Commutative Algebra

· Spring 2024 .
· Prof: A. Buch

Author: Carlos Tapp

Advice for the reader: This set of notes is taken from the course Math 559 Commutative Algebra at Rutgers during Spring 2024 by A. Buch. In that class we were mainly following Eisenbud's book "Commutative algebra with a view towards Algebraic Geometry".

I organized the notes in two parts. The first concerning basic constructions and the second one dimension theory. Each part is divided in sections (1-28) which kind of match with sections from Eisenbud; at the start of each section I write the main reference. In between sections 12 and 14 there are 4 "sections" named A, B, C, D which were not covered in class (I added because I wanted to make sure I knew the material)

The reader should know that my goal writing this is to learn myself so at many points I wrote extra details (and extra results) that were not mentioned in class. These extra words are usually written in this colour.
I also make reference to other set of notes that I have and other type of material, sorry for that.

Any mistake here is of course my fault and not the instructor's fault.

Commutative algebra is a toolbox for Algebraic Geometry, number theory and invariant theory. We will "follow" Eisenbud's textbook. The main difference with Atiyah-Macdonald is that the later gives a direct and unmotivated exposition (this might also have benefits). Eisenbud's book is huge so I will primarily write here what Buch does in class / assigns for exercise or reading and I will have the book as a source of context, notation, extra topics and simultaneous reading of what he covers (know where things are). The most elementary things that I do not say here are in Alg qual notes. (ch on rings and intro to modules) Also pag 11-15 of Eisenbud contain very elementary things. I will assume this known, but I'll repeat things if needed. After this course I hope Alg geo will be digested more easily and also that this and number thy will be very well complemented.

Some things here, I have already covered them. But If Anders does it I will repeat the proof.

VIDEO: Geometry discussions.

Sections 1.2, 1.3, 1.4 give nice historic comments on N.Thy / Alg geo / Inv. Theory.

In this course a ring means commutative ring with 1 (The 0 ring is part of our rings)

Ring homs take $1 \to 1$.

Part 1: Basic constructions.

(Video Trivial note)

1. THE BASIS THEOREM

(~ 1.4 Eisenbud)

DEF Let R be a ring. We say that R is noetherian if every ideal is finitely generated.

$$\left(\begin{matrix} I = Ra_1 + \cdots + Ra_n \\ \text{note } Ra_1 = a_1R = Ra_1R \end{matrix} \right)$$

(Quotient of noeth is noeth; save for Artinian)

Prop 1 Let R be a ring, TFAE

i) R is noetherian

ii) Every ascending chain of ideals stabilizes

iii) Every collection of ideals has a maximal element

Proof/ See alg qual notes.

Example Let K be a field, then $K[x_1, \ldots, x_n]$ the polynomial ring (of course) in n-variables is noetherian. Why?

Thm 2 (Hilbert basis thm) Let R be a ring. R noetherian $\longrightarrow$ $R[X]$ (poly ring.) noetherian.

Proof/ Assume I is an ideal in $R[X]$ not fg. Choose $f_1 \in I \setminus \{0\}$ of minimal degree. Of course has degree ≥ 1 (if the ideal is $\subseteq R$ then is fg). By induction choose

$f_i \in I \setminus \langle f_1, \ldots, f_{i-1} \rangle$ of minimal degree. Let $a_i \in R$ be the leading coefficient of f_i

ideal generated by; as it was said on alg qual notes $A \subseteq R$, $\langle A \rangle$ ideal gen by and if $A = \{a_1, \ldots, a_n\}$, $\langle A \rangle := \langle a_1, \ldots, a_n \rangle$.

Let $J := \langle a_1, -, a_i, .. \rangle \subseteq R$. Since R noetherian $J = \langle a_1, -, a_m \rangle$ for some n. Then $a_{m+1} = \sum_{i=1}^{m} r_i a_i$ with $r_i \in R$. Let $f' := f_{m+1} - \sum_{i=1}^{m} r_i f_i x^{\deg f_{m+1} - \deg f_i}$

By construction $\deg(f') < \deg(f_{m+1})$ and $f' \in I \setminus \langle f_1, -, f_m \rangle$ which is a contradiction $\square$

(and gives a corollary of thm 2)

Now Eisenbud on p. 28 covers Noetherian Modules, we will cover it in sec 5. (not the corollary).

We work toward algebraic geometry (Buch is an alg. geometer)

2. ALGEBRA AND GEOMETRY

(≃ 1.6 Eisenbud)

Fundamental thm of algebra establishes the link between algebra and geometry.

" $\underbrace{f \in \mathbb{C}[x]}_{\text{Alg object}}$ determined up to scalar by $\underbrace{\text{the set of roots with multiplicities}}_{\text{Geometric object}}$ "

(saying geometric object is smth purely intuitive)

Hilbert's Nullstellensatz extends this link to certain ideals of polys in many variables.

- let k be a field, $\mathbb{A}^n = k^n = \overset{\text{n-tuples}}{k \times \cdots \times k}$ is usually called the affine space of dim n.

It is appropriate to forget the vector space structure for our purposes. (Buch said)

Given $f \in k[x_1, -, x_n]$ we define $f : \mathbb{A}^n \longrightarrow k$

$$(a_1, -, a_n) \longmapsto f(a_1, -, a_n)$$

If we just say A^n we understand that there is an underlying k. (maybe specified maybe not)

Exercise: Let K be an infinite field. Then $f = 0$ as a function iff $f = 0 \in K[x_1, -, x_n]$

In finite fields doesn't happen

alg closed fields are infinite.

Proof/ • Let $K = F_2$ the field with 2 elements. $f = x(x-1) \in K[x] \setminus \{0\}$ but $f : \{0, 1\} \longrightarrow F$

$$0 \longmapsto f(0) = 0$$
$$1 \longmapsto f(1) = 0$$

• $\longleftarrow$) Clear

number of variables of poly. ring over a field.

$\longrightarrow$) Suppose $f \in K[x_1, -, x_n] \setminus \{0\}$ We proceed by induction on n to prove $f \neq 0$ as a function on A^n.

<u>n=1</u> A polynomial in one variable can have only finitely many roots by division algorithm. Since $|K| = \infty$, $\exists \alpha \in K : f(\alpha) \neq 0$ as wanted

<u>Induction step</u> $f(x_1, -, x_n) \in K[x_1, -, x_n] \setminus \{0\}$ (WMA x_i appears in f $\forall i = 1, -, n$; otherwise induction applies) See this as a polynomial $(K[x_1])([x_2, -, x_{n-1}])$ ie with coefficients in $K[x_1]$, and $n-1$ variables. We substitute x_1 by α_1 so that some coefficient of our expression is nonzero (can do this by the case $n=1$). This yields a nonzero pol in $n-1$ variables. By induction $\exists$ $(\alpha_2, -, \alpha_n) \in K^{n-1}$ st the poly evaluated at that point is $\neq 0$. $(\alpha_1 \alpha_2, -, \alpha_n)$ is a point in which $f(\alpha_1, -, \alpha_n) \neq 0$.

Corollary 3 If $|K| = \infty$, $f \neq g \in K[x_1, -, x_n]$ then $f \neq g : \mathbb{A}^n \longrightarrow K$.

So we may regard $K[x_1, -, x_n]$ as the ring of polynomial functions on $\mathbb{A}^n$.

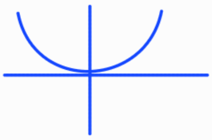
There is a set theoretic difference but the two rings are isomorphic. Also the notation we always use makes the identification totally natural. (I see this more as a "be careful in finite fields")

DEF If $I \subseteq K[x_1, -, x_n]$ is a subset then the vanishing set of I is defined to be

$$Z(I) = \{a \in \mathbb{A}^n \mid f(a) = 0 \ \forall f \in I\}$$; this is called an algebraic set

(affine alg sets to distinguish from future objects)

The study of algebraic sets is the root of alg geometry. (solutions of systems of polynomial eqn)

Example : $I = \{y - x^2\} \subseteq \mathbb{R}[x,y]$, $Z(I) =$  $\subseteq \mathbb{R}^2$

Observations i) $I \subseteq J \subseteq K[x_1, -, x_n]$, then $Z(I) \supseteq Z(J)$

All are trivial to prove

ii) Let $I \subseteq K[x_1, -, x_n]$, $Z(\langle I \rangle) = Z(I)$. [So when we study alg sets we can see them as $Z(I)$ where $I \trianglelefteq K[x_1, -, x_n]$. And since I is fg by $f_1, -, f_k$ then again using this $Z(I) = Z(\{f_1, -, f_k\})$ So we are studying the solutions of finite systems of polynomial equations]

iii) Let $I_\alpha \subseteq K[x_1, -, x_n]$, $\alpha \in A$ arbitrary indexing set

$$\bigcap_{\alpha \in A} Z(I_\alpha) = Z\left(\bigcup_{\alpha \in A} I_\alpha\right)$$

iv) Let $I_1, \dots, I_m \subseteq K[x_1, -, x_n]$

$Z(I_1) \cup \dots \cup Z(I_m) = Z(I_1 \cdots I_m)$ where $I_1 \cdots I_m = \{a_1 \cdots a_m \mid a_i \in I\}$.

Usually I_i will be ideals and $I_i I_j = \{$ sums of $a_i b_j$ with $a_i \in I_i, b_j \in I_j\}$ as usual. And $Z(I_i I_j)$ is the same no matter what notation we use. But in a ring $A, B \subseteq R$ generally means $\{ab \mid a \in A, b \in B\}$, but if $A, B \trianglelefteq R$ then dis

v) $Z(\{0\}) = \mathbb{A}^n \wedge Z(\mathbb{A}^n) = \emptyset$

We define a topology on $\mathbb{A}^n$ by setting the closed sets to be the algebraic subsets (note that by the previous observation this indeed defines a topology) It is called Zariski Topology

Let $n = 1$, $\underset{= \mathbb{R}}{K = \mathbb{C}}$, then the open subsets are the cofinite sets (complement is finite) [Clear]

Given $X \subseteq \mathbb{A}^n$ we define $I(X) = \{f \in K[x_1, -, x_n] : f(a) = 0 \ \forall a \in X\} \subseteq K[x_1, -, x_n]$

note it is an ideal of $K[x_1, -, x_n]$.

Note If $f, g \in K[x_1, -, x_n]$ and define the same function $f = g : \overset{\subseteq \mathbb{A}^n}{X} \longrightarrow K$

then $f - g \in I(X)$ so $\bar{f} = \bar{g} \in K[x_1, -, x_n] / I(X)$

For this reason we define

DEF Let $X \subseteq k^n$ (usually an algebraic set), $A(X) := k[x_1, -, x_n]/I(X)$ is the coordinate ring of X.

This should be interpreted as the ring of polynomial functions at X (since we are identifying two elements of $k[x_1, -, x_n]$ ie two polynomial functions on $\mathbb{A}^n$ if they agree on X ie if they define the same polynomial function on X.

× The reason for that name is that it is the k-algebra of functions on X generated by the coordinate functions x_i

↳ More formal: Define $A(X)$ to be the ring of polynomial functions on X. Then it is a fact that $A(X) \cong k[x_1, -, x_n]/I(X)$ and we identify them.

This gives dictionary between Alg. Geo and commutative algebra: Alg Geo $\longleftrightarrow$ Com alg

X $\longleftrightarrow$ $A[X]$.

alg set — coordinate ring

Facts: i) Let $J \subseteq k[x_1, \dots, x_n]$ then, $J \subseteq I(Z(J))$

ii) Let $X \subseteq k^n$, then $X \subseteq Z(I(X))$

Trivial.

DEF Let R be a ring $I \subseteq R$ an ideal, $\sqrt{I} := \{ f \in R : \exists n \geqslant 1 : f^n \in I \}$ is called the radical of I. We say that an ideal I is radical if $\sqrt{I} = I$

Note $\sqrt{I}$ is itself an ideal.

(It contains the nth roots of the elements in I)

Facts i) $\sqrt{I} \subseteq R$ is radical ideal.

ii) Recall that $P \subseteq R$ an ideal is said to be prime if $P < R \wedge ab \in P$ implies $a \in P \vee b \in P \vee$ $a, b \in P$

Recall
- P prime $\leftrightarrow$ R/P integral domain
- I maximal $\leftrightarrow$ R/I field
- I maximal $\longrightarrow$ I prime

Prime ideals are all radical.

Trivial.

If k is alg closed, $f \in k[X]$ it factors as a product of degree 1 polynomials. It is easy to see that if $I = (f)$, $I = \sqrt{I}$ iff has no multiple roots. In this case If $X = \{$roots of $f\}$, $I(X) = I$. The next theorem extends this to many variables. It is the main connection between algebra and geometry.

↙ where are the zeros ↙ see beginning of sec 14 for more info.

Theorem 4 (Hilbert Nullstellensatz) Let $k = \bar{k}$. If $J \subseteq k[x_1, -, x_n]$ ideal. Then $I(Z(J)) = \sqrt{J}$. Thus the map

$$\{\text{alg subset of } \mathbb{A}^n = \mathbb{K}^n\} \longleftrightarrow \{\text{radical ideal of } k[x_1, -, x_n]\} \text{ is a bijection}$$

$$X \text{ is } Z(J) \ J \text{ ideal} \longrightarrow I(X)$$

$$Z(J) \longleftarrow J$$

· $Z(J) = Z(\sqrt{J})$ elementary; needs no assumption on k. (Helps to see the bijection)

We will prove this later. For now, some consequences

<u>Corollary 5</u> Let k be alg closed, $f_1, \dots, f_m \in k[x_1, \dots, x_n]$. Then

$$\langle f_1, \dots, f_m \rangle = \langle 1 \rangle \text{ iff } Z(\{f_1, \dots, f_m\}) = \emptyset .$$

. Read: 1 can be written as a k linear comb of f_i iff the system $\left\{ \begin{array}{l} f_1(x_1, \dots, x_n) = 0 \\ \vdots \\ f_m(x_1, \dots, x_n) = 0 \end{array} \right.$ has no sol.

Proof/ $\longrightarrow$) $Z(\{f_1, \dots, f_m\}) = Z(\langle 1 \rangle) = \emptyset$

$\longleftarrow$) Let $J = \langle f_1, \dots, f_m \rangle$, $\langle 1 \rangle = I(\emptyset) = I(Z(\{f_1, \dots, f_m\}) = I(Z(J)) = \sqrt{J}$. So $1 \in \sqrt{J}$ so $1 \in J$ hence $J = \langle 1 \rangle$. □

These corollaries (any of them) are called Weak Nullstellensatz and Thm 4 can be deduced from them (see alg geo notes)

<u>Corollary 6</u> Let $k = \overline{k}$ every maximal ideal $J \subsetneq k[x_1, \dots, x_n]$ has the form $J = \langle x_1 - a_1, \dots, x_n - a_n \rangle$ for $a = (a_1, \dots, a_n) \in \mathbb{A}^n$.

Proof/ Suppose J is maximal then $1 \notin J$ so $1 \notin \sqrt{J} \overset{\text{always}}{\supseteq} J$. By maximality we have

$$J = \sqrt{J} = I(Z(J)) \underset{\substack{\downarrow}}{\subseteq} I(\{a\}) = \langle x_1 - a_1, \dots, x_n - a_n \rangle$$

By the last corollary
$Z(J) \neq \emptyset$ so $\exists a \in Z(J)$
Note we are using $k[x_1, \dots, x_n]$ noeth.

So $\supseteq$) is trivial. If we show that the RHS is a maximal ideal then we are done by maximality. To do this I personally want to take a general approach.

Useful: Let R be a ring then $R[x_1, \dots, x_n] / (x_1 - a_1, \dots, x_n - a_n) \cong R$

Informal: You are identifying x_i with a_i so $R[x_1, \dots, x_n] = R$

Proof/ Let $\varphi : R[x_1, \dots, x_n] \longrightarrow R$ surj ring hom.

$$r \longmapsto r$$
$$x_i \longmapsto a_i$$

Let $f \in \ker \varphi$. Then $f(x_1, \dots, x_n)$ vanishes at $(a_1, \dots, a_n)$.

<u>Claim</u> $f(x_1, \dots, x_n) = f(a_1, x_2, \dots, x_n) + (x_1 - a_1) g(x_1, \dots, x_n)$.

Observe for $m \geq 0$, $x_1^m - a_1^m \underset{\downarrow}{=} (x_1 - a_1) t(x_1)$. Hence $x_1^m = a_1^m + (x_1 - a_1) t(x_1)$

$x_1 - a_1$ has leading term a unit so we have div alg
For example in Ch 16 Isaacs Algebra.

Now for each monomial of $f(x_1, \dots, x_n)$ we have x_1 appearing with power m_i (i runs through the monomials)

Substitute $x_1^{m_i}$ by $a_1^{m_i} + (x_1 - a_1) t_1(x_1)$

Each monomial decomposes into 2. One is the original with x_1 substituted by a_1 and the other is just $(x_1 - a_1) \cdot$ something.

We add them all and get $f(x_1, \dots, x_n) = f(a_1, x_2, \dots, x_n) + (x_1 - a_1) g(x_1, \dots, x_n)$ //

We now apply this again and get $f(x_1, \dots, x_n) = f(a_1, a_2, x_3, \dots, x_n) + (x_2 - a_2) g_1(x_1, \dots, x_n) + (x_1 - a_1) g(x_1, \dots, x_n)$. Applying this $n-2$ more times we get $f(x_1, \dots, x_n) = f(a_1, \dots, a_n) + e$ where $e \in \langle x_1 - a_1, \dots, x_n - a_n \rangle$ but $f(a_1, \dots, a_n) = 0$ hence $f \in \langle x_1 - a_1, \dots, x_n - a_n \rangle$

So $\ker \varphi \subseteq \langle x_1 - a_1, \dots, x_n - a_n \rangle$. Hence $R[x_1, \dots, x_n] / \langle x_1 - a_1, \dots, x_n - a_n \rangle \simeq R$.

$\supseteq$ Obvious. Note I prove this.

So with this $k[x_1, \dots, x_n] / \langle x_1 - a_1, \dots, x_n - a_n \rangle \simeq k$ so a field hence $\langle x_1 - a_1, \dots, x_n - a_n \rangle$ is always maximal. (nullstellensatz gives the converse). ☐

This shows that points in $\mathbb{A}^n$ are in bijective corresp to maximal ideals of $k[x_1, \dots, x_n]$. (also in $A(X)$ by the corresp. thm; Eisenbud does it this way).

Fact If R ring I ideal then it is contained in a maximal ideal.
Buch proved this a bit later but it is Thm 16 of Alg qual notes (Intro to rings)
Recall uses Zorn's lemma: | Every totally ordered subset of A poset is dominated by an elmt of A then A has a maximal elmt.

And it takes $A = \{$proper ideals $\supseteq I\}$ ordered by inclusion.

Eisenbud writes the action of R on the left. We define $mr := rm$ this we know it causes no trouble since R commutative (read first page on modules of D&F)

3. LOCALIZATION

($\simeq$ 2.1 Eisenbud).

Note: Eisenbuds introduction to ch2 has a nice motivation to localization via alg geometry example

DEF Let R be a ring, $U \subseteq R$ subset. We say that U is multiplicatively closed if

- $1 \in U$
- $f, g \in U \longrightarrow fg \in U$

(not subring since not necessarily closed under addition)

Given R a ring, U multiplicatively closed, M an R-module we define $U^{-1}M := M[U^{-1}] :=$

$$\underset{\text{cartesian product}}{(M \times U)} / \sim \quad \text{where } (m,u) \sim (m',u') \text{ if } \exists v \in U: \ v(mu' - m'u) = 0$$

(Generalization of ring of fractions)

We call this the localization of M at U. We denote by $\frac{m}{u} = [(m,u)] \in U^{-1}M$

Make it possible to divide by u.

- $U^{-1}M$ carries a natural structure of R-module

The operations are (of course one needs to check this is well defined in the quotient and the operations in the denominator and numerator are the ones in M as an R-module)

$$\cdot \ \frac{m}{u}+\frac{m'}{u'}=\frac{u'm+um'}{uu'} \qquad \cdot \ r\left(\frac{m}{u}\right)=\frac{rm}{u}$$

. Note that $\frac{u'm}{u'u}=\frac{m}{u}$ (because $1\in U$, $(u'm, u'u)\sim(m,u)$)

and also note that the additive inverse of $\frac{m}{u}$ is $\frac{(-m)}{u}$

. If $U\subset R$, and $\bar{U}$ is the multiplicatively closed set of products in U, $U^{-1}M := \bar{U}^{-1}M$

- If we take M to be R, then $U^{-1}R$ happens to be a ring

The operations are $\frac{r}{u}+\frac{r'}{u'}=\frac{u'r+ur'}{uu'}$, $\frac{r}{u}\cdot\frac{r'}{u'}=\frac{rr'}{uu'}$

- Finally, if R ring, $\overset{\subseteq R}{U}$ mult. closed, M R-module; we have that $U^{-1}M$ is an $U^{-1}R$- module

$U^{-1}R$ is a ring, $U^{-1}M$ has an additive group structure as above and

$$\frac{r}{u}\left(\frac{m}{u'}\right) := \frac{rm}{uu'} \quad \text{for } r\in R,\ m\in M,\ u,u'\in U.$$

Notation Let $f\in R$, let $U:=\{f^n : n\in\mathbb{Z}_{\geq 0}\}$ we write $M_f := U^{-1}M = \{\frac{m}{f^n}\}$ "local f"

Exercise: let $\varphi: M\to N$ be an R module hom, let $U\subseteq R$ be a mult closed set

Then $\tilde{\varphi}: U^{-1}M \longrightarrow U^{-1}N$ is a $U^{-1}R$-module hom. (R-mod hom = R-hom = R-linear)

$$\frac{m}{u} \longrightarrow \frac{\varphi(m)}{u}$$

(See stupid Rmk in Rec 26)

This is just trivial checks, $\tilde{\varphi}$ is denoted by $\varphi[U^{-1}]$ by Eisenbud and he calls it localization of φ.

- **Note** Let R be a ring, U mult closed subset then $\pi: R\longrightarrow U^{-1}R$ is a ring hom

$$r \longmapsto \frac{r}{1}$$

Important : π is 1-1 iff U contains no zero divisor.

a ∈ R zero divisor if ∃ b ∈ R \ {0} : ab = 0

$\longrightarrow$) Assume it contains $\overset{\in U}{a}$ zero divisor. Take $b\in R\setminus\{0\}$ st $ab=0$.

Then $\frac{b}{1}-\frac{b}{a}=\frac{ab-b}{a}=\frac{-b}{a}$ So $\frac{b}{1}=0$ in $U^{-1}R$

Hence $0\neq b\in \ker\pi$ so π not injective.

$\longleftarrow$) Suppose not injective so $\exists\, r_1\neq r_2$ st $\frac{r_1}{1}=\frac{r_2}{1}$ $\exists\, v\in U$ such that $v(r_1-r_2)=0$

thus $v\in U$ is a zero divisor ⨍. So 1-1.

So If U has no zero divisors we have R as a subring of $U^{-1}R$ (with surgery)

We have recovered "ring of $\overset{\text{alg qual}}{\text{fractions}}$". If $U=R\setminus\{0\}$ has no zero divisors we get a field

This is what we call field of fractions and this is a generalized construction of $\mathbb{Q}$.

(As a further cavet I will just state the obvious analogue for modules.

"DEF" $\delta \in R$ is a nonzero divisor on M (nzd) an R-module if $\begin{array}{c} M \longrightarrow M \\ m \longmapsto \delta m \end{array}$ is 1-1.

Ex: $\begin{array}{c} M \longrightarrow U^{-1}M \\ m \longrightarrow \frac{m}{u} \end{array}$ is 1-1 iff $\forall u \in U$, u is a nzd on M.)

Theorem 7 (Universal property of Localization) Let $\varphi : R \longrightarrow S$ be a ring hom such that $\forall u \in U$ mult closed subset $\varphi(u)$ is a unit in S then $\exists ! \ \varphi' : U^{-1}R \longrightarrow S$ ring hom st

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[dr, "\pi"'] & S \\ & U^{-1}R \arrow[u, "\varphi'"'] \end{tikzcd}$$

commutes.

Proof/ Let $\begin{array}{c} \varphi' : U^{-1}R \longrightarrow S \\ \frac{r}{u} \longmapsto \varphi(r)\varphi(u)^{-1} \end{array}$, takes $1_{U^{-1}R}$ to 1_S

Well defined $\frac{r}{u} = \frac{r'}{u'}$ then $\exists u'' \in U : \ u''(ru' - r'u) = 0$ so

$\varphi(u'')(\varphi(ru') - \varphi(r'u)) = 0$. So since $\varphi(u'')$ unit then $\varphi(r)\varphi(u') = \varphi(r')\varphi(u)$

Now since $\varphi(u), \varphi(u')$ units $\varphi(r)\varphi(u)^{-1} = \varphi(r')\varphi(u')^{-1}$

Ring hom

- $\varphi'\left(\frac{r}{u} + \frac{r'}{u'}\right) = \varphi(ru' + r'u)\varphi(uu')^{-1} = (\varphi(r)\varphi(u') + \varphi(r')\varphi(u))\varphi(u)^{-1}\varphi(u')^{-1} =$
  $= \varphi(r)\varphi(u)^{-1} + \varphi(r')\varphi(u')^{-1}$
- $\varphi'(r/u) + \varphi'(\frac{r'}{u'}) = \varphi(r)\varphi(u)^{-1} + \varphi(r')\varphi(u')^{-1}$ ✓
- $\varphi(\frac{r}{u}\frac{r'}{u'}) = \varphi(rr')\varphi(uu')^{-1} = \varphi(r)\varphi(u)^{-1}\varphi(r')\varphi(u')^{-1} = \varphi(r/u)\varphi(r'/u')$

Uniqueness $\frac{r}{u} = \frac{r}{1}\frac{1}{u}$; Suppose that φ'' is other such hom, $\varphi''(r/u) = \varphi''(r/1)\varphi''(\frac{1}{u})$

$= \varphi(r)\varphi''(1/u)$. Now, $1 = \varphi(1) = \varphi''(\frac{u}{u}) = \varphi''(\frac{u}{1}\cdot\frac{1}{u}) = \varphi''(\frac{u}{1})\varphi''(1/u) =$

$= \varphi(u)\varphi''(1/u)$ so $\varphi''(1/u) = \varphi(u)^{-1}$ and we are done □

DEF Let $\varphi : R \longrightarrow S$ a ring hom

i) $J \subseteq S$ an ideal, then $R \cap J := \varphi^{-1}(J) \subseteq R$ an ideal

ii) $I \subseteq R$ an ideal then $IS := \varphi(I)S = \langle \varphi(I) \rangle$ of course an ideal.

Note that : $I \subseteq R \cap (IS)$, $(R \cap J)S \subseteq J$

DEF Let R be a ring, we will call spec (R) = {prime ideals in R} ⊇ {Maximal}

Prop 8 let $\pi : R \longrightarrow U^{-1}R$ where R ring, U mult closed set in R.
$\qquad r \longmapsto r/1$

i) Let $J \subseteq U^{-1}R$ be an ideal. $(R\cap J)U^{-1}R = J$

ii) $\mathrm{Spec}(U^{-1}R) \longrightarrow \{P \in \mathrm{Spec}(R) : P\cap U = \emptyset\}$ is a bijection
$\qquad Q \longmapsto R\cap Q$

Pf/ i) By the note $(R\cap J)U^{-1}R \subseteq J$. Let $r/u \in J$, because this is an ideal $\frac{r}{1} = \frac{u}{1}\frac{r}{u} \in J$ then $r \in R\cap J$ so $\frac{r}{1} \in (R\cap J)U^{-1}R$ and since this is an ideal $\frac{r}{1}\cdot\frac{1}{u} \in (R\cap J)U^{-1}R$ so $\frac{r}{u} \in (R\cap J)U^{-1}R$

ii). $R\cap Q$ ideal of R: see def above

. $R\cap Q$ prime is easy: Q is prime, assume by contradiction $R\cap Q$ not prime
$\exists\, ab \in R\cap Q$ such that $a \notin R\cap Q$ $b \notin R\cap Q$. Recall $R\cap Q = \pi^{-1}(Q)$
Thus $\frac{ab}{1} \in Q$ so $\frac{a}{1}\cdot\frac{b}{1} \in Q$ wlog that $\frac{a}{1} \in Q$ since Q is prime hence $a \in R\cap Q$ $\lightning$

. If $Q \in \mathrm{Spec}(U^{-1}R)$ then $(R\cap Q)\cap U = \emptyset$
Suppose $(R\cap Q)\cap U \neq \emptyset$. Take $u \in U$; $u \in R\cap Q$ then $\frac{u}{1} \in Q$ ideal in $U^{-1}R$
hence $1_{U^{-1}R} = \frac{1}{u}\,\frac{u}{1} \in Q$ so $Q = U^{-1}R$ $\lightning$ since it is prime

. 1-1 easily follows from i.

So far the map is well defined and 1-1. We have to check surjectivity. Let $P \in \mathrm{Spec}(R)$ $P\cap U = \emptyset$. Consider $P(U^{-1}R) :=$ the ideal generated by $\pi(P)$ in $U^{-1}R$

* $P(U^{-1}R)$ is prime.
Suppose that $\frac{r}{u}\,\frac{r'}{u'} \in P(U^{-1}R)$ but $\frac{r}{u}, \frac{r'}{u'} \notin P(U^{-1}R)$
Note $\frac{r}{1} \notin P(U^{-1}R)$ (if so, $\frac{1}{u}\cdot\frac{r}{1} \in P(U^{-1}R)$ which is a contradiction)
Similarly $\frac{r'}{1} \notin P(U^{-1}R)$. Since $\frac{rr'}{uu'} \in P(U^{-1}R)$ then $\frac{uu'}{1}\,\frac{rr'}{uu'} = \frac{rr'}{1} \in P(U^{-1}R) = \langle \pi(P)\rangle$

Then $\frac{rr'}{1} = \frac{r_1}{u_1}\frac{p_1}{1} + \cdots + \frac{r_n}{u_n}\frac{p_n}{1}$ with $u_i \in U, r_i \in R, p_i \in P$

Hence $\frac{rr'\cdot u_1 \cdots u_n}{1} = \frac{s}{1}$ with $s \in P$ so $\exists u \in U : rr'u_1\cdots u_n u = su \in P$
but non of the u_i nor $u \in P$ since $P\cap U = \emptyset$ and also $r, r' \notin P$ (otherwise $\frac{r}{1}$ or $\frac{r'}{1} \in \pi(P)$)
this contradicts the fact that P is prime.

$P \subseteq R\cap(P(U^{-1}R))$. If the inclusion is proper then $\exists\, t \in \pi^{-1}(\langle\pi(P)\rangle) \setminus P$.
and we can see this is impossible with a similar argument to the one above ($\frac{rr'}{1}$ changes to $\frac{t}{1}$).
So $P = R\cap(P(U^{-1}R))$ giving surjectivity. □

Corollary 9 Let R be a noetherian ring, $U \subseteq R$ multiplicatively closed subset. Then $U^{-1}R$ is noetherian.

Proof/ let $J \subseteq U^{-1}R$ be an ideal $R \cap J$ is fg since R noetherian
$J = (R \cap J)U^{-1}R$ which is finitely generated (the image of the generators generates) $\square$

· Observe that if $P \subseteq R$ is a prime ideal then $R \setminus P$ is mult closed. We define $R_P := (R\setminus P)^{-1}R$. Similarly if $M_P := (R \setminus P)^{-1}M$

DEF A local ring is a ring with exactly one maximal ideal. If R is a local ring we denote by m_R its maximal ideal

Observe: R_P is local with $m_{R_P} = P \cdot R_P$ $\left(\pi : R \longrightarrow R_P \quad r \longmapsto \frac{r}{1} \right)$

Let $I \subseteq R_P$ an ideal $I \nsubseteq P \cdot R_P$
$\exists\ \frac{a}{b} \in I \setminus PR_P$ so $b \in R\setminus P$ and $\frac{a}{1} \notin PR_P$ so $a \notin P$. Thus $a, b \in R\setminus P$
thus $\frac{b}{a} \in R_P$ hence $\frac{b}{a}\frac{a}{b} \in I$ so $I = R_P$ this proves PR_P is the unique maximal ideal.

Example Let $X \subseteq \mathbb{A}^n$ be an algebraic subset. Let $a = (a_1, \ldots, a_n) \in X$

$I(\{a\}) = \langle x_1 - a_1, \ldots, x_n - a_n \rangle \subseteq k[x_1, \ldots, x_n]$ maximal ideal

Let $m = I(\{a\}) / I(X) \subseteq A(X)$ of course m maximal ideal in $A(X)$ by corresp.
(polynomial functions in X vanishing at a)

Note $A(X) \setminus m = \{ f \in A(X) : f(a) \neq 0 \}$ a bit of abusing notation. [Note we are identifying pol funct on $X = A(X)$ with $k[x_1, \ldots, x_n] / I(X)$ so it makes sense]
(working with identification after defn.

Here $A(X)_m \ (= (A(X) \setminus m)^{-1} A(X)) = \{ f/g : f, g \in A(X)\ g$ not vanishing at $a \}$
$\downarrow$
"local ring of X at a"
It is local by the preceding obs

this is vain to or even equal if we see $A(X)$ as poly functions on X (which is vain to our construction of $A(X)$). → "rational functions which may not be defined everywhere but at least they are on a"

· See WARNING II in "Topology of Spec(R)", What does it mean for $N \subseteq M$, to have $U^{-1}N \subseteq U^{-1}M$??
· See Remark before C.24; $U^{-1}I = I(U^{-1}R)$
· might need the full exercise in the next section to fully understand.

There can be seen a remarks about Localisation that could have been said here and should be read NOW to keep going safely, and with the whole picture in mind.

4. TENSOR PRODUCTS & CONSTRUCTION OF PRIMES

(~ 2.2, 2.3 Eisenbud ; although 2.2 says much more ; talks about Hom)

Much of this is in my alg. qual notes ; I will repeat things as Buch did it.
useful to read it first, while, or after this.

Let R be a ring, M, N, P R-modules. We recall that

$\varphi : M \times N \longrightarrow P$ is **R-bilinear** (or just bilinear) if

$$\left| \begin{array}{l} \varphi(am_1+m_2, n) = a\varphi(m_1,n)+\varphi(m_2,n) \\ \varphi(m, bn_1+n_2) = b\varphi(m,n_1)+\varphi(m,n_2) \end{array} \right.$$

In other words, fix coor - , get R-module hom

alt way to do things. Same as "group is a set considered with.. or a pair (G, +).. "

DEF A **tensor product of M and N over R** is an R-module T together with a universal bilinear map $\alpha : M\times N \longrightarrow T$ st given any φ bilinear $M\times N \xrightarrow{\varphi} P$ with P an R-module $\exists!\ \tilde{\varphi}$ R-module hom st the following diagram commutes ($\tilde{\varphi}\circ\alpha = \varphi$)

$$\begin{tikzcd}
M\times N \arrow[r, "\varphi"] \arrow[dr, "\alpha"'] & P \\
& T \arrow[u, dashed, "\tilde{\varphi}"']
\end{tikzcd}$$

- Uniqueness up to isomorphism : Suppose $\exists\ T'$ another tensor product of N, M over R. Let α' be the universal bilinear map ;

$$\begin{tikzcd}
M\times N \arrow[r, "\alpha"] \arrow[dr, "\alpha'"'] & T \arrow[d, dashed, shift left, "\tilde{\tilde{\varphi}}"] \\
& T' \arrow[u, dashed, shift left, "\tilde{\varphi}"]
\end{tikzcd}$$

On one hand $\exists!\ \tilde{\varphi} : T \longrightarrow T'$ st $\tilde{\varphi}\circ\alpha' = \alpha$ (*)

$\exists!\ \tilde{\tilde{\varphi}} : T' \longrightarrow T$ st $\tilde{\tilde{\varphi}}\circ\alpha = \alpha'$

Now take P = T in the def, $\alpha = \varphi$.

$$\begin{tikzcd}
M\times N \arrow[r, "\alpha"] \arrow[dr, "\alpha"'] & T \\
& T \arrow[u, "Id_T"']
\end{tikzcd}$$

. Note that $Id_T : T \longrightarrow T$ is an R-module hom satisfying that the diagram commutes, therefore it is the only one

But from (*) $\tilde{\varphi}\circ\tilde{\tilde{\varphi}}\circ\alpha = \alpha$, by uniqueness $\tilde{\varphi}\circ\tilde{\tilde{\varphi}} = Id_T$. Similarly $\tilde{\tilde{\varphi}}\circ\tilde{\varphi} = Id_{T'}$

Therefore $\tilde{\varphi} : T' \longrightarrow T$ iso ($\tilde{\varphi}$ is the unique R-module hom satisfying $\underset{\downarrow}{\varphi}\circ\alpha' = \underset{\downarrow}{\alpha}$)
universal maps.

(elementary tensors)

We denote T by $M\otimes_R N$ or $M\otimes N$ if R is clear; also $\alpha((m,n)) := m\otimes_R n \equiv m\otimes n$

Does this exist? Yes ; proceed as in the proof of algebra qual (so I do not complete details) but the idea Buch gives (which is the meat of the construction) is the following

- Take F free R-module with basis $M \times N$. There is a natural inclusion map

$$M \times N \longrightarrow F$$

This map is not nec. R-bilinear; define a quotient in F so that this natural map is bilinear but do it using minimal relations.

$$\begin{tikzcd} M \times N \arrow[r, "i"'] \arrow[rr, bend right, "\alpha"'] & F \arrow[r, "\pi"'] & F/\text{min rel} \end{tikzcd}$$

So as a set this $M \otimes_R N$ comes from here but there is this philosophy of "forgetting how is built and only care about the universal property". For me that is maybe too much, I prefer to keep in mind the construction. Also my background makes me think more naturally as

"let $M \otimes_R N$ be as constructed (with α), then it satisfies the univ prop and is unique up to... "

So when I write $M \otimes_R N$ I know at least where it comes from (not needed; but more natural to me).

Prop 10 (Properties of tensor product) Let $M, N \overset{Q}{,} P$ be R-modules then

i) $M \otimes_R N$ is generated by $\{m \otimes n : m \in M, n \in N\}$ as an R-module. (Although not every, in general element is of this form)

ii) $M \otimes_R R \cong M$ canonically isomorphic

iii) $M \otimes_R N \cong N \otimes_R M$ canonically isomorphic. (Buch writes $=$)

iv) $(M \otimes_R N) \otimes_R P \cong M \otimes_R (N \otimes_R P)$ canonically isomorphic.

v) $\underbrace{(M \oplus N)}_{\text{Cart product} \dots} \otimes_R P \cong (M \otimes_R P) \oplus (N \otimes_R P)$ canonically isomorphic.

vi) $M \xrightarrow{\alpha} N \xrightarrow{\beta} P \longrightarrow 0$ exact implies $M \otimes_R Q \longrightarrow N \otimes_R Q \longrightarrow P \otimes_R Q \longrightarrow 0$ exact

$$m \otimes q \longmapsto \alpha(m) \otimes q$$
$$n \otimes q \longmapsto \beta(n) \otimes q$$

this is $\alpha \otimes \mathrm{Id}_Q$ in the language of vii).

"Tensor product is right exact functor"

vii) If $\varphi : M \longrightarrow N$, $\varphi' : P \longrightarrow Q$ R-homs

$\exists!$ $\varphi \otimes_R \varphi' : M \otimes_R P \longrightarrow N \otimes_R Q$, the tensor product of two homs.

$$m \otimes p \longmapsto \varphi(m) \otimes \varphi'(p)$$

Rmk: i) Everytime I write $\otimes_R$ I could write $\otimes$

ii) Two concepts that Buch uses and I was not so familiar with

- $M \xrightarrow{\alpha} N$, then $\operatorname{Coker} \alpha := N/\alpha(M)$ (M, N could be rings groups, R-modules..)
- A short exact sequence $0 \longrightarrow A \xrightarrow{a} B \xrightarrow{b} C \longrightarrow 0$ is split if it is isomorphic (alg qual notes) to $0 \longrightarrow A \xrightarrow{i} A \oplus C \xrightarrow{\pi} C \longrightarrow 0$

· Of course $A \oplus C$ is internal or external direct sum (they are isomorphic since we have finitely many summands)

If considered as external $i(a) = (a, 0)$

. This concept came to me "naturally" in the alg ch3 section 12 . (see notes) .

- An exact sequence $A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ is called right exact
  $0 \to A \xrightarrow{\alpha} B \to C$ is called left exact .

It is not true that $M \xrightarrow{\alpha} N \xrightarrow{\beta} P$ exact seq of R-modules then

$M \otimes Q \xrightarrow{\alpha \otimes 1} N \otimes Q \xrightarrow{\beta \otimes 1} P \otimes Q$ is exact (see Atiyah-Macdonald p.29)

iii) In my alg qual notes I also discuss $M \otimes N \otimes P$ (see) ;

iv) Eisenbud along with this , discuss left exactness of Hom . (and flatness). Buch has not said anything so far so I stick to him .
In fact Atiyah proves vi) with Hom .

Proof / Buch said "prove it just using universal property" . Well i) is direct by the construction so I do not see why not use it . (that is why I think is better to think in both terms at the same time)
So i) and the note after it are on my alg qual notes .

ii) We want to prove $M \otimes R \to M$, $m \otimes r \mapsto mr$ is an R-module iso ; let us use the univ prop

since $B : M \times R \to M$ defined by $B((m,r)) = mr$ R-bilinear we have that :

$$\begin{tikzcd} M \times R \arrow[r, "B"] \arrow[dr, "\alpha"'] & M \\ & M \otimes_R R \arrow[u, "\varphi"'] \end{tikzcd}$$

$\exists !\ \varphi : M \otimes_R R \to M$ R-module st $\varphi(m \otimes r) = mr$

Of course it is surjective (let $m \in M$, $\varphi(m \otimes 1) = m$)

Now let $M \xrightarrow{\tilde{\varphi}} M \otimes_R R$, $m \mapsto m \otimes_R 1$ and note it is an R-module hom $\tilde{\varphi}(rm) = rm \otimes_R 1 \underset{\substack{\downarrow \\ \text{Bilinearity} \\ \text{of } \alpha}}{=} r(m \otimes_R 1) = r\tilde{\varphi}(m)$

$\varphi \circ \tilde{\varphi}(m) = m$, $\tilde{\varphi} \circ \varphi(m \otimes r) = \tilde{\varphi}(mr) = r\tilde{\varphi}(m) = r(m \otimes 1) = m \otimes r$.

v) (iii, iv are easier versions of this ; in fact iv is proved in alg qual notes)
(in iii, iv we have to use universal prop to give the inverse too !)

Let $B : M \oplus N \times P \longrightarrow (M \otimes P) \oplus (N \otimes P)$ R-bilinear , then by universal prop $\exists !$
$((m,n),p) \longmapsto (m \otimes p , n \otimes p)$

$\varphi : (M \oplus N) \otimes P \longrightarrow (M \otimes P) \oplus (N \otimes P)$ R-hom such that $\varphi((m,n) \otimes p)) = (m \otimes p, n \otimes p)$.

It is surjective since it covers all the generators . Now define $\tilde{\varphi} : (M \otimes P) \oplus (N \otimes P) \longrightarrow (M \oplus N) \otimes P$
$(m \otimes p , n \otimes p) \longmapsto (m,n) \otimes p$

and exten by R-linearity this is an R-hom and easily check that inverts φ .

vii) Was discussed in alg qual notes and it is easy .

For vi) we know all the maps are R-module homs by vii) and the fact that is right-exact needs a bit of detail that I'll omit for now .

$\square$

Example Let $N = R^n = R\oplus\cdots\oplus R$; $M\otimes_R N = M\otimes_R(R\oplus\cdots\oplus R) = (M\otimes_R R)\oplus\cdots\oplus(M\otimes_R R) =$

$= M\oplus\cdots\oplus M = M^n$ (meaning iso; canonically)

- Tensor products allow us to do base change (extension/restriction of scalars) (We applied this in Lie algebras)

  - Let $\pi : R \longrightarrow S$ be a ring hom. N an S-module,

    Then N is also an R-module $r.n = \pi(r)\cdot n$ $(\pi : Q - R)$

    Also if M is an R module we can take $M\otimes_R S$ (S is an R-module $rs = \pi(r)s$)

    and this has a natural S-module structure $s(m\otimes s') = m\otimes ss'$.

    This S-module is said to be obtained by extension of scalars. (note $M\otimes_R S$ depends on π)

Exercise: Let R be a ring $U\subseteq R$ mult closed, M, M', M'' R-modules. Then

i) $M\otimes_R U^{-1}R \cong U^{-1}M$ canonically iso $\left(m\otimes_R \frac{r}{u} \longmapsto \frac{rm}{u}\right)$

ii) If $\varphi : M \longrightarrow N$ is 1-1 then $\varphi_U : U^{-1}M \longrightarrow U^{-1}N$ is 1-1

$$\frac{m}{u} \longmapsto \frac{\varphi(m)}{u}$$

iii) Suppose $0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0$ is exact, then

$0 \longrightarrow U^{-1}M' \xrightarrow{\alpha_U} U^{-1}M \xrightarrow{\beta_U} U^{-1}M'' \longrightarrow 0$ is also exact

(in the proof I see them as R-homs but the exactness is just injectivity so I can see them as $U^{-1}R$-homs)

__Proof__: Short version: i) Universal prop. ii) Easy. iii) Use ii) for the first, for the rest combine i) and right exactness of tensor. Now we proceed

i) Consider $B : M\times U^{-1}R \longrightarrow U^{-1}M$ R-bilinear then $\exists!\ \varphi : M\otimes_R U^{-1}R \longrightarrow U^{-1}R$

$\qquad (m, r/u) \longmapsto mr/u$

st $\varphi(m\otimes r/u) = \frac{rm}{u}$. Take $U^{-1}M \xrightarrow{\tilde{\varphi}} M\otimes U^{-1}R$ if we check that it is well

$$\frac{m}{u} \longmapsto m\otimes\frac{1}{u}$$

defined then it is clear that it will be an R-hom (by bilinearity of universal α) and invert

φ. Suppose $\frac{m}{u} = \frac{m'}{u'}$. $\exists v\in U$: $vu'm = vum'$. Therefore $vu'm\otimes\frac{1}{vu'u} = vum'\otimes\frac{1}{vu'u}$

But LHS by def of the tensor product (bilinearity of α) $m\otimes\frac{1}{u}$

Similarly the RHS is $m'\otimes\frac{1}{u'}$. Now it is clear that it is well defined.

ii) Suppose $\tilde{\varphi}(m/u) = \tilde{\varphi}(m'/u')$ then $\frac{\varphi(m)}{u} = \frac{\varphi(m')}{u'}$ So $\exists v\in U$ st

$vu'\varphi(m) = vu\varphi(m')$. But φ R-module hom so $\varphi(vu'm) = \varphi(vum')$ and 1-1 so

$vu'm = vum'$ which is $^u/_m = ^u/_{m'}$

iii) $\tilde{\alpha}$ is 1-1 by ii). We have to check that if

$$M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0 \quad \text{is exact then so it is} \quad U^{-1}M' \xrightarrow{\alpha_U} U^{-1}M \xrightarrow{\beta_U} U^{-1}M'' \longrightarrow 0$$

By the last proposition we have that

Consider the isos from i)

$$\begin{tikzcd}
M' \otimes_R U^{-1}R \arrow[r, "\alpha\otimes 1"] \arrow[d, shift left, "a"] & M \otimes U^{-1}R \arrow[r, "\beta\otimes 1"] \arrow[d, shift left, "b"] & M'' \otimes U^{-1}R \arrow[r] \arrow[d, shift left, "c"] & 0 & \Big\} \text{ is exact} \\
U^{-1}M' \arrow[r, "\alpha_U"] \arrow[u, shift left, "a^{-1}"] & U^{-1}M \arrow[r, "\beta_U"] \arrow[u, shift left, "b^{-1}"] & U^{-1}M'' \arrow[r] \arrow[u, shift left, "c^{-1}"] & 0
\end{tikzcd}$$

(R-modules)

It is trivial to check that this diagram commutes (everything is canonic).

For example:

$$\begin{tikzcd}
m' \otimes \frac{r}{u} \arrow[r, "a"] \arrow[rr, bend right, "\tilde{\alpha}\circ a"'] & \frac{rm'}{u} \arrow[r, "\alpha_U"] & \frac{r\alpha(m')}{u}
\end{tikzcd} = \begin{tikzcd}
m' \otimes \frac{r}{u} \arrow[r, "\alpha\otimes 1"] \arrow[rr, bend right] & \alpha(m') \otimes \frac{r}{u} \arrow[r, "b"] & \frac{r\alpha(m')}{u}
\end{tikzcd}$$

It is easy that to see now that the later is exact. (easy checks; video) □

People will just say tensor is exact and then use ii since everything is canonic.

DEF Let M be an R-module then $\mathrm{Ann}(M) = \{r \in R \mid rm = 0 \ \forall m \in M\}$. (the annihilator of M in R)

Note it is an ideal in R. Obviously it is clear what $\mathrm{Ann}(B)$ means for $B \subseteq M$.

Prop 11 Let $U \subseteq R$ be a mult closed set. M-Rmodule and $m \in M$

i) $\frac{m}{1} = 0 \in U^{-1}M$ iff $\exists u \in U : um = 0$

ii) If M is fg then $U^{-1}M = 0$ iff $\mathrm{Ann}(M) \cap U \neq \emptyset$

iii) If M is fg, $P \subseteq R$ prime ideal then $M_P \neq 0 \longleftrightarrow \mathrm{Ann}(M) \subseteq P$.

Related to Tor, alg qual → $\mathrm{Tor}(M) \subseteq M$.

Proof/ i) Trivial

ii) $\longleftarrow$) Needs no fg. If $u \in U \cap \mathrm{Ann}(M)$ by i) $\frac{m}{1} = 0 \in U^{-1}M \ \forall m \in M$

so $\frac{m}{u} = \frac{1}{u}\frac{m}{1} = 0$.

$\longrightarrow$) Let M be generated by $m_1, \dots, m_n$ then $\frac{m_i}{1} = 0 \in U^{-1}M \ \forall i = 1, \dots, n$

So by i) $\exists u_i \in U : u_i m_i = 0$. Let $u := u_1 \cdots u_n \in U$ (mult closed)

Then it is clear that $u \in \mathrm{Ann}(M)$.

iii) Let $U = R \setminus P$. $M_P = U^{-1}R$, then $M_P \neq 0$ iff $\mathrm{Ann}(M) \cap U = \emptyset$

by ii) but $U = R \setminus P$ so this is $\mathrm{Ann}(M) \subseteq P$.

□

DEF Let M be an R-module ; $\mathrm{Supp}(M) = \{ p \in \mathrm{Spec}(R) : M_p \neq 0 \}$

If $I \subseteq R$ ideal $Z(I) = \{ P \in \mathrm{Spec}(R) : I \subseteq P \}$

Remark

When Buch gave this def he kept calling this the vanishing set of I". Why?

- For $J \subseteq k[x_1, \dots, x_n]$, ideal, $k = \bar{k}$ $\mathcal{Z}(J) = \{ \alpha \in \mathbb{A}^n : f(\alpha) = 0 \ \forall f \in J \}$.

  For $\alpha \in \mathcal{Z}(J)$, $I(\{\alpha\}) = \langle x_1 - \alpha_1, \dots, x_n - \alpha_n \rangle = \{ f \in k[x_1, \dots, x_n] : f(\alpha) = 0 \}$.
  (obs from C.6)

Claim $\mathcal{Z}(J) \longrightarrow \{ P \subseteq R \text{ maximal} : J \subseteq P \}$ is a bijection
$\alpha \longmapsto I(\{\alpha\})$

Proof/ $I(\{\alpha\})$ maximal and every pol in J vanishes at α so indeed $I(\{\alpha\}) \in \{ P \subseteq R \text{ max st } J \subseteq P \}$. 1-1 obvious. Now let $P \in \{ P \subseteq R \text{ max} : J \subseteq P \}$ By weak nullstellensatz + obs in proof of cor 6, $P = I(\{\alpha\})$ for some $\alpha \in \mathbb{A}^n$.
Now if $f \in J$, $f \in P$ so $f(\alpha) = 0$ so $\alpha \in \mathcal{Z}(J)$ □

This justifies the language in the sense that : if we take the corresponding ideal of each point in $\mathcal{Z}(J)$ and form the set we get $\{ P \subseteq R \text{ max} : J \subseteq P \}$.

Now I asked Buch; Wouldn't it be more natural to call $Z(I) = \{ P \subseteq R \text{ max} : I \subseteq P \}$
He said that in Scheme world we want this. This gives good picture. I will try to stick to $\mathcal{Z}(I)$ to mean points in $\mathbb{A}$, $Z(I)$ to mean prime ideals...
(this would avoid any confussion but if R arbitrary ring there was no confusion)

Note If M is a fg R-module then $\mathrm{supp}(M) = \mathcal{Z}(\mathrm{Ann}(M))$ (this is not true if not fg think counter example)
Direct by previous prop.

Lemma 12 Let R be a ring, M an R-module, $m \in M$

i) $m = 0 \leftrightarrow \frac{m}{1} = 0 \in M_P \ \ \forall P \subseteq R$ max ideal

ii) $M = 0 \leftrightarrow M_P = 0 \ \ \forall P \subseteq R$ max ideal . So $M = 0$ iff $\mathrm{supp}(M) = \emptyset$.

Proof $\rightarrow$) Clear in both cases

i) $\leftarrow$) $\frac{m}{1} = 0 \in M_P \ \forall P \subseteq R$ maximal then $\mathrm{Ann}(m) \nsubseteq P \ \forall P$ maximal.

If $\mathrm{Ann}(m) \subseteq P$ and $\frac{m}{1} = 0 \in M_P$ $\exists\, u \in R \setminus P$ st $um = 0$ So...

So $\mathrm{Ann}(m)$ is an ideal not contained in any maximal. Therefore (by the fact at the end of sec 2) $\mathrm{Ann}(m) = R$ so $m \cdot 1 = 0$.

ii) $\leftarrow$) $M_P = 0 \ \forall P \subseteq R$ max ideal. So $m = 0 \ \forall m \in M$ by i) □

Corollary 12* Let $\varphi : M \longrightarrow N$ be an R module hom then φ is 1-1 (surj) iff $\varphi_P : M_P \longrightarrow N_P$ is 1-1 (surj) $\forall P \subseteq R$ max ideal.

$$m/u \longmapsto \varphi(m)/u$$

Proof/ We prove it for 1-1 (analogous for surj)

Let $K = \ker \varphi$, now, $0 \longrightarrow K \xrightarrow{i} M \xrightarrow{\varphi} N$ is exact (left exact)

By iii) of last exercise (if we cut the seq of course holds)

$0 \longrightarrow K_P \xrightarrow{i} M_P \xrightarrow{\varphi_P} N_P$ is exact ; φ 1-1 iff $K = 0$ iff $K_P = 0$ $\forall P \subseteq R$ max ideal

by the last prop because K is an R-module. Now $K_P = 0$ $\forall P \subseteq R$ max ideal iff φ_P 1-1 $\forall$ $P \subseteq R$ max ideal is clear by the exactness □

Lemma 14 Let $U \subseteq R$ be a multiplicatively closed subset. Assume $I \subseteq R$ ideal maximal among the ideals disjoint from U. Then I is a prime ideal in R.

(If $0 \notin U$ there is one such for example. But for arbitrary U there might not be; we are assuming $\exists$ one.)

Proof/ Let $r, s \in R \setminus I$.

Then $\langle r, I \rangle \cap U \neq \emptyset$ $\exists a \in R, a' \in I$: $ra + a' \in U$.

$\langle s, I \rangle \cap U \neq \emptyset$ $\exists b \in R, b' \in I$: $sb + b' \in U$

Since U mult closed $(ar + a')(bs + b') \in U$; $abrs + \underbrace{ab'r + a'bs + a'b'}_{\in I} \notin I$ so $abrs \notin I$ so $rs \notin I$. This shows I prime □

Corollary 15 Let $I \subseteq R$ be an ideal then $\sqrt{I} = \bigcap_{P \in Z(I)} P$

Proof/ $\subseteq$) Let $P \in Z(I)$ then $I \subseteq P$ so $\sqrt{I} \subseteq \sqrt{P} = P$ since P prime so $\sqrt{I} \subseteq \bigcap_{P \in Z(I)} P$

$\supseteq$) Let $f \in R \setminus \sqrt{I}$, then $\{f^n : n \geq 0\}$ is a mult closed subset and $\{f^n : n \geq 0\} \cap I = \emptyset$, choose $P \supseteq I$ maximal among the ideals disjoint from $\{f^n : n \geq 0\}$ (we are using that every ideal is contained in a maximal as justified at the end of sec 2 ; also I is an ideal disjoint from that set so we can do it).

Then by the last lemma $P \in Z(I)$ and $f \notin P$, so $f \notin \bigcap_{P \in Z(I)} P$ □

5. LENGTH

($\simeq$ 2.4 Eisenbud)

DEF A nonzero R-module M is **simple** if M has no nonzero proper submodules

Lemma 16 M simple R-module $\longleftrightarrow$ $M \cong R/p$ with $P \subsetneq R$ maximal ideal.

