be an R-module and S be a multiplicative subset of R. Then

$M_S \simeq M \otimes_R R_S$.

<u>Proof:</u> Consider the map $M \otimes_R R_S \longrightarrow M_S$ given by $m \otimes_R \frac{r}{s} \longmapsto \frac{rm}{s}$ on elementary tensors.

(well-defined, because induced by an R-bilinear map)

This map has an inverse:

$$M_S \longrightarrow M \otimes_R R_S \,, \quad \frac{m}{s} \longmapsto m \otimes_R \frac{1}{s}.$$

(well-defined: $\frac{m_1}{s_1} = \frac{m_2}{s_2} \Rightarrow \exists\, t \in S : t(s_2 m_1 - s_1 m_2) = 0_M$

$\Rightarrow 0 = t(s_1 m_2 - s_2 m_1) \otimes_R \frac{1}{t s_1 s_2} = m_2 \otimes_R \frac{1}{s_2} - m_1 \otimes_R \frac{1}{s_1}$)

$\square$

<u>Prop 115</u>: Localization is exact: Let R be a ring and $S \subseteq R$ be a multiplicatively closed subset.

Suppose $0 \to M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3 \to 0$ is an exact sequence of R-modules. Then

$$0 \to M_{1S} \xrightarrow{\alpha_S} M_{2S} \xrightarrow{\beta_S} M_{3S} \to 0 \text{ is}$$

exact. $\left(\alpha_S\left(\frac{m}{s}\right) := \frac{\alpha(m)}{s}. \right)$

<u>Proof:</u> At first verify that α_S is well-defined.

$M_{1_S} \ni \frac{m_1}{s_1} = \frac{m_2}{s_2} \Rightarrow \exists t \in S : t(s_2 m_1 - s_1 m_2) = 0.$

$$\Rightarrow \exists t \in S : t(s_2 \alpha(m_1) - s_1 \alpha(m_2)) = \alpha(t(s_2 m_1 - s_1 m_2))$$

$$= 0_{M_2}$$

$$\Rightarrow \frac{\alpha(m_1)}{s_1} = \frac{\alpha(m_2)}{s_2}$$

- α_S is injective: $\alpha_S\left(\frac{m_1}{s}\right) = 0_{M_{2S}} = \frac{0_{M_2}}{1}$

$$\Rightarrow \exists t \in S : \underbrace{t(\alpha(m_1) - s 0_{M_2})}_{= \alpha(t(m_1 - s \cdot 0_{M_1}))} = 0_{M_2}$$

α inj $\Rightarrow t(m_1 - s \cdot 0_{M_1}) = 0_{M_1} \Rightarrow \frac{m_1}{s} = \frac{0_{M_1}}{1}.$

- β_S is surjective: Take $\frac{m_3}{s} \in M_{3_S}$

β surjective $\Rightarrow \exists\, m_2 \in M_2 : \beta(m_2) = m_3.$

$$\Rightarrow \beta_S\left(\frac{m_2}{s}\right) = \frac{\beta(m_2)}{s} = \frac{m_3}{s}$$

- $\beta_S \circ \alpha_S = (\underbrace{\beta \circ \alpha}_{0\text{-map}})_S = 0\text{-map}.$

- $\mathrm{im}(\alpha_S) \supseteq \ker(\beta_S)$: Take $\frac{m_2}{s} \in \ker(\beta_S)$

$$\Rightarrow \exists t \in S : \underbrace{t\,\beta(m_2)}_{= \beta(t m_2)} = 0_{M_3} \underset{\text{inj } \alpha \text{ or } \beta}{\Rightarrow} \exists m_1 \in M_1 : \alpha(m_1) = t m_2$$

$$\Rightarrow \quad \alpha_S\left(\frac{m_1}{ts}\right) = \frac{\alpha(m_1)}{ts} = \frac{t m_2}{ts} = \frac{m_2}{s}. \qquad \square$$

II.2. Local rings

<u>Def 116:</u> A ring R is called local if $|\mathrm{Specm}(R)| = 1$.

<u>Prop 117:</u> Let R be a ring. Then are equivalent:

1° R is local

2° $R \setminus R^\times$ is an ideal of R.

<u>Proof:</u> 1° $\Rightarrow$ 2° Suppose R is local $\mathrm{Specm}(R) = \{\mathfrak{m}\}$.

Claim $R \setminus R^\times = \mathfrak{m}$.

<u>Pf:</u> "$\supseteq$" ✓ because $\mathfrak{m} \neq R$.

"$\subseteq$" Take $x \in R \setminus R^\times$. $\Rightarrow Rx =: \mathfrak{a}$ is an ideal $\neq R$, so $\exists$ maximal ideal $\mathfrak{n}$ of R such that $\mathfrak{a} \subseteq_R \mathfrak{n}$.

R has only the max. ideal $\mathfrak{m}$. $\Rightarrow \mathfrak{n} = \mathfrak{m}$

$\Rightarrow x \in \mathfrak{a} \subseteq \mathfrak{m}$. $\square$

2° $\Rightarrow$ 1° Suppose $\mathfrak{a} := R \setminus R^\times$ is an ideal of R.

$\Rightarrow \mathfrak{a}$ is maximal, because an ideal $\mathfrak{b}$ with $\mathfrak{a} \subsetneq \mathfrak{b} \subseteq R$ satisfies $R^\times \cap \mathfrak{b} \neq \emptyset$ and ~~that~~ therefore $\mathfrak{b} = R$.

By the same argument: Every ideal of R different from R must be contained in $\mathfrak{M}$.

$\Rightarrow \operatorname{Specm}(R) = \{\mathfrak{M}\}$. $\square$

<u>Example 118:</u> (1) The most important local rings for us are $R_{\mathfrak{p}}$, $\mathfrak{p} \in \operatorname{Spec}(R)$.

(2) Let us answer what $\mathcal{O}_{V,x}$ should be for the variety $V = V(P_1, \dots, P_e)$.

$$\mathcal{O}_{V,x} = \mathcal{O}_V(V)_{(\bar{X}_1 - x_1, \dots, \bar{X}_m - x_m)}$$

$$\simeq k[\bar{X}_1, \dots, \bar{X}_m]_{(\bar{X}_1 - x_1, \dots, \bar{X}_m - x_m)}$$

end of lecture 16.

<u>Prop 119:</u> Let M be a f.g. module over a local ring R. T.a.c.:

1° M projective

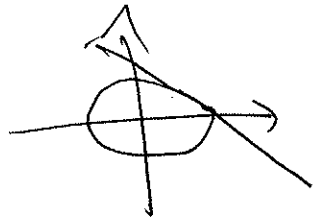
2° M is fpf

<u>Proof:</u> Only need $1^\circ \Rightarrow 2^\circ$. Take $n \in \mathbb{N}$ minimal s.t. $\exists\, \varepsilon \in \operatorname{Epi}_R(R^n, M)$ (suppose $M \neq 0$)

We denote $n =: \mu_R(M)$

Example 11.8-1:

① $S^1_{\mathbb{R}} = V_{\mathbb{R}}(X^2+Y^2-1) \subseteq \mathbb{R}^2$



$\mathcal{O}_{S^1_{\mathbb{R}}}(S^1_{\mathbb{R}}) =: \mathbb{R}[S^1_{\mathbb{R}}]$ other notation.

$$\mathbb{R}[S^1_{\mathbb{R}}] = \mathbb{R}[X,Y]/(X^2+Y^2-1) \qquad P := X^2+Y^2-1$$

Take $(x,y) \in S^1_{\mathbb{R}}$.

- tangent space at (x,y): Consider $\frac{\partial P}{\partial X}(x,y)(X-x) + \frac{\partial P}{\partial Y}(x,y)(Y-y)$

$$T_{(x,y)}(S^1_{\mathbb{R}}) = (x,y) + V(2xX+2yY)$$

$$= (x,y) + \{t(y,-x) \mid t \in \mathbb{R}\}$$

a 1-dimensional affine line

- Consider $\mathfrak{m} := \mathfrak{m}_{(x,y)} \subseteq \mathbb{R}[S^1_{\mathbb{R}}]$

$$\mathfrak{m} = (X-x, Y-y)/(X^2+Y^2-1) =: \tilde{\mathfrak{m}}/(X^2+Y^2-1)$$

<u>Question</u>: What is $\dim_{\mathbb{R}} \mathfrak{m}/\mathfrak{m}^2$?

we have:

$$X^2+Y^2-1 \equiv_{\tilde{\mathfrak{m}}^2} -x^2+2xX-y^2+2yY-1$$

$$\equiv_{\tilde{\mathfrak{m}}^2} -2(1-xX-yY)$$

$$\Rightarrow \quad 1-x\bar{X}-y\bar{Y} \equiv_{\mathfrak{m}^2} 0.$$

W.l.o.g. $x \neq 0$.

$$x(\bar{X} - x) \equiv_{\mathfrak{m}^2} -x^2 + 1 - x\bar{X} \equiv_{\mathfrak{m}^2} -x - y^2 + 1 - x(\bar{Y} - y)$$

$$\equiv_{\mathfrak{m}^2} -y(\bar{Y} - y)$$

$$\Rightarrow \mathfrak{m}/\mathfrak{m}^2 = (\bar{Y} - y) + \mathfrak{m}^2/\mathfrak{m}^2$$

Note $\bar{Y} - y \notin \mathfrak{m}^2$, because $Y - y \notin \tilde{\mathfrak{m}}^2 + (X^2 + Y^2 - 1)_{R(X,Y)}$

because if

$$Y - y \in \tilde{\mathfrak{m}}^2 + Q(X,Y)\underbrace{(X^2 + Y^2 - 1)}_{(X^2 - x^2) + (Y^2 - y^2)}$$

then

$$Y - y \equiv_{\tilde{\mathfrak{m}}^2} Q(x,y)\big((X - x)(X + x) + (Y - y)(Y + y)\big)$$

$$\equiv_{\tilde{\mathfrak{m}}^2} Q(x,y)(2xX + 2yY - 2)$$

$$\equiv_{\tilde{\mathfrak{m}}^2} Q(x,y)\big(2x(X - x) + 2y(Y - y)\big)$$

$$\Rightarrow \quad Q(x,y) = \frac{1}{2} \text{ and } x = 0 \quad ↯.$$

So $\dim_{\mathbb{R}} \mathfrak{m}/\mathfrak{m}^2 = 1$.

② $\tilde{X} := V_{\mathbb{R}}(X \cdot Y) \ni (x,y) \qquad (x = 0 \text{ or } y = 0)$

<u>Case $x \neq 0$:</u> tangent ~~line~~ space

$$T_{(x,y)}(\tilde{X}) = (x,0) + V_{\mathbb{R}}(0X + xY)$$

$$= (x,y) + \{t(1,0) \mid t \in \mathbb{R}\}$$

$$\mathfrak{m} := \mathfrak{m}_{(x,0)} \subseteq \mathbb{R}[\bar{X},\bar{Y}]/(\bar{X}\bar{Y}) =: \mathbb{R}[X]$$

$$\| $$

$$(\bar{X}-x, \bar{Y})/(\bar{X}\bar{Y})$$

$$\mathfrak{m}/\mathfrak{m}^2 = (\bar{X}-x)+\mathfrak{m}^2/\mathfrak{m}^2 \text{ has } \mathbb{R}\text{-dim } 1.$$

(Note $\bar{X}-x \notin \mathfrak{m}^2$)

Case $y \neq 0$ ✓

case $(x,y) = (0,0)$:

$$T_{(0,0)}(\tilde{X}) = (0,0) + V(0\bar{X} + 0\bar{Y}) = \mathbb{R}^2$$

$$\mathfrak{m}_{(0,0)}/\mathfrak{m}^2_{(0,0)} \simeq (\bar{X},\bar{Y})/(\bar{X}^2, \bar{X}\bar{Y}, \bar{Y}^2) \text{ has } \mathbb{R}\text{-dimension } 2.$$

$$\uparrow$$

$$\mathfrak{m}_{(0,0)} = (\bar{X},\bar{Y})/(\bar{X}\bar{Y})$$

~~$\mathfrak{m}/\mathfrak{m}^2_{(0,0)}$~~

But still there is no prime ideal $\mathfrak{p}$ of $\mathbb{R}[\tilde{X}]$ such that

$(\bar{X},\bar{Y}) \supsetneq \mathfrak{p}$ ~~[illegible]~~. $\supsetneq (\bar{X})$ or

$\supsetneq \mathfrak{p} \supsetneq (\bar{Y})$.

because if

$$(X, \cancel{Y}) \subsetneq \tilde{\mathfrak{p}} \subsetneq (X, XY) = (X) \text{ in } \mathbb{R}[X, Y]$$

then $\exists\, Q(Y) \in \mathbb{R}[Y] : \quad Y Q(Y) \in \tilde{\mathfrak{p}}$.

$$\underset{\substack{\uparrow \\ \mathbb{R}^\times \cap \tilde{\mathfrak{p}} = \emptyset}}{\Rightarrow} \quad Y \in \tilde{\mathfrak{p}}. \ \lightning$$

This last fact is related to the dimension of $\tilde{X}$

(max ℓ s.t. $\exists\, \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_\ell$ prime ideals in $\mathbb{R}[\tilde{X}]$)

So $\mathbb{R}[\tilde{X}]_{\mathfrak{m}}$ can see $\dim \tilde{X}$ and

the tangent space: $\left(\mathfrak{m}_{\mathfrak{m}} / \mathfrak{m}_{\mathfrak{m}}^2\right)^* \simeq \left(\mathfrak{m}/\mathfrak{m}^2\right)^*$

$$= \mathrm{Hom}_{\underbrace{\mathbb{R}[\tilde{X}]/\mathfrak{m}}_{\mathbb{R}}}\left(\left(\mathfrak{m}_{\mathfrak{m}} / \mathfrak{m}_{\mathfrak{m}}^2\right), \underbrace{\mathbb{R}[\tilde{X}]/\mathfrak{m}}_{\mathbb{R}}\right)$$

There is an example in the homework.

<u>Def 118-2:</u> Let R be a ring.

(1) We call the following supremum:

$$\sup\{\ell \in \mathbb{N} \mid \exists\, \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \dots \subsetneq \mathfrak{p}_\ell \text{ in } \operatorname{Spec}(R)\} \in \mathbb{N} \cup \{\infty\}$$

the "Krull-dimension" of R. We write $\dim_{\text{Krull}} R$

(2) Let R be a noetherian local ring with maximal ideal $\mathfrak{m}$.

R is called regular ~~iff~~ if

$$\dim_{\text{Krull}} R = \dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2).$$

Def 119: Let M be an R-module. M is called finitely presented iff $\exists_{n,m \in \mathbb{N}} \varphi \in \mathrm{Hom}_R(R^n, R^m)$:

$\mathrm{coker}(\varphi) \cong M$

(Recall: $\mathrm{coker}(f) := U/\mathrm{im} f$ for $f \in \mathrm{Hom}_R(N, U)$)
"cokernel" of f.

Remark 120: 1) If R is noetherian then
"f.g." = "finitely presented (f.p.)"

2) Let M be a f.g. R-module and projective
~~Then as equivalent:~~
~~is~~
Then M is finitely presented.

Proof: 2) Take $\varepsilon \in \mathrm{Epi}_R(R^n, M)$ and a sections.
$\Rightarrow \ker(\varepsilon) \oplus \mathrm{im}(s) = R^n$
The image of $\pi : R^n \twoheadrightarrow \ker(\varepsilon)$ is generated
$a + s \longmapsto a$
$\ker(\varepsilon) \quad s(M)$

by $\pi(e_i)$, $i = 1, 2, \dots, n$. $\square$

<u>Prop 121:</u> Let M be an R-module. T.a.e:

1° M f.p.

2° $\exists\ \exists_{n,m \in \mathbb{N}}$ exact sequence: $R^{(n)} \to R^m \to M \to 0$

3° $\exists\ \exists_{m \in \mathbb{N}}\ \varepsilon \in \mathrm{Epi}_R(R^m, M)$: $\ker(\varepsilon)$ is f.g.

4° $\forall_{m \in \mathbb{N}}\ \forall \varepsilon \in \mathrm{Epi}_R(R^m, M)$: $\ker(\varepsilon)$ is f.g.

<u>Proof:</u> 1° $\Leftrightarrow$ 2° $\Leftrightarrow$ 3° trivial.

4° $\Rightarrow$ 3° ✓

3° $\Rightarrow$ 4°: $\exists_{m \in \mathbb{N}}\ \exists\ \varepsilon \in \mathrm{Epi}_R(R^m, M)$:

$\ker(\varepsilon)$ is f.g.

Take $n \in \mathbb{N}$ and $\varrho \in \mathrm{Epi}_R(R^n, M)$.

To show $\ker(\varrho)$ is f.g..

We have

$$\begin{array}{ccccccccc} 0 & \to & \ker(\varepsilon) & \to & R^m & \xrightarrow{\varepsilon} & M & \to & 0 \\ & & & & & & \| & & \\ 0 & \to & \ker(\varrho) & \to & R^n & \xrightarrow{\varrho} & M & \to & 0 \end{array}$$

both exact

Lemma 122 (Schanuel)

$\Rightarrow \quad \ker(\varrho) \oplus R^m \simeq \ker(\varepsilon) \oplus R^n$.

$\Rightarrow \quad \ker(\varrho)$ f.g. $\qquad \square$

<u>Lemma 122 (Schanuel)</u>

Let M be an R-module and P, Q be projective " ".

Suppose $\varepsilon \in \mathrm{Epi}_R(P, M)$ and $\eta \in \mathrm{Epi}_R(Q, M)$.

Then: $\ker(\varepsilon) \oplus Q \simeq \ker(\eta) \oplus P$.

$$\begin{tikzcd}
0 \arrow[r] & \ker(\varepsilon) \arrow[r] & P \arrow[r, "\varepsilon"] & M \arrow[r] & 0 \\
0 \arrow[r] & \ker(\eta) \arrow[r] & Q \arrow[r, "\eta"] & M \arrow[r] \arrow[u, equal, "id_M"] & 0
\end{tikzcd}$$

<u>Proof:</u> projectivity $\Rightarrow$ $\exists\, f: Q \longrightarrow P$ and $g: P \longrightarrow Q$ such that

$$\begin{tikzcd}
P \arrow[r, two heads] & M \\
Q \arrow[u, "f"] \arrow[r, two heads] \arrow[ur, phantom, "\circlearrowleft"] & M \arrow[u, equal]
\end{tikzcd}
\quad \text{and} \quad
\begin{tikzcd}
P \arrow[r, two heads] \arrow[d, "g"'] \arrow[dr, phantom, "\circlearrowleft"] & M \arrow[d, equal] \\
Q \arrow[r, two heads] & M
\end{tikzcd}$$

We consider the following diagram:

$$\begin{tikzcd}
0 \arrow[r] & \ker(\varepsilon) \oplus \ker(\eta) \arrow[r] & \ker(\eta) \oplus P \arrow[r] & M \arrow[r] & 0 \\
0 \arrow[r] & \ker(\varepsilon) \oplus \ker(\eta) \arrow[r] \arrow[u, dashed, "u"] \arrow[ur, phantom, "\circlearrowleft"] & \ker(\eta) \oplus Q \arrow[r] \arrow[u, dashed, "v"] \arrow[ur, phantom, "\circlearrowleft"] & M \arrow[r] \arrow[u, equal] & 0
\end{tikzcd}$$

$$u(a + b) := (\underset{\ker(\varepsilon)}{a + f(b)}) + (\underset{\ker(\eta)}{b - g(f(b))} - g(a))$$

$$v(a + q) := (q - g(f(q)) - g(a)) + (f(q) + a).$$

We show that u is bijective.

<u>injective:</u> $u(a+b)=0$

$\Rightarrow a+f(b)=0$ and $b-g(a+f(b))=0$

$\Rightarrow b=0$ and $a=0$

<u>surjective:</u> Given $(A,B)\in \ker(\varepsilon)\oplus\ker(\eta)$

$b:=B+g(A)$ $\quad a:=A-f(b)$

Then $\eta(b)=\eta(\underbrace{g(A)}_{\in\ker(\eta)})=0$

$\varepsilon(a)=\varepsilon(A)-\varepsilon(\underbrace{f(b)}_{b\in\ker\eta\Rightarrow f(b)\in\ker\varepsilon})=0$

and $u(a,b)=(a+f(b),\, b-g(f(a))-g(a))$

$=(A,\, b-g(A))=(A,B)$.

Snake-Lemma $\Rightarrow$ v is an isomorphism. $\square$
(next intermezzo).

end of lecture 17!

Intermezzo: Diagram chase

<u>Lemma 123:</u> Consider the following commutative diagram with exact rows.

$$\begin{tikzcd}
M_1 \arrow[r, "f_1"] \arrow[d, "\alpha"'] \arrow[dr, phantom, "\circlearrowleft"] & M_2 \arrow[r, "f_2"] \arrow[d, "\beta"'] \arrow[dr, phantom, "\circlearrowleft"] & M_3 \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & N_1 \arrow[r, "g_1"'] & N_2 \arrow[r, "g_2"'] & N_3
\end{tikzcd}$$

Then $\exists\ \delta : \ker(\gamma) \longrightarrow \operatorname{Coker}(\alpha)$

s.t.

$$\begin{tikzcd} \ker(\alpha) \arrow[r, "f_1"] & \ker(\beta) \arrow[r, "f_2"] & \ker(\gamma) \arrow[dll, "\delta"'] \\ \operatorname{coker}(\alpha) \arrow[r, "\bar{g}_1"'] & \operatorname{coker}(\beta) \arrow[r, "\bar{g}_2"'] & \operatorname{coker}(\gamma) \end{tikzcd}$$

is exact.

Picture:

$$\begin{tikzcd} & \ker\alpha \arrow[r] \arrow[d] & \ker\beta \arrow[r] \arrow[d] & \ker\gamma \arrow[d] & \\ & M_1 \arrow[r] \arrow[d] & M_2 \arrow[r] \arrow[d] & M_3 \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & M \arrow[r] \arrow[d] & N_2 \arrow[r] \arrow[d] & N_3 \arrow[d] & \\ & \operatorname{Coker}(\alpha) \arrow[r] & \operatorname{Coker}\beta \arrow[r] & \operatorname{Coker}\gamma & \end{tikzcd}$$

Proof: $f_1, f_2, \bar{g}_1, \bar{g}_2$ are well-defined by the commutativity of the diagram.