Proof/ $\longrightarrow$) If M simple, let $m \in M \setminus \{0\}$, then $R \longrightarrow M$, $r \longmapsto rm$ R-module hom

By simplicity it has to be surjective so $M \cong R/I$

R/I simple then of course I has to be a maximal ideal (R-submodules of R = Ideals)

$\longleftarrow$) Clear with the caveat above (In both we're using corresp thm). ☐

DEF Let M be an R-module, a **decomposition series of M** is a **chain** (sequence of submodules with strict inclusions) $M = M_r \supsetneq M_{r-1} \supsetneq \cdots \supsetneq M_0 = 0$ such that M_i/M_{i-1} is simple (R-module)

r is called the **length of the dec.**

Prop 17 Let M be an R-module. Any two decomposition series for M have the same length.

Proof/ Suppose we have $M = M_r \supsetneq \cdots \supsetneq M_0 = 0$ two dec series. We form the following diagram
$M = N_s \supsetneq \cdots \supsetneq N_0 = 0$

$$\begin{tikzcd}
M = M_r \cap N_s \arrow[r, phantom, "\supseteq"] \arrow[d, phantom, sloped, "\supseteq"] & M_r \cap N_{s-1} \arrow[r, phantom, "\supseteq"] \arrow[d, phantom, sloped, "\supseteq"] & \cdots \arrow[r, phantom, "\supseteq"] & M_r \cap N_0 \arrow[d, phantom, sloped, "\supseteq"] \\
M_{r-1} \cap N_s \arrow[r, phantom, "\supseteq"] \arrow[d, phantom, sloped, "\supseteq"] & M_{r-1} \cap N_{s-1} \arrow[r, phantom, "\supseteq"] & \cdots \arrow[r, phantom, "\supseteq"] & M_{r-1} \cap N_0 \arrow[d, phantom, "\vdots"] \\
\vdots \arrow[d, phantom, sloped, "\supseteq"] & & & \vdots \arrow[d, phantom, sloped, "\supseteq"] \\
M_0 \cap N_s \arrow[r, phantom, "\supseteq"] & M_0 \cap N_{s-1} \arrow[r, phantom, "\supseteq"] & \cdots & M_0 \cap N_0
\end{tikzcd}$$

This is just the series for N so after elimination length s

This is just the M_i series; after elimination length r

- Note $M_i \cap N_j / M_i \cap N_{j-1} \cong \dfrac{(M_i \cap N_j) + N_{j-1}}{N_{j-1}} \leq N_j/N_{j-1}$. Thus $M_i \cap N_j / M_i \cap N_{j-1}$ is 0 or simple

$\downarrow$ submodule

2nd iso for modules

$$\begin{tikzcd}
& (M_i \cap N_j) + N_{j-1} \arrow[dl, dash] \arrow[dr, dash] & \\
M_i \cap N_j \arrow[dr, dash] & & N_{j-1} \arrow[dl, dash] \\
& M_i \cap N_{j-1} &
\end{tikzcd}$$

If 0 thinking as groups we have $M_i \cap N_j = M_i \cap N_{j-1}$ (just one coset)

Similarly $M_i \cap N_j / M_{i-1} \cap N_j$ 0 or simple

We look at a square

$$\begin{tikzcd}
M_i \cap N_j \arrow[r, phantom, "\supseteq"] \arrow[d, phantom, sloped, "\supseteq"] & M_i \cap N_{j-1} \arrow[d, phantom, sloped, "\supseteq"] \\
M_{i-1} \cap N_j \arrow[r, phantom, "\supseteq"] & M_{i-1} \cap N_{j-1}
\end{tikzcd}$$

A

B

since
$$\left[\begin{tikzcd}
& M_i \cap N_j \arrow[dl, dash] \arrow[dr, dash] & \\
M_i \cap N_{j-1} \arrow[dr, dash] & & M_{i-1} \cap N_j \arrow[dl, dash] \\
& M_{i-1} \cap N_{j-1} &
\end{tikzcd}\right]$$
it follows that the number of simple quotients ($\in \{0,1,2\}$) in path A, coincides with the n° of simple quotients in path B. Now we are done (watch video "same length" in files) ☐

DEF Let M be an R-module; we define $\text{length}_R(M) := \text{lengt}(M) = \begin{cases} r & \text{if } \exists \text{ dec series of length } r \\ \infty & \text{if } \nexists \end{cases}$

Exercise Let M be an R-module, $N \subseteq M$ a submodule. Then

i) $\text{length}(M) = \text{length}(N) + \text{length}(M/N)$ (even if ∞)

ii) If $\text{length}(M) < \infty$, any chain of submodules $0 = M_0 \subsetneq M_1 \cdots \subsetneq M$ can be refined to a decomposition series. (I put strict inclusion to avoid being boring; if not just eliminate).

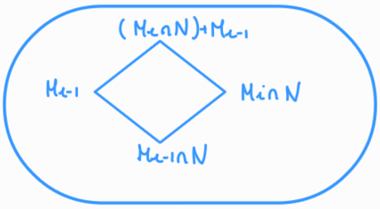
Proof/ • **STEP1**. If $\text{length}(M) < \infty$ then $\text{length}(N) < \infty$. In fact $\exists$ comp series with N as a member and $\text{length}(M) = \text{length}(N) + \text{length}(M/N)$

Proof: Let $r = \text{length}(M)$. Then $\exists$ $0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_r = M$ submodules with M_i/M_{i-1} simple.

Consider $K_i := M_i \cap N$ submodule of N. $0 = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r = N$

$$K_i/K_{i-1} = M_i \cap N / M_{i-1} \cap N \cong \frac{(M_i \cap N) + M_{i-1}}{M_{i-1}}$$ submodule of M_i/M_{i-1} so (by corresp)

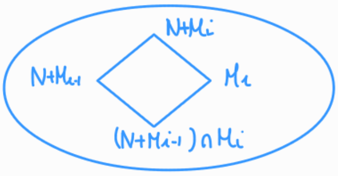
by simplicity of the latter



we get that K_i/K_{i-1} is either 0 or simple. Thus by elimination we are getting a dec series for N so $\text{length}(N) < \infty$.

Now consider $L_i := N + M_i$. So $N = L_0 \subseteq L_1 \cdots \subseteq L_r = M$.

$$L_i/L_{i-1} = \frac{N + M_i}{N + M_{i-1}} \cong M_i/(N + M_{i-1}) \cap M_i$$



but

$$\begin{tikzcd} M_i \arrow[d, dash] \\ (N + M_{i-1}) \cap M_i \arrow[d, dash] \\ M_{i-1} \end{tikzcd}$$

simple so

by third iso thm $M_i/(N + M_{i-1}) \cap M_i$ is simple or zero. After elimination we get $N = L_0 \subsetneq L_1 \cdots \subsetneq L_s = M$ which by corresp yields a dec series for M/N

If we join both we get dec series for M, containing N and $\text{Length}(M) = \text{lengt}(N) + \text{lengt}(M/N)$ (since this things are already well defined and we have constructed a precise dec. series)

If $\text{length}(N) < \infty$, $\text{length}(M/N) < \infty$ we can join both by correspondence and get a (finite) dec series for M. So for i) has been proved (think but it follows directly from what we've shown so far). Also note that ii) is also direct from what we've done

$0=M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_t = M$. Now $\exists$ dec series containg M_{t-1}; we add between M and M_{t-1} all the factors. Same process between M_{t-1} and M_{t-2} ... finite number of times (So step 1 gives us everything). Thus we can add submodules to get dec series containg every element of the original chain.

note $t \leq \text{length}(M)$ (If $t > \text{length}(M)$ the process we describe would lead to a dec series of length $\geq t > \text{length}(M)$ ↯)

□

(This def is in my alg qual notes)

DEF An R-module M is said to be noetherian if every submodule of M is fg

Remark i) TFAE
- ACC on submodules (wrt inclusion)
- Every nonempty set of submodules has a maximal element
- M noetherian

(see alg qual notes)

ii) R is noeth as a ring iff is noeth as an R-module (natural structure)
Ideals = submodules.

iii) WARNING. Submodules of a fg module are not necessarily fg (see alg qual notes for examples)

iv) By def it is obvious that submodule of noeth is noeth module and the same for quotients. It is also not hard to see that if N noeth, M/N noeth → M is noeth.

Exercise (Imp) Let R be a noetherian ring, M a fg R-module. Then M is noetherian.

Proof/ Suppose M is generated by $f_1,\dots,f_t$ (distinct). We show by induction on t that M is noetherian

- $t=1$ Then if N is a submodule; then $N = \{ r f_1$ for some $r \in R \}$

Consider $\{ r \in R \mid r f_1 \in N \}$. It is an ideal in R so it is gener. by $r_1,\dots,r_s$ thus N is generated by $r_1 f_1, \dots, r_s f_1$, so N fg. So M noeth.

$\pi^{-1}(N)$ where $\pi: R \longrightarrow M$, $r \longmapsto r f_1$

- $t>1$ (assume true for modules generated by less than t elements)

Let N be a submodule. $M = Rf_1 + \cdots + Rf_t$; let N be a submodule. Consider

$\bar{M} = M/Rf_1$; $\pi : M \longrightarrow \bar{M}$, $m \longmapsto \bar{m} = m + Rf_1$ this is surjective and $\bar{f}_2,\dots,\bar{f}_t$ generate $\bar{M}$ as an R-module. So by induction $\bar{M}$ is noetherian. Let $\bar{N} = \pi(N)$ submodule so fg by $\bar{g}_1, \dots, \bar{g}_s$ ($g_1,\dots,g_s \in N$). Now $N \cap Rf_1$ is a submodule of Rf_1 noeth so f.g. by $h_1,\dots,h_u \in N$. We now take $n \in N$ consider $n + Rf_1 = \bar{n} = r_1\bar{g}_1 + \cdots + r_s\bar{g}_s =$

$= r_1 g_1 + \cdots r_s g_s + Rf_1$. Now $n - \underset{\in N}{(r_1 g_1 + \cdots + r_s g_s)} \in N \cap Rf_1$ so it is of the form

$\tilde{r}_1 h_1 + \cdots + \tilde{r}_k h_k$ with $\tilde{r}_i \in R$. Therefore n is an R-linear comb of $g_1, -, g_s, h_1, -, h_k$. So N is fg hence M noeth $\square$

{Note; if you do $N \cap (Rf_1 + - + Rf_{t-1})$ fg and $N \cap Rf_t$ you don't get anything: $n \in N$ $n = r_1 f_1 + \cdots + r_{t-1} f_{t-1} + r_t f_t$ but why $r_t f_t \in N$? you don't know. This way of thinking is valid in vector spaces where you count dimensions; otherwise no!}

DEF An R-module M is Artinian if DCC on submodules hold. (ie $M_1 \supseteq M_2 \cdots$ descending chain of submodules, it stabilizes. $\exists N \in \mathbb{N}: M_N = M_{N+1} = \cdots$)

We say that a ring is Artinian if it is as an R-module (DCC on ideals)

Examples

Artinian	Noeth	Ex
YES	NO	$\mathbb{Z}_p/\mathbb{Z}$ with $\mathbb{Z}_p = \{\frac{k}{p^n} : n \in \mathbb{N}, k \in \mathbb{Z}\}$, $\mathbb{Z}$ module
YES	YES	$\mathbb{Z}/3\mathbb{Z}$ as a $\mathbb{Z}$ module (finite)
NO	YES	$\mathbb{Z}$ as a $\mathbb{Z}$ module
NO	NO	$K[x_1, ---]$ as a module over itself (not noeth ring so not artinian) want

Prop 18 Let M be an R-module. Then length$(M) < \infty \longleftrightarrow$ M is Artinian and Noetherian

Proof/ $\longleftarrow$) If M simple it is obvious. WMA not simple

Claim Since M noetherian $\exists M_1 \subsetneq M$ maximal submodule

Assume by contradiction $\nexists$. Then let $0 \subsetneq N \subsetneq M$ be a submodule, $\exists N \subsetneq N_1 \subsetneq M$ submodule since N not maximal. N_1 not maximal so $\exists N_1 \subsetneq N_2 \subsetneq M$ submodule. By induction we get an increasing chain that does not stop. $\lightning$ Noeth.

Now M_1 is again noetherian so $\exists M_2 \subsetneq M_1$ maximal. By the Artinian property $M_r = 0$ for some r (take the smallest). This of course gives a dec series of length r.

$\longrightarrow$) Assume M has finite length. Let $M_1 \subseteq M_2 \subseteq \cdots$ an ascending chain of submodules Then by the first exercise of the section $\underset{\in\mathbb{Z}}{\text{length}(M_1)} \leq \underset{\in\mathbb{Z}}{\text{length}(M_2)} \cdots < \infty$

so $\exists N \in \mathbb{N}$ such that length$(M_N) =$ length(M_{N+n}) $\forall n \in \mathbb{N}$; and again by the exercise we conclude that it stabilizes. So noetherian.

Similarly if $S_1 \supseteq S_2 \cdots\cdots$ descending chain of submodules $\infty >$ length$(S_1) \geq \cdots \geq 0$ by the exercise so reasoning as above we get that M is Artinian $\square$

The next theorem describes the structure of modules of finite length. It contains Jordan-Hölder for modules and Chinese Remainder theorem (see alg qual notes).

STUPID OBS: Let R be a ring, P, Q prime ideals st $R/P = R/Q \longrightarrow P = Q$

$\pi : R \longrightarrow R/P$, $\ker \pi = P$ but $R/P = R/Q$ so $\ker \pi = Q$ so $P = Q$
$r \longmapsto r + P$

Theorem 19 Assume M is an R-module of finite length. Let $0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M$ be a dec series. Then

i) $M \cong \bigoplus_{\left[\begin{smallmatrix} P \subseteq R \text{ maximal ideal st} \\ R/P \cong M_{i+1}/M_i \text{ for some } i \end{smallmatrix}\right]} M_P$ (localization of M at $R \setminus P$).

$m \longmapsto (m/1, \ldots, m/1)$

ii) $\text{length}_R(M_P) = \# \{ i : M_i/M_{i-1} \cong R/P \}$ ↙ R-modules.

iii) $M = M_P \longleftrightarrow P^s \cdot M = 0$ for some $s \in \mathbb{N}$, P max ideal

↳ sums of products of s elements of P (of course)

Proof: I will treat things in a way that are less to the point but will make me learn more.

Observation 0: Suppose I, J are ideals in R. Consider R/J, R/I which are rings but consider them with the natural R-module structure. If $R/J \cong R/I$ as R-modules then $I = J$

$I = J$. Pf/ let $\tau : R/I \longrightarrow R/J$ R-module hom. Then let $j \in J$, $\tau(j + I) =$

$= \tau(j \cdot 1 + I) = j\,\tau(1 + I) = 0 + J$. So $j + I \in \ker \tau = \{I\}$. So $j + I = I \rightarrow J \subseteq I$

$\downarrow$
$j\,\tau(1+I) = j\,(a+J) = 0+J$

Similarly, working with τ^{-1}, $I \subseteq J$.

Observation 1: $\{ P \subseteq R \text{ max ideal st } \underset{\text{(R-modules)}}{R/P \cong M_i/M_{i-1}} \text{ for some } i \}$ is finite

N is a simple nonzero R-module

Let $n \in N \setminus \{0\}$ $R \xrightarrow{\cdot n} N$, the image is a submodule nonzero so surjective. Let $P = \ker(\cdot n)$
$r \longmapsto rn$

Hence $R/P \cong N$ as R-modules. The simplicity of R/P as an R-module implies P is maximal.

Now for each $i \in \{1, \ldots, n\}$ M_i/M_{i-1} is a simple nonzero R-module so i determines 1 and only 1 (by obs 0) maximal ideal P st $R/P \cong M_i/M_{i-1}$. Thus in our set we have at most n maximal ideals (note that mult by any other elmt will also yield P as kernel so $P \cdot N = 0$)

So indeed we have a direct sum $\equiv$ direct product on the RHS.

Observation 2: Let N be a submodule, $(M/N)_P \cong M_P/N_P$

of course this is valid for U any mult set $U^{-1}(M/N) \cong U^{-1}M/U^{-1}N$

Be aware that here $U^{-1}N \subseteq U^{-1}M$ See warning in "top of spec(R)"

Proof: $0 \longrightarrow N \xrightarrow{i} M \xrightarrow{\pi} M/N \longrightarrow 0$ short exact sequence

Then by sec 3, $0 \longrightarrow N_P \xrightarrow{i} M_P \xrightarrow{\pi_P} (M/N)_P \longrightarrow 0$ is again exact

therefore by 1st iso thm on π_P, $M_P/N_P \cong (M/N)_P$ (as R-modules and as R_P too)
I will see everything as R-modules

Observation 3: Let P max ideal, $N := R/P$ and $Q \subseteq R$ prime then $N_Q \cong \begin{cases} N & \text{if } Q = P \\ 0 & \text{if } Q \neq P \end{cases}$ (as R-modules)

Proof/ • If $Q = P$, R/Q is a field so the elements of outside Q act as units on R/Q

So $(R/Q)_Q \cong R/Q$ (canonic $\frac{r+Q}{s} \longmapsto rs+Q$ ($s \in R\setminus Q$) ; see it as R-modules.)

• If $P \neq Q$ since P max $P \not\subseteq Q$ so $\exists\, f \in P \setminus Q$. Note $f \cdot N = 0$

so $N_Q = 0$ by prop 11, ii).

$\frac{s}{p} = \frac{s'}{p'}$ $\tilde{p} s p' = s' p \tilde{p}$ $sr - s'r$

Observation 4: let N be a (nonzero) simple R-module, then $N \cong R/P$ for some P maximal and $N_Q \cong \begin{cases} N & \text{if } Q = P \\ 0 & \text{otherwise} \end{cases}$

$N \cong R/P$ as R-modules by obs 1 (underlined part)

we get $\underset{\overset{\downarrow}{12^*}}{N_Q \cong} (R/P)_Q \cong \begin{cases} R/P \cong N & \text{if } Q = P \\ 0 & \text{if } Q \neq P \end{cases}$

Therefore if N simple R-module $P \neq Q$ maximal ideals $(N_P)_Q = 0$

• If $N \cong R/P$ then $\underset{(\text{obs } 3)}{N_P \cong N}$ so $N_P \cong R/P$ So $(N_P)_Q = 0$ by obs 4

If $N \cong R/S$ with $S \neq P$ then $(N)_P = 0$, So $(N_P)_Q = 0$.

(From this it also follows that if $R/P \cong R/Q$ then $P = Q$. But only for max)

After this prelim. we can start the proof

ii) $0 = M_0 \subsetneq M_1 \cdots \subsetneq M_n = M$. Now take Q maximal ideal by the comment above

$0 = (M_0)_Q \subseteq (M_1)_Q \subseteq \cdots \subseteq (M_n)_Q$ where $(M_i)_Q/(M_{i-1})_Q \cong (M_i/M_{i-1})_Q$ which

is $\cong M_i/M_{i-1}$ if $M_i/M_{i-1} \cong R/Q$

$\cong 0$ otherwise

So we get the following, if $\exists\, i \in \{1, \dots, n\}$: $M_i/M_{i-1} \cong R/Q$ then M_Q has a decomposition as an R-module of length $\#\{i\in\{1,\dots,n\} : M_i/M_{i-1}\cong R/Q\}$. If not then $M_Q=0$.

We've proved ii).

Note: $\bigoplus_{\substack{P \text{ max ideal} \\ \text{in } R \text{ with} \\ R/P\cong M_i/M_{i-1} \\ i\in\{1,\dots,n\}}} M_P = \bigoplus_{\substack{P \text{ max} \\ \text{ideals}}} M_P$. Why? $M_Q=0$ $\forall$ Q max ideal $R/Q\not\cong M_i/M_{i-1}$ for any $i\in\{1,\dots,n\}$ (recall $R/P\cong R/Q$ as R-modules $\longleftrightarrow$ $P=Q$)

↳ So this is actually a direct sum (we are adding perhaps infinitely many zeros)

↳ This is what Buch wrote.

i) $M \xrightarrow{\varphi} \bigoplus_{\substack{P \max \\ R/P\cong M_i/M_{i-1}}} M_P$

$m \longmapsto (m/1,\dots,m/1)$.

By 12* iff $\forall Q$ max $M_Q \xrightarrow{\varphi_Q} \left(\bigoplus_{\cdots} M_P\right)_Q$ is an isom.

$m/t \longmapsto \dfrac{\varphi(m)}{t}$

Note that if $M_1,\dots,M_n$ are R-modules U mult closed subset of R

$$U^{-1}(M_1\oplus\cdots\oplus M_n)\cong M_1\oplus\cdots\oplus M_n\otimes_R U^{-1}R \cong (M_1\otimes_R U^{-1}R)\oplus\cdots\oplus(M_n\otimes_R U^{-1}R)$$

exercise after prop 10. Canonical

tensor product prop, canonical too

$\cong U^{-1}M_1\oplus\cdots\oplus U^{-1}M_n$ with every step being canonical so $\dfrac{(m_1,\dots,m_n)}{u}\to\left(\dfrac{m_1}{u},\dots,\dfrac{m_n}{u}\right)$

again ex 10

By the note we need to check that $M_Q \longrightarrow \bigoplus_{\cdots}(M_P)_Q$ is an isom.

$m/t \longmapsto \left(\dfrac{m/1}{t},\dots,\dfrac{m/1}{t}\right)$

- If Q is not st $R/Q\cong M_i/M_{i-1}$, $i\in\{1,\dots,n\}$ then $M_Q=0$ and $(M_P)_Q=0$ $\forall P : R/P\cong M_i/M_{i-1}$ for some i

So the map above is just sending $0\to 0$ so isom.

- If Q is st $R/Q\cong M_i/M_{i-1}$, then on the RHS we have $0\oplus\cdots\oplus(M_Q)_Q\oplus\cdots\oplus 0$

But by obs 4, $(M_Q)_Q\cong M_Q$ $\left(\dfrac{m/t_1}{t_2}\mapsto m/t_1t_2\right)$. Now by composing with this iso we get the identity map on M_Q hence our original map is an isomorphism.

↳ I checked this is an isom, easy.

Since this works for every Q, the initial map is an isom.

I did the extra effort of proving that the natural map was the isom. But if I just want them to be isom I safe effort.

What the book, and Buch do is write $=$ and this means canonically iso.

iii) $\longrightarrow$) Then $M_i/M_{i-1} \cong R/p$. Obs 0, Obs 1 yield that $P = \ker \varphi$; $\varphi : R \longrightarrow M_i/M_{i-1}$, $r \longmapsto r m_i + M_{i-1}$, $m_i \in M_i$

so $PM_i \subseteq M_{i-1}$. So $PM \subseteq M_{n-1}$, $P^2 M \subseteq M_{n-2}$, ..., $P^n M = 0$.

$\longleftarrow$) If $P^s M = 0$ for some $s \in \mathbb{N}$. Let Q maximal $P \neq Q$ then $\exists f \in P \setminus Q$ such that $f^s . M = 0$, this easily implies $M_Q = 0$ so $M \cong M_P$ by i). $(M \neq 0)$

$\square$

Note: Not hard to prove directly that if M finite length $\text{length}_R(M_P) = \text{length}_{R_P}(M_P)$

- Take $0 = (M_0)_P \subsetneq \cdots \subseteq (M_i)_P \subsetneq (M_{i+1})_P \subsetneq \cdots \subsetneq (M_t)_P = M_P$

If $(M_{i+1})_P/(M_i)_P$ is simple as an R-module means $\nexists$ R-submodules in between $(M_i)_P$ and $(M_{i+1})_P$

If $\exists$ an R_P-module S in between it would for sure be an R-submodule so the quotient are simple when seen as R_P-modules. So we have that the same dec series works. $\square$

Example Let $R = \mathbb{Z}$, $M = \mathbb{Z}/\langle a \rangle$ with $a = p_1^{r_1} \cdots p_k^{r_k}$ prime fact

Suppose p is a prime st $\gcd(p, a) = 1$, then $M_P = 0$, $P = \langle p \rangle$ prime ideal.

Let $r + \langle a \rangle \in M$, $r \notin \langle a \rangle$. Now take any $\frac{r + \langle a \rangle}{t} \in M_P$, $t \in \mathbb{Z} \setminus P$

$\frac{r + \langle a \rangle}{t} = 0$ in M_P iff $\exists u \in \mathbb{Z} \setminus P$: $u(r + \langle a \rangle) = \langle a \rangle$; take $u = a$, we see $(L12.1)$.

$M_P = 0$

By 1) $\mathbb{Z}/\langle a \rangle \cong M_{\langle p_1 \rangle} \oplus \cdots \oplus M_{\langle p_k \rangle}$ (we can see that $M_{\langle p_i \rangle} \neq 0$ and then apply i)

It is not hard to prove (basically for the same reason $\mathbb{Z}/\langle p_i^{r_i} \rangle = M_{\langle p_i \rangle}$ so this is CRT

$$\mathbb{Z}/\langle p_i^{r_i} \rangle \cong \mathbb{Z}/p_i^{a}\mathbb{Z}$$

Theorem 20 Let R be a ring. TFAE

i) R noeth and all prime ideals are maximal

ii) $\text{length}_R(R) < \infty$ (R as an R-module)

iii) R is artinian

If this situation occurs $\exists$ only finitely many max ideals

Proof/ Assume i) holds but supp. $\text{length}_R(R) = \infty$. Let I be maximal among the ideals such that $\text{length}_R(R/I) = \infty$ (0 is one such and we can take maximal by noeth prop).

$\hookrightarrow$ R-modules.

<u>Claim</u> I is prime.

Let $ab \in I$ with $a \notin I$. Let $\overset{\text{ideal}}{(I :_R a)} = \{r \in R \mid ra \in I\} \supseteq I$.

This notation is a special case of a general not. $(X :_Y Z) = \{y \in Y : yZ \subseteq X\}$ in whatever context it makes sense

Consider
$$\begin{tikzcd} R \arrow[r, "\varphi"] & R/I \\ r \arrow[r, mapsto] & ar + I \end{tikzcd}$$
. $\ker \varphi = (I :_R a)$.

Thus
$$\begin{tikzcd} 0 \arrow[r] & R/(I :_R a) \arrow[r] & R/I \arrow[r] & R/\langle a \rangle + I \arrow[r] & 0 \\ & r + (I :_R a) \arrow[r, mapsto] & ar + I & & \\ & & r + I \arrow[r] & r + (\langle a \rangle + I) & \end{tikzcd}$$

is exact, note $I < \langle a \rangle + I$ so $\text{length}_R(R/\langle a \rangle + I) < \infty$

If $b \notin I$ then $I < (I :_R a)$ so $\text{lenth}_R(R/(I :_R a)) < \infty$ by our choice of I

But then $\text{length}_R(R/I) < \infty$ ↯. Thus shows I prime.

$\downarrow$

$R/(I :_R a)$ embeded as a submodule of R/I with finite length and whose quotient is iso to $R/\langle a \rangle + I$ with finite lenth. We are exactly in the situation of the 1st ex of the section.

Now suppose that every prime is maximal (thus i suppose i) holds but ii) no).

Then $\text{length}_R(R/I) = 1$ ↯

STUPID OBS R ring, $I \trianglelefteq R$. R/I is a ring and it is a module over itself and an R-module. An R-submodule is a subgroup so A/I with A additive subgroup such that $r(a + I) = ra + I \in A/I$ $\forall r \in R$ so $ra \in A$ $\forall r \in R$ so A is an ideal in R. Thus R-submodules of R/I are A/I A ideal in R.

Now R/I submoduls are ideals in R/I which by corresp for rings are just A/I with A ideal in R. Same thing.

ii $\to$ iii) Has already been discussed

iii $\to$ ii) Assume R is artinian;

<u>Claim</u> $0 \trianglelefteq R$ is a product of (finitely many) maximal ideals.

(sums of products of elmts of those ideals; as always)

Since R is artinian we can take $J \trianglelefteq R$ minimal ideal such that J is product of maximal ideals (finitely many)

Let $M \trianglelefteq R$ maximal, $MJ \subseteq J$. By minimality $\overset{M_J}{\supseteq}$ $MJ = J$. Therefore $J^2 \subseteq J$ (J is product of max ideals)

So $J^2 = J$. If $J \neq 0$ then choose I minimal (by art and we have J) such that $IJ \neq 0$

So $\exists f \in I$ such that $fJ \neq \{0\}$ so since I is minimal $I = (f)$

Also $IJ \neq 0$ $\wedge$ $IJ \subseteq I$ so $IJJ = IJ^2 = IJ \neq 0$, by minimality $IJ = I$

So $\langle f \rangle J = \langle f \rangle$ thus $\exists$ $g \in J$: $fg = f$ so $(1 - g)f = 0$. Now since $g \in J \subseteq M$ $\forall M$ max

$1 - g \notin M$ for any max ideal, so $g - 1$ is a unit (the ideal it generates can't be proper) so $f=0$ (by multiplying by inverse) thus $IJ=0 \subsetneq$. So $J=0$ product of finitely many max ideals.

So $0 = M_1 \cdots M_t$ $\quad M_i \subseteq R$ max ideal.

Now note that for each i, $M_1 \cdots M_i / M_1 \cdots M_{i+1}$ is a R/M_{i+1}-vector space.

"local Art ring" not for from field

Here, subspaces correspond to ideals of R containing $M_1 \cdots M_{i+1}$ contained in $M_1 \cdots M_i$

Similarly any descending chain of subspaces corresponds to descending chain of ideals of R and since R art this shows that any descending chain of subspaces is finite. So the vector space is f dim. In particular we find a finitely many ideals ordered by proper inclusion from $M_1 \cdots M_{i+1}$ to $M_1 \cdots M_i$ with no ideals in between. Putting all of this together we get a chain $0 \subsetneq I_1 \subsetneq \cdots \underset{M_1}{\overset{}{I_t}} \subsetneq R$ with no ideals in between on each step, this is a finite dec series for R as an R-module hence R is noetherian.

Let P be prime, $0 = \underbrace{M_1 \cdots M_t}_{\text{max ideals}} \subseteq P \rightarrow \underset{\text{prime}}{M_j} \subseteq P$, so $P = M_j$ by maximality of M_j

In particular P is one of the M_j so every maximal ideal is one of the M_j. (finitely many) $\square$

$A \subseteq M_1 \ldots M_i$, $A/M_1 \ldots M_{i+1}$ is a subspace iff.
$\forall$ A additive subgroup (easy) and
$(r + M_{i+1})(a + M_1 \ldots M_{i+1}) := ra + M_1 \ldots M_{i+1} \in A/M_1 \ldots M_{i+1}$
(easy to check it is well defined.
so this is $ra \in A$ $\forall a \in A$ $r \in R$. Therefore
iff $A \trianglelefteq R$, $M_1 \cdots M_{i+1} \subseteq A \subseteq M_1 \cdots M_i$

We now apply this result in the geometric context to get:

Corollary 21 Let $X \subseteq \mathbb{A}^n$ be an algebraic set, our field is k. TFAE
i) X is finite
ii) $A(X)$ f dim vector space over k and $\dim_k(A(X)) = |X|$
iii) $A(X)$ is an artinian ring

Proof/ i $\longrightarrow$ ii) $A(X)$ is (clearly) always a k-vector space; it is the is the ring of polynomial functions restricted to X (an algebra). Since X is finite it is clear that this is just all functions from $X \longrightarrow k$. This is clearly a vector space of dim $|X|$.

<u>Formal argument</u>: $X = \{v_1, \ldots, v_t\}$, $A(X) = \dfrac{k[x_1, \ldots, x_n]}{I(v_1) \cap \cdots I(v_n)} = I(X)$
$|X| = t$

Take $\varphi : k[x_1, \dots, x_n] \longrightarrow K^t$ linear map , $\ker \varphi = I(X)$

$P(x_1, \dots, x_n) \longmapsto (P(v_1), \dots, P(v_t))$ $\quad v_1 = (v_{11}, \dots, v_{1n}) \dots\dots v_t = (v_{t1}, \dots, \underset{\overset{\Downarrow}{}}{\overset{K}{v_{tn}}})$

We show the map is surjective. Let $P(x_1, \dots, x_n) = \left(\sum_{i=1}^{n} x_i - v_{2i}\right)\left(\sum_{i=1}^{n} x_i - v_{3i}\right) \dots \left(\sum_{i=1}^{n} x_i - v_{ti}\right)$

Note $P(v_1) \neq 0$ (if 0 then one of the terms would vanish $\longrightarrow v_1 = v_i$ for some i)

$P(v_i) = 0 \ \forall i \neq 1$ So by scaling, $e_1 \in \varphi(k[x_1, \dots x_n])$. Similarly $e_i \in \operatorname{Im} \varphi \ \forall i \in \{1, \dots, t\}$

Since φ linear, has a basis of the range φ is surjective. $k[x_1, \dots x_n] / I(X) \cong k^t$.

ii → iii) It's easy to see that ideals in $A(X)$ are vector subspaces of $A(X)$ as a k-vector space therefore any descending chain of ideals gives descending chain of subspaces and by f. dim must terminate.

Note Reason to Eisenbud's proof: D&F for example (once it starts with comm alg) says that a ring is a K-algebra if $K \subseteq R$ field sharing 1. (R has a copy of k inside). In this case if R ring which is a k-algebra I ideal of R is a k-subspace. So if $\dim_k R < \infty$, DCC, ACC hold. This is (more or less) what was happening above. (I think in the case above this happens $r + M_{t+1} \longrightarrow r + M_1 \dots M_{t+1}$ embedding but also subspaces correspond to ideals.

iii → i) $A(X)$ is artinian, by the previous thm $A(X)$ has finitely many max ideals

Now if $\alpha \in X$, $\langle x_1 - \alpha_1, \dots, x_n - \alpha_n \rangle^{= I(\alpha)}$ is a maximal ideal of $k[x_1, \dots, x_n]$ containing $I(X)$. Therefore $\langle x_1 - \alpha_1, \dots, x_n - \alpha_n \rangle / I(X)$ maximal ideal of $A(X)$.

Of course this gives finitely many possibilities of points in X.

□

STUPID OBS Let G be a group $N \trianglelefteq G$, $H/N = K/N \rightarrow K = H$

Let $h \in H$, $h \in kN$ for some $k \in K$

but then is $h \in K$ $(N \subseteq K)$

So $H \subseteq K$. Similarly $K \subseteq H$

Corollary 22 ("Structure thm" of Artinian rings) Any artinian ring is a finite direct product of local Artinian rings.

Proof R artinian. Then R has finite length as an R-module over itself. By thm 19

$R \cong \bigoplus_{\substack{P \triangleleft R \\ \max}} R_P$ R-module hom. Since we know how the map works we also see it's a ring hom

Since we have finitely many it is a direct product. From what we've done is clear R_P artinian and local. □

Corollary 23 (Caracterization of finite length modules over Noeth rings)

Let R be a Noetherian ring, M a fg R-module. TFAE

i) $\text{length}_R(M) < \infty$

ii) $\exists$ Max ideals $P_1, \ldots, P_n \subseteq R$: $P_1 \cdots P_n M = 0$

iii) All prime ideals $P \supseteq \text{Ann}(M)$ are max

iv) $R/\text{Ann}(M)$ Artinian ring (ideals here are just $I/\text{Ann}(M)$ $I \trianglelefteq R$) .

(As a consequence : R artinian local $\to$ maximal ideal is nilpotent)

If Art then noeth . let $M = R$ as an R-module

let P be the max ideal , $P^n \cdot R = 0$ so $P^n = 0$.

(As a consequence : R noeth local with max ideal nilp $\to$ R Artinian ($\text{Ann}(R) = 0$ of course))

Proof/ i $\to$ ii) $0 \subsetneq M_0 \subsetneq M_1 \cdots \subsetneq M_n = M$ dec series

M_i/M_{i-1} simple so $\cong R/P_i$ with P_i max ideal (the unique max ideal satisfying this)

and $P_i M_i \subseteq M_{i-1}$ (it was the kernel of mult map by an elmt of M_i/M_{i-1} ; and by the considerations we made, the kernel of mult by any elmt)

Therefore $P_1 \cdots P_n M = 0$

ii $\to$ iii) Take $P_1, \ldots, P_n$ maximal ideals with $P_1 \cdots P_n M = 0$. Then take P prime $P \supseteq \text{Ann}(M)$

$P \supseteq P_1 \cdots P_n$ so since P prime $P \supseteq P_i$; now by maximality $P_i = P$.

iii $\to$ iv) In the ring $R/\text{Ann}(M)$ all primes are maximal , also since R noeth ring

$R/\text{Ann}(M)$ also so by 20, $R/\text{Ann}(M)$ Artinian

iv $\to$ i) Consider $S = R/\text{Ann}(M)$ Artinian ring , S has finite length as an S-module .

(By one of the stupid observations S has finite length as an R-module)

M is also an S-module , easily seen to be finitely generated . Take $\{m_1, \ldots, m_n\}$ generators ,

$\varphi : S^n \longrightarrow M$ defined by $(1, 0, \ldots, 0) \longmapsto m_1$ extended by S linearly

$(0, 1, 0, \ldots, 0) \longmapsto m_2$

$\vdots$

this is an S-hom but also an R-hom (surjective) so $\text{length}_R(M) < \text{length}_R(S^n) =$

$= n \, \text{length}_R(S) < \infty$. (Nontrivial , but correct) $\square$

$\downarrow$

easy

Remark Let $I \subseteq R$ be an ideal, $U \subseteq R$ mult closed. $I(U^{-1}R)$ ideal in $U^{-1}R$ ($\pi : R \to U^{-1}R$, $\langle \pi(I) \rangle$)

$r \longmapsto r/1$

If we see I as an R-module $0 \to I \xrightarrow{i} R$ exact seq of R-modules ,

Since localization is exact , $0 \to U^{-1}I \xrightarrow{i_U} U^{-1}R$ is also exact and these are $U^{-1}R$ module homs

Now $U^{-1}I$ is a $U^{-1}R$ submodule of $U^{-1}R$, hence an ideal . It contains

$\pi(I)$ so $\langle \pi(I) \rangle \subseteq U^{-1}I$. Now if $i \in I$, $\frac{i}{1} \in \langle \pi(I) \rangle$ and $\frac{1}{u}\frac{i}{1} \in \langle \pi(I) \rangle$

See WARNING II in discussion "topology of spec (R)". Without this we are not done!!

hence $U^{-1}I \subseteq \langle \pi(I) \rangle$. Therefore $I(U^{-1}R) = U^{-1}I$. (If P prime, in R_P, I_P is $(R \setminus P)^{-1}I = I((R \setminus P)^{-1}R)$)

<u>Corollary 24</u> Let $I \subseteq P \subseteq R$ be ideals, R noeth, P prime. TFAE

i) P minimal prime over I (P minimal among the primes of R containing I)

ii) R_P/I_P Artinian (local) ring (${R_P}$ local so R_P/I_P local too)

iii) $P_P^N \subseteq I_P$ (this is inside R_P) for some $N \in \mathbb{N}$

also read warning II.

Proof/ i → ii) R_P noetherian ring so R_P/I_P too.

<u>Claim</u> P_P/I_P is the only prime in R_P/I_P.

$\pi : R \to R_P$
$r \mapsto r/1$

$Q/I_P \subseteq R_P/I_P$ prime then Q is a prime ideal in R_P; by prop 8 ii, $Q \cap R \in \mathrm{Spec}(R)$
$(Q \cap R) \cap (R \setminus P) = \emptyset$

so $I \subseteq I_P \cap R \subseteq Q \cap R \subseteq P$. By minimality of P, $Q \cap R = P$

So $\underset{\overset{\parallel \text{ by } 8.i)}{Q}}{(Q \cap R)U^{-1}R}$ is $PU^{-1}R = P_P$ by the remark.

ii) → iii) $0 \subseteq R_P/I_P$, now $\sqrt{0} = P_P/I_P$ intersection of all prime ideals C.15

So for $f \in P_P$, $\exists\, N_f \in \mathbb{N} : f^N \in I_P$. Now R noetherian so R_P too by corollary 9 hence P_P is noeth so f generated by $f_1, \dots, f_n$, now we take N large enough so that $f_i^N \in I_P \; \forall i \in \{1, \dots, n\}$, now $P_P^M \subseteq I_P$ for M suff large (note we are doing finite sums so $\exists$ such M)

iii → i) Assume $I \subseteq Q \subseteq P$, Q prime then $P_P^N \subseteq I_P \subseteq Q_P$ prime

$P_P = Q_P \longrightarrow Q = P$. (bijection of thm 8 or by obs.)

(Buch didn't say anything about 2.5; quite short)

6. ASSOCIATED PRIMES & PRIMARY DECOMPOSITION.

(Eisenbud 3.1, 3.2, 3.3, 3.4, 3.8 approx)

Motivation

ATIYAH-MAC. The decomposition of an ideal into primary ideals is a pillar of ideal theory. It provides the algebraic foundation for decomposing an algebraic set into its irreducible components (the algebraic picture is more complicated than the naïve geometry would suggest) From another POV, primary decomposition provides a generalization of the factorization of an integer as product of prime powers

EISENBUD, BUCH

Number theory (vd in class): $n = p_1^{d_1} \dots p_n^{d_n}$ prime fact.

In the ring $\mathbb{Z}$, $\langle n \rangle = \langle p_1^{d_1} \rangle \cap \dots \cap \langle p_n^{d_n} \rangle$ (not difficult to prove using things from alg qual.)

In this case · the associated primes will be $\langle p_i \rangle$

· the primary components will be $\langle p_i^{n_i} \rangle$

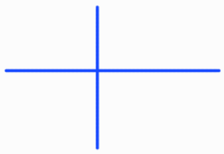
This is the sense in which primary dec generalizes U Fact of integers

Algebraic Geometry (some defs and exercises are also "not motivation")

DEF A topological space X is said to be irreducible if $X = X_1 \cup X_2$ X_i closed then $X = X_i$ for $i \in \{1,2\}$.

Example $\mathbb{A}^2$, with Zariski topology, $Z(\{xy\}) = \{(z_1, z_2) \in \mathbb{C} \times \mathbb{C} \mid z_1 z_2 = 0\}$ $= \{(0,z) : z \in \mathbb{C}\} \cup \{(z,0) : z \in \mathbb{C}\} = Z(\{x\}) \cup Z(\{y\})$ not irreducible

Picture (in alg geo we draw $\mathbb{C}^2$ as $\mathbb{R}^2$; see alg geo notes)



· In the following $\mathbb{A}^n$ affine space over $\mathbb{K} = \overline{\mathbb{K}}$, $\mathbb{A}^n$ considered with Zariski topology

↳ For the next two exercises is not needed

Exercise Consider $X \subseteq \mathbb{A}^n$ algebraic set. X is irreducible iff $I(X)$ is prime ideal in $k[x_1, \dots, x_n]$. ($\longleftrightarrow$ $A(X)$ integral domain)

Remark In this case X is closed and by X irred we mean in the induced Zariski topology therefore (since closed subsets in X are closed subsets in $\mathbb{A}^n$ contained in X, we have that X is irreducible iff $X = X_1 \cup X_2$ with $X_1, X_2 \subseteq \mathbb{A}^n$ alg sets implies $X = X_i$ for some $i \in \{1,2\}$

PS/

$\longrightarrow$) Suppose X irreducible, let $fg \in I(X)$. Thus $Z(I \cup \{f\}) \cup Z(I \cup \{g\}) = X$

By the irreducibility of X, f or g must vanish on all X hence $I(X)$ prime

$\longleftarrow$) let $X = \underset{\text{alg sets}}{X_1 \cup X_2}$, if $X_i < X$ then $\exists\, f_i \in I(X_i) \setminus I(X)$ for $i = 1, 2$.

Now $f_1 f_2$ vanishes on $X_1 \cup X_2 = X$ so $f_1 f_2 \in I(X)$ with $f_1, f_2 \notin I(X)$ $\lightning$. //

(every ideal is f.g.)

| Since X_1 is closed $X_1 = Z(g_1, \dots, g_k) \subsetneq X$
| So $\exists\, g_t$ vanishing at X_1 not vanishing at X
| So $g_t \in I(X_1) \setminus I(X)$

(affine) algebraic variety

Exercise Let $X \subseteq \mathbb{A}^n$ algebraic set. Then $X = X_1 \cup \dots \cup X_t$ with $\underbrace{X_i \text{ irreducible alg set}}$.

Pf/ If the result is false it is clear that $\exists X_1 \subsetneq X$, $X_2 \subsetneq X$ both closed, st $X = X_1 \cup X_2$

Note $I(X) \subsetneq I(X_1)$. At least one of them does not yield dec into irreducibles
$\subsetneq I(X_2)$

(if both do, then X does). So we can (WLOG) write $X_1 = X_3 \cup X_4$ union of closed

Doing this by induction we get an $\overset{\text{(strictly)}}{\text{ascending}}$ chain of ideals which is infinite $\lightning$. Then X must admit such dec. ☐

If we require that $X_i \not\subseteq X_j$ for $i \neq j$ the expression is unique.

Pf/ Suppose that $Y_1 \cup \dots \cup Y_r$ is another such rep. $Y_1 \subseteq X = X_1 \cup \dots \cup X_t$. So $Y_1 = \bigcup_{i=1}^{t} X_i \cap Y_1$

By the irreducibility of Y_1, $Y_1 \subseteq X_i$ say X_1. Similarly $X_1 \subseteq Y_j$ so $Y_1 \subseteq X_1 \subseteq Y_j$

thus $j = 1$ and $X_1 = Y_1$. By induction we easily conclude the argument ☐

Now take X alg set then $X = X_1 \cup \dots \cup X_n$ irreducible closed $X_i \not\subseteq X_j$ unique), let $J = I(X)$; $J = \sqrt{J}$

$J = \sqrt{J} = I(X_1 \cup \dots \cup X_n) = I(X_1) \cap \dots \cap I(X_n)$, $I(X_i) = \{f : f = 0 \text{ on } X_i\}$ prime ideals

The primary decomposition of I corresponds to this. (We'll see)

Just for a picture; Take $X \subseteq k[x_1, \dots, x_n]$ alg set, $Y \subseteq X$ closed

$I(X) \subseteq I(Y)$. Now $I(Y)$ is of course radical ideal (if f^n vanishes at Y then f does) So we have that $\dfrac{I(Y)}{I(X)} \subseteq A(X)$ radical ideal

Polys in X vanishing at Y so we see $I(Y) \subseteq A(X)$.

By Nullstellensatz we have

$$\{\text{closed subsets of } X\} \longleftrightarrow \{\text{radical ideal in } A(X)\}$$
$$Y \longmapsto I(Y)/I(X)$$
$$(\text{in } X)\ Z(J) \longleftarrow\!\shortmid J/I(X)$$

Under this correspondence if we restrict it to:

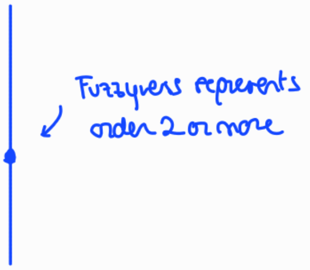
$$\{\text{irred closed subsets of } X\} \longleftrightarrow \{\text{prime ideals of } A(X)\}$$
$$\{\text{points}\} \longleftrightarrow \{\text{max ideals of } A(X)\}$$

For the surj of this take prime in $A(X)$, it is radical so it is $I(Y)/I(X)$ for Y closed, $I(Y)$ prime so Y irred.

Some sort of alg geo $I := \langle x^2, xy\rangle \subset k[x,y]$ not radical $(\sqrt{I} = \langle x\rangle)$

We have (if $|k| = \infty$) $k[x,y] \cong$ ring of poly functions) so this may be seen as the polynomial functions vanishing when $x = 0$, and at least to the order two when $(x,y) = 0$

(Drawing in $\mathbb{R}^2$ to picture smth which potentially is for $k = \mathbb{C}$ "alg geo style")



$$I = \langle x\rangle \cap \langle x^2, xy, y^2\rangle = \langle x\rangle \cap \langle x^2, y\rangle$$

$\Big\}$ rad $\qquad \Big\}$ rad $\qquad \Big\}$ rad

$\langle x\rangle \qquad \langle x, y\rangle \longleftarrow$ associated primes $\qquad \langle x, y\rangle$

We shall see that the primary component corresp to the prime $\langle x\rangle$ is $\langle x\rangle$ while the primary component of $\langle x,y\rangle$ not uniquely det. May be taken as $\langle x^2, y\rangle$ or $\langle x^2, xy, y^2\rangle$

We're only talked about ideals but we'll do things in the more general setting of submodules

We start with a very useful Lemma

Lemma 25 (Prime Avoidance) Let $I_1, \dots, I_n, J \subseteq R$ be ideals

Assume $J \subseteq I_1 \cup \dots \cup I_n$. If R contains an infinite field or at most 2 of the I_i are not prime

Then $J \subseteq I_i$ for some i. (Eisenbud gives geometric interpret and reason to the name)

Proof. If R contains an ^{k}infinite field, any vector space can't be written as a finite union of subspaces (see Lie alg notes for proof). R is a vector space over K and ideals are subspaces. $J \subseteq I_1 \cup \dots \cup I_n$

Suppose $J \nsubseteq I_i$ for any i then $J \subseteq (I_1 \cup \dots \cup I_n) \cap J = (I_1 \cap J) \cup \dots \cup (I_n \cap J) \subseteq J$

So J is a vector space over k union of finitely many proper subspaces ↯.

- Assume that at most 2 of the I_i are not prime. Now we work by induction

$\underline{n=1}$ Trivial

$\underline{n>1}$ If J is contained in any smaller union we are done by induction so suppose $J \nsubseteq \bigcup_{j \neq i} I_i$ for each fixed j. Choose $x_j \in J$ st $x_j \notin I_i$ for $i \neq j$. Then $x_j \in I_j$

If $n = 2$ then $x_1 + x_2 \in J \setminus I_1 \cup I_2$ ↯ So J must be contained in one of I_1 or I_2.

If $n \geq 3$, I_1 is prime (if not relabel) $y = x_1 + x_2 x_3 \cdots\cdots \notin I_i$ $i \in \{1, \dots, n\}$.

Why? $x_1 \in I_1$, $x_i \notin I_1$ for $i > 1$ thus since I_1 prime $x_2 x_3 \cdots \notin I_1$ so $y \notin I_1$. Now $x_2 x_3 \cdots \in I_i$ $i > 1$ but $x_1 \notin I_i$ so $y \notin I_i$ $i > 1$.

But that is a contradiction since $y \in J$. So J must be contained in a smaller union and we are done by induction. (Note If we have 3 not prime we can't say I_1 for $n = 3$ is prime!).

$\square$

Now I will discuss three extra facts that are useful to know (one of them is an exercise suggested by Eisenbud) This could have been done after C.15. I put it here cause it came to me during this section (For example with this 30 makes more sense)

<u>Exercise</u> a) Let R be a ring, $I \subseteq R$ an ideal, then $\exists$ P prime minimal among the primes containing I. (wrt inclussion).

(If I prime obvious) Let $P \supseteq I$ maximal, then it is prime. Now the nonempty partially ordered set of prime ideals over I. Take a totally ordered subset; the intersection of all the elements in this totally ordered subset is prime containg I and a lower bound by Zorn's lemma (dual version of the usually stated) our poset contains a minimal element.

b) (Emmy Noether) Let R be noetherian, $I \subset R$ ideal consider the set of prime ideals over I minimal wrt inclussion (meaning no other prime strictly smaller contains I). Then this set is finite. This elements are called minimal primes of I or minimal primes over I.
(nonempty)

Suppose false. Then $\exists$ $I \subseteq R$ ideal maximal among the set of ideals for which the prop fails (by Noeth. prop). Of course I is not prime (otherwise its set of minimal primes would be finite; only I). So $\exists f, g \notin I : fg \in I$.

<u>Claim</u> Let $Q \supseteq I$ be minimal prime over I. Then Q minimal prime over $\langle I, f\rangle$ or $\langle I, g\rangle$.

$Q \ni fg$ so wma $Q \ni f$ hence $Q \supseteq \langle I, f\rangle$; Q is prime and if $\exists$ $Q' \subsetneq Q$ prime containg $\langle I, f\rangle$ then it also contains I so Q is not minimal prime over I ↯.

So Q minimal prime over $\langle I, f\rangle$.

Since I has infinitely many minimal primes over it, at least one of $\langle I, f\rangle$, $\langle I, g\rangle$ also have infinitely many minimal primes over it ↯. □

* If I prime then $\{I\}$ = minimal primes over I.

c) Let R be a noetherian ring, then if $I \subseteq R$ an ideal $\sqrt{I} = \bigcap_{i=1}^{t} P_i$ where $\{P_1, \dots, P_t\}$ are the minimal primes over I. If I prime trivial, otherwise

$\sqrt{I} = \bigcap_{P \in Z(I)} P$, let $P \in Z(I) = \{P \in \mathrm{Spec}(R),\ I \subseteq P\}$. If P is not minimal among the primes that contain I consider the prime ideals contained in P containg I. Repeating the argument in a) we can find $P_i \in \{P_1, \dots, P_t\}$, $P_i \subseteq P$

Now it follows that $\bigcap_{P \in Z(I)} P = \bigcap_{i=1}^{t} P_i$

$\subseteq$) ✓

$\supseteq$) Let $x \in \bigcap_{i=t}^{t} P_i$, then take $P \in Z(I)$, $\exists i \in \{1, \dots, t\}$ st $\underset{\substack{\rotatebox{90}{$\in$}\\ x}}{P_i} \subseteq P$.

DEF Let R be a ring, M an R-module. A prime ideal $P \subseteq R$ is associated to M if $\exists m \in M : P = \text{Ann}(m) = \{r \in R : r \cdot m = 0\}$. (Note annihilators do not need to be prime in general)

We denote by $\text{Ass}_R(M) = \text{Ass}(M) = \{P \in \text{Spec}(R) : P \text{ associated to } M\}$
(if R clear)

Tradition dictates one exception with this terminology, $I \subseteq R$ ideal ; $\text{Ass}_R(I) := \text{Ass}_R(R/I)$.

(the associated primes of I as an R-module are not interesting, if R domain $I \neq 0$ then the only associated prime of the R-module I is 0)

Remarks i) P is prime so proper. Thus we could say $P \in \text{Ass}(M)$ iff $P = \text{Ann}(m)$ for $m \in M \setminus \{0\}$

ii) Let P be prime. $P \in \text{Ass}(M)$ iff R/P iso to submodule of M. (as R-modules)

It is clear that $P \in \text{Ass}(M)$ iff $P = \ker \varphi_m$ with $\varphi_m : \begin{array}{ccc} R & \xrightarrow{m} & M \\ r & \longmapsto & rm \end{array}$ for some $m \in M \setminus \{0\}$

$\longrightarrow$) ✓

$\longleftarrow$) Take $R/P \xrightarrow{\varphi} M$ $\overset{R\text{ modules}}{\text{1-1 hom}}$, since this is injective (and $1 \notin P$) $\varphi(1+P) = n \in M \setminus \{0\}$

Now for $s \in P$, $s \cdot n = s\varphi(1+P) = \varphi(s+P) = \varphi(0+P) = 0$

Now if $r \cdot n = 0$ then $r\varphi(1+P) = 0$ so $r+P \in \ker \varphi$ so $r \in P$.

Thus $P = \ker(\text{mult by } n)$. (Note the submodule is $\neq 0$; otherwise $P = R$)

Buch writes $R/P \subseteq M$ for this. (of course abuse but it makes sense)

iii) Let $P \subseteq R$ prime, $\text{Ass}_R(P) = \text{Ass}_R(R/P) = \{P\}$

If Q prime ideal, $Q \in \text{Ass}_R(R/P)$ then

$Q = \{s \in R : s(r+P) = 0 \text{ in } R/P \text{ for some } r \in R \setminus P\} = \{s \in R : sr \in P \text{ for some } r \in R \setminus P\}$

$= P$ ($\subseteq$ follows from P being prime ; $\supseteq$ P ideal)

iv) If $P \in \text{Ass}_R(M)$ then $\text{Ann}_R(M) \subseteq P$

Prop 26 Let R be a ring, M an R-module. If I is maximal among the ideals that are annihilators of nonzero elements in M, then $I \in \text{Ass}_R(M)$. So if R noetherian, $M \neq 0$ then $\text{Ass}_R(M) \neq \emptyset$.

Proof/ We just have to show that I prime. Let $m \in M \setminus \{0\} : I = \text{Ann}(m)$.