We construct δ: $m_3 \in \ker(\gamma)$.

$\underset{\substack{\uparrow \\ f_2 \text{ surj}}}{\Rightarrow}$ $\exists\, m_2 \in M_2 : f_2(m_2) = m_3$

$\Rightarrow$ $g_2(\beta(m_2)) = \gamma(f_2(m_2)) = 0$

$\Rightarrow$ $\exists\, n_1 \in N_1 : g_1(n_1) = \beta(m_2)$

Define $\delta(m_2) := [n_1]_{\operatorname{im}(\alpha)} \in \operatorname{Coker}\alpha = N_1 / \operatorname{im}\alpha$.

<u>Exercise</u>: δ is well-defined and the ker – coker sequence is exact. $\square$

~~<u>Corollary 124</u>: Let R be a ring~~

$$\begin{tikzcd}
 & \cdot \arrow[r, "f_1"] \arrow[d, "\gamma_2"] & \cdot \arrow[r, "f_2"] \arrow[d, "\beta_2"] & \cdot \arrow[d, "\alpha_2"] \\
0 \arrow[r] & \cdot \arrow[r, "g_1"] \arrow[d, "\gamma_3"] & \cdot \arrow[r, "g_2"] \arrow[d, "\beta_3"] & \cdot \\
 & \cdot \arrow[r, "g"] \arrow[d] & \cdot & \\
 & 0 & &
\end{tikzcd}$$

<u>Corollary 124</u>: Suppose that the diagram

$$\begin{tikzcd}
0 \arrow[r] & \cdot \arrow[r] \arrow[d, "\alpha"] & \cdot \arrow[r] \arrow[d, "\beta"] & \cdot \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & \cdot \arrow[r] & \cdot \arrow[r] & \cdot \arrow[r] & 0
\end{tikzcd}$$

is commutative and the rows are exact. Then: If two of the maps α, β, γ are bijective then the third is bijective too.

<u>Proof</u> Follows from the Snake lemma (Lemma 123). $\square$

Lemma 125 (Meta lemma).

Suppose in the diagram of R-modules

$$\begin{tikzcd}
 & & 0 \arrow[d] \\
 & \bullet \arrow[r, "f_1"] \arrow[d, "\gamma_1"] & \bullet \arrow[r, "f_2"] \arrow[d, "\beta_1"] & \bullet \arrow[d, "\alpha_1"] \\
0 \arrow[r] & \bullet \arrow[r, "g_1"] \arrow[d, "\gamma_2"] & \bullet \arrow[r, "g_2"] \arrow[d, "\beta_2"] & \bullet \\
 & \bullet \arrow[r, "h_1"] \arrow[d] & \bullet & \\
 & 0 & &
\end{tikzcd}$$

all rows and columns are exact and suppose the diagram is commutative.

Then h_1 is injective.

Proof: diagram chase. $\square$

Example 126: An R-module f.g., but not f.p.:

$R = \mathbb{R}[X_1, X_2, \dots]$. $M := R/(X_1, X_2, \dots)_R$

$\varepsilon : R \twoheadrightarrow M$ canonical projection has not a f.g. kernel. $\overset{121}{\Longrightarrow}$ M is not f.p.

Theorem 127: Let R be a local ring and M be an R-module f.p.

Then are equivalent

1° M is flat

2° M is projective

3° M is free.

<u>Lemma 128:</u> Let R be a ring M a flat R-module and $0 \to M_1 \to M_2 \xrightarrow{f} M \to 0$ exact.

Then $\forall$ N R-module:

$$0 \to M_1 \otimes_R N \to M_2 \otimes_R N \to M \otimes_R N \to 0$$ is exact.

<u>Proof:</u> (We use the Meta lemma)

Take a free R-module F and $\varepsilon \in \mathrm{Epi}_R(F, M)$.

$$\begin{tikzcd}
 & M_1 \otimes \ker(\varepsilon) \arrow[r] \arrow[d] & M_2 \otimes \ker(\varepsilon) \arrow[r] \arrow[d] & M \otimes \ker(\varepsilon) \arrow[d] \arrow[d, shift left=6ex, "0"] \\
0 \arrow[r] & M_1 \otimes F \arrow[r] \arrow[d] & M_2 \otimes F \arrow[r] \arrow[d] & M \otimes F \\
 & M_1 \otimes N \arrow[r] \arrow[d] & M_2 \otimes N & \\
 & 0 & &
\end{tikzcd}$$

1st row and 1st and 2nd column are exact because of the right exactness of $\otimes$ ~~and the flatness of F~~.

The second row and the 3rd column are exact because of the flatness of M and F.

Meta lemma (125) $\Longrightarrow$ $M_1 \otimes N \to M_2 \otimes N$ is injective. $\square$

<u>Proof of Theorem 127:</u>

$2^0 \Rightarrow 3^0$: $\exists n \in \mathbb{N} : \exists \varepsilon \in \mathrm{Epi}_R(R^n, M)$:

$\mathrm{Ker}(\varepsilon)$ is f.g. M projective $\Rightarrow \exists s \in \mathrm{Monop}(M, R^n)$:

$$\begin{tikzcd} R^n \arrow[r, shift left, "\varepsilon"] & M \arrow[l, shift left, "s"] \end{tikzcd} \quad : \quad \varepsilon \circ s = \mathrm{id}_M$$

$\Rightarrow R^n = \mathrm{Ker}(\varepsilon) \oplus \mathrm{im}(s)$.

Let n be minimal $\mu_R(M) := n$ (notation)

To show: ε is injective.

(Lemma of Nakayama: we have to show that $\mathfrak{M}\,\mathrm{Ker}(\varepsilon) = \mathrm{Ker}(\varepsilon)$.)

⌈ Exercise (Lemma of Nakayama) 129: M be a f.g. R-module and $\mathfrak{a} \leq_R \mathrm{Rad}(R) = \bigcap_{\mathfrak{M}\,\mathrm{max}} \mathfrak{M}$ s.t. $\mathfrak{a}M = M$

Then $M = \{0\}$ ⌋

~~Suppose~~

<u>We show first</u> $\mathrm{Ker}(\varepsilon) \subseteq \mathfrak{M}R^n$.

Assume $\exists (x_1, \dots, x_n) \in \mathrm{Ker}(\varepsilon) \subseteq R^n$ with $x_1 \notin \mathfrak{M}$

$$\Rightarrow 0 = \sum_{i=1}^n x_i \varepsilon(e_i)$$

$$\Rightarrow x_1 \varepsilon(e_1) = -\sum_{i=2}^n \varepsilon(e_i) \overset{x_1 \in R \setminus \mathfrak{M} = R^\times}{\Longrightarrow}$$

$\varepsilon(e_1) \in \langle \varepsilon(e_2), \dots, \varepsilon(e_n) \rangle_R$ ↯

<u>We show</u> $\mathrm{Ker}(\varepsilon) = \mathfrak{M}\,\mathrm{Ker}(\varepsilon)$:

$$\mathfrak{m}\ker(\varepsilon) \oplus \mathfrak{m}S(M) = \mathfrak{m}R^n \supseteq \ker(\varepsilon)$$

$$\Rightarrow \quad \mathfrak{m}\ker(\varepsilon) \supseteq \ker(\varepsilon).$$

$\uparrow$

$\ker(\varepsilon) \cap S(M) = \{0\}$

Lemma of Nakayama (29) $\Rightarrow \ker(\varepsilon) = \{0\}$

<u>$1^\circ \Rightarrow 3^\circ$:</u> Let M be R-flat.

M f.p. $\Rightarrow \exists_{n \in \mathbb{N}} \exists\, \varepsilon \in \mathrm{Epi}_R(R^n, M)$: $\ker(\varepsilon)$ is f.g.

$$\begin{tikzcd}
0 \arrow[r] & \ker(\varepsilon) \otimes_R R/\mathfrak{m} \arrow[r] \arrow[d, phantom, "\cong"] & R^n \otimes_R R/\mathfrak{m} \arrow[r] \arrow[d, phantom, "\cong"] & M \otimes_R R/\mathfrak{m} \arrow[r] \arrow[d, phantom, "\cong"] & 0 \\
0 \arrow[r] & \ker(\varepsilon)/\mathfrak{m}\ker(\varepsilon) \arrow[r, "i"] & (R/\mathfrak{m})^n \arrow[r] & M/\mathfrak{m}M \arrow[r] & 0
\end{tikzcd}$$

The upper sequence is exact, so the second too.

$\Rightarrow i$ is injective

Let n be minimal. (for $\exists\, \varepsilon$)

$$\Rightarrow \quad \ker(\varepsilon) \subseteq \mathfrak{m}R^n \Rightarrow \operatorname{im} i = \{0\}$$

$\uparrow$

as in $2^\circ \Rightarrow 3^\circ$

i is injective $\Rightarrow \ker(\varepsilon)/\mathfrak{m}\ker(\varepsilon) = \{0\}$

$$\Rightarrow \quad \ker(\varepsilon) = \mathfrak{m}\ker(\varepsilon).$$

Lemma of Nakayama (note $\ker(\varepsilon)$ is f.g.)

$\Rightarrow \quad \ker(\varepsilon) = \{0\}.$ $\square$

Examples 130:

Some examples corresponding to Lemma 129.

1) $\mathrm{Rad}(\mathbb{Z}) = \bigcap_{\mathfrak{m} \in \mathrm{Specm}(\mathbb{Z})} \mathfrak{m} = \bigcap_{p \text{ prime number}} p\mathbb{Z} = \{0\}$.

$$\mathrm{Rad}\left(\mathbb{Z}/36\mathbb{Z}\right) = 3\mathbb{Z}/36\mathbb{Z} \cap 2\mathbb{Z}/36\mathbb{Z} \underset{\text{div. by 2 and 3}}{=} 6\mathbb{Z}/36\mathbb{Z}.$$

$(36 = 2^2 \cdot 3^2$. "$\mathrm{rad}(36)$" $= 2 \cdot 3)$

$\sqrt{(36)_{\mathbb{Z}}} = (6)_{\mathbb{Z}}$.

$$\mathrm{Rad}(\mathbb{R} \times \mathbb{R}) = (\{0\} \times \mathbb{R}) \cap (\mathbb{R} \times \{0\}) = \{(0,0)\}.$$

2) Let R be a ring and $\mathrm{Rad}(R) = \{0\}$.
Then R can be embedded in a product of fields

$$R \hookrightarrow R/\mathrm{Rad}(R) \hookrightarrow \prod_{\mathfrak{m} \in \mathrm{Specm}(R)} R/\mathfrak{m}.$$

~~3) If R is Artinian,~~

Def 131: An R-module M is called Artinian if $\forall$ chain of R-submodules

$$M \supseteq M_0 \supseteq M_1 \supseteq M_2 \supseteq \dots :$$

$$\exists k \in \mathbb{N}\ \forall n \geq k : M_k = M_n.$$

A ring R is called artinian if it is an artinian R-module.

<u>Prop 132:</u> An artinian ring is noetherian.

end of lecture 18

<u>Def 132-1:</u> (1) An R-module is called simple if it is a non-zero R-module with exactly two submodules.

(2) An R-module is called semisimple if it is a sum of simple R-modules.

(We have the same definition for left and right modules in the non-commutative case)

<u>Examples 132-2:</u> (1) Vector spaces are semisimple

(2) $M_n(\mathbb{R})$ is semisimple as an $M_n(\mathbb{R})$-left-module.

<u>Pf:</u> $M_n(\mathbb{R}) = \begin{pmatrix} * & 0 & \cdots & 0 \\ \vdots & & & \\ * & 0 & \cdots & 0 \end{pmatrix} + \begin{pmatrix} 0 & * & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & * & 0 & \cdots & 0 \end{pmatrix} + \cdots + \begin{pmatrix} 0 & \cdots & 0 & * \\ \vdots & & \vdots & \vdots \\ 0 & \cdots & 0 & * \end{pmatrix}$. $\square$

(3) $\mathbb{Z}^n$ is not semisimple, because the simple $\mathbb{Z}$-modules are of the form $\mathbb{Z}/p\mathbb{Z}$, p a prime number, and $\mathbb{Z}^n$ has no torsion.

<u>Lemma 132—3:</u> Let M be a semisimple R-module. Then M is a direct sum of simple R-modules.

<u>Proof:</u> Suppose $M \neq 0$. (Otherwise there is nothing to show.) M is semisimple, so a sum of simple submodules $\underset{M \neq 0}{\Longrightarrow} \exists N$ simple $N \leq_R M$.

So $\mathfrak{M} = \{ A \mid A$ is a non-empty set of simple submodules of M s.t. $\sum_{N \in A} N = \bigoplus_{N \in A} N$, i.e. their sum is direct. $\}$

is non-empty and inductively ordered w.r.t. $\subseteq$.

Zorn's lemma $\Longrightarrow \exists \hat{A} \in \mathfrak{M} : \hat{A}$ is $\subseteq$-maximal.

$M_0 := \sum_{N \in \hat{A}} N$. If $M_0 \subsetneq M$ then

$\exists N \leq_R M$ simple: $N \not\subseteq M_0$ (because M is a sum of simple modules.

$\Longrightarrow M_0 \cap N = \{0\}$, because N is simple.

$\Longrightarrow \hat{A} \cup \{N\} \in \mathfrak{M}$ $\lightning$

$\square$

<u>Notation 132 – 4:</u> Let R be a ring we have two notions of radical:

Nil radical of R : $\mathrm{Nil}(R) := \bigcap_{\mathfrak{p} \in \mathrm{Spec}(R)} \mathfrak{p}$

Jacobson radical of R : $\mathrm{Jac}(R) := \bigcap_{\mathfrak{m} \in \mathrm{Specm}(R)} \mathfrak{m}$

$\mathrm{Jac}(R) = \mathrm{Rad}(R)$

<u>Proof of Prop 132:</u> $J := \mathrm{Jac}(R)$.

<u>Step 1:</u> J is nilpotent, i.e. $\exists\, n \in \mathbb{N} : J^n = \{0\}$.

<u>Pf:</u> $J \supseteq J^2 \supseteq J^3 \supseteq \dots$

R is artinian $\Rightarrow \exists\, k \in \mathbb{N}\ \forall n \geq k : J^k = J^n$.

Assume $J^k \neq \{0\}$. Let I be minimal among the ideals I' satisfying $I' J^k \neq \{0\}$.

Then ① $IJ = I$ because
$(IJ)J^k = IJ^{k+1} = IJ^k \neq \{0\}$ and $IJ \leq_R I$.

② $\exists\, x \in R \setminus \{0\} : (x)_R = I$.

<u>Pf:</u> Take $x \in I \setminus \{0\}$, s.t. $xJ^k \neq \{0\}$.
$Rx \leq_R I$ and I was chosen minimal. $\Rightarrow Rx = I$ □

Lemma of Nakayama $\Rightarrow I = \{0\}$ ↯ because $IJ^k \neq \{0\}$.

Thus $J^k = \{0\}$.

<u>Step 2:</u> Take $n_0 \in \mathbb{N}$ s.t. $J^{n_0} = \{0\}$.
We show that $\forall_{k=0,\dots,n_0-1}$:

$$J^k / J^{k+1} \text{ is a semisimple } R\text{-module.}$$

<u>Proof:</u> <u>$k=0$:</u> J is an intersection of finitely many maximal ideals, otherwise

$$\mathfrak{m}_1 \supsetneq \mathfrak{m}_1 \cap \mathfrak{m}_2 \supsetneq \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \mathfrak{m}_3 \supsetneq \dots \}$$

Say $J = \mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_\ell$.

In particular $\mathrm{Specm}(R) = \{\mathfrak{m}_1, \dots, \mathfrak{m}_\ell\}$

$$\text{CRT} \Rightarrow \quad R/J \simeq R/\mathfrak{m}_1 \times \dots \times R/\mathfrak{m}_\ell$$
$$\simeq R/\mathfrak{m}_1 \oplus \dots \oplus R/\mathfrak{m}_\ell$$

<u>$k>0$:</u> J^k / J^{k+1} is an R/J-module

$$J^k / J^{k+1} = \sum_{x \in J^k} R/J \cdot [x]_{J^{k+1}} \quad \text{is a}$$

sum of simple R/J-, in particular R-, modules.

$\square$

<u>Step 3:</u> R is noetherian

<u>Pf:</u> $\forall_{k=0,\dots,n_0-1}$: J^k/J^{k+1} is a direct sum of simple modules by Step 2 and Lemma 137-2.

$$J^k/J^{k+1} = \bigoplus_{\lambda\in\Lambda_k} N_\lambda$$

<u>Claim</u> Λ_k is finite: Otherwise $\Lambda_k \supseteq \{\lambda_1, \lambda_2, \lambda_3, \dots\}$ and we get the chain

$$\bigoplus_{i=1}^{\infty} N_{\lambda_i} \supsetneq \bigoplus_{i=2}^{\infty} N_{\lambda_i} \supsetneq \bigoplus_{i=3}^{\infty} N_{\lambda_i} \supsetneq \dots \quad ↯.$$

Thus J^k/J^{k+1} is noetherian.

Now

$$0 \to J \to R \to R/J \to 0$$

$$0 \to J^{k+1} \to J^k \to J^k/J^{k+1} \to 0 \qquad k = n_0-1, \dots, 0.$$

By induction the modules $J^{n_0-1}, J^{n_0-2}, \dots, J^2, J^1, R$ are noetherian $\square$

<u>Corollary B3:</u> Let R be artinian and $\mathrm{Jac}(R) = \{0\}$. Then R is a product of fields.

<u>Proof:</u> $(0) = \mathrm{Jac}(R) = \mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_\ell$ $\quad \mathfrak{m}_i \neq \mathfrak{m}_j \ \forall i \neq j$

$\Rightarrow \mathfrak{m}_i + \mathfrak{m}_j = R \ \forall i \neq j \overset{CRT}{\Rightarrow} R \simeq \times R/\mathfrak{m}_i$ $\square$

II.5. Local-global principle of commutative algebra

Prop 134: Let M be an R-module.

T.a.e.:

1° $M = \{0\}$

2° $M_{\mathfrak{m}} = 0 \quad \forall_{\mathfrak{m} \in \operatorname{Spec}(R)}$

3° $M_{\mathfrak{p}} = 0 \quad \forall_{\mathfrak{p} \in \operatorname{Spec}(R)}$

Proof: $1° \Rightarrow 3° \Rightarrow 2°$ ✓

$2° \Rightarrow 1°$: Take $m \in M$.

$\mathfrak{a} = \{ r \in R \mid rm = 0 \} = \operatorname{ann}(m)$

$\mathfrak{a}$ is an ideal.

Take $\mathfrak{m} \in \operatorname{Specm}(R)$.

Then $\exists\, s \in R \setminus \mathfrak{m}$: $sm = 0_M \Rightarrow \mathfrak{a} \not\subseteq \mathfrak{m}$.

$\mathfrak{m}$ arbitrary $\Rightarrow \mathfrak{a} = R \Rightarrow 1 \cdot m = 0$.

So $M = \{0\}$ $\square$

Cor 135: Let $f \in \operatorname{Hom}_R(M, N)$. T.a.e.

1° f is injective (surjective)

2° $\forall_{\mathfrak{m} \in \operatorname{Specm}(R)}$ $f_{\mathfrak{m}}$ injective (surjective)

<u>Proof:</u> $1^\circ \Rightarrow 2^\circ$ exactness of localization.

$2^\circ \Rightarrow 1^\circ$ ~~for injectivity.~~ Consider

exact $\rightsquigarrow$ by exactness of loc.

exact. $\rightsquigarrow$ trivial.

$$\begin{tikzcd}
 & & & \operatorname{Coker}(f)_S \arrow[d, equal] & \\
0 \arrow[r] & \ker(f)_S \arrow[r] \arrow[d, "\alpha"] & N_S \arrow[r] \arrow[d, equal] & \left(N/\operatorname{im}(f)\right)_S \arrow[r] \arrow[d, "\beta"] & 0 \\
0 \arrow[r] & \ker(f_S) \arrow[r] & N_S \arrow[r, "{[\frac{n}{s}]}"] & \operatorname{Coker}(f_S) \arrow[r] & 0
\end{tikzcd}$$

$\frac{m}{s} \mapsto \frac{m}{s}$

For $S = R \setminus \mathfrak{m}$

α is injective because $\ker(f)_S \hookrightarrow N_S$ is.

β is well-defined:

$$\frac{[n_1]}{s_1} = \frac{[n_2]}{s_2} \Rightarrow \exists t \in S : t(s_2[n_1] - s_1[n_2]) = [0_N]$$

$$\Rightarrow [t(s_2 n_1 - s_1 n_2)] = [0_N]$$

$$\Rightarrow t(s_2 n_1 - s_1 n_2) \in \operatorname{im}(f)$$

Apply $N \to N_S$, $n \mapsto \frac{n}{1}$.

$$\Rightarrow \frac{t(s_2 n_1 - s_1 n_2)}{1} \in \operatorname{im}(f_S)$$

$$\Rightarrow \frac{n_1}{s_1} - \frac{n_2}{s_2} \in \operatorname{im}(f_S).$$

β is surjective. ✓

Snake Lemma $\Rightarrow$ $\ker(\beta) \simeq \operatorname{coker}(\alpha)$.

α is surjective: $\frac{m}{s} \in \ker(f_s)$

$\Rightarrow \frac{f(m)}{s} = \frac{0_N}{s} \Rightarrow \exists t \in S: t f(m) = 0_N$

$\Rightarrow f(tm) = 0_N \Rightarrow tm \in \ker(f) \Rightarrow \frac{m}{s} \in \ker(f)_S.$

$\Rightarrow \underset{\in \ker(f)_S}{\alpha\left(\frac{m}{s}\right)} = \underset{\ker(f_S)}{\frac{m}{s}}$

Thus $\ker(\beta) \subseteq \operatorname{Coker}(\alpha) = 0.$

Now $2^\circ \Rightarrow 1^\circ$ follows from Prop 134. $\square$

<u>Theorem 136:</u> (Local – global principle for flatness) Let M be an R-module.