Suppose $rs \in I$ with $s \notin I$. Then $rsm = 0$ but $sm \neq 0$. Consider $\text{Ann}(sm)$

then $I \subseteq \text{Ann}(sm)$ and $r \subseteq \text{Ann}(sm)$ so $R \supsetneq \text{Ann}(sm) \supseteq \langle I, r \rangle$
(1 does not annihilate)

By maximality $r \in I$. $\square$

Corollary 27 Let R be noetherian ring, M an R-module. Then

i) $m \in M$, $m=0$ iff $\frac{m}{1} = 0 \in M_P$ $\forall P \in \mathrm{Ass}(M)$

ii) $K \subseteq M$ submodule; then $K=0 \leftrightarrow K_P = 0$ $\forall P \in \mathrm{Ass}(M)$

iii) Let $\varphi : M \to N$ hom of R-modules. Then φ 1-1 iff $\varphi_P : M_P \to N_P$ 1-1 $\forall P \in \mathrm{Ass}(M)$
$$\frac{m}{u} \longmapsto \frac{\varphi(m)}{u}$$

Proof/ Of course $\rightarrow$) trivial in three cases. For the last one use ex after prop 10.

i) If $m \neq 0$ then by the previous result we can choose $P \supseteq \mathrm{Ann}(m)$, $P \in \mathrm{Ass}_R(M)$
(R noeth)

then $\frac{m}{1} \neq 0 \in M_P$ ($\frac{m}{1} = 0 \in M_P$ iff $\exists\, u \in R \setminus P$ $u.m = 0$ but $\mathrm{Ann}(m) \subseteq P$)

ii) If $K \neq 0$ choose $0 \neq m \in K$ then by i) $\exists\, P \in \mathrm{Ass}(M)$: $\frac{m}{1} \neq 0 \in K_P$

iii) It is easy to see $(\ker \varphi)_P = \ker \varphi_P$. Now apply ii). ☐

Lemma 28 Let R be a ring, M', M'' R-modules. Let $M = M' \oplus M''$.
Then $\mathrm{Ass}(M) = \mathrm{Ass}(M') \cup \mathrm{Ass}(M'')$. Also if we have
$$0 \to N' \xrightarrow{\varphi} N \xrightarrow{\theta} N'' \to 0$$
short exact seq. of R-modules

then $\mathrm{Ass}(N') \subseteq \mathrm{Ass}(N) \subseteq \mathrm{Ass}(N') \cup \mathrm{Ass}(N'')$

Proof/ It is clear that the 1st part follows from the second.
$$0 \to M' \xrightarrow{i} M \xrightarrow{\pi} M'' \to 0$$
short exact seqs.
$$0 \to M'' \to M \xrightarrow{\pi} M' \to 0$$

We prove the second part. $P \in \mathrm{Ass}(N') \longrightarrow R/p$ $\overset{\text{(R-mod)}}{\text{iso}}$ to a submodule of N'. But N' is iso to a submodule of N so $R/p \cong$ to submodule of N. By remark 2 $P \in \mathrm{Ass}(N)$

So $\mathrm{Ass}(N') \subseteq \mathrm{Ass}(N)$. Let $P \in \mathrm{Ass}(N) \setminus \mathrm{Ass}(N')$. If let $x \in N$: $P = \mathrm{Ann}(x)$

Then $R/p \cong R \cdot x = \{rx : r \in R\}$. But now every $s \in R \cdot x \setminus \{0\}$ (P is prime) has also P as annihilator thus $R \cdot x \cap N = \varphi^{-1}(R \cdot x) = 0$ (if $n' \in \varphi^{-1}(R \cdot x)$ $n' \neq 0$

then for $p \in P$ $\varphi(pn') = p\underset{\in R \cdot x \setminus \{0\}}{\varphi(n')} = 0$ so $pn' = 0$ since φ is 1-1 thus $P \subseteq \mathrm{Ann}(n')$

but if $sn' = 0$ then $s\underset{\in R \cdot x \setminus \{0\}}{\varphi(n')} = 0$ so $s \in \mathrm{Ann}(r \cdot x) = P$. So we would have $P = \mathrm{Ann}(n')$ $n' \in N' \setminus \{0\}$ ↯)

Consider $\theta : R \cdot x \longrightarrow N''$, then $R \cdot x \cap \ker \theta = R \cdot x \cap \mathrm{Im}\, \varphi = 0$ so this is an injective R-hom

Thus $R\cdot x$ is isomorphic to submodule of N'' but $R\cdot x \cong R/p$ so $P \in \mathrm{Ass}(N'')$. The result follows □

get filtration.

Prop 29 Let R be a noetherian ring, M a fg R-module then $\exists$ a filtration

$$0 = M_0 \subsetneq M_1 \subsetneq M_2 \cdots \subsetneq M_n = M \text{; such that } M_i/M_{i-1} \underset{R\text{-modules}}{\cong} R/P_i \text{ where } P_i \subseteq R \text{ prime ideal.}$$

(Note it does not imply f length; P_i would need to be maximal)

Proof/ If $M=0$ then trivial. If $M \neq 0$ then we know M noetherian R-module and we also know by Corollary 26 that that $\mathrm{Ass}_R(M) \neq \emptyset$. This is, $\exists \overset{\neq 0}{M_1}$ submodule of M P_1 prime ideal in R such that $R/P_1 \cong M_1$. Now if $M_1 = M$ then we are done. Otherwise we apply the same to M/M_1 to produce a R-submodule of this R-module iso to R/P_2 with P_2 prime. By correspondence is of the form $M_2/M_1 \neq 0$ so $M_2 \supsetneq M_1$. We do this again and again (induction) but by Noeth property we must reach M at some point so $M_n = M$ for some $n \in \mathbb{N}$. Thus given the desired dec. □

Eisenbud: If M is an R-module with dec like in prop 29 where each $P_i \in \mathrm{Ass}_R(M)$; M is called clean

Theorem 30 (Central Results about associated primes) Let R be a Noetherian ring, $M \neq 0$ fg R-module. Then

this handles the case in which $\mathrm{Ann}(M)$ prime; then $\mathrm{Ann}(M)$ is the only minimal prime over itself

i) $\mathrm{Ass}_R(M)$ is a finite nonempty set containing all minimal primes over $\mathrm{Ann}(M)$.

ii) $\bigcup_{P \in \mathrm{Ass}_R(M)} P = \{ r \in R : \exists\, 0 \neq m \in M, rm = 0 \}$ the set of zero divisors.

Prime containing the ideal and no strictly smaller prime contains it.

iii) $U \subseteq R$ mult. closed then $\mathrm{Ass}_{U^{-1}R}(U^{-1}M) = \{ \underset{\text{in } U^{-1}R\text{; see warning II.}}{U^{-1}P} : P \in \mathrm{Ass}_R(M),\ P \cap U = \emptyset \}$

(if $U \ni 0$ then $U^{-1}M = 0$)

Proof: ii) $\subseteq$) Obvious.

$\supseteq$) let $r \in R$ st $rm = 0$ for $m \neq 0 \in M$, then $r \in \mathrm{Ann}(m)$. By noetherian prop $\exists I$ maximal, $I \supseteq \mathrm{Ann}(m)$ and by prop 26, $I \in \mathrm{Ass}_R(M)$, $r \in I$.

(warning II considered)

iii) By prop 8 and Rmk before C.24 we recall that $\mathrm{spec}(U^{-1}R) = \{ U^{-1}P : P \in \mathrm{Spec}(R), P \cap U = \emptyset \}$

$\supseteq$) Let $P \in \mathrm{Ass}_R(M)$, $P \cap U = \emptyset$ and consider $U^{-1}P$. We want to check that $U^{-1}P \in \mathrm{Ass}_{U^{-1}R}(U^{-1}M)$. By the recall $U^{-1}P$ is prime in $U^{-1}R$

Also since $P \in \mathrm{Ass}_R(M)$, R/P iso to a submodule of M ie

$\exists\ 0 \longrightarrow R/P \xrightarrow{\psi} M$ exact. Therefore we have an exact sequence $0 \longrightarrow U^{-1}(R/P) \longrightarrow U^{-1}M$

(same proof)

But by observation ii of thm 19 $U^{-1}(R/P) \cong U^{-1}R/_{U^{-1}P}$ so $U^{-1}R/_{U^{-1}P}$ is iso to a submodule of $U^{-1}M$ hence $U^{-1}P \in \mathrm{Ass}_{U^{-1}R}(U^{-1}M)$.

$\subseteq$) Take an elmt of $\mathrm{Ass}_{U^{-1}R}(U^{-1}M)$; By the recall this elmt is of the form $U^{-1}P$ $P \in \mathrm{Spec}(R)$, $P \cap U = \emptyset$. We know that $U^{-1}P = \mathrm{Ann}_{U^{-1}R}(m/u)$ where $m/u \in U^{-1}M \setminus \{0\}$ and we want to check $P \in \mathrm{Ass}_R(M)$

Note $U^{-1}P = \mathrm{Ann}_{U^{-1}R}(m/u) = \mathrm{Ann}_{U^{-1}R}(\overset{\neq 0}{m/1})$. Since R is noetherian ring we can choose $u' \in U$ st $\mathrm{Ann}_R(u'm) \subsetneq R$ is maximal among the $\mathrm{Ann}_R(um)$ with $um \in M \setminus \{0\}$. ($1 \in U$ so in the family we have $\mathrm{Ann}_R(m) < R$, $m \neq 0$)

Claim $P = \mathrm{Ann}_R(u'm)$. Note this gives $P \in \mathrm{Ass}_R(M)$ and gives the other inclusion.

$\mathrm{Ann}_R(\overset{\in M}{t}) = R$ iff $t = 0$.

$\supseteq$) If $ru'm = 0$, $\frac{r}{1} \in \mathrm{Ann}_{U^{-1}M}\left(\frac{u'm}{1}\right) = U^{-1}P$

So $\frac{r}{1} = \frac{s}{u}$ with $s \in P$ thus $\exists u' \in U$: $\underbrace{uu'}_{\notin P}r = su' \in P$ so $r \in P$

$\frac{s}{v} \cdot \frac{u'm}{1} = 0$ then $\frac{su'}{v} \in U^{-1}P$, $\frac{su'}{v} = \frac{p}{v'}$ $\to$ $\exists v'' \in U \cdot \underbrace{v''v'u'}_{\notin p}s = vv''p \in P$ so $s \in P$.

The other inclusion is obvious

$\subseteq$) Let $r \in P$, $\frac{r}{1}\frac{u'm}{1} = \frac{u'}{1}\frac{r}{1}\frac{m}{1} = 0$ since $U^{-1}P = \mathrm{Ann}_{U^{-1}R}(m/1)$

So $\exists u'' \in U$: $u'u''rm = 0$. Consider $u'u''m$; if $u'u''m = 0$ then $\frac{u'u''}{1}\frac{m}{1} = 0$ so $\frac{1}{u'u''}\frac{u'u''}{1}\frac{m}{1} = \frac{m}{1} = 0$ ↯ Thus $u'u''m \neq 0$ and

$\mathrm{Ann}_R(u''u'm) \supseteq \mathrm{Ann}_R(u'm)$. So by maximality $\underset{\in r}{r \in} \mathrm{Ann}_R(u'm)$ thus $\subseteq$ is clear //

i) We already know it is nonempty ; by prop 29 we have

$0 = M_0 \subsetneq M_1 \subsetneq M_2 \cdots \subsetneq M_n = M$; such that $M_i/M_{i-1} \underset{R\text{-modules}}{\cong} R/P_i$ where $P_i \subseteq R$ prime ideal.

We prove that $\mathrm{Ass}_R(M) \subseteq \{P_1, .., P_n\}$

By induction. If $n = 1$, then $M \cong R/p$ for P prime. $R/p \xrightarrow{\varphi} M$ iso of R-modules we can easily prove that $\mathrm{Ann}(m) = P$ $\forall$ $m \in M \setminus \{0\}$ so $\mathrm{Ass}_R(M) = P$. Now for $n \geq 2$. We know that $\mathrm{Ass}_R(M_{n-1}) \subseteq \{P_1, \ldots, P_{n-1}\}$.

$$0 \longrightarrow M_{n-1} \xrightarrow{\iota} M \xrightarrow{\pi} M/M_{n-1} \longrightarrow 0$$ exact so

by the L28 $\mathrm{Ass}(M_{n-1}) \subseteq \mathrm{Ass}(M) \subseteq \mathrm{Ass}(M_{n-1}) \cup \mathrm{Ass}(M/M_{n-1}) \subseteq \{P_1, \ldots, P_{n-1}\} \cup \mathrm{Ass}(M/M_{n-1})$

$= \{P_1, .. P_{n-1}\} \cup \{P_n\}$ by the case 1.

We must show that if Q minimal prime over $\mathrm{Ann}(M)$, then $Q \in \mathrm{Ass}_R(M)$

$Q \supseteq \mathrm{Ann}(M)$ so $M_Q \neq 0$

Now since R_Q is noeth

$\mathrm{Ass}_{R_Q}(M_Q) \neq 0$ by prop 26

otherwise take $m_1, \dots, m_t$ generators of M, $M_Q = 0$ so $\frac{m_1}{1}, \dots \frac{m_t}{1} = 0$ in $(R \setminus Q)^{-1} M$. For each of these $\exists\, u_i \in \overset{U}{R \setminus Q}$ st $u_i m_i = 0$ hence $u_1 \cdots u_t \in U$ and annihilates M but $U \cap \mathrm{Ann}\, M = \emptyset$ ↯.

$\downarrow$

Consider an element in $\mathrm{Ass}_{R_Q}(M_Q)$; it is of the form P_Q with $P \in \mathrm{Ass}_R(M)$

$P \cap (R \setminus Q) = \emptyset$ so P prime $P \subseteq Q$ and $\mathrm{Ann}_R(M) \subseteq P$ so by minimality $P = Q$

So $Q \in \mathrm{Ass}_R(M)$ (and $\mathrm{Ass}_{R_Q}(M_Q) = \{Q_Q\}$) $\square$

↳ Alternatively we could use that R_Q is local with $Q R_Q = Q_Q$ only prime ideal.

Example. Let K be a field, $R = K[x,y]$, $I = \langle x^2, xy \rangle = \langle x \rangle \cap \langle x^2, xy, y^2 \rangle$

Then $\mathrm{Ass}_R(R/I) = \{\langle x \rangle, \langle x, y \rangle\}$

$\mathrm{Ass}_R(R/\langle x \rangle) = \{\langle x \rangle\}$

$\mathrm{Ass}_R(R/\langle x^2, xy, y^2 \rangle) = \{\langle x, y \rangle\}$

Note: The main focus of this course is to learn the algebra; People kept asking about geometry (which we use as motivation and also see some applications to it) and Buch answered this after repeated questions

DEF Let R be a noetherian ring, M a fg R-module. We say that M is coprimary if $\mathrm{Ass}_R(M)$ has just one element. M is P-coprimary if $\mathrm{Ass}_R(M) = \{P\}$. (same thing, we specify which)
(by the last thm we see it is prime)

Prop 31 Let $P \subseteq R$ be a prime ideal, $M \neq 0$ fg R-module. TFAE

i) M is P-coprimary.

ii) $P^n M = 0$ for some n, and all elements in $R \setminus P$ are nzdivisors on M.

iii) P minimal over $\mathrm{Ann}(M)$, and all elements in $R \setminus P$ are nzdivisors on M.

Proof/ i → ii) By 30, P is the only minimal prime over $\mathrm{Ann}(M)$ (by the exercise at the beginning $\exists$ minimal prime over any ideal) Therefore $\sqrt{\mathrm{Ann}(M)} = P$ (again by the exercise)

So $P^n \subseteq \mathrm{Ann}(M)$ (P is fg since R noetherian; same idea as in C24), thus $P^n M = 0$

Now by 30 ii $P = \{\text{zero divisors}\}$.

ii → iii) We have to prove P minimal over $\mathrm{Ann}(M)$. First $\mathrm{Ann}(M) \subseteq \text{Zero divisors}(M) \subseteq P$

Now since $P^n M = 0$, $P \subseteq \sqrt{\mathrm{Ann}(M)} = \bigcap_{i=1}^{t} P_i$ with P_i minimal primes over $\mathrm{Ann}(M)$

So of course $P \in \{P_1, \dots, P_t\}$ (in fact we've proved more ☺)

ii → i) Let $Q \in Ass(M)$, then $Q \subseteq$ Zero divisors $(M) \subseteq P$. By minimality of P, $Q = P$. So $Ass(M) = \{P\}$

□

DEF Let R be a Noetherian ring, M a fg R-module. Let $N \subseteq M$ be a submodule. N is a (P-) primary submodule if M/N is (P-) coprimary.

Corollary 32 Let R noetherian ring, $I \subsetneq R$ proper ideal. TFAE (P prime ideal)

i) I P-primary (I seen as an R-submodule of the R-module R)

ii) $P^n \subseteq I$ for some n, $rs \in I$ with $r \notin P \longrightarrow s \in I$

iii) $P = \sqrt{I}$ and $rs \in I$, $r \notin P \longrightarrow s \in I$.

Pf/ $M = R/I$ is P-coprimary iff $P^n M = 0$ and all elements in $R \setminus P$ nzds on M. (Previous prop)

So clearly i is equiv to ii. Now assume iii)

iii → ii) P is fg so clear

i,ii → iii) let $r \in I$ but $r \notin P$ then by ii $1 = s \in I$ ↯ so $I \subseteq P \underset{ii}{\underset{\downarrow}{\subseteq}} \sqrt{I}$

But $P = \sqrt{P}$ so $\sqrt{I} \subseteq P$ thus $\sqrt{I} = P$.

□

Lemma 33 Let R be a noeth ring, M fg R-module. Let $N_1, \dots, N_t \subseteq M$ P-primary submodules, then $N_1 \cap \dots \cap N_t$ is P-primary.

Proof: By induction WMA $t = 2$.

$$M/_{N_1 \cap N_2} \xrightarrow[\text{obv inject}]{} M/_{N_1} \oplus M/_{N_2}$$. So $Ass(M/_{N_1 \cap N_2}) \underset{\downarrow}{\subseteq} Ass(M/_{N_1} \oplus M/_{N_2}) \underset{\downarrow}{\subseteq} \{P\}$

Just see it inside and then by def the ass (submodule) ⊆ ass (module)

both P-cop ∧ L.28

□

Example. $I = \langle x^2, xy \rangle$, $Ass_R(R/I) = \{\langle x \rangle, \langle x, y \rangle\}$ So I not $\langle x \rangle$-primary however $\sqrt{I} = \langle x \rangle$

We now formulate the big theorem. As we said we will formulate this in the more general context of submodules. Then we'll see what it says for ideals.

Theorem 34 (Primary decomp) Let R be Noetherian, M a fg R-module. Then every submodule $M' \subseteq M$ can be written as $M' = M_1 \cap \dots \cap M_n$ where $M_i \subseteq M$ submodule P_i-primary $\forall i$. Also

↳ This is called a primary decomposition of M' in M over R

i) $\mathrm{Ass}_R(M/M') \subseteq \{P_1, \dots P_n\}$ we may have reps (small abuse of notation; properly: "contained among P_i's")

ii) If the expression $M_1 \cap \dots \cap M_n = M'$ is not redundant then $\mathrm{Ass}_R(M/M') = \{P_1, \dots P_n\}$ ← we may have reps

$1 \leq i \leq n$

iii) If n is minimal ($\nexists\, M' = N_1 \cap \dots \cap N_s$ with N_i primary submodules and $s < n$) then $n = |\mathrm{Ass}_R(M/M')|$ (all P_j are different). In this case when P_i minimal prime over $\mathrm{Ann}(M/M')$ then we have that M_i must be precisely $\ker\left(\begin{matrix} M \longrightarrow (M/M')_{P_i} \\ m \longmapsto \frac{(m+M')}{1} \end{matrix}\right)$.

↳ minimal among the primes containing $\mathrm{Ann}(M/M')$.

If you have a dec with $|\mathrm{Ass}_R(M/M')|$ terms it must be minimal by iii)

↳ So M_i determined and it is called P_i-primary component of M' in M over R

We have some part that is unique when not redundant and minimal.

iv) If n is minimal, $U \subseteq R$ mult closed and $P_j \cap U = \emptyset$ iff $j \leq t$. Then $U^{-1}M' = U^{-1}M_1 \cap \dots \cap U^{-1}M_t$ is a minimal primary dec of $U^{-1}M'$ in $U^{-1}M$ over $U^{-1}R$

↳ so all these are seen inside $U^{-1}M$ (warning II considered,

Proof: We shall say that a submodule N of M is irreducible if $N = N_1 \cap N_2$ where N_1, N_2 are submodules of M implies $N = N_1 \vee N = N_2$. (this can be taken as a general def)

→ in our case M is noeth.

Claim 1 M noetherian implies that if M' is a submodule then $M' = M_1 \cap \dots \cap M_n$ with M_i irreducible.

If this is false then by Noeth. we can take a maximal counterexample M'. Now M' is not irreducible so $M' = M_1 \cap M_2$ with $M' \subsetneq M_1$, $\subsetneq M_2$ but M_1, M_2 can't be counterexamples so $M_1 = N_1 \cap \dots \cap N_k$ with N_i irred
$M_2 = T_1 \cap \dots \cap T_s$ with T_i irred

so $M' = N_1 \cap \dots \cap N_k \cap T_1 \cap \dots \cap T_s$ with all irred $\lightning$ □

Claim 2 If $N \subsetneq M$ is irreducible then N is primary.

Otherwise $\mathrm{Ass}_R(M/N) \supseteq \{P, Q\}$ with $P \neq Q$ primes.

By the remarks we know that $R/Q \cong \overline{K_1}$ submodule of M/N so $\overline{K_1} = K_1/N$ by corr. $N \subsetneq K_1 \subseteq M$ submod
ii)

$R/P \cong \overline{K_2}$ submodule of M/N so $\overline{K_2} = K_2/N$ by corr $N \subsetneq K_2 \subseteq M$

If $\overset{0}{\bar{x}} \neq \in \overline{K_1} \cap \overline{K_2}$ then $P = \mathrm{Ann}(x) = Q$ $\lightning$

(note this can be worked out very easily taking $\varphi : R/P \to \overline{K_1}$ isom of R-modules. If $r\bar{x} = 0$ with $\bar{x} \neq 0$ then take $s + P$ with $s \notin P$ st $\varphi(s+P) = \bar{x}$. Now $r\varphi(s+P) = 0$ so $rs \in P$ so $r \in P$.... at this point this must be clear)

so $\overline{K_1} \cap \overline{K_2} = 0$ so $K_1 \cap K_2 = N$ with $K_1 \supsetneq N$, $K_2 \supsetneq N$ submodules $\lightning$

So N is primary. (we have not used noeth).

So we have a primary decomposition.

i) $M/_{M'} = M/_{M_1\cap\cdots\cap M_n} \longrightarrow \bigoplus_{i=1}^{n} M/_{M_i}$ is a 1-1 module hom so we can see

$m+M' \longmapsto (m+M_1, \dots, m+M_n)$

" N, M R-modules N ≩ submodule of M then $\mathrm{Ass}_R(N) \subseteq \mathrm{Ass}_R(M)$; trivial "

$M/_{M'}$ canonically embeded on the RHS so every associated prime of $M/_{M'}$ is one of the associated primes of $\bigoplus_{i=1}^{n} M/M_i$ which by lemma 28 $\subseteq \bigcup_{i=1}^{n} \mathrm{Ass}_R(M/M_i) = \{P_1, \dots, P_n\}$

may be reps

ii) The decomposition is not redundant so $\forall j \in \{1,\dots,n\}$ $N_j = \bigcap_{i\neq j} M_i \neq M'$

So $N_j \cap M_j = M'$, thus $N_j/_{M'} = \dfrac{N_j}{N_j\cap M_j} \cong \dfrac{N_j+M_j}{M_j} \subseteq \dfrac{M}{M_j}$ so $N_j/_{M'}$ is iso to a

$$\begin{tikzcd} & N_j+M_j & \\ N_j \arrow[ur, dash] & & M_j \arrow[ul, dash] \\ & M' \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd}$$

submodule of $M/_{M_j}$ which is P_j - coprimary . So $\mathrm{Ass}_R(N_j/_{M'}) \subseteq \mathrm{Ass}_R(M/_{M_j}) = \{P_j\}$ and the first is non empty by thm 30 ; thus $\mathrm{Ass}_R(N_j/_{M'}) = \{P_j\}$ therefore $\mathrm{Ass}_R(M/_{M'}) \supseteq \{P_j\}$ $\forall j \in \{1,\dots,n\}$. This with i) gives $\mathrm{Ass}_R(M/_{M'}) = \{P_1, \dots, P_n\}$.

we might have reps

iii) By lemma 33 if $P_i = P_j$ then $M_i \cap M_j$ is P_i-primary so we could write M' as ($P_1 = P_2$) $N_1 \cap M_3 \cap \cdots \cap M_n$ with $N_1 = M_1 \cap M_2$ P_1-primary. Hence minimality of n implies P_i are all distinct. This combined with ii) yields the first part of iii .

Now suppose P_i minimal prime over $\mathrm{Ann}(M/_{M'})$; consider $\alpha, \gamma, \delta, \beta$ all natural maps

$$\begin{tikzcd} & (M/_{M'})_{P_i} \arrow[dr, "\gamma"'] & \\ M \arrow[ur, "\text{loc map}\circ\text{proj}", "\alpha"'] \arrow[dr, "\beta"'] & & (M/_{M_i})_{P_i} \\ & M/_{M_i} \arrow[ur, "\delta\quad\text{loc}"'] & \end{tikzcd}$$

$\dfrac{m+M'}{s} \to \dfrac{m+M_i}{s}$

It is clear that this diagram of R-homs commutes . If γ, δ are 1-1 then $\ker\alpha = \ker\beta$

So $M_i = \ker\left(M \longrightarrow (M/_{M'})_{P_i}\right)$ as wanted .

γ is 1-1 The map $M/M' \longrightarrow \bigoplus_{i=1}^{n} M/M_i$ is 1-1. (if $m+M' \in \ker$ then $m \in M_1 \cap \dots \cap M_n$

$$m+M' \longmapsto (m+M_1, -, m+M_n)$$

Therefore $(M/M')_{P_i} \longrightarrow \left(\bigoplus_{j=1}^{n} M/M_j\right)_{P_i} \cong \bigoplus_{j=1}^{n} (M/M_j)_{P_i}$

$\downarrow$ is 1-1 by corollary 12*

$\downarrow$ canonical see note in proof of thm 19

$$\frac{m+M'}{s} \longmapsto \left(\frac{m+M_1}{s}, \dots, \frac{m+M_n}{s}\right) \quad \text{is } 1-1$$

If $j \neq i$ then $P_i \neq P_j$ and $P_j \nsubseteq P_i$ by minimality of P_i therefore $\exists r \in P_j \setminus P_i$. By prop 31 since M/M_j is P_j-coprimary $\exists k \geq 0$; $r^k . M/M_j = 0$ Therefore $(M/M_j)_{P_i} = 0$

($\frac{m+M_j}{1} \in (M/M_j)_{P_i}$ satisfies that if we take the r from above $\frac{m+M_j}{1} = \frac{r^k m + M_j}{r^k} = 0$)

$\lfloor$ M/M_j R-module.

So our map $(M/M')_{P_i} \longrightarrow \hat{\bigoplus_{j=1}} (M/M_j)_{P_i}$ is 1-1 hence γ is 1-1.

$$\frac{m+M'}{s} \longmapsto \left(0, -, 0, \frac{m+M_i}{s}, 0, - 0.\right)$$

δ is 1-1 suppose $\frac{m+M_i}{1}$ is 0 in $(M/M_i)_{P_i}$ then $\exists\, q \in R \setminus P_i$: $qm \in M_i$
Now $\text{Ass}_R(M/M_i) = \{P_i\}$ so the prop 31 says that all $R \setminus P_i$ are nzdivisors on M/M_i ; the above can't happen

iv) We know that $\text{Ass}_R(U^{-1}(M/M_i)) = \{U^{-1}P$ with $P \in \overset{\{P_i\}}{\text{Ass}_R}(M/M_i)$ and $P \cap U = \emptyset\}$ by thm 30

so $\text{Ass}_R(U^{-1}(M/M_i)) = \{U^{-1}P_i\}$ for $i \leq t$
$= \emptyset \quad i > t$

(since $U^{-1}M/_{U^{-1}M_i} \cong U^{-1}(M/M_i)$ the associated primes are the same)

Therefore applying thm 30 i) , $U^{-1}M = U^{-1}M_i$ for $i > t$
$U^{-1}M \supsetneq U^{-1}M_i$ and $U^{-1}M_i$ is $U^{-1}P_i$ - primary. $i \leq t$

Now $U^{-1}M' = U^{-1}M_1 \cap \dots \cap U^{-1}M_t \cap \dots \cap U^{-1}M_n$

$= U^{-1}M_1 \cap \dots \cap U^{-1}M_t$; clearly is a primary decomposition.

To show minimality we have to see by part 3 that $t = |\text{Ass}_R(U^{-1}M/_{U^{-1}M'})|$
But the set is $= \{U^{-1}P,\ P \in \{P_1, -, P_n\} : P_i \cap U = \emptyset\} = \{U^{-1}P_1, -, U^{-1}P_t\}$ which we know has cardinality t because n minimal so all P_i are distinct.

$\square$

What does this say in case we take the primary dec of an ideal?

- Let R be noeth ring, $I \subseteq R$ ideal. Consider $M = R/I$ R-module, then $\mathrm{Ann}(M) = \{ r \in R : rs \in I \ \ \forall s \in R \} = I$ so;

$$\mathrm{Ass}_R(I) \underset{\substack{\downarrow \\ \text{def}}}{=} \mathrm{Ass}_R(R/I) \underset{\substack{\downarrow \\ \text{prop30}}}{=} \{ \underbrace{P_1, \ldots, P_t}_{\substack{\text{minimal} \\ \text{primes over} \\ I,\ t \geq 1}}, \underbrace{P_{t+1}, \ldots, P_n}_{\text{this are called embedded primes}} \}$$

We have that $\exists$ minimal primary dec $I = I_1 \cap \cdots \cap I_t \cap I_{t+1} \cdots \cap I_n$

where I_j ideal in R which is P_j-primary

meaning $\mathrm{Ass}_R(R/I_j) = \{P_j\}$; by corollary 32 we have $[P_j = \sqrt{I_j}$ and $rs \in I_j$ $r \notin P_j \longrightarrow s \in I_j]$

$I_1, \ldots, I_t$ are the primary components of the minimal primes (uniquely determined; in any such dec they will appear)

$I_{t+1}, \ldots, I_n$ are called the embedded components

Example Let $I \subseteq K[x_1, \ldots, x_n] := R$ an ideal (take k alg closed)

Take $I = \bigcap_{j=1}^{n} I_j$ a minimal primary dec. $Z(I) = \bigcup_{j=1}^{n} Z(I_j)$

- If I is radical, then by exercise c) after prime avoidance $I = \bigcap_{i=1}^{t} P_i$ with P_i minimal primes over I note that P_i is P_i primary. From this and the discussion above it follows $t = n$ and this is the decomposition.

So $Z(I) = \bigcup_{j=1}^{t} Z(P_i)$, note $I(Z(P_i)) \underset{\substack{| \\ \text{Nullstellensatz.}}}{=} \sqrt{P_i} = P_i$ prime so by a previous exercise $Z(P_i)$ is irreducible. Also if $Z(P_i) \subseteq Z(P_j)$ $i \neq j$ then $I(Z(P_j)) \subseteq I(Z(P_i))$ so $P_j \subseteq P_i$ so $i = j$ by minimality of P_i, therefore as claimed at the beginning this gives the (unique) decomposition of X alg set as union of irreducible alg sets (start with $X = Z(I) = Z(J)$ where $J = \sqrt{I}$ and use this we get the unique union by means of this theory).

The algebra is done and it is all clear; (every ideal/submodule can be written in some close to canonical way which generalizes UFact in integers for example and also as we have seen it provides the unique way of writing an alg set as union of irreducibles... so at a first look we already see how these abstract things are useful.)
(also it is quite beautiful that with just ACC we can develop all this theory that gives to ideals this UFact flavour)

(The following is just some capture of what I interpret now based on my own conclusions and Buch's words. So no math until end of this discussion)

However (this is not formal but in Scheme theory it is formalized) given an ideal $I \subseteq k[x_1, \dots, x_n]$ and a primary decomposition $I = \underbrace{I_1 \cap \dots \cap I_t}_{\text{primary comp of min primes over } I} \cap I_{j+1} \cap \dots \cap I_n$ (minimal)

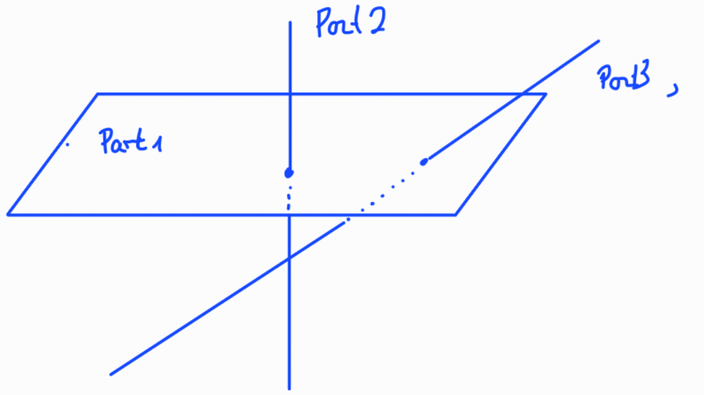
we can give some geometric meaning to what it means for f to be in I. Note f is in I iff it is in every I_i. First of all lets see what $Z(I)$ is.

$Z(I) = Z(\sqrt{I})$, $\sqrt{I} = \bigcap_{i=1}^{t} P_i$ where P_i are the minimal primes over I

STUPID OBS Let R be noetherian, the minimal primes over I are exactly the minimal primes over $\sqrt{I}$. $I \subseteq \sqrt{I}$, if P minimal prime over I then $\sqrt{I} \subseteq P$ by and if it is not a minimal prime over $\sqrt{I}$ then $\exists\ \sqrt{I} \subseteq P_1 \subsetneq P$ prime but this contradicts the fact that P minimal over I so P minimal over $\sqrt{I}$. Let Q be minimal over $\sqrt{I}$ then Q is prime over I, if it is not minimal then $\exists\ I \subseteq P \subsetneq Q$ with P minimal prime over I, but then $\sqrt{I} \subseteq P$ ∫. So Q minimal over I.

(maybe there is a more elementary approach; not important now

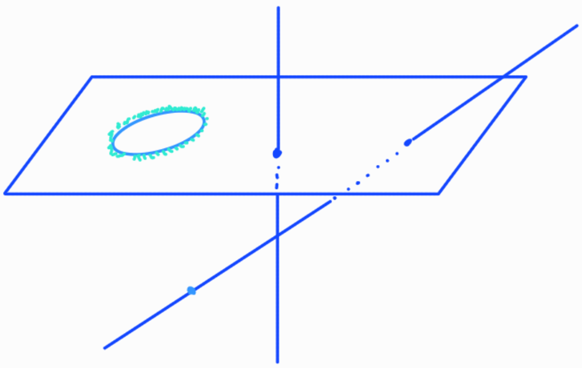
So by the discussion above $Z(I) = Z(\sqrt{I})$ is the Union of the zero sets of the minimal primes over I.



, "Part i is the $Z(P_i)$ where P_i minimal primes over I (or $\sqrt{I}$)."

So if $f \in I$ then f vanishes on that picture. However when we have the primary decomposition we can say a bit more. $f \in I = I_1 \cap \dots \cap I_t \cap I_{t+1} \cap \dots \cap I_n$,

$$\underset{\underset{Z(\sqrt{I})}{\shortparallel}}{Z(I)} = \underset{\underset{Z(P_1)}{\shortparallel}}{Z(I_1)} \cup \dots \cup \underset{\underset{Z(P_t)}{\shortparallel}}{Z(I_t)} \cup \underbrace{Z(I_{t+1}) \cup \dots \cup Z(I_n)}_{\text{these zero sets are embedded in the picture}}$$



Note that for I_j an embedded prime, then it is not radical; if so $I_j = \sqrt{I_j} = P_j$ but it is not minimal over I (embedded part) so we have that $\exists\, i \in \{1, \dots, l\}$: $P_i \subseteq P_j = I_j$, but $I_i \subseteq \sqrt{I_i} = P_i$ so $I_i \subseteq I_j$ ↯ (minimality of expression)

So this could mean that I_j is generated by polynomials vanishing to a higher order (fuzzyness)

($I \subsetneq \sqrt{I}$ so $\exists f \notin I : f^n \in I$)

So if $f \in I$ then f is in every I_j of the primary decomposition and this means that f vanishes in $Z(I_j)$ which means that it possibly vanishes to a higher order close to $Z(P_j)$.

Different decompositions yield different interpretations

Ex: $I = \langle x^2, xy \rangle = \langle x \rangle \cap \langle x^2, y \rangle = \langle x \rangle \cap \langle x^2, xy, y^2 \rangle$

So for the first one $f \in \langle x \rangle \cap \langle x^2, xy, y^2 \rangle$, it vannishes on $x = 0$ and on $(0,0)$ to a higher order

. If we take $f \in$ we do not have the info "derivative vannishing on the vertical direction"

so our mental picture is

Exercise $R = \mathbb{C}[x,y]$, $I = \langle x^3, x^2y \rangle$ find primary dec

Claim $\mathrm{Ass}_R(I) = \{\langle x \rangle, \langle x, y \rangle\}$

Let $m = x^2 + I \in R/_I = M$, $\mathrm{Ann}(m) = \{f \in \mathbb{C}[x,y]\ fx^2 \in I\} = \langle x, y \rangle$ prime (since it is maximal $\langle x-0, y-0 \rangle$); $m = xy + I \in M$, $\mathrm{Ann}(m) = \langle x \rangle$ (we use UFD of $\mathbb{C}[x,y]$)

To see that we do not miss anything use thm 30 ii

Now $I = \langle x^3, y \rangle \cap \langle x^3, x^2 \rangle = \underset{\langle x,y \rangle\text{-primary}}{\underset{\downarrow}{\langle x^3, y \rangle}} \cap \underset{\langle x \rangle\text{-primary}}{\underset{\downarrow}{\langle x^2 \rangle}}$ (using C32) $\square$

- For "monomial ideals" there is a general approach which is more or less elementary (look for Primary dec of monomial ideals) (In exercises Ch 3 Eisenbud too).
- In general it is quite tedious but luckily there is an algorithmic approach (Grobner basis).

We now will give a nice UFD criterion.

Recall, if R is a domain, $x \in R$ nonzero nonunit is said to be:

- Irreducible if $\forall a,b \in R$ $x = ab$ implies a unit or b unit.
- Prime if $\langle x \rangle \subseteq R$ prime ideal.

Also recall prime $\longrightarrow$ irred

Lemma 35 Let R be a noetherian domain. Then R is a UFD $\longleftrightarrow$ all irred elements are primes.

Proof/ $\longrightarrow$) ✓ In UFD prime = irred (see alg qual notes)

$\longleftarrow$) Let $a \in R$ nonzero non unit, we need to show a is product of primes

Assume by contradiction that this is false. Then by noeth take a counterexample with $\langle a \rangle \subseteq R$ maximal (among the ideals generated by elements that fail to be a prod. of primes)

a is not prime so a is not irred so $a = a_1 a_2$ with a_i nonzero nonunit

If a_1, a_2 are both product of primes then so is a so WMA a_1 is not a product of primes

Since $\langle a \rangle \subseteq \langle a_1 \rangle$, by maximality $\langle a \rangle = \langle a_1 \rangle$ so $\exists r \in R : a_1 = ra = r a_1 a_2$

So $a_1(1 - r a_2) = 0$, but we are in a domain so $r a_2 = 1$ so a_2 unit ↯.

Uniqueness is easy with induction.

□

Prop 36 Let R be a noetherian domain

i) If $f \in R$, $f = p_1^{e_1} \cdots p_n^{e_n}$ with $\overset{\text{primes}}{p_i} \in R$, $\langle p_i \rangle \neq \langle p_j \rangle$ for $i \neq j$, $e_i > 0$

Then $\langle f \rangle = \langle p_1^{e_1} \rangle \cap \cdots \cap \langle p_n^{e_n} \rangle$ is minimal primary dec of $\langle f \rangle$

ii) R UFD iff all $\underline{\text{minimal primes over principal ideals}}$ are principal.

$\longrightarrow$ prime ideal minimal among the prime ideals over a principal ideal

Pf/ i) First we show that $\langle p_i^{e_i} \rangle$ is $\langle p_i \rangle$-primary.

- $\langle p_i \rangle^{e_i} \subseteq \langle p_i^{e_i} \rangle$
- If $rs \in \langle p_i^{e_i} \rangle$ with $r \notin \langle p_i \rangle$ then $s \in \langle p_i^{e_i} \rangle$

We proceed by induction on e_i. If $e_i = 1$ clear because p_i prime. Assume $e_i > 1$

$rs = a p_i^{e_i}$ for some a, so $rs \in \langle p_i \rangle$ but $r \notin \langle p_i \rangle$ so $s \in \langle p_i \rangle$. Thus $s = p_i s'$

Now $rs' = a p_i^{e_i - 1} \in \langle p_i^{e_i - 1} \rangle$ with $r \notin \langle p_i \rangle$ so by induction $s' \in \langle p_i^{e_i - 1} \rangle$ so $s \in \langle p_i^{e_i} \rangle$.

By corollary 32 $\langle p_i^{e_i} \rangle$ is $\langle p_i \rangle$-primary.

Secondly we prove $\langle f \rangle = \langle p_1^{e_1} \rangle \cap \cdots \cap \langle p_n^{e_n} \rangle$. $\subseteq$) Trivial.

We prove $\supseteq$).

It is enough to prove that if $p\in R$ prime, $g\in R\setminus\langle p\rangle$ then $\langle p^e g\rangle=\langle p^e\rangle\cap\langle g\rangle$. (Of course)

$\subseteq)$ ✓

$\supseteq)$ Let $gh\in\langle p^e\rangle\cap\langle g\rangle$. $gh=p^e k\in\langle p\rangle$ prime so $h\in\langle p\rangle$ hence we can write

$\frac{h}{p}$ to denote $r\in R$: $h=pr$ and since we are in a domain it is uniquely determined.

So $g\left(\frac{h}{p}\right)\in\langle p^{e-1}\rangle$ repeating this argument we see $h\in\langle p^e\rangle$ so $gh\in\langle p^e g\rangle$ //

We now have that $\langle f\rangle=\langle p_1^{e_1}\rangle\cap\cdots\cap\langle p_n^{e_n}\rangle$ is a primary dec for $I=\langle f\rangle$

So $\mathrm{Ass}_R(R/\langle f\rangle)\subseteq\{\langle p_1\rangle,\ldots,\langle p_n\rangle\}$

Also each $\langle p_i\rangle$ is contained in an associated prime of $\langle f\rangle$, let $m=p_1^{e_1}\cdots p_{i-1}^{e_{i-1}}p_{i+1}^{e_{i+1}}\cdots p_n^{e_n}+\langle f\rangle$

then $p_i\in\mathrm{Ann}_R(m)$. Therefore it follows that $\mathrm{Ass}_R(R/\langle f\rangle)=\{\langle p_1\rangle,\ldots,\langle p_n\rangle\}$

and thus set has exactly n elements. By thm 34 iii it is minimal.

ii) $\longrightarrow)$ Let P be minimal over $\langle f\rangle$. Then $f=p_1^{e_1}\cdots p_n^{e_n}$ (fact. into irreds)

so $\langle f\rangle\subseteq\langle p_i\rangle\subseteq P$ for some i since P is prime. But $\langle p_i\rangle$ prime so $P=\langle p_i\rangle$

$\longleftarrow)$ Let $x\in R$ irreducible, we want to check it is prime (by the last lemma)

Note $\langle x\rangle<R$. Let P minimal prime over $\langle x\rangle$, $P=\langle p\rangle\ni x$. So $x=ap$. Since x irred

a or p is a unit; P prime so p non unit hence a unit so $\langle x\rangle=\langle p\rangle=P$ prime so x is prime □.

7. TOPOLOGY OF SPEC(R)

(digression from Buch; he called it topology of affine schemes but we didn't define affine scheme)

People in the class were asking a lot of questions about the "geometry" so Buch decided to digress a bit and talk about the following.

- Let R be a ring, recall that $\text{spec}(R)=\{P\subseteq R : P \text{ prime ideal}\}$, $Z(I)=\{P\in \text{Spec}(R) : I\subseteq P\}$ for $I\subseteq R$ an ideal.

Examples Let $K=\bar{K}$ and for this discussion $\mathbb{A}^n=K^n$

i) $\text{Spec}(K)=\{0\}$

ii) $\text{Spec}(K[x])=\{\langle x-a\rangle : a\in K\}\cup\{0\}$. Why?

- poly ring is a PID (alg qual)
- In a PID prime ideal is maximal (alg qual)
- We already discussed how prime ideals are

$\updownarrow$ by $\mathbb{A}^1$

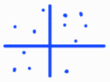
this is called "generic point"

iii) $\text{Spec}(K[x,y])=\{\langle x-a, y-b\rangle : (a,b)\in\mathbb{A}^2\}\cup\{\langle p(x,y)\rangle : p\in K[x,y] \text{ irred}\}\cup\{0\}$

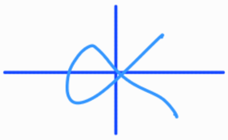
these are the maximal ideals

$\updownarrow$

$\mathbb{A}^2$



these correspond to "irreducible curves in $\mathbb{A}^2$"



$\supseteq$) This is clear.

$\subseteq$) Yes. Why? Because krull dim $k[x,y]=2$ (We will attack this later in the course)

Easy facts Let $E\subseteq R$, $Z(E):=\{P\in\text{Spec}(R) : E\subseteq P\}$.

- $Z(E)=Z(\langle E\rangle)$
- $Z(I)=Z(\sqrt{I})$ for $I\subseteq R$ ideal
- $Z(0)=\text{Spec}(R)$, $Z(R)=\emptyset$
- $\{I_k\}$ family of ideals $Z(\bigcup_k I_k)=\bigcap_k Z(I_k)$
- $Z(I\cap J)=Z(IJ)=Z(I)\cup Z(J)$ for I,J ideals of R

We declare a topology on spec(R) via: closed sets are $Z(I)$ for $I\subseteq R$ ideal and we call this Zariski topology on spec(R).

(note it is the same as if we say $I\subseteq R$.)

Buch said; for us so far spec(R) with the topology is an affine scheme; however the real def of affine scheme needs more, I guess this is an example (perhaps the prototype) of affine scheme. That is why Buch gave the title topology of affine schemes.

Of course R denotes a commutative ring, I ideal, and $\mathrm{Spec}(R)$ carries Zariski topology.

Note $\varphi : \mathrm{Spec}(R/I) \longrightarrow Z(I) \subseteq \mathrm{Spec}(R)$; if we consider the induced topology in

$$P/I \longrightarrow P$$

$Z(I)$ this is a homeomorphism, so informally $\mathrm{Spec}(R/I) \subseteq \mathrm{Spec}(R)$ as a closed subset (Buch said closed "subscheme")

- Let $S \subseteq \mathrm{Spec}(R)$ be a subset ; then the closure of S, $\bar{S} = Z(I)$ for some I. It turns out that $I = \bigcap_{P \in S} P$. $\bar{S}$ is the smallest closed subset containing S. $Z(I)$ closed, let $P \in S$ then $P \in \mathrm{Spec}(R)$, $I \subseteq P$ so $P \in Z(I)$ so $S \subseteq Z(I) \rightarrow \bar{S} \subseteq Z(I)$. Suppose $Z(J) \subseteq \mathrm{Spec}(R$ contains S. We NTS $Z(I) \subseteq Z(J)$. $S \subseteq Z(J)$ so $\forall P \in S$, $J \subseteq P$, therefore $J \subseteq I$, so if $Q \in Z(I)$ clearly $Q \in Z(J)$ so $Z(I) \subseteq Z(J)$ □

- Let $P \in \mathrm{Spec}(R)$. $\{P\}$ closed iff P maximal ideal.

$$\{P\} = \overline{\{P\}} \underset{\text{previous item}}{\longleftrightarrow} \{P\} = Z(P) \longleftrightarrow P \text{ maximal ideal}$$

We denote by Spec-m$(R) = \{P \subseteq R : P \text{ max ideal}\} \subseteq \mathrm{Spec}(R)$. It is not open/closed in general. We consider it as a topological space with the subspace topology.

Example

i) ($K = \bar{K}$) Spec-m $(K[x_1,\dots,x_n]) = \{\langle x_1 - a_1, \dots, x_n - a_n\rangle : (a_1,\dots,a_n) \in \mathbb{A}^n\}$ in bijection.

What if $K \neq \bar{K}$?

ii) Spec-m$(\mathbb{R}[x]) = \{\langle x - a\rangle : a \in \mathbb{R}\} \cup \{\langle (x-c)(x-\bar{c})\rangle : c \in \mathbb{C}, \mathrm{Im}\, c > 0\}$

So it is in bijection with $\{x+iy \in \mathbb{C} : y \geq 0\}$

Let $I \subseteq \mathbb{R}[x]$ be a maximal ideal. Then since $\mathbb{R}$ field $\mathbb{R}[x]$ is a PID so $I = (f(x))$. I is maximal iff $f(x) \in \mathbb{R}[x]$ irreducible in $\mathbb{R}[x]$ (by Alg qual notes, see the 5 of Part3 rings). It is elementary (using F Thm of algebra and that $z \in \mathbb{C}$ root $\rightarrow \bar{z}$ root) that the polys described above are all the irreducible polys in $\mathbb{R}[x]$.

• This will be again defined later but, if R is a (commutative) ring, a (commutative) R-algebra is a (commutative) ring S together with a ring hom $\varphi : R \longrightarrow S$. We write rs in place of $\varphi(r)s$.
S is fg R-algebra if $\exists\, n \in \mathbb{N}, s_1, \dots, s_n \in S$: $S = Rs_1 + \dots + Rs_n$.

If K any field and R is a fg K-algebra we say that R is an affine ring

- This is only used in the next fact (which is given as curiosity / motivation). Later we will again define all of this (in the same way).

  If we look at the defn of alg given $\varphi(R) \subseteq Z(S)$ the center but here S is commutative.

- In every course "algebra" has a slightly different precise def but they are all brothers

Fact If K is any field and R is an affine ring then $\operatorname{Spec-m}(R)$ is a dense subset of $\operatorname{Spec}(R)$. I will prove this result later (After proving Nullst.)

DEF A ring R is reduced if $\sqrt{(0)} = (0)$ i.e. there are no nonzero nilpotent elemts.

· Exercise If R ring, I ideal and $U \subseteq R$ mult closed then

$$U^{-1}\sqrt{I} = \sqrt{U^{-1}I} \text{ in } U^{-1}R.$$

WARNING II WE MUST BE CAREFUL!!! Let N be an R-module, $U \subseteq R$ mult closed considered $U^{-1}N$. Take an element in this module, this is an equivalence class so take a representative n/u. By construction of $U^{-1}N$, $n \in N$. However if $N \leq M$ submodule we often say $U^{-1}N \subseteq U^{-1}M$....
What this means ?? What we mean when we say this is that in $U^{-1}M$ you are considering $\{ g/v : g \in N, v \in U \} \subseteq U^{-1}M$; here you can have representatives $f/u = g/v \in U^{-1}N$ $g \in N, v \in U$ with $f \notin N$. For example, $M = R$, $N = J$ an ideal, $f/u \in U^{-1}J$ means that $\frac{f}{u} = \frac{g}{v}$ with $g \in J$, $v \in U$, so $\exists\, v'' \in U$ st $fvv'' = guv'' \in J$. Why should $f \in J$?
No reason, so in general it doesn't.
So, when you see the def of $U^{-1}N$, any elemt in equivalence class is n/u with $n \in N, u \in U$; however $U^{-1}N \subseteq U^{-1}M$ means : $N \xrightarrow{\varphi} M$ inclusion, take localization map, then $U^{-1}N \xrightarrow{\varphi_U} U^{-1}M$ this is 1-1 hom, so $U^{-1}N \subseteq U^{-1}M$ denotes $\varphi_U(U^{-1}N)$; this is actually. $\varphi_U(U^{-1}N)$ and $U^{-1}N$ are isomorphic; set theoretically they are equal for some adequate fixing of representatives but in $\varphi_U(U^{-1}N)$, an equiv class might have more reps.

* In anything above, when doing $U^{-1}M/U^{-1}N$, $U^{-1}N$ is considered to be

Better to think as
$\{ g/v : g \in N, v \in U \}$

(VIDEO ; "WARNING II")

$\subseteq$) By the above remark, if we take $U^{-1}\sqrt{I} \subseteq U^{-1}R$ then an arbitrary element in $U^{-1}\sqrt{I}$ has a representative of the form $\frac{f}{u}$ with $u \in U$, $f \in \sqrt{I}$ then $\exists n \in \mathbb{N} : f^n \in I$

so $\left(\frac{f}{u}\right)^n = \frac{f^n}{u^n} \in U^{-1}I$ So $f/u \in \sqrt{U^{-1}I} \subseteq U^{-1}R$.

this is omitted when it is clear where are we working.

$\supseteq$) let $f/u \in \sqrt{U^{-1}I}$ then $f^n/u^n \in U^{-1}I$ so $\exists\, v \in U, g \in I$ st $\frac{f^n}{u^n} = \frac{g}{v}$ so $\exists\, v' \in U$

st $v'vf^n = v'u^n g \in I$ so $(v'vf)^n \in I$ $\frac{f}{u} = \frac{fv'v}{uv'v} \in U^{-1}\sqrt{I}$. //

Corollary 37 Let R be a ring, then $\{P \in \mathrm{Spec}(R) : R_P \text{ is reduced}\} = \mathrm{Spec}(R) \setminus \mathrm{Supp}(\sqrt{0})$

Furthermore if R noeth then this set is open. (Buch called this the reduced locus)

Proof/ R_P reduced iff $\sqrt{0_P} = 0_P \subseteq R_P$. iff $(\sqrt{0})_P = 0_P \subseteq R_P$

iff $P \notin \mathrm{Supp}(\sqrt{0})$

↳ def

↳ R-module.

↳ the zero ideal in R_P canden with 0_P; warning considered.

(exercise)

If R noetherian then $\sqrt{0}$ is f.g as an R-module (trivial since ideals are f.g)

So $\mathrm{supp}(\sqrt{0}) = Z(\mathrm{Ann}(\sqrt{0}))$ so closed

↓ Prop 11 iii.

□

Remark Let R be a ring, $U \subseteq \mathrm{Spec}(R)$ open. Let $P \in \mathrm{Spec}(R)$, $Q \in \mathrm{Spec\text{-}m}(R)$ with $P \subseteq Q$

- If $Q \in U \longrightarrow P \in U$ ($Q \in \overline{\{P\}}$ would imply this by elementary point set topology) But this is true since $\overline{\{P\}} = Z(P) \ni Q$.

↳ by one of the items before the last example

- If R affine ring then, let $U \subseteq \mathrm{Spec}(R)$ open, $P \in \mathrm{Spec}(R)$; $P \in U \longleftrightarrow \exists\, Q \in \mathrm{Spec\text{-}m}(R) : P \subseteq Q$ and $Q \in U$.

$\longleftarrow$) ✓

$\longrightarrow$) We know that $\mathrm{spec\text{-}m}(R)$ is dense $\mathrm{Spec}(R)$. Now $\mathrm{Spec}(R/P) \cong Z(P)$ with induced top

This easily implies that $\mathrm{spec\text{-}m}(R) \cap Z(P)$ dense in $Z(P)$

Now $U \cap Z(P)$ open in $Z(P)$ (nonempty) so $\mathrm{Spec\text{-}m}(R) \cap Z(P) \cap U \neq \emptyset$ (dense and open)

Take Q in that intersection

DEF A ring R is generically reduced if R_P reduced for each minimal prime $P \in R$.

If R noeth by ex 6 after L25 there are finitely many minimal primes in R.

Lemma 38 Let R be a noetherian ring, $P \subseteq R$ minimal prime. TFAE

i) R_P reduced
ii) R_P is a field
iii) $P_P = \{0\} \subseteq R_P$
iv) $P = \ker(R \xrightarrow[r \mapsto r/1]{} R_P)$ ⟶ P primary component of the ideal 0 in R (Thm 34)

Proof/ $\mathrm{Spec}(R_P) = \{P_P\}$ seeing $P_P \subseteq R_P$ (this is because R_P local with max $P \cdot R_P \underset{\substack{\downarrow \\ \text{rework} \\ \text{before C.24}}}{=} P_P \subseteq R_P$)

Also note $\underset{\substack{\downarrow \\ \text{the zero ideal in } R_P \text{ coincide with } 0_P \text{ (warning considered)}}}{\sqrt{0_P}} = P_P \subseteq R_P$ ↳ corollary 15. Finally R_P reduced iff $\sqrt{0_P} = 0_P$

With this considerations i ⟷ ii ⟷ iii is clear. Now iii ⟷ iv. If $P = \ker(R \longrightarrow R_P)$ it is clear that $P_P = 0$ inside R_P ($p/1 = 0 \ \forall p \in P$ so $p/u = 0 \ \forall p \in P, u \in R \setminus P$ and since any element in P_P can be represented by one such, we are done)

We only need to prove iii ⟶ iv). Note $\ker(R \to R_P)$ always contained in P. Now, let us
If $r/1 = 0$ in R_P $\exists \, u \in R \setminus P$ st $ru = 0 \in P$ so $r \in P$.
take $p \in P$, $p/1 = 0$ in R_P by iii so $P \subseteq \ker(R - R_P)$, so they are equal and iv follows. □

Proposition 39 A noetherian ring is reduced ⟷ R is generically reduced and R has no embedded primes, meaning that $\mathrm{Ass}(R/0) = \{\text{minimal primes over } 0\}$
(Thm 34, and version for ideals in mind)

Pf/ Let $P_1, \dots, P_n \subseteq R$ be the minimal primes (over 0)

$\sqrt{0} = P_1 \cap \dots \cap P_n$ (ex 3 after L25)

R is reduced iff $0 = \overset{(P_i \text{ is } P_i\text{-primary})}{P_1 \cap \dots \cap P_n}$. This holds iff this is a $\overset{\text{minimal}}{\text{primary}}$ dec of the 0 ideal so iff $\mathrm{Ass}_R(R/0) = \{\text{min primes over } 0\}$ and $P_i = \ker(R \longrightarrow R_{P_i}) \equiv R_{P_i}$ reduced $\forall i$ so this is saying R is generically reduced. □

In algebraic Geometry one wants to prove that some things are reduced (Buch said: "When you have an affine ring, you get an "algebraic scheme over the field" if that scheme is a "variety" then there are more theorems we can use to understand it. To have ⟵ we need the coordinate ring to be reduced). Prove that something is reduced is hard, this makes it a bit easier

For example if R is "Cohen-Macauley" then R has no embedded primes; also methods from intersection theory can help to prove generically reduced (by far easier than reduced).