Then are equivalent:

1° M is flat

2° M_m is R_m-flat $\forall m \in \operatorname{Spec}(R)$

<u>Proof:</u> $1^\circ \Rightarrow 2^\circ$

$N_1 \hookrightarrow N_2$ $\quad N_i$ R_m-modules.

$\Rightarrow N_i$ are R-modules

$\Rightarrow N_1 \otimes_R M \hookrightarrow N_2 \otimes_R M.$

$$N_1 \otimes_R M = N_1 \otimes_{R_m} (R_m \otimes_R M) \simeq N_1 \otimes_{R_m} M_m.$$

So $N_1 \otimes_{R_m} M_m \hookrightarrow N_2 \otimes_{R_m} M_m$.

$2° \Rightarrow 1°$: Take $N_1 \overset{f}{\hookrightarrow} N_2$ two R-modules.

$$\begin{tikzcd}
(N_1 \otimes_R M)_m \arrow[r, "(f \otimes id)_m"] \arrow[d, "\wr"] & (N_2 \otimes_R M)_m \arrow[dddd, "\wr"] \\
N_1 \otimes_R M \otimes_R R_m \arrow[d, "\wr"] & \\
N_1 \otimes_R R_m \otimes_{R_m} R_m \otimes_R M \arrow[d, "\wr"] & \\
N_{1m} \otimes_{R_m} M_m \arrow[r, hook, "f_m \otimes id_m"] & N_{2m} \otimes_{R_m} M_m
\end{tikzcd}$$

$f_m \otimes id_m$ is injective by $2°$

m arbitrary + Cor 135 $\Longrightarrow$ $f \otimes id$ is injective. $\square$

<u>Theorem 137</u> (Local-global principle for projectivity)

Let M be an R-module. Suppose M is f.p. Then are equivalent:

1° M is projective

2° $\forall_{m \in \operatorname{Specm}(R)}$: M_m is a projective A_m-module (in fact free by Theorem 127)

<u>Lemma 138:</u> Let M be a f.p. R-module and N be an R-module. Then.

$$\operatorname{Hom}_{R_S}(M_S, N_S) \xrightarrow{\sim} (\operatorname{Hom}_R(M,N))_S$$
$$f_S \longleftarrow\!\shortmid f$$

for all S mult. closed with $0 \notin S$.

<u>Proof:</u>

$$R^n \longrightarrow R^m \longrightarrow M \longrightarrow 0 \text{ exact}$$

so

$$R_S^n \longrightarrow R_S^m \longrightarrow M_S \longrightarrow 0 \text{ exact}$$

$$\begin{tikzcd}
0 \arrow[r] & (\operatorname{Hom}_R(M,N))_S \arrow[r] \arrow[d, "\alpha"] \arrow[dr, phantom, "\circlearrowleft"] & (\operatorname{Hom}_R(R^m,N))_S \arrow[r] \arrow[d, "\beta"] \arrow[dr, phantom, "\circlearrowleft"] & (\operatorname{Hom}_R(R^n,N))_S \arrow[d, "\gamma"] \\
0 \arrow[r] & \operatorname{Hom}_{R_S}(M_S,N_S) \arrow[r] & \operatorname{Hom}_{R_S}(R_S^m,N_S) \arrow[r] & \operatorname{Hom}_{R_S}(R_S^n,N_S)
\end{tikzcd}$$

has exact rows.

We have

$$\begin{tikzcd}
(\mathrm{Hom}_R(R^m, N))_S \arrow[d, phantom, "\cong"] \arrow[dd, bend left, "\beta"] \\
\left(\bigoplus \mathrm{Hom}_R(R, N)\right)_S \arrow[d, phantom, "\cup"] \\
\left(\bigoplus N\right)_S \arrow[d, phantom, "\cong"] \\
\bigoplus N_S \simeq \bigoplus \mathrm{Hom}_{R_S}(R_S^m, N_S)
\end{tikzcd}$$

So β and γ are bijective.

$\Rightarrow$ α is bijective (diagram chase.) $\square$

<u>Proof</u> (Thm 137): Exercise. Use Lemma 138. $\square$

end lecture 19

III Integral ring extensions and ideal theory

III.1. 1st definitions and properties

Def. 139: (1) Let R and S be two rings. We call S a ring extension of R if $R \subseteq S$ and $1_R = 1_S$. We write $S|R$.

(2) Let $S|R$ be a ring extension. An element $x \in S$ is called integral over R if $\exists$ a monic polynomial $P \in R[X]$ which has x as a root.

(3) A ring extension $S|R$ is called integral if every element of S is integral over R.

Example 140: (a) Every element of $\mathbb{Z}[\sqrt{2}]$ is integral over $\mathbb{Z}$:

Proof: $\mathbb{C} \supseteq \mathbb{Z}[\sqrt{2}] = \mathbb{Z} \oplus \mathbb{Z}\sqrt{2} =: S$

Take $\alpha := z_1 + z_2\sqrt{2} \in S$.

$P_\alpha(X) := X^2 - 2z_1X + (z_1^2 - 2z_2^2)$

has α as a root. $\square$

(b) We will see that no other elements of $\mathbb{Q}(\sqrt{2})$ are integral over $\mathbb{Z}$.

(c) No element of $\mathbb{Q} \setminus \mathbb{Z}$ is integral over $\mathbb{Z}$.

<u>Proof:</u> $\alpha := \frac{p}{q} \in \mathbb{Q} \setminus \mathbb{Z}$ $\quad \gcd(p,q) = 1$

Assume α is integral over $\mathbb{Z}$. Then there exists a polynomial $P(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0 \in \mathbb{Z}[X]$ with $n \geq 1$ such that $P(\alpha) = 0$.

$$\Rightarrow \quad p^n + a_{n-1} q p^{n-1} + \dots + q^{n-1} p a_1 + q^n a_0 = 0$$

$\Rightarrow \quad \mathrm{rad}(q) \mid p \quad \Rightarrow \quad q \in \{\pm 1\}$ because $\gcd(p,q) = 1$. $\Rightarrow \alpha \in \mathbb{Z}$ ↯. $\square$

A first useful application of integral ring extensions is:

<u>Prop. 140:</u> Let $S|R$ be an integral ring extension of integral domains. Then are equivalent:

1° R is a field.

2° S is a field.

<u>Proof:</u> $1° \Rightarrow 2°$ $\quad \alpha \in S$ is integral over R.

$$\Rightarrow \exists_{n \in \mathbb{N}} \exists \; a_{n-1}, a_{n-2}, \dots, a_0 \in R:$$

$$\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_0 = 0$$

~~Sup~~ We choose n minimal.

Then $a_0 \neq 0$.

$$\Rightarrow \underbrace{a_0 \frac{1}{\alpha}}_{\in Q(S)} \in S \quad \underset{\substack{a_0 \text{ is} \\ \text{invertible in } R}}{\Rightarrow} \quad \frac{1}{\alpha} \in S.$$

$2^\circ \Rightarrow 1^\circ$ $\alpha \in R \Rightarrow \beta := \frac{1}{\alpha} \in S$ is integral over R.

$$\Rightarrow \exists_{n \in \mathbb{N}} \exists_{a_{n-1}, \dots, a_0 \in R} : \beta^n + a_{n-1}\beta^{n-1} + \dots + a_1\beta + a_0 = 0$$

$$\Rightarrow \beta \equiv_R -a_0\alpha^{n-1} - a_1\alpha^{n-2} - \dots - a_{n-1} \equiv_R 0.$$

$$\Rightarrow \beta \in R \qquad \square$$

For the basic properties integral ring extensions behave like field extensions.

<u>Prop 141:</u> (a) Let $S \rangle R$ be a ring extension and $\alpha \in S$.

Then are equivalent:

1° α is integral over R.

2° $R[\alpha] = \sum_{i=0}^{\infty} R\alpha^i$ is a finitely generated R-module.

3° $\exists_{S_1 | R}$: S_1 is a f.g. R-module and $\alpha \in S_1$.

(b) Let $S | S_2 | S_1 | R$ be a tower of ring ~~exent~~ extensions. Suppose $S_2 | S_1$ and $S_1 | R$ are integral. Then $S_2 | R$ is integral.

<u>Proof:</u> (a) $1^\circ \Rightarrow 2^\circ$ is easy. $\exists_{n\in\mathbb{N}} \exists a_{n-1},\dots,a_0 \in R$:

$$\alpha^n = a_{n-1}\alpha^{n-1} + \dots + a_0.$$

$$\Rightarrow \langle \{1, \alpha, \dots, \alpha^{n-1}\} \rangle_R = R[\alpha].$$

$$\| $$

$$R + R\alpha + \dots + R\alpha^{n-1}$$

$2^\circ \Rightarrow 3^\circ$ Take $S_1 = R[\alpha]$.

$3^\circ \Rightarrow 1^\circ$ Noether's determinant trick.

$$S_1 = R\alpha_1 + R\alpha_2 + \dots + R\alpha_\ell \ni \alpha.$$

Then $\begin{pmatrix} \alpha\alpha_1 \\ \vdots \\ \alpha\alpha_\ell \end{pmatrix} = A \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_\ell \end{pmatrix}$ for some $A \in R^{\ell\times\ell}$

$\Rightarrow$ Multiply $B := \alpha I_\ell - A$ with the cofactor matrix from the left.

$$\Rightarrow \det(\alpha I_\ell - A) \cdot \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_\ell \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

$1 \in S_1 = R\alpha_1 + \dots + R\alpha_\ell \Rightarrow \det(\alpha I_\ell - A) = 0.$

$\Rightarrow \alpha$ is integral over R.

(b) Take $\alpha \in S_2 \Rightarrow \exists_{n\in\mathbb{N}} \exists a_0,\dots,a_{n-1} \in S_1$:

α is integral over $R[a_0,\dots,a_{n-1}]$.

$a_0,\dots,a_{n-1}$ are integral over R. $\Rightarrow$

$R[a_0,\dots,a_{n-1}]$ is a finitely generated R-module

and $R[a_0, \dots, a_{n-1}, \alpha]$ is a f.g. $R[a_0, \dots, a_{n-1}]$-module, all by (a) ($1^\circ \Rightarrow 2^\circ$).

Now (a) ($3^\circ \Rightarrow 1^\circ$) implies that α is integral over R. $\square$

<u>Corollary 142:</u> Let $S|R$ be a ring extension.

The set

$$\bar{R}^S := \{\alpha \in S \mid \alpha \text{ is integral over } R\} \text{ is}$$

a subring of S, the "integral closure of R in S".

<u>Proof:</u> Exercise $\square$

<u>Proof for Example 140 (a):</u>

$$\alpha \in \mathbb{Q}(\sqrt{2}) = \mathbb{Q} \oplus \mathbb{Q}\cdot\sqrt{2} \qquad (\sqrt{2} \text{ is algebraic over } \mathbb{Q})$$

$$\alpha = z_1 + z_2\sqrt{2}$$

~~$\sqrt{2}$~~ Suppose α is integral over $\mathbb{Z}$.

<u>Case 1:</u> ($z_2 = 0$) $\Longrightarrow$ $\alpha \in \mathbb{Q} \overset{\alpha \text{ integral}/\mathbb{Z}}{\Longrightarrow} \alpha \in \mathbb{Z}$, by 140 (c).

<u>Case 2:</u> ($z_2 \neq 0$). $\beta := z_1 - z_2\sqrt{2}$.

$$P_2(X) := (X - \alpha)(X - \beta) = X^2 - 2z_1X + (z_1^2 - 2z_2^2)$$

is the minimal polynomial of α over $\mathbb{Q}$.

(degree 1 not possible, because $\alpha \notin \mathbb{Q}$.)

α is integral over $\mathbb{Z}$ $\Rightarrow \exists$ monic $P \in \mathbb{Z}[X]$:

$P(\alpha) = 0$.

P_α is irreducible in $\mathbb{Q}[X]$. $\Longrightarrow P_\alpha \mid P$ in $\mathbb{Q}[X]$

$\Rightarrow \exists Q \in \mathbb{Q}[X]$: $P_\alpha \cdot Q = P$.

⌜ <u>Claim</u>: $Q \in \mathbb{Z}[X]$.

<u>Proof</u>: Q is monic. $Q = (X - \alpha_1) \cdots (X - \alpha_\ell)$

in $\mathbb{C}[X]$, with $\alpha_1, \dots, \alpha_\ell \in \overline{\mathbb{Z}}^{\mathbb{C}}$. (They

are roots of P!)

$\Rightarrow$ The coefficients of Q are in $\overline{\mathbb{Z}}^{\mathbb{Q}} = \mathbb{Z}$.

$\square$ ⌟

$\Rightarrow \beta$ is a root of P. $\Rightarrow \beta \in \overline{\mathbb{Z}}^{\mathbb{Q}(\sqrt{2})}$.

$\Rightarrow \alpha + \beta = 2z_1$, $\alpha\beta = z_1^2 - 2z_2^2 \in \overline{\mathbb{Z}}^{\mathbb{Q}} = \mathbb{Z}$.

~~$\Rightarrow 8z_2^2$~~

Exercise $\Rightarrow z_1, z_2 \in \mathbb{Z}$. $\square$

$\downarrow$

($8z_2^2$ is an ~~even~~ integer $\Rightarrow (4z_2)^2$ is an even

integer $\Rightarrow 4z_2 \in 2\mathbb{Z} \Rightarrow 2z_2 \in \mathbb{Z}$.

$\Rightarrow 4z_1^2 \in 4\mathbb{Z} + 2(2z_2)^2 \subseteq 2\mathbb{Z}$

$\Rightarrow 2z_1 \in 2\mathbb{Z} \Rightarrow z_1 \in \mathbb{Z}$.

$\Rightarrow 2z_2^2 \in \mathbb{Z} \Rightarrow 4z_2^2 \in 2\mathbb{Z} \Rightarrow z_2 \in \mathbb{Z}$.)

<u>Prop. 143</u>: Let $d \in \mathbb{Z}^{>0}$ be squarefree and let $R \subseteq \mathbb{Q}(\sqrt{d})$ be the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$. Then

$$R = \begin{cases} \mathbb{Z}[\sqrt{d}], & \text{if } d \not\equiv_4 1 \\ \mathbb{Z}\left[\frac{\sqrt{d}-1}{2}\right], & \text{if } d \equiv_4 1 \end{cases}$$

<u>Proof</u>: Exercise. $\square$

A first application of the theory of integral ring extensions is Hilbert's Nullstellensatz.

<u>III 2. Hilbert's Nullstellensatz and consequences.</u>

<u>1st Motivation</u>: Let k be a field and $\mathfrak{a} \subsetneq k[X_1, \dots, X_n]$ an ideal. Does there exist an element of k^n which is a root of every polynomial in $\mathfrak{a}$?

<u>Answer</u>: In general not: $k = \mathbb{R}$. $\mathfrak{a} = (X^2+1)_{\mathbb{R}[X]} \subsetneq \mathbb{R}[X]$.

But X^2+1 has a root in $\mathbb{C}$. So what about algebraically closed fields?

<u>Answer</u>: If $k = \bar{k}$ (means k is alg. closed) then Yes!

Theorem 144: (Hilbert's Nullstellensatz)

Let k be an algebraically closed field and $\mathfrak{a} \subsetneq k[X_1, \dots, X_\ell]$ an ideal.

Then $\exists\, \underline{x} \in k^n : \forall P \in \mathfrak{a} : P(\underline{x}) = 0$.

Lemma 145: Let $K|k$ be a field ~~ext~~ extension and $x_1, \dots, x_\ell \in K$ s.t. $L := k(x_1, \dots, x_\ell) = k[x_1, \dots, x_\ell]$.

Then $L|k$ is algebraic.

end of lecture 20

Proof: $\ell = 1$: $\quad k[X_1] \xrightarrow[q]{P \mapsto P(x_1)} L = k[x_1]$ a field.

$\Rightarrow \ker(q) \neq (0)$ because L is a field, so $\neq k[X]$.

$\Rightarrow \exists\, Q \in \ker(q) \setminus \{0\} : \quad Q(x_1) = 0$.

$\Rightarrow x_1$ alg. over k. $\Rightarrow L|k$ algebraic.

$\ell > 1$: We have $k(x_1, \dots, x_\ell) = k[x_1, \dots, x_\ell]$ and we need to show $k(x_1, \dots, x_{\ell-1}) = k[x_1, \dots, x_{\ell-1}]$.

(Then we can use the induction hypothesis.)

We have to show that $k[x_1, \dots, x_{\ell-1}]$ is a field.

We have $k[x_1, \dots, x_\ell] = \underbrace{k[x_1, \dots, x_{\ell-1}]}_{=: \mathfrak{A}}[x_\ell] = L$

We have that $Q(M)[x_\ell] = L = Q(M)(x_\ell)$

$\Rightarrow$ x_ℓ is algebraic over $Q(M)$

$\Rightarrow \exists\ \tilde{P} = X^d + \frac{p_{d-1}}{q_{d-1}} X^{d-1} + \dots + \frac{p_1}{q_1} X + \frac{p_0}{q_0}$

$\in Q(M)[X]$ with $p_i \in M$, $q_i \in M \setminus \{0\}$: $\tilde{P}(x_\ell) = 0$.

Put $y := q_0 \cdots q_{d-1} \in M \setminus \{0\}$.

$\Rightarrow$ x_ℓ is integral over $M[\frac{1}{y}]$. So $M[\frac{1}{y}]$ is a field by Prop. 140. So w.l.o.g. $L = M[\frac{1}{y}]$.

Assume that M is not a field.

$$y \neq (0) \Longrightarrow \quad y \in r(0) \underset{\substack{\uparrow \\ \text{next Lemma}}}{=} \bigcap_{\mathfrak{m} \in \operatorname{Specm}(M)} \mathfrak{m}$$

$\Rightarrow \exists\ \mathfrak{m} \in \operatorname{Specm}(M)$: $y \notin \mathfrak{m}$.

$\bigcup_{i=1}^{\infty} \frac{1}{y^i} \mathfrak{m}$ is an ideal of $M[\frac{1}{y}] = L$

and non-zero.

$\Rightarrow \exists\ i_0 \in \mathbb{N}$: $\frac{1}{y^{i_0}} \mathfrak{m} \ni 1 \Rightarrow y^{i_0} \in \mathfrak{m}$

$\Rightarrow y \in \mathfrak{m}$ ↯

$\square$

Lemma 145-2: Let $S|R$ be an integral ring extension.

(1) $\forall\, \mathfrak{p} \in \mathrm{Spec}(R)\ \exists\, \mathfrak{q} \in \mathrm{Spec}(S): \mathfrak{q} \cap R = \mathfrak{p}$.

(2) $\forall\, \mathfrak{m} \in \mathrm{Spec}(R)\ \exists\, \mathfrak{q} \in \mathrm{Specm}(S): \mathfrak{q} \cap R = \mathfrak{m}$

(3) $\forall\, \mathfrak{q} \in \mathrm{Specm}(S): \mathfrak{q} \cap R \in \mathrm{Specm}(R)$.

(4) $\mathrm{Jac}(S) \cap R = \mathrm{Jac}(R)$.

(5) If R is an integral domain and $\mathrm{Jac}(R) = (0)$. Then $\mathrm{Jac}(S) = (0)$.

(6) Let k be a field and $R \supseteq k$ a ring extension (R Integraldomäne) and $x_1, \dots, x_e \in R$.

Then $\mathrm{Jac}(k[x_1, \dots, x_e]) = (0)$.

Proof: (1) $T := R \setminus \mathfrak{p}$.

$R_T \subseteq S_T$ is an integral ring extension. S_T contains a maximal ideal $\tilde{\mathfrak{q}}$. $\Rightarrow$ $\tilde{\mathfrak{q}} \cap R_T$ is a max ideal by Prop 140. $\Rightarrow$ $\tilde{\mathfrak{q}} \cap R_T = \mathfrak{p} R_T$

$\varphi_T : R \to R_T \qquad \mathfrak{p} = \varphi_T^{-1}(\mathfrak{p} R_T)$

$\psi_T : S \to S_T \qquad \mathfrak{q} := \psi_T^{-1}(\tilde{\mathfrak{q}})$

$$\Rightarrow \quad \mathfrak{q} \cap R = \mathrm{incl}_{R \subseteq S}^{-1}(\psi_T^{-1}(\tilde{\mathfrak{q}}))$$
$$= \varphi_T^{-1}(\mathrm{incl}_{R_T \subseteq S_T}^{-1}(\tilde{\mathfrak{q}}))$$
$$= \varphi_T^{-1}(\mathfrak{p} R_T) = \mathfrak{p}.$$

(2) $\mathfrak{m} = \mathfrak{q} \cap R$ for some $\mathfrak{q} \in \mathrm{Spec}(S)$

Prop 140 $\Rightarrow$ $\mathfrak{q}$ is maximal.

(3) By Prop 140.

(4) follows from (2) and (3)

(5) Suppose S is an integral domain and $\mathrm{Jac}(R) = (0)$.

<u>Assume</u> $\mathrm{Jac}(S) \neq (0)$

Then take $y \in \mathrm{Jac}(S) \setminus \{0\}$.

$\Rightarrow \exists\, n \in \mathbb{N} \ \exists\, a_0, \dots, a_{n-1} \in R$:

$$y^n + a_{n-1} y^{n-1} + \dots + a_1 y + a_0 = 0$$

Take n minimal. Then $a_0 \neq 0$.

And $a_0 \in \mathrm{Jac}(S) \cap R = \mathrm{Jac}(R) = (0)$ ↯.

(6) By induction on ℓ.

$\underline{\ell = 0}$: $\mathrm{Jac}(k) = (0)$, because $\mathrm{Specm}(k) = \{(0)\}$

$\underline{\ell > 0}$: $k[X_1, \dots, X_\ell] \twoheadleftarrow \sim \; k[X_1, \dots, X_\ell]/\mathfrak{a}$

$\underline{\text{Case } \mathfrak{a} = (0)}$: Then

$$\mathrm{Jac}(k[X_1, \dots, X_\ell]) \subseteq \{ p \in k[X_1, \dots, X_\ell] \mid 1 + p \in k[X_1, \dots, X_\ell]^\times \} \subseteq k$$

$$\Rightarrow \mathrm{Jac}(k[X_1, \dots, X_\ell]) = (0).$$

$\underline{\text{Case } \mathfrak{a} \neq (0)}$: ~~(Weierstraß preparation)~~

$\mathfrak{a}$ is a prime ideal and

$k[X_1, \dots, X_\ell] \subseteq \bar{k}[X_1, \dots, X_\ell]$ is

integral $\Rightarrow \exists\, \tilde{\mathfrak{a}} \in \mathrm{Spec}(\bar{k}[X_1, \dots, X_\ell])$:

$\tilde{\mathfrak{a}} \cap k[X_1, \dots, X_\ell] = \mathfrak{a}$.