8. CAYLEY HAMILTON, INTEGRALITY, NAK. (≃4.1 Eis)

The Cayley Hamilton theorem learnt in linear algebra (Alg qual notes / Alg 2 from my undergrad) says that the characteristic polynomial of an endomorphism $\varphi : V \to V$ is satisfied by φ. For our purposes we need a more general one, this is sometimes called determinant trick, and the proof is "the same".

Theorem 40 (General Cayley-Hamilton) Let R be a ring, $J \subseteq R$ ideal. Let M be an R-module generated by n elements. Assume we have $\varphi : M \longrightarrow M$ R-hom, $\varphi(M) \subseteq J.M$ (R-submodule). Then $\exists$ $p(x) = x^n + a_1 x^{n-1} + \dots + a_n \overset{\in R[x]}{}$: with $a_i \in J^i$ and $p(\varphi) = 0$ as an endomorphism of M.

Pf/ Suppose M generated by $m_1, \dots, m_n \in M$. Write $\varphi(m_i) = \sum_{j=1}^{n} a_{ij} m_j$ with $a_{ij} \in J$. Take $A = (a_{ij}) \in M_{n \times n}(J)$, we see M as an $R[x]$-module with $x.m = \varphi(m)$ (so $p(x).m = p(\varphi)m$)

It holds that $(xI - A)\begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$. Now multiplying both sides by cofactor matrix (Thm30 Vspaces alg qual) ($R[x]$ is the countable ring)

we get $\det(xI - A) I_{n \times n} \begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$ so $\det(xI - A) m_i = 0$ $\forall i$

So $p(x) = \det(xI - A)$ is the desired poly, $P(\varphi) = 0$. Expanding the determinant $a_i \in J^i$. ∎

Note that the statement itself does not generalize Cayley-Hamilton but from the proof if $M = V$ n-dim vspace over $R = F$ a field, the poly we get is the characteristic poly. We now give an application. Let $A \subseteq M$ where M is R-mod recall that we say that M is free on A if $\forall m \in M$, $\exists!$ R-linear comb of elmts in A giving m. Then A is called a free basis of M and if $\underbrace{|A| = n}_{\text{called rank}} < \infty$, $M \cong R^n$ as R-modules.

Corollary 41 Let R be a ring, M a fg R-module then

i) Every surjective R-hom $\alpha : M \longrightarrow M$ is an isom (for noeth this is by taking $\operatorname{Ker} \alpha^n$; this is much stronger)

ii) If $M \cong R^n$ and if we have n elmts $\{m_1, \dots, m_n\} \subseteq M$ that generate M, they form a (free) basis (import $R^n \cong R^m$ as R-modules then $n = m$) → this was left as an exercise in alg qual notes,

Pf/ We define in M an $R[t]$-module structure via $p(t).m = p(\alpha)m$. It is of course fg $R[t]$-module (say) with n generators. Let $\varphi = Id : M \longrightarrow M$, since α is surjective $\varphi(M) \subseteq \langle t \rangle M$. ($\langle t \rangle$ in $R[t]$)

By Cayley-Hamilton $\exists$ $p(x) = x^n + a_1 x^{n-1} + \dots + a_n$ such that $a_i \in \langle t \rangle^i$ and $p(Id) = 0$ as an endomorphism of M

It follows that $\exists$ $q(t) \in R[t]$: $(1 - tq(t)).m = 0$ $\forall m \in M$ so $Id - \alpha q(\alpha) = 0$ as an end of M hence $q(\alpha)$ is an inverse for α.

ii) let $\varphi : R^n \longrightarrow M$. Since $\{m_1, -, m_n\}$ generate M this is a surjection
$e_i \longmapsto m_i$

now since M is free of rank n we may choose $\gamma : M \longrightarrow R^n$ isomorphism of R-modules
$\gamma \circ \varphi$ is a surjection hence it is an isomorphism by i. Now $\gamma^{-1}(\gamma \circ \varphi)$ is an isomorphism
but this is φ, so now it is clear that (def from alg qual easy to check) the m_i form
a free basis.
For the iii particular (also proved in alg qual) if $R^n \cong R^m$ with $m<n$, we take a
free basis of R^m with m elements. Then extend this set with some 0 to get n generators
these are not a free basis so we contradict the first part of ii) $\square$

See video for rank discussion. For us if M free and $M \cong R^n$, we say rank$(M)=n$. Also if (on same set)
we say that M is free of rk n, or has free rank n, we mean $M \cong R^n$ (as R-modules)
and this is equivalent to have a free basis of n elements and if $n \neq m$, you can't find $M \cong R^m$,
or a free basis of m elements. (In general rk is defined for M free; however in alg qual notes
for R domain it is defined even if not free; it generalises it "free of rk n will have general rk n".)
(So if M free on A finite rk(M) well defined; $M \cong R^{rk(M)}$ and is the only R^{smth} st M is iso to).

← poly ring ↙ view this as an R-module $r\bar{x} := \overline{rx}$

<u>Prop 42</u> Let R be a ring, $J \subseteq R[x]$ an ideal. Let $S = R[x]/J$ and denote by $\bar{x} := x + J \in S$
i) S is generated by $\leq n$ elements as an R-module $\longleftrightarrow$ J contains a monic poly of degree n
In this case S gen by $1, \bar{x}, -, \bar{x}^{n-1}$ (1 is $\bar{\ }(1)$, $\bar{\ } : R[x] \rightarrow S$ projection)
ii) S is a free R-module of rk n iff J is generated by a monic polynomial of deg n. In this case
$\{1, \bar{x}, -, \bar{x}^{n-1}\}$ is a basis.

Pf/ i) $\longleftarrow$) Let $p(x) = x^n + a_1 x^{n-1} + \dots + a_n \in J$
Note S is generated by $1, \bar{x}, \bar{x}^2, \dots$ as an R-module.
Let $d \geq m$, then $\bar{x}^d = \bar{x}^{d-n} \cdot \bar{x}^n = \bar{x}^{d-n}(-a_1\bar{x}^{(n-1)} - \dots - a_n) = -(a_1\bar{x}^{d-1} + \dots + a_n) \in S$
So the first n powers of $\bar{x}$ generate S as an R-module ($\{1, -, \bar{x}^{n-1}\}$ generate)
$\longrightarrow$) $\varphi : S \longrightarrow S$ R-module hom. $\varphi(S) \subseteq R \cdot S$. By CH $\varphi^n + a_1\varphi^{n-1} + \dots + a_n = 0$ as
$m \longmapsto \bar{x}m$ $\qquad$ $\overset{\shortparallel}{\langle 1 \rangle}$
R module hom from S to S. So $\bar{x}^n + a_1\bar{x}^{n-1} + \dots + a_n = 0$ in S hence $x^n + a_1 x^{n-1} + \dots + a_n \in J$.
Here we're saying: "if gen by n elements $\exists$ monic of degree n. So if gen by $m<n$ elements $\exists$ monic of degree m so monic of degree n, since J is an ideal.

ii) $\longleftarrow$) Let $J = \langle p(x) \rangle$, $p(x) = x^n + a_1$

By i) $1, \bar{x}, \dots, \bar{x}^{n-1}$ generate S as an R-module. NTS li

Suppose $b_0 \cdot 1 + b_1 \cdot \bar{x} + \dots + b_{n-1}\bar{x}^{n-1} = 0$ by def of the module structure and since $\bar{\ }$ is a ring hom

$\overline{b_0 + \dots + b_{n-1}x^{n-1}} = 0$ so $b_{n-1}x^{n-1} + \dots + b_0 \in \langle p(x) \rangle$ but p(x) monic of higher degree so $b_i = 0$.

$\longrightarrow$) Let n be its rank, $S \cong R^n$ by i) $\exists p(x) = x^n + a_1 x^{n-1} + \dots + a_n \in J$ we know that $1, \bar{x}, \bar{x}^2, \dots, \bar{x}^{n-1}$ generate S. By the corollary it is a basis. We claim that p(x) generates J

Let $f \in J$, let q be the remainder after div by p (monic so we can do this always; see alg tema 3 anillos $\overset{\text{valencia}}{}$)

deg q < n and $q \in J$. Now $q(x) = a_m x^m + \dots + a_0$, $m < n$. So in S, $a_m \bar{x}^m + \dots + a_0 = 0$

But $\{1, \dots, \bar{x}^m\}$ li so $a_i = 0$ hence $q = 0$ and thus p generates J □

Now I repeat some of the definitions from the last section and give new ones

DEF Let R be a ring, $\varphi : R \longrightarrow S$ ring hom, S is said to be an (commutative) **R-algebra**

we write $r \cdot s$ to mean $\varphi(r)s$. (In noncommutative case one asks for $\varphi(R) \subseteq$ center of S).

Let S be an R-algebra (there is a hom..) then

0) $S_1 \subseteq S$ a subring is said to be an **R-subalgebra** if $\varphi(R) \subseteq S_1 \equiv r \cdot s_1 \in S_1 \ \forall r \in R, s_1 \in S_1$.

i) **$s \in S$** is said to be **integral** over R if s is a root of a monic poly with coeff in R

ii) **S is integral over** R if all elements are integral over R

iv) **S is finite over R** if S is fg as an R-module ($S = Rs_1 + \dots + Rs_n$)

- Natural gen of notion of algebraic in field extensions.
- If $R \subseteq S$, S R-alg φ = inclusion.

Lemma 43 Let S be an R-algebra, S finite over R. Then S is integral over R.

Proof/ Let $s \in S$, $\varphi : S \longrightarrow S$, $m \longmapsto sm$ this is an R-homomorphism seeing S as an R-module. Now by Cayley-Hamilton (finiteness used here) $\exists p \in R[X]$ monic such that $p(\varphi) = 0$. Let $s \in S$, $p(s) = p(\varphi)(1) = 0$

Corollary 44 Let S be an R-algebra. S is finite over R iff S is generated as an R-algebra by finitely many integral elts.

$\longrightarrow$) Clear from lemma ($s_1, \dots, s_n$ generate S as an R-module, so as an R-algebra too and they are integral)

$\exists a_1, \dots, a_n \in S$ such that $S = R[a_1, \dots, a_n]$ the smallest ring containing $a_1, \dots, a_n$ st it is an R-subalgebra of S. Its elements are polynomials in n variables with coefs in R and the variables substituted by a_i. (This is why we use brackets notation)

$\longleftarrow$) Let $S = R[a_1, \dots, a_n]$ with a_i integral over R

We prove that S is finite over R by induction on n. For n=1 clear

let $S' = R[a_1, \dots, a_{n-1}]$, by induction it is finite over R. So

$S' = Rs_1 + \dots + Rs_t$ for some $s_1, \dots, s_t \in S$. Now a_n is integral over R so it is also integral over S', hence since $S = S'[a_n]$, we claim that S is finite over S'.

Now, $R[x]$, $R[a_1]$ can mean two diff things; usually $R[x]$, $R[t]$ poly rings but also context + I will try to be clear; will help to distinguish.

Consider $\varphi : S'[x] \longrightarrow S$ surjective (ring hom / R-module hom), let $J = \ker\varphi$. a_n is integral over S'
$x \longmapsto a_n$

so J contains a monic polynomial so $S'[x]/_J$ is generated by finitely many elmts as an S'-module by prop 42. So S is fg as an S' module.

Let $\{t_1, \ldots, t_k\} \subseteq S$ be this set of generators of S as an S' module. It is easy to see that $\{t_i s_j\}_{i=1,\ldots,k \atop s=1,\ldots,t}$ generate S as an R module. $\square$

Easy case If R is noetherian and S is noetherian is much easier (smth like $\langle 1, s, \ldots s^n \rangle$ acc argument)

We write $\bar{R}^S$ when needed

Theorem 45 Let R be a ring, S an R-algebra. Let $\bar{R} = \{s \in S : s$ integral over $R\}$ (integral closure/normalization of R in S) ($S = \mathbb{C}$, $R = \mathbb{Z}$) is a ring; so a subring of S.

Pf/ Let $s_1, s_2 \in \bar{R}$. Consider $R[s_1, s_2]$, by collallory 44 it is finite over R, so by 43 it is integral hence $r+s, r-s, rs \in \bar{R}$. It follows that $\bar{R}$ is a ring. $\square$

- Let R be a ring, S an R-algebra. $\bar{\bar{R}} = \{s \in S : s$ is integral over $\bar{R}\} = \bar{R}$. This follows from the next (maybe to formally prove it, we need a bit of the last 3 results) (of carse all closures are over S here.

. R is said integrally closed in S / normal in S if $R = \bar{R}^S$

Prop 46 Let $R \subseteq S \subseteq T$ be rings, suppose S is integral over R, T integral over S. Then T is integral over R.

$$\begin{tikzcd} T \arrow[d, no head] \arrow[d, shift left=3] \arrow[dd, bend left=40] \\ S \arrow[d, no head] \arrow[d, shift left=3] \\ R \end{tikzcd}$$

Proof/ Let $t \in T$. We know $t^n + a_1 t^{n-1} + \ldots + a_n = 0$ for some $a_i \in S$.
Let $R' = R[a_1, \ldots, a_n] \subseteq S$ is finite over R by corollary 44.
Now $R'[t]$ is again finite over R' by C.44. It is easy to see now that $R'[t]$ finite over R
So by L43 t is integral. $\square$

Corollary 47 Let M be a fg R-module, $I \subseteq R$ an ideal. Suppose $M = IM$. Then $\exists r \in I$ such that $rm = m$ $\forall m \in M$

Pf/ Let $\varphi = Id : M \longrightarrow M$. $\varphi(M) \subseteq IM$ by Cayley Hamilton we have that $\varphi^n + a_1 \varphi^{n-1} + \ldots + a_n = 0$ as an R-hom of M with $a_i \in I$. Thus
$m + a_1 m + \ldots + a_n = 0$ $\forall m \in M$ since $\varphi = Id_M$. Let $r = -(a_1 + \ldots + a_n) \in I$
Then $m - rm = 0$ $\forall m \in M$ $\square$

DEF Let R be a ring, the Jacobson radical of R is $\text{Jacobson}(R) = \bigcap_{P \subseteq R \atop \text{max. ideal}} P$.

Notes i) It is of carse related to the one in Group reps but there the algebra may not be commutative so do not worry to much trying to connect those.

ii) $r \in \text{Jacobson}(R)$, $r - 1 \in R^{\times}$ is a unit

Note $r - 1 \notin P$ for any P maximal ideal so $\langle r-1 \rangle = R$. (every proper ideal is contained in a maximal)

Theorem 48 (Nakayama's lemma "NAK"; very used Let R be a ring, M a fg R-module let I be an ideal of R, $I \subseteq$ Jacobson(R). Then

i) If $IM = M$ then $M = 0$

ii) If $m_1, \dots, m_n \in M$ are such that $R\bar{m}_1 + \dots + R\bar{m}_n = M/IM$ then $M = Rm_1 + \dots + Rm_n$ $\quad (\bar{m}_i = m_i + IM)$

generate as R-module.

Canonic application : Let R be local with m maximal ((R,m) local) if $mM = M$ then $M = 0$ (for M fg R-module)

Proof / i) Choose $r \in I$ st $rm = m$ $\forall m \in M$ by last corollary. So $(r-1)m = 0$ $\forall m \in M$

But $r \in I \subseteq$ Jacobson(R) so $r - 1 \in R^*$ hence $m = 0$.

ii) Let $N = M/(Rm_1 + \dots + Rm_n)$ quotient R-module. M/IM is generated as an R-module by $\{\bar{m}_i\}$. So $M = IM + Rm_1 + \dots + Rm_n$. This makes clear that IN is just N

So by i) $N = 0$ as wanted $\square$

Example : It doesn't hold when the module is not fg, let $R = \mathbb{Z}_{\langle p \rangle}$, $\mathbb{Z}$ localised at the prime ideal $\langle p \rangle$, this is $\{\frac{a}{b} \in \mathbb{Q} : (p,b) = 1\}$ Let $M = \mathbb{Q}$, $\langle p \rangle \mathbb{Q} = \mathbb{Q}$ but $\mathbb{Q} \neq 0$.

Exercise: Let R be a ring, M, N R-modules, $U \subseteq R$ mult closed. Then $U^{-1}(M \otimes_R N) = U^{-1}M \otimes_{U^{-1}R} U^{-1}N$

canonically iso

$\cdot$ $U^{-1}M \otimes_{U^{-1}R} U^{-1}N \cong (M \otimes_R U^{-1}R) \otimes_{U^{-1}R} (N \otimes_R U^{-1}R)$

In the exercise after prop 10 we proved $M \otimes_R U^{-1}R \cong U^{-1}M$ canonically isomorphic. This iso is also a $U^{-1}R$-module iso.

Now I need some technicality that I extract from my tensor product notes in alg geom (Atiyah p.27)

Let A, B be (commutative rings), let M be an A-module, P be a B-module an N an (A,B)-module (def: A module and B module simultaneously and the structures are compatible, $(ax)b = a(xb)$ $\forall a \in A$, $b \in B$, $x \in N$.) Then

- $M \otimes_A N$ is naturally a B-module
- $N \otimes_B P$ is naturally an A-module

and $(M \otimes_A N) \otimes_B P \cong M \otimes_A (N \otimes_B P)$

$(M \otimes_R U^{-1}R) \otimes_{U^{-1}R} (N \otimes_R U^{-1}R) \cong M \otimes_R (U^{-1}R \otimes_{U^{-1}R} (N \otimes_R U^{-1}R)) \cong$

Prop with $U^{-1}R$ as an $(R, U^{-1}R)$-module

natural R-module

$\cong M \otimes_R (N \otimes_R U^{-1}R) \cong (M \otimes_R N) \otimes_R U^{-1}R \cong U^{-1}(M \otimes_R N)$.

Prop 10 ii

$U^{-1}R \otimes_{U^{-1}R} (\dots) \cong (\dots)$ as $U^{-1}R$ modules

it should be clear that it is also an R-mod

Ex after prop 10

Everything is canonic

Corollary 49 Let M, N be fg R-modules. Then

i) $M \otimes_R N = 0 \longrightarrow \mathrm{Ann}(M) + \mathrm{Ann}(N) = R$

ii) Also if R is local, $M \otimes_R N = 0$ iff $M = 0$ or $N = 0$.

Proof/ i) STEP 1 WMA R is local.

Assume this is proved for local rings. Let R be any ring, suppose $M \otimes_R N = 0 \wedge \mathrm{Ann}(M) + \mathrm{Ann}(M) < R$. Choose $P \supseteq \mathrm{Ann}(M) + \mathrm{Ann}(N)$ maximal in part prime.

Claim $\mathrm{Ann}(M_p) = \mathrm{Ann}(M)_p$ (here M_p is seen as an R_p-module; this equality is seen inside R_p (warning II in mind))

$\mathrm{Ann}(M_p) = \{ r/u \in R_p : \frac{r}{u}\frac{m}{v} = 0 \ \forall m \in M, v \in R \setminus P \}$

$\mathrm{Ann}(M)_p = \{ s/w : s \in R, sm = 0 \ \forall m \in M, w \in \underset{U''}{R \setminus P} \}$.

$\supseteq$) Trivial. $\subseteq$) as follows:

Let $r/u \in \mathrm{Ann}(M_p)$. Let $m_1, \dots, m_n$ be generators of M as an R-module

$\frac{r}{u}\frac{m_i}{1} = 0$ so $\exists u_i \in U$ st $u_i r m_i = 0$. Let $v := u_1 \cdots u_n$. It is clear that $vr \in \mathrm{Ann}_R(M)$

So $\frac{r}{u} = \frac{vr}{vu} \in \mathrm{Ann}(M)_p$ ($\exists$ rep of that form (warning in mind))

$\mathrm{Ann}(M_p) + \mathrm{Ann}(N_p) \underset{\substack{\downarrow \\ \text{warning II} \\ \text{in mind}}}{=} \mathrm{Ann}(M)_p + \mathrm{Ann}(N)_p \subseteq P_p \underset{\text{(easy)}}{\subsetneq} R_p$.

But $M_p \otimes_{R_p} N_p \underset{\substack{\downarrow \\ \text{canonically} \\ \text{by exercise}}}{\cong} (M \otimes_R N)_p = 0$, so we get a contradiction (because we are assuming true for the local case).

Therefore if we prove it for local rings it follows in general

If M is 0 we are done, assume $M \neq 0$, R local. By Nak $M/PM \neq 0$; also it is easy to see (using nothing) that it is a R/p vector space. So $\exists$ R/p-linear map

$$\begin{tikzcd} M/PM \arrow[r] & R/p \end{tikzcd} \text{ surj; hence } \begin{tikzcd} M \arrow[r] \arrow[rr, bend right, "\varphi"'] & M/PM \arrow[r] & R/p \end{tikzcd} \text{ surjective } R\text{-hom}$$

So it is clear that we get $M \otimes_R N \xrightarrow{\varphi \otimes \mathrm{Id}} R/p \otimes_R N$ surjective R-hom.

But $R/p \otimes_R N \cong N/PN$ (Important idea, general fact ex 2 p31 A&M)

- $0 \longrightarrow P \xrightarrow{\iota} R \xrightarrow{\pi} R/p \longrightarrow 0$ is exact so
- $0 \longrightarrow P \otimes_R N \longrightarrow R \otimes_R N \longrightarrow R/p \otimes_R N \longrightarrow 0$ is exact hence $\underbrace{R \otimes_R N / P \otimes_R N}_{\text{(the image; same remark as in warning II)}} \cong R/p \otimes_R N$

  $p \otimes_R n \longmapsto p \otimes_R n$

  But $R \otimes_R N / \text{(image of) } P \otimes_R N$ is canonically iso to N/PN (Prop 10 ii same idea)

So $0 \twoheadrightarrow N/PN$ thus $PN = N$ and by NAK $N = 0$ so $\mathrm{Ann}(N) = R$ and the result holds for the local case.

ii) Exactly follows from what we've done in the local case. □

<u>Note</u> Let R be a ring, M, N R-modules. $\mathrm{Supp}(M\otimes_R N) = \mathrm{Supp}(M) \cap \mathrm{Supp}(N) \subseteq \mathrm{Spec}(R)$
↘ R-module.

$(M\otimes_R N)_P \overset{\text{can (see by ex}}{=} M_P \otimes_{R_P} N_P$ this is 0 ⟺ M_P is 0 or N_P is 0 by the last result since R_P local

So $\{P\in\mathrm{Spec}(R) : (M\otimes_R N)_P \neq 0\} = \{P\in\mathrm{Spec}(R) : M_P \neq 0\} \cap \{P\in\mathrm{Spec}(R) : N_P \neq 0\}$

9. NORMAL DOMAINS

(≃ 4.2 Eis)

we will use this to refer to the field of fractions.

Let R be a domain, let $K = K(R)$ the field of fractions of R (this was already defined in alg geom notes but we do not need to re do it because this is by def R_0 ie R localised at $R\setminus\{0\}$, our ideal is 0)

We say that **R is normal** if $R = \overline{R}$ the normalisation of R in K ($R = \{s\in K : s \text{ integral over } R\}$)

or integrally closed

(We are seeing $R \subseteq K$ as $\{r/1 : r\in R\} \subseteq K$)
(or $R \to K$, $r \mapsto r/1$)

<u>Note</u> $K(\overline{R}) = K$ and recall from the last section that $\overline{\overline{R}} = \overline{R}$ in K.
(canonically iso I guess)

<u>Prop 50</u> If a ring R is a UFD then it is normal.

<u>Proof</u>/ Assume $r/s \in K$ integral over R. WLOG r, s are relatively prime (if not $\frac{r}{s} = \frac{r'}{s'}$ with these rel prime)
We are in UFD so clear notion.

$\left(\frac{r}{s}\right)^n + a_1\left(\frac{r}{s}\right)^{n-1} + \dots + a_n = 0$ with $a_i \in R$

Then $r^n + a_1 s r^{n-1} + \dots + a_n s^n = 0$ so $s \mid r^n \longrightarrow s$ is a unit so r/s is in $R \subseteq K$. □

<u>Notes</u> i) This is generalising "the algebraic elements in $\mathbb{Q}$ are $\mathbb{Z}$".
ii) Ex 4.18 (Buch did not mention) R normal iff $R[x]$ normal.

We now generalise Gauss lemma.

<u>Prop 51 ("Gauss' Lemma")</u> Let $R \subseteq S$ rings, $f(x) \in R[x]$ monic. Assume $f(x) = g(x)h(x)$ where $g(x), h(x) \in S[x]$ monic. Then $g(x), h(x) \in \overline{R}[x]$, where $\overline{R}$ is the integral closure of R in S.

<u>Proof</u>/ We proceed by induction on $\deg(g(x))$. If $\deg(g(x)) = 0$ then $h(x) = f(x) \in R[x]$

Assume that $\deg(g(x)) \geq 1$ (monic). $\exists S' \supseteq S$ ring and $\alpha \in S'$ st $g(\alpha) = 0$.

Let $S[t]$ denote poly ring in variable t, $\bar{\ } : S[t] \longrightarrow S[t]/\langle g(t)\rangle$ ring hom.
$$f(t) \longmapsto f(t) + \langle g(t)\rangle$$

Let $S' = S[t]/\langle g(t)\rangle$, ring. Let $n := \deg(g)$. By prop 42 $S' = S\cdot\bar{1} + S\cdot\bar{t} + \dots + S\bar{t}^{n-1}$

$\{\bar{1}, \bar{t}, \dots, \bar{t}^{n-1}\}$ is an S-basis of S' as an S-module. It is free of rank n and the S-module structure is via $s \cdot \overline{f(t)} = \overline{sf(t)}$.

This allows us to see $\varphi : S \longrightarrow S'$ as a ring hom and 1-1, if $s\bar{1} = 0$ then $s = 0$ (basis)
$$s \longmapsto s\cdot\bar{1}$$

So we can see $S \subseteq S'$ (surjecty and get the same because it is embedded)

Now $g(x) = x^n + a_{n-1}x^{n-1} + \dots + a_n \in S[x] \subseteq S'[x]$ But $g(\bar{t}) = \overline{g(t)} = 0$

So $\exists\, \alpha \in S'$: α is a root of $g(x) \in S'[x]$.

Now recall that in a commutative ring we can perform division algorithm when we are dividing by a monic polynomial (16.3 Isaacs Algebra, so in my ring they notes from VIC for ex)

$g(x) = (x-\alpha)g_1(x)$ in $S'[x]$ (g_1 monic)

So $f(x) = (x-\alpha)f_1(x)$ in $R'[x]$ where $R' = R[\alpha] \subseteq S'$

Now $(x-\alpha)f_1(x) = (x-\alpha)g_1(x)h(x) \xrightarrow[x-\alpha \text{ monic}]{} f_1(x) = g_1(x)h(x)$ in $S'[x]$

so $(x-\alpha)f = 0$
means $f = 0$ easily

By induction $g_1(x), h(x) \in \overline{R'}^{S'}[x]$. Now $f(\alpha) = 0$ so $\alpha \in \overline{R}^{S'}$. This implies that $\overline{R'}^{S'} = \overline{R}^{S'}$ $\supseteq$) Clear. $\subseteq$) Let $s' \in \overline{R[\alpha]}^{S'}$. Then is $R'[s']$ is finite over R'. $R' = R[\alpha]$ is finite over R (all by C44). Now $R'[s']$ is finite over R and hence s' integral over R. So $s' \in \overline{R}^{S'}$.

So $g_1(x), h(x) \in \overline{R}^{S'}[x]$. Since $\alpha \in \overline{R}^{S'}$ we have that $g(x) \in (\overline{R}^{S'} \cap S)[x]$

But this is exactly $\overline{R}^{S}[x]$. $h(x) \in (\overline{R}^{S'} \cap S)[x]$ (g, h were already in $S[x]$) □

Corollary 52 Let R be a normal domain, $K = K(R)$. Let $f(x) \in R[x]$ monic.

i) $f(x)$ irreducible in $R[x]$ iff $f(x)$ irreducible in $K[x]$.

ii) $f(x)$ irreducible in $R[x]$ $\longrightarrow$ $f(x)$ is a prime element in $R[x]$.

Proof/ i) $\longleftarrow$) Trivial. $\longrightarrow$) Suppose $f(x) = g(x)h(x)$ in $K[x]$ (degree ≥ 1)

Note that $g(x) = \frac{\alpha}{\beta}x^n + \dots$, $h(x) = \frac{\gamma}{z}x^m + \dots$ with $\frac{\alpha\gamma}{\beta z} = 1$

$g(x)h(x) = \frac{\tau}{\gamma}\frac{\gamma}{\tau} g(x)h(x) = \frac{\gamma}{\tau}g(x)\cdot\frac{\tau}{\gamma}h(x) = \tilde{g}(x)\tilde{h}(x)$ monic. By Gauss Lemma $f(x) = \tilde{g}(x)\tilde{h}(x)$, $\tilde{g}, \tilde{h} \in \overline{R}[x] = R[x]$ since $\overline{R}^K = R$ (R is normal)

ii) Let $f(x) \in R[x]$ irreducible and monic. Then by i) $f(x) \in K[x]$ is irred monic also. Hence $\langle f(x)\rangle \subseteq K[X]$ is a prime ideal ($K[X]$ is UFD, and prime = irred in UFD)

By Prop 42, $R[x]/\langle f(x)\rangle$ is a fg free R-module.

$\varphi : R[x]/\langle f(x)\rangle \longrightarrow R[x]/\langle f(x)\rangle \otimes_R K$, R-hom and 1-1

$\bar{g} \longmapsto \bar{g} \otimes_R 1$

If $\bar{g} \otimes_R 1 = 0$ then write $r_1 \cdot 1 + r_2\bar{x} + \dots + r_{n-1}\bar{x}^{n-1} = \bar{g}$ (note $\{1, \dots, \bar{x}^{n-1}\}$ is an R-basis)

$\bar{g} \otimes_R 1 = r_1\, 1 \otimes_R 1 + \dots + r_{n-1}\,\bar{x}^{n-1} \otimes 1 = 0 \underset{\downarrow}{\longrightarrow} r_i = 0$

> If F, F' are free A modules with bases $\{e_i\}_{i\in I}$, $\{e_j'\}_{j\in J}$ then $F \otimes_A F'$ is free A-module with basis $\{e_i \otimes e_j'\}_{(i,j)\in I\times J}$
>
> (this is prop 3 of my tensor product notes)

It is easy to see that $R[x]/\langle f(x)\rangle \otimes_R K \cong K/\langle f(x)\rangle$
$\downarrow$
canonically via $\bar{f}(x) \otimes_R k = k\bar{f}(x) \otimes_R 1 \longrightarrow k\bar{f}(x)$.

and the composition of these two is ring hom also so $R[x]/\langle f(x)\rangle$ is iso to a subring of $K[x]/\langle f(x)\rangle$

So it is a domain and therefore (alg qual) $\langle f(x)\rangle$ is prime. □

<u>Proposition 53 (localization commutes normalization)</u> Let $R \subseteq S$ be rings, $U \subseteq R$ mult closed

$U^{-1}(\overline{R}^S) = \overline{U^{-1}R}^{U^{-1}S} \subseteq U^{-1}S$ (Here note that everything is clear, VIDEO)

Proof/ $\subseteq$) let us consider an element in $U^{-1}(\overline{R}^S)^{\subseteq U^{-1}S}$. This is an equiv class and we know (warning II) that we can take $\frac{s}{u}$ with $s \in \overline{R}^S \subseteq S$, $u \in U$ as a rep. $\frac{s}{1} \in \overline{U^{-1}R}^{U^{-1}S}$, also $\underset{\in U^{-1}S}{\frac{1}{u}}$ is integral over $U^{-1}R$ (take $x - \frac{1}{u}$). So $\frac{s}{u} \in U^{-1}S$ is integral over $U^{-1}R$, $\frac{s}{u} \in \overline{U^{-1}R}^{U^{-1}S}$.

$\supseteq$) Let $\frac{s}{u} \in U^{-1}S$ integral over $U^{-1}R$. We need to show $\exists v \in U$ s.t. sv integral over R this way $\frac{s}{u} = \frac{sv}{uv} \in U^{-1}(\overline{R}^S) \subseteq U^{-1}S$. (important). If

$(\frac{s}{u})^n + (\frac{r_1}{u_1})(\frac{s}{u})^{n-1} + \dots + \frac{r_n}{u_n} = 0$, multiplying by $(uu_1 \cdots u_n)^n$ we get that in S

$(\frac{su_1\cdots u_n}{1})^n + \frac{r_1\,(uu_2\cdots u_n)(su_1\cdots u_n)^{n-1}}{1} + \dots = 0$. Let $\tilde{u} = u_1 \cdots u_n \in U$

$$\frac{(s\tilde{u})^n + \tilde{r}_1 (s\tilde{u})^{n-1} + \cdots}{1} = 0 \quad \text{with } \tilde{r}_i \in R .$$

So $\exists w \in U$: $w((s\tilde{u})^n + \tilde{r}_1 (s\tilde{u})^{n-1} + \cdots +) = 0$ in S

So this also holds if we multiply by w^n. So $(sw\tilde{u})^n + \tilde{r}_1 w (sw\tilde{u})^{n-1} + \cdots = 0$ in S

Let $v = w\tilde{u}$, sv satisfies a $\overset{\text{monic}}{\text{polynomial}}$ in $R[x]$ as wanted $\square$

Corollary 54 Let R be a normal domain, $0 \notin U$. Then $U^{-1}R$ is a normal domain

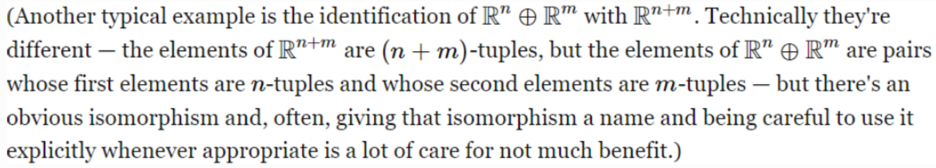
Proof/ We have to check that $\overline{U^{-1}R}^{K(U^{-1}R)} = U^{-1}R$. We know $\overline{R}^{K(R)} = R$

Since $0 \notin U$, $K(U^{-1}R) = K(R) = U^{-1}K(R)$ canonically $\overset{\text{identified)}}{}$ (sau and $U^{-1}R$ is of course embedded each of them; therefore taking the int. closure of $U^{-1}R$ in $K(U^{-1}R)$ gives elmts in $K(U^{-1}R)$ which after the identification are the same as if we take int. closure of $U^{-1}R$ in $K(R)$...

So working with these fields naturally identified $\overline{U^{-1}R}^{K(U^{-1}R)} = \overline{U^{-1}R}^{U^{-1}(K(R))} = U^{-1}(\overline{R}^{K(R)}) = \underset{\text{in } K(R)}{U^{-1}R}$

(this has many identifications going on, but ensures that the integral elmts of $U^{-1}R$ in its field of fractions are only $U^{-1}R$. $\square$

VIDEO (Identification; triangule)



(Another typical example is the identification of $\mathbb{R}^n \oplus \mathbb{R}^m$ with $\mathbb{R}^{n+m}$. Technically they're different — the elements of $\mathbb{R}^{n+m}$ are $(n+m)$-tuples, but the elements of $\mathbb{R}^n \oplus \mathbb{R}^m$ are pairs whose first elements are n-tuples and whose second elements are m-tuples — but there's an obvious isomorphism and, often, giving that isomorphism a name and being careful to use it explicitly whenever appropriate is a lot of care for not much benefit.)

Geometric meaning / Some motivation

A paragraph with { means it contains more than known and should be taken as intuition.

· Let $K = \overline{K}$, $\mathbb{A}^n = K^n$. Let $X \subseteq \mathbb{A}^n$ alg set, $A(X) = K[x_1, -, x_n]/I(X)$

If $A(X)$ is a normal domain, then the "singularities" of X form a closed subset of X of "codim" ≥ 2. To define singularities we need to talk about dimension, it will come. But the mental picture of singularity is clear, so for now this can be taken as "this serves for some purpose in alg geo".

$A(X)$ not normal,

$A(X)$ is normal.

So if X is a "curve" (will define as Krull dimension 1), then $A(X)$ normal $\longleftrightarrow$ X is nonsingular.

· We will soon talk about "finiteness of integral closure". We will prove the following:

Thm

Let R be a domain, which is a finitely generated k-algebra over a field k. (affine domain over k). Let $K = K(R)$ its field of fractions. Consider $K \subseteq L$ finite field extension. Then $\overline{R}^L$ is a finitely generated R-module. In particular $\overline{R}^L$ domain fg k-algebra.

Note If, R_1, R_2 are S-algebras, $\varphi: R_1 \longrightarrow R_2$ ring hom is said to be a S-algebra hom if $\varphi(s \cdot r) = s \cdot \varphi(r)$ $\forall$ $r \in R_1$, $s \in S$ (Of course)

this is the hom $S \to R_1$

this is the hom $S \to R_2$

OBVIOUS OBSERVATION: R k-algebra. It is fg iff $R \cong k[x_1, \ldots, x_n]/I$ on some ideal I

as k-algebras ($k[x_1, \ldots, x_n]/I$ k-alg in the obvious sense)

Proof/ $\longrightarrow$) R is a k-algebra, fg so $R = k[a_1, \ldots, a_n]$ for some $a_i \in R$

Let $k[x_1, \ldots, x_n] \longrightarrow R = k[a_1, \ldots, a_n]$, k-algebra hom so $R \cong k[x_1, \ldots, x_n]/I$ as k-alg

$f(x_1, \ldots, x_n) \longmapsto f(a_1, \ldots, a_n)$

(as rings by 1st iso thm, now it is obvious that this iso from the thm carries the k-alg structure)

$\longleftarrow$) $k[x_1, \ldots, x_n]$ fg as a k-algebra so image by surjective hom is also fg k-algebra. $\square$

So if we start with $X \subseteq \mathbb{A}^n$ ($k = \overline{k}$) irreducible alg set. Then $A(X) = \frac{k[x_1, \ldots, x_n]}{I}$ with I prime ideal (this was done in the motivation part of section 6). Since we are taking a quotient over a prime ideal, $A(X)$ is a domain and by the obvious observation is a fg k-algebra.

Therefore if we consider $\overline{A(X)}$ the normalization in its field of fractions, by the result we will prove $\overline{A(X)}$ is a fg (domain) k-algebra so again by the obvious obs, $\overline{A(X)} \cong k[y_1, \ldots, y_n]/J$ where J is an ideal; prime (since $\overline{A(X)}$ is a domain)

- We define $\overline{X} = Z(J) \subseteq \mathbb{A}^n$ the normalization of X

¡Another irreducible alg set! $I(Z(J)) \overset{\text{nullst.}}{=} \sqrt{J} = J$ prime, so the discussion at the beginning of sec 6 applies

- What is the relation between X and $\overline{X}$?

Let us try to see ("try") that $\overline{X}$ is X but with "worst singularities" straightened out.

Let $x_i := x_i + I(X) \in A(X) \subseteq \overline{A(X)} \cong k[y_1, \ldots, y_n]/J$, so $x_i = f_i(y_1, \ldots, y_n) + J \equiv$

$\equiv f_i(y_1, \ldots, y_n)$. (a bit abusive)

Define $\pi: \overline{X} \longrightarrow X$

$(b_1, \ldots, b_n) \longmapsto (f_1(b), \ldots, f_n(b))$

- Where "nonsingular" locally gives "iso of varieties".
- $A(\overline{X}) = \overline{A(X)}$ (clear) and this is normal so "a bit less singular".

This map is "bijective most places" (follows from things we will prove later). He said a few more things, see his handwritten notes. But at this point I think it is better to stay like this. (I have a few recordings VIDEO: Norm of X)

Rmks: i) He gave an example (see his handwritten notes) but not very enlightening for me now

ii) The significance of $\overline{U^{-1}R} = U^{-1}\overline{R}$ (prop 53) is that is needed to prove smth about normalize by pieces and glue together.

PLAN: The theorem we've mentioned above is thm 4.14 in Eisenbud; Eisenbud proves 4.14 as a consequence of a thm called Noether Normalization. This is thm 13.3 in Eisenbud but 13.3 presents a very general statement. Eisenbud primarily calls Noether normalization to the A1 in Ch8; Our plan is

- Prove a Baby version (but gives the essence) thus Noeth Norm thm (that has NOTHING to do with the normalization explained above; is just a name)
- as a conseq of Noeth Norm
 Prove Nullstellensatz and add some " Corollaries and " Geometry discussion (With some intentions and more or less following our sec 7)
- Briefly say smth about regular functions ("extra"; cause I asked him).
- Prove Lying over / Going up... (4.4 Eis)
- Prove the theorem 4.14 (finiteness of integral closure). Take this as an opportunity to review Galois theory. (Including sep.)
 (this makes use of Noether norm)

(After this discussions everything that follows is somewhat motivated)

10. NOETHER NORMALIZATION (LITE)

"Eisenbud" (baby version of thm 13.3; mentioned with a bit more generality than us in the A1 of sec 8.2)

Recall that R affine ring is by definition a ring that it is fg as an algebra over a field k ($R = k[a_1, \dots, a_n]$)

This is equivalent to say that R is k-alg, $R \underset{(k\text{-alg})}{\cong} k[x_1, \dots, x_n]/_I$ poly ring.

Stupid rmk If $R \neq 0$ affine ring over k, then $k \hookrightarrow R$ (ie the k-alg map is injective).

Wma $R = k[x_1, \dots, x_n]/_I$ I proper. If this is not true then $\tilde{\varphi}: k \xrightarrow{\varphi} k[x_1, \dots, x_n] \xrightarrow{\pi} k[x_1, \dots, x_n]/_I$

$\exists \lambda \in k \setminus \{0\}: \varphi(\lambda) \in I$. But then $\underset{\substack{\| \\ 1}}{\varphi(\lambda^{-1})\varphi(\lambda)} \in I$. So $I = k[x_1, \dots, x_n]$ ∎.

(No harm to take $\lambda \in R$ ($\lambda \in k$)) this is just $\lambda \cdot 1$)

As we said before the next thm has nothing to do with normalization

Theorem 55 (Noether Normalization) Every affine ring $\neq 0$ is a finite extension of a polynomial ring. More precisely

If R affine ring $\neq 0$ over k, $\exists S \subseteq R$ subring (which is also a k-subalgebra) st R is fg S-module ($R = Sa_1 + \dots + Sa_m$)

and $S \underset{(k\text{-alg iso; } \exists \text{ natural structure})}{\cong} k[x_1, \dots, x_n]$ polynomial ring over k. (possibly 0 variables; k)

Proof/ We proceed by induction on the number generators of R over k ($R = k[a_1, \dots a_i]$)

- If we have zero generators then by definition this is $\varphi: k \to R$ (the k-algebra map) is an isomorphism. So $R \cong k$ as k-alg and we can take $S = R$.

- Assume R is generated by n elements as a k-algebra: We know that $R \underset{(\text{as k-alg})}{\cong} k[x_1, \dots, x_n]/_I$ → poly ring

So of course we may assume $R = k[x_1, \dots, x_n]/_I$. If $I = 0$ then $S = R$ so WLOG $I \neq 0$.
 (we are going to make an assertion about a subring.)

CASE 1 $\exists f \in I \setminus \{0\}$ monic in x_n ☆ $\longrightarrow$ we are done. (if $n=1$, $f_i \in k$)

($f = f_0 + f_1 x_n + \dots + f_{d-1} x_n^{d-1} + x_n^d$, $f_i \in k[x_1, \dots, x_{n-1}]$.)

Let $T = k[x_1, \dots, x_{n-1}, f]$ subring of $k[x_1, \dots, x_n]$ (also k-subalgebra, by def of $k[\dots]$. Contains k: note the k-alg structure of $k[x_1, \dots, x_n]$ is given by "inclusion", and check the def of k-subalgebra).

Now, we see $T[x_n]$ as an algebra over T, note that x_n integral over T (see expression of f) so by C44 $T[x_n]$ is finite over T. Note $T[x_n] = k[x_1, \dots, x_n]$ as a set. So $k[x_1, \dots, x_n]$ is fg as a T module.

So $R = k[x_1, \dots, x_n]/I$ finite over $\frac{T+I}{I}$ (it inherits a $\frac{T+I}{I}$ module structure and we can use the generators of $k[x_1, \dots, x_n]$ as a T module to generate this) Note $T+I/I$ inherits a k-algebra structure and also $f \in I$ so $T+I/I$ is generated* by $\overline{x_1}, \dots, \overline{x_{n-1}}$ as a k-algebra. By induction $\exists S \subseteq T+I/I$ k-subalgebra such that $T+I/I$ is finite over S and $S \simeq$ poly ring over k (or k). Clearly R is finite over S. ($S \subseteq R$ k-subalgebra)

*If $n=1$. Then $T = k[f] = \{\lambda_0 + \lambda_1 f + \lambda_2 f^2 + \dots + \lambda_n f^n \mid n \in \mathbb{N}, \lambda_i \in k\}$
So $T+I/I = \{\lambda + I : \lambda \in k\}$, so satisfies the def of gen by 0 elements and the induction applies

(R has S-module structure and $R = \frac{T+I}{I} a_1 + \dots + \frac{T+I}{I} a_m$
$\hookrightarrow b_1 S + \dots + b_l S$)

Note in the case $n=1$ we are done since I ideal $\neq 0$ always contains a monic pol. So recall case $n \geq 1$.

GENERAL CASE: Let $f = \sum c_q x^q$, $c_q \in K$, $x^q = x_1^{a_1} \cdots x_n^{a_n}$

Choose $e \in \mathbb{N}$ st $e > \max\{a_1, \dots, a_n\}$ for all q st $c_q \neq 0$. Set $x_i' = x_i - x_n^{e^i}$ for $1 \leq i \leq n-1$

Now $k[x_1, \dots, x_n] = k[x_1', \dots, x_{n-1}', x_n]$ where the last set is first seen as k-algebra gen by.

__Claim__ $\exists g \in I$ monic x_n as a "polynomial" in $k[x_1', \dots, x_{n-1}', x_n]$ (See video Noeth Norm)

$x_1^{a_1} \cdots x_n^{a_n} = (x_1' + x_n^e)^{a_1} \cdots (x_2' + x_n^{e^{n-1}})^{a_{n-1}} x_n^{a_n}$; this monomial is monic in x_n

note the largest term is $x_n^{a_n + a_1 e + \dots + e^{n-1} a_{n-1}}$. By our choice of e all monomials occurring in f have distinct degree highest term in x_n so they do not cancel and by reorganizing we end up with $f = c_x x_n^d + x_n^{d-1} f_1 + \dots$ $f_i \in k[x_1', \dots, x_{n-1}']$

multiplying f by a constant we get $g \in k[x_1', \dots, x_{n-1}', x_n]$ monic in x_n.

Note that $k[x_1', \dots, x_{n-1}', x_n]$ as a k-algebra is iso to the poly ring $k[x_1', \dots, x_{n-1}', x_n]$

Apply Case I to $k[x_1', \dots, x_{n-1}', x_n]/I$ and the subalg S we get iso to a poly ring
(S pulled back to $k[x_1', \dots, x_{n-1}', x_n] \overset{(=)}{\subseteq} k[x_1, \dots, x_n]$)

is of course (closed under sums and mult) a subalg of R and since $k[x_1', \dots, x_{n-1}', x_n]/I$ fg as an S module (this is only saying smth about the set) R is fg as an S-module

$\square$

☆In his notes Buch says: "Let $f \in k[x_1, \dots, x_n]$, f is always $f = f_0 + f_1 x_n + \dots + f_d x_n^d$, $f_i \in k[x_1, \dots, x_{n-1}]$ f monic in x_n means $f_d \in K$..." For me monic is $f_d = 1$. Both make sense and my proof is consistent with my terminology.

(with proofs)

11 NULLSTELLENSATZ

(~ This is Buch's way; instead of 4.5 we do smth closer to 13.2. As we prove Nullst. as a consequence of Noether normalisation. We do not follow exactly the book but 4.5 are Nullst sections in Eis. 13.2)

So far we've been using Nullstellensatz in our Geometry discussions. Now we prove it/them (a general form) Th 4, 5, 6.

<u>Lemma 56</u> Let $R \subseteq S$ be an integral extension of domains. Then R field $\longleftrightarrow$ S field.

Proof/ $\longrightarrow$) Let $s \in S$, $s \neq 0$. Then $s^n + a_{n-1}s^{n-1} + \dots + a_1 s + a_0 = 0$ with $a_i \in R$

If $a_0 = 0$ then $s(\underbrace{s^{n-1} + a_{n-1}s^{n-2} + \dots + a_1}) = 0$ so $= 0$ since we are in a domain

So wlog $a_0 \neq 0$. Let $m = -a_0^{-1}(s^{n-1} + a_{n-1}s^{n-1} + \dots + a_1)$; $sm = -a_0^{-1}(-a_0) = 1$. So $m = s^{-1}$.

$\longleftarrow$) Let $r \in R$, $r \neq 0$. $\exists r^{-1} \in S$ we have to check it is in R. Denote r^{-1} by $1/r$

By integrality $\left(\frac{1}{r}\right)^n + a_1\left(\frac{1}{r}\right)^{n-1} + \dots + a_n = 0$ for some $a_i \in R$

$1 + a_1 r + \dots + r^n a_n = 0$ with $a_i \in R$, $1 = r(a_1 + \dots + r^{n-1}a_n)$ so $r^{-1} \in R$. □

Anders named the following theorem as Weak Nullstellensatz

<u>Theorem 57</u> Let K be any field, let R $\overset{\neq 0}{\text{(ring)}}$ be an affine k-algebra. Suppose $P \subseteq R$ is a maximal ideal. R/p has a natural k-alg structure, $\tilde{\varphi}: K \longrightarrow R/p$ ($\tilde{\varphi} = \pi \circ \varphi$ in the lang of the proof)

Then $\tilde{\varphi}: K \longrightarrow \tilde{\varphi}(K)$ is a field isom and $|R/p : \tilde{\varphi}(K)|$ finite field ext.

(Informally $K \subseteq R/p$ is a finite field extension). This lang is good since in this case k injects to R/p).

Proof/ Let $K \xrightarrow{\varphi} R \xrightarrow{\pi} R/p$ make R/p into a k-algebra. (φ is the k-algebra ring hom π is the canonical projection)

It is clear that R/p is an affine ring over k.

By Noether's normalization $\exists S \subseteq R/p$ k-subalgebra st $S \overset{(k\text{-alg hom})}{\cong} k[x_1, -, x_n]$ and R/p is a fg S-module. If we look at the extension $S \subseteq R/p$ is finite so integral. By the last lemma S is a field. Since $k[x_1, -, x_n]$ is not a field for $n \geq 1$, $S \cong K$ as fields but also k-algebra hom. (Note Noeth. Norm gives some abstract hom but in the case we have no variables means that S is k) Let $\theta: K \longrightarrow S$ be this isomorphism, $\theta(1) = 1$, $\theta(\lambda) = \lambda \cdot \theta(1) = \lambda \cdot 1_{R/p} = \pi(\varphi(\lambda))$ the map that R/p into a k-alg is $\pi(\varphi(\cdot))$

Thus $k \xrightarrow{\varphi} \varphi(k) \subseteq R \xrightarrow{\pi} S$ is a field hom.

Now the fact that R/p is fg as an S-module it means that $S \subseteq R/p$ is a finite field ext (real sense) □

(Note $S = \{\lambda \cdot 1_{R/p} : \lambda \in K\}$ and the natural $\lambda \to \lambda_{R/p}$ is a field hom).

<u>Corollary 58</u> Suppose $k = \bar{k}$, $I \subseteq S = k[x_1, -, x_n]$ ideal. Then

$$\Psi: Z(I) \subseteq \mathbb{A}^n = K^n \longrightarrow \text{Spec-m}(S/I)$$

$$(a_1, -, a_n) \longmapsto \langle x_1 - a_1, -, x_n - a_n \rangle / I$$

is a bijection.

Proof/. **Recall**: By the caveat in corollary 6 (which of course is independent of Corollary 6 itself; which assume Nullstellensatz) $k[x_1,-,x_n]/\langle x_1-a_1,-,x_n-a_n\rangle \cong k$ so $\langle x_1-a_1,-,x_n-a_n\rangle$ maximal and $I(\{a\}) = \langle x_1-a_1,-,x_n-a_n\rangle$.

. If $a\in Z(I)$ then $I(\{a\})\supseteq I$ (if $f\in I$, $f(a)=0$) so indeed Ψ takes $Z(I)$ to spec-m(S/I) (by correspondence thm)

. The fact that this map is 1-1 is trivial (Let G be a group $H,J\leq G$ with $H/N = J/N \to J=H$)

. We NTS it is onto: Let $P\subseteq S$ be a maximal ideal by the last theorem

$$\begin{tikzcd} k \arrow[r] & k[x_1,-,x_n] \arrow[r] \arrow[u, "S"] & S/P \\ \lambda \arrow[r, mapsto] & \lambda \arrow[r, mapsto] & \lambda+P \end{tikzcd}$$

is an isomorphism of fields and the extension $|S/P : k|<\infty$
↳ we mean $\{\lambda+P : \lambda\in k\}$.

But $k=\bar{k}$ so this index is 1 (this is by 17.24 Isaacs which I'll cover in the next section but I already mentioned it in Sec 8.4 from Lie algebra notes) Hence,

$$\begin{tikzcd} K \arrow[r, "\theta"] & S/P \\ \lambda \arrow[r, mapsto] & \lambda+P \end{tikzcd}$$

is an isomorphism of fields. Let $a_i = \varphi^{-1}(x_i+P)$. Since $\varphi(a_i)=a_i$ and this is injective $x_i-a_i\in P$. So $P\supseteq \underbrace{\langle x_1-a_1,--,x_n-a_n\rangle}_{\text{maximal}}$ so they are equal.
$\overset{\wedge}{S/P}$

This shows that Ψ is surjective [every element in spec-m(S/I) is by correspondence thm $\langle x_1-a_1,-,x_n-a_n\rangle/I$; let $f\in I$ then $f\in\langle x_1-a_1,-,x_n-a_n\rangle = I(\{a\})$ where $a=(a_1,-,a_n)$ so $f(a)=0$ hence $a\in Z(I)$]. □

Corollary 59 Let $k=\bar{k}$, $I\subsetneq k[x_1,-,x_n]$ a proper ideal. Then $Z(I)\neq\emptyset$
↳ $\mathbb{A}^n$ (just points)

Proof/ $S/I\neq 0$, thus spec-m$(S/I)\neq\emptyset$. Now apply the last result.

Theorem 60 Let k be any field, $R\neq 0$ an affine k-algebra. Let $I\subsetneq R$ be an ideal. Then
(otherwise not interesting)

$$\sqrt{I} = \bigcap_{\substack{P\subseteq R \text{ max ideal} \\ P\supseteq I}} P \quad \Big(= \bigcap_{P\in Z(I)\cap \text{Spec-m}(R)} P \Big)$$
↳ of course.

(Ander called this : Nullstellensatz)

Rmk The IS says pure.

Proof: $\subseteq$) Clear (the IS for example)

$\supseteq$) Let $f\in R\setminus\sqrt{I}$, (this means f not nilpotent in R/I) we want to see that $\exists P$ maximal, $I\subseteq P$, $f\notin I$. If we see this we are done.

Let $S = (R/I)_f$, this ring is nonzero ($\bar{1} := 1+I$. If $\frac{\bar{1}}{1}=0$ $\exists n\in\mathbb{Z}_{\geq 0}$: $f^n(1+I) = I$ if $n=0$ this $1\in I$ so $I=R$ ↯. Thus $f^n\in I$ $n>0$ ↯).

Choose $Q\subseteq S$ maximal ideal. Letting

$$\begin{tikzcd} R/I \arrow[r] & (R/I)_f = S \\ r+I \arrow[r, dash] & \frac{r+I}{1} \end{tikzcd}$$

Consider $P/I = R/I \cap Q$, ie

the preimage of Q under this ring hom (we know that it is an ideal so we write it in the form P/I by corresp)

Note $I \subseteq P$ ideal in R, $f \notin P$ $\left[\text{if so } \frac{f+I}{1} \in Q \text{ then } \frac{f+I}{1} \cdot \overset{\in S}{\frac{1+I}{f}} \in Q \text{ since it is an ideal} \right.$

We NTS $P \subseteq R$ maximal. $\left. \text{but this is } \frac{1+I}{1} = \frac{f+I}{f} \in Q \text{ so } Q = S \text{ and thus } Q \text{ not max} \right]$

For this note S inherits a k-algebra structure

$$\left(k \xrightarrow[\text{k-alg hom}]{\varphi} R \xrightarrow[\text{natural proj}]{\pi} R/I \xrightarrow{\pi'} \overset{"S}{(R/I)_f} \right) \quad \text{(call } \hat{\varphi} \text{ this comp)}$$

$$r+I \to \frac{r+I}{1}$$

S is also fg over k. (If $a_1, \dots, a_n$ generate R as a k-alg, $\bar{a}_1, \dots, \bar{a}_n$ generate R/I as a k-alg. Now the $\frac{\bar{a}_i}{1}$ generate $\{\frac{\bar{r}}{1} : \bar{r} \in R/I\}$ as a k-alg. Since our mult closed subset is $\{1, f, f^2, \dots\}$. By considering $\frac{\bar{a}_i}{1}$, $\frac{1}{f}$ we can generate S as a k-alg.)