By (4) we only have to show

$$\mathrm{Jac}\left(\bar{k}[X_1, \dots, X_\ell]/\tilde{\mathfrak{a}} \right) = (0).$$

So we can assume w.l.o.g. that k is algebraically closed.

(Weierstraß preparation):

Take $Q \in \mathfrak{a} \setminus \{0\}$. $\deg Q = d \geq 0$

Consider for $(\lambda_1, \dots, \lambda_\ell) \in k^\ell$ the k-algebra isomorphism:

$$k[X_1, \dots, X_\ell] \xrightarrow[\sim]{\varphi} k[X_1, \dots, X_\ell]$$

given by

$$X_1 \longmapsto \lambda_1 X_1$$
$$X_2 \longmapsto X_2 + \lambda_2 X_1$$
$$\vdots$$
$$X_\ell \longmapsto X_\ell + \lambda_\ell X_1.$$

$$\Rightarrow \quad Q \longmapsto Q_d(\lambda_1, \dots, \lambda_\ell) X_1^d + h_{d-1}(X_2, \dots, X_\ell) X_1^{d-1} + \dots + h_2(X_2, \dots, X_\ell) X_1^2 + h_1(X_2, \dots, X_\ell) X_1 + h_0(X_2, \dots, X_\ell).$$

$$(Q = Q_d + Q_{d-1} + \dots + Q_1 + Q_0)$$

degrees.

$|k| = \infty \Rightarrow \exists\, \underline{1} \in k^n : \; Q_d(\underline{1}) \neq 0.$

k alg. closed: $\exists\, \mu \in k : \; \mu^d = \dfrac{1}{Q_d(\underline{1})}.$

Now consider $X_1 \longmapsto \frac{1}{\mu} X_1$

$X_i \longmapsto X_i \quad \forall i = 2, \dots, \ell.$

Then $\varphi(Q)$ maps to X_1^d + lower degree in X_1 terms.

W.l.o.g. $Q = X_1^d$ + lower $\deg_{X_1}$ terms.

$$\Rightarrow \quad k[X_1, \dots, X_\ell] / \mathfrak{U} \supseteq k[X_1, \dots, X_\ell] / \mathfrak{U} \cap k[X_2, \dots, X_\ell]$$

is integral

$$(IH) \Rightarrow \operatorname{Jac}\left(k[X_2, \dots, X_\ell] / \mathfrak{U} \cap k[X_2, \dots, X_\ell] \right) = (0)$$

$$(5) \Rightarrow \operatorname{Jac}\left(k[X_1, \dots, X_\ell] / \mathfrak{U} \right) = (0) \qquad \square$$

$\Rightarrow \exists\, y \in M \setminus \{0\}\ \exists\, P \in M[X] \setminus M$ monic:

$P(yx_\ell) = 0$, i.e. yx_ℓ is integral over M.

$\Rightarrow \quad L = M[x_\ell] = M[yx_\ell] \mid M$ is integral,

because $M[yx_\ell] \mid M$ is finitely generated as an M-module.

L is a field $\overset{\text{Prop 140}}{\Longrightarrow}$ M is a field. $\square$

<u>Proof of Theorem 144:</u> Take $\mathfrak{a} \subsetneq k[X_1, \dots, X_\ell]$.

Then take $\mathfrak{m}$ maximal ideal s.t.

$\mathfrak{m} \supseteq \mathfrak{a}$.

We need to show that $\mathfrak{m}$ has a root in k^ℓ.

$K := k[X_1, \dots, X_\ell]/\mathfrak{m}$ a field. (because $\mathfrak{m}$ is maximal)

$$k \hookrightarrow K \qquad x_i := [X_i]_{\mathfrak{m}}, \quad i = 1, \dots, \ell.$$
$$x \longmapsto [x]_{\mathfrak{m}}$$

Then $K = k[x_1, \dots, x_\ell] = k(x_1, \dots, x_\ell)$.

Lemma 145 $\Rightarrow$ $K \mid k$ is algebraic $\overset{k = \bar{k}}{\Longrightarrow}$ $K = \bar{k} = k$.

$$\Rightarrow \exists\, a_1, \dots, a_\ell \in k : \forall_{i=1,\dots,\ell}\ X_i \equiv_{\mathfrak{M}} a_i .$$

i.e. $\forall_i\ X_i - a_i \in \mathfrak{M}$, i.e.

$$(X_1 - a_1, \dots, X_\ell - a_\ell) \subseteq \mathfrak{M} .$$

The first one is maximal, so $\mathfrak{M} = (X_1 - a_1, \dots, X_\ell - a_\ell)$ and has the root $(a_1, \dots, a_\ell)$ $\square$

<u>end of lecture 21</u>

<u>Remark</u>: (geometric interpretation)

Over algebraically closed fields we can identify ~~the~~ a variety with its Grothendieck spectrum.

<u>Def 146</u>: (1) Let R be a ring.

Then we have on $\mathrm{Spec}(R)$ a "Zariski"-topology:

"The closed sets are the sets

$$V^{Gd}(\mathfrak{A}) = \{ \mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{p} \supseteq \mathfrak{A} \}$$ "

"open sets: $D^{Gd}(\mathfrak{A}) := \{ \mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{p} \not\supseteq \mathfrak{A} \}$"

$V^{Gd}_{max}(\mathfrak{A}) = V^{Gd}(\mathfrak{A}) \cap \mathrm{Specm}(R)$

(2) Let k be a field and $\mathfrak{A} \subseteq k[X_1, \dots, X_\ell]$

Then we ~~have~~ consider the set:

$$V^{var}(\mathfrak{a}) := \{ \underline{x} \in k^\ell \mid \forall p \in \mathfrak{a} : p(\underline{x}) = 0 \}$$

(also for subsets $S \subseteq k[X_1, \dots, X_\ell]$
$V^{var}(S)$.)

The sets $V^{var}(\mathfrak{a})$, $\mathfrak{a} \subseteq k[X_1, \dots, X_\ell]$ ideal form the collection of closed sets for a topology (also called the "Zariski" topology on k^ℓ).
$\overset{\shortparallel}{\mathbb{A}^\ell_k}$

<u>Proof of 146(2):</u> $R := k[X_1, \dots, X_\ell]$

$$\emptyset = V^{var}(R)$$

$$k^n = V^{var}((0))$$

Let $\mathfrak{a}_1, \dots, \mathfrak{a}_t$ ideals of R.

$$\Rightarrow \quad V^{var}(\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_t) = V^{var}(\mathfrak{a}_1) \cup \ldots \cup V^{var}(\mathfrak{a}_t)$$

~~Is~~ So this union is closed.

Let $\mathfrak{a}_i$, $i \in I$, be ideals of R.

Then $\bigcap_{i \in I} V^{var}(\mathfrak{a}_i) = V^{var}(\sum_{i \in I} \mathfrak{a}_i)$.

$\square$

Now we attach to a variety a Grothendieck spectrum.

<u>Def 147:</u> $V/_k$ a variety in k^n, say $V = V^{var}(\mathfrak{a})$, $\mathfrak{a} \leq k[X_1, \dots, X_n]$

$I(V) := \{ p \in k[X_1, \dots, X_n] \mid p \text{ is zero on } V \}$

is called the vanishing ideal of V.

$k[V] := k[X_1, \dots, X_n] / I(V)$ is called the coordinate ring of V.

(It is generated by the "coordinates $x_1, \dots, x_n$", $x_i := [X_i]$)

So we have the Grothendieck spectrum

$\mathrm{Spec}(k[V])$.

<u>Question 148:</u> How are V and $\mathrm{Spec}(k[V])$ related to each other?

We have the following map

$$V \longrightarrow \mathrm{Specm}(k[V])$$
$$\underline{x} \longmapsto (\bar{X}_1 - x_1, \dots, \bar{X}_n - x_n)$$

<u>Theorem 149:</u> Let V be a non-empty variety over k.

(1) The map $V \longrightarrow \operatorname{Specm}(k[V])$ is injective and continuous

(2) Suppose $k = \bar{k}$, then it is a homeomorphism.

<u>Def. 150:</u> We consider a ring R and its Gothen dieck spectrum $\operatorname{Spec}(R)$.

(1) Let $T \subseteq \operatorname{Spec}(R)$.
We define $I(T) := I^{Gd}(T) := \bigcap_{\mathfrak{p} \in T} \mathfrak{p}$.

(Hopefully there is no confusion with the vanishing ideal of a variety)

~~Let~~ ~~For~~

<u>Theorem 150:</u> Let R be a ring, ~~V a variety over k~~. $V \neq \emptyset$ a variety/k

(1) For $\mathfrak{a} \trianglelefteq_R R$: $I(V^{Gd}(\mathfrak{a})) = \sqrt{\mathfrak{a}}$.

(2) For $\mathfrak{a} \trianglelefteq_{k[V]} k[V]$: $I(V^{Gd}_{max}(\mathfrak{a})) = \sqrt{\mathfrak{a}}$

(3) ~~For~~ Suppose $V = V^{var}(\mathfrak{b})$,
$\mathfrak{b} \trianglelefteq k[X_1, \dots, X_n]$ ideal.

Then
$$I^{Gd}(V^{Gd}(\mathfrak{b})) = I^{Gd}(V^{Gd}_{max}(\mathfrak{b})) = \sqrt{\mathfrak{b}}$$
$$\subseteq I(V). \text{ with equality if } k = \bar{k}$$

<u>Proof</u> (Theorem 149)

(1)
$$\begin{aligned} V &\xrightarrow{\varphi} \operatorname{Specm}(k[V]) \\ x &\longmapsto (\bar{X}_1 - x_1, \dots, \bar{X}_\ell - x_\ell) \end{aligned}$$

<u>continuity:</u> $W \subseteq \operatorname{Specm}(k[V])$ closed.

$\Rightarrow \exists\ \mathfrak{a} \subseteq k[V]$ ideal : $W = V^{Gal}_{max}(\mathfrak{a})$

$$\begin{aligned} \varphi^{-1}(W) &= \{ x \in k^\ell \mid (\bar{X}_1 - x_1, \dots, \bar{X}_\ell - x_\ell) \in W \} \\ &= \{ x \in V \mid (\bar{X}_1 - x_1, \dots, \bar{X}_\ell - x_\ell) \supseteq \mathfrak{a} \} \\ &= \{ x \in V \mid (x_1, \dots, x_\ell) \text{ is a root of } \mathfrak{a} \} \end{aligned}$$

(i.e. a root of $\tilde{\mathfrak{a}} \subseteq k[\bar{X}_1, \dots, \bar{X}_\ell]$ $\tilde{\mathfrak{a}}$ the preimage of $\mathfrak{a}$ in $k[\bar{X}_1, \dots, \bar{X}_\ell]$ and $k[\bar{X}_1, \dots, \bar{X}_\ell] \xrightarrow{\pi} k[V]$)

$$= V^{zar}(\tilde{\mathfrak{a}})$$

<u>injectivity:</u> $\underline{x}, \underline{y}$ s.t. $\varphi(\underline{x}) = \varphi(\underline{y})$

$$\Rightarrow (\bar{X}_1 - x_1, \dots, \bar{X}_\ell - x_\ell) + \mathfrak{a} = (\bar{X}_1 - y_1, \dots, \bar{X}_\ell - y_\ell) + \mathfrak{a}$$

in $k[\bar{X}_1, \dots, \bar{X}_\ell]$

$\underline{x} \in V = V^{zar}(\mathfrak{a}) \Rightarrow \mathfrak{a} \subseteq (\bar{X}_1 - x_1, \dots, \bar{X}_\ell - x_\ell)$

Thus $(\bar{X}_1 - x_1, \dots, \bar{X}_\ell - x_\ell) = (\bar{X}_1 - y_1, \dots, \bar{X}_\ell - y_\ell)$

Plugin $\underline{x}$ in $P := \bar{X}_1 - y_1$. $\Rightarrow 0 = P(\underline{x}) = x_1 - y_1$

$\Rightarrow x_1 = y_1$. Analogously $\underline{x} = \underline{y}$.

(2) Suppose $k = \bar{k}$.

<u>Surjectivity:</u> Take $\mathfrak{m} \in \mathrm{Specm}(k[V])$.

$\tilde{\mathfrak{m}} := \pi^{-1}(\mathfrak{m})$.

HNS $\Rightarrow \exists\, \underline{x} \in k^\ell : \tilde{\mathfrak{m}} = (X_1 - x_1, \dots, X_\ell - x_\ell)$

$\tilde{\mathfrak{m}} \supseteq \pi^{-1}((0)) = I(V) \supseteq \mathfrak{a}$.

$\Rightarrow \forall p \in \mathfrak{a}: \quad p(\underline{x}) = 0. \Rightarrow \underline{x} \in V = V^{\mathrm{Zar}}(\mathfrak{a})$

$\Rightarrow \mathfrak{m} = (\bar{X}_1 - x_1, \dots, \bar{X}_\ell - x_\ell) \in \varphi(V)$.

<u>Closedness:</u> Let $W^{\mathrm{Zar}} \subseteq V = V^{\mathrm{Zar}}(\mathfrak{a})$ be a Zariski-closed subset of V.

$\Rightarrow \exists\, \tilde{\mathfrak{b}} \supseteq \mathfrak{a}$ ideal of $k[X_1, \dots, X_\ell]$: $W^{\mathrm{Zar}} = V^{\mathrm{Zar}}(\tilde{\mathfrak{b}})$.

$$\varphi(W^{\mathrm{Zar}}) = \{ (\bar{X}_1 - x_1, \dots, \bar{X}_\ell - x_\ell) \mid \underline{x} \in W^{\mathrm{Zar}} \}$$

$$= \{ \quad \text{—"—} \quad \mid (X_1 - x_1, \dots, X_\ell - x_\ell) \supseteq \tilde{\mathfrak{b}} \text{ and } \underline{x} \in k^\ell \}$$

$$\underset{\text{HNS.}}{=} \{ \pi(\tilde{\mathfrak{m}}) \mid \tilde{\mathfrak{m}} \in V^{\mathrm{Zar}}_{\max}(\tilde{\mathfrak{b}}) \}$$

$$= \{ \mathfrak{m} \mid \mathfrak{m} \in V^{\mathrm{Zar}}_{\max}(\pi(\tilde{\mathfrak{b}})) \}$$

$$= V^{\mathrm{Zar}}_{\max}(\pi(\tilde{\mathfrak{b}})). \qquad \square$$

Proof (Theorem 151):

(1) by Theorem 51.

(2) $\mathfrak{a} \leq_{k[V]} k[V]$.

$k[V]/\mathfrak{a}$ is a finitely generated algebra over a field k. Exercise (Krull's intersection theorem) $\Longrightarrow$ $\mathrm{Jac}(k[V]/\mathfrak{a}) = \mathrm{Nil}(k[V]/\mathfrak{a})$

$$\mathrm{Nil}(k[V]/\mathfrak{a}) = \sqrt{\mathfrak{a}}/\mathfrak{a}$$

$$\Longrightarrow \bigcap_{\mathfrak{m} \in V^{Gd}_{max}(\mathfrak{a})} \mathfrak{m} = \sqrt{\mathfrak{a}}.$$

(3) $\mathfrak{b} \leq k[X_1, \dots, X_\ell]$ s.t. $V = V^{Zar}(\mathfrak{b}) \subseteq k^\ell$.

$$I^{Gd}(V^{Gd}(\mathfrak{b})) = \sqrt{\mathfrak{b}} \underset{(2)}{=} I^{Gd}(V^{Gd}_{max}(\mathfrak{b}))$$

$$\cancel{\subseteq I^{Gd}(\mathcal{C}(V^{Zar}(\mathfrak{b}))) = \bigcap}$$

~~maybe less maximal ideals.~~

$$= \bigcap_{\substack{\mathfrak{m} \in \mathrm{Specm}(k[X_1, \dots, X_\ell]) \\ \mathfrak{m} \supseteq \mathfrak{b}}} \mathfrak{m} \subseteq \bigcap_{x \in V^{Zar}(\mathfrak{b})} (X_1 - x_1, \dots, X_\ell - x_\ell) = I(V^{Zar}(\mathfrak{b})).$$

The inclusion "$\subseteq$" is an equality if $k = \bar{k}$, because then every maximal ideal of $k[X_1, \dots, X_\ell]$ has the form $(X_1 - x_1, \dots, X_\ell - x_\ell)$.

end of lecture 22

151-1

<u>Remark</u>: 1) Let k be a field $k \neq \bar{k}$ and

$P_1, \dots, P_e \in k[X_1, \dots, X_n]$.

$V := V(P_1, \dots, P_e) = \{ x \in k^n \mid P_1(x) = \dots = P_e(x) = 0 \}$

$k[V] = k[X_1, \dots, X_n] / I(V)$ is not

the right coordinate ring to look at.
It can have no information about $(P_1, \dots, P_e)$.

Better idea:

$\tilde{V} = V_{\bar{k}}(P_1, \dots, P_e) \subseteq \bar{k}^n$.

$k[\tilde{V}] := k[X_1, \dots, X_n] / I(\tilde{V}_{\bar{k}}) \cap k[X_1, \dots, X_n]$.

2) <u>Example</u>:

2.1) $P_1 = P = X^p - T \qquad k = \mathbb{F}_p(T)$.

$k[\tilde{V}] = k[X] / (X^p - T)$

$k[V] = k[X] / k[X]$ 0-ring.

~~2.2)~~

3) φ not a homeomorphism. $V = \mathbb{R}^1 = V((0))$

$\mathrm{Specm}(\underbrace{\mathbb{R}[V]}_{\simeq \mathbb{R}[X]})$ contains max. ideals different from $(X - r)$, $r \in \mathbb{R}$.

<u>Example 152:</u>

(a) $R := \mathbb{Z}_{(p)} = \{ \frac{a}{b} \in \mathbb{Q} \mid a \in \mathbb{Z}, b \in \mathbb{Z}, p \nmid b \}$

(p a prime number)

R is a local integral domain.

$\mathrm{Jac}(R) = p\,\mathbb{Z}_{(p)}$

$\mathrm{Nil}(R) = (0)$.

(b) In (a) we have $\mathbb{Z} = \bigcap_{\substack{p \text{ prime} \\ \text{number.}}} \mathbb{Z}_{(p)}$

Exercise: Show that an integral domain satisfies:

$$R = \bigcap_{\substack{\mathfrak{m} \\ \in \\ \mathrm{Specm}(R)}} R_{\mathfrak{m}}.$$

(c) Transfer from positive characteristic to characteristic 0.. Given $\overline{\mathbb{F}}_p$ we want to realize it as a quotient of a subring of $\mathbb{C}$.

$R := \overline{\mathbb{Z}}_{(p)}^{\mathbb{C}} \supsetneq \mathfrak{m}$ a maximal ideal containing $p\,\mathbb{Z}_{(p)}$

<u>Claim:</u> $R/\mathfrak{m} \simeq \overline{\mathbb{F}}_p$.

<u>Proof:</u> $R/\mathfrak{m} \mid \mathbb{F}_p$ is integral, so algebraic. So we get a field embedding

$$R/\mathfrak{m} \hookrightarrow \overline{\mathbb{F}_p}.$$

Surjectivity: $\overline{\mathbb{F}_p} = \bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^n}$.

$\mathbb{F}_{p^n} = \mathbb{F}_p[x_n]$ where x_n is an element of $\overline{\mathbb{F}_p}$ satisfying $\underbrace{X^{p^n} - X}_{=: P_n} = 0$.

Take a root ζ_n of P_n in $\mathbb{C}$. (seeing P_n as a polynomial in $\mathbb{C}[X]$) which does not satisfy any P_m with $m \in \mathbb{N} < n$. (primitive e.g. $p^n - 1$ -th root of unity in $\mathbb{C}$)

Then $\zeta_n \in R$ and $[\zeta_n]_{\mathfrak{m}}$ generates $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$.

$\square$

How to use it? Let G be a finite group and $\rho : G \longrightarrow GL_m(\overline{\mathbb{F}_p})$ a group homomorphism. "$(\rho, \overline{\mathbb{F}_p}^m)$ is called a representation of G."

III 3. Going up and going down lemma.

<u>Recall:</u> Given a ring R and $\mathfrak{p} \in \operatorname{Spec}(R)$ we have the height of $\mathfrak{p}$:

$$\operatorname{ht}(\mathfrak{p}) := \max\{n \in \mathbb{N}_0 \mid \exists\, \mathfrak{p}_0, \mathfrak{p}_1, \dots, \mathfrak{p}_{n-1} \in \operatorname{Spec}(R):$$

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_{n-1} \subsetneq \mathfrak{p}_n := \mathfrak{p}\}$$

and the Krull dimension:

$$\dim_{\text{Krull}}(R) = \sup\{\operatorname{ht}(\mathfrak{p}) \mid \mathfrak{p} \in \operatorname{Spec}(R)\}$$

<u>Question:</u> Let $K|\mathbb{Q}$ be an algebraic extension of finite degree ("finite extension"). Put

$$\mathcal{O}_K := \overline{\mathbb{Z}}^{\mathbb{Q}}.$$

What is the Krull dimension of $\mathcal{O}_K$?

<u>Theorem 153</u> (Going up lemma from Cohen-Seidenberg)

Let $S|R$ be an integral ring extension, $\mathfrak{p}_1, \mathfrak{p}_2 \in \operatorname{Spec}(R)$, $\mathfrak{q}_1 \in \operatorname{Spec}(S)$ such that $\mathfrak{q}_1 \cap R = \mathfrak{p}_1 \subsetneq \mathfrak{p}_2$.

Then we have two characters (traces)

① $\mathrm{tr}_\rho(g) := \mathrm{tr}(\rho(g))$

② $G_0 := \{g \in G \mid p \nmid \mathrm{ord}(g)\}$

$\Rightarrow \forall g \in G_0 : \rho(g)$ is conjugate

to $\begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_m \end{pmatrix}$ with $\lambda_1, \dots, \lambda_m$

roots of unity in $\mathbb{C}$.

Define $\chi_\rho(g) := \sum_{i=1}^{m} \lambda_i \quad , g \in G_{0p}$

χ_ρ is called the Brauer character of G.

Then $\exists\, \mathfrak{q}_2 \supsetneq \mathfrak{q}_1$ prime ideal in S: $\mathfrak{q}_2 \cap R = \mathfrak{p}_2$

<u>Proof:</u> $R/\mathfrak{p}_1 \subseteq S/\mathfrak{q}_1$ is integral. Take a prime ideal

$\overline{\mathfrak{q}}_2$ of $S/\mathfrak{q}_1$ s.t. $\overline{\mathfrak{q}}_2 \cap R/\mathfrak{p}_1 = \overline{\mathfrak{p}}_2$.

$\mathfrak{q}_2 := \pi_S^{-1}(\overline{\mathfrak{q}}_2)$ $\quad \pi_S : S \longrightarrow S/\mathfrak{q}_1$ $\quad \square$

<u>Prop 154:</u> Let $S|R$ be an integral ring extension. and $\mathfrak{q}_2 \supsetneq \mathfrak{q}_1$ prime ideals in S. Then

$\mathfrak{q}_2 \cap R \neq \mathfrak{q}_1 \cap R$.

<u>Proof:</u> follows from Prop 140:

If $\mathfrak{q}_2 \cap R = \mathfrak{q}_1 \cap R =: \mathfrak{p}$. $T := R \setminus \mathfrak{p}$.

$S_T | R_T$ is integral and $\mathfrak{q}_{iT}$ is max

imal for $i = 1, 2$. $\Longrightarrow$ $\mathfrak{q}_{1T} = \mathfrak{q}_{2T} \Rightarrow \mathfrak{q}_1 = \mathfrak{q}_2$ ↯

$\square$

<u>Corollary 155:</u> Let $S|R$ be an integral ring extension. Then $\dim_{Krull}(S) = \dim_{Krull}(R)$.

<u>Proof:</u> Follows from Prop. 154, Thm. 153 and Lemma 145-2(1) $\square$

<u>Example 156:</u> $K|\mathbb{Q}$ finite field extension.

$$\Rightarrow \dim_{Krull}(\underset{\overset{\shortparallel}{\mathbb{Z}^K}}{\mathcal{O}_K}) = \dim_{Krull}(\mathbb{Z}) = 1.$$

So every non-zero prime ideal of $\mathcal{O}_K$ is maximal.

<u>Def 157:</u> (1) An integral domain R is called normal if $\overline{R}^{Q(R)} = R$. (give examples.)

(2) A normal noetherian integral domain of Krull dimension 1 is called Dedekind domain.

($\mathcal{O}_K$ above is a Dedekind domain)

There is a fact for Dedekind domains from "Algebraic Number Theory".

<u>Theorem 158:</u> Let R be a Dedekind domain and $\mathfrak{a}$ be a non-~~zero~~ zero ideal of R. Then $\exists_{l \in \mathbb{N}_0}\ \exists\ \mathfrak{p}_1, \dots, \mathfrak{p}_l \in \mathrm{Spec}(R)$:

$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_l$ and this decomposition is unique upto permutation of the factors $\mathfrak{p}_i$. (We do not prove this here.)

Example 159: $(6)_{\mathbb{Z}[\sqrt{-5}]} = (2, 1+\sqrt{-5})^2 \cdot (3, 1+\sqrt{-5}) \cdot (3, 1-\sqrt{-5})$

We also have a going down Lemma:

Theorem 160 (Krull's going down lemma)

Let $S|R$ be an integral extension of integral domains and suppose R is normal.

Let $\mathfrak{p}_1 \supsetneq \mathfrak{p}_0$ be prim ideals of R and $\mathfrak{q}_1 \in \operatorname{Spec}(S)$ s.t. $\mathfrak{q}_1 \cap R = \mathfrak{p}_1$.

Then $\exists\, \mathfrak{q}_0 \in \operatorname{Spec}(S)$: $\mathfrak{q}_0 \cap R = \mathfrak{p}_0$.

Lemma 161: Let $S|R$ be a ring extension and $\mathfrak{a} \trianglelefteq_R R$.

Define $\overline{\mathfrak{a}}^S := \{ s \in S \mid \exists\, \ell \in \mathbb{N}\ \exists\, a_0, \dots, a_{\ell-1} \in \mathfrak{a}: s^\ell + \sum_{i=0}^{\ell-1} a_i s^i = 0 \}$

Then $\overline{\mathfrak{a}}^S = \sqrt{\mathfrak{a}\overline{R}^S} \subseteq \overline{R}^S$

end of lecture 23

Proof: "$\supseteq$" $b \in \sqrt{\mathfrak{a}\overline{R}^S} \Rightarrow \exists\, n \in \mathbb{N}: b^n = \sum_{i=1}^{\ell} a_i c_i$ with $a_i \in \mathfrak{a}$ and $c_i \in \overline{R}^S$.

$R[c_1, \dots, c_\ell]$ is f.g. over R, because $c_1, \dots, c_\ell$ are integral over R, say

$R[c_1, \dots, c_\ell] = R r_1 + \dots + R r_t$

$$\Rightarrow \quad b^n \eta_i = \sum_{j=1}^{t} \alpha_{ij} \eta_j \quad \text{with } \alpha_{ij} \in \mathfrak{a}$$

$$\left(b^n \eta_i \in \mathfrak{a} R[c_1, \dots, c_\ell] = \mathfrak{a}\eta_1 + \dots + \mathfrak{a}\eta_t \right)$$

Noether's determinant trick

$$\Rightarrow \quad b^n \in \overline{\mathfrak{a}}^S \Rightarrow b \in \overline{\mathfrak{a}}^S.$$

"$\subseteq$" $\quad b \in \overline{\mathfrak{a}}^S \Rightarrow \exists_{\ell \in \mathbb{N}} \exists a_0, \dots, a_{\ell-1} \in \mathfrak{a}$

$$b^\ell + \sum_{i=0}^{\ell-1} a_i b^i = 0$$

$$\Rightarrow b^\ell \in \mathfrak{a} \cdot \overline{R}^S \Rightarrow b \in \sqrt{\mathfrak{a} \overline{R}^S} \quad \square$$

$\uparrow$

$b^i \in \overline{\mathfrak{a}}^S \subseteq \overline{R}^S$

<u>Lemma 1.62</u> Let $\varphi : R \to S$ be a ring homomorphism with $\varphi(1) = 1$. Then we set $\varphi^* : \operatorname{Spec}(S) \to \operatorname{Spec}(R)$ via $\varphi^*(\mathfrak{q}) = \varphi^{-1}(\mathfrak{q})$.

Then

$$\operatorname{im}(\varphi^*) = \{ \mathfrak{p} \in \operatorname{Spec}(R) \mid \varphi^{-1}(\varphi(\mathfrak{p}) S) = \mathfrak{p} \}$$

<u>Proof</u>: (Exercise)

Hint: For "$\supseteq$" localize w.r.t. $\varphi(A \setminus \mathfrak{p})$. $\square$

<u>Remark 163:</u> Let R be a normal integral domain, $\mathfrak{a} \trianglelefteq_R R$ and $\alpha \in \overline{\mathfrak{a}}^{\overline{Q(R)}}$ ($\overline{Q(R)}$ an algebraic closure of $Q(R)$.)

Then the minimal polynomial $\mu_{\alpha, Q(R)} \in Q(R)[X]$ has all coefficients in $\sqrt{\mathfrak{a}}$ except the leading one.

<u>Proof:</u> The roots of $\mu_{\alpha, Q(R)}$ are integral over $\mathfrak{a}$, so the coeff. of $\mu_{\alpha, Q(R)}$ too (except the leading one)

$$\mu_{\alpha, Q(R)} = X^n + a_{n-1}X^{n-1} + \dots + a_1 X + a_0$$

$$\Rightarrow \quad a_i \in \overline{\mathfrak{a}}^{Q(R)} = \sqrt{\mathfrak{a}\overline{R}^{Q(R)}}$$

$$\underset{\substack{\uparrow \\ R \text{ is normal}}}{=} \sqrt{\mathfrak{a} R} = \sqrt{\mathfrak{a}}. \quad \square$$

Proof of Theorem 160

$\mathfrak{p}_1 \supsetneq \mathfrak{p}_0$ in $\operatorname{Spec}(R)$, $\mathfrak{q}_1 \in \operatorname{Spec}(S)$

$\mathfrak{q}_1 \cap R = \mathfrak{p}_1$. We want $\mathfrak{q}_0$ with $\mathfrak{q}_0 \cap R = \mathfrak{p}_0$

Consider
$$\begin{tikzcd} R \arrow[r, hook] \arrow[rr, hook, bend right, "i"'] & S \arrow[r, hook] & S_{\mathfrak{q}_1} \subseteq Q(S) \end{tikzcd}$$

To show $i^{-1}(i(\mathfrak{p}_0) S_{\mathfrak{q}_1}) = \mathfrak{p}_0$

$$\begin{array}{c} \shortparallel \\ R \cap \mathfrak{p}_0 S_{\mathfrak{q}_1} \end{array}$$

"$\supseteq$" ✓

"$\subseteq$" $\frac{p}{t} \in R \cap \mathfrak{p}_0 S_{\mathfrak{q}_1}$ $\quad \frac{p}{t} = \frac{r}{1}$, $r \in R$, $p \in \mathfrak{p}_0 S$

<u>To show:</u> $r \in \mathfrak{p}_0$.

- We have $tr \in \mathfrak{p}_0 S$ and
  $tr \in \mathfrak{p}_0 S \subseteq \mathfrak{q}_1$, i.e. $r \in \mathfrak{q}_1$.
  $\Rightarrow r \in \mathfrak{q}_1 \cap R = \mathfrak{p}_1$.
- $tr = p \in \mathfrak{p}_0 S \subseteq \sqrt{\mathfrak{p}_0 S} = \sqrt{\mathfrak{p}_0 \overline{R}^S} = \overline{\mathfrak{p}_0}^S$

R normal $\overset{\text{Lemma 163}}{\Longrightarrow}$ $\exists\, \ell \in \mathbb{N}\ \exists\, a_0, \dots, a_{\ell-1} \in \mathfrak{p}_0$:
$(tr)^\ell + a_{\ell-1}(tr)^{\ell-1} + \dots + a_1(tr) + a_0 = 0$

is the equation given by the minimal polynomial $\mu_{tr, Q(R)}$.

W.l.o.g. $r \neq 0$. Then $\mu_{t, Q(R)}(X) = \mu_{tr, Q(R)}(rX) \cdot \frac{1}{r^l}$

$t \in \overline{R}^S$ and R is normal

$\overset{\text{Lemma 163}}{\Longrightarrow}$ coeff. of $\mu_{t, Q(R)}$ are all in R.

$$\Longrightarrow \forall_{i=0,\dots,l-1}: \quad \frac{a_i r^i}{r^l} \in R$$

Now $\forall_{i=0,\dots,l-1}: \quad r^{l-i} \cdot \left(\frac{a_i r^i}{r^l}\right) = a_i \in \mathfrak{p}_0$

Thus $\underset{(\mathrm{I})}{r \in \mathfrak{p}_0}$ or $\underset{(\mathrm{II})}{\forall_{i=0,\dots,l-1} \left(\frac{a_i r^i}{r^l}\right) \in \mathfrak{p}_0}$

Assume II $\Longrightarrow t \in \overline{\mathfrak{p}_0}^S = \sqrt{\mathfrak{p}_0 S} \subseteq \mathfrak{q}_1$ ↯

□

<u>Example 164:</u> $\dim_{Krull}(k[X_1, \dots, X_n]) = n$, k a field.

<u>Proof:</u> <u>$n=0$:</u> $\dim_{Krull} k = 0$

<u>$n=1$:</u> $\dim_{Krull} k[X] = 1$ because every non-zero prime ideal is maximal.

<u>$n > 1$:</u> w.l.o.g. $k = \bar{k}$. Take a chain of prime ideals

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_\ell \quad \text{in } k[X_1, \dots, X_n]$$

with $\mathfrak{p}_0 = (0)$.

$\mathfrak{p}_1$ contains an irreducible polynomial P.

Weierstraß preparation

$$\Rightarrow \text{W.l.o.g.} \quad \underbrace{k[X_1, \dots, X_n]/(P)}_{=:S} \;\Big|\; \underbrace{k[X_1, \dots, X_{n-1}]/(P) \cap k[X_1, \dots, X_n]}_{=:R}$$

is integral

$$\dim_{\text{Krull}} R \leq \dim_{\text{Krull}} k[X_1, \dots, X_{n-1}] \underset{\text{(IH)}}{=} n-1$$

$$\Rightarrow \dim_{\text{Krull}} S \leq n-1 \Rightarrow \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_\ell$$

~~contains~~ consists of at most n prime ideals,

i.e. $\ell \leq n$. $\square$

IV Completion & Hensel's Lemma

IV 1. Topology given by a filtration

Def 165: Let G be a group and

$$G \geq H_1 \geq H_2 \geq H_3 \geq \dots \quad \text{be}$$

a "filtration" of normal subgroups of G.

(A "filtration" of groups is a sequence of groups $(G_i)_{i\in\mathbb{N}}$ s.t. $G_1 \geq G_2 \geq G_3 \geq \dots$)

$$\mathcal{T} := \mathcal{T}_{\underline{H}} := \{ U \subseteq G \mid \forall u \in U \ \exists n \in \mathbb{N} : uH_n \subseteq U \}$$

is called the "Krull topology" on G w.r.t. $\underline{H} := (H_i)_{i\in\mathbb{N}}$.

Lemma 166: Let G be a group and $\underline{H} = (H_i)_{i\in\mathbb{N}}$ be a filtration of normal subgroups of G.

(i) $\cdot : G \times G \to G$ and $()^{-1} : G \to G$ are continuous w.r.t. $\mathcal{T}_{\underline{H}}$

(ii) G is Hausdorff w.r.t. $\mathcal{T}_{\underline{H}}$ $\iff$ $\{1_G\} = \bigcap_{i=1}^{\infty} H_i$

<u>Proof:</u> (i) $\varphi := *$ We only need to show that $\varphi^{-1}(gH_n)$ is open for all $g \in G$ and $n \in \mathbb{N}$.

$(g_1, g_2) \in \varphi^{-1}(gH_n) \Rightarrow gH_n = g_1 g_2 H_n$

$\Rightarrow \varphi(g_1 H_n \times g_2 H_n) = g_1 H_n g_2 H_n \underset{\substack{\uparrow \\ H_n \trianglelefteq G}}{=} g_1 g_2 H_n = gH$

$\Rightarrow g_1 H_n \times g_2 H_n \subseteq \varphi^{-1}(gH)$ containing (g_1, g_2)

$\overset{(g_1, g_2) \text{ arbitrary}}{\Rightarrow} \varphi^{-1}(gH_n)$ is open.

The continuity of the inverse-map: $g \mapsto g^{-1}$ is an exercise.

(ii) Recall: Separation axioms: (X, τ) topol. space.

<u>T0:</u> $\forall_{x,y \in X} \exists_{U \in \tau}: (x \in U \wedge y \notin U)$ or $(y \in U \wedge x \notin U)$

<u>T1:</u> $\forall_{x,y \in X} \exists_{U_1, U_2 \in \tau}: x \in U_1 \setminus U_2$ and $y \in U_2 \setminus U_1$.

$(\Leftrightarrow \forall_{x \in X}: \{x\}$ is closed.$)$

<u>T2</u> (Hausdorff): $\forall_{x,y \in X}: \exists U_1, U_2 \in \tau:$ $x \in U_1, y \in U_2 \wedge U_1 \cap U_2 = \emptyset$

"$\Rightarrow$" To show $\bigcap_{i=1}^{\infty} H_i = \{1_G\}$.

$x \in \bigcap_{i=1}^{\infty} H_i$. Assume $x \neq 1_G$.

$\Rightarrow \exists U_1, U_2 \in \tau_{\underline{H}}$ disjoint: $x \in U_1 \wedge 1_G \in U_2$

$\Rightarrow \exists g_1, g_2 \in G \; \exists H_{n_1}, H_{n_2}$: $x \in g_1 H_{n_1} \subseteq U_1$

$1_G \in g_2 H_{n_2} \subseteq U_2$

We can take $g_1 = x$ and $g_2 = 1_G$. and $n_1 = n_2 =: n$.

$\Rightarrow H_n \cap U_1 \subseteq U_2 \cap U_1 = \emptyset$ and

$x \in \left(\bigcap_{i=1}^{\infty} H_i\right) \cap U_1 \subseteq H_n \cap U_1$ ↯.

"$\Leftarrow$" <u>Note:</u> All sets gH_n are ~~open~~ closed and open. (Why?)

Thus G is T_1 because $\forall g \in G: \{g\} = \bigcap_{n=1}^{\infty} gH_n$

<u>T_2:</u> Take $g_1, g_2 \in G$ different.

$\Rightarrow g_2^{-1} g_1 \neq 1_G \Rightarrow \exists n \in \mathbb{N}: g_2^{-1} g_1 \notin H_n$

$\Rightarrow g_2 H_n \cap g_1 H_n = \emptyset$. □

End of lecture 24

<u>Def 167:</u> (a) A sequence $(g_n)_{n \in \mathbb{N}}$ is called a Cauchy sequence w.r.t. $\underline{H}$ if $\forall n \in \mathbb{N}$ $\exists M \in \mathbb{N}$ $\forall m_1, m_2 \in \mathbb{N}$ $m_1, m_2 \geq M$: $g_{m_2}^{-1} g_{m_1} \in H_n$.

(b) A sequence $(g_m)_{m\in\mathbb{N}}$ is called a 1_G-sequence (or null-sequence in case of abelian groups) if $g_n \xrightarrow{n\to\infty} 1_G$.

<u>Lemma 188</u>: Given $\underline{H}$ for G then

(i) $\mathrm{Cauchy}(G,\underline{H}) := \{(g_m)_{m\in\mathbb{N}} \mid (g_n)$ a Cauchy sequence$\}$ is a group with normal subgroup $\mathrm{null}(G,\underline{H}) := \{(g_n) \mid g_n \xrightarrow{n\to\infty} 1_G\}$.

(ii) Consider the group $\overline{G}_{\underline{H}} := \mathrm{Cauchy}(G,\underline{H}) / \mathrm{null}(G,\underline{H})$.

Then
$$H_n := \{[(g_m)] \mid \exists_{\mu\in\mathbb{N}} : \forall_{m\geq\mu} : g_m \in H_n\}$$
is a normal subgroup of $\overline{G}_{\underline{H}}$.

(iii) $\overline{G}_{\underline{H}}$ is <u>complete</u> w.r.t. $(H_n)_{\mathbb{N}} =: \underline{H}$ and $\overline{G}_{\underline{H}}$ is Hausdorff.

(iv) The image of $G \xrightarrow{g \mapsto [(g)]} \overline{G}_{\underline{H}}$ is dense.

<u>Proof:</u> (i) trivial.

(ii) ✓

(iii) At first: If $[(g_n)] \in \bigcap_{n=1}^{\infty} \overline{H_n}$ then

$$\forall_n \; \exists_{\mu(n)} \; \forall m \geq \mu(n) : 1_G^{-1} g_m \in H_n.$$

i.e. $(1_G) \equiv (g_m)_{\mathbb{N}}$ mod null$(G, \underline{H})$

i.e. $(g_m)_{\mathbb{N}}$ is a 1_G-sequence.

$$\Rightarrow \quad [(g_m)] = [(1_G)].$$

Now let $[(g_m^{(n)})]$, $n \in \mathbb{N}$, be a Cauchy sequence in $\overline{G}_{\underline{H}}$ w.r.t. $\underline{H}$.

Write $\underline{g}^{(n)}$ for $(g_m^{(n)})_{\mathbb{N}}$.

W.l.o.g. we can assume

$$g_m^{(n)-1} g_\ell^{(n)} \in H_m \quad \forall_{m \in \mathbb{N}} \forall_{\ell \geq m}.$$

(Why?)

$\underline{g}^{(1)}$: $g_1^{(1)}, g_2^{(1)}, g_3^{(1)}, \dots$

$\underline{g}^{(2)}$: $g_1^{(2)}, g_2^{(2)}, g_3^{(2)} \dots$

$\vdots$

<u>Note:</u> We have $g_m^{(n)} H_m = g_{m+1}^{(n)} H_m = g_{m+2}^{(n)} H_m = \dots$
$= g_\ell^{(n)} H_m \ \forall \ell \geq m.$

We need a limit $\underline{g}$.

<u>$i=1$:</u> (Define g_1): $(\underline{g}^{(n)})_n$ is Cauchy w.r.t $\overline{\underline{H}}$,

$\Rightarrow \exists_{M(1)} : \forall_{\ell, n \geq M(1)} : (\underline{g}^{(n)})^{-1} \underline{g}^{(\ell)} \in \overline{H}_1$

Exercise $\Rightarrow \forall_{\ell, n \geq M(1)} \ \forall_{j \in \mathbb{N}} : g_j^{(n)^{-1}} \cdot g_j^{(\ell)} \in H_1$.

So $g_1^{(M(1))} = g_1^{(M(1)+1)} = g_1^{(n)} \ \forall_{n \in \mathbb{N}, n \geq M(1)}$.

Put $g_1 := g_1^{M(1)}$

<u>$i > 1$:</u> We have defined $g_1, \dots, g_{i-1}$ and $M(1), \dots, M(i-1)$

Cauchy $\Rightarrow \exists_{M(i) \geq M(i-1)} \forall_{\ell, n \geq M(i)}$

$\forall_{j \geq i} : g_j^{(n)^{-1}} g_j^{(\ell)} \in H_i$.

Put $g_i := g_i^{(M(i))}$.

<u>Claim</u> ① $\underline{g}$ is a Cauchy sequence in G.

② $[\underline{g}^{(n)}] \xrightarrow{n\to\infty} [\underline{g}]$.

<u>Proof</u>: Exercise. $\square$ (iii)

(iv) Take $[(g_n)] \in \overline{G}_{\underline{H}}$ and ~~get~~ define

$\underline{g}^{(m)} := (g_m)_{n\in\mathbb{N}}$ constant sequence

$(g_m, g_m, g_m, \dots) \in \mathrm{Cauchy}(G, \underline{H})$.