If U is an arbitrary mult closed then we may not be able to do this so be careful

By Corollary 57 $k \xrightarrow{\hat{\varphi}} S \xrightarrow{\text{proj} = \pi''} S/Q$ injects k in S/Q and we have a finite field ext.
(field hom with the image)

$\boxed{\text{Idea of what follows " } k \overset{\text{injects}}{\subseteq} R/P \overset{\text{injects as k-alg hom}}{\subseteq} S/Q \text{ so } R/P \text{ domain, so } R/P \subseteq S/Q \text{ finite hence integral so by 56 } R/P \text{ field so } P \text{ is maximal ideal.}}$

$$\underbrace{k \subseteq R/p \subseteq S/Q}_{\text{finite}}$$

This should be enough but I will try to make sure I can explain COMPLETELY what happens here

What are we saying? k has an isomorphic copy in S/Q via

$$\begin{tikzcd} k \arrow[r, "\varphi"] \arrow[rr, bend left, "\hat{\varphi}"] & R \arrow[r, "\pi"] & R/I \arrow[r, "\pi'"] & S \arrow[r, "\pi''"] & S/Q \end{tikzcd}$$

$k \mapsto \varphi(k)$

$r \mapsto r+I \longrightarrow \frac{r+I}{1} \longrightarrow \frac{r+I}{1} + Q$

These are ring homs but since these maps are used to define the k-alg structure also k-alg homs

The isomorphic copy of k living in S/Q is $\{\frac{\varphi(k)+I}{1} + Q : k \in K\} := \underset{\text{via the map above}}{\hat{K} \cong k}$ as fields

Now consider $R/I \xrightarrow{\pi'} S \xrightarrow{\pi''} S/Q$; the kernel of this ring hom is $\{r+I : \frac{r+I}{1} \in Q\} = P/I$

Now by the 3rd and 1st iso. thus we get

$$R/P \to \frac{R/I}{P/I} \longrightarrow S/Q \quad \text{is a 1-1 ring hom} \quad ⊛$$

(k-alg too but we don't care)

$$r+P \longmapsto (r+I)+(P+I) \longmapsto \left(\frac{r+I}{1}\right) + Q$$

Also $k \xrightarrow{\varphi} R \xrightarrow[\text{natural proj}]{} R/P$ is a 1-1 ring hom by stupid rmk at the beginning of sec 10. (∗∗)

If we now take k to S/Q via (*)(**). We get that our image is $\left\{\frac{\varphi(k)+I}{1}+Q : k\in k\right\}=\hat{k}$

Therefore R/p has an isomorphic copy in S/Q which contains $\hat{k}$.
(as rings; maybe more but we do not care)

So $\overset{\substack{k\\ \wr\wr}}{\hat{k}} \subseteq \overset{\substack{R/p\\ \wr\wr}}{\widehat{R/p}} \subseteq S/Q$ field; it is immediate that $\widehat{R/p}$ domain so R/p domain (isom rings)

S/Q is a finite dim vspace over $\hat{k}$; S/Q is a module over $\widehat{R/p}$ in a natural manner and since S/Q is fg as a $\hat{k}$ vspace it will clearly be gen by finitely many elnts as a $\widehat{R/p}$ module (use the same gen.; $\hat{k}\subseteq\widehat{R/p}$)
by lemma 43 the extension is integral so by lemma 56 $\widehat{R/p}$ field so R/p field
and therefore P is maximal □

□

Corollary 61 Let $k=\bar{k}$, $I\subseteq k[x_1,\dots,x_n]$ an ideal. Then $\sqrt{I}=I(Z(I))$

Proof/ Claim $I(Z(I))=\bigcap_{\substack{P \text{ maximal}\\ P\supseteq I}} P$

⊆) Let $f\in I(Z(I))$ then $f(a)=0$ $\forall a\in Z(I)$, thus $f\in I(\{a\})=\langle x_1-a_1,\dots,x_n-a_n\rangle$
by C.58 $f\in\bigcap_{\substack{P \max\\ P\supseteq I}} P$.

⊇) Let $f\in\bigcap_{\substack{P \max\\ P\supseteq I}} P$. Let $a\in Z(I)$, consider $P=\langle x_1-a_1,\dots,x_n-a_n\rangle\supseteq I$ maximal (by C58)

$f\in P$ so $f\in I(\{a\})$ hence $f(a)=0$. Therefore $f(a)=0$ $\forall a\in Z(I)$ so $f\in I(Z(I))$ //

Now if $I=0$ the result is trivial. If $I\neq 0$, the claim and thm 60 give the result. □

Observation i) In section 2 we assumed 61 (thm 4; note that the second part gave that the follows immediately: $X=Z(\sqrt{J})\xrightarrow[\text{take } I(\cdot\cdot)]{}\sqrt{J}\xrightarrow[\text{take } Z]{}Z(\sqrt{J})=X$; $\sqrt{J}\xrightarrow[\text{take } Z]{}Z(\sqrt{J})\xrightarrow[\text{take } I]{}\sqrt{J}$)
and then we proved 5, 6 as consequences. Here the order is different but everything is clear now.
(Now all we've done as a conseq. of Nullstellensatz is proved; for example in motivation of sec 6 the ☐ part is very important)

ii) I have seen people calling Nullst. to any of [57, 61], but the most common is 61.

Some consequences of this : (here k is any field ; until next title)

Remark Weak Nullstellensatz can be reformulated to : k-algebra, k field is a k vs.

Let $R^{\neq 0}$ be an affine domain over k , R field $\longleftrightarrow$ $\dim_k(R) < \infty$.

$\rightarrow$) 0 is a maximal ideal so $\varphi : k \to R$ injects k in k as a field and $|R : k \cdot 1|$ is finite ($\varphi(k)$)

So we are done .

$\leftarrow$) $k \cdot 1 \subseteq R$ finite ext of domains so integral and we are done by L56 .

Now some actual corollaries (these follows concepts from sec 7)

Corollary 62 Let R be an affine k-algebra . Then spec-m (R) is dense in spec (R) (Zariski top ; sec7)

Proof/ We have to see that its closure in spec (R) is spec (R) . For this let us consider a closed set containing it . Let $Z(I) \supseteq$ spec-m (R) . $I \subseteq \bigcap_{\substack{P \subseteq R \\ \max}} P = \sqrt{0} = \bigcap_{P \in \mathrm{spec}(R)} P$. So $I \subseteq P \ \forall \ P \in \mathrm{Spec}(R)$

($I \subseteq R$ ideal .) Nullst (thm 60) Cor 15

So $Z(I) = \mathrm{spec}(R)$ ☐

Corollary 63 Let R be an affine k-algebra . Let $U \subseteq \mathrm{Spec}(R)$ open , $P \in \mathrm{Spec}(R)$. Then $P \in U$ iff $Z(P) \cap U$ contains a closed point in spec (R) .

Proof/ Recall that a point is closed in spec (R) iff it is a maximal ideal .

We proved in sec 7 that $P \in U$ iff $\exists Q \in$ spec-m(R) : $Q \supseteq P$, $Q \in U$ (using C62)

NTS : $\exists Q \in$ spec-m(R) : $P \subseteq Q \in U$ iff $Z(P) \cap U$ contains a maximal ideal ; immediate ☐

Some Geometry discussion (If there is something that goes beyond what we know I will put { as a sign)

Let us fix $k = \bar{k}$ field .

Of course $\mathbb{A}^n = k^n \longleftrightarrow$ spec-m ($k[x_1, \dots, x_n]$) bij

$(a_1, \dots, a_n) \longmapsto \langle x_1 - a_1, \dots, x_n - a_n \rangle = I(\{a\})$

If $X \subseteq \mathbb{A}^n$ alg set $X \longleftrightarrow$ spec-m (A(X)) bij

$a \longmapsto I(\{a\}) / I(X)$

With this in mind let us start from scratch . Let A be any reduced affine k-algebra

- As we've seen sometimes in this course, after doing proper math , we play a bit with examples in which some "undefi" things appear . Even in these extra discussions 90 % is rigorous and I stress what sentences I shouldn't be worried if I do not fully get now . But these discussions are very instructive !!

We might not say things in the most standard way , but instructive .

Let $f \in A$ define (abuse of notation) $f : \text{Spec-m}(A) \longrightarrow K$ as follows,

$$\begin{tikzcd} P \arrow[r] \arrow[d] & f(P) \\ k \arrow[r, "k\text{-alg}"'] & A \arrow[r, "\text{proj}"'] & A/P \end{tikzcd}$$

$f(P)$, the unique $k \in K$ st $f - \underbrace{k \cdot 1}_{k \text{ seen in } A} \in P$: Preimage of $f+P$ under the map

by weak NNS and the fact that k alg closed field case. (this result is stated at the beginning of next section)

So far nothing depends on A being reduced, but if so

{ **Claim** Spec-m(A) "is an algebraic set" with coordinate ring A. (A affine reduce k-alg)

"**Proof**": ↳ What does he mean? There is a more general concept called variety that should be learnt in alg geo. (Potentially I will write notes following Gathmann and it will be there) ut since this can be seen as an extra discussion let us try to see what happens; for fun

Certainly,

$A \cong k[x_1, \dots, x_n]/I$ as k-algebras. I radical since A is reduced (obvious)

$Z(I) \subseteq \mathbb{A}^n \longleftrightarrow \text{spec-m}(A)$ is a bijection & $k[x_1, \dots, x_n]/I(Z(I)) \underset{\text{nullst + reduced}}{=} k[x_1, \dots, x_n]/I \cong A$

$\left(a \underset{\text{Cor 5.8}}{\longmapsto} I(\{a\})/I \underset{\text{the bijection above}}{\longrightarrow} \text{max ideal in } A \right)$

But how do we want this bijection to be? He said: { Homeomorphism + regular function in $Z(I)$ composed with the map, gives reg function on spec-m(A)

A GLIMPSE OF REGULAR FUNCTIONS (this is legit math)

Let A be a reduced affine k-algebra, $k = \bar{k}$. Let $X = \text{Spec-m}(A)$ with the induced Zariski topology.

DEF Let $U \subseteq X$ open. $f : U \longrightarrow k$ a function. We say that f is a regular function if f is locally rational : $\forall x \in U$, $\exists\, x \in U' \subseteq U$ open and $p, q \in A$: $\forall y \in U'$, $q(y) \neq 0$, $f(y) = \frac{p(y)}{q(y)}$ $(= p(y)\, q(y)^{-1})$.

Note $y \in \text{Spec-m}(A)$, $p, q \in A$ so $p(y), q(y)$ are defined as above.

Remark If $A = k[x_1, \dots, x_n]$, $\mathbb{A}^n \xrightarrow{\Psi} \text{Spec-m}(A)$

$(a_1, \dots, a_n) \longmapsto \langle x_1 - a_1, \dots, x_n - a_n \rangle$

Homeomorphism. Bij: ✓. Let $Z(I) \subseteq \mathbb{A}^n$ zariski closed. $\Psi(Z(I)) = \{$ max ideals corresp to points in $Z(I) \}$

Consider $I \subseteq A$ as an ideal $Z(I) = \{P \in \operatorname{Spec}(A) : I \subseteq P\}$

claim $Z(I) \cap \operatorname{Spec-m}(A) = \Psi(Z(I))$

$\subseteq$) Let $\langle x_1-a_1, \dots, x_n-a_n\rangle \in Z(I)$ then if $f \in I$, since $\langle x_1-a_1, \dots, x_n-a_n\rangle \supseteq I$ $f \in I \subseteq I(\{a\})$ so $f(a)=0$ hence $a \in Z(I)$ so $\langle x_1-a_1, \dots, x_n-a_n\rangle \in \Psi(Z(I))$

$\supseteq$) Consider $\langle x_1-a_1, \dots, x_n-a_n\rangle$ where $a=(a_1, \dots, a_n) \in Z(I)$. This ideal contains I ($f \in I$ then $f(a)=0$ so $f \in I(\{a\})$.) and is maximal.

So Image of closed is closed. Now if C closed in the codomain, $C = \operatorname{spec-m}(A) \cap Z(I)$ for some ideal $I \subseteq A$. By the claim above, its preimage is $Z(I)$.

Now take $U \subseteq \operatorname{Spec-m}(A)$ open and $f: U \to K$ regular function

Let $\tilde{U} = \Psi^{-1}(U)$; we get $\tilde{U} \xrightarrow{\Psi} U \xrightarrow{f} K$ and $\forall a \in \tilde{U}, \exists\, a \in V \subseteq \tilde{U}$ open

and $\underset{k[x_1, \dots, x_n]}{p, q \in A}$: $\forall y \in V$, $f(\Psi(y)) = \dfrac{p(\langle x_1-y_1, \dots, x_n-y_n\rangle)}{q(\langle x_1-y_1, \dots, x_n-y_n\rangle)} = \dfrac{p(y_1, \dots, y_n)}{q(y_1, \dots, y_n)} \neq 0$.

notation from beginning of last page.

by def this is the unique $\lambda \in k$ st $p(x_1, \dots x_n) - \lambda \in \langle x_1-y_1, \dots x_n-y_n\rangle$ Which is $p(y_1, \dots y_n)$

Similarly if $A = k[x_1, \dots x_n]/I$, with I radical then

$$\begin{tikzcd} Z(I) \arrow[r, leftrightarrow, "\Psi"] & \operatorname{spec-m}(A) \\ a \arrow[r, mapsto] & \langle x_1-a_1, \dots, x_n-a_n\rangle/I \end{tikzcd}$$

is a homeomorphism, same argument.

Now as above $U \subseteq \operatorname{Spec-m}(A)$ open and $f: U \to K$ regular function

Let $\tilde{U} = \Psi^{-1}(U)$; we get $\tilde{U} \xrightarrow{\Psi} U \xrightarrow{f} K$ and $\forall a \in \tilde{U}, \exists\, a \in V \subseteq \tilde{U}$ open

and $p, q \in A = k[x_1, \dots, x_n]/I$, then $\forall y \in V$, $f(\psi(y)) = \dfrac{p(\langle x_1-y_1, \dots, x_n-y_n\rangle/I)}{q(\langle x_1-y_1, \dots, x_n-y_n\rangle/I)} = \dfrac{p(y_1, \dots y_n)}{q(y_1, \dots, y_n)} \neq 0$

($p \in A$ so $p = \underset{\in k[x_1, \dots x_n]}{p(x_1, \dots, x_n)} + I$ similarly for g.)

By def, the unique $\lambda \in k$ st $(g(x_1, \dots, x_n) + I) - k + I \in \langle x_1-y_1, \dots x_n-y_n\rangle/I$

$$\left(k \longrightarrow k[x_1, \dots x_n]/I \longrightarrow \frac{k[x_1, \dots, x_n]/I}{\langle x_1-a_1, \dots, x_n-a_n\rangle/I} \right)$$

Picture of the beginning of last page but for this case

$\lambda = g(y_1, \dots y_n)$ satisfies it since $g(x_1, \dots x_n) - g(y_1, \dots, y_n)$ vanishes at y.

$\downarrow$ $g(x_1, \dots x_n) \in k[x_1, \dots, x_n]$

So by uniqueness we are done.

This should be taken as a stupid remark:

Let $f \in A(X) = k[x_1, \dots, x_n]/I(X)$ alg set.

then $f(b)$ is completely determined for $b \in X$.

OF COURSE! and by a poly (or many) in $k[x_1, \dots x_n]$

So all in all this is a more general perspective of what one would define as a rational function of an alg set. (see def 3.1 Gathmann 2014). It becomes very obvious

Def $\mathcal{O}_X(U) = \{f: U \to k \text{ regular}\}$; $\mathcal{O}_X$ is called structure sheaf.

Buch mentioned that a manifold is determined up to diffeom. by its C^∞ functions. So this is more a less analogue.

Why care about this? "Keep track of the structure of alg variety ≡ keep track of its reg. func"

If $f \in \mathcal{O}_X(U)$ we denote $U_f = \{x \in U : f(x) \neq 0\}$

Example $A = \mathbb{C}[x,y,z,w]/\langle xy - zw \rangle$

Let $X = \text{spec-m}(A)$, in bijection to $Z(xy - zw) \subseteq \mathbb{A}^4$. Let $U = X_y \cup X_w \subseteq X$ open. Let $f : U \longrightarrow k$ given by $\frac{x}{w}$ on X_w and $\frac{z}{y}$ on X_y. $f \in \mathcal{O}_X(U)$

Exercise; $\nexists\, p, q \in A : f(x) = \frac{p(x)}{q(x)}$ $\forall x \in U$,

Fact (Exercise 2). In general $\mathcal{O}_X(X) = A$ (from nulls). (of course, from above (elements in A define functions))

I did these two exercises in office hours with him. I'll try to upload pictures

We continue in the claim; recall $A \cong k[x_1, \dots, x_n]/I$ as k-algebras. Look at

$$Z(I) \subseteq \mathbb{A}^n \longleftrightarrow \text{spec-m}(k[x_1,\dots,x_n]/I)$$, bijection clear, and $A(Z(I)) = \frac{k[x_1,\dots,x_n]}{I}$

$$(a \longmapsto \frac{\langle x_1 - a_1, \dots, x_n - a_n \rangle}{I}$$

Cor 5.8

It should now be clear that this is a homeomorphism; discussed in the remark. in the remark. Moreover we've seen in the remark that if we start with a rational function on U open set of $\text{spec-m}(k[x_1,\dots,x_n]/I)$ the composition with $Z(I) \to \text{spec-m}(\frac{k[x_1,\dots,x_n]}{I})$ yields a rational function on an open subset of $Z(I)$. This is the path I explore for now, for more conclussions see video "spec-m is alg set"

END of claim

Let A, B be reduced affine k-algebras, $\varphi : A \longrightarrow B$ k-algebra hom $\varphi(k) = k$ $\forall k \in K$ (we have already clear that $k \subseteq A$; $k \cdot 1_A$ / $k \subseteq B$; $k \cdot 1_B$)

If $Q \subseteq B$ is maximal, then $Q \cap A := \varphi^{-1}(Q)$ is maximal ideal (he said that still true if not alg closed. But we don't in $k = \bar{k}$)

Pf/ The preimage (ring hom) of a prime ideal is prime so $\varphi^{-1}(Q)$ prime (not A; otherwise $1 \in Q$)

$A/\varphi^{-1}(Q)$ is a fg k-algebra so k injects naturally also there is a natural injection k-alg hom (k-alg hom)

$A/\varphi^{-1}(Q) \hookrightarrow B/Q$ sends $k + \varphi^{-1}(Q) \mapsto k + Q$ since $\varphi(k) = k$. But k also injects to B/Q (k-alg hom too). and it is a finite field ext; since k alg closed

this injection is an iso. This forces $A/\varphi^{-1}(Q)$ to be a field (isom canonically to k) so $\varphi^{-1}(Q)$ max.

After the above this should be enough.

This gives $\tilde{\varphi} : \text{Spec-m}(B) \longrightarrow \text{spec-m}(A)$ (no reduced needed)

$Q \longmapsto \varphi^{-1}(Q) \equiv A \cap Q$

Assume $A = k[x_1, \dots, x_n]/I$, $B = k[y_1, \dots, y_m]/J$, $\varphi(\bar{x}_i) = f_i(y_1, \dots, y_m) + J$, $f_i \in k[y_1, \dots, y_m]$ (of course it has to be like this without thinking; the elements on the RHS one of that form. Maybe not unique f_i.)

(reasonable assumption :))

This gives $\hat{\varphi} : \mathbb{A}^m \longrightarrow \mathbb{A}^n$
$b \longmapsto (f_1(b), \ldots, f_n(b))$) ; $\hat{\varphi}(Z(J)) \subseteq Z(I)$

Pf/ let $b \in Z(J)$, $h \in I$. Then $h(\hat{\varphi}(b)) = h(f_1(b), \ldots, f_n(b))$
$= \varphi(\bar{h})(b) = 0$

↓ read in opposite direction + stupid obs

↘ $h \in I$ so $\bar{h} = 0$ in A so $\varphi(\bar{h}) = 0$ in B so $\varphi(\bar{h}) \in J$ and $b \in Z(J)$.

And its an exercise to verify (easy).

$$\begin{tikzcd}
Z(J) \arrow[r, "\hat{\varphi}"] \arrow[d, leftrightarrow] & Z(I) \arrow[d, leftrightarrow] \\
\text{spec-m}(B) \arrow[r, "\tilde{\varphi}"'] & \text{spec-m}(A)
\end{tikzcd}$$

commutes

⟶ these are the bijections as in the claim, of course. (that is why we ask A, B to be reduced)

12. PRIMES IN AN INTEGRAL EXTENSION

Proposition 64 (Going up) Let $R \subseteq S$ be an integral ext. of rings. Let $P \subseteq R$ be a prime ideal $J \subseteq S$ an ideal such that $R \cap J \subseteq P$. Then $\exists Q \subseteq S$ prime st $R \cap Q = P$ and $J \subseteq Q$

$$\begin{tikzcd}
R \arrow[r] & S \\
P = Q\cap R \arrow[u] \arrow[r] & \exists Q \arrow[u, phantom, "\text{UI}"] \\
R\cap J \arrow[u] \arrow[r] & J \arrow[u, phantom, "\text{UI}"]
\end{tikzcd}$$

the direction of the arrows means contained and we forget the usual group theory rules for diagrams.

Proof/ STEP 1 WMA $J = 0$

the primes of the quotient are the quotient of primes

Assume this is proved for $J = 0$. Now we want to prove the theorem, if we consider $R/_{J\cap R}$, $S/_J$ we have that $R/_{J\cap R} \subseteq S/_J$ is integral of course and $P/_{J\cap R}$ is prime $\subseteq R/_{J\cap R}$ by the case 0, $\exists\, Q/_J$ prime st $R/_{J\cap R} \cap Q/_J = P/_{J\cap R}$.

so this Q is the desired Q (easy)

$$\begin{tikzcd}
R/_{J\cap R} \arrow[r] & S/_J \\
r + J\cap R \arrow[r, mapsto] & r + J
\end{tikzcd}$$

- is 1-1 : $r_1 + J = r_2 + J$ means $r_1 - r_2 \in J$ so $r_1 - r_2 \in R \cap J$ so $r_1 + R\cap J = r_2 + R\cap J$
- ring hom ✓.

So we really mean the image of this map ; same for $P/_{J\cap R}$ since $P \subseteq R$.

So NTS : $R \subseteq S$ integral ring ext, $P \subseteq R$ prime then $\exists\, Q \subseteq S$ prime st $R \cap Q = P$.

STEP 2 WMA R is local with P unique prime

Assume we prove it for the small ring local.

Then if not take $(R \setminus P)^{-1} R \subseteq (R\setminus P)^{-1} S$ (wrong II)

The first ring R_P local with $(R\setminus P)^{-1} P$ max so $\exists$ an ideal Σ in $(R\setminus P)^{-1} S$ prime st $R_P \cap \Sigma = P_P$

$$\begin{tikzcd}
 & \frac{r}{u} \arrow[r, mapsto] & \frac{r}{u} & \\
\frac{r}{1} & R_p \arrow[r, "\iota_{(R\setminus P)}"'] & (R\setminus P)S & s/1 \\
r \arrow[u, mapsto] & R \arrow[u] \arrow[r, "i"] & S \arrow[u] & s \arrow[u, mapsto]
\end{tikzcd}$$

By sec 4, $\iota_{R\setminus P}$ is 1-1 ring hom. Diagram commutes

Let Q be the preimage of Σ (is prime; preimage of prime ideal by ring hom is prime)

Now $R\cap Q$ is the preimage of Σ by ↲ in the diagram. Since the diagram commutes it coincides with the preimage by ⬐. But this is the first pull back is P_p; and the second P. So $P = R\cap Q$.

So NTS that if $R\subseteq S$ with R local $P\subseteq R$ max ideal then $\exists Q\in S$ prime st $R\cap Q = P$.

STEP 3 $PS \subsetneq S$.

If $PS = S$ then $1 = p_1s_1+\dots+p_ns_n$ $p_i\in P$, $s_i\in S$. Let $S' = R[s_1,\dots,s_n]$ finite over R and $PS' = S'$

so by NAK, $S' = 0$ ↯.

Finally just take $Q\subseteq S$ maximal $PS\subseteq Q$; step 3 tells us it exists (and the existence of max ideals containing a proper ideal)

Note $P\subseteq Q\cap R\subsetneq R$. But R local so $Q\cap R = P$ □

(if $R\subseteq Q$ then $1\in Q$ so $Q = S$ since it is ideal)

NOTE POWER OF LOC By localizing at (the complement of) a prime we get a local ring. For local rings we can prove the result easily. Without localization [which reduces the problem (since it has nice properties; exact ...)] I do not know how one could prove such result.

Lemma 6.5 Let $R\subseteq S$ be domains, not nec integral. Suppose $K(R)\subseteq K(S)$ is an algebraic extension of fields. If $0\neq J\subseteq S$ ideal then $J\cap R\neq 0$.

Remarks i) $K(R) = (R\setminus\{0\})^{-1}R$, $k(S) = (S\setminus\{0\})^{-1}S$.

ii) $K(R)$ injects naturally in $k(S)$; so we are considering that injection

$K(R) \longrightarrow k(S)$

$r_0/r_1 \longmapsto r_0/r_1$ in $k(S)$ may have more reps

1-1: if $\frac{r_0}{r_1} = \frac{r_2}{r_3}$ in $k(S)$ $\exists s\in S\setminus\{0\}$ such that $s(r_3r_0 - r_1r_2) = 0$. Since S domain $\frac{r_0}{r_1} = \frac{r_2}{r_3}$ in R.

iii) $K(R)\subseteq K(S)$ alg field ext is weaker notion than $R\subseteq S$ integral.

- If $R\subseteq S$ int, $k(R)\subseteq k(S)$ alg is easy
- $\mathbb{Z}\subseteq\mathbb{Q}$ not integral but $k(\mathbb{Z})\cong\mathbb{Q}\cong k(\mathbb{Q})$.

Proof/ Let $0\neq x\in J$. Let $\left(\frac{x}{1}\right)^n + \frac{a_1}{b_1}\left(\frac{x}{1}\right)^{n-1}+\dots+\frac{a_n}{b_n} = 0$ with $a_i, b_i\in R$

Let $y = b_1\cdots b_n x\in J$ then since $\frac{b_1\cdots b_n x^n}{1} + \frac{a_1 b_2\cdots b_n x^{n-1}}{1}+\dots+\frac{a_n b_1\cdots b_{n-1}}{2} = 0$

So since we are in a domain we can cancel the one and by multiplying by b_1^n, then $b_2^{n'}$ and so on we get $y^n + a_1' y^{n-1} + \dots + a_n' = 0$ for $a_i' \in R$ WLOG $a_n' \neq 0$. From then $a_n' \in \langle y \rangle \subseteq J$ so $a_n' \in R \cap J \setminus \{0\}$. (if not factor, we are in a domain until getting what we need) □

Remark i) From here one can also derive L56 ($R \subseteq S$ integral ext, R field $\leftrightarrow$ S field)

ii) STUPID REMINDER: $\varphi : R \to S$ ring hom, $P \subseteq S$ prime, $\varphi^{-1}(P)$ prime ideal

(maybe I've used it 10 times but since I will use it more I put it here.

iii) STUPID TAKE into account: The maximal ideals over an ideal $\equiv$ max ideals over its radical.

$\{$ Let $M \supseteq I$ max, then $\sqrt{I} \subseteq \sqrt{M} = M$, maximal)

Let $\sqrt{I} \subset M$ max then $I \subseteq \sqrt{I} \subseteq M$. □

same with primes; same proof.

The next corollary is important in dimension theory.

Corollary 66 (Incomparability) Let $R \subseteq S$ be an integral ext of rings. Then

i) Let $Q \subseteq S$ prime. Then $Q \subseteq S$ maximal iff $R \cap Q \subseteq R$ maximal

ii) Let $Q_1 \subsetneq Q \subseteq S$ primes, then $Q_1 \cap R \subsetneq Q \cap R$. (I think only need Q_1 prime; from proof + Stack exch.)

Proof/ i)
$$\begin{tikzcd} R \arrow[r, "i"] & S \\ r \arrow[r, mapsto] & r \end{tikzcd}$$
; Q is prime so the preimage $R \cap Q$ is prime by stupid reminder.

Now $R/_{R \cap Q}$ is a domain. Let
$$\begin{tikzcd} R/_{R\cap Q} \arrow[r] & S/_Q \\ r + R\cap Q \arrow[r, mapsto] & r + Q \end{tikzcd}$$
this is a 1-1 ring hom

and the image $\{r+Q : r \in R\}$ is isom to $R/_{R \cap Q}$. Note $S/_Q \supseteq \{r+Q : r \in R\}$ is an integral ext of domains. Now Q max iff S/Q field iff $R/_{R\cap Q}$ field iff $R \cap Q$ maximal.

ii) STEP 1: WMA $Q_1 = 0$, and R, S domains

If we prove it in this case; let us see what happens in general

Consider $R/_{R\cap Q_1} \overset{\text{int of dom}}{\subseteq} S/_{Q_1}$ (with the map above; isom copy inside $\{r + Q_1 : r \in R\}$.)

$Q/_{Q_1}$ is a proper prime in $S/_{Q_1}$. By the assumed case $Q/_{Q_1} \cap \{r+Q_1 : r \in R\}$ is proper in $S/_{Q_1}$. Hence $R \cap Q \supsetneq R \cap Q_1$.

We NTS $Q \subseteq S$ proper prime then $Q \cap R \neq 0$; this is just the lemma (and remark iii) □

The next corollary applies this to obtain a (rigorous and clear) result related to the geom. disc.

Corollary 65 Let A, B be affine k-algebras ($k = \bar{k}$). Let $f : A \longrightarrow B$ be a k-alg hom $\varphi(1) = 1$, suppose B is integral over A (B is an A-alg). Then $\tilde{f} : \text{spec-m}(B) \longrightarrow \text{spec-m}(A)$ is a closed map

(Exha?).

Rmk Anders said it could be done without $k=\bar{k}$ (but in the Geom. discussion we justified the existence of $\hat{f}$ with $k=\bar{k}$ so we stick to it. VIDEO (Prueba mia I)

Proof/ Let $I=\ker f$, B contains a isomorphic (as k-alg) copy of A/I

$$\left(\begin{array}{ll} \underline{f}: A/I \longrightarrow B & \text{we will denote } A/I \text{ to } \underline{f}(A/I) \\ \quad a+\ker f \mapsto \varphi(a) & \\ \text{is a 1-1 k-alg hom} & \end{array}\right)$$

- Rutinary obs: B is integral over A/I. Therefore $A/I \subseteq B$ is an integral extension.
- Other obs, spec-m$(A/I) = \{P/I : P \in \text{spec-m}(A),\ P \supseteq I\}$ (easy concept th...)

  and if we do

$$\begin{tikzcd} \text{spec-m}(A/I) \arrow[r] & \text{spec-m}(A) \\ P/I \arrow[r, mapsto] & P \end{tikzcd}$$

  is closed easily.
- Also spec-m$(A/I) = \{P/I = \underline{f}(P/I) : P/I \in \text{spec-m}(A/I)\}$ and since the rings are iso

$$\begin{tikzcd} \text{spec-m}(A/I) \arrow[r] & \text{spec-m}(A/I) \\ P/I & P/I \end{tikzcd}$$

  is also closed.

Now let $P/I \in \text{spec-m}(A/I)$, by Going up, $\exists Q_0 \in \text{spec}(B)$: $Q_0 \cap A/I = P/I$

Therefore by taking $Q \in \text{Spec-m}(B)$, $Q_0 \subseteq Q$, $Q \cap A/I = P/I$: [$\underset{\text{easy}}{Q\cap A/I}$ is an ideal in A/I if it is A/I then $Q \ni 1_S$ (A/I subring) so it is proper. Clearly contains P/I so it is all clear.]

Thus,

$$\begin{tikzcd} \text{spec-m}(B) \arrow[r, "\underline{f}"] & \text{spec-m}(A/I) \\ Q \arrow[r, mapsto] & Q \cap A/I \end{tikzcd}$$

- is surjective (by what we said above);
- well def? $Q \cap A/I$ is a prime ideal (easy). Maximal by incomparability
- Is it closed?

Let $L \subseteq B$ ideal. Consider $C = Z(L) \cap \text{Spec-m}(B)$ a closed subset of spec-m(B); all look like this. Consider $\tilde{I} = \bigcap_{P\in C} P$. It is clear that it is prime and the maximal ideals over it are exactly those in C ($L \subseteq \tilde{I}$). So WHA L is prime. Consider $L \cap A/I$. We want to argue that the maximal ideals in A/I that contain it are exactly $\underline{f}(C)$. By incomparability they contain it. For facilitate notation call $B \to S$, $A/I \to R$ integral ext.

Suppose that $P \cap R$ maximal in R containing $L \cap R$.

$$\begin{tikzcd} R/L\cap R \arrow[r, hook] & S/L \\ r + L\cap R \arrow[r, mapsto] & r + L \end{tikzcd}$$

1-1 ring hom, since $R \subseteq S$ integral, this too. Call $R/L\cap R$, $P\cap R/L\cap R$ the images. By Going up $\exists\, Q/L$ prime in S/L such that $Q/L \cap R/L\cap R = \frac{P\cap R}{L\cap R}$

Note Q prime in S, $Q \supseteq L$, $Q \cap R = P \cap R$.

$\{q+L : q \in Q\} \cap \{r+L : r \in R\} = \{p+L : p \in P \cap R\}$

$\supseteq$). Let $p \in P \cap R$, then $\exists\, q \in Q, r \in R$: $q+L = r+L = p+L$

this means $p-q \in L$ so $p \in L+q \subseteq Q$ so $p \in Q$ and R so $p \in Q \cap R$.

$\subseteq$). $P \cap R$ maximal in R, if $Q \cap R \supsetneq P \cap R$ it is R and thus $Q \ni 1$. $\int$.

Coming back to the previous language $\exists\, Q$ prime in B st $Q \cap A/_I = P \cap A/_I$ $Q \supseteq L$. By incomparability it follows that Q maximal $\supseteq L$. So $P \cap A/_I \in \xi(C)$.

Now $\text{spec-m}(B) \xrightarrow{\xi} \text{spec-m}(A/I) \rightarrow \text{spec-m}(A/I) \rightarrow \text{spec-m}(A)$

is closed and by construction it is $\tilde{f}$.

Anders confirmed that the idea is correct; so perhaps I was very careful but the proof should be fine ✓.

A . SOME FIELD THEORY (AND GALOIS)

Now Anders' goal is proving the finiteness of integral closure. Before doing so he spent a bit of time reviewing Field / Galois thy. I take this as an opportunity to do something I've been wanting to do for a while.

Gabriel's course was good but he did not mention separability, and he skipped some things that are usually covered (finite fields, Cyclotomic ext ....). My goal in this section is to try to (assuming known Ecal's content) say what we did until sec 2 included) of part 2 with the generality that is usually provided. The end of sec 2 part 2 matches perfectly with the end of ch 18 from Isaacs. So the goal is not to cover 17, 18 Isaacs from scratch but to try to state what I already proved in the usual generality, so I will not care much about proofs since they could be done similarly.

(and add what's in there that Gabriel ignored)

Remark about notation: • Shortly after defining R-algebra we introduced the notation (if S is an R-alg) $R[a_1, \dots, a_n]$ $a_i \in S$. These notation was convenient since the elmts here are polys in $R[x_1, \dots, x_n]$ with variables substituted.

(R-alg gen by a_i) → If $R \subseteq S$ this is just the smallest ring containing R, a_i.

• In Ecal we proved that if $k \subseteq L$ is a field ext, $\alpha \in L$. Then $k(\alpha)$ the smallest subfield of L containing K and α is $= \{ f(\alpha) g(\alpha)^{-1} : f, g \in k[x], g(\alpha) \neq 0 \}$. This can be thought as rational

(if α algebraic, just polys)

functions (fraction field / loc of $k[x]$) st the denominator does not vannish in α, evaluated in α (this would formaly give elmts in some localization of L, which is identified with L (of course).

at a set not having 0

[All in all, we think of [ ] as substitute in polys, ( ) as substitute in rational functions].

ring gen by

field generated by

in this course but I think is quite general.

• Let $k \subseteq L$ be a field extension, $\alpha \in L$ algebraic over k. Then it is clear (proof of fin elmt is alg) that

$$k[x] / \langle \mathrm{Irr}(\alpha, k, x) \rangle \cong k(\alpha)$$

fields

• Here it is used that $k[x]$ is a PID, and $\mathrm{Irr}(\alpha, k, x)$ is the minimal polynomial of α over $k[x]$; unique monic irreducible poly vanishing at α.

Recall that a field L is algebraically closed if $\forall f \in L[x] \setminus \{0\}$, f splits in L. Also recall (mentioned in Ch 2 we alg) that if $L \supseteq k$ is a field extension, L is an algebraic closure of K if

- $L \supseteq k$ algebraic
- $f \in k[x] \setminus \{0\}$ splits over L.

<u>Lemma</u> (Isaacs 17.24) Let $k \subseteq L$ be an alg field ext. TFAE

i) L alg closed

ii) L alg closure of K

iii) $\nexists$ $F \supsetneq L$ field with F alg over k

iv) $\nexists$ $F \supsetneq L$ field with F alg over L.

As a consequence (Cor 17.25 Isaacs) If $k \subseteq L$ alg closed, $E = \{\alpha \in L : \alpha \text{ alg over } k\}$ is the unique algebraic closure of k in L. ($\mathbb{C}$ alg closed, Alg numbers is an alg closure of $\mathbb{Q}$ so alg closed)

(When we say $k = \bar{k}$ we mean k alg closed; of course)

<u>Theorem (17.27, 17.30 Isaacs)</u> Let k be any field. There exist $E \supseteq k$ an algebraic closure for k (might be instructive to look at the construct.) If $\varphi : F_1 \to F_2$ is a field isom, $E_i \supseteq F_i$ alg closure then φ extends to an isom of E_i. Therefore if k any field, $E_1, E_2 \supseteq k$ two alg closures then E_i are k-isom ($\exists$ field isom $\varphi : E_1 \to E_2$ fixing k)

We denote (unique up to k-isom) $\bar{k}$ the algebraic closure of k.

- Let F be any field, $f \in F[x]$ of degree n is said to be separable if f has n different roots over any $E \supseteq F$ st f splits over E.

<u>Lemma (18.7 Isaacs)</u> Let $f \in F[x] \setminus \{0\}$. TFAE
i) f is separable
ii) If $K \supseteq F$, $\alpha \in K$ then $(x-\alpha)^2 \nmid_{K[x]} f$
iii) $\exists K \supseteq F$: f has $\deg(f)$ roots in k (distinct).

(So it is also common to see the definition: $f \in F[x]$ is separable if it has distinct roots in $\bar{F}[x]$)

<u>Caution</u>: In Isaacs book this is called "f has distinct roots" and he gives another definition of separable but according to Wikipedia Isaacs def is no longer in use.

I skip some very obvious properties.

<u>DEF</u> Let $F \subseteq E$ be any field extension. $\alpha \in E$ algebraic over F is said to be separable over F if $\text{Irr}(\alpha, F, x)$ is separable. $E \supseteq F$ is called separable extension if $\forall \alpha \in E$, α sep over F.

18.12 Easy.

$F \subseteq K \subseteq E$ with E sep over F then
E sep over K and K sep over F.

See proof.

Recall $\boxed{\text{thm C}}$ from seminario 1 Ecal: $K \subseteq E$ field ext, $p \in K[x]$: $\overset{\text{(see seminar)}}{p'(x) \neq 0}$ let $a \in E$. Then

i) a multiple root iff $p(a) = p'(a) = 0$
ii) $\gcd(p(x), p'(x)) = 1 \to p$ does not have mult. roots (for more defn see seminar and ecal)
iii) If p irreducible in $k[x]$ then p has no mult roots in E

<u>Observation</u> If char $F = 0$, $\alpha \in E \supseteq F$ algebraic over F then α is separable.

Let $f(x) = \text{Irr}(\alpha, F, x) \in F[x]$ consider $f(x) = \prod_{i=1}^{n} (x - \alpha_i)$ $\alpha_i \in \bar{F}$. The leading term of this polynomial is x^n. Thus $f'(x) \in F[x] \setminus \{0\}$ since char $F = 0$. Now we can apply thm C Seminar 1 Ecal. to say that $f(x)$ has no multiple roots in any $L \supseteq F$ in part in $\bar{F}$. So $f(x)$ separable.

Thm/Def Let $E \supseteq F$ field extension (finite!) we say that it is Galois if it satisfies any of these equivalent cond

i) E is normal and separable over F

ii) $F = C_E(\mathrm{Gal}(E/F)) := \{ \lambda \in F : \sigma(\lambda) = \lambda \ \forall \sigma \in \mathrm{Gal}(E/F) \}$

iii) $|\mathrm{Gal}(E/F)| = |E : F|$. (In general, if the extension is finite we just have

iv) E is the splitting field over F of some separable poly $f(x) \in F[x]$

Comments: i) If we say char $F = 0$ then you can omit the word separable and we recover what we did in Ecal (so if we work in a base field of char 0 we forget separability)

ii) Different sources give different definitions you can start with any and recover the rest ; I will not redo it because I am quite sure that I could redo what we did in Ecal but adding separability when needed to make sense of all these equivalences. Isaacs starts with ii), D&F with iii) , Gabriel with "i)".

Now the point is that everything we say in Part 1 Ecal and Part 2 (sec 1,2 for now) which mentions char 0 (or Galois) is still true if we write separable (or keep Galois). Namely, (I essentially restate, but I write what Isaacs did so might contain a bit more; this should be the thus I take have and Ecal allows me to skip proof)
(So for the following I believe the proof but I should "prove in my head" why was this true in Ecal.)
Of course examples remain the same (in char 0 which is what we did in Ecal)

Prop (18.15) $F \subseteq K \subseteq E$ ext, E Galois over F then so is E over K. (I mention it for completeness but it follows directly from the last theorem and things did in Ecal...)

Thm Artin (18.20) $G \leq \mathrm{Aut}(E)$, E any field let $F = C_E(G)$ and assume $|G| = n < \infty$. Then

i) $|G| = |E : F|$

ii) $G = \mathrm{Gal}(E/F)$

iii) E is Galois over F

Thm Fundamental of Galois theory (18.21) Let E/F Galois $G = \mathrm{Gal}(E/F)$. Let $\mathcal{S} = \{ H \leq G \}$, $\mathcal{K} = \{ F \subseteq L \subseteq E \}$ subfields

i) $f : \mathcal{S} \longrightarrow \mathcal{K}$, $H \longmapsto C_E(H)$ $\qquad g : \mathcal{K} \longrightarrow \mathcal{S}$, $L \longmapsto \mathrm{Gal}(E/L)$ bijections inverse of each other moreover (Gal corresp)

they reverse containments $F \subseteq L \subseteq K \subseteq E$ iff $\mathrm{Gal}(E/K) \leq \mathrm{Gal}(E/L)$

ii) If $g(K) = H$ then $|E : K| = |H|$ and $|K : F| = |G : H|$ so $|E : F| = |G|$.

iii) If $g(K) = H$, $\sigma \in G$. Then $\mathrm{Gal}(E/\sigma(K)) = H^{\sigma}$. Also $H \trianglelefteq G$ iff K Galois over F

in this case $\mathrm{Gal}(K/F) \cong G/H$

One result that was mentioned as extra in Ecal

Thm Primitive element (18.17) $E \supseteq F$ finite separable. Then $E = F[\alpha]$ for some $\alpha \in E$.

Idea of proof: 1) E/F finite then $E = F[\alpha]$ iff $\exists$ finitely many subfields of F containg F. (17.11 Isaacs)

2) If $E \supseteq F$ finite sep then $\exists\, L \supseteq E$: L Galois over F. (related to Galois closures)

3) Use Galois correspondence to be able to apply 1.

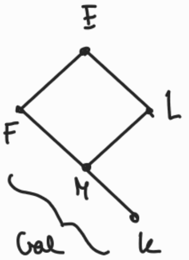
↳ Isaacs establishes the precise correspondence needed for this before FTGT so this appears before. No worries

(same)

Thm Natural Irrationalities 18.22 Suppose E/K extension, $K \subseteq L \subseteq E$ subfields and $K \subseteq F \subseteq E$

suppose $\langle L, F\rangle = E$. Let $M = F \cap L$ assume F Galois over K.

↳smallest subfield of E containg both.



Then E/L Galois and $Gal(E/L) \to Gal(F/M)$ isom of groups.

$$\sigma \longmapsto \sigma|_F$$

Also, if $|E:K| < \infty$ then $|E:F| = |L:M|$.

Moreover if $|L:K| < \infty$ then $|E:K| = \dfrac{|F:K|\,|L:K|}{|M:K|}$ (D&F 14.4 C20; obvious from the above (all)).

So far this integrates / Generalises Part 1 ecal and first 2 sections of part 2 with ch 17, 18 Isaacs.

For the rest of the section I'll cover some easy consequences of this (Isaacs, Ecal don't seem to mention) extracted from 14.4 D&F.

Proposition (Intersection and composite of Galois)

Let $F \subseteq K_1, K_2 \subseteq E$ fields st $E = \langle K_1, K_2\rangle$ and K_i/F are Galois. Then

i) M/F Galois where $M = K_1 \cap K_2$

ii) E Galois over F and $Gal(E/F) \cong H \leq Gal(K_1/F) \times Gal(K_2/F)$ where $H =$

$= \{(\sigma, \tau) : \sigma|_{K_1 \cap K_2} = \tau|_{K_1 \cap K_2}\}$

In particular if $K_1 \cap K_2 = F$, $Gal(E/F) \cong Gal(K_1/F) \times Gal(K_2/F)$

Conversely E Galois over F and $Gal(E/F) = G_1 \times G_2$ direct product of two subgroups then $E = \langle K_1, K_2\rangle$, for some $F \subseteq K_1, K_2 \subseteq E$ with $K_1 \cap K_2 = F$ and $Gal(K_i/F) = G_i$

Easy and I have many tools to try something different to what D&F does. Worst case look at the proof there.

B. SEPARABILITY/INSEPARABILITY. SOME FINITE FIELDS

In this section I'll cover whats on ch 19 Isaacs (also 13.5 and a bit of 14.9 D&F). Anders discussed pure inseparability so again I take this as an opportunity. (Also I will recall what I know on finite fields)

Corollary Let F be any field, $f \in F[x]$ irred. Then f separable iff $f' \neq 0$

Pf/ $\leftarrow$) Thm C

$\rightarrow$) If $f' = 0$ let $E \supseteq F$ splitting field for F then let $\alpha \in E : f(\alpha) = 0$ then $f'(\alpha) = f(\alpha) = 0$ so by the C f is not separable.

Corollary $f \in F[x]$ irred with char $F = 0$ is separable and $h \in F[x]$ separable iff product of distinct irreducibles.

Pf/ 1st part is obvious. For the second part let $f \neq g \in F[x]$ irred (here F is any field) if they have a common zero $\underset{\alpha}{}$ in a field extension $E \supseteq F$ then $f = Irr(\alpha, F, x) = g$ by thm elt to alg ↯. □

Corollary Let $f \in F[x]$ irreducible not separable. Then $char(F) = p \neq 0$ and $f(x) = g(x^p)$ for some $g \in F[x]$ irred.

Proof/ By the last corollary $f' = 0$ from this we easily see char $F \neq 0$.

Write $f(x) = \sum_{i=0}^{n} a_i x^i$, $f' = 0$ so $\sum_{i=1}^{n} i a_i x^{i-1} = 0$ thus $a_i = 0$ $\forall i : p \nmid i$.

So $f(x) = \sum_{j=0}^{n/p} a_{pj} x^{p \cdot j} = g(x^p)$ for $g = \sum_{j=0}^{n/p} a_{pj} x^j$

To see g is irred, we observe that a fact of g yields one of f. □

It is a good moment to recall what we know about finite fields. In the second seminar of ecal we proved.

Lemma (Freshman's dream) Let F be a field of charact p. Then

$$\begin{aligned} \varphi : F &\longrightarrow F \\ a &\longmapsto a^p \end{aligned}$$

is an injective field hom (called Frobenius endomorphism of F)
The image is denoted by F^p

Proof/ We saw $\varphi(a+b) = \varphi(a) + \varphi(b)$ in the seminar. $\varphi(ab) = \varphi(a)\varphi(b)$ is obvious.

If $\varphi(a) = 0$ and $a \neq 0$, $a^p = 0$ so $a^p a^{-1} = 0$ ... $a = 0$ ↯. □

In fact if char $F = p$, $f(x) = \sum_{i=0}^{n} a_i x^i \in F[x]$ then $f(x)^p = \sum_{i=0}^{n} a_i^p x^{ip}$ (see proof in seminar ecal of Freshman dream; it follows)

Thm Let K be a field, char $K = 0$ or char $K = p$ prime (of course). If K is finite then it has prime characteristic and char $K = p$ iff $|K| = p^n$. Moreover up to isom $\exists!$ field of p^n elements (namely the splitting field of $x^{p^n} - x \in \mathbb{Z}/_{p\mathbb{Z}}[x]$)

↓

Instructive to see the proof!! Specially if I am going to work with this field.

This field is usually called $GF(p^n)$. ✓ Galois field

DEF A field K of char $K = p > 0$ is called perfect if $K = K^p$. (Ex, let F char p, $F(X)$ not perfect)

(finite fields are of course perfect.) $\mathbb{F}_p \xrightarrow{\varphi} \mathbb{F}_p$ is the identity $\left(\alpha^{p-1} = 1 \ (\mathbb{F}_p^\times \text{ has order } p-1)\right)$

Thm Let $f \in F[x]$ irreducible not separable. Then char $F = p > 0$ and F not perfect. In particular every irreducible poly in a finite field is separable ∧ If $f \in F[x]$ (F finite) separable iff product of distinct irred polys.

Proof/ The in particular follows directly from the first statement and the proof of the second corollary of the section. We prove the first statement.

By the third corollary char $F = p > 0$ $f(x) = g(x^p)$ for some $g \in F[x]$. If F perfect $g(x) = \sum a_i^p x^i$ with $a_i \in F$. Thus $f(x) = g(x^p) = \sum a_i^p x^{pi} = (\sum a_i x^i)^p$ f irreducibility ☐

$\downarrow$

comment after F. Dream.

Now I mention two more corollaries

Corollary Suppose that F is a field with either char $F = 0$ or char $F = p$ and perfect. Then any algebraic field ext is separable. Clear.

Secondly, if char $F = p$ and let $f \in F[X]$ irreducible. Then $f(x) = g(x^{p^n})$ for some $n \in \mathbb{Z}_{\geq 0}$ and some $g \in F[X]$ separable irreducible. Proof/ If f separable $n = 0$ $g = f$. If not work by induction on $\deg(f)$ and use the third corollary of the section. ☐

This g is unique (see D&F) and sometimes denoted by f_{sep}. The degree of f_{sep} is called the separable degree of f; $\deg_s f(x)$. The p^n is called inseparable degree of $f(x)$ denoted $\deg_i f(x)$

Note Let $f(x) \in F[X]$ irred (char $F = p > 0$) then separable iff $\deg(f) = \deg_s(f)$
$\deg_i(f) = 1$

Also $\deg(f(x)) = (\deg_i(f(x)))(\deg_s(f(x)))$

With this we've covered 19 A, 13.5.
Isaacs D&F

Pure inseparability.

(We cover the rest of ch 19 Isaacs)

DEF let $F \subseteq E$ be an algebraic field extension. Suppose that if $\alpha \in E \setminus F$ then α is not separable. Then we say that E is purely inseparable over F. ($F \subseteq F$ is a trivial example)

Note that nontrivial $E \supsetneq F$ purely inseparable forces char $F = p$, F not perfect. (since α is not separable)

(19.10)

Theorem Suppose $F \subseteq E$ algebraic extension with char $F = p \neq 0$. TFAE

i) E is purely inseparable over F

ii) $\forall \alpha \in E$, $\exists \underset{\in \mathbb{Z}}{n \geq 0}$: $\alpha^{p^n} \in F$

iii) $\forall e \in E$, $\mathrm{Irr}(e, F, x) = x^{p^n} - a$ for some $n \in \mathbb{Z}_{\geq 0}$ $a \in F$.

Proof/ i→ii) Let $\alpha \in E$ and let $f = \mathrm{Irr}(\alpha, F, x) \in F[x]$. By the last corollary $f(x) = g(x^{p^n})$ $n \in \mathbb{Z}_{\geq 0}$, $g \in F[x]$ irreducible and separable over F. $f(\alpha) = g(\alpha^{p^n}) = 0$ so it follows that $g = \mathrm{Irr}(\alpha^{p^n}, F, x)$. Since g is separable, α^{p^n} is also separable so by pure inseparability $\alpha^{p^n} \in F$.

ii→iii) Let $\alpha \in E$, then $\alpha^{p^n} \in F$ for some $n \in \mathbb{Z}_{\geq 0}$. Thus α root of $\overset{= g(x)}{x^{p^n} - \alpha^{p^n}} \in F[x]$.

Note $g(x) = (x-\alpha)^{p^n}$, so every irreducible monic factor of g is $\overset{f(x)}{\overset{\shortparallel}{(x-\alpha)^r}}$ for some $r \in \mathbb{Z}_{\geq 0}$ by UFD.

In particular $f(\alpha) = 0$ So $f = \mathrm{Irr}(\alpha, F, x)$ uniquely determined. It follows $r \mid p^n$ so $r = p^m$ and $f(x) = x^{p^m} - \underset{\underset{a}{\shortparallel}}{\alpha^{p^m}} \in F[x]$

iii→i) Let $\alpha \in E$ separable over F, NTS $\alpha \in F$. Let $f = \mathrm{Irr}(\alpha, F, x) = x^{p^n} - a$. $\alpha^{p^n} = a$ since f has α as a root so $f(x) = (x-\alpha)^{p^n}$. Since $f \in F[x]$ irreducible and separable by 18.7 (here) $(x-\alpha)^2 \nmid_{F[x]} f$ so $f = x - \alpha$ so $\alpha \in F$. □

<u>Examples</u> i) Suppose $\overset{\text{char } F = p \neq 0}{E = F[\alpha]}$ and $\alpha^{p^n} \in F$ (so α algebraic thus $F[\alpha] = F(\alpha)$ field) for some $n \in \mathbb{Z}_{\geq 0}$ then E is purely inseparable over F.

You let $\beta \in E$ and try to find p-power of β lying in F. To do so, write β as a poly in α, use Freshman's dream to see $\beta^{p^n} \in F$.

ii) If F not perfect of characteristic p, then it has a nontrivial purely inseparable ext.

Let $a \in F \setminus F^p$. Let $f(x) = x^p - a$, then it has no root in F. Let E be a splitting field for f over F.
Let $\alpha \in E$: $f(\alpha) = 0$ note $\underset{\shortparallel\ F(\alpha) \text{ since it is a field}}{F[\alpha]} \supsetneq F$. By the corollary we are done. Actually we have $x^p - a = x^p - \alpha^p = (x-\alpha)^p$

$E = F[\alpha]$.

Now I mention two easy corollaries; the proofs are quite legible (19.12, 19.13)

<u>Corollary</u> Let $\mathrm{char}(F) = p \neq 0$ and suppose $F \subseteq E$ is a purely insep ext. Then

i) $F \subseteq K \subseteq E$ then K purely insep over F, E purely insep over K

ii) If $|E:F| < \infty$ then $|E:F| = p^n$.

Conversely, if $F \subseteq K \subseteq E$ and $\underset{E}{K}$ purely insep over $\underset{F}{F}$ then E is purely insep. over F.

The next goal is to see how these extensions arise naturally.

Lemma Let $E = F[\alpha, \beta]$ $(= F(\alpha, \beta))$ with α, β separable over F. Then E is sep over F.

Here $\alpha \neq \beta$ but it could be $\beta \in F$ so $F[\alpha]$ is here too

Proof/ Let $f = \mathrm{Irr}(\alpha, F, x)\,\mathrm{Irr}(\beta, F, x) \in F[x]$

Since $\alpha \neq \beta$ by trans elmts alg it is clear that f is separable. Let L be a splitting field for f over E. Note it is a splitting field for f over F. By thm/Def of Galois extension L is separable over F. So clearly E sep over F. □

Thm (19.14) Let $F \subseteq E$ be an algebraic field extension let $S = \{\alpha \in E : \alpha \text{ sep over } F\}$ then

i) S is a field

ii) It is the unique field between F, E st it is sep over F and E purely insep over it.

Proof/ i) Let $\alpha, \beta \in S$ then $F[\alpha, \beta] \subseteq S$ so this is clear that S is a field

ii) By def S is sep over F.

Claim E purely insep over S.

WMA char $F = p \neq 0$ (else $S = E$), let $\alpha \in E$ we need to show $\alpha^{p^n} \in S$ by the previous theorem.

Let $f = \mathrm{Irr}(\alpha, F, x)$. By the last corollary before pure insep $f(x) = g(x^{p^n})$ for some $n \in \mathbb{Z}_{\geq 0}$ $g \in F[x]$ irreducible separable. Then $g(\alpha^{p^n}) = 0$ so $g = \mathrm{Irr}(\alpha^{p^n}, F, x)$. Since g is sep we conclude $\alpha^{p^n} \in S$.

Claim It is unique.

Suppose $\underbrace{F \subseteq T}_{\text{sep}} \underbrace{\subseteq E}_{\text{purely insep}}$. Then clearly $T \subseteq S$; by the last corollary S purely insep over T. But by 18.12

S separable over T. It follows $S = T$ □

Now some corollaries

Corollary (19.16, 19.17) Let $F \subseteq E$ finite degree insep. extension. Then char $F \mid |E:F|$

(Converse to 18.12) Let $F \subseteq L \subseteq E$ with L/F sep, E/L sep. Then E is sep over F.