Then $[\underline{g}^{(m)}] \xrightarrow{m\to\infty} \cancel{[(g_n)_{n\in\mathbb{N}}]}$. $[\underline{g}]$. $\square$ (iv)

$\square$

<u>Examples 169:</u>

(a) Take $H_n = \{1_G\}$, $n \in \mathbb{N}$.

~~Then Cauchy$(G, \underline{H}) = \{[(g)_{n\in\mathbb{N}}] \mid g \in G\}$~~

~~and null$(G, \underline{H}) = \{[(1_G)_{n\in\mathbb{N}}]\}$~~

$\mathrm{Cauchy}(G, \underline{H}) = \{ (g_n)_{n\in\mathbb{N}} \mid \exists_{M\in\mathbb{N}} : \exists_{g\in G}$
$\forall_{n\geq M} : g_n = g \}$

$\mathrm{null}(G, \underline{H}) := \{ (g_n)_{n\in\mathbb{N}} \mid \exists_{M\in\mathbb{N}} \forall_{n\geq M} : g_n = 1_G \}$

$$\text{—} \overset{192}{\Rightarrow} \text{—} \; G \xrightarrow{\varphi} \overline{G}_{\underline{H}}$$

$$g \longmapsto [(g)] \quad \text{is bijective.}$$

with $\varphi(gH_n) = [(g)] \cdot \overline{H}_n$.

So $G \overset{\text{homeo}}{\cong} \overline{G}_{\underline{H}}$.

(b) $G = (\mathbb{Z}, +)$, $p \in \mathbb{N}$ prime,

$H_n := p^n \mathbb{Z}$

$$\mathrm{Cauchy}(G, \underline{H}) = \{ (z_m)_{m \in \mathbb{N}} \mid \forall_{n \in \mathbb{N}} \exists_{M(n) \in \mathbb{N}} \forall_{\mathbb{N} \ni s, t \geq M(n)} : z_s \equiv z_t \bmod p^n \}$$

$$\mathrm{null}(G, \underline{H}) = \{ \ldots \quad z_s \equiv_{p^n} 0 \}$$

$$\mathrm{Cauchy}(G, \underline{H}) \twoheadrightarrow \mathbb{Z}_p := \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}.$$

$$(z_n)_{n \in \mathbb{N}} \longmapsto ([\tilde{z}_n])_{n \in \mathbb{N}}$$

with $\tilde{z}_n \equiv z_s \bmod p^n$ for all s big enough.

The kernel of this ring homomorphism is $\mathrm{null}(G, \underline{H})$.

And $\overline{G}_{\underline{H}} \xrightarrow[\sim]{\varphi} \mathbb{Z}_p$ satisfies

$$\varphi(H_m) = \left(\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}\right) \cap \left\{([z_n])_n \,\middle|\, z_n \equiv 0 \bmod p^m\right\}$$

$$= \left(\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}\right) \cap \left(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z} \times \cdots \times \{[0]_{p^m}\} \times \mathbb{Z}/p^{m+1}\mathbb{Z} \times \mathbb{Z}/p^{m+2}\mathbb{Z} \times \cdots\right)$$

is open and the translates of sets of the latter form form a subbase of the topology of $\mathbb{Z}_p$.

So φ is a homeo. (Something is hidden. What?)

Embedd $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ $\quad z \mapsto ([z]_{p^n})_{\mathbb{N}}$.

identify $\mathbb{Z}$ with image.

Then $\forall x \in \mathbb{Z}_p \ \exists\, a_0, a_1, \ldots \in \{0, \ldots, p-1\}$:

$$x = \lim_{m \to \infty} \sum_{i=0}^{m} a_i p^i = \sum_{i=0}^{\infty} a_i p^i.$$

(c) Let R be a ring and $\mathfrak{m}$ a maximal ideal. We write

$\overline{R}_{\mathfrak{m}}$ for the completion w.r.t.

$\mathfrak{m} \supseteq \mathfrak{m}^2 \supseteq \mathfrak{m}^3 \supseteq \dots$

<u>Exercise</u>: Prove that this notation is not confusing, i.e.

We have

(I) the completion of R w.r.t.

$\mathfrak{m} \supseteq \mathfrak{m}^2 \supseteq \mathfrak{m}^3 \supseteq \mathfrak{m}^4 \supseteq \dots$

(II) the completion of $R_{\mathfrak{m}}$ w.r.t.

$\mathfrak{m}R_{\mathfrak{m}} \supseteq \mathfrak{m}^2 R_{\mathfrak{m}} \supseteq \mathfrak{m}^3 R_{\mathfrak{m}} \supseteq \dots$

Show that there is a canonical homeomorphism between these completions:

$$\overline{R} \longrightarrow \overline{R_{\mathfrak{m}}}$$

$$[(r_n)] \longmapsto \left[\left(\frac{r_n}{1}\right)\right].$$

(d) Completion of $k[\underline{X}]$ w.r.t. $(\underline{X})_{k[\underline{X}]}$.

<u>Claim:</u> This completion is homeomorphic as ring to $k[[\underline{X}]]$ the Taylor series ring.

<u>Proof:</u> topology on $S = k[[\underline{X}]]$: It is the topology w.r.t. the filtration

$$\underline{X}S \supseteq \underline{X}^2 S \supseteq \underline{X}^3 S \supseteq \dots$$

We have: $k[\underline{X}] \xhookrightarrow{\varphi} k[[\underline{X}]]$

$$P \longmapsto P$$

continuous.

$\operatorname{im}\varphi$ is dense in $k[[\underline{X}]]$.

$\Rightarrow \exists$ ring homomorphism: $\overline{k[\underline{X}]} \xrightarrow{\overline{\varphi}} k[[\underline{X}]]$

continuous

Note $k[\underline{X}] \xrightarrow[\sim]{\varphi} \operatorname{im}\varphi$ is a homeomorphism, because φ respects the filtration.

Thus $\overline{\varphi}$ is injective:

$\overline{\varphi}(x) = 0 \Rightarrow \exists (x_n)_{n\in\mathbb{N}}$ in $k[\underline{X}]$

$x_n \xrightarrow{n\to\infty} x$ s.t. $\varphi(x_n) \longrightarrow 0 \in \operatorname{im}(\varphi)$

$k[\underline{X}] \overset{\varphi}{\cong} \operatorname{im}\varphi$ homeom. $\Rightarrow$ $x_n \longrightarrow 0$.

$\Longrightarrow x = 0.$

Put $H_n := X^n k[X]$

Then $\bar{\varphi}(\bar{H}_n) = X^n k[[X]]$ (exercise)

Thus $\bar{\varphi}$ is open.

$\Rightarrow$ $\bar{\varphi}$ is an ~~homeomor~~ isomorphism of topological rings. (rather, topological k-algebras)

2nd of lecture 25

<u>Def 170:</u> A ring R together with a topology τ on R is called topological ring if $+, \cdot$ are continuous.

(Similar: "topological group", "topological k-algebras".)

A ring isomorphism φ between topological rings (R, τ_R), (S, τ_S) is called ~~topological~~ ring homeomorphism if φ is a homeomorphism.

We also say "isomorphism of topological rings".

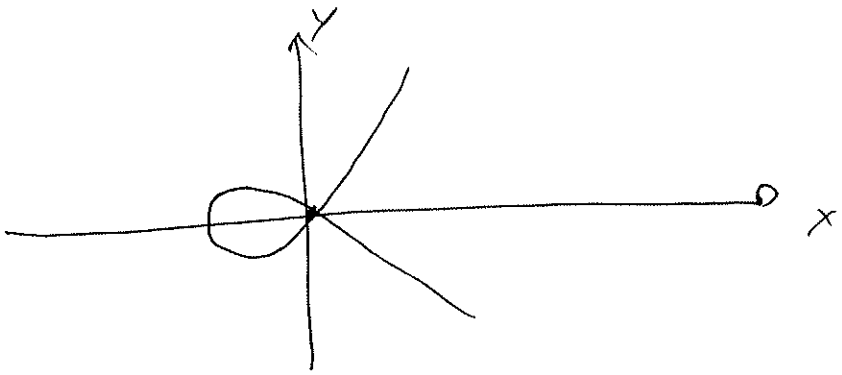
IV.2. Motivation from Alg. geometry

<u>Example 170:</u> The Zariski topology on a variety is too coarse. So the stalk does not see the full behaviour of the variety around a point.

So we need to complete the stalk.

$V = V(P) \subseteq \bar{k}^2 = \mathbb{A}^2_{\bar{k}}$, $\mathrm{char}(k) \neq 2$,
$P = Y^2 - X^2(X+1)$.

Picture of the $\mathbb{R}$-points (for $k = \mathbb{R}$)



Near $(0,0)$ V looks reducible (almost a union of two lines)

~~But the completion of $R := k[X,Y]/(X_1$~~

But the stalk of $(0,0)$: $k[V]_{\mathfrak{m}} = \left(k[X,Y] \big/ I_{\bar{k}}(V) \cap k[X,Y] \right)_{\mathfrak{m}}$

$$= \left(k[X,Y] \big/ (P)_{k[X,Y]} \right)_{\mathfrak{m}}, \quad \mathfrak{m} = (x,y)_{k[V]}$$

is still an integral domain, because all open sets $D(f)$, $f \in \cancel{k[X]}$, $k[V] \setminus \{0\}$, are irreducible. (They are not enough!)

Let's go to the completion:

$$k[[X,Y]] \big/ (P)_{k[[X,Y]]}$$

This is not an integral domain, because

$$\sqrt{1+X} = 1 + \left(\tfrac{1}{2}\right)X - \tfrac{1}{8}X^2 + \tfrac{1}{16}X^3 - \tfrac{5}{128}X^4 \ldots$$

$$\in k[[X]].$$

What would be a better topology?

Instead of Zariski open sets in V we consider certain polynomial maps $U \xrightarrow{\varphi} V$ from a connected Zariski open U in some other variety.

(Property: Locally: On the tangent space at $x \in U$ we want $d\varphi : T_x U \xrightarrow{\sim} T_{\varphi(x)} V$

in fact we want it on the "tangent cone")

$$\alpha = \frac{1}{[X]} \in Q(k[V]) \Rightarrow \frac{[X+1]}{[X]^2} = \alpha^2$$

In $k[V][\alpha]$ $[X+1]$ is a square.

Consider $k[V] \hookrightarrow k[V][T] \big/ (T^2 - [X+1])$

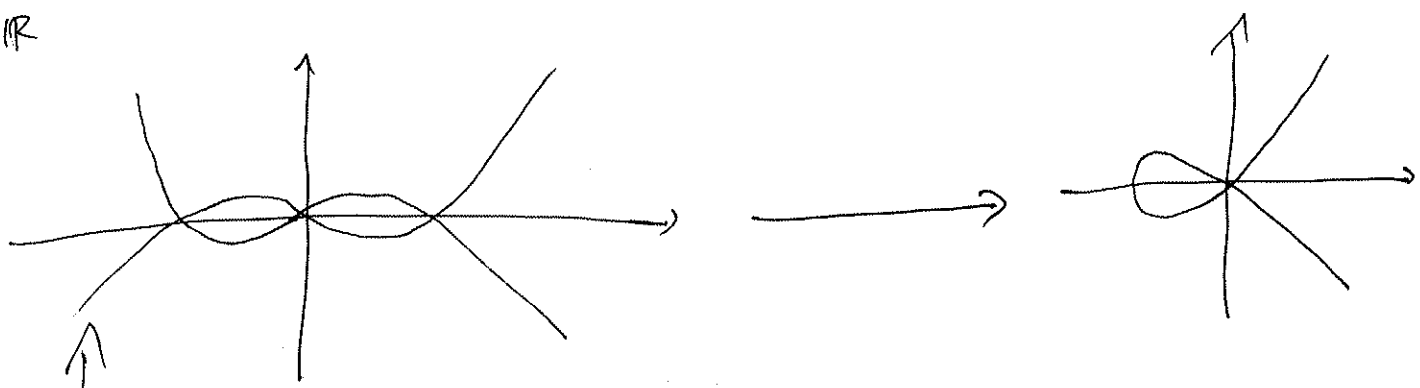
$$\cong$$

$$k[Y,Z] \big/ (P)_{k[Y,Z]} \simeq k[X,Y,Z] \big/ (P,\ Z^2-(1+X))_{k[X,Y,Z]}$$

$$\cong$$

$$k[Y,Z] \big/ \cancel{((Y-X(1+X))(Y-}\ (Y-(Z^2-1)Z)(Y+(Z^2-1)Z))$$

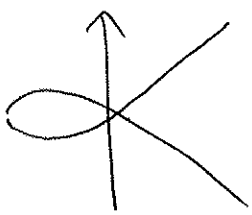
$k = \mathbb{R}$

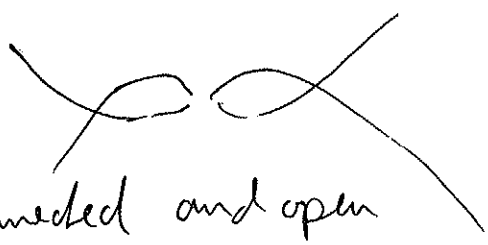


$$(Y,Z) \longmapsto (Z^2-1,\ Y)$$

$$\tilde{V} = V\big((Y-(Z^2-1)Z)(Y+(Z^2-1)Z)\big) = \tilde{V}_1 \cup \tilde{V}_2 \subseteq \bar{k}^2$$

$$U := \tilde{V} \setminus \{(0,0)\} \xrightarrow{\varphi}$$



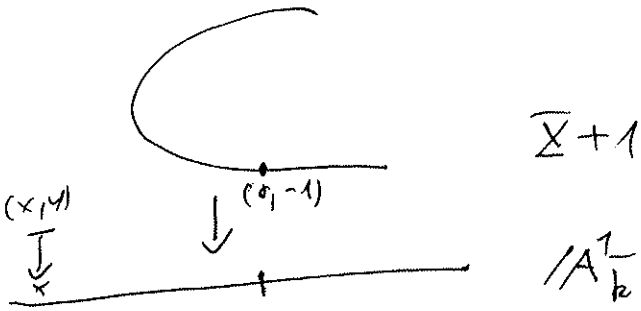


U is connected and open in $\tilde{V}$. But $U = (\tilde{V}_1 \cap U) \cup (\tilde{V}_2 \cap U)$

so U is not irreducible. φ corresponds to the "étale topologies"

<u>Example 17 ~~1~~:</u> (Inverse function theorem)

char $k \neq 2$



$$X+1 = Y^2$$

It looks that it should be locally invertible with a polynomial map.
This is not the case, because $x \longmapsto (x, \sqrt{x+1})$ is not polynomial.
The reason here is that this map is not locally injective w.r.t. the Zariski ~~topoly~~ topology, because the Zariski open sets are too big.
(If U ~~Zariski~~ is Zariski open and $U \ni (0,-1) = P$, then $U = V$ because V is irreducible.)

Go to the completions of the stalks.

$$\left(k[X,Y]/(Y^2-X-1)\right)_{(x,y+1)} \xrightarrow{\text{complete}} k[[X,Y]]/(Y^2-X-1) = k[[X,Y]]/(Y^2-(X+1))$$

$$\uparrow \qquad\qquad\qquad \uparrow$$

$$k[X]_{(X)} \qquad\qquad k[[X]]$$

$$X \mapsto X, \quad X \mapsto [Y], \quad [X] \mapsto X, \quad \sqrt{X+1} \mapsto [Y]$$

So we find a right inverse of $(x,y) \longmapsto x$ between the completion of the stalks.

IV.3. Hensel's Lemma

I do not like the notation from the book.
From now on we write $\overline{R}^{\mathfrak{m}}$ for the completion
R w.r.t. $\mathfrak{m} \neq R$

<u>Question</u> 172 ① Does the polynomial
$P := X^6 - X^5 + 3X^4 + X^3 + 1$ has a
root in $\mathbb{Z}_7$?
$\mathbb{Z}_7 = \overline{\mathbb{Z}}^{(7)}$

Let's check $\overline{P} = P \bmod 7$. (Note $\mathbb{Z}_7/7\mathbb{Z}_7 \simeq \mathbb{Z}/7\mathbb{Z} = \mathbb{F}_7$)

$\overline{P}$ has the root $-\overline{3} = [-3]_7$ and
it is a simple root.

$$\overline{P} = (X + \overline{3})\underbrace{(X^5 + \overline{3}X^4 + X^3 - \overline{3}X^2 + \overline{3}X - \overline{2})}_{\overline{Q}}$$

$$\overline{Q}(-\overline{3}) = -\overline{12} + \overline{12} - \overline{6} - \overline{6} - \overline{2} - \overline{2} = -\overline{2} \neq \overline{0}.$$

i.e. $\gcd(\overline{P}, \overline{Q}) = 1$.

End of lecture 26

② How many roots of unity with order prime to p has $\mathbb{Z}_p$?

(Call this set $\mu_{p\nmid}(\mathbb{Z}_p)$.)

We have a map $\mu_{p\nmid}(\mathbb{Z}_p) \xrightarrow{\varphi} \mathbb{F}_p^\times$

$$\zeta \longmapsto \bar{\zeta}.$$

Is this map bijective?

<u>Injectivity</u>: $\zeta \in \mu_{p\nmid}(\mathbb{Z}_p)$ s.t. $\bar{\zeta} = \bar{1}$.

$\Rightarrow \exists x \in \mathbb{Z}_p : \zeta = 1 + px$

$\zeta \in \mu_{p\nmid}(\mathbb{Z}_p) \Rightarrow \exists \underset{p\nmid m}{m \in \mathbb{N}} : \zeta^m = 1.$

$\Rightarrow 1 = 1 + mpx + p^2 y$ for some $y \in \mathbb{Z}_p$

$\Rightarrow 1 \equiv 1 + mpx \mod p^2$

$\underset{p\nmid m}{\Rightarrow} p \mid x$

Inductively $\forall_{\ell \in \mathbb{N}} \; p^\ell \underset{\mathbb{Z}_p}{\mid} x \Rightarrow x = 0.$

<u>Surjectivity?</u> Consider $P = X^{p-1} - \bar{1}$

$$= \prod_{a \in \mathbb{F}_p^\times} (X - a).$$

Can we lift all of them?

<u>Theorem 173:</u> (Hensel's lemma I)

Let R be a noetherian ring. Suppose R is complete w.r.t. an ideal $\mathfrak{m}$. Suppose that $F \in R[X]$ has a reduction mod $\mathfrak{m}$, $f \in R/\mathfrak{m}[X]$, which factorizes as

$f = g_1 g_2$, $g_i \in R/\mathfrak{m}[X]$, s.t.

(a) $(g_1, g_2)_{R/\mathfrak{m}[X]} = R/\mathfrak{m}[X]$

(b) g_1 is monic

Then $\exists!\, G_1, G_2 \in R[X]$ s.t.

$F = G_1 G_2$, $\overline{G_1} = g_1$, $\overline{G_2} = g_2$ and G_1 is monic.

We will prove the theorem along the exercises given in the text book.

<u>Lemma 174:</u> Let S be a ring, $g_1, g_2 \in S[X]$, such that g_1 is monic and of degree $d \in \mathbb{N}_0$ and such that $(g_1, g_2)_{S[X]} \ni 1$.

Let $h \in S[X]$. Then $\exists!\, h_1, h_2 \in S[X]$ with $\deg h_2 < d$:

$h = h_1 g_1 + h_2 g_2$.

<u>Proof:</u> We obtain an expression $h = h_1 g_1 + h_2 g_2$ because $\{g_1, g_2\}$ generates $S[X]$ and we can achieve $\deg h_2 < d$, because for every term of degree $\geq d$ we can substract a multiple of g_1.

(g_1 is monic!)

<u>Uniqueness:</u> $h = h_1 g_1 + h_2 g_2 = \tilde{h}_1 g_1 + \tilde{h}_2 g_2$, $\deg h_2, \deg \tilde{h}_2 < d$

$1 \in (g_1, g_2)_{S[X]} \Rightarrow \exists\, a_1, a_2 \in S[X]$, $\deg a_2 < d$:

$a_1 g_1 + a_2 g_2 = 1.$

$$\Rightarrow \quad 0 = a_2 (h_1 - \tilde{h}_1) g_1 + a_2 (h_2 - \tilde{h}_2) g_2$$

$$= \underbrace{(a_2 (h_1 - \tilde{h}_1) - a_1 (h_2 - \tilde{h}_2)) g_1}_{\deg \in \{-\infty\} \cup \mathbb{N} \geq d} + \underbrace{(h_2 - \tilde{h}_2)}_{\deg \in \{-\infty\} \cup \mathbb{N}_0^{\leq d-1}}$$

$$\Rightarrow \quad h_2 = \tilde{h}_2 \Rightarrow (h_1 - \tilde{h}_1) g_1 = 0 \underset{\substack{\uparrow \\ g_1 \text{ is monic.}}}{\Rightarrow} h_1 = \tilde{h}_1 \qquad \square$$

<u>Lemma 175:</u> Under the conditions of Lemma 174 suppose that $S = R/\mathfrak{m}$ for a ring R and an ideal $\mathfrak{m} \subseteq \mathrm{Jac}(R)$ and that $G_1, G_2 \in R[X]$ such that $G_i \bmod \mathfrak{m} = g_i$ and G_1 is monic.

Then G_1 and G_2 generate $R[X]$, i.e.

$$G_1 R[X] + G_2 R[X] = R[X].$$

<u>Proof:</u> Consider $M := R[X] / (G_1)$.

Then, because $g_1 S[X] + g_2 S[X] = S[X]$, we have

$$M = R[X] \cdot v + \mathfrak{m} M \qquad \text{with } v = [G_2]_{(G_1)}.$$

M is a f.g. R-module because G_1 is monic.

Nakayama's lemma $\Rightarrow$ $M = R[X] v$

$\Rightarrow \forall H \in R[X] \ \exists A_2 \in R[X] : \quad H \in A_2 \cdot G_2 + (G_1)$

In particular for $H = 1$. $\square$

<u>Proof of Hensel's lemma:</u>

Take $G_1^{(1)}, G_2^{(1)}$ such that $G_i^{(1)} \bmod \mathfrak{m} = g_i$, $i = 1, 2$,

~~deg~~ G_1 monic and $\deg G_2^{(1)} \leq \deg F - d$.

We can apply Lemma 175, because

$\mathfrak{m} \subseteq \mathrm{Jac}(R)$, because R is complete w.r.t. $\mathfrak{m}$.

(Exercise!)

Lemma 175 $\Rightarrow$ $(G_1^{(1)}, G_2^{(1)})_{R[X]} = R[X]$.

$\Longrightarrow$ (by Lemma 174):

$\exists\ H_1^{(1)}, H_2^{(1)} \in R[X]$: $F - G_1^{(1)} G_2^{(1)} = G_1^{(1)} H_1^{(1)} + G_2^{(1)} H_2^{(1)}$

$\deg H_2^{(1)} < d$ and $\deg H_1^{(1)} \leq \deg F - d$

(because $F - G_1^{(1)} G_2^{(1)}$ has no terms of degree $> \deg F$.)

mod m $\Longrightarrow$ $0 = g_1 \overline{H_1^{(1)}} + \overline{g_2 H_2^{(1)}}$

Uniqueness $\Longrightarrow$ $H_1^{(1)}, H_2^{(1)} \in m R[X]$.

Put $G_1^{(2)} := G_1^{(1)} + H_2^{(1)}$ and $G_2^{(2)} := G_2^{(1)} + H_1^{(1)}$

$\Longrightarrow$ $F - G_1^{(2)} G_2^{(2)} = - H_1^{(1)} H_2^{(1)} \in m^2 R[X]$.

We have $G_i^{(2)} \bmod m = g_i$ and $G_1^{(2)}$ is monic, so $G_1^{(2)}$ and $G_2^{(2)}$ generate as an ideal the ring $R[X]$.

$\Longrightarrow$ $G_1^{(2)} \bmod m^2$ and $G_2^{(2)} \bmod m^2$ generate $R/m^2[X]$.

R is complete w.r.t. m^2.

Induction $\Longrightarrow$ We obtain $G_1^{(1)}, G_1^{(2)}, G_1^{(3)}, \ldots$

and $G_2^{(1)}, G_2^{(2)}, G_2^{(3)}, G_2^{(4)}, \ldots$

such that:
- $G_1^{(i)}$ is monic
- $\deg G_2^{(i)} \leq \deg F - d$.

- $G_1^{(i)} \bmod \mathfrak{m}^{i-1} = G_1^{(i-1)} \quad \forall_{i=2,\dots}$
- $G_2^{(i)}$ — " — $G_2^{(i-1)}$ — " —

$$G_1 := \lim_{i\to\infty} G_1^{(i)} \qquad G_2 := \lim_{i\to\infty} G_2^{(i)}$$

$\Rightarrow F = G_1 \cdot G_2$, because $F - G_1^{(m)} G_2^{(m)}$ is a null-sequence. $\square$

~~<u>Theorem 176:</u> (Hensel's Lemma II)~~

~~Let R be a ring which is complete w.r.t. an ideal $\mathfrak{m}$ and let $F(X) \in R[X]$ be a polynomial s.t. its reduction mod $\mathfrak{m}$, say $f(X) \in R/\mathfrak{m}[X]$, has a root $\alpha \in R/\mathfrak{m}$, s.t. $f'(\alpha)$~~

~~$f(\alpha) \not\equiv 0$~~

~~Corollary 176~~

<u>end of Lecture 27</u>

<u>Theorem 176</u> (Hensel's Lemma)

Let R be a ring which is complete w.r.t. an ideal $\mathfrak{m}$ an let $f \in R[X]$ be a polynomial and $a \in R$ s.t.

$$f(a) \equiv 0 \mod f'(a)^2 \mathfrak{m}$$

("a is an approximate root of f")

Then $\exists\, b \in R$: $b \equiv a \mod f'(a)\mathfrak{m}$ and $f(b) = 0$.

If $f'(a)$ is a non zerodivisor then b is unique.

<u>Proof</u>: (only for $f'(a) \in R^\times$).

$\bar{f} := f \mod \mathfrak{m}$

$\bar{f}(\bar{a}) = 0$ and $\bar{f}'(\bar{a}) = \overline{f'(a)} \in (R/\mathfrak{m})^\times$

Thus $\bar{f}(X) = (X - \bar{a})\, g(X)$ $\quad g \in R/\mathfrak{m}[X]$

and $g(\bar{a}) = \bar{f}'(\bar{a}) \in (R/\mathfrak{m})^\times$

Thus $g(X) = h(X)(X - \bar{a}) + \bar{r}$, $\bar{r} \in (R/\mathfrak{m})^\times$, $h \in R/\mathfrak{m}[X]$

So $g(X)\, R/\mathfrak{m}[X] + (X - \bar{a})\, R/\mathfrak{m}[X] = R/\mathfrak{m}[X]$

Hensel's Lemma (Thm 173) $\Rightarrow$ ✓ $\square$

Examples 177:

(a) Completion can produce inverses:

In $\mathbb{Z}$ only ± 1 are invertible.

But in $\mathbb{Z}_2$ all odd integers are invertible

in fact

$\mathbb{Z}_2^\times = \mathbb{Z}_2 \setminus 2\mathbb{Z}_2$, because $\mathbb{Z}_2$ is a local ring with unique maximal ideal $2\mathbb{Z}_2$.

Ex: In $\mathbb{Z}_2$: $\frac{1}{7} = \frac{1}{2^3-1} = -\frac{1}{1-2^3}$

$$= -(1+2^3+2^6+2^9+\dots)$$

$$\frac{1}{3} = \frac{1}{1+2} = 1-2+4-8+16-\dots$$

$$= 1+2+2^3+2^5+\dots$$

(b) Suppose p is an odd prime

Then are equivalent:

1° $p \equiv_4 1$

2° All elements of $\mathbb{Z}_p$ are sum of 2 squares.

Proof: $1° \Rightarrow 2°$ $p \equiv_4 1 \overset{\text{Ex.}}{\Longleftrightarrow}$ (-1) is a square in $\mathbb{F}_p$.

Take $x \in p\mathbb{Z}_p$, (-1), $1+x$ ~~and~~ are ~~a~~ squares by Hensel's Lemma. $\Rightarrow$ $x = (1+y) + (-1)$ is a sum of two squares.

Take $x \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$ Then x is mod p congruent to a sum of two squares, because

in $\mathbb{F}_p$ every element is a sum of two squares.

(<u>Proof</u>: We only need to show that there is a non-square in $\mathbb{F}_p$ which is a sum of two squares. If this is false then a sum of two squares in $\mathbb{F}_p$ would be always a square:

Then $0, 1, 1+1, 1+1+1, \ldots$, i.e. all elements of $\mathbb{F}_p$, would be squares. ↯ $\square$)

So $\exists\, y, z \in \mathbb{Z}_p$ $\quad x \equiv_p y^2 + z^2$. Put $\zeta := x^{-1}(y^2+z^2)$.

Then $\zeta \equiv_p 1$, so ζ is a square in $\mathbb{Z}_p$ by Hensel's lemma.

$\Rightarrow \quad x = \zeta^{-1} y^2 + \zeta^{-1} z^2$ is a sum of two squares.

$2^\circ \Rightarrow 1^\circ$ $\quad \varpi := p$ is a sum of two squares

$\Rightarrow \exists\, y, z \in \mathbb{Z}_p \quad y^2 + z^2 = p.$

$\Rightarrow \quad y^2 \equiv_p -z^2$.

y and z are not in $p\mathbb{Z}_p$, because otherwise $p^2 \mid p$ ↯.

$\Rightarrow$ z is invertible in $\mathbb{Z}_p$. and

$(yz^{-1})^2 \equiv_p -1$. Thus $p \equiv_4 1$. $\square$

<u>Def 178:</u> (1) A ring R together with a direct sum decomposition

$$R = \bigoplus_{j \in J} R_j \qquad (*)$$

is called a J-graded ring if

(a) J is an ~~[illegible]~~ abelian semigroup with neutral element

(b) $\forall_{j_1, j_2 \in J}: \quad R_{j_1} \cdot R_{j_2} \subseteq R_{j_1 + j_2}$

(2) Let R be a J-graded ring with decomposition $(*)$. An R-module M together with a direct sum decomposition $M = \bigoplus_{j \in J} M_j$ is called J-graded

if $\forall_{j_1, j_2 \in J}: \quad R_{j_1} M_{j_2} \subseteq M_{j_1 + j_2}$.

(3) Let R be a ring, $J \leq_R R$ and M be an R-module.

We call $\operatorname{gr}_J M := M/JM \oplus JM/J^2M \oplus J^2M/J^3M \oplus \cdots$

"The associated $(\mathbb{N}_0)$-graded $\operatorname{gr}_J R$-module w.r.t. J."

where $\operatorname{gr}_J R = R/J \oplus J/J^2 \oplus J^2/J^3 \oplus \cdots$ is

called "the associated graded ring of R w.r.t. J."

<u>Example 179</u> (1) Every ring R can be made to a graded ring trivially by putting $R_0 = R$ and $R_i = 0 \ \forall_{i \in \mathbb{N}}$.

(2) Let R be a ring. Then $R[X_1, \ldots, X_n]$

can be made into an $\mathbb{N}_0$-graded ring via putting $R_i := (\{\text{monomials of degree } i\})_R$.

<u>Claim:</u> $R[X_1, \dots, X_n]$ is R-algebra isomorphic to $\operatorname{gr}_{(X_1, \dots, X_n)} R[X_1, \dots, X_n]$.

<u>Proof:</u> Easy □

Further $R[X_1, \dots, X_n]$ is also $\mathbb{N}_0^n$-graded.

(3) $R[X, Y]$ is a graded $R[Y]$-module.

- $R[Y]$ with the grading $R[Y] = \bigoplus_{i \in \mathbb{N}_0} R\, Y^i$
- $R[X, Y]$ — " — $R[X, Y] = \bigoplus_{i \in \mathbb{N}_0} Y^i R[X]$

<u>Def. 180:</u> Let R be a J-graded ring and M be a J-graded R-module.
A sub-module N of M is called <u>homogeneous</u> if $N = \bigoplus_{j \in J} (N \cap M_j)$.
An element x of M is called <u>homogeneous</u> (or better <u>j-homogeneous</u>) if $\exists j \in J : x \in M_j$ $(x \in M_j)$.

<u>Example 181:</u> (1) The homogeneous elements of $R[X_1, \dots, X_n]$ (by grading given by degree) are the polynomials which are R-linear combinations of monomials of the same degree.

(2) Under the conditions of Def 180, suppose N is generated by homogeneous elements. Then N is homogeneous.

<u>Proof:</u> Obviously $N \supseteq \bigoplus_{j\in J} (N \cap M_j)$

Take $n \in N = \langle n_\lambda \mid \lambda \in \Lambda \rangle_R$ (all n_λ, $\lambda \in \Lambda$ are supposed to be homogeneous.

$\Rightarrow \exists_{\lambda_1,\dots,\lambda_\ell \in \Lambda} \exists_{r_1,\dots,r_\ell \in R}$: $n = \sum_{i=1}^{\ell} r_i n_{\lambda_i}$

$r_i n_{\lambda_i}$ is a sum of homogeneous elements because r_i is and n_{λ_i} is homogeneous, and those homogeneous summands lie in N.

$\Rightarrow n \in \bigoplus_{j\in J} (M_j \cap N)$ $\square$

<u>End of Lecture 28</u>

<u>Prop. 182:</u> Let R be a $\mathbb{N}_0$-graded ring. Then are equivalent:

1° R is noetherian.

2° R_0 is noetherian and R is f.g. as an algebra over R_0

<u>Proof:</u> 1° $\Rightarrow$ 2° Suppose R is noetherian.

Then R_0 is noetherian.

($\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \dots$ ideal chain in R_0

Put $R_+ = 0 \oplus R_1 \oplus R_2 \oplus \dots$

Then $\mathfrak{a}_1 \oplus R_+ \subseteq \mathfrak{a}_2 \oplus R_+ \dots$ is an ideal chain in R. So it stabilizes.)

Let $R_+ = y_1 R + y_2 R + \dots + y_\ell R$.

W.l.o.g. $y_1, \dots, y_\ell$ are non-zero. Other $R = R_0$ is noetherian.

$R_+ = R_1 \oplus R_2 \oplus R_3 \oplus \dots$

let $d := \max\{\deg(Y_i) \mid i = 1, \dots, \ell\}$

$\ulcorner \deg Y := \begin{cases} -\infty, & \text{if } Y = 0 \\ \max\{i \in \mathbb{N}_0 \mid \pi_i(Y) \neq 0\} \end{cases}$

where $\pi_i : R \longrightarrow R_i \qquad (x_j)_{j \in \mathbb{N}_0} \longmapsto x_i \quad \lrcorner$

~~Then~~ Every R_i is a f.g. R_0-module (why?)

So $R_1 \oplus \dots \oplus R_d$ is a f.g. R_0-module.

Take homogeneous non-zero elements $x_1, \dots, x_s \in R_1 \oplus \dots \oplus R_d$

such that $\langle x_1, \dots, x_s \rangle_{R_0} = R_1 \oplus \dots \oplus R_d$

Then $(x_1, \dots, x_s)_R = (Y_1, \dots, Y_\ell)_R = R_+$.

<u>Claim:</u> $R = R_0[x_1, \dots, x_s] =: T$

<u>Proof:</u> "$\supseteq$" ✓ "$\subseteq$" We show that $\forall n \in \mathbb{N}_0$: $R_n \subseteq T$.

<u>$n = 0$:</u> $R_0 \subseteq T$

<u>$1 \leq n \leq d$:</u> $R_n \subseteq R_1 + \dots + R_d \subseteq T$.

<u>$n > d$!</u> $x \in R_n \underset{(x_1, \dots, x_s)_R = R_+}{\Rightarrow} \exists\, r_1, \dots, r_s$ homogeneous : $\sum r_i x_i = x$

and ($r_i x_i \in R_n \; \forall i = 1, \dots, s$.)

If $r_i \neq 0$ then $1 \leq \deg r_i = n - \deg x_i < n$

Thus $r_i x_i \in T \cdot T \subseteq T$. So $x \in T$. $\square$

"2° ⇒ 1°" Hilbert's basis theorem. $\square$

<u>Corollary 183:</u> Let R be a noetherian ring and $\mathfrak{a} \neq R$ be an ideal of R. Then $\mathrm{gr}_{\mathfrak{a}} R$ is noetherian.

<u>Proof:</u> $\mathfrak{a}/\mathfrak{a}^2$ is f.g. as an $R/\mathfrak{a}$-module.

Take $a_1, \dots, a_l \in R$ s.t. $\langle \bar{a}_1, \dots, \bar{a}_l \rangle_{R/\mathfrak{a}} = \mathfrak{a}/\mathfrak{a}^2$

Take $\bar{b} \in \mathfrak{a}^m/\mathfrak{a}^{m+1}$. Then $\exists\, r_{i_1, \dots, i_m} \in R$:

$$b \equiv \sum_{i_1=1}^{l} \sum_{i_2=1}^{l} \cdots \sum_{i_m=1}^{l} r_{i_1, \dots, i_m} a_{i_1} \cdots a_{i_m} \mod \mathfrak{a}^{m+1}$$

$$\Rightarrow \quad [b]_{\mathfrak{a}^{r+1}} = \sum \cdots \sum \underbrace{[r_{i_1, \dots, i_m}]_{\mathfrak{a}} [a_{i_1}]_{\mathfrak{a}^2} \cdots [a_{i_m}]_{\mathfrak{a}^2}}_{\text{product in } \mathrm{gr}_{\mathfrak{a}} R}$$

$\Rightarrow$ $\mathrm{gr}_{\mathfrak{a}} R$ is a f.g. $R/\mathfrak{a}$-~~alg~~ algebra.

Prop 182 $\Rightarrow$ $\mathrm{gr}_{\mathfrak{a}} R$ is a noetherian ring. $\square$

$\uparrow$

$R/\mathfrak{a}$ is noetherian because R is

For complete rings we have the converse.

To see this we need some preparation.

<u>Def 184:</u> (1) Let R be a ring with ideals

$\underbrace{R \supsetneq \mathfrak{m}_1 \supseteq \mathfrak{m}_2 \supseteq \dots}_{\underline{\mathfrak{m}}}$ such that $\mathfrak{m}_i \mathfrak{m}_j \subseteq \mathfrak{m}_{i+j}$.

Then $\operatorname{gr}_{\underline{\mathfrak{m}}} R := R/\mathfrak{m}_1 \oplus \mathfrak{m}_1/\mathfrak{m}_2 \oplus \mathfrak{m}_2/\mathfrak{m}_3 \oplus \dots$

is again a ring. "The graded ring of R w.r.t. $\underline{\mathfrak{m}}$".

(<u>Example</u>: Take $\mathfrak{m}_i = \mathfrak{a}^i$ for some ideal $\overset{R}{\overset{\shortparallel}{\mathfrak{a}}}$.)

(2) Given $R, \underline{\mathfrak{m}}$ in (1) and $a \in R$.

Put $\operatorname{in}(a) := \begin{cases} [0]_{\mathfrak{m}_1} & a = 0 \text{ or } a \in \bigcap_{i=1}^{\infty} \mathfrak{m}_i \\ [a]_{\mathfrak{m}_{i+1}} & \text{if } a \in \mathfrak{m}_i \setminus \mathfrak{m}_{i+1}. \end{cases}$

"the initial of a."

Let $\mathfrak{a}$ be an ideal of R.

We put $\operatorname{in}(\mathfrak{a}) := \{ \operatorname{in}(a_1) + \dots + \operatorname{in}(a_\ell) \mid \ell \in \mathbb{N}_0,\ a_1, \dots, a_\ell \in \mathfrak{a} \}$

is an ideal in $\operatorname{gr}_{\underline{\mathfrak{m}}} R$. (Why?)

"the initial ideal of $\mathfrak{a}$".

<u>Example 185:</u> (1) $R = \mathbb{Z}$, $\mathfrak{a} = 6\mathbb{Z}$, $\operatorname{gr}_{\mathfrak{a}} R = \mathbb{Z}/6\mathbb{Z} \oplus 6\mathbb{Z}/36\mathbb{Z} \oplus 36\mathbb{Z}/216\mathbb{Z} \oplus \dots$

$\operatorname{in}(3) = [3]_6$.

$\cdot\ \mathrm{in}(108) = [108]_{216}$

$(108 = 27 \cdot 4 = 3 \cdot 36 \in 36\mathbb{Z} \setminus 216\mathbb{Z})$

$\cdot\ \mathrm{in}(135) = [135]_{216}.$

$\cdot\ \mathrm{in}(42) = [42]_{36} = [6]_{36}.$

$$\mathrm{in}(3\mathbb{Z}) = \underbrace{3\mathbb{Z}/6\mathbb{Z}}_{\text{in degree } 0} \oplus 6\mathbb{Z}/36\mathbb{Z} \oplus 36\mathbb{Z}/216\mathbb{Z} \oplus$$

$$= 3\mathbb{Z}/6\mathbb{Z} \oplus (\mathrm{gr}_{\mathfrak{U}} R)_+.$$

(2) $R = \mathbb{Z}$, $\mathfrak{U} = 7\mathbb{Z}$, $S := \mathrm{gr}_{\mathfrak{U}} R$

$\mathrm{in}(35\mathbb{Z}) = S_+$ (Exercise.)

End of Lecture 29.

<u>Lemma 185:</u> Let R be a ring and $\underline{\mathfrak{M}} := (\mathfrak{M}_1 \supseteq \mathfrak{M}_2 \supseteq \ldots)$ be a filtration of ideals of R s.t. $\mathfrak{M}_i \mathfrak{M}_j \subseteq \mathfrak{M}_{i+j}$. $\forall i, j \in \mathbb{N}$.

Suppose that R is complete w.r.t. $\underline{\mathfrak{M}}$.

Let $\mathfrak{U}$ be an ideal of R and $a_1, \ldots, a_\ell \in \mathfrak{U}$ such that $\mathrm{in}(\mathfrak{U})$ is generated by $\mathrm{in}(a_1), \ldots, \mathrm{in}(a_\ell)$ as an ideal in $\mathrm{gr}_{\underline{\mathfrak{M}}}(R)$.

Then $\mathfrak{U} = (a_1, \ldots, a_\ell) R$.

<u>Proof:</u> Put $\mathfrak{a}' = (a_1, \dots, a_\ell)_R$.

We have $\mathfrak{a}' \subseteq \mathfrak{a}$.

<u>Case 1:</u> If all a_i are ~~non~~ zero then

$\mathrm{in}(\mathfrak{a})$ which is generated by $\mathrm{in}(a_1), \dots, \mathrm{in}(a_\ell)$

is the zero ideal in $\mathrm{gr}_{\underline{m}} R$, and

therefore $\mathfrak{a}$ is the zero ideal, because

$\bigcap_{i=1}^{\infty} m_i = \{0\}$, because R is complete w.r.t. $\underline{m}$.

$\Rightarrow \mathfrak{a}' = \mathfrak{a}$

<u>Case 2:</u> Assume that all a_i are non-zero.

Assume $\exists\, a \in \mathfrak{a} \setminus \mathfrak{a}' \Rightarrow \exists\, r_1, \dots, r_\ell \in R : \mathrm{in}(a) = \sum_{i=1}^{\ell} \mathrm{in}(r_i)\,\mathrm{in}(a_i)$

$$\Rightarrow \deg \mathrm{in}\Big(a - \sum_{i=1}^{\ell} r_i a_i\Big) > \deg \mathrm{in}(a).$$

Put $r_i^{(0)} := r_i$, $i = 1, \dots, \ell$.

Let $d := \max\{\deg(\mathrm{in}(a_i)) \mid i = 1, \dots, \ell\}$

Then $r_i = 0$ or $\deg r_i = \deg(\mathrm{in}(a)) - \deg(\mathrm{in}(a_i))$
$\geq \deg(\mathrm{in}(a)) - d$

Iteratively: $\exists\, (r_j^{(0)})_{i=1,\dots,\ell}, (r_i^{(1)})_{i=1,\dots,\ell}, (r_i^{(2)}), \dots$ in R s.t.