Proof/ i) Note that E/F algebraic so if char 0 is sep thus char $F = p$ prime. Let S be as in the previous thm, $S < E$ since E not sep over F. E is purely insep over S so $p \mid |E:S|$ by the last corollary.

ii) Let S be the elmts of E separable over F. Note $L \subseteq S \subseteq E$; by 18.12 E sep over S (note E alg over F) but by 19.14 E purely insep over S so $E = S$ □.

By 19.14 any algebraic extension E/F can be understood as two successive extensions ; one separable S/F and one purely inseparable E/S. Assume further that $|E:F|<\infty$. We denote $|E:F|_{sep} = |S:F|$ and call it separable degree/separable part of the degree of the extension

Isaacs does not define it but $|E:F|_{insep} = |E:S|$ inseparable degree...

(obviously $|E:F| = |E:F|_{sep} |E:F|_{insep}$; the ext is sep iff $|E:F| = |E:F|_{sep}$ and if E inseparable over F then we have that $|E:F|_{insep}$ is a power of the characteristic by 19.12)

Our next topic is try to reverse the order ie find $E \supseteq K \supseteq F$ so that E/K sep, K/F purely insep. In general this can't be done.

Theorem 19.18 Let $F \subseteq E$ finite field ext. Assume E normal over F. Let $K = C_E(Gal(E/F))$. Then K purely insep over F, E sep. over K.

Proof/ STEP 1 E sep over K.

✓ By Artin (18.20 c).

STEP 2 K purely insep over F.

Let $\alpha \in K \setminus F$ assume α is separable over F. Let $f = Irr(\alpha, F, x)$; by the normality assumption f splits over E. Note $\deg(f) \geq 2$ and since it is separable $\exists \beta \neq \alpha : f(\beta) = 0$. By [illegible] $\exists \sigma \in Gal(E/F) : \sigma(\alpha) = \beta$. ↯ $\alpha \in C_E(Gal(E/F))$. So K purely insep. □

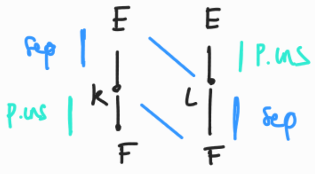
The natural question is ; in 19.18 $|E:K| = |E:F|_{sep}$?

Lemma (19.20) Suppose $F \subseteq K$ purely insep. ext. Let $f \in F[x]$ separable irred then it remains irreducible in $K[x]$.

Proof/ Suppose $g \in K[x]$ monic $g \mid_{K[x]} f$. Claim $\deg(f) = \deg(g)$. (of course this concludes the lemma)

Let E be a splitting field for f over K. Then $g = \prod (x - \alpha_i)$. Each α_i is of course root of f so sep over K. Let $S = \{\alpha \in E : \alpha \text{ sep over } F\}$ then each $x - \alpha_i \in S[x]$ so $g \in S[x]$ so the coeff of g lie in $\underset{\substack{\downarrow \\ K/F \text{ purely insep}}}{S \cap K = F}$. By the irreducibility of f over F we are done □

Thm 19.19 Let E/F be a finite extension. Let $F \subseteq L, K \subseteq E$ so that L/F, E/K are separable and K/F, E/L purely insep. Then $|L:F| = |E:K|$.



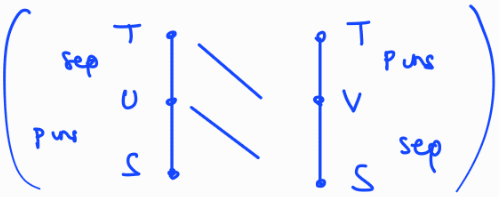
Pf/ Read from book.

Corollary 19.21 Let $F \subseteq U \subseteq E$ fields with $|F:E| < \infty$. Then $|E:U|_{sep}\, |U:F|_{sep} = |E:F|_{sep}$

Proof/ By 19.14 let $\underbrace{F \subseteq S}_{sep} \underbrace{\subseteq U}_{purely\ unsep}$, $\underbrace{U \subseteq T}_{sep} \underbrace{\subseteq E}_{purely\ unsep}$, $\underbrace{S \subseteq V}_{sep} \underbrace{\subseteq T}_{purely\ unsep}$.

By 19.17 V is separable over F, by 19.12/13 E purely unsep over V so by uniqueness of 19.14 $V = \{\alpha \in E : \alpha \text{ sep over } F\}$. Thus $|E:F|_{sep} = |E:V|$

Now $|V:F| = |V:S|\, \underset{\underset{|U:F|_{sep}}{\shortparallel}}{|S:F|}$ and $|V:S| =$



$= |T:U| = |E:U|_{sep}$ □

Finally I mention one interesting thm (read proof from book) that concludes ch 19.

Thm 19.22 Let $F \subseteq E$ alg field ext. Suppose $\forall f \in F[x] \setminus F$ f has at least one root in E. Then E is alg closed.

(Nice way to prove algebraically closed)

C. SOME NUMBER THEORY: CYCLOTOMY ; DIRICHLET

The goal of this section is to complete section 3 of part 2 ecal by extending Seminar 1 (the 1st part)

This will contain the material from ch 20 Isaacs (ignoring Gauss. constructions; covered in ecal) and if I see smth from 13.6, 14.5 D&F which is not here I'll add it.

(the 1st two results are trivial but I add for completeness)

Generalities.

Recall that if F is a field $\varepsilon \in F$ is said to be a root of unity if $o(\varepsilon) < \infty$ in $F^{\times}$. If $o(\varepsilon) = n$ then we say it is a primitive nth root of unity.

(20.1)
Lemma Let F be a field $n \geq 1$. The set of nth roots of unity in F is a cyclic subgroup of F with order dividing n. This has order n iff F contains a primitive nth root of unity.

Proof/ $C = \{$nth roots of unity$\}$ are the roots of $x^n - 1 \in F[x]$ so finite. Subgroup is clear. Now in seminar 4 Ecal we proved $G \leq F^{\times}$ finite is cyclic. Write $|C| = m$ let $C = \langle \varepsilon \rangle$ then $m = o(\varepsilon)$ and $\varepsilon^n = 1$ so $m \mid n$.

The iff is obvious □

Now I mention an obvious corollary which follows from cyclic groups ($\varphi(n)$: # $k \in \mathbb{Z}_{>0} : (n,k)=1$)

Corollary 20.2 Let $\varepsilon \in F$ be a primitive nth root of unity. Then

i) $\{\varepsilon^k \mid 0 \leq k < n\}$ has cardinality n and are all the nth roots of unity

ii) $\{\varepsilon^k \mid 0 \leq k < n, (k,n)=1\}$ are all the primitive nth roots of unity; $\exists$ exactly $\varphi(n)$ of them.

Suppose that a field fails to have a primitive nth root. Can we adjoin one? How many fields we get.
This theorem is a generalisation of the first thm of sec 3 part 2 Ecal.

Thm (20.3) Let F be a field; then $\exists E \supseteq F$: $\varepsilon \in E$ is a primitive nth root of unity iff char $F \nmid n$.
If $F \subseteq E$, $\varepsilon \in E$ is a primitive nth root of unity then $F[\varepsilon] = F(\varepsilon)$ is a splitting field for $x^n - 1$ over F.
In particular $F[\varepsilon]$ uniquely (up to iso that fixes F) determined by F, n.

Proof/ The in particular follows clearly (part 1 ecal)

$\longrightarrow$) Char $F \mid n$, then char $F = p$ prime. Write $n = pm$. Then $\overset{f(x)}{\overset{\shortparallel}{(x^n-1)}} = (x^m-1)^p \in F[x]$
and this polynomial can have at most m roots in any extension of F. Thus no extension of F can contain n nth roots of unity so by last corollary no field extension contains a primitive nth root

$\longleftarrow$) If char $F \nmid n$ then the unique root of $f' \in F[x]$ (as defined in sem 1) is 0 ($f'(x) = nx^{n-1}$)
By the (sem 1 it follows f is separable. If E is a splitting field for f it follows it has n distinct roots
By 20.1 contains a primitive root.

The second assertion is easy to see. If $F \subseteq E$, $\varepsilon \in E$ primitive nth root then clearly $x^n - 1$ splits over $F(\varepsilon)$
and $F(1, \varepsilon, \ldots, \varepsilon^{n-1}) = F(\varepsilon)$. □

I mention two more generalities now.

Lemma 20.6 Let C be a cyclic group of order n. Then $\mathrm{Aut}(C) \cong \overset{\text{group of units}}{(\mathbb{Z}/n\mathbb{Z})^{\times}}$; in particular it is abelian. If n prime $\mathrm{Aut}(C) = C_{n-1}$ (this group has $\varphi(n)$ elements)

Proof/ $|\mathbb{Z}/n\mathbb{Z}^{\times}| = \varphi(n)$ by part 1 ring thy algebra qual. $C = \mathbb{Z}/n\mathbb{Z}$ additively
mult by $u \in \mathbb{Z}/n\mathbb{Z}^{\times}$ defines automorphisms so $\mathbb{Z}/n\mathbb{Z}^{\times}$ injects in $\mathrm{Aut}(C)$. But $\mathrm{Aut}(C)$ has $\varphi(n)$
elements (send gen to generator). For the second part look at ; it also gives how to compute $\varphi(n)$ via CRT. □

The next theorem is a generalised version of the second theorem of sec 3 part 2 ecal.

Lemma 20.7 Let $F \subseteq E$ field extension and suppose $E = F[\varepsilon]$ ($= F(\varepsilon)$) where ε is a root of unity
Then E/F Galois and $\mathrm{Gal}(E/F) \lesssim \mathrm{Aut}(C)$ where $C = \langle \varepsilon \rangle \leq E^{\times}$. In part abelian.

Proof/ STEP 1 E Galois over F. $(n = |\langle \varepsilon \rangle|)$

We prove that E is the splitting field of a separable poly over F. Let $\overset{f}{\overbrace{x^n - 1}} \in F[x]$. Note that since $E = F[\varepsilon]$ is a splitting field of f over F. Now ε has order n so f is separable thus E/F Galois

(Note how similar this proof is to the one in Ecal; this is how we extend; not worth it to take a course)

STEP 2 $\mathrm{Gal}(E/F) \lesssim \mathrm{Aut}(C)$ (this is essentially what we did in Ecal)

Let $\sigma \in \mathrm{Gal}(E/F)$, by above remarks (and 20.2) $\sigma(\varepsilon) \in C$. Thus $\sigma|_C : C \to C$ so automorphism. So we have a group hom $\mathrm{Gal}(E/F) \to \mathrm{Aut}(C)$. It is easy to see it has trivial kernel. □

Cyclotomic polynomial

We now focus on $\mathbb{C}$. $\forall n \in \mathbb{N}_{\geq 1}$, $\mathbb{C}$ contains a primitive nth root of unity $e^{i2\pi/n}$ and so $\varphi(n)$ primitive nth roots.

The nth cyclotomic polynomial, denoted $\Phi_n(x) \in \mathbb{C}[x]$ is the monic poly whose roots are precisely the primitive nth roots of unity.

$$\Phi_n(x) = \prod_{\substack{\varepsilon \in \mathbb{C} \\ \text{st } o(\varepsilon) = n}} (x - \varepsilon) = \prod_{\substack{0 \leq k < n \\ (n,k)=1}} (x - e^{2\pi i n/k}) \quad ; \text{ note } \deg(\Phi_n) = \varphi(n)$$

Examples
$\Phi_1(x) = x - 1$
$\Phi_2(x) = x + 1$
$\Phi_3(x) = (x - \omega)(x - \omega^2) = x^2 + x + 1$ where $\omega = e^{2\pi i/3}$
$\Phi_4(x) = (x - i)(x + i) = x^2 + 1$

To compute more we need a lemma.

Lemma (20.4) $x^n - 1 = \prod_{\substack{d \mid n \\ d > 0}} \Phi_d(x)$ (note a comparison of degrees yields $n = \sum_{\substack{d \mid n \\ d > 0}} \varphi(d)$)

Proof/ $x^n - 1 = \prod_{\substack{\varepsilon \text{ nth} \\ \text{root of unity}}} (x - \varepsilon)$ Each ε has mult order $d \mid n$ (by easy group thy). Conversely $\forall d \mid n$ a primitive dth root of unity is an nth root of unity. By grouping factors the result follows. □

Corollary 20.5 All coefficients of Φ_n lie in $\mathbb{Z}$ (D&F)

Proof/ By the previous lemma $\Big(\overbrace{\prod_{\substack{d \mid n \\ d < n}} \Phi_d(x)}^{= r(x)}\Big) \Phi_n(x) = x^n - 1$ so $r(x) \underset{\mathbb{Q}(\varepsilon)[x]}{\mid} x^n - 1$ and by induction $r(x) \in \mathbb{Z}[x]$

(and it is monic). This division is performed in $\mathbb{Q}(\varepsilon)$ where ε primitive nth root (in $\mathbb{C}$) (note by def $\Phi_n(x) \in \mathbb{Q}(\varepsilon)[x]$)

Now by section 2 in part 3 ring thy alg qual $r(x) \mid x^n - 1$ in $\mathbb{Q}[x]$. Now by Gauss lemma (alg qual) $r(x) \mid x^n - 1$ in $\mathbb{Z}[x]$

so $\Phi_n(x) \in \mathbb{Z}[x]$. (domain). □

Examples We are now able to compute: If p prime then

- $\Phi_p(x) = x^{p-1}+\dots+x+1$ (in recall we proved that it is irreducible in $\mathbb{Q}[x]$)

Why? $x^p - 1 = \Phi_p(x)\Phi_1(x) = \Phi_p(x)(x-1)$ So $\Phi_p(x) = x^p - 1 / x-1 = x^{p-1}+\dots+x+1$

↓ either in field of fractions or just division in a ring.

- $\Phi_6(x) = \dfrac{x^6-1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)} = x^2 - x + 1$

- $\Phi_{15}(x) = \dfrac{x^{15}-1}{\Phi_5(x)\Phi_3(x)\Phi_1(x)} = \dfrac{x^{15}-1}{(x^5-1)\Phi_3(x)} = \dots = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$

(by checking it; to compute you need to know how to "divide". See it as a trick to obtain smth that after you check it holds)

Lemma p prime $n \geq 1$, $\Phi_{pn}(x) = \begin{cases} \Phi_n(x^p) & p \mid n \\ \Phi_n(x^p)/\Phi_n(x) & p \nmid n \end{cases}$ (think)

With this for example $\Phi_8(x) = \Phi_4(x^2) = x^4+1$; $\Phi_{12}(x) = \Phi_6(x^2) = x^4 - x^2 + 1$

Notes i) With the techniques we have so far we can compute a bunch of them

ii) All the non zero coeff seem to be ±1. This holds until n = 105 (by computation). A thm of Migotti asserts that in order to have a coefficient other than 0, ±1 we need n to be divisible by at least 3 different odd primes.

Let ε_n denote $e^{2\pi i/n} \in \mathbb{C}$ (primitive nth root of unity in $\mathbb{C}$). Write $\mathbb{Q}_n := \mathbb{Q}(\varepsilon_n)$ and call it the nth cyclotomic field.

- $\mathbb{Q}_n$ is the splitting field of $x^n - 1$ over $\mathbb{Q}$ in $\mathbb{C}$. So $\mathbb{Q}_n/\mathbb{Q}$ is Galois ($x^n - 1 \in \mathbb{Q}[x]$ is separable)

We now compute Galois group. By 20.7 $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \overset{<}{\cong} \mathrm{Aut}(C_n)$. $|\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})| \underset{\downarrow}{=} |\mathbb{Q}_n : \mathbb{Q}| =$

$\quad\quad$ 20.6 $\mathrm{Aut}(C_n) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ $\quad\quad$ Galois ext

$= \deg(\mathrm{Irr}(\varepsilon_n, \mathbb{Q}, x))$

↳ see alg qual ring thy part L for more about this.

Claim $\mathrm{Irr}(\varepsilon_n, \mathbb{Q}, x) = \Phi_n(x)$. Therefore $|\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})| = \varphi(n)$ hence $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$

We already know it is monic and ε_n root of $\Phi_n(x)$. NTS irred over $\mathbb{Q}[x]$.

Thm (20.8) The cyclotomic poly $\Phi_n(x)$ is irreducible in $\mathbb{Q}[x]$ $\forall n \geq 1$.

Proof/ Suppose not. Then we have a factorization $\Phi_n(x) = f(x)g(x)$ with $f, g \in \mathbb{Z}[x]$ monic by Gauss lemma. We take $f(x)$ to be irreducible factor (in $\mathbb{Q}[x]$ see Gauss lemma). $\deg(f), \deg(g) \geq 1$.

Let ξ be primitive nth root of unity which is root of f. ($f = \mathrm{Irr}(\xi, \mathbb{Q}, x)$) Let p any prime $p \nmid n$.

Then ξ^p is again a primitive nth root of unity (group thy) so root of f or g. Suppose $g(\xi^p) = 0$

Then ξ root of $g(x^p)$ thus $f(x) \underset{\mathbb{Q}[x]}{\Big|} g(x^p)$ so also divide in $\mathbb{Z}[x]$ by Gauss' lemma.

So $g(x^p) = f(x)h(x)$, $h(x) \in \mathbb{Z}[x]$. If we reduce them mod p, (each coef)

$$\bar{g}(x^p) = \bar{f}(x)\bar{h}(x) \quad \text{in } \mathbb{F}_p[x].$$

But in $\mathbb{F}_p$, $\alpha^{p-1} = 1$ ($\mathbb{F}_p^\times$ has order $p-1$) so $\alpha^p = \alpha$; this and the comment after Freshman's dream it follows $\bar{g}(x^p) = (\bar{g}(x))^p$. Thus $(\bar{g}(x))^p = \bar{f}(x)\bar{h}(x)$. Thus $\bar{f} \underset{\mathbb{F}_p[x] \text{ (UFD)}}{\Big|} \bar{g}^p$ so they have a common irred factor ($\bar{f}$ has deg > 0 since f monic)

Since $fg = \Phi_n \underset{\mathbb{Z}[x]}{\Big|} x^n - 1$ it follows $\bar{f}\bar{g} \underset{\mathbb{F}_p[x]}{\Big|} \overline{x^n - 1} = x^n - 1 \in \mathbb{F}_p[x]$

So $x^n - 1 \in \mathbb{F}_p[x]$ is divisible by the square of the common irreducible factor of $\bar{f}, \bar{g}$ so $x^n - 1 \in \mathbb{F}_p[x]$ not separable. This is a contradiction since $p \nmid n$ so $(x^n-1)' \in \mathbb{F}_p[x] \setminus \{0\}$ and only has 0 as a root which is not a root of $x^n - 1$ (so contradiction with thm C).

So ξ^p root of $f(x)$. This applies to every root of f. It follows ξ^a root $\forall a \in \mathbb{Z} : (a, n) = 1$. Thus every primitive nth root of unity (by cyclic groups thm) is a root of f so $\Phi_n(x) = f(x)$ thus $\deg(g) \leq 1$ ʃ so $\Phi_n(x)$ irred □

Recall that if $m, n \in \mathbb{Z}_{\geq 1}$
(i is alg qual; ii follows from i)

i) If $\gcd(m,n) = 1 \to (\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$

ii) If $\gcd(m,n) = 1$ $\varphi(mn) = \varphi(m)\varphi(n)$

So in general $\varphi(m)\varphi(n) = \varphi(\mathrm{lcm}(m,n))\,\varphi(\gcd(m,n))$ (thanks to ii).

<u>Theorem (20.12)</u> Let $m, n \in \mathbb{Z}_{\geq 1}$ let $\ell = \mathrm{lcm}(m,n)$, $d = \gcd(m,n)$. Then

i) $\langle \mathbb{Q}_m, \mathbb{Q}_n \rangle_{\subseteq \mathbb{C}} = \mathbb{Q}_\ell$

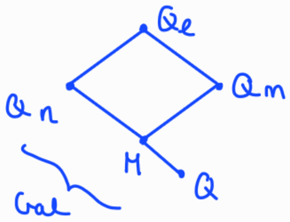
ii) $\mathbb{Q}_m \cap \mathbb{Q}_n = \mathbb{Q}_d$

Proof/ i) $\subseteq$) Since $m \mid \ell$, $n \mid \ell$ $\mathbb{Q}_m \subseteq \mathbb{Q}_\ell$, $\mathbb{Q}_n \subseteq \mathbb{Q}_\ell$

$\supseteq$) $\langle \varepsilon_m, \varepsilon_m \rangle \leq \langle \varepsilon_\ell \rangle$ but the first subgroup has order divisible by m, n so by L so $\langle \varepsilon_m, \varepsilon_n \rangle = \langle \varepsilon_\ell \rangle$

Thus $\mathbb{Q}_\ell \subseteq \langle \mathbb{Q}_m, \mathbb{Q}_n \rangle$

ii)



By natural irrationalities $|\mathbb{Q}_e : \mathbb{Q}_m| = |\mathbb{Q}_n : \mathbb{Q}_n \cap \mathbb{Q}_m|$

Now $|\mathbb{Q}_e : \mathbb{Q}_m| = \dfrac{|\mathbb{Q}_e : \mathbb{Q}|}{|\mathbb{Q}_m : \mathbb{Q}|} = \dfrac{\varphi(e)}{\varphi(m)}$ and similarly $|\mathbb{Q}_n : \mathbb{Q}_d| = \dfrac{\varphi(n)}{\varphi(d)} \overset{\text{obs before thm.}}{=} \dfrac{\varphi(e)}{\varphi(m)}$

Thus $|\mathbb{Q}_e : \mathbb{Q}_m| = |\mathbb{Q}_n : \mathbb{Q}_m \cap \mathbb{Q}_n| \underset{\downarrow}{\leq} |\mathbb{Q}_n : \mathbb{Q}_d| = \dfrac{\varphi(e)}{\varphi(m)} = |\mathbb{Q}_e : \mathbb{Q}_m|$ So $\mathbb{Q}_n \cap \mathbb{Q}_m = \mathbb{Q}_d$. □

$\mathbb{Q}_m \cap \mathbb{Q}_n \subseteq \mathbb{Q}_d$
obvious (if $o(\varepsilon) \mid n$, $o(\varepsilon) \mid m$ $\rightarrow$ $o(\varepsilon) \mid d$)

<u>Note</u> if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ prime fact $p_i \neq p_j$. $Gal(\mathbb{Q}_n/\mathbb{Q}) \underset{\downarrow}{\cong} Gal(\mathbb{Q}_{p_1^{\alpha_1}}/\mathbb{Q}) \times \cdots \times Gal(\mathbb{Q}_{p_k^{\alpha_k}}/\mathbb{Q}) \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^{\times} \times \cdots$

last thm combined with last prop before separability section

<u>Note</u> In Ecal we define E/k to be abelian if Galois (normal + char 0) with abelian Galois group; in general E/k is abelian if Galois with abelian Galois group. (✓) (Note that the lemma we mention in Ecal after def of abelian extension remains true (with the same proof but using 18.12) with the new meaning of Galois).

Now watch video "Last things in Ecal". (MUST) Ch 22 Issues, galois groups of polys and how does ecal conclude.

↳ see 2nd paragraph p627 D&F for the most general version of Grand theorem de Galois. (they never proved in that case and the gen. is obvious)

· A part from practica 2 Ecal, 14.8 D&F can be a good source for techniques about computing Galois groups.

Applications

We attempt to prove two nice theorems.

<u>Lemma 20.15</u> Let p be a prime divisor of $\Phi_n(m)$ $n, m \in \mathbb{Z}_{\geq 1}$. Then $p \nmid m$. If also $p \nmid n$ then $p \equiv 1 \bmod n$

Proof/ By 20.4 $\Phi_n(x) \underset{\mathbb{Z}[x]}{\mid} x^n - 1$ so $\Phi_n(m) \underset{\mathbb{Z}}{\mid} m^n - 1$ so $m^n \equiv 1 \bmod p$ in part $p \nmid m$

Let $\bar{m} \in \mathbb{Z}/p\mathbb{Z}$ let $d = o(\bar{m})$ in $(\mathbb{Z}/p\mathbb{Z})^{\times}$ by Lagrange $d \mid p-1$. Suppose $p \nmid n$, NTS $d = n$.

Since $m^n \equiv 1 \bmod p$, $d \mid n$ so $n = de$ for some $e \in \mathbb{Z}_{>0}$. NTS $e > 1$ then $p \mid n$ (and then we conclude)

Since d is a proper divisor of n $(x^d)^e - 1 = x^n - 1 = \Phi_n(x)\,\Phi_d(x)\,g(x)$ where $g = 1$ or g product of cyclotomic polys by 20.4. Dividing by $x^d - 1$, $1 + x^d + (x^d)^2 + \dots + (x^d)^{e-1} = \Phi_n(x)\,g(x)$ (check).

So $p \mid \underset{\mathbb{Z}}{\Phi_n(m) \mid} 1 + m^d + \dots + (m^d)^{e-1}$. $\wedge$ $m^d \equiv 1 \bmod p$. Thus clearly $e \equiv 0 \bmod p$

And since $e \mid n$, $p \mid n$. □ □

<u>Obs</u> $n \in \mathbb{Z}_{\geq 1}$, if $p \mid \Phi_n(n)$ then $p \equiv 1 \bmod n$

<u>Lemma 20.17</u> Let $n > 1$ then $|\Phi_n(x)| > x - 1$ $\forall x \geq 2$ $x \in \mathbb{R}$.

Pf/ The closest point to x (usual distance) in unit circle is 1. So $|x - \varepsilon| > x - 1$ $\forall \varepsilon$ nontrivial root of unity ε. Since $\Phi_n(x)$ is a product of $\varphi(n)$ factors of the form $x - \varepsilon$, $|\Phi_n(x)| > (x-1)^{\varphi(n)} \geq x - 1$

□

<u>Thm (Baby Dirichlet) 20.14</u> $\forall n \in \mathbb{Z}_{>0}$ $\exists$ infinitely many primes p st $p \equiv 1 \bmod n$

Proof/ $n = 1$ clear. Suppose $n > 1$, let $k \geq 1$ and let $N_k = \Phi_{kn}(nk) \in \mathbb{Z}$ (Φ_s is integer poly)

By L20.17 $|N_k| > 1$ so it has some prime divisor p_k. By 20.16 $p_k \equiv 1 \bmod nk$ so $p_k \equiv 1 \bmod n$

Since $1 < p_k \equiv 1 \bmod nk$, $p_k > nk$ so we can find arbitrarily large primes among the p_k thus there are infinitely many

□

<u>Thm (nice)</u> Let G be any finite abelian group, then $\exists E \subseteq \mathbb{C}$: $E/\mathbb{Q}$ Galois and $\mathrm{Gal}(E/\mathbb{Q})$

Proof/ By Fund. thm of abelian groups $G \cong C_1 \times C_2 \cdots \times C_r$, C_i cyclic of order n_i. By 20.14 choose p_i prime : $p_i \equiv 1 \bmod n_i$ all distinct. Let $n = p_1 \cdots p_r$. Note (2nd to last note before applications) that

$\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong (\mathbb{Z}/p_1\mathbb{Z})^\times \cdots (\mathbb{Z}/p_r\mathbb{Z})^\times$; note $(\mathbb{Z}/p_i\mathbb{Z})^\times \cong C_{p_i - 1}$. Since $n_i \mid p_i - 1$

we can choose $V_i \leq (\mathbb{Z}/p_i\mathbb{Z})^\times$ with index n_i. Note $\dfrac{(\mathbb{Z}/p_1\mathbb{Z})^\times \times \dots \times (\mathbb{Z}/p_r\mathbb{Z})^\times}{V_1 \times \dots \times V_r} \cong G$

So $\exists H \leq \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$: $\dfrac{\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})}{H} \cong G$. Let $E = C_{\mathbb{Q}}(H)$. Then E Galois over $\mathbb{Q}$ ($H \trianglelefteq \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$)

and $\mathrm{Gal}(E/\mathbb{Q}) \underset{\substack{\downarrow \\ \text{Galois corresp thm.}}}{\cong} \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})/H \cong G$.

□

nice discussion in pag 606 D&F.

(not proved in D&F nor Isaacs)

Of course E subfield of $\mathbb{Q}_n$! (the converse of this is Kronecker-Weber : $\mathbb{Q} \leq E \leq \mathbb{C}$, $E/\mathbb{Q}$ finite abelian; then $E \leq \mathbb{Q}_n$)

(Section 14.5 and 20D Isaacs discuss geometric const; also 13.3 if I ever need more than what done in Ecal; which was decent) and example for me now

- There are a few nice exercises in ch 20 that I should frequently look in case I need, for example Gauss sums are introduced

D. FINITE FIELDS

The goal of this section is to say a few more things than what we already mentioned (coming from ecal seminar) about finite fields. I will either cover or mention what is on 14.3 D&F ∧ ch 21 Isaacs.
(the first results of ch 21 are essentially covered in the ecal seminar that we reviewed a few pages before)

(I mention one Lemma that Isaacs uses to prove what we already know (so I skip proof; but good to have it stated)
probably embedded in a proof sem ecal 2.

Lemma 21.4 L field char $L = p$ prime. Let $q = p^n$. L contains a field of order q iff $x^q - x$ splits in $L[x]$.
In this case $E = \{\alpha \in L : \alpha^q = \alpha\}$ is the unique subfield of L of order q)

conseq of all we know (not just this lemma).

Corollary 21.6 Let $F = F_p$ where p is a prime and let n be a positive integer. Then $\exists f \in F[x]$ irreducible (over $F[x]$) with degree n.

Proof/ Let $E = GF(p^n)$ and identify F with the prime subfield. We know $E^\times$ is cyclic (seminar Ecal) so we can write $E^\times = \langle \alpha \rangle$. Then $E = F[\alpha]$ $(= F(\alpha))$ and $\deg(\operatorname{Irr}(\alpha, F, x)) = |E:F| = n$ $\square$

E is a finite dimensional vspace over F
so $E \cong F^m$ where $m = \dim_F E = |E:F|$
thus $|E| = p^m$ so $m = n$

Subfield structure of finite fields.

Now we can try to sharpen this and count the number of irreducible polys of degree n in $F[x]$, F finite field.
↳ by studying subfields of finite fields.

Theorem 21.7 Let $F = GF(q^n)$ with q a prime power. If $m \in \mathbb{Z}_{\geq 1}$ TFAE

i) E has a subfield of order q^m

ii) $m \mid n$

iii) $q^m - 1 \mid q^n - 1$

Also if q is prime then every subfield of E has order q^m for some integer $m \mid n$.

Proof/ i → ii) $F \subseteq E$ subfield $|F| = q^m$. E is an F vector space of finite dimension so $E \cong F^s$ thus $(q^m)^s = q^n$ so $ms = n$ thus $m \mid n$

ii → iii) $n = ms$. $x^s - 1 = (x-1)(x^{s-1} + \dots + x + 1)$. Substitute q^m

(Note $E^\times = C_{q^n - 1}$ and it has a subgroup of order equal to any given divisor of $q^n - 1$)

iii → i) $\exists H \leq E^{\times}$ $|H| = q^m - 1$. Clearly each of the q^m elmts of $H \cup \{0\}$ is a root of $x^{q^m} - x$ (if $h \in H$ $h^{q^m - 1} = 1$). Now as in the section (using freshman's dream) we see H subfield.
recall

Finally if q is prime, $q = char(E)$ so if $F \subseteq E$ subfield $|F| = q^m$ and $m|n$ by i) → ii). ☐

<u>Corollary 21.8 21.9</u>

i) Let $E, F \subseteq L$ where $|E| = q^n$, $|F| = q^m$ q prime power. Then $|E \cap F| = q^d$ where $d = gcd(m,n)$

In particular $F \subseteq E$ if $m|n$.

ii) Let $F \subseteq E$ with $|F| = q < \infty$, $|E:F| = n < \infty$. Then $\forall m|n$ $\exists!$ K subfield $F \subseteq K \subseteq E$ st $|K| = q^m$ and $\nexists$ other intermediate subfields.

Proof/ i) By 21.7 each of E, F have a subfield of order q^d. By L21.4 L has at most one subfield of order q^d thus $|F \cap E| \geq q^d$ (easy to argue by contradiction).

Let $p = char F$, write $q = p^a$. Then $|E \cap F| = p^e$ for some e. By 21.7 $e|ma$ $e|na$ so $e | gcd(ma, na) = da$ so $|E \cap F| \leq p^{da} = q^d$. For the in particular, if $m|n$, $d = m$ and $|F| = |F \cap E|$ so $F \cap E = F$ thus $F \subseteq E$

ii) If $F \subseteq K \subseteq E$ write $|K:F| = m$. Then $m|n$ by 21.7 and easily $|K| = q^m$.
Also K unique of its order by 21.4. Let $m|n$. By 21.7 $\exists K \subseteq E$: $|K| = q^m$. Since $|F| = q^1$ and $1|m$ $F \subseteq K$ by i). ☐

Algebraic closure of finite field: (maybe excessive details)

We are now ready to give a more explicit view of the algebraic closure of a finite field. We know by 17.27, 17.30 the $\exists!$ of this but seeing the proof I do not get much intuition. My approach here follows "Finite rings with identity by McDonald" (there are other very similar approaches in D&F p588, Exercise in Lang)
<u>so of course the explicit constructions may vary</u>.

Fix p prime. If $e|f$ $GF(p^e) \subseteq GF(p^f)$ (meaning that the second has a subfield of order p^e (unique field of that order up to iso))

Thus we can write $GF(p) \subseteq GF(p^{2!}) \subseteq GF(p^{3!}) \dots \subseteq GF(p^{n!}) \subseteq \dots$
using 21.7

(to be formal you start with some explicit $GF(p)$. Then take an explicit $GF(p^2)$ in a way such that properly contains the previous field as sets (we can do it with surgery); do this again and again by induction.)
(now with $GF(p^2) \subseteq GF(p^{3!})$)

Let $GF(p^{\infty}) = \bigcup_{n=1}^{\infty} GF(p^{n!})$

Theorem $GF(p^\infty)$ is an alg closed field of char p. Moreover

Short note video.

i) $GF(p^e) \subseteq GF(p^\infty)$ $\forall e \geq 1$ (contains every finite field of char p "up to iso")

Let F be finite of char p, $\exists \tilde{F} \cong F : \tilde{F} \subseteq GF(p^\infty)$.

ii) $GF(p^\infty)$ is an algebraic closure of any subfield. In part if we start with $GF(p^e)$ $e \geq 1$ then we do surgery so that this field is in $GF(p^\infty)$ (build some explicit $GF(p^\infty)$ so that our field is inside) and it follows that is an alg closure.

iii) $GF(p^\infty)$ countable.

Proof / ii) Follows from the 1st statement via 17.24. iii) Clear by construction. To prove the 1st statement and i):

<u>$GF(p^\infty)$ is a field</u> : Let $x, y \in GF(p^\infty)$ $\exists n :$ $x, y \in GF(p^{n!})$ so $x-y$, $xy \in GF(p^{n!}) \subseteq GF(p^\infty)$

So properties of field inherited.

<u>i)</u> $e \geq 1$. Then $GF(p^e) \subseteq GF(p^{e!})$ (by 21.7 F field of order p^e is has an isomorphic copy inside any
$\subseteq GF(p^\infty)$ explicit $GF(p^e)$ in part the one we fixed)

<u>Alg closed</u> : Let $p(x) \in GF(p^\infty)[x]$. $\exists n \in \mathbb{N} :$ $p(x) \in GF(p^{n!})[x]$. The splitting field is a finite extension of $GF(p^{n!})$ so field of order^{K} p^e containing our $GF(p^{n!})$ Consider our explicit $GF(p^e) \subseteq GF(p^\infty)$ Since $K \cong GF(p^e)$ (fixing the explicit $GF(p^{n!})$) it is clear that it is also a splitting field for f so f splits over $GF(p^\infty)$.

($g(x) \in F[x]$, $E = F(\alpha_1, \dots, \alpha_n)$ splitting field for F, $K \underset{\sigma \text{ fixing } F}{\cong} E$

$f = (X-\alpha_1) \cdots (X-\alpha_n)$

$\sigma(f) = f$ so $f = (X-\sigma(\alpha_1)) \cdots (X-\sigma(\alpha_n))$

and easy $K = F(\sigma(\alpha_1), \dots, \sigma(\alpha_n))$) □

The following result is useful for proving 21.9 with Galois theory but also important to know.

<u>Theorem 20.10 (Galois group of extensions of finite fields)</u> Let $F \subseteq E$ finite fields with $|F| = q$. Then E Galois over F and $G = Gal(E/F)$ cyclic. In fact $G = \langle \sigma \rangle$ $\sigma : \begin{array}{l} E \to E \\ \alpha \mapsto \alpha^q \end{array}$ $\alpha \in E$.

Proof / Let $p = char(F)$. The Frobenius map $\begin{array}{l} E \to E \\ \alpha \mapsto \alpha^p \end{array}$ is an iso. Since σ power of this map $\sigma \in Aut(E)$

By 21.4 we know $F = \{\alpha \in E : \alpha^q = \alpha\} = C_E(\sigma)$. By 18.20 (Artin) E Galois over F, $Gal(E/F) = \langle \sigma \rangle$. □

Continuation of 21.6 (Irreducible polys over finite fields)

Now that we know more about the subfields of finite fields we are ready to extend 21.6

For me it is more important to know what is above so I'll just extend the result and say that the proof is about 2 pages including lemmas in 21B Isaacs (check it if interested)

<u>Theorem 21.11</u> Let N denote # irred monic polys of degree n over GF(q). Then

i) $N \geqslant \frac{1}{n}\left(q^n - \sum_{\substack{r \text{ prime } (>0) \\ r \mid n}} q^{n/r}\right)$

of course irrelevant

ii) $N = \frac{1}{n} \sum_{\substack{s \text{ division of } n \\ \text{st } s \text{ product of} \\ \text{distinct primes allowing} \\ s=1}} \mu(s) q^{n/s}$; $\mu(s) = (-1)^k$ when s product of k primes.

<u>Observation</u> Let E : GF(q), then $\frac{\#\text{ irreducible polys in } E[x] \text{ of deg } n}{\#\text{ polys in } E[x] \text{ of deg } n}$ close to $1/n$ (as n gets bigger)

Justification: (imprecise statement so imprecise justification)

$\frac{\#\text{ monic irreducible polys in } E[x] \text{ of deg } n}{\#\text{ monic polys in } E[x] \text{ of deg } n} \approx 1/n$ but the numerator is N and the denominator is q^n (obviously). So our number is $N/q^n \geqslant \frac{\frac{1}{n}\left(q^n - \sum_{\substack{r \text{ prime} \\ r \mid n}} q^{n/r}\right)}{q^n} = \frac{1}{n} - \frac{\sum_{\substack{r \text{ prime} \\ r \mid n}} q^{n/r}}{n q^n} := 1/n - \varepsilon$

Since $\sum_{\substack{r \text{ prime} \\ r \mid n}} q^{n/r} \leq \sum_{i=0}^{n/2} q^i < q^{1+n/2}$ so $\varepsilon < q/nq^{n/2}$ tiny for moderately large n.

Suppose we want to find explicitly an irreducible poly of degree n over some finite field

Suppose deg 100 in GF(2). The "probability" of a random poly of degree 100 being irred is 1/100

So we just need an algorithmic procedure to decide if a poly is irred or not. With that decision alg one just picks polys at random and check. Unless we are extremely unlucky this procedure will soon produce the desired poly. A fast irreducibility alg is available and using it we can easily satisfy our goal with a computer. This alg is Berlekamp algorithm and Isaacs describes it in 21C.

Wedderburn

We conclude this section (and Isaacs ch 21) with Wedderburn's thm. (This is the only part of the course in which we do not assume commutativity).

<u>Lemma 21.21</u> Let D be a division ring, $a \in D$. Then $C_D(a) = \{x \in D : xa = ax\}$ is a subdivision ring of D and Z(D) is a subfield of D.

Proof / Elementary.

Thm 21.20 (Wedderburn) Let D be a finite division ring. Then D is commutative (so a field).

Proof/ Let $Z = Z(D)$ so that Z field by Lemma. Thus $|Z| = q$ prime power.

Let $a \in D$, $Z \subseteq C_D(a)$ thus $C_D(a)$ is a Z vs. Write $d(a) = \dim_Z(C_D(a))$. $|C(a)| = q^{d(a)}$.

In particular $|D| = q^n$, $n = d(1)$. (NTS $n = 1$).

$D^\times$ finite group. Choose S set of reps of conjugacy classes of $D^\times$ which are noncentral (it will end up being empty).

If $a \in S$ let K_a be the conjugacy class of a in $D^\times$, $|K_a| = |D^\times : C_{D^\times}(a)| = \frac{q^n - 1}{q^{d(a)} - 1} \in \mathbb{Z}$ so

Class eq

$$q^n - 1 \overset{\downarrow}{=} (q-1) + \sum_{a \in S} \frac{q^n - 1}{q^{d(a)} - 1}$$

By 21.7 $d(a) \mid n$. By 20.4 $\Phi_n(x) \mid_{\mathbb{Z}[x]} \frac{x^n - 1}{x^{d(a)} - 1}$ so each summand of is a multiple of $\Phi_n(q)$

So it follows from the above equation that (since $\Phi_n(q) \mid q^n - 1$) that $\Phi_n(q) \mid q - 1$

Thus $|\Phi_n(q)| \leq q - 1$ however by 20.17 $\Phi_n(q) > q - 1$ when $n > 1$ so $n = 1$ $\square$

VIDEO : WHAT IS "LEFT"

14. FINITENESS OF INTEGRAL CLOUSURE. (≃13.5 E,S)

Following the plan now the goal is to prove Finiteness of integral closure. We've discussed a bunch of things above but I'll write what we need now:

- i) $L=K(\alpha_1,\dots,\alpha_n)$ with each α_i separable over K then L/K separable (lemma before 19.14)
- ii) L/K Galois then $|\mathrm{Gal}(L/K)|=|L:K|$ (also we denote $\mathrm{Gal}(L/K)=\mathrm{Aut}_K(L)$) (clear)
- iii) L/K finite separable then $\exists\alpha\in L: L=K(\alpha)$ (primitive element)

"DEF" $\alpha,\beta\in L$ are conjugate over K if $\mathrm{Irr}(\alpha,K,x)=\mathrm{Irr}(\beta,K,x)$

- iv) N/K finite normal extension and $\alpha,\beta\in N$ conjugate over K then $\exists\varphi\in\mathrm{Aut}_K(N):\varphi(\alpha)=\beta$. (acción sobre raíces) essentially.
- v) Let E be any field, $G\leq\mathrm{Aut}(E)$ finite let $E^G:=C_E(G)=\{\alpha\in E:\sigma(\alpha)=\alpha\ \forall\sigma\in G\}$. Then E/E^G Galois with Galois group G. (Artin (new))

(Maybe we do not need all but Anders used i – iii to prove iv, v)

DEF Let $K\leq L$ be a finite field extension; $L=K[\alpha_1,\dots,\alpha_n]$ (since this a field $=K(\alpha_1,\dots,\alpha_n)$). Let $f(x):=\prod_{i=1}^{n}\mathrm{Irr}(\alpha_i,K,x)\in K[x]$. Consider $f(x)\in\overline{K}[x]$ (we know $\overline{L}\cong\overline{K}$ (fixing K) since both are alg closures of K so we identify them so that $L\leq\overline{K}=\overline{L}$) Write $f(x)=\prod_{j=1}^{m}(x-\beta_j)$ $\beta_j\in\overline{K}$. Then $N=K[\beta_1,\dots,\beta_m](=K(\beta_1,\dots,\beta_n))$ is called the normal clausure of L over K.

<u>Notes</u> i) Normal (clear N is a splitting field of f over K)

ii) No other E with $K\leq L\leq E<N$ is normal over K

Proof/ Suppose $K\leq L\leq E<N$ E/K normal. Note $f(x)\in K[x]$ and $\alpha_i\in E$ $f(\alpha_i)=0$ thus by teorema de la familia unida f splits over E thus $\beta_i\in E$ hence $N=K[\beta_1,\dots,\beta_m]\leq E$ ↯.

iii) Suppose that $N'\leq\overline{K}$ satisfies this property ($K\leq L\leq N'$ ∧ N'/K normal with no other....) easily we see that $N\cong N'$ (consider f...). Thus the normal clausure inside a fixed $\overline{K}$ is completely determined by this property so well defined (indep α_i) and unique inside a fixed $\overline{K}$.

(so in general unique up to iso) using $\overline{K}$ by 17.27, 17.30 above)

iv) If we start with L/K separable then by primitive element $L=K[\alpha]$ with α separable so $f=\mathrm{Irr}(\alpha,K,x)\in K[x]$ separable thus then $N[\text{roots of } f]/K$ is also separable hence N/K Galois.

v) Assume N/K finite normal field extension. Then $G:=\mathrm{Gal}(N/K)\leq\mathrm{Aut}(N)$ (finite easy) then by (previous) v) we have N/N^G is Galois.

Moreover N^G/k is purely inseparable by 19.18 See B.

· Let R be a domain. Let $K = K(R)$ fraction field. Suppose L/K is an algebraic extension. Let $\bar{R} \subseteq L$ the integral closure of R in L

<u>Claim</u> $L = K \cdot \bar{R}$ $\left(= \{ \lambda \cdot s : \lambda \in K \; s \in \bar{R} \} = K\text{-span of } \bar{R} \right)$

Proof/ Let $\ell \in L$; it is algebraic over K so $\exists$ $x^n + \frac{a_1}{b_1} x^{n-1} + \dots + \frac{a_n}{b_n} \in K[x]$ satisfied by ℓ $(a_i, b_i \in R \;\; b_i \neq 0)$. Note $b_1 \cdots b_n \ell \in \bar{R}$ thus $\ell = \underbrace{(b_1 \cdots b_n)^{-1}}_{\in K} \underbrace{(b_1 \cdots b_n x)}_{\in \bar{R}}$ □

<u>Theorem 66 (Finiteness of integral closure)</u>

Let R be a domain, which is a finitely generated k-algebra over a field k (any!). (affine domain over k). Let $K = K(R)$ its field of fractions. Consider $K \subseteq L$ finite field extension. Then $\bar{R}^L$ is a finitely generated R-module. In particular $\bar{R}^L$ domain fg k-algebra.

Proof/ For the in particular: $\bar{R}^L \subseteq L$ field so domain. Let $s_1, \dots, s_n$ generate $\bar{R}^L$ as an R-module then $\bar{R}^L = Rs_1 + \dots + Rs_n \overset{\uparrow}{\subseteq} k[a_1, \dots, a_m, s_1, \dots, s_n] \subseteq \bar{R}^L$. So fg as a k-alg.

$R = k[a_1, \dots, a_m]$

<u>STEP 1</u> We may assume $R = k[x_1, \dots, x_n]$ poly ring so K is the field of rational functions $k(x_1, \dots, x_n)$)

By Noether normalization $\exists S \subseteq R$ subring (k-subalgebra) st R is fg S-module and $S \underset{k\text{-alg}}{\cong} k[x_1, \dots, x_n]$ poly ring over k. Let $T = K(S)$ field of fractions $\underbrace{T \subseteq K}_{\text{finite}} \underbrace{\subseteq L}_{\text{finite}}$ (*) then by assumption $\bar{S}^L$ fg S-module.

$\bar{S}^L = \{ \ell \in L : \ell \text{ integral over } S \} = \bar{R}^L = \{ \ell \in L : \ell \text{ integral over } R \}$

$\subseteq$) ✓

$\supseteq$) $\bar{R}^L$ integral over R. By L43, C44 R is integral over S thus $\bar{R}^L$ integral over S

Thus $\bar{R}^L$ fg S-module so fg R-module.

(*) Suppose $R = Sa_1 + \dots + Sa_n$. Then $K(R) = K(S)(a_1, \dots, a_n)$

$\supseteq$) ✓

$\subseteq$) Let $y \in K(R)$. Then $\exists b \in R \setminus \{0\} : by \in R$ thus $b, by \in K(S)(a_1, \dots, a_n)$ which is a field so $y \in K(S)(a_1, \dots, a_n)$

Since $a_i \in R$ integral over S, a_i are alg over $K(S)$ thus $K(R)$ finite over $K(S)$ (exal) □

STEP 2 We may assume that L/K is a normal field extension.

Assume it is proved in that case. Consider $K \subseteq L \subseteq N$ the normal closure of L over K. Note it is finite so $\overline{R}^N$ is fg as an R-module. $R = k[x_1, \ldots, x_n]$ is Noetherian so $\overline{R}^N$ Noeth R-module by Imp ex before prop 18. Now $\overline{R}^L$ is a submodule of $\overline{R}^N$ so also fg R-module

So NTS that if $R = k[x_1, \ldots, x_n]$, $K = k(x_1, \ldots, x_n)$, L/K normal then $\overline{R}^L$ fg R-module.

Let $G = Gal(L/K)$; $L = K(\beta_1, \ldots, \beta_n)$ so by "Acción sobre raíces" $Gal(L/K)$ finite. By note w/
$R \subseteq K \subseteq L^G \subseteq L$. Let $T = \overline{R}^L \cap L^G \; (= \overline{R}^{L^G})$

$$\underset{\substack{\text{purely}\\ \text{unsep.}}}{K \subseteq L^G} \qquad \underset{\text{Galois}}{L^G \subseteq L}$$

(below we see T normal, $K(T) = L^G$)

Claim T is a finitely generated R-module (and noetherian)

If $L^G = K$ then $T = \overline{R}^L \cap K = \overline{R}^K = R$, $R = k[x_1, \ldots, x_n]$ UFD so normal domain by prop 50 so the assertion is obvious. Thus we suppose that $L^G \neq K$ so $K \subsetneq L^G$.

Since this extension is purely inseparable by sec B necessarily $\text{char}(K) \overset{\text{char}(k)}{=} p \neq 0$. Now L/K finite so L^G/K too and thus $L^G = K(\alpha_1, \ldots, \alpha_d)$ for some $\alpha_i \in L^G$. Now by 19.10 sec B $\exists r \in \mathbb{N}$: if $q = p^r$ then $\alpha_i^q \in K \; \forall i \in \{1, \ldots, d\}$

Now since $K = k(x_1, \ldots, x_n)$, $\alpha_i^q = \dfrac{g_i(x_1, \ldots, x_n)}{h_i(x_1, \ldots, x_n)} =: f_i$ with $g_i(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$, $h_i(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n] \setminus \{0\}$.

So $L^G = K(\sqrt[q]{f_i}, \ldots, \sqrt[q]{f_m})$ (note in char p we have that Frob endomorphism is injective so clear notation)

Define $k' = k$(qth roots of coefficients of g_i, h_i). Consider now $x_i \in K$, let $K[y]$ poly ring $\exists$ extension such that $y^q - x_i$ has a root and in this extension the root is unique (Frobenius) we write $x_i^{1/q}$. Consider now $k'(\sqrt[q]{x_1}, \ldots, \sqrt[q]{x_n}) \supseteq K$ and also $\exists g_i \in k'(\sqrt[q]{x_1}, \ldots, \sqrt[q]{x_n}) : g_i^q = f_i$ $\quad ((a+b)^q = a^q + b^q)$

Thus by doing surgery $L^G \subseteq k'(\sqrt[q]{x_1}, \ldots, \sqrt[q]{x_n})$

Now note $\overline{R}^{L^G} \subseteq k'[\sqrt[q]{x_1}, \ldots, \sqrt[q]{x_n}]$ (if $\overset{e}{\text{something}}$ in L^G is integral over R means that $e^k + f_{k-1}(x_1, \ldots, x_n) e^{k-1} + \cdots + f_0(x_1, \ldots, x_n) = 0$ and this e can be expressed as quotients products sums of polys in $k[x_1, \ldots, x_n]$ and "polys" in $(x_i)^{1/q}$ with coef in k'. By clearing out denominators the inclusion is clear)

Now $K'[\sqrt[q]{x_1}, -, \sqrt[q]{x_n}]$ is a finitely generated R-module (gen by qth roots of coef of g_i, h_i and $\sqrt[q]{x_i}$)

Since R noeth and $T = \overline{R}^{L^G}$ R-submodule, T is also noetherian □

Note that T is normal. $T = \overline{R}^{L^G}$, now the field of fractions of $L^G = L^G$ since it is already a field so it is clear that $\overline{T} = T$ in its field of fractions

If we prove that $\underset{\overline{\overline{R}^{L^G}}^{L}}{\underset{\parallel}{\overline{T}^L}}$ fg T module we have that $\overline{R}^L$ fg T-module

Proof/ $\overline{R}^L \subseteq \overline{T}^L$ easily. T integral over R, $\overline{T}^L$ integral over T so $\overline{T}^L$ integral over R thus $\overline{T}^L \subseteq \overline{R}^L$.

And T is a fg R module so it will follow that $\overline{R}^L$ fg R-module.

(Obvious but let's see it: $\overline{R}^L = Ta_1 + \dots + Ta_t$ for $a_i \in \overline{R}^L$, $T = Rb_1 + \dots + Rb_s$ $b_i \in T$

so $\overline{R}^L = + Rb_ja_i$ with $b_ja_i \in \overline{R}^L$ since $T \subseteq \overline{R}^L$

So NTS $\overline{T}^L$ fg T-module. Suppose we prove in general:

{Claim T Noetherian normal ring, $K(T) \subseteq L$ finite separable then $\overline{T}^L$ fg T-module

Then going back to our situation, since $\underbrace{K \subseteq K(T) = L^G}_{\text{finite}} \subseteq L$, $K(T) \subseteq L$ is finite and separable (see above)

so by the claim we would be done.

→ $T \subseteq L^G$ field so $K(T) \subseteq L^G$. Let $s \in L^G$ then by clearing denominators s is a root of some nonzero poly over R. Let a be the leading coeff. Check that as integral over R. Thus $as \in T$ so $s = t/a$ with $t \in T$, $a \in R \subseteq T$. //

multiply poly by $a^{\text{deg poly} - 1}$.

We will prove the claim as a separate proposition

Proposition 67 Let R be a noetherian normal ring, $K = K(R)$, $K \subseteq L$ finite separable extension Then $\overline{R}^L$ is a fg R-module

Proof/ Arguing exactly as in step 2 of the last proof we may assume that L/K is normal. Let $G = Gal(L/K) = \{\sigma_1, -, \sigma_n\}$ (finite extension; $|Gal(L/K)| = |L:K|$). By the claim before the last theorem $L = span_K \overline{R}^L$

Now L is a fdim K vs and $\overline{R}^L$ spans so $\exists\, b_1, -, b_n \in \overline{R}^L$ K-basis of L. Set

$$M = \begin{bmatrix} \sigma_1(b_1) & \sigma_1(b_2) & \cdots & \sigma_1(b_n) \\ \vdots & & & \\ \sigma_n(b_1) & \sigma_n(b_2) & \cdot & \sigma_n(b_n) \end{bmatrix} \in M_n(\overline{R}^L)$$

. By Dedekind (Ecal) $\{\sigma_1, -, \sigma_n\}$ are K li

easy to see that if $\alpha \in \overline{R}$, $\sigma \in Gal(L/K)$, $\sigma(\alpha) \in \overline{R}$ (just write the poly)

So $\det(M) = d \in \overline{R}$ is nonzero (if zero the linear dependence of rows would contradict

Claim $\overline{R}^L \subseteq R\frac{b_1}{d^2} + \dots + R\frac{b_n}{d^2}$ (If we prove this $\overline{R}^L$ R-submodule of a fg R-module; since R is noeth we are done (fg R-modules are noeth))

Pf/ It is clear that $\sigma_i(d) = \pm d$
$\hookrightarrow$ determinant of a permutation of rows of M.

Thus $\sigma_i(d^2) = d^2$ so $d^2 \in$ Fixed field of the Galois extension so $d^2 \in K$.

Let $x \in \overline{R}^L$ then $x = c_1 b_1 + \dots + c_n b_n$ with $c_i \in K$. Now $x = d^2 c_1 \frac{b_1}{d^2} + \dots + d^2 c_n \frac{b_n}{d^2}$

and observe

$$M\begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} = \begin{bmatrix} \sum_{j=1}^{n} \sigma_1(b_j)c_j \\ \vdots \\ \sum_{j=1}^{n} \sigma_n(b_j)c_j \end{bmatrix} \underset{\substack{\downarrow \\ \sigma_i \text{ fixes } K}}{=} \begin{bmatrix} \sigma_1(x) \\ \vdots \\ \sigma_n(x) \end{bmatrix} \in \left(\overline{R}^L\right)^n \quad \text{since } \sigma_i(x) \in \overline{R}^L \text{ (as above)}$$

Multiplying by the $\overset{\in M_n(\overline{R}^L)}{\text{cofactor}}$ matrix (see lin alg notes for alg qual thm 3c) we get $d\begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} \in \left(\overline{R}^L\right)^n$

So $dc_i \in \overline{R}^L$. Thus $d^2 c_i \in \overline{R}^L$ since $d \in \overline{R}^L$; but $d^2 \in K$, $c_i \in K$ so

$d^2 c_i \in \overline{R}^L \cap K = R$
$\hookrightarrow$ integral closure of R in K but R normal

So $x = d^2 c_1 \frac{b_1}{d^2} + \dots + d^2 c_n \frac{b_n}{d^2}$ with $d^2 c_i \in R$, as wanted □ ▨

Example (number theory) Let $\mathbb{Q} \subseteq L$ (number field) finite extension. Let $\overline{\mathbb{Z}}^L \subset L$ (number ring) integral closure by thus, $\overline{\mathbb{Z}}$ is a fg $\mathbb{Z}$ module. (no torsion elements so free and thus noetherian)

Geometry discussion (This discussion is essentially saying more about the map π we consider between X and its normalization at the end of sec 9 but with more generality thanks to the geometry discussion after that). (Again I try to be as clear as possible but this should be taken as "see how this is used" "mot. for alg geo". Rather than Alg geo.)