$r_i^{(m)} = 0$ or $\deg r_i^{(m)} \geq \deg(\mathrm{in}(a)) + m - d$

and $\deg\left(\operatorname{in}\left(a - \sum_{i=1}^{\ell}\left(r_i^{(0)} + r_i^{(1)} + \dots + r_i^{(m)}\right)a_i\right)\right)$

$$> \deg\left(\operatorname{in}\left(a - \sum_{i=1}^{\ell}\left(r_i^{(0)} + \dots + r_i^{(m-1)}\right)a_i\right)\right)$$

$\forall_{m \geq 1}$.

Thus, because R is complete w.r.t. $\underline{\mathfrak{M}}$,

$\exists\, \tilde{r}_1, \dots, \tilde{r}_\ell \in R \;\forall_{1 \leq i \leq \ell}: r_i^{(0)} + \dots + r_i^{(m)} \longrightarrow \tilde{r}_i$.

and $a = \lim_{m \to \infty} \sum_{i=1}^{\ell}\left(r_i^{(0)} + \dots + r_i^{(m-1)}\right)a_i$

$$= \sum_{i=1}^{\ell} \tilde{r}_i a_i \in \mathfrak{a}' \lightning.$$

$\square$

<u>Lemma 186:</u> Let R be a ring with filtration $\underline{\mathfrak{M}}$ s.t. $\mathfrak{M}_i \mathfrak{M}_j \subseteq \mathfrak{M}_{i+j}\; \forall_{i,j \in \mathbb{N}}$.

Then the map
$$R \to \varprojlim_{n \in \mathbb{N}} R/\mathfrak{M}_n$$
$$r \longmapsto \left([r]_{\mathfrak{M}_n}\right)_{n \in \mathbb{N}}$$

induces a ring isomorphism
$$\overline{R}^{\underline{\mathfrak{M}}} \longrightarrow \varprojlim_{n \in \mathbb{N}} R/\mathfrak{M}_n =: T$$

which map $\overline{\mathfrak{M}}_n$ onto $\left\{\left([r_m]_{\mathfrak{M}_m}\right)_{m \in T} \,\middle|\, [r_n]_{\mathfrak{M}_n} = [0]_{\mathfrak{M}_n}\right\}$

<u>Proof</u>: The proof is similar to the proof of Example 169(b) $\square$

<u>Corollary 187</u>: $(R, \underline{\mathfrak{m}})$ given as in Lemma 186. Then $\forall_{n \in \mathbb{N}}$ $\overline{\mathfrak{m}_n} / \overline{\mathfrak{m}_{n+1}} \simeq \mathfrak{m}_n / \mathfrak{m}_{n+1}$

and $\operatorname{gr}_{\underline{\mathfrak{m}}} R \simeq \operatorname{gr}_{\overline{\underline{\mathfrak{m}}}} \overline{R}^{\underline{\mathfrak{m}}}$.

<u>Prop. 188</u>: Let R be a ring with filtration $\underline{\mathfrak{m}}$ s.t. $\mathfrak{m}_i \mathfrak{m}_j \subseteq \mathfrak{m}_{i+j}$ $\forall_{i,j \in \mathbb{N}}$.

Suppose R is complete w.r.t. $\underline{\mathfrak{m}}$.
Then ~~are~~ R is noetherian if $\operatorname{gr}_{\underline{\mathfrak{m}}} R$ is noetherian.

<u>Proof</u>: This follows directly from Lemma 185. $\square$

<u>Theorem 189</u>: Let R be a ring and $\mathfrak{m}$ be an ideal of R. Suppose R is noetherian. Then $\overline{R}^{\mathfrak{m}}$ is noetherian.

— 220 —

<u>Proof:</u> R is noetherian.

Cor 183 $\Longrightarrow$ $\mathrm{gr}_{\mathfrak{m}} R$ is noetherian.

$\overset{\text{Cor 187}}{\Longrightarrow}$ $\mathrm{gr}_{(\overline{\mathfrak{m}^n})_{n\in\mathbb{N}}} \overline{R}^{\mathfrak{m}}$ is noetherian.

$\overset{\text{Prop 188}}{\Longrightarrow}$ $\overline{R}^{\mathfrak{m}}$ is noetherian $\square$

<u>Remark 190:</u> If R is noetherian and $\mathfrak{m} \underset{\neq R}{\subset} R$

then $\mathfrak{m}^n \overline{R}^{\mathfrak{m}} = \overline{\mathfrak{m}^n}$ for all $n \in \mathbb{N}$.

<u>Summary:</u> $(\overset{\text{noetherian}}{R}, \overset{\neq R}{\mathfrak{a}})$ be given. $S = \overline{R}^{\mathfrak{a}}$

Then (1) $\mathrm{gr}_{\mathfrak{a}} R \cong \mathrm{gr}_{\mathfrak{a}S} S$

and (2) S is noetherian

and (3) in S we have Hensel's Lemma:

IV.4. Exercise section.

(1) Let R be complete w.r.t. $\mathfrak{a} \trianglelefteq_R R$.
Prove that for $x \in R$ we have
$$x \in R^\times \iff [x]_{\mathfrak{a}} \in \left(R/\mathfrak{a}\right)^\times.$$

(2) Explain Hensel's lemma:
Given $(R, \mathfrak{a})$ and $F \in R[X]$ s.t.
$f := F \bmod \mathfrak{a} \in R/\mathfrak{a}\,[X]$ has a root
$a \in R/\mathfrak{a}$.

<u>Question:</u> $\exists \alpha \in R : F(\alpha) = 0$ and $[\alpha]_{\mathfrak{a}} = a$?

Answer (Hensel's lemma): Yes if R is complete ~~w.r.t.~~ with respect to $\mathfrak{a}$ and $f'(a) \in \left(R/\mathfrak{a}\right)^\times$.

(2.1) Show that 19 is a square in $\mathbb{Z}_5$.

(2.2) Show that 19 is a cube in $\mathbb{Z}_5$.

(2.3) Show that 19 is not a 4th power in $\mathbb{Z}_5$

(2.4) Is 19 a 5th power in $\mathbb{Z}_5$?

V Gröbner bases

<u>Problem</u> (membership problem):

$S := k[X_1, \dots, X_r]$, k a field.

$I \subseteq S$ an ideal. $f \in S$

How to decide (to compute) if $f \in I$?

<u>Example</u> (191:1) $r = 2$. $I := (X^2+Y, X+Y^2) \subseteq \mathbb{R}[X,Y]$.

Is there a monomial in I?

If $X^a Y^b \in I$ with $a, b \in \mathbb{N}_0$ s.t. $a+b>0$

then $\exists\, n \in \mathbb{N}$: $X^n \in I$ or $Y^n \in I$. (Why?)

$\Rightarrow \exists\, R, Q \in \mathbb{R}[X,Y]$: $X^n = (X^2+Y)\,Q + (X+Y^2)\,R$

$$\underset{\substack{Y := -T^2 \\ X := T}}{\Rightarrow} \quad T^n = (T^2 - T^2)\,Q(T, -T^2) + (T + T^4)\,R(T, -T^2)$$

$$= (T + T^4)\,R(T, -T).$$

$\Rightarrow$ -1 is a root of T^n ↯.

So the answer is no.

2) Say $I \subseteq S$ is generated by monomials.

Hilbert's basis theorem $\Rightarrow$ Only finitely many monomials are needed, say $m_1, \dots, m_\ell$

Then $f \in S$:

$f \in I \Leftrightarrow$ Every monomial occuring in f is divisible by one of the m_i.

<u>Ex:</u> $I = (X^2, Z)$.

$X + 2XY \notin I$ and $ZX + X^3 \in I$.

How to proceed if I is not ~~homogen~~ generated by monomials?

$\rightsquigarrow$ Gröbner basis and Buchberger algorithm.

<u>Def 192:</u> A total order "$>$" on the set of monomials of S is called ~~monomial~~ <u>monomial</u> if

$\forall$ monomials m_1, m_2 $\forall$ monomials $n \neq 1$ with $m_1 > m_2$:

$n m_1 > n m_2 > m_2$.

<u>Ex 193:</u> 1) We fix a total order on $\{X_1, \dots, X_r\}$

$X_1 > X_2 > X_3 > \dots > X_r$.

We define $X_1^{a_1} \cdot X_2^{a_2} \cdot X_3^{a_3} \cdot \ldots \cdot X_r^{a_r} > X_1^{b_1} \cdot \ldots \cdot X_r^{b_r}$

iff ($a_1 + \ldots + a_r > b_1 + \ldots + b_r$

or ($a_1 + \ldots + a_r = b_1 + \ldots + b_r$ and

at the first i with $a_i \neq b_i$ we have $a_i > b_i$)

"homogeneous lexicographic order".

2) $X_1 > \ldots > X_r$

$X^{\underline{a}} > X^{\underline{b}} \Leftrightarrow_{def}$ ($a_i > b_i$ at the first index with $a_i \neq b_i$)

"lexicographic order."

3) "reverse lexicographic order" $X^{\underline{a}} > X^{\underline{b}} \Leftrightarrow_{def}$ ($\deg X^{\underline{a}} > \deg X^{\underline{b}}$ or ($\deg X^{\underline{a}} = \deg X^{\underline{b}}$ and $a_i < b_i$ for the last i n.t. $a_i \neq b_i$))

<u>Def 194</u> Let "$>$" be a monomial order on S.

For $f \in S$ and $I \leq_S S$ we put

$$In_>(f) := \begin{cases} 0, & f = 0 \\ \text{the maximal monomial term of } f, & f \neq 0 \end{cases}$$

"initial term of f"

and $In_>(I) = (\{In_>(f) \mid f \in I\})_S$.

"initial ideal of I".

<u>Ex 195</u> 1) $k = \mathbb{R}$, $f = 3X^3Y^3 + X^4Y^2 + 2X^5Z + X^2XZ + 3$

$$\mathrm{In}_{>_{lex}}(f) = 2X^5Z = \mathrm{In}_{>_{hlex}}(f)$$

$$\mathrm{In}_{>_{rlex}}(f) = X^4Z^2$$

2) $k = \mathbb{R}$ $\quad f = 7X^4Z^2 + \frac{3}{5}X^5$

$$\mathrm{In}_{>_{lex}}(f) = \frac{3}{5}X^5$$

$$\mathrm{In}_{>_{hlex}}(f) = 7X^4Z^2 = \mathrm{In}_{>_{rlex}}(f)$$

Exercise: Find a polynomial where $\mathrm{In}_{>_{hlex}}(f)$, $\mathrm{In}_{>_{lex}}(f)$ and $\mathrm{In}_{>_{rlex}}(f)$ are pairwise different.

3) $k = \mathbb{R}$, $I = (X + Z^2, Y + X^2)$

$$\mathrm{In}_{>_{hlex}}(I) = (X^2, Z^2)$$

<u>Proof:</u> Assume $\supseteq$, ~~Take~~ i.e.

$$XZ \in \mathrm{In}_{>_{hlex}}(I).$$

$\Rightarrow \exists f \in I : \mathrm{In}_{>_{lex}}(f) = XZ$, in particular

$f = XZ + bZ + aX + cZ^2$, for $a, b, c \in \mathbb{R}$.

$Z^2 \in \mathrm{In}_{>_{hlex}}(I) \Rightarrow$ W.l.o.g. $c = 0$.

From $f \in I$ follows

$$h := -X^3 - bX^2 + aX \in I$$

Note: h has at most 2 non-zero roots for X in $\mathbb{C}$.

$h \in I \Rightarrow \exists\, Q, R : h = (X^2+Y)Q + (X+X^4)R.$

$\Rightarrow h(T) = (T+T^4)R(T, -T^2)$

$T+T^4$ has 3 different non-zero roots

$\Rightarrow \lightning$ $\square$

4) Find $In_{>_{lex}}(I)$ and $In_{>_{rlex}}(I)$.
($\rightsquigarrow 20^*$ points)

We fix a monomial order "$>$" on S.

<u>Def 196:</u> Let I be an ideal of S.

A set $\{g_1, \dots, g_\ell\} \subseteq I$ is called a Gröbner basis of I if $In_>(g_1), \dots, In_>(g_\ell)$ generate $In_>(I)$.

<u>Prop 197:</u> If $\{g_1, \dots, g_\ell\}$ is a Gröbner basis of I then $I = (g_1, \dots, g_\ell)S$.

<u>Proof:</u> Easy. $\square$

In fact we have

<u>Prop 198:</u> Suppose $\mathfrak{a} \subseteq \mathfrak{b}$ are ideals in S s.t. $In_>(\mathfrak{a}) = In_>(\mathfrak{b})$. Then $\mathfrak{a} = \mathfrak{b}$.

<u>Proof:</u> Easy $\square$

<u>Remark 199.</u> 1) We can decide if $f \in I$ is checking if $In_>(I) = In_>(I + fS)$.

2) This gives the following abstract concept:

$I = (g_1, \dots, g_\ell)_S$ $\{g_1, \dots, g_\ell\}$ is a Gröbner basis.

$f \in S$.

<u>Step 1:</u> Check $\mathrm{In}_>(f) \in \mathrm{In}_>(I)$, i.e. " if all monomial terms of f are divisible by one of the $\mathrm{In}_>(g_i)$.

No $\longrightarrow$ $f \notin I$

Yes $\longrightarrow$ Go to step 2.

<u>Step 2:</u> Check if $\{g_1, \dots, g_\ell, f\}$ is a Gröbner basis.

Yes $\longrightarrow$ $f \in I$

No $\longrightarrow$ $f \notin I$.

3) Once we are given a Gröbner basis $\{g_1, \dots, g_\ell\}$ for I we have an algorithm to decide the membership problem.

Take $f \in S$. Question $f \in S$?

<u>Step 1:</u> $\mathrm{In}_>(f) \in \mathrm{In}_>(I) = (\mathrm{In}_>(g_1), \dots, \mathrm{In}_>(g_\ell))$?

If "no", then terminate and return "No".

If "Yes", say $\mathrm{In}_>(g_{i_0}) \mid \mathrm{In}_>(f)$, then

replace f by $f - \frac{\mathrm{In}_>(f)}{\mathrm{In}_>(g_{i_0})} g_{i_0}$ ~~and go~~

<u>Step 2!</u> If $f \neq 0$, then go to
to Step 1,
else terminate and return "Yes".

So we need to know how to find a Gröbner basis for I.

<u>Def 200</u> (division with remainder)

Let $f, g_1, \dots, g_\ell \in S$. Then $\exists\ f_1, \dots, f_\ell, r \in S$:

$$\left.\begin{array}{l} f = \sum_{i=1}^{\ell} f_i g_i + r \quad \text{s.t.} \\ \mathrm{In}_>(f) \geq \mathrm{In}_>(f_i g_i) \text{ for all } i = 1, \dots, \ell \\ \text{and such that no monomial term of } r \\ \text{is divisible by one of the } \mathrm{In}_>(g_i). \end{array}\right\} \text{(SF)}$$

We call such an expression a standard expression of f in terms of $g_1, \dots, g_\ell$.

Example 201: $k = \mathbb{R}$ $g_1 = X + Y^2$, $g_2 = X^2 + Y$.

$$f = X^4 Y + 2X^2 Y + X + Y$$

$>_{ex}$: $$f = X^2 Y g_1 + (-Y^2) X^2 + 2X^2 Y + X + Y$$
$$= (X^2 Y - Y^2 + 2Y) g_1 + Y^3 - 2Y^2 + X + Y$$
$$= (X^2 Y - Y^2 + 2Y) g_1 + g_2 + \underbrace{Y^3 - 3Y^2 + Y}_{r}$$

$In_>(g_1) >> In_>(g_2)$

This is not unique

$$f = (X^3 Y + 2XY + 1) g_2 - X^3 Y^3 - 2XY^3 - Y^2 + Y$$
$$= (-X^2 Y^3 - 2Y^3 + X^3 Y + 2XY + 1) g_2 + X^2 Y^5 + 2Y^5 - Y^2 + Y$$
$$= (-X^2 Y^3 - 2Y^3 + X^3 Y + 2XY + 1 + XY^5 - Y^7) g_2 + Y^9 + 2Y^5 - Y^2 + Y.$$

$>_{lex}$: $In_>(g_1) = X^2 >_{lex} Y^2 = In_>(g_2)$

$$f = (X^2 Y - Y^2 + 2Y) g_1 + Y^3 - 2Y^2 + X + Y$$
$$= (X^2 Y - Y^2 + 2Y) g_1 + (Y - 2) g_2 \underbrace{- (Y-2) X + X + Y}_{r}$$

<u>Remark: 202:</u> Say $(g_1, \dots, g_\ell)_S = I$ and all

$g_i \neq 0$

Take $f \in I \setminus \{0\}$.

Then $f = \sum_{i=1}^{\ell} \left(\sum_{j=1}^{r_i} \lambda_{ij} n_{i,j} \right) g_i$

with $\lambda_{ij} \in k$ and $n_{i,1} > n_{i,2} > \dots > n_{i,r_i}$

Suppose w.l.o.g. that $g_1, \dots, g_\ell$ are monic w.r.t. ">".

If the sum has at least two terms

$n_1 g_{i_1}$ and $n_2 g_{i_2}$ such that

$\mathrm{In}_>(n_1 g_{i_1}) = \mathrm{In}_>(n_2 g_{i_2})$ then

$f = \lambda_1 n_1 g_{i_1} + \lambda_2 n_2 g_{i_2} +$ other terms

$= \lambda_1 n_1 g_{i_1} + \lambda_2 n_1 g_{i_1} + \lambda_2 (n_2 g_{i_2} - n_1 g_{i_1}) + \dots$

$= (\lambda_1 + \lambda_2) n_1 g_{i_1} + \quad - \quad '' \quad -$

If $(n_2 g_{i_2} - n_1 g_{i_1})$ can be written with

$m g_i$ s.t. $\mathrm{In}_>(m g_i) < \mathrm{In}_>(n_1 g_{i_1})$

then we can reduce the summands max. w.r.t. ">".

This gives the following.

<u>Theorem 203:</u> Let $(g_1, \dots, g_\ell)_S = I$ with $g_i \neq 0, i=1,\dots,\ell$.
(Buchberger Criterion)
Define $\sigma_{ij} := m_{ij} g_i - m_{ji} g_j$ ~~tsh~~ with

$$m_{ij} := \frac{\mathrm{In}_>(g_j)}{\gcd(\mathrm{In}_>(g_i), \mathrm{In}_>(g_j))} \quad \text{for all } i \neq j.$$

Suppose that for every $i \neq j$ we have ~~the~~ a standard expression

$$\sigma_{ij} = \sum_{u} f_{u,ij}\, g_u + h_{ij}.$$

Then $\{g_1, \dots, g_\ell\}$ is a Gröbner basis for I if and only if $\forall_{i \neq j}\ h_{ij} = 0$.

<u>Proof:</u> "$\Leftarrow$" By Remark 202. Because $0 \neq f \in I$ can be written as

$$f = r_1 g_{i_1} + r_2 g_{i_2} + r_3 g_{i_3} + \dots + r_t g_{i_t}$$

with $\mathrm{In}_>(r_1 g_{i_1}) > \mathrm{In}_>(r_2 g_{i_2}) > \dots > \mathrm{In}(r_t g_{i_t})$

So $\mathrm{In}_>(f) = \mathrm{In}_>(r_1 g_{i_1}) \in \mathrm{In}_>(I)$.

"$\Rightarrow$" $h_{ij} \in I \Rightarrow \mathrm{In}_>(h_{ij}) \in \mathrm{In}(I) = \langle \mathrm{In}_>(g_i) \mid i \rangle_S$

No term of h_{ij} is divisible by any $\mathrm{In}_>(g_i)$

So $h_{ij} = 0$. $\square$

<u>Remark 204:</u> (Buchberger algorithm)

Start with $(g_1, \dots, g_e) = I$. with $g_i \neq 0 \; \forall i = 1, \dots, e$.

Put $T := \{g_1, \dots, g_e\}$.

Compute all the h_{ij} by division with remainder.

Until all $h_{ij} = 0$ do

Take one non-zero h_{ij}

and ~~put T:=~~ replace T by $T \cup \{h_{ij}\}$

Compute all h_{ij} w.r.t. T.

return T

<u>Example 205:</u> 1) $I = (\underbrace{X + Y^2}_{g_2}, \underbrace{X^2 + Y}_{g_1})$

and $> = >_{lex}$.

$$s_{1,2} = \frac{\mathrm{In}_>(g_2)}{\gcd(\;)} g_1 - \frac{\mathrm{In}_>(g_1)}{\gcd(\;)} g_2 = g_1 - X g_2$$

$$= X^4 + Y - X^2 - XY^2$$

$$= -XY^2 + Y$$

$$s_{1,2} = -Y^2 g_2 + \underbrace{Y^4 + Y}_{h_{12}}$$

2: $h_{12} \neq 0$ $\qquad g_3 = Y^4 + Y$

So put $T = \{g_1, g_2, h_{12}\}$

$\sigma_{1,2}$ as above now with $h_{12} = 0$

$$\sigma_{1,3} = Y^4 g_1 - X^2 g_3 = Y^5 - X^2 Y = -Y g_1 + Y^5 + Y^2$$

$$= -Y g_1 + Y g_3 \quad \text{so } h_{1,3} = 0$$

$$\sigma_{2,3} = Y^4 g_2 - X g_3 = Y^6 - XY = -Y g_2 + Y^3 + Y^6$$

$$= -Y g_2 + Y^2 g_3 \Rightarrow h_{2,3} = 0.$$

Thus T is a Gröbner basis.

In particular $\mathrm{In}_{>_{lex}} I = (X^2, X, Y^4)_S = (X, Y^4)_S$

2) $> = >_{lex}$: $\qquad g_1 = X^2 + Y, \; g_2 = X + Y^2$

$$\sigma_{1,2} = Y^2 g_1 - X^2 g_2 = Y^3 - \cancel{X^2 Y^2} X^3$$

$$\cancel{= -Y^2 g_1 + Y^3 + Y^3}$$

$$\cancel{= -Y^2 g_1 + Y g_2 - Y^3}$$

$$= -X g_1 + XY + Y^3 = -X g_1 + Y g_2$$

So $h_{12} = 0$.

$\Rightarrow \{g_1, g_2\}$ is a Gröbner basis w.r.t. $>_{lex}$.