- Fix $k = \overline{k}$, let A affine domain over k (in part reduced affine k-alg) we saw that $A \cong k[x_1, \dots, x_n]/_I$ as k-algebras where I radical (and prime since A domain) and we established a bijection $Z(I) \subseteq \mathbb{A}^n \longleftrightarrow \text{spec-m}(A) =: X$ which preserved
$a \longmapsto I(\{a\})/_I$ inside A (max ideal)

regular functions (this in alg geo will mean iso varieties) and $Z(I)$ note is an irred alg set

Now we can consider $\overline{A} \subseteq K(A)$ the normalization of A. By finiteness of integral closure $\overline{A}$ affine domain over K. Set $\overline{X} = \text{spec-m}(\overline{A})$ and as above this is also "an irred alg set"

Now we have a k-alg hom $A \xrightarrow{inc} \bar{A}$ and following the last geometry discussion before sec 12

This gives $\pi : \bar{X} \to X$ (If we translate this to pure alg sets this would be the π in the previous disc.)
$Q \longmapsto Q \cap A$ See from previous discussions

And now we can say a bit more about π.

· <u>π is surjective</u> By Going up ($A \subseteq \bar{A}$ is an integral ext of rings so) $\forall P \in$ spec-m $(A) = X$
$\exists Q \in \mathrm{Spec}(\hat{A})$ st $P = Q \cap A$. Now by incomparability $Q \in$ spec-m $(\bar{A}) = \bar{X}$.
So $\pi(Q) = P$. //

· <u>π has finite fibers</u> ie $\pi^{-1}(P)$ finite $\forall P \in X$

Note $Q \in \pi^{-1}(P)$ iff $Q \supseteq P \cdot \bar{A}$. By incomparability Q must be minimal over $P \cdot \bar{A}$

(if not $\exists S \subsetneq Q$ prime: $P \cdot \bar{A} \subseteq S \subsetneq Q$. Now (by i) in incomparability S is maximal ↯)

So $\pi^{-1}(P) \underset{(=)}{\subseteq} \mathrm{Ass}\left(\bar{A}/_{P \cdot \bar{A}}\right)$ we know it is finite. ($\bar{A}$ noetherian ; quotient of poly ring) //

as above, so X irred.

↙ If A is a coord ring this is easier to interpret so picture that. This generalizes.

· <u>Almost bijective</u> Let $0 \neq f \in A$ (see Geometry disc before sec 12) $X_f = \{P \in X : f(P) \neq 0\}$ (here ‾ means normaliz. not closure)

<u>Claim</u>: X_f is homeomorphic to spec-m (A_f)

By prop 8 $\mathrm{Spec}(A_f) \longrightarrow \{P \in \mathrm{Spec}(A) : f \notin P\}$ bijection (bicont is easy)
$U \longmapsto U \cap A$ (notation of prop 8)

This restricts to spec-m $(A_f) \to \{P \in$ Spec-m $(A) : f \notin P\} = X_f$, see def of $f(P)$.

Now $\bar{A}$ is a finitely generated A-module in particular we have that

$\bar{A} = A[g_1/h_1, \dots, g_r/h_r] \subseteq K(A)$. Set $f = h_1 \cdots h_r$

Then $(\bar{A})_f \underset{\substack{\downarrow \\ \text{easy.}}}{=} A_f \subseteq K(A)$ (we've already discussed why is important to say $\subseteq K(A)$)). But since normalization commutes with loc (prop 53) this is saying that A_f is normal. Thus if we identify X_f with spec-m (A_f) we have $X_f = \overline{X_f}$ in the language from above. (this is reading spec-m $(A_f) = \overline{\text{spec-m}(A_f)}$)

So if we look at $\pi : \underset{\text{" spec-m}(\bar{A})}{\bar{X}} \longrightarrow X$ what can we say?

↙ this refers to normalization, not closure

<u>Claim</u> $X_f \subseteq X$ is a dense open subset. (similarly $\overline{\text{spec-m}(A_f)} \subseteq \overline{\text{spec-m}(A)}$ dense open)

We have to see $X \setminus X_f = \{P \in X : f(P) = 0\}$ is closed in spec-m (A) with the subspace topology

But this is $\{P \in X : f \in P\} = Z(\{f\}) \cap$ spec-m (A) closed

Now dense. X is irreducible as a topological space with Zariski top (induced) (See homeomorphism in geom. discussion before sec 12)

So if $\mathrm{cl}(X_f) \neq X$ then $X = \mathrm{cl}(X_f) \cup (X \setminus X_f)$ ↯ irred. (nonempty open in irred top. space is dense).

So we have

$$\begin{tikzcd}
\pi : \overline{X} \arrow[r] \arrow[d, phantom, sloped, "\supseteq"] & X \arrow[d, phantom, sloped, "\supseteq"] \\
\overline{X_g} \arrow[r, phantom, "\cong"] & X_g
\end{tikzcd}$$

So the map π is a homeo in dense (Zariski) open subset. So most places is biject //

$\downarrow$ $X_g \cong \text{spec-m}(A_g) = \overline{\text{spec-m}(A_g)} = \overline{X_g}$

via this

(chare of the dam)

what we are denoting by

Again the philosofy of these discussions is trying to see what happens with the geometry by getting our hands dirty and exploring from what we know maybe adding some extra concepts (not in this case). But not presenting alg geo in a very organized and structured way. (It will come natural after).

15. GRADED RINGS/MODULES & HILBERT POLYNOMIALS

(~ Eis 1.5, 1.9)

DEF A graded ring is a ring R together with a direct sum decomposition

$R = R_0 \oplus R_1 \oplus \cdots$ as abelian groups (meaning that $\forall r \in R$ we can write it uniquely as finite sum of … so on/ideal)

such that $R_i R_j \subseteq R_{i+j}$. A homogeneous element of R is an element of R_i. A homogeneous ideal is an ideal generated by homogeneous elements

call it homogeneous components of r

Example i) $k[x_1, -, x_n] = R$. If the monomials of $f \in R$ are all of the same degree we say f is homogeneous. Let $R_d = \{$homogeneous polys of degree $d\}$. (k-vector space) "Graded by degree"

ii) If R graded, $1 \in R_0$ (Easy exercise by contradiction)

DEF If R is a graded ring $R = R_0 \oplus R_1 \oplus \cdots$, then a graded R-module M is an R-module M with a dec $M = \bigoplus_{d \in \mathbb{Z}} M_d$ as abelian groups ($\forall m \in M\ \exists!$ expression as finite sum…) such that $R_i \cdot M_j \subseteq M_{i+j}$. If $N \subseteq M$ R submodule we say that it is a graded submodule if

$\bigoplus_{d \in \mathbb{Z}} N \cap M_d = N$, so it inherits a graded R-module structure.

In this case $M/N \cong \bigoplus_d M_d/N_d$ also graded. (inherits structure of graded via that iso of R-modules (external))

If M, N are two graded R-modules $\varphi : M \to N$ R-hom is said to be a graded hom of degree d if $\varphi(M_n) \subseteq N_{n+d}$ $\forall n$. If $\varphi : M \to N$ is a bijective graded hom of deg 0 we say they are isomorphic as graded R-modules. (Same notion for rings)

DEF If M is a fg graded module over $R = \mathbb{K}[x_1, -, x_n]$ (with grading by degree) the function

(M fg $\wedge$ M graded.) (field)

$$H_M : \mathbb{Z} \longrightarrow \mathbb{N}$$
$$d \longmapsto H_M(d) = \dim_{\mathbb{K} = R_0}(M_d)$$

is called the Hilbert function of M.

Note if M, N are iso as graded R-modules $H_M = H_N$.

Exercise: Show that above $\dim_{\mathbb{K}}(M_d) < \infty$.

- STEP 1 Finitely generated graded means that as an R-module is generated by finitely many elements.

Let $\{m_1, -, m_n\}$ generate M as an R-module. Then each m_i is sum of homogeneous polynomials $m_i^1, -, m_i^{k_i}$. $\{m_1^1, -, m_1^{k_1}, m_2^1, - - -\}$ are homogeneous and generate M as an R-module

STEP 2 We may asume that $\{m_1, \dots m_t\}$ homogeneous they generate M as an R-module. We may assume that $\forall i \leq e$, $m_i \in M_{d_i}$ with $d_i \leq d$ and $\forall j > e$ $m_j \in M_{d_j}$ with $d_j > d$. For each $m_i \in M_{d_i}$ we have that for any monic monomial of degree $d - d_i$, that monomial $\cdot m_i \in M_d$. We have finitely many such monomials for each m_{d_i}, I claim that all of these generate M_d as a k-vector space. Indeed if $n \in M_d$, then $\exists f_1, \dots, f_t \in k[x_1, \dots, x_n]$: $n = f_1 m_1 + \dots + f_t m_t$. Write f_i as sum of homogeneous polys and rewrite as

$n = g_{i_1} m_{i_1} + \dots + g_{i_s} m_{i_s}$ with g_{i_j} homogeneous, $g_{i_j} m_{i_j} \neq 0$., $\{m_{i_j}\} \subseteq \{m_1, \dots, m_t\}$.

Now it is obvious that $\{m_{i_j}\} \subseteq \{m_1, \dots, m_e\}$. Since each g_{i_1} is a k-linear combo of $\overset{\text{monic}}{\text{monomials}}$ of the apropiate degree it follows that n is a k-linear combo of our prefixed elements.

DEF We denote $\binom{X}{r} = \frac{X(X-1)\cdots(X-r+1)}{r!} \in \mathbb{Q}[X]$ for $r \in \mathbb{N}$. $\binom{X}{0} := 1$.

Note i) $\{\binom{X}{r} : r \in \mathbb{N}\}$ is a basis of $\mathbb{Q}[X]$ as a $\mathbb{Q}$-vspace. $\binom{X}{r}$ is monic of degree r so it is clear.

ii) $\sum_{i=0}^{m} \binom{i}{r} = \binom{m+1}{r+1}$ by induction where by convention $\binom{i}{r} = 0$ if $r > i$. $(i, m, r \in \mathbb{Z}_{\geq 0})$

Lemma 68 (Combinatorial) Let $H : \mathbb{N} \to \mathbb{Z}$ any function, define $\Delta H : \mathbb{N} \longrightarrow \mathbb{Z}$

$d \longmapsto H(d+1) - H(d)$

Then $H \in \mathbb{Q}[X]$ iff $\Delta H \in \mathbb{Q}[X]$. (meaning you can compute H by evaluating at some $f \in \mathbb{Q}[X]$)

Proof / $\rightarrow$) Clear

$\leftarrow$) Suppose $\Delta H(n) = f(n)$ for some $f \in \mathbb{Q}[X]$ then write $f(x) = \sum_{r=0}^{d} a_r \binom{x}{r}$ $a_r \in \mathbb{Q}$.

$$\text{Now } H(n) = H(0) + \sum_{i=0}^{n-1} \Delta H(i) = H(0) + \sum_{i=1}^{n-1} \left(\sum_{r=0}^{d} a_r \binom{i}{r} \right) = H(0) + \sum_{r=0}^{d} a_r \left(\sum_{i=0}^{n-1} \binom{i}{r} \right) =$$

$$= H(0) + \sum_{r=0}^{d} a_r \binom{n-1}{r+1} = g(n) \text{ where } g(x) = H(0) + \sum_{r=0}^{d} a_r \binom{x}{r+1} \in \mathbb{Q}[X].$$ □

The next exercise shows why $\{\binom{x}{r}\}$ is a good basis.

Exercise Let $H(x) = \sum_{r=0}^{d} a_r \binom{x}{r} \in \mathbb{Q}[X]$. TFAE
i) $a_r \in \mathbb{Z}$
ii) $H(m) \in \mathbb{Z}$ $\forall m \in \mathbb{Z}$
iii) $H(m) \in \mathbb{Z}$ $\forall m \in \mathbb{N}$, $m >> 0$ sufficiently large

Proof: Start by observing that $\Delta H(x) = \sum_{r=0}^{d} a_r \binom{x+1}{r} - \sum_{r=0}^{d} a_r \binom{x}{r} = \sum_{r=0}^{d} a_r \left(\binom{x+1}{r} - \binom{x}{r} \right) =$

$$\sum_{r=1}^{d} a_r \left(\binom{x+1}{r} - \binom{x}{r} \right) \underset{\downarrow}{=} \sum_{r=1}^{d} a_r \binom{x}{r-1} = \sum_{r=0}^{d-1} a_{r+1} \binom{x}{r}$$

Just check

$i \rightarrow ii$) Obvious, $\binom{m}{r} \in \mathbb{Z}$; $ii \rightarrow iii$) obvious. Now assume iii) we try to prove i); $\forall m \geq M \in \mathbb{N}$, $H(m) \in \mathbb{Z}$ thus $\Delta H(m) \in \mathbb{Z}$ for any m bigger than some constant. Now thus again implies that $\Delta\Delta H(m) \in \mathbb{Z}$ $\forall m$ bigger than some constant but thus is $\sum_{r=0}^{d-2} a_{r+2} \binom{x}{r}$. We keep applying this until we get that $\sum_{r=0}^{d-(d-1)} a_{r+d-1} \binom{x}{r}$ is integer valued for m suff large but this is $\sum_{r=0}^{1} a_{r+d-1} \binom{x}{r} = a_{d-1} + a_d x$ is integer valued for m suff large. We apply Δ one last time and get $T(x) = a_d$ integer valued for m suff large so $a_d \in \mathbb{Z}$.

Now we substract $H(x) - a_d \binom{x}{d}$ and again is integer valued for suff large m. So applying the same $a_{d-1} \in \mathbb{Z}$ $\square$

<u>Theorem 6.9 (Hilbert)</u> Let $R = k[x_1, \dots, x_n]$, k field and R graded by degree. Let M be fg graded R-module. Then $\exists P_M(x) \in \mathbb{Q}[x]$ such that $H_M(d) = P_M(d)$ $\forall d \gg 0$

$(\exists n_0 : \forall n \geq n_0 \; H_M(n) = P_M(n))$

This polynomial is called Hilbert polynomial of M.

Grading of R relevant: $R = k[x]$. Set $\deg x = 2$ meaning $R_2 = \{\lambda x : \lambda \in K\}$ we can define the rest of R_i naturally so that we have a grading in R. Note that $R_i = 0$ for i odd and $\dim R_j = 1$ for j even. If $M = R$ $P_M(x)$ is not a poly.

<u>Note</u> Write $P_M(x) = \sum_{r=0}^{d} a_r \binom{x}{r}$ ($\exists ! \; a_0, \dots, a_r \in \mathbb{Q}$ satisfying this). By the exercise $a_0, \dots, a_d \in \mathbb{Z}$ and these are important invariants of M as a graded R-module. (Two iso as graded modules give the same)

Proof/ We work by induction on n. For $n = 0$, M is a f dimensional vspace over k so take $P_M(x) = 0$. Now suppose $n \geq 0$. Let us consider the following hom $M \xrightarrow{\cdot x_n} M$. Let $\underline{K} = \ker(\cdot x_n)$ and note $\cdot x_n(M) = x_n M$ so we get the following exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \underline{K} \arrow[r] & M \arrow[r, "\cdot x_n"] & M \arrow[r] & M/x_n M \arrow[r] & 0 \end{tikzcd}$$

Now since we are multiplying by homogeneous poly, $\underline{K}$, $x_n M$ are graded submodules. So we can take $d \in \mathbb{N}$ and consider this same exact sequence starting in $\underline{K}_d$

$$\begin{tikzcd} 0 \arrow[r] & \underline{K}_d \arrow[r] & M_d \arrow[r, "x_n \cdot"] & M_{d+1} \arrow[r] & (M/x_n M)_{d+1} \arrow[r] & 0 \end{tikzcd}$$

$$M/x_n M \cong \bigoplus_{d \in \mathbb{Z}} M_d/(x_n M)_d = \bigoplus_{d \in \mathbb{Z}} M_d / x_n M \cap M_d$$

This is a short exact sequence of k-vector spaces so

$$\dim_k M_d = \dim_k((x_n M_d)) - \dim_k(\underline{K}_d)$$

$$\dim_k M_{d+1} = \dim_k((M/x_n M)_{d+1}) - \dim_k(x_n M_d)$$

Now, $\underline{K} = \bigoplus_{d \in \mathbb{Z}} \underline{K} \cap M_d = \bigoplus_{d \in \mathbb{Z}} \underline{K}_d$ R-submodule. Now R is noeth so M is noeth thus $\underline{K}$ is also fg $k[x_1, \dots, x_n]$-module and it inherits a fg $k[x_1, \dots, x_{n-1}]$ graded module structure with the same grading (direct sum dec. mult by x_n gives 0). Now $M/x_n M$ is also fg as an R-module and it has a graded R-module structure via $M/x_n M \cong \bigoplus_{d \in \mathbb{Z}} M_d / x_n M \cap M_d$. Of course this is also a graded $k[x_1, \dots, x_{n-1}]$ module with the same grading. It now follows that

Thus $\Delta H_M(d) = H_{M/x_n M}(d+1) - H_{\underline{K}}(d) = P_{M/x_n M}(d+1) - P_{\underline{K}}(d)$ by induction (and because the grading as $k[x_1, x_{n-1}]$ is the same) for $P_{M/x_nM}(x) \in \mathbb{Q}[x]$, $P_{\underline{K}}(x) \in \mathbb{Q}[X]$ for d suff large. It follows that

$\Delta H_M(d)$ is given by evaluation at a rational poly for d suff large. $\square$

For what we did here, Eisenbud introduces "shifting".

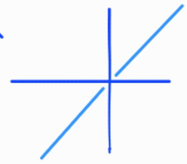
What can we use this for?

BASIC PROJECTIVE VARITIES (~1.9)

(~1.9 (This section is: We introduce $\mathbb{P}^n$ and we see how the previous section is useful to define dimension; which we will study shortly)

Let $k = \bar{k}$, denote $k^* := k - \{0\}$ as a mult. group. Let k^* act on $\mathbb{A}^{n+1} \setminus \{0\}$ by $t \cdot (a_0, -, a_n) = (ta_0, -, ta_n)$

$\mathbb{P}^n = (\mathbb{A}^{n+1} \setminus \{0\}) / k^*$ (set of all orbits). These orbits are lines through the origin and the origin has been removed. (This language is common. "Consider a point in $\mathbb{P}^n$ of homogeneous coord. $a_0, -, a_n$" This means $p \in \mathbb{P}^n$ st $(a_0, -, a_n)$ is in the line p. Defined up to scalar)



The map $\pi : \mathbb{A}^{n+1} \setminus \{0\} \longrightarrow \mathbb{P}^n$ is useful to think about when confused. (He said something like "if you cant understand something for $\mathbb{P}^n$ you translate it to $\mathbb{A}^{n+1}$ via π and it becomes simple to understand)

Let $I \subseteq S = k[x_0, -, x_n]$ homogeneous ideal (S graded by degree) then if we consider $Z(I)$ this set is k^* stable. Meaning that if $(a_0, -, a_n) \in Z(I)$ then $\forall \lambda \in k^*$, $\lambda \cdot (a_0, -, a_n) \in Z(I)$

We now define $Z(I) := Z(I)/_{k^*} \subseteq \mathbb{P}^n$ and these sets are called projective algebraic $\overset{\text{sub}}{\text{sets}}$ (or alg subset of proj. space)

Here there is some overlap in notation. It will be clear from context. $Z(I)$ always $\subseteq \mathbb{A}^n$. $Z(I)$ ideals or proj alg set

Note $Z(I) = \{ (a_0, \ldots, a_n) \in \mathbb{P}^n : f(a_0, -, a_n) = 0 \ \forall f \in I \text{ homogeneous} \}$

denotes a line; so homog coord.

also write $(a_0 : \cdots : a_n)$

so that this is well defined

- If $X \subseteq \mathbb{P}^n$ any subset, define $I(X) := I(\pi^{-1}(X) \cup \{0\}) \subseteq S$ is a homogeneous ideal of S. (easy).

Let $X \subseteq \mathbb{P}^n$ projective algebraic subset then $S/_{I(X)}$ by the previous section this has a natural graded module structure. (Note S is a graded module over S, $I(X)$ as homogeneous ideal is a graded submodule) It's called projective coord ring. We can now consider $P_{S/I(X)}(x) \in \mathbb{Q}[x]$ the Hilbert polynomial and we call it $P_X(x)$; the Hilbert polynomial of $X \subseteq \mathbb{P}^n$. We can write it as $a_0 + a_1 \binom{x}{1} + \cdots + a_d \binom{x}{d} \in \mathbb{Q}[x]$, $a_d \neq 0$. We could "define" $\dim(X) = d$, $\deg(X) = a_d \in \mathbb{N}$.

meaning that we do not fix it for the rest of the course.

This is our first attempt to define dimension. We will explore dimension thy later on.

We did not end up making sense of this in this course; but is not bad. (Gathan, Nathan ...)

- Anders and Eisenbud both say that the proj coord ring depends on "the embedding of X in $\mathbb{P}^n$". I think this is something like: You can have "iso projective varieties" with their proj coord rings not iso as rings. Think of $X \subseteq \mathbb{P}^3$ now see it as $\subseteq \mathbb{P}^4$. The proj coord rings may not be iso. He said that $\dim(X)$ is indep of "embedding" but one needs to prove that. He mentions, degree depends on "embedding".

I will learn more about these things in alg geo where the previous paragraph will make sense.

Exercise: $X \subseteq \mathbb{P}^n$ finite. In this case $P_X = |X|$. So $\dim X = 0$ so $\deg X = |X|$.

For computing the degree we mention:

Bezout's theorem Let $h_1, \dots, h_r \in S = \overset{\text{we fixed } k = \bar{k}}{k}[x_1, \dots, x_n]$ homogeneous of degree $\deg(h_i) = d_i$. Let $I = \langle h_1, \dots, h_r \rangle \subseteq S$

Assume $\dim Z(I) = n - r$, $Z(I) \subseteq \mathbb{P}^n$ Then $\deg(S/I) = d_1 \cdots d_r$

(if equations non redundant, cut by one equation, reduce dim by one)

This is: I is hom ideal so S/I graded S-module; take its hilbert polynomial and write it as $a_0 + a_1\binom{x}{1} + \dots$ $\dots + a_m\binom{x}{m}$. Then we mean a_m

- If $X = Z(I) \neq \emptyset$ then $I(X) = \sqrt{I}$ so $\deg(X) = \deg(S/\sqrt{I})$

so if $I = \sqrt{I}$ we get $\deg(X)$.

(Proj. Nullst)

Proof: $I(X) = I(\pi^{-1}(Z(I)) \cup \{0\})$

$= I(Z(I) \cup \{0\}) =$

Now I gen by hom polys and non empty so $Z(I) = Z(f_1, \dots, f_m)$ for $f_1, \dots, f_m \in k[x_0, \dots, x_n] \setminus k$ homogeneous

Thus $0 \in Z(I)$

$= I(Z(I)) \underset{\text{nullst}}{\overset{}{=}} \sqrt{I}$.

He talked about what happens in non alg closed (too much for now).

- All in all we've seen how hilbert polys are useful to define dimension of proj alg sets. These $Z(I)$, the previous $Z(I)$, $Z(I)$ are all something called varieties (will study in alg geo) and this was just a first touch. Also we'll soon start covering dimension theory so this was also a first attempt.

This and much more things about proj space.

We go back to our generalities (and attempting to give them some meaning).

16 FILTRATIONS AND BLOW UPS

(~ ch 5 Eis.)

DEF Let R be a ring, (sums of ...) $I \subseteq R$ ideal. We define the associated graded ring of R wrt I.

$$gr_I(R) = \bigoplus_{j \geq 0} I^j/I^{j+1} \quad (I^0 = R)$$

where mult is $\left(\begin{array}{l} a \in I^m, b \in I^n \text{ then } \bar{a} \in I^m/I^{m+1}, \bar{b} \in I^n/I^{n+1} \\ \bar{a}\bar{b} := \overline{ab} \in I^{n+m}/I^{n+m+1} \text{ and extend this naturally} \end{array} \right)$

this is defined as a external direct sum but we view its elements as formal sums with finitely many nonzero terms. So that this is actually graded and $I^j/I^{j+1} \subseteq gr_I(R)$

So we have a graded ring.

Examples i) $R = k[x_1, \dots, x_n]$, $I = \langle x_1, \dots, x_n \rangle$. Note $I^j = \operatorname{Span}_{\mathbb{K}}\{x_1^{a_1} \cdots x_n^{a_n} : \sum a_i \geq j\}$

From this $I^j/I^{j+1} =$ "{forms of degree j}" and $gr_I(R) \cong k[x_1, \dots, x_n]$

ii) Let $R=k[x,y]$, $I=\langle xy\rangle \subseteq R$ then $gr_I(R) \supseteq R/_I$ not domain.

iii) R local ring with max ideal I, I fg. Then $gr_I(R)$ affine ring over $K=R/_I$ (graded)

(it was not said but I guess that $gr_I(R) \underset{\text{as graded rings}}{\cong} k[x_1,\dots,x_n]/_J$ ← natural grading)

<u>DEF</u> Let $I\subseteq R$ ideal, M an R-module. An **I-filtration of M** is a filtration (chain)

$M=M_0\supseteq M_1\supseteq M_2 \dots$ M_i submodules such that $IM_j\subseteq M_{j+1}$.

We say that it is **I-stable** if $\forall j\gg 0$ $IM_j=M_{j+1}$.

<u>Note</u> If $M_{j+1}=IM_j$ $\forall j\geq n$ then the filtration is determined by $M_0,\dots,M_n,I$.

<u>DEF</u> Let $J: M=M_0\supseteq M_1\dots$ be an I-filtration we define $gr_J M \overset{\text{same consideration as above.}}{=} \bigoplus_{j\geq 0} M_j/_{M_{j+1}}$

We make **$gr_J(M)$** into a graded $gr_I(R)$-module.

Let $a\in I^s$, $m\in M_t$ consider $\bar{a}\in I^s/_{I^{s+1}}$, $\bar{m}\in M_t/_{M_{t+1}}$

Since we have I filt $am\in M_{s+t}$

So we define $\bar{a}\bar{m}=\overline{am}\in M_{s+t}/_{M_{s+t+1}}$ (well def..)

(the remaining operations; natural)

Prop70 Let M be fg R-module. Let $J: M=M_0\supseteq M_1\dots$ I stable filtration by fg submodules
↳ this are the ones important in practice.

Then $gr_J(M)$ is fg over $gr_I(R)$.

Proof/ Assume $IM_i=M_{i+1}$ $\forall i\geq n$ then $(I/_{I^2})(M_i/_{M_{i+1}})=M_{i+1}/_{M_{i+2}}\subseteq gr_J(M)$ $\forall i\geq n$ thus $gr_J(M)$ generated by generators of $M/_{M_1},\dots,M_n/_{M_{n+1}}$ □

<u>DEF</u> Let R be a local ring with fg maximal ideal $I\subseteq R$. Set $H_R(n)=\dim_{R/_I}(I^n/_{I^{n+1}})$ $\forall n\in\mathbb{N}$ as an $R/_I$ vs. If M fg R-module set $H_M(n)=\dim_{R/_I}(I^nM/_{I^{n+1}M})$ (these things are finite because of fg). **(Hilbert functions)**

Note that in this situation $\exists\, P_M(x)\in\mathbb{Q}[x]: P_M(n)=H_M(n)$ $\forall n\gg 0$.

Proof/ Let $S=gr_I(R)=\bigoplus_{n\geq 0} I^n/_{I^{n+1}}$ is an affine ring over $k=R/_I$. Thus $S\underset{\text{k-alg (and graded ring)}}{\cong} k[x_1,\dots,x_n]/_J$

Now M is a fg R-module define the filtration $J := M_j=I^jM$. Note it is I-stable ($IM_j=I^{j+1}M=M_{j+1}$) filtration by fg submodules thus by prop 70 $gr_J(M)$ fg graded S-module. So it is also a fg graded module over $\underset{\text{(grade by degree)}}{k[x_1,\dots,x_n]}$ so we apply the 69 □

DEF Let R be a ring, I ideal. M an R-module $\mathcal{J}$ an I-filtration so that $gr_{\mathcal{J}}(M)$ is a graded $gr_I(R)$ module we have the following map of sets called **initial term**.

$$in : M \longrightarrow gr_{\mathcal{J}}(M)$$
$$m \longmapsto \begin{cases} \bar{m} \in M_j / M_{j+1} & \text{if } \exists j : m \in M_j \setminus M_{j+1} \\ 0 & \text{if } m \in \bigcap_{j \geq 0} M_j \end{cases}$$

$\left(\begin{array}{l} M \to gr_{\mathcal{J}}(M) \text{ does not give too much} \\ m \to m + M_1 \end{array} \right)$

Example $M = R = k[x_1, -, x_n]$ with k field. $I = \langle x_1, -, x_n \rangle$; $M_j = I^d \subseteq M$

if $f \in R$ $\quad f = \underset{\in R_d}{f_d} + \underset{\in R_{d+1}}{f_{d+1}} + \cdots + f_e \quad f_d \neq 0$. Then $in(f) = f_d$ (for Anders; form of deg d is hom poly of deg d)

DEF Let R be a ring, $I \subseteq R$ an ideal. M R-module and $M' \subseteq M$ submodule. Let $\mathcal{J} : M = M_0 \supseteq M_1 \supseteq \cdots$ an I-filtration we set the **initial module of M'** to be the submodule generated by $in(m') : m' \in M'$ $\subseteq gr_{\mathcal{J}}(M)$.

Example Let $R = M = k[x, y]$. Set $I = \langle x, y \rangle$, $M_j = I^d$ and $M' = \langle xy + y^3, x^2 \rangle$

It is an exercise to check $in(M') = \langle xy, x^2, y^5 \rangle$

↳ $in(xy + y^3) = xy$, $in(x^2) = x^2$ so $\langle x^2, xy \rangle \subseteq$ initial module of M'
but $x(xy + y^3) - yx^2 = xy^3 \in M'$ so $y^2(xy + y^3) - xy^3 = y^5 \in M'$ so y^5 ✓
(check that it is all

For the remaining part of the lecture he gave a short intro to Groebner Bases. (this last thing he said it has to do with G. Bases) "They are already kind of motivated in the course (useful for computations) and essentially grading and these are ways to organize your ring". Since he didn't say much and ch 15 Eisenbud (6 min) is all about this; I'll skip it (read intro from Eisenbud).

We now discuss the Blow-up algebra.

DEF Let R be a ring, $I \subseteq R$ ideal. We define **$B_I(R)$** $\overset{\text{same remark as above for } gr_I(R)}{:=}$ $R \oplus I \oplus I^2 \cdots\cdots \overset{\text{identified}}{\cong} R[tI] \subset R[t]$

We call it the **blow up algebra of I in R** (R-algebra)

Notes i) $B_I(R) / I B_I(R) = gr_I(R)$
↳ they are equal since formal sums are sequences so quot also sequences

ii) R noetherian $\to B_I(R)$ noetherian (R noeth so $I = \langle f_1, -, f_n \rangle$ thus $B_I(R) \cong R[tf_1, -, tf_n] \subseteq R[t]$

$R[t_1, t_2, -, t_n] / \langle t_1 - tf_1, t_2 - tf_2, -, t_n - tf_n \rangle \cong R[tf_1, -, tf_n]$ quotient of poly ring in finitely many variables (noeth by Hilb basis)
↳ to prove this it follows (as we proceed) from the similar thing we did at the beginning.

Geometry discussion : Geometry of the blow up algebra

Let $Y \subseteq \mathbb{A}^n$ (affine) alg set ; (in practice is irred most of the time) . Let $X \subseteq Y$ Zariski closed subset .

Let $I = I(X) = \langle f_0, \dots, f_m \rangle \subseteq A(Y)$

kind of abuse

Define $\varphi : Y \setminus X \longrightarrow \mathbb{P}^m$

$y \longmapsto (f_0(y) : f_1(y) : \dots : f_m(y))$

note even though we made an abuse above; this is a well defined element of k .

. We define the blow up of Y among X

$Bl_X(Y) = Cl(\{(y, \varphi(y)) : y \in Y \setminus X\}) \subseteq Y \times \mathbb{P}^m$ closure taken in product topology

Consider $\pi : Bl_X(Y) \longrightarrow Y$ the projection . Let now $\pi : \pi^{-1}(Y \setminus X) \longrightarrow Y \setminus X$

This is an "iso of varieties". We have not defined this completely (not our goal) but now I have a very clear picture of what this means homeo + reg functions .

We are not focused now on proving this (alg geo) but the point is that outside X "nothing changes". So the blow up modifies X but leaves $Y \setminus X$ "the same".

The point of this blow-up thing is that if we start with Y "singular" along X and we consider $Bl_X(Y)$ is "less singular". Note I see some connections at least philosophically with normalization ; There are more theorems about nonsingular things. Also I guess that by the naturality of normalization and blow up there are thms which relate properties of alg sets and their normalizations and blow ups . So when one is trying to prove smth for a singular variety , one replaces it by its norm or blow up (depending on context) proves it there and tries to recover it . (Anders agreed)

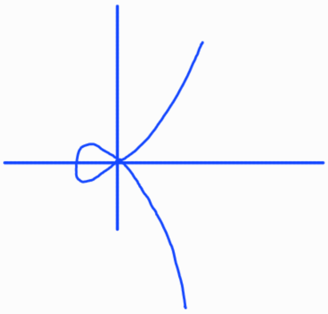
(k = C ; comfortable)

Example $Y = Z(y^2 - x^2(x+1)) \subseteq \mathbb{A}^2$ $X = \{(0,0)\}$

Consider $I(X) = \langle x, y \rangle \subseteq A(Y) = k[x,y]/\langle y^2 - x^2(x+1) \rangle$

easy

(also we see the abuse)



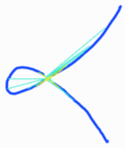
Let us compute the blow up $\varphi : Y \setminus \{(0,0)\} \longrightarrow \mathbb{P}^1$

$P = (a,b) \longmapsto$ line through $(0,0)$ and (a,b) $= (a:b)$

Now $Bl_X(Y) \subseteq Y \times \mathbb{P}^1$

one can prove this is the closure but it is also kind of intuitive if we think topologically

$= \{((a,b), \varphi(a,b)) : (a,b) \neq (0,0)\} \cup \{((0,0),(1:1)), ((0,0),(1:-1))\}$



This is nice but what does this have to do with blow up alg?

Recall that $Bl_X(Y) \subseteq Y \times \mathbb{P}^m$ closed. Let $J = \{ f \in \overset{\text{ring}}{A(Y)}[\overset{\text{variables}}{z_0,\dots,z_m}] : f(y,(a_0:\dots:a_m)) = 0$ $\forall (y,(a_0:\dots:a_n)) \in Bl_X(Y) \}$

Here we mean; take $f \in A(Y)[z_0,\dots,z_m]$. Poly in $z_0,\dots,z_n$ with coeff "polys" in $x_1,\dots,x_n$. Take an elmt of $Bl_X(Y)$ this is a point in Y and a line. We care about those f st vanish at all the tuples formed by "that point in Y" "point in corresp line" (for every elmt in $Bl_X(Y)$).

We denote this by $I(Bl_X(Y))$ (natural def).

($Bl_X(Y)$ will be a variety in the general sense and these objects will have coord rings.)

↳ we are slowly making alg geo very natural from the algebra.

The ring $A(Y)[z_0,\dots,z_n]$ can be graded (everything in the coordinate ring of Y as deg 0 and $z_0,\dots,z_n$ as degree 1 (this words define a graded ring structure; of course))

J is a homogeneous ideal wrt this grading

<u>Claim</u> $A(Y)[z_0,\dots,z_n]/J \underset{\substack{\downarrow \\ \text{as } A(Y) \text{ algebras}}}{\cong} B_I(A(Y))$ $(I = I(X))$

Note that $Bl_X(Y)$ was constructed using specific generators of $I(X)$. This claim says that the "coordinate ring of $Bl_X(Y)$" does not depend on the generators. (Other generators give iso coord ring). This will say that $B_X(Y)$ as a "variety" only depends on X, Y.

The quoted concepts go a bit beyond the course (already mentioned)

Now Anders justified the claim; a few things happen that I do not quite like since I feel that one needs to know a bit of varieties in general to treat (alg variety × proj variety). So the following can be skipped; I leave it here in case in case I need the idea; but again I should skip.

$\varphi : Y \setminus X \longrightarrow \mathbb{P}^m$ we now define the following

$y \longmapsto (f_0(y) : \dots : f_n(y))$

$\psi : Y \times \mathbb{A}^1 \longrightarrow Y \times \mathbb{A}^{m+1}$ (my only issue with this is ")

$(y,t) \longmapsto (y,(tf_0(y),\dots,tf_n(y)))$

Where does $(y,0)$ go?

this descends to

$\downarrow$

$Y \times \mathbb{P}^m \supseteq Bl_X(Y)$

this induces a map $A(Y)[z_1,\dots,z_m] \xrightarrow{\psi^*} A(Y)[t]$

$z_i \longmapsto tf_i$

$\overline{\psi(Y \times \mathbb{A}^1)}$ is called the cone over the blow up and one sees that $\underset{\substack{\| \\ Ker(\psi^*)}}{J} = I(\underset{\downarrow \text{think}}{\psi(Y \times \mathbb{A}^1)}) \subseteq A(Y)[z_0,\dots,z_m]$

↳ need to make sense of this but quite clear.

So $A(Y)[z_0,\dots,z_n]/J \cong Im(\psi^*) \overset{\substack{\text{think.} \\ \uparrow}}{=} B_I A(Y)$

(something common in alg geo; morphism of varieties gives hom of coord rings)

(Blow up and normalization philosophically have the same reason to exist)

At this point Anders moved to dimension theory but there are a few interesting results that he skipped. The proofs seem very readable from Eisenbud, so I skip.

Proposition Let R be a ring, $I \subset R$ ideal M fg R-module $\mathcal{J}: M = M_0 \supset M_1 \supset \cdots$ I-filtration by fg modules M_i. $\mathcal{J}$ is I-stable iff the $B_I(R)$-module $B_{\mathcal{J}}(M)$ is fg.

$\overset{\shortparallel}{} M \oplus M_1 \oplus \cdots$

↳ graded $B_I(R)$ module.

Artin-Rees Let R be a noeth ring, $I \subset R$ ideal. Let $M' \subset M$ fg R-modules. If $M = M_0 \supset M_1 \supset \cdots$ is an I-stable filtration then the induced filtration $M' \supset M' \cap M_1 \supset M' \cap M_2 \cdots$ is also I-stable.

Another application is

Krull Int thm Let R be a Noetherian ring, $I \subset R$ ideal.

i) If M is fg R-module then $\exists r \in I$ st $(1-r)\left(\bigcap_{d=1}^{\infty} I^d M\right) = 0$.

ii) If R is a domain or local ring and I proper then $\bigcap_{d=1}^{\infty} I^d = 0$

I prove it just to show that these are easy.

Pf/ By Artin-Rees applied to the submodule $\bigcap_{d=1}^{\infty} I^d M \subset M$, $\exists p \in \mathbb{N}$: $\bigcap_{d=1}^{\infty} I^d M = \left(\bigcap_{d=1}^{\infty} I^d M\right) \cap I^{p+1} M =$

$= I\left(\left(\bigcap_{d=1}^{\infty} I^d M\right) \cap I^p M\right) = I\left(\bigcap_{d=1}^{\infty} I^d M\right)$

By C47 $\exists r \in I$: $rm = m$ $\forall m \in \left(\bigcap_{d=1}^{\infty} I^d M\right)$ so i) ✓. For the second statement take $M = R$ we know that $(1-r)\left(\bigcap_{d=1}^{\infty} I^d R\right) = 0$. If we show $1-r$ nzd we are done.

I is proper so $r \neq 1$ thus $1-r \neq 0$. If R domain ✓. If R local $I \subseteq$ the maximal ideal so r too thus $1-r$ unit (easy exercise) □

The next corollary is an example of a line of results saying that good properties of $gr_I R$ imply good properties of R.

Corollary Let R be noeth local, I proper ideal of R. If $gr_I(R)$ domain then R domain.

Proof/ Suppose $fg = 0$ $f, g \in R$ then $in(f)in(g) = 0 \in gr_I R$. So wma $in(f) = 0$ so $f \in \bigcap_{i=1}^{\infty} I^d \underset{\substack{\downarrow \\ \text{Krull} \\ \text{int thm}}}{=} 0$ □

PART 2 : DIMENSION THEORY

Of course we are not following Eisenbud line by line but so far we've done (Anders way) Part 1 except ch 6,7. (Not exactly because we've done things in Ch 13 without mentioning the word dimension) We will not do ch 7. Ch 6 discusses flatness and we will talk about it here when we need it, but now our focus is in Part 2 Eisenbud "Dimension theory". When we discussed Hilbert polys the word dimension appeared for the first time (outside v.spaces).

17. TRASCENDENCE DEGREE

(~ Anders + Ch 24 Isaacs ; Eisenbud has an appendix on this but says way less)
A

DEF Let $k \subseteq L$ be a field extension we say that $S \subseteq L$ is algebraically independent over k if $\forall s_1,\dots,s_n \in S$ distinct $k[x_1,\dots,x_n] \to L$, $x_i \longmapsto s_i$ is injective. $(f(s_1,\dots,s_n) \neq 0$ for $f \in k[x_1,\dots,x_n] \setminus \{0\})$

We say that $B \subseteq L$ is a trascendence basis of L over k if B alg. indep. over k and $k(B) \subseteq L$ is an algebraic extension ($k(B)$ subfield of L gen by B) can be the empty set.

not get confused with fract field; this is just attaching elements.

"kind of generalisation of li; think of B as spanning set"

Of course subsets of alg indep are alg indep.

Lemma 71 $k \subseteq L$ field ext, $S \subseteq L$ alg indep over k. If $\alpha \in L \setminus S$ then $S \cup \{\alpha\}$ is alg indep over k iff α not algebraic (trascendental) over $k(S)$.

The proof is quite routinary (Lemma 24.2 Isaacs Algebra)

Proposition 72 Let $k \subseteq L$ be a field extension. Suppose $S \subseteq L$ alg indep over k. Suppose $T \subseteq L$ such that $k(T) \subseteq L$ algebraic. Then

subfield gen by

i) If $S \subseteq T \to \exists$ trascendence basis $B : S \subseteq B \subseteq T$ (so trascendence basis exist)

ii) If $S \nsubseteq T \to \exists s \in S \setminus T$, $t \in T$: $(S - \{s\}) \cup \{t\}$ alg indep over k.

iii) $\# S \leq \# T$ (we only prove it under certain assumptions)

iv) All trascendence bases have same cardinality.

This common cardinality is called trascendence degree of L over k ($\mathrm{tr.deg}_k L = \mathrm{tr.deg}\, L/k$)

(a bit of work; we order wrt inclusion then if you have linearly ordered subset you take union to be upper bound..)

Proof/ i) By Zorn's lemma $\exists B : S \subseteq B \subseteq T$ B alg indep over k maximal wrt to this property

Since B is maximal all elmts in T are algebraic over $K(B)$.

Suppose $b \in T$ trancendental over $k(B)$ then $S \cup \{t\} \subseteq T$ alg indep over k by L71.

So $k(T)/k(B)$ is alg and $L/k(T)$ alg thus by part 1 ex 15 Ecal (or more generally integral ext) $L/k(B)$ is alg so B is a trancendence basis of L over k.

ii) Choose $s \in S \setminus T$. The extension $k(S\setminus\{s\}) \subseteq L$ is not algebraic (for example $s \in L$ is not alg over $k(S\setminus\{s\})$ by lemma 71) If T alg over $k(S\setminus\{s\})$ then as above L alg over $k(S\setminus\{s\})$ so $\exists$ $t \in T$ not alg over $k(S\setminus\{s\})$, by L71 $k(S\setminus\{s\}) \cup \{t\}$ alg indep.

iii) We only prove it under the assumption that $|\{s \in S \mid s \notin T\}| < \infty$. (In general is a bit more difficult)

We induct on that number n. If $n=0$ then $S \subseteq T$ so ✓

For $n>0$, $S' = (S\setminus\{s\}) \cup \{t\}$ is alg indep over k for some $s \in S \setminus T$, $t \in T$. So by induction (since $\#S'\setminus T = (\# S\setminus T) - 1$) $\#S = \#S' \leq \#T$

iv) Is immediate. □

Anders stopped here; this is a short version of section 24.A of Isaacs Algebra. In this section he does a few more things that are good to know. I will go over this section, however, I will skip most proofs here. Proofs in that book are very easy to read.

L24.1 $k \subseteq L$ field extension, $S \subseteq L$ alg indep over k. Then $k(S)$ is k-isomorphic (via fixing k) to a rational function field in a set of indeterminates in bijective correspondence to S.

Proof/ Read from Isaacs; 7 lines very clear.

DEF A field extension $k \subseteq L$ is said to be purely trancendental if $L = k(S)$ with S algebraically indep over k. (Also a extension $E \subseteq F$ is said to be totally trancendental or trancendental if $\forall \alpha \in F\setminus E$ α not alg over F)

Corollary 24.3 A purely trancendental extension is totally trancendental. (easy to read)

Now Isaacs gives an example of totally trancendental which is not purely trancendental.

$k = \mathbb{Q}[\underset{\substack{\downarrow \\ \text{undet.}}}{T}]$, $f \in k[X]$ poly ring; $f(X) = X^2 + (T^2+1)$. Let $E = k[\alpha]$ $(= k(\alpha))$ α root of f

E/Q is the desired extension.

Exact statements of how Isaacs gets to prop 72

Now Isaacs works to prove the analogue of prop 72. Its lemma 24.4 is part i of thm 72

For the rest of the thm he does the following:

L24.6, T24.5, C24.7
- Let $F \subseteq E$ field ext, S_1, S_2 disjoint subsets with S_1 algebraically indep. over F. Let $K = F(S_1)$. Then $S_1 \cup S_2$ alg indep over F iff S_2 alg indep over K.
- $F \subseteq E$ field ext. Suppose $E = F(S)$ for S finite subset of E. Suppose $E/F(S)$ algebraic then $\forall S' \subseteq E$ with $|S'| > |S|$, S' is not alg indep over F
- If E/F field extension, E has a finite trancendence basis over F; then all trancendence basis for E over F have same cardinality.

Finally he mentions that this last statement also holds in the infinite case.

Now that we are on the same page as Isaacs I will cover the rest of ch 24 (without (all) proofs; because they are easy to read so I feel this is good enough).

Notes Let E/F be a field ex then

i) $\mathrm{Trdeg}_F(E) = 0 \longleftrightarrow E/F$ algebraic. (clear)

ii) $\mathrm{Trdeg}_F(E) < \infty \longleftrightarrow E/K$ alg for some $F \subseteq K \subseteq E$, K finitely generated over F.

$\longrightarrow$) Def

$\longleftarrow$) K has a finite trancendence basis over F by prop 72. Since E/K algebraic from the defn we see that this trancendence basis is also a trancendence basis of E over F.

Theorem 24.8 Let $F \subseteq E \subseteq L$. Then $\mathrm{trdeg}_F(L) = \mathrm{tr.deg}_F(E) + \mathrm{tr.deg}_E(L)$. In particular the degree on the left is infinite iff one of the degrees on the right is infinite.

Proof/ Easy, see from book.

With this sec 24A ends. (VIDEO: Tr.deg and ch 24)

18. KRULL DIMENSION

(~ Intro of ch 9 Eis)

Let $X \subseteq \mathbb{A}^n \overset{= k^n}{}$ be an alg subset. We would like to define $\dim(X)$. If X irreducible we know that $A(X) = k[x_1, \dots, x_n] / I(X)$ affine domain over k.

fraction field (field of rational funct on the alg. set)

The classical definition is $\dim(X) = \text{tr.deg}_k(K(A(X)))$

In algebra in contrast to diff geo we have things that are "singular" (V); in diff geo a manifold is locally homeo to $\mathbb{R}^n$ so in that case is very easy to define dimension.

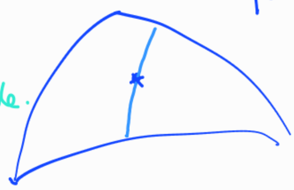
This def is still used but in general we want a defn in any commutative ring (the ring $A(X)$ contains k; this is of course crucial in the def)

to prove things by induction over dim for example

Motivation

We will see better in example.

"surface"



$\underbrace{\text{Point} - \text{line} - \text{surface}}$

chain of closed irred subsets of length 2 so we "want" dimension to be 2.

corresp before L25

$\equiv$ Prime ideal in coord ring $\subsetneq$ Prime ideal in coord ring $\subsetneq$ Coord ring

DEF Let R be a ring, we define the Krull dimension of R to be $\dim(R) = \sup\{r : \exists P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_r\}$ with $P_i \in \text{Spec}(R)$.

(and the dim of an alg set is the dim. of the coordinate ring)

(of course this is either $< \infty$ or ∞)

Notes i) This dimension can be infinite; even if R Noetherian

The most known example is one by Nagata where $R = k[x_1, \dots\dots]$. Heuristically any particular chain $P_0 \subsetneq P_1 \subsetneq \dots R$ will stop but you could have other chain longer... (PIT will say something more about descending chains) (see Ex 11.1 k Vakil. for details / Ex 9.6 Eisenbud)

ii) If R affine ring (over field) or R local noetherian then $\dim(R) < \infty$. (We'll see)

in corollary 78 I clarify why there are prime.

iii) Of course we want $\dim(\mathbb{A}^n) = n$. Well, $A(\mathbb{A}^n) = k[x_1, \dots, x_n]$; so for we have $0 \subsetneq \langle x_1 \rangle \subsetneq \dots \subsetneq \langle x_1, \dots, x_n \rangle$ so $\dim(\mathbb{A}^n) \geq n$. We will see that it is exactly n.

field of frac.

iv) We will see that: R affine domain over k, $\dim R = \text{tr deg}_k(K(R))$

DEF Let $I \subseteq R$ be an ideal, (historically people write) $\dim(I) = \dim(R/I) \overset{\text{corresp}}{=} \sup\{r : I \subseteq P_0 \subsetneq \cdots P_R ;\ P_i \in \text{Spec}(R)\}$

Reason: If R is coord ring of an alg set; $R = A(X)$ then we want $\dim I$ to be the dimension of the subset corresp to I (vanishing set). The coord ring of this set is of course R/I. (functions on X restricted to V mod out by those who coincide on V.
V

similar story as in associated primes

This def (now motivated) might cause a bit of confusion but from context will be clear what we do. The rule is if $\square$ is seen as a ring $\dim \square = \sup \dots$. If $\square$ is seen as an ideal in a bigger ring $\dim(\square) = \dim(K/\square)$

We also set $\text{codim}(I) = \inf\{\dim R_P : I \subseteq P, P \in \text{Spec}(R)\}$
(or height)

by well ordering I think is a minimum.

Note let $P \subseteq R$ prime. Then $\operatorname{codim} P = \dim R_P = \sup\{r : \exists P_0 \subsetneq \cdots \subsetneq P_r = P\}$ $P_i \in \operatorname{Spec}(R)$

STEP 1 $\operatorname{Dim}(R_P)$ = sup of lengths of chains of primes descending from P

Let $Q_0 \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_n$ be a chain of prime ideals in R_P. Since we are taking sup assume that Q_n is P_P the unique maximal ideal of R_P. By prop 8 we have bijection $\operatorname{Spec}(R_P) \longleftrightarrow \{J \in \operatorname{Spec}(R) : J \cap (R \setminus P) = \emptyset\} = \{J \in \operatorname{Spec}(R) . J \subset P\}$

$Q \longmapsto R \cap Q$

Now if $Q_i \subseteq Q_j$ then $R \cap Q_i \subseteq R \cap Q_j$. Trivial (but we are using $\pi : R \to R_P$, $r \longmapsto r/1$). So if $Q_i \subsetneq Q_{i+1}$ then since is 1-1, $Q_i \subsetneq Q_{i+1}$. Thus the chain $Q_0 \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_n$ corresponds to a chain of primes in R descending from P ($P_P \cap R = P$).

STEP 2 $\dim(P) = \inf\{\dim R_Q : P \subseteq Q \in \operatorname{Spec}(R)\} \overset{\text{step 1}}{=} \dim(R_P)$ //

Thus $\operatorname{codim} I = \inf\{\operatorname{codim} P : I \subseteq P \in \operatorname{Spec}(R)\} = \inf\{\operatorname{codim} P : I \subseteq P \text{ minimal prime over } I\}$

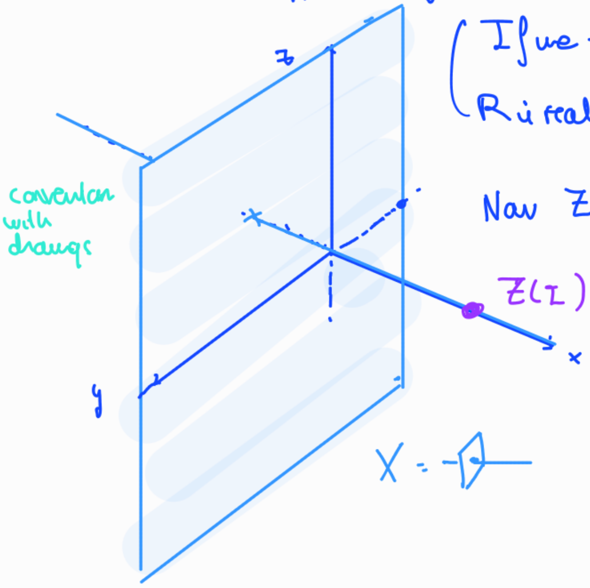
If $I \subseteq Q \in \operatorname{Spec}(R)$ not minimal prime $I \subseteq P \subsetneq Q$; by the 1st part of note $\in \operatorname{Spec}(R)$
$\operatorname{codim} P < \operatorname{codim} Q$. So the integer $\operatorname{codim} Q$ can be omitted from the list.

(and seeing that our defs are good)

Example (Building intuition) $R = k[x,y,z]/\langle xy, xz\rangle$, $I = \langle x-1, y, z\rangle / \langle xy, xz\rangle$

(Working implicitly under the knowledge of ☐ before lemma 25)

If we take the (affine) alg set corresp to R this is $X = Z(\langle xy, xz\rangle)$.



(If we take $k = \mathbb{C}$, since $I(X) = \sqrt{\langle xy, xz\rangle} = \langle xy, xz\rangle$ then R is really the coord ring of X.)

Now $Z(I) = Z(\{x-1, y, z\}) = (1, 0, 0)$

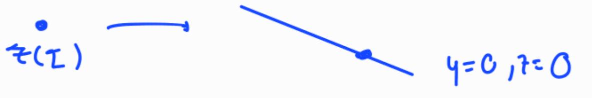
(so in the corresp before L25 $I/\langle xy, xz\rangle \leftrightarrow Z(I)$)

(In that corresp, closed irreducible subsets of X appear but from the picture (and in general) those are easy to detect)

Now $\dim I = \dim(R/I) = 0$ corresponds with the fact that $Z(I)$ is a point.
$\downarrow$
I max ideal (of course)

Codim I = The largest chain of primes in R descending from I

If we look at the correspondence before L25 a descending chain of primes from I corresp to ascending collection of irred closed subsets (of X) starting from $Z(I)$. This directly tells us



: Now in X we do not have

any other irred. closed containg —— so we stop; thus codim $I = 1$. We now have a nice interpretation of codimension (codim of larger ideal is larger) (corresp to smaller alg set so we can go up longer)

Finally $\dim(R)$ $(= \dim(X)) = 2$

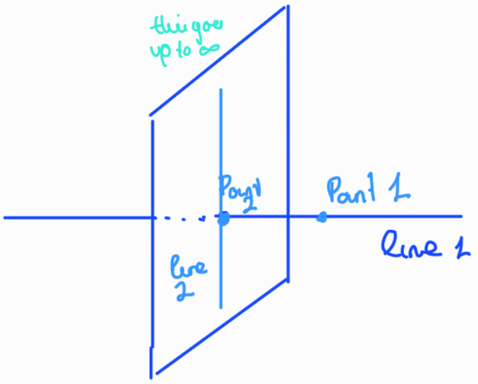
Again we go to the corresp before L25. A chain of prime ideals in R corresponds to: irred closed subset $\supsetneq$ irred closed subset $\supsetneq \cdots$

makes sense. Dim(X) means dim $I(X)/I(X) = 0$ ideal in $k[x,y,z]/I(X)$ which is dim $(R/0) = \dim(R)$.

Note: (def + correspondence before L25)

In general, codim I is the minimal codimension of irred comp of $Z(I)$. and to see the codim of irred closed comp of $Z(I)$ we do it as in the example; ascending chain of closed irred subsets (by the note and correspondence, so completely convinced this process (kind of intuitive) gives correct answer)

(when we say dim or codim of alg set we mean dim or codim of the ideal corresp to that under the corresp before L25)



Codim (line 2) = 1

Codim (line 1) = 0

Codim (Point 1) = 1

Codim (Point 2) = 2

He gave another way of thinking about it as the difference between maximum dimension of closed irred containg it and the dim of the closed irred you start with. For now I understand the other completely; this other way of thinking I think requires a proof (maybe obvious). So for now I take this one as pure intuition and the previous one as justified

we mean dim of corresponding prime ideal (so dim of quotient)

Note $\underset{0}{\dim I} + \underset{1}{\text{codim } I}$ (here I is $\langle x-1, y, z\rangle / \langle xy, xz\rangle$) $< \underset{2}{\dim X}$

This was for affine rings but building intuition for affine rings is good for rings in general

Exercise Let R be a ring, $I \subseteq R$ ideal. Then $\dim I + \text{codim } I \leq \dim R$

Obvious build appropriate chain (there is a bit argue when we have inf or sup but is still easy and clear).

In the previous example we saw that equality is not necessarily true. A fact that might come is R affine domain over k, $\dim(I) + \text{codim}(I) = \dim R$.

↳ it will not be proved but I'll say a few words

19 DIMENSION ZERO (~ 9.1 Eisenbud)

" Doing things more generally than 99.9 % or even 100 % of what we need in practical applications allows arguments that are sometimes easier in the general case and then you come back to your examples. As Complex numbers solving equations "

Let R be a Noetherian ring (in dimension theory of commutative rings R is usually Noetherian) then $\dim R = 0$ iff R Artinian

Proof/ $\mathrm{Dim}(R) = 0$ iff all prime ideals are maximal iff R artinian (prop 20)

Thus if $X \subseteq \mathbb{A}^n = k^n$ algebraic set, $\dim(X) = 0$ iff X finite set.

$R = A(X) = k[x_1, \ldots, x_n] / I(X)$. If X is finite again by corollary 21 $A(X)$ is artinian so $\dim(X) = 0$

If $\dim(X) = 0$, $A(X)$ artinian so X finite by corollary 21 again.

__Prop 73__ Let $\varphi: R \to S$ be a ring hom with S integral over R. Then (no need of noeth)

i) $P \subseteq R$ prime, $\ker(\varphi) \subseteq P$. Then $\exists\, Q \subseteq S$ prime : $P = R \cap Q$

ii) $I \subseteq S$ ideal, then $\underset{\overset{\|}{\dim(I)}}{\dim(S/_I)} = \underset{\overset{\|}{\dim(\varphi^{-1}(I))}}{\dim(R/_{R\cap I})}$

Proof/

Claim : WLOG $R \subseteq S$, φ = inclusion (this are some straight forward details that I skip)

i) Is a direct application of going up.

ii) Suppose that we have a chain of prime ideals $R \cap I \subseteq P_0 \subsetneq \cdots \subsetneq P_r$ $\quad P_i \in \mathrm{Spec}(R)$

then by going up, $\exists\; I \subseteq Q_0 \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_r \subseteq S$ $\quad Q_i \in \mathrm{Spec}(S)$

This shows $\dim(R/_{I\cap R}) \leq$

$\leq \dim(S/_I)$.

$$\left(\begin{array}{l} Q_i \cap R = P_i \\ \qquad\qquad\;\; \subsetneq \\ Q_{i+1} \cap R = P_{i+1} \end{array}\right.$$

On the other hand if $I \subseteq Q_0 \subsetneq \cdots \subsetneq Q_r \subseteq S$ by incomparability $R \cap I \subseteq R \cap Q_0 \subsetneq \cdots \subsetneq R \cap Q_r \subseteq R$

so we get the reverse inequality □

__Note__ Now Eisenbud gives a geometric version of this (C9.3) Anders skipped it but good to know it follows from this (see Eisenbud; uses the word morphism)

20 THE PRINCIPAL IDEAL THM (~ ch10.0 Eis)

In this section unless otherwise stated all rings are Noetherian.

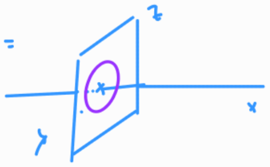
Theorem 74 (PIT V1) Let R be a Noeth ring, $f \in R$. Let P minimal prime over $\langle f \rangle$.

Then $\operatorname{codim}(P) \leq 1$

this is V1 because our we are cutting by one equation.

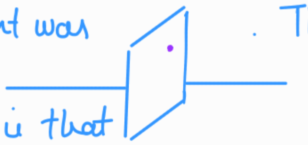
(Minimal prime over principal ideal has codim ≤ 1)

Let us see what we are saying. Think of R as $A(X)$

$X =$ 

f is a poly function in X. Its vanishing set "y^2+z^2-1"

What are we saying?
Intuition: (this is mine)

is somewhere in X (and outside but we do not care; suppose is  the purple part. A minimal prime over $\langle f \rangle$ corresponds to an irred closed subset contained in ○. Now with a bit of work one sees that this is irred closed ($\langle f \rangle$ prime exercise I guess) and here clearly codim $P = 1$. What if the purple part was . This would end up with codim $P = 2$ but the point is that this never happens. As the zero set of a 3 variable poly has "dim 2" so will always cut a plane in a "curve". A line will be cut in either a point or the line itself so  this could happen but here codim$(P) = 1$. ✓.

as a manifold
reg.surf....

The general PIT cuts by more equations.

completely unprecise

(Other possibility  ; here you have two minimal primes.)

Proof/STEP 1: We may assume R is local with max ideal P.

Assume true in this case. Then consider $\langle f/_1 \rangle \subseteq R_P$ we know that R_P local with max ideal $\langle \{ p/_1 : p \in P \} \rangle = P \cdot R_P$ $= P_P$ see last thing in sec 3. (notation ch 1). By the thm in this case codim $P \cdot R_P \leq 1$ this means that (by previous note) $\sup\{r : Q_0 \subsetneq Q_1 \subsetneq \dots \subsetneq Q_r \} \leq 1$. But by prop 8 this is
$Q_i \in \operatorname{Spec}(R_P)$
(take $Q_i \cap R$)

$\sup\{r : P_0 \subsetneq P_1 \subsetneq \dots \subsetneq P_r = P\} \leq 1$ and by the note, since P prime this is codim $P \leq 1$

($R_P \cap P = P$: $r/_1$ has preimage in P thus $\exists s \in P$: $r/_1 = s/_1$
so $\exists u \in R \setminus P$: $u(r-s) \in P$ thus $r-s \in P$ so $r \in P$)

STEP 2: NTS $Q \overset{\in \operatorname{Spec}(R)}{\subsetneq} P$ then codim$Q = 0$ Obvious. (Obvious by note before ex)

· Now consider R_Q, this is again local with max ideal Q_Q ($:= Q \cdot R_Q = \cdot\cdot$) already discussed what was (Wrong?)

Define $Q^{(n)} = \{ r \in R : \exists s \in R \setminus Q : rs \in Q^n \}$. It is routinary to check $Q^{(n)} = (Q_Q)^n \cap R$
(Symbolic nth power of Q) $\supseteq Q^{(n+1)}$ since $Q^n \supseteq Q^{n+1}$ $\subseteq R_Q$ ideal so has of...

· P is minimal over $\langle f \rangle$ so $R/\langle f \rangle$ is artinian. (i → iii in thm 20)

Thus $R \supseteq \langle f \rangle + Q^{(1)} \supseteq \langle f \rangle + Q^{(2)} \supseteq \cdots\cdots$ corresponds to a descending chain of ideals inside $R/\langle f \rangle$ so it stabilises by Artinian property. So $\exists n \in \mathbb{N} : \langle f \rangle + Q^{(N)} = \langle f \rangle + Q^{(n)} \quad \forall N \geq n$

<u>Claim</u> $\forall N \geq n$, $Q^{(N)} = f \cdot Q^{(N)} + Q^{(N+1)}$.

$\supseteq)$ ✓

$\subseteq)$ let $h \in Q^{(N)}$, $h = af + g$ with $a \in R$, $g \in Q^{(N+1)}$ since $Q^{(N)} \subseteq \langle f \rangle + Q^{(n)} = \langle f \rangle + Q^{(N+1)}$

thus $af \in Q^{(N)}$. Since P minimal prime over $\langle f \rangle$ and $Q \subsetneq P$ $f \notin Q$ so $a \in Q^{(N)}$

by def

Thus $Q^{(N)}/Q^{(N+1)} = f \cdot Q^{(N)}/Q^{(N+1)})$; since R local $f \in P$ by Nak $Q^{(N+1)} = Q^{(N)}$ $\forall N \geq n$

However note $Q^{(m)} \cdot R_Q = (Q_Q)^m$ from defn (little exercise)

Thus $(Q_Q)^N = (Q_Q)^{N+1} = (Q_Q)^N Q_Q$ so again by Nak; $\underset{\subseteq R_Q}{(Q_Q)}^N = 0$ $\forall N \geq n$

Thus $\operatorname{codim} Q = \dim R_Q \underset{!}{=} 0$ as wanted.

(By corollary 23 (R_Q as an R_Q-module) R_Q is Artinian ; now apply one cond from above) □

Now we prove the full PIT (The interpretation is that now you cut by more polynomial equations)

<u>Thm 75 (PIT)</u> Let R be a Noetherian ring $\overset{(c \in \mathbb{N})}{x_1, \ldots, x_c} \in R$. $P \subseteq R$ minimal over $\langle x_1, \ldots, x_c \rangle$ then $\operatorname{codim}(P) \leq c$

Proof/ Exactly as above we may assume R local with max. ideal P. Let $P_1 \subsetneq P$ <u>any</u> prime with no primes in between. Consider the primes strictly contained in P, if $\nexists$ then $\operatorname{codim} P = 0$ ✓. If $\exists$ then by noeth property we can find a maximal one. If P_1 minimal over an ideal generated by $c-1$ elements by induction on c (base of induction is thm 74) $\operatorname{codim}(P) \leq c-1$. Thus by the note before the big example (and since we've said "any") $\operatorname{codim}(P) \leq c$.

So NTS P_1 minimal over an ideal gen by $c-1$ elmts. If $x_1, \ldots, x_c \in P_1$ then P not minimal over $\langle x_1, \ldots, x_c \rangle$ so we may assume $x_1 \notin P_1$. Note that P minimal over $\langle P_1, x_1 \rangle$. Recalling that the unique maximal ideal of R is P we can argue as above (20 i-iii) to say $R/\langle P_1, x_1 \rangle$ Artinian

This forces x_i to be nilpotent mod $\langle P_1, x_1 \rangle$ $\forall i$. By converse of corollary 23 (and correspondence thm) $P/\langle P_1, x_1 \rangle$ is nilpotent.

Thus $\exists n \in \mathbb{N}$ $a_i \in R$ $y_i \in P_1$: $x_i^n = a_i x_1 + y_i$. Claim P_1 minimal over $\langle y_2, -, y_c\rangle$. If we prove this we are done. Note $R/\langle x_1, - x_n\rangle$ is Artinian (P minimal over $\langle x_1, - x_n\rangle$, R local with max ideal P and thm 20). So by conseq of corollary 23 P nilpotent mod $\langle x_1, -, x_c\rangle$ so $\exists m \in \mathbb{N}$: $P^m \subseteq \langle x_1, -, x_c\rangle$. Thus $P^{mnc} \subseteq \langle x_1, -, x_c\rangle^{nc} \subseteq \langle x_1, y_2, -, y_n\rangle$

$(r_1^1 x_1 + \dots + r_c^1 x_c) \cdots (r_1^{nc} x_1 + \dots + r_c^{nc} x_c) \in \langle x_1, y_2, - y_n\rangle$
An arbitrary elmt is sum of this. When I do this product I get a sum of elmts of the form
$r x_1^{a_1} \cdots x_c^{a_c}$ $a_1 + \dots + a_c = nc$
If all $a_i < n$ then that equality does not hold so at least x_i^n appears (maybe more power but we only look at that. Now $x_i^n \in \langle x_1, y_2, -, y_n\rangle$ thus $r x_1^{a_1} \cdots x_c^{a_c}$ too (ideal) so we conclude that

Therefore $R/\langle x_1, y_2, -, y_c\rangle$ is Artinian

(local ring with max ideal nilpotent; see conseq of C23)

note y_i's $P_1 \subseteq P$

Now this implies $P/\langle y_2 - y_c\rangle \subseteq R/\langle y_2, - , y_c\rangle$ is minimal over the ideal generated by x_1 in $R/\langle y_2, -, y_c\rangle$

· Call $\langle y_2, -, y_c\rangle = I$, $J = \langle x_1 + J\rangle \leq R/I$; $J = \langle x_1\rangle + I / I$; $\frac{R/I}{J} \cong R/\langle x_1\rangle + I$ but $\langle x_1\rangle + I = \langle x_1, y_2, -, y_c\rangle$

$\Big[_I \begin{array}{c} R \\ | \\ \langle x_1\rangle + I \\ | \\ I \end{array} \Big]$ Canonically !

. Take Q/I minimal prime over J. If we mod out by J we get $Q/\langle x_1, y_2, -, y_c\rangle$ and $Q/\langle x_1, y_2, -, y_c\rangle$ prime in $R/\langle x_1, --\rangle$

But by thm 20 since $R/\langle x_1, y_2, -, y_c\rangle$ Art , $Q/\langle x_1, y_2, - y_c\rangle$ maximal but $R/\langle x_1, y_2, -, y_c\rangle$ local so $Q/\langle x_1, y_2, - y_c\rangle = P/\langle x_1, y_2, - y_c\rangle$ so $Q = P$

By the PIT vs 1 codim $(P/\langle y_2, -, y_c\rangle) \leq 1$. By choice of P_1 codim$\left(P_1/\langle y_2, - y_c\rangle\right) = 0$ and this directly implies P_1 minimal over $\langle y_2, -, y_c\rangle$ as wanted . ◻

Now we explore a bunch of corollaries (the first one proves part of note ii after def of Krull dim)

Corollary 76 Any local Noetherian ring has finite dimension. (At most # generators of maximal ideal)

Proof / If R local we know that dim(R) = codim(I) where I max ideal (by note before big example) Now just apply PIT with the generators of I ◻

VIDEO : Desc chain Noeth

Corollary 77 Any descending chain of prime ideals in a Noetherian ring stabilizes. (Striking !)

Proof : $P \supseteq P_2 \supseteq \cdots$ descending chain of prime ideals. Consider R_P this is a local Noetherian ring (C.9). This descending chain gives a descending chain in R_P (of primes) with the same type of inclusions (elementary) ↳ localization of prime is prime.. and now we apply 76 and def of dim to say that in that chain are at most finitely many strict inclusions ◻

(of course any c variables)

Corollary 78 Let $I = \langle x_1-a_1,\dots,x_c-a_c\rangle \subseteq k[x_1,\dots,x_n]$ where k is a field. Then $\operatorname{codim} I = c$

Proof/ In $k[x_1,\dots,x_n]$, I is prime.

Proof: $k[x_1,\dots,x_n] \xrightarrow{\varphi} k[x_{c+1},\dots,x_n]$ surjective ring hom

$$x_i \longmapsto \begin{cases} a_i & i \le c \\ x_i & i > c \end{cases}$$

$$\lambda \longmapsto \lambda$$

Read the proof of the note after corollary 6. If $f \in \ker\varphi$ we have (arguing as in the proof) that

$f(x_1,\dots,x_n) = f(a_1,\dots,a_c,x_{c+1},\dots,x_n) + (x_c-a_c)q_1(x_1,\dots,x_n) + \dots + (x_1-a_1)q_n(x_1,\dots,x_n)$ with $q_i \in k[x_1,\dots,x_n]$

The fact that $f \in \ker\varphi$ means that $f(a_1,\dots,a_c,x_{c+1},\dots,x_n) = 0 \in k[x_{c+1},\dots,x_n]$

Thus $f \in \langle x_1-a_1,\dots,x_c-a_c\rangle$ thus $\ker\varphi \underset{\supseteq\checkmark}{\subseteq} \langle x_1-a_1,\dots,x_c-a_c\rangle$. Thus $\dfrac{k[x_1,\dots,x_n]}{\langle x_1-a_1,\dots,x_c-a_c\rangle} \cong \underset{\text{domain}}{k[x_{c+1},\dots,x_n]}$

so I is prime //

Knowing this we can say that $\le$ is because of PIT and $\ge$ follows by taking

$\langle x_1,\dots,x_c\rangle \underset{\neq}{\supseteq} \langle x_1,\dots,x_{c-1}\rangle \underset{\neq}{\supseteq} \dots \underset{\neq}{\supseteq} \langle x_1\rangle$ (which are primes by the claim) $\square$

Corollary 79 Let k be any field then $\dim(k[x_1,\dots,x_n]) = n$ ($\dim \mathbb{A}^n = n$)

Proof/ · STEP 1 $\dim \bar{k}[x_1,\dots,x_n] = n$.

↘ Note that this implies that if R affine ring over a field ($R \cong k[x_1,\dots,x_n]/I$ sec 10) then $\dim R < \infty$. So the claim is after defn ✓.

$\ge$) ✓ $\bar{k}$ is a field so we already discussed this.

$\le$) We need $P \subseteq S = \bar{k}[x_1,\dots,x_n]$ max ideal then $\operatorname{codim}(P) \le n$.

We know that $P = \langle x_1-a_1,\dots,x_n-a_n\rangle$ by Nullstellensatz (which uses Noether norm)

Codim $P = n$ by 78. So $\dim(\bar{k}[x_1,\dots,x_n]) = n$

· STEP 2 Conclude

But $k[x_1,\dots,x_n] \subseteq \bar{k}[x_1,\dots,x_n]$ is an integral extension (easy an elementary)

By prop 73 with $I = 0$, φ inclusion map, $\dim k[x_1,\dots,x_n] = \dim \bar{k}[x_1,\dots,x_n] = n$. $\square$

We now provide a converse of PIT

Theorem 80 (Reverse PIT) Let R be a Noetherian ring, P prime $\operatorname{codim}(P) = c \in \mathbb{N}$ then P minimal over an ideal generated by c elements.

↖ that is why we define codim of arbitrary ideal.

Proof/ We will show that $\exists x_1,\dots,x_c \in P$: $\operatorname{codim}(\langle x_1,\dots,x_c\rangle) = c$. If P not minimal over $\langle x_1,\dots,x_c\rangle$ $\exists \langle x_1,\dots,x_c\rangle \subseteq \underset{\in \operatorname{Spec}(R)}{Q} \subsetneq P$. Now $\operatorname{codim} Q < \underset{c}{\operatorname{Codim} P}$ so $\underset{<c}{\operatorname{codim}(\langle x_1,\dots,x_c\rangle)}$ ↯.

Thus NTS $\exists x_1, \ldots, x_c \in P$: codim$(\langle x_1, \ldots, x_c \rangle) = c$. We do it by induction on $0 \leq r \leq c$.
For $r = 0$, codim $0 = 0$ (take minimal prime over 0 and see defn). Assume we have $x_1, \ldots, x_{r-1} \in P$ codim $\langle x_1, \ldots, x_{r-1} \rangle = r-1 < c$. Let $P_1, \ldots, P_m$ be all the minimal primes over $\langle x_1, \ldots, x_{r-1} \rangle$. By PIT codim$(P_i) = r-1$ (cex b before def of associated)

If $P \subseteq \bigcup_{i=1}^{m} P_i$ by prime avoidance $P \subseteq P_i$ but codim $P_i = r-1 < c$ ↯ So $\exists x_r \in P$: $x_r \notin \bigcup P_i$. Now by PIT codim$(\langle x_1, \ldots, x_r \rangle) = r$: Codim$(\langle x_1, \ldots, x_r \rangle) \leq r$ by PIT and the note before big example. However if you take any prime over $\langle x_1, \ldots, x_r \rangle$ it contains by descending chain condition of prime ideals a minimal prime over $\langle x_1, \ldots, x_{r-1} \rangle$, say P_i. But $x_r \notin P_i$ so it contains it properly. Thus codim (any prime $\supseteq \langle x_1, \ldots, x_r \rangle$) $>$ codim $P_i = r-1$.

This shows that $\exists x_1, \ldots, x_c \in P$ (distinct) such that codim$(\langle x_1, \ldots, x_c \rangle) = c$ as wanted □

<u>Corollary 81</u> Let R be a Noetherian domain. R UFD iff all primes of codim 1 are principal.

Proof/ By PIT, Reverse PIT codim 1 prime ideals are exactly minimal primes over principal ideals, now apply prop 36.

□

21 SYSTEMS OF PARAMETERS

(~ 10.1 Eis + Equiv with trdeg $\subseteq$ Ch13)

Again all our rings will be Noetherian.

<u>Corollary 82</u> Let R be a local Noetherian ring, $m \subseteq R$ max ideal. Then $\dim(R)$ is the smallest d : $\exists x_1, \ldots, x_d \in m$: $m^n \subseteq \langle x_1, \ldots, x_d \rangle$ $\forall n \gg 0$ (suff large)

Proof/ $m^n \subseteq \langle x_1, \ldots, x_d \rangle$ $\forall n \gg 0$ iff $R/\langle x_1, \ldots, x_d \rangle$ Artinian iff m minimal over $\langle x_1, \ldots, x_d \rangle$

(Corollary 23 $M = R/\langle x_1, \ldots, x_d \rangle$)

(again either 23 or 20 work) but we are using R local.

Now we are in a (noeth) local ring so $\dim R$ = codim m.
PIT + Reverse PIT say that codim m is the smallest number of elmts in the ring such that m is minimal over an ideal generated by that many elmts.

□

<u>DEF</u> Let R be local Noeth with $m \subseteq R$ the max ideal. An ideal $I \subseteq m$ has finite colength if R/I Artinian. Note this is equivalent to say
- length$(R/I) < \infty$
- m minimal over I
- $m^n \subseteq I$ for $n \gg 0$.

(by Cor 20, 23 as in the previous proof)

R/I is an R-module. See stupid obs in proof of 20.

A sequence $x_1, \ldots, x_d \in m$ is a system of parameters of (R, m) if $d = \dim R$ and $R/\langle x_1, \ldots, x_d \rangle$ Artinian.

(again we get those equivalences)

Geometrically ...

Geometric meaning Read p.237 from Eisenbud for (very) rough idea. I will not think much for now and wait. He made a few claims but they needed facts about alg geo that we have not covered. So better to not think to deeply about meaning for now. If I ever encounter this I'll probably know the needed geometry. (He said take $X \subseteq \mathbb{A}^n$ alg set $p \in X$, it corresponds to $P \in \operatorname{Spec-m}$ and said something like if $x_1, \dots, x_d$ system of param then p isolated in $Z(\langle x_1, \dots, x_n \rangle)$).
(poly functions ...)

Don't worry too much.

DEF Let R be local Noeth with max ideal m. Let $I \subseteq m$ be an ideal, M fg R-module we say that I has finite colength on M if $\operatorname{length}(M/IM) < \infty$.

* **Observation**: M/IM has finite length $\xleftrightarrow{c23}$ M/IM annihilated by some product of max ideals

$\underset{R \text{ local}}{\longleftrightarrow}$ $m^n \subseteq \operatorname{ann}(M/IM)$ $\forall n \gg 0$ $\longleftrightarrow$ $m = \sqrt{\operatorname{ann}(M/IM)}$ or $M/IM = 0$

$\leftarrow)$ ✓

$\rightarrow)$ $m^n \subseteq \operatorname{ann}(M/IM)$ implies (taking radicals) $m \subseteq \sqrt{\operatorname{ann}(M/IM)}$. m is maximal so they are equal as long as $\sqrt{\operatorname{ann}(M/IM)} \neq R$ (but $\sqrt{\operatorname{ann}(M/IM)} = R \rightarrow 1 \in \operatorname{ann}(M/IM)$ so $M/IM = 0$)

(Of course if R field M Rvs $\overset{\text{linear algebra}}{\dim_R(M)} \neq$ Krull dim of M)

DEF Let R be a ring (not nec noeth; any commutative) M an R-module. We define the (Krull) dimension and codimension of M (write $\dim(M)$, $\operatorname{codim} M$) to be the dim / codim of $\operatorname{ann}(M)$.

If $M \subseteq R$ ideal there is a conflict of defn. Perhaps because there two defns (dim ideal / dim module) give such different answers (ex in Eis p228) there does not seem to be much conflict. It will be clear. If we take I ideal and say $\dim(I)$ we mean $\dim(R/I)$ ...

Prop 83 Let R be a Noetherian ring, $I \subseteq R$, M a fg R-module. Then $\sqrt{\operatorname{ann}(M/IM)} = \sqrt{I + \operatorname{ann}(M)}$

Assume R local with max ideal m. Then

i) I has finite colength on M iff $m^n \subseteq I + \operatorname{ann}(M)$ $\forall n \gg 0$ iff I has finite colength on $R/\operatorname{ann}(M)$

ii) Given a short exact sequence of R-modules (all fg) $0 \to M' \to M \to M'' \to 0$ then I has finite colength on M iff I has finite colength on M' and M''.

iii) $\dim M$ = least d st $\exists$ ideal of finite colength on M gen by d elements

Proof/ We first show $\sqrt{\operatorname{ann}(M/IM)} = \sqrt{I + \operatorname{ann}(M)}$. By Corollary 15 NTS

That $P \in \operatorname{Spec}(R)$ $\operatorname{ann}(M/IM) \subseteq P$ iff $P \supseteq \operatorname{ann}(M) + I$

Now $P \supseteq \mathrm{ann}(M/IM) \underset{\text{prop 11}}{\longleftrightarrow} (M/IM)_P \neq 0 \underset{\substack{\text{obs 2}\\ \text{proof}\\ \text{of thm 19}}}{\longleftrightarrow} M_P/(IM)_P \neq 0 \longleftrightarrow M_P/I_PM_P \neq 0$

$\longleftrightarrow M_P \neq 0$ and $I_P \subseteq P_P \longleftrightarrow P \supseteq I + \mathrm{Ann}(M)$

$\rightarrow$) If $M_P = 0$ or $I_P \not\subseteq P_P$ then $M_P = 0$ or $I_P = R_P$ (R_P local) and in any of these $M_P/I_PM_P = 0$

$\leftarrow$) NAK

prop 11 + $I_P \subseteq P_P \leftrightarrow I \subseteq P$ (routine ...)

Now we prove i): Set $\bar{R} := R/\mathrm{ann}(M)$ then $\mathrm{ann}(\bar{R}/I\bar{R}) = I + \mathrm{ann}(M)$ (directly see them)

I has finite colength on M $\underset{\text{obs}\,*}{\longleftrightarrow} m^n \subseteq \mathrm{ann}(M/IM)\ \forall n \gg 0 \underset{\text{obs}\,*}{\longleftrightarrow} m = \sqrt{\mathrm{ann}(M/IM)}$ or $M/IM = 0$

$\underset{\text{(first part)}}{\longleftrightarrow} m = \sqrt{I + \mathrm{ann}(M)}$ or $M = IM \longleftrightarrow m = \sqrt{I + \mathrm{ann}(M)}$ or $M = (I + \mathrm{ann}(M))M \underset{\text{obs}\,*}{\longleftrightarrow} m^n \subseteq$ $I + \mathrm{ann}(M)\ \forall n \gg 0 \underset{\text{obs}}{\longleftrightarrow}$ I has finite colength on $R/\mathrm{ann}(M)$

ii) $0 \to M' \to M \to M'' \to 0$. If we tensor by R/I we get (prop 10)

$$M' \otimes_R R/I \to M \otimes_R R/I \to M'' \otimes_R R/I \to 0$$ (this homs come from the ones above as in prop 10

But canonically this gives (via the important idea of prop 49) right exact seq

$$M'/IM' \to M/IM \xrightarrow[\text{surj}]{} M''/IM'' \to 0$$

By looking at this we see that if M'/IM', M''/IM'' have finite length then M/IM has finite length so, I finite colength on M', M'' $\to$ I finite colength on M

$M''/IM'' \cong \dfrac{M/IM}{\mathrm{Im}(M'/IM' \to M/IM)}$; by the ex after def of length we are done.

If I has finite colength on M then it has for M', M'' because $\mathrm{ann}(M') \supseteq \mathrm{ann}(M)$, $\mathrm{ann}(M'') \supseteq \mathrm{ann}(M)$ so by i) we are done

iii) $\dim(M) = \dim(\mathrm{ann}(M)) = \dim(R/\mathrm{ann}(M))$. (i) + cor 82 ; worse to write it than say it)

By i) NTS $\dim M$ is the smallest d : $\exists$ ideal of finite colength on $R/\mathrm{ann}(M)$ gen by d elements

By the proof of i) that d is the smallest d, $\exists\, x_1, \ldots, x_d \in m$: $m^n \subseteq \langle x_1, \ldots, x_d \rangle + \mathrm{ann}(M)$ $(I \subseteq m)$

Now by Cor 82 $\dim(R/\mathrm{ann}(M))$ is the smallest t : $\exists\, \bar{y}_1, \ldots, \bar{y}_t \in \dfrac{m + \mathrm{ann}(M)}{\mathrm{ann}(M)}$ with $\dfrac{m^n + \mathrm{ann}(M)}{\mathrm{ann}(M)} \subseteq \langle \bar{y}_1, \ldots, \bar{y}_t \rangle$. If $\mathrm{ann}(M) \neq R$ then $\mathrm{ann}(M) \subseteq m$ max ideal so there two (ideal) things are the same. If $\mathrm{ann}(M) = R$ the situation is trivial

□

The principal ideal thm talks about codim rather than dimension. A version for dimension follows in the local case. The following corollary "justifies" talking about colength.

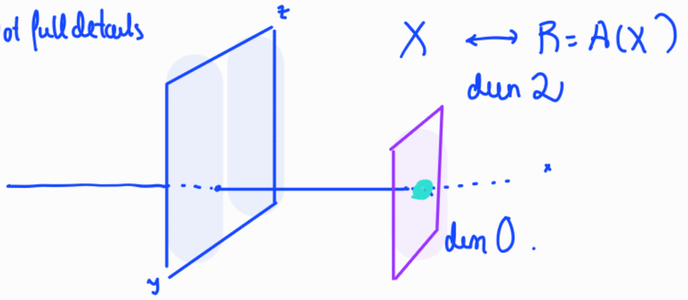
Corollary 84 Let R be a local Noetherian ring with max ideal m. M a fg R-module and $x \in m$ then $\dim(M/xM) \geq \dim M - 1$. $\langle x \rangle M$ (R-submodule)

- **Stupid obs** $\dim(M/xM) \leq \dim M$: Of course $\mathrm{ann}(M/xM) \supseteq \mathrm{ann}(M)$. Now $\dim(M) =$ $= \dim(\mathrm{ann}(M)) = \dim(R/\mathrm{ann}(M)) = \underset{P_i \in \mathrm{Spec}(R)}{\sup\{r : \mathrm{ann}(M) \subseteq P_0 \subsetneq P_1 \cdots \subsetneq P_r\}} \underset{\text{clear}}{\geq} \underset{P_i \in \mathrm{Spec}(R)}{\sup\{r : \mathrm{ann}(M/xM) \subsetneq P_0 \cdots \subsetneq P_r\}}$ $= \dim(R/\mathrm{ann}(M/xM)) = \dim(M/xM)$.

- Applied to R, $\dim(R) - 1 \leq \dim(\underset{\text{ideal gen by } x}{\langle x \rangle})$ so when we cut out by poly equation dimension goes down by at most one.

- Local is needed. If not, trivial counterexample.

Not full details



$f = x - 1 + \langle xy, xz \rangle \in A(X) = k[x,y,z]/\langle xy, xz \rangle$

let $J = fR$ → $\langle f \rangle$ in R. This ideal corresponds to $Z(f)$ (in X; we consider poly functions in X) which is ● (we are cutting out by ). Easily see that since this is a point $\dim(\text{Ideal}) = 0$ which is $\dim(R/fR)$; so we go down by 2

Proof/ let $d = \dim(M/xM)$, by the last prop $\exists\, x_1, \ldots, x_d \in m$ st $\langle x_1, \ldots, x_d \rangle$ has finite (see def of finite colength) colength on M/xM. This means that the module $\dfrac{M/xM}{\langle x_1, \ldots, x_d \rangle M/xM}$ has finite length

$$\left(\begin{array}{ccc} M/xM & \longrightarrow & M/\langle x, x_1, \ldots, x_d \rangle M \\ a + xM & \longmapsfrom & a + \langle x, x_1, \ldots, x_d \rangle M \end{array} \right)$$

But this is iso to $M/\langle x, x_1, \ldots, x_d \rangle M$ so $\langle x, x_1, \ldots, x_d \rangle$ has finite colength thus $\dim M \leq d+1$ (by last prop) $\square$

Equivalence with tr.deg def. It is a good moment to make sense of this.

Recall that when $X \subseteq \mathbb{A}^n = k^n$ irreducible alg set we said that classically the dimension of X is $\mathrm{trdeg}_k(K(A(X)))$ ($A(X) = k[x_1, \ldots, x_n]/I(X)$ affine domain over k).

Goal A affine domain over k, then $\dim(A)$ (krull dim) $= \mathrm{tr.deg}_k(K(A))$ ← abusively $\mathrm{tr.deg}_k(A)$ (see $p^{290}_{E_{15}}$)

By Noether Normalization $A \supseteq \underset{k\text{-subalg}}{S} \underset{\text{as } k\text{-alg}}{\cong} k[x_1, \ldots, x_m]$ and A finitely generated as an S module.

↙ even if I write this I mean the elmts in S.

Claim $x_1, \dots, x_m$ are a transcendence basis of $K(A)$ over k.

(Not get confused, here S is the subring and the tr basis $\{x_1, \dots x_n\} \subseteq S$)

- Alg indep over k: This is trivial. Let $f \in \overset{\swarrow \text{ poly ring}}{k[y_1, \dots, y_n]} \setminus \{0\}$; $f(x_1, \dots, x_n) \neq 0$
- $k(x_1, \dots, x_m) \subseteq K(A)$ algebraic extension.

To see this, note $k(x_1, \dots, x_n) = K(S)$ (fraction field of S). By L43, A finite over S implies A integral over S. It is trivial that $K(A)$ algebraic over $K(S)$ ($a/t \in K(A)$), check that a, t are alg over $k(S)$; clear since they are integral over S so $a/_t$ alg).

Thus $\text{tr.deg}_k(K(A)) = m$. Now $\dim(S) = m$ by corollary 79. $A \supseteq S$ integral so by prop 73 $\dim(A) =$
$= \dim(S) = m$ //

Now we have proved all the notes after the defn of Krull dim. Initially Anders gave another proof in which he said that $\dim A = \dim A_q$ because $A \to A_q$ is flat and flatness preserves
(localit at a point)

dimension. It is a good moment to digress a little bit and study flatness. We've been avoiding it and it is embedded in Eis. Then we will go back to 10.2

(! means kind of extra) • 22 FLAT MODULES (Introduced by Serre in 1956)

Let R be a ring, M - R module. If we have a short exact seq $0 \to N' \to \overset{(R\text{-module})}{N} \to N'' \to 0$ and we get a right exact seq $N' \otimes_R M \to N \otimes_R M \to N'' \otimes_R M \to 0$

DEF Let R be a ring, M an R-module. We say that M is flat if $\forall\ 0 \to N' \to N$ left exact seq of R-modules we get $0 \to N' \otimes_R M \to N \otimes_R M$.
(This is $\forall\ N' \xrightarrow{\varphi} N$ injective R-hom ; $N' \otimes_R M \xrightarrow{\varphi \otimes \mathrm{Id}} N \otimes_R M$ is also injective)
therefore transforms short exact in short exact.

<u>Examples</u> i) $R = \mathbb{Z}$, $M = \mathbb{Z}/_{2\mathbb{Z}}$ consider $0 \to \mathbb{Z} \xrightarrow{2\cdot} \mathbb{Z}$ (injective)
but if we tensor with M, $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/_{2\mathbb{Z}} \longrightarrow \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/_{2\mathbb{Z}}$ we see that this is the zero map

$$\lambda \otimes 1 \longmapsto \underset{\text{alg qual}}{2\lambda \otimes 1 \overset{\downarrow}{=}} \lambda \otimes 2 \cdot 1 = \lambda \otimes 0 \underset{\text{alg qual.}}{\overset{\downarrow}{=}} 0$$

ii) Let $F = R^n$ free. It is flat.

$N' \xrightarrow{\varphi} N$ 1-1 then $N' \otimes_R R^n \to N \otimes_R R^n$ 1-1 since canonically (see ex after prop10)
this is $\underset{n \text{ copies}}{N' \oplus \cdots \oplus N'} \longrightarrow N \oplus \cdots \oplus N$. What we are saying is precisely that
$(n_1', \dots, n_n') \longmapsto (\varphi(n_1'), \dots, \varphi(n_n'))$) (Good ✓. This type of thing will appear again)

$N' \otimes_R R^n$ canonically isom to $N' \oplus \dots \oplus N'$; $N \otimes_R R^n$ canonically isom to $N \oplus \dots \oplus N$ and the map

$\varphi\otimes Id$ translated to the canonical isoms is precisely the one we write, so we see is 1-1 (usual details, see prop 10)

iii) $U\subseteq R$ mult closed, $U^{-1}R$ is a flat R-module

$N\to N'$ 1-1 if we tensor $N\otimes_R U^{-1}R \to N'\otimes_R U^{-1}R$ and loc. is exact.

$$\begin{tikzcd} N\otimes_R U^{-1}R \arrow[r] \arrow[d, equal] & N'\otimes_R U^{-1}R \arrow[d, equal] \\ U^{-1}N \arrow[r] & U^{-1}M \end{tikzcd}$$

(everything is done canonically so diagram commutes) same words as above

iv) M_1, M_2 flat then $M_1\otimes_R M_2$ is flat (also easy to check; associativity of tensor)

In particular if M flat $U^{-1}M$ also flat. ($M\otimes_R U^{-1}R \underset{\downarrow}{=} U^{-1}M$)
can. isom; we did this

DEF A ring hom $\varphi: R\to S$ is flat if S is flat as an R-module.
✓ see alg qual.

Example Let $f\in R[X]$ monic of degree d. $R[X]/\langle f\rangle$ free R-module with basis $\{\bar{1}, \bar{x}, \dots, \bar{x}^{d-1}\}$ so $R[X]/\langle f\rangle$ flat by example ii). Thus $R\longrightarrow R[X]/\langle f\rangle$ flat.

Note Let $x\in R$ nzd. M a flat R-module then x is a nzd on M.

$R\xrightarrow{x\cdot}R$ is 1-1, now $R\otimes_R M\longrightarrow R\otimes_R M$ is 1-1 but this translates to ...

$$\begin{tikzcd} R\otimes_R M \arrow[r] \arrow[d, equal] \arrow[dr, phantom, "\text{commutes}"] & R\otimes_R M \arrow[d, equal, "\text{canonically isom.}"] \\ M \arrow[r, "x\cdot"'] & M \end{tikzcd}$$

(same details, we end up with $M\xrightarrow[x\cdot]{} M$

(This theory usually comes with theory of tor functor; wait for now)

Exercise Let S be a flat R-module. $R\longrightarrow\tilde{R}$ ring hom, then $\tilde{R}\otimes_R S$ is a flat $\tilde{R}$-module
($\tilde{R}$ R-module)

This is ex 2.20 A&M. Idea, start with $N\xrightarrow{\varphi}M$ $\tilde{R}$ hom and $N\otimes_{\tilde{R}}(\tilde{R}\otimes_R S) =$

$\underset{\downarrow}{=} (N\otimes_{\tilde{R}}\tilde{R})\otimes_R S \underset{\downarrow}{=} N\otimes_R S$. With some easy details we can conclude.

can isom
(see ex in prop 48)

Exercise we did
can isom)

naturally $\tilde{R}$-module

It can be nice to now define:

DEF let $k=\bar{k}$, $X\subseteq \mathbb{A}^n = k^n$, $Y\subseteq \mathbb{A}^m = k^m$ algebraic sets. Then a map $\Psi: X\longrightarrow Y$ is called a morphism of alg sets if $\exists f_1,\dots,f_m\in A(X)$: $\Psi(a_1,\dots,a_n) = (f_1(a_1,\dots,a_n),\dots,f_m(a_1,\dots,a_n))$

Notes i) If we see $A(X)$ as $k[x_1,\dots,x_n]/I(X)$, f_i = poly + $I(X)$. But we know evaluation of poly is well defined so what we say is perfectly clear (abusively we say $f_i\in A(X)$ but we mean a rep.)

If we see $A(X)$ as polys in $k[x_1,\dots,x_n]$ restricted to X no trouble.

ii) In alg geo we will see that this is a "theorem" since we will have morphism as something much more general and we will have to check that in alg sets translates to this (that will be a local defn and our discussion on regular functions will play a role. (E is given this def directly, not as a thm
so good enough for comm. alg)

* Not forget that here the geometry is just motiv of why we say things and to make things more intuitive. But we are doing comm. alg.

iii) $\psi : X \to Y$ morphism induces a ring homomorphism $\left\{ \begin{array}{l} k[y_1, \dots, y_m] \xrightarrow{\psi^\#} k[x_1, \dots, x_n] \\ y_i \longmapsto f_i(x_1, \dots, x_n) \end{array} \right.$

It is easy to see that if $g(y_1, \dots, y_m) \in \mathcal{I}(Y)$, then $\psi^\#(g) \in \mathcal{I}(X)$ thus this induces a map which we also call $\psi^\# : A(Y) \to A(X)$
(k-alg hom)

(If we regard $A(X)$, $A(Y)$ as ring of functions on X, Y then $\psi^\#$ is just composition with ψ.)

$\psi^\#(g)$ as a poly in X is $g(f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n))$; $\psi^\#(g)(a_1, \dots, a_n) = g(\psi(a_1, \dots, a_n))$

iv) The process can be reversed, given $\varphi : A(Y) \to A(X)$ k-alg hom, if we choose f_i rep of $\varphi(y_i)$ we can use those f_i to define a morphism $X \xrightarrow{\psi} Y$ (if we do $\psi^\#$ we get φ)

So morphism of alg sets determines unique k-alg hom and the other way around.

v) Suppose $\psi : X \to Y$ morphism $\psi^\# : A(Y) \longrightarrow A(X)$ induced. We already had a correspondence

$\{\text{Closed subsets of } X\} \xleftrightarrow{\theta_1} \{\text{radical ideals of } A(X)\}$ (*)
$\{\text{closed subsets of } Y\} \xleftrightarrow[\theta_2]{} \{\text{radical ideals of } A(Y)\}$

Where irred closed ones corresponded to primes and points to maximal ideals.

Let $p \in X$, who is $\psi(p)$ in terms of $\psi^\#$? $p \underset{\theta_1}{\equiv} P \in \text{Spec-m}(A(X))$ we know how max ideals are by nullst so $A(X)/P = \dfrac{k[x_1, \dots, x_n]/\mathcal{I}(X)}{(x_1 - a_1, \dots, x_n - a_n)/\mathcal{I}(X)} \simeq \dfrac{k[x_1, \dots, x_n]}{(x_1 - a_1, \dots, x_n - a_n)} \simeq k$ (bequeg of course)

$\downarrow$
$(a_1, \dots, a_n) = p$

The composite $A(Y) \xrightarrow{\psi^\#} A(X) \xrightarrow{\xi} A(X)/P = k$ is a surjection because $\psi^\#(k) = k$ (k-alg hom) (*)

The kernel of that composite map is a max ideal, by Nullstellensatz it corresponds to a point $q \in Y$

What happens is that $\psi(p) = q$. (routinary checks) (Read paragraph before C.1.10 Eis for extra thing)

Need to show that the ideal of poly functions vanishing at $\psi(p)$ is that kernel

$\{ g \in k[y_1, \dots, y_m]/\mathcal{I}(Y) : g(f_1(a_1, \dots, a_n), \dots, f_m(a_1, \dots, a_n)) = 0 \} = \{ g \in k[y_1, \dots, y_m]/\mathcal{I}(Y) : \psi^\#(g)(p) = 0 \}$

$= \{ g \in A(Y) : \psi^\#(g) \in P \} = \text{Ker}(\xi \circ \psi^\#)$

$\psi^\#$ gives map $\text{spec-m}(A(X)) \to \text{Spec-m}(A(Y))$ which is the map $\psi : X \to Y$

Thus the ideal corresp to $\overset{\psi(p)}{\overset{\shortparallel}{q}}$ is sent by $\psi^\#$ to a set contained in the ideal corresp to p.

Example $\begin{array}{l} k[t] \xrightarrow{\psi^\#} k[x, y] \\ t \longmapsto x^2 \end{array}$ $\equiv$ $\begin{array}{l} \mathbb{A}^2 \xrightarrow{\psi} \mathbb{A}^1 \\ (x, y) \longmapsto x^2 \end{array}$. Take $p = (1, 0)$, $\psi(p) = 1$

the corresp ideal is $\langle t - 1 \rangle$ maximal in $k[t]$. $\psi^\#(\langle t - 1 \rangle)$ is not an ideal but generates $\langle x^2 - 1 \rangle = x^2 - 1 \cdot k[x, y]$. This ideal has zero set

$\subsetneq \langle x - 1, y \rangle$ ideal corresp to p.

$\psi^{-1}(q)$.

Moreover if $p=(0,0)$, $\psi(p)=0$ the ideal is $\langle t\rangle$ and the ideal gen by the image is $x^2k[x,y]$ not even radical.

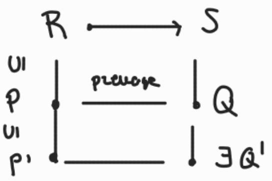
DEF A morphism of alg sets $X \to Y$ is said to be flat if the ring hom $A(Y)\to A(X)$ is flat. (Def for the class)

- He said that "open embeddings", "projections" are flat (I do not go into much detail with this since I think is better to see it in alg geo if appears; notion of products..., more general def of morphism would be better...)

- A good reason to care about flat morph. is that if $\varphi : X\to Y$ flat then $\varphi(X)$ dense and $\forall y\in\varphi(X)$, $\dim(\varphi^{-1}(y)) = \dim X - \dim Y$; so very nice properties

It is convenient to review "Going up" now.

Theorem 85 (Going down, flat version) Let $\varphi : R\to S$ flat hom of Noetherian rings. Let $P'\subseteq P\subseteq R$, $P,P'\in\mathrm{Spec}(R)$. $Q\in\mathrm{Spec}(S)$ and $P = R\cap Q$ ($=\varphi^{-1}(Q)$). Then $\exists\, Q'\in\mathrm{Spec}(S)$ such that $P' = R\cap Q'$, $Q'\subseteq Q$



Proof/ Consider $\langle\varphi(P')\rangle \subseteq \langle\varphi(P)\rangle \subseteq Q$ $\overset{}{=} P'S$ we work in a Noetherian ring so $\exists\, Q'\subseteq Q$, $Q'\in\mathrm{Spec}(S)$ minimal over $\langle\varphi(P')\rangle$. (By desc chain cond for primes for example). The claim is that this is the Q' we need so NTS $\varphi^{-1}(Q') = P'$

We may assume $P'=0$ Note $S/\langle\varphi(P')\rangle \underset{\text{canonically iso}}{\cong}$ $S\otimes_R R/_{P'}$ is a flat $R/_{P'}$ module by the last exercise. (Important idea in cor 49)

So if we assume true in that case we apply the thm for $R/_{P'}$ (instead of R), $S/_{\langle\varphi(P')\rangle}$ instead of S. With some obvious details we find Q'.

Need to show $\varphi^{-1}(Q') = \{0\}$. But now $0 = P'\in\mathrm{Spec}(R)$ so we have that R is a domain (we have reduced the situation to consider this case). Thus $\forall x\in R\setminus\{0\}$ x is a nzd thus $\varphi(x)$ is a nzd on S by the note before the exercise (S flat over R).
(mult by x in S as an R-module is mult by $\varphi(x)$ in S as a ring)

On the other hand Q' minimal prime in S. By thm 30, $Q'\in\mathrm{Ass}_S(S)$ so again by thm 30 Q' consists of zero divisors so if $x\in R\setminus\{0\}$ $\varphi(x)\notin Q'$ thus $\varphi^{-1}(Q')=\{0\}$ □

Geometry discussion: Let X, Y be alg sets. Let $R = A(Y)$, $S = A(X)$ and take $R \xrightarrow{\varphi} S$ k-alg hom. This gives a morphism $X \xrightarrow{\psi} Y$. Suppose that going down holds between $R \overset{\varphi}{-} S$ (saying φ flat is enough)

Q corresponds (table before L25) to a closed irreducible subset Z of X. And W closed irreducible subset of Y such that $\psi(Z) \subset W$. If going down holds with a bit of work one can prove that $\exists$ $Z \subset V \subseteq X$ alg subset such that $\psi(V)$ dense in W.

- A more careful analysis similar to C65 says that $\varphi: X \to Y$ st the induced k-alg hom $\psi: A(Y) \to A(X)$ is flat ($A(X)$ flat $A(Y)$ module) then φ carries open sets to open sets.
- Knowing these things one can by "drawing" already know if a given map is flat or not (see fig 10.4 Eis)

(p293 Eis ; thm A)

"If A affine domain over k, $I \subseteq A$ ideal $\dim I + \operatorname{codim} I = \dim A$." We did not prove it. It is C.13.4 In Eisenbud. We know that if A affine domain over k $\dim A = \operatorname{trdeg}_k(K(A))$. With a bit of work (going down for integral ext ; stronger Noether norm) one can prove that the length of ANY maximal chain of primes is this $\dim A$. Thus $\dim A$ can be computed in terms of a maximal chain of primes that includes a given minimal prime over I. Now the result follows.

VIDEO : Affine domains are catenary

22. DIMENSION OF BASE AND FIBER. (~10.2)

We now see flatness and dimension theory.

Theorem 85 Let R, S local noeth rings with max ideals m, n respect. Let $\varphi: R \to S$ local ring hom ($\varphi(m) \subseteq n$). Then $\dim(S) \leq \dim(R) + \dim(S/\underbrace{mS}_{\langle \varphi(m) \rangle})$

If S flat over R then we have equality. (He gave interpretation)

Proof/ Let $d = \dim(R)$, $e = \dim(S/mS)$. By Cor 82 $\exists x_1, \ldots, x_d \in m$: $m^s \subseteq \langle x_1, \ldots, x_d \rangle$ $\forall s \gg 0$. Similarly $\exists y_1, \ldots, y_e \in n$: $n^t \subseteq mS + \langle y_1, \ldots, y_e \rangle$ $\forall t \gg 0$

Note $n^{st} \subseteq (mS + \langle y_1, \ldots, y_e \rangle)^s \subseteq m^s S + \langle y_1, \ldots, y_e \rangle \subseteq \langle x_1, \ldots, x_d, y_1, \ldots, y_e \rangle$ for $s, t \gg 0$

By C82 $\dim S \leq e + d$.

(minimal prime)

Now if S is flat over R. We start by realizing the dimension. Of course we can choose $Q \supseteq mS$ st $\dim(S/mS) = \dim(S/Q)$. In general $\dim(S) \geq \dim(S/Q) + \operatorname{codim}(Q) = \dim(S/mS) + \operatorname{codim}(Q)$. If we show $\operatorname{codim} Q \geq \dim R$ then $\dim S \geq \dim(S/mS) + \dim R$ ✓. So NTS $\operatorname{codim} Q \geq \dim R$

Recall we are assume $\varphi : R \to S$ flat. Note $R \cap Q = \varphi^{-1}(Q) \supseteq \varphi^{-1}(\langle \varphi(m) \rangle) \overset{?}{=} m$ but m is the max ideal (and $\varphi^{-1}(Q) \neq R$ otherwise $1 \in Q$) so $\overset{\text{note } R \cap Q = m}{R \cap Q = n}$. Now by going down we easily

$$\begin{tikzcd}
R \arrow[r, dash] \arrow[d, dash] & S \\
m \arrow[r, dash] \arrow[d, phantom, sloped, "\supsetneq"] & Q \arrow[d, phantom, sloped, "\supsetneq"] \\
P_{d-1} \arrow[d, phantom, sloped, "\supsetneq"] & Q_{d-1} \\
\vdots & \vdots \arrow[d, phantom, sloped, "\supsetneq"] \\
P_0 & Q_0
\end{tikzcd}$$

by successive applications so $\operatorname{codim}(Q) \geq d = \dim R$. □

Some Geometry Let X, Y alg sets $\overset{(k = \bar{k})}{.}$ ← irreducible. $\psi : X \longrightarrow Y$ morphism $y \in Y$, $x \in \psi^{-1}(\{y\})$.

Let $R = A(Y)_{I(\{y\})}$ ← max ideal local ring denoted $\mathcal{O}_{Y,y}$ (noeth) (this is rational functions in $\underset{X}{Y}$ defined in $\underset{x}{y}$)

$S = A(X)_{I(\{x\})}$ local ring denoted $\mathcal{O}_{X,x}$

↓ as when we defined $A(X)$ we could say iso to and we identify.

We can thus define $\psi^{\#} : R \to S$ local ring hom (check)

$g \in R$; $\psi^{\#}(g)(p) = g(\psi(p))$. Then let $m_R = I(\{y\})_{I(\{y\})}$ max ideal of R

Then $\dim S \leq \dim R + \dim\left(S/m_R S\right)$. This can be translated back.

(also he got kind of confused when doing this so just pay attention to dark blue part)

" He ended up saying something like $\dim_X(\psi^{-1}(y)) \geq \dim X - \dim Y$; If I ever need smth like then it will be clear how to prove it because I will know what I need. I have some doubts on his translation. For example I see $\dim X = \dim S$. Since $A(X)$ affine domain any maximal chain of primes has length $\dim(A(X))$ (not proved) this easily gives $\dim A(X) = \dim(A(X)_{I(\{x\})})$ with prop 8. Still a bit doubtfull about $\dim_X(\psi^{-1}(y))$ part, I think he needs some extra hypothesis. Not worry much but this is the context where it applies."

Corollary 8.6 R Noetherian then $\dim R[X] = \dim R + 1$

Proof / Let R be a field we already know it but notice what would we do if we try to prove it we would try $\dim R[X] = 1$. Well certainly $0 \subsetneq \langle x \rangle$ so $\dim R[X] \geq 1$. On the other hand if $Q \subseteq R[X]$ prime is maximal ($R[X]$ PID, see alg qual) so $0 \subsetneq Q$ thus $\operatorname{codim} Q \geq 1$

But $Q = \langle f \rangle$ so by PIT $\operatorname{codim} Q \leq 1$ so $\dim R[X] = 1$

In general case, <u>Claim</u> $\dim R[x] \geq \dim R + 1$
(we proved it is finite)

let $d = \dim R$, $\exists$ $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_d \subseteq R$ chain of prime ideals. We can turn it into a chain of primes $P_0R[x] \subsetneq P_1R[x] \subsetneq \cdots \subsetneq P_dR[x] \subsetneq P_dR[x] + \langle x \rangle$ chain of primes in $R[x]$

. Why primes? $R[x]/P_iR[x] \cong R/P_i[x]$ domain so $P_iR[x]$ prime.
↳domain

$$R[x]/P_dR[x]+\langle x \rangle \underset{\downarrow}{\cong} R/P_d \text{ domain}$$

elementary exercise, very predictable

. The strict containments are obvious (if $x \in P_dR[x]$ we easily derive contradictions)

<u>Claim</u> $\dim R[x] \leq \dim R+1$: $\dim R[x]$ is finite so will be realised by some chain. Let $Q \subseteq R[x]$ be the biggest prime in that chain. We need (by prop 8) to show $\dim R[x]_Q \leq \dim R+1$

Look at $P := R \cap Q \subseteq R$ prime (usual intersection)

We may assume R local with max ideal P. (Assume true in local case. Now $\dim R_P[x]_{Q \cdot R_P[x]} \leq \dim R_P + 1$. But $R_P[x]_{Q \cdot R_P[x]} = R[x]_Q$ and $\dim R_P \leq \dim R$ easily)
↓
VIDEO: equality C86

Then we have
$$\begin{tikzcd} R \arrow[r] \arrow[rr, bend left] & R[x] \arrow[r] & R[x]_Q \end{tikzcd}$$
the max idea P is sent to smth contained in the max ideal of $R[x]_Q$ so local ring hom. By the last thm $\dim(R[x]_Q) \leq \dim R + \dim\left(\frac{R[x]_Q}{PR[x]_Q}\right)$
↳ P/1

So NTS $\dim(R[x]_Q / PR[x]_Q) \leq 1$

But $P \cdot R[x]_Q \underset{\downarrow}{=} (PR[x])_Q$ so $R[x]_Q / PR[x]_Q = \dfrac{R[x]_Q}{(PR[x])_Q} \underset{\downarrow}{\cong} \left(R[x]/PR[x]\right)_Q \cong$
warning 2 ... proof of prop 14

$\underset{\downarrow}{\cong} (R/P[x])_{Q \subseteq R/P[x]}$
alg qual

But $\dim(R/P[x]) = 1$ (field) so $\dim((R/P[x])_Q) \leq 1$ (prop 8 + def of dim) □

23. REGULAR LOCAL RINGS (~10.3 Eisenbud)

Again all rings are Noetherian.

Let R local Noeth, m max ideal. Let $k = R/m$ field. Then m/m^2 is a k-vsp.

Claim $\dim_k(m/m^2) = \min \#$ of gen of m → (dim as vs. not Krull) \ easy check of well defined operations (intuitive also)

· If $m = \langle x_1, -, x_d \rangle$, $m/m^2 = \text{span}_k \{\bar{x}_1, -, \bar{x}_d\}$ so $\dim_k(m/m^2) \leq \min \#$ gen.

. Choose $x_1, -, x_d \in m$ st $\{\bar{x}_1, -, \bar{x}_d\}$ k-basis of m/m^2.
Note $m = \langle x_1, -, x_d \rangle + m^2$ thus by Nak $m = \langle x_1, -, x_d \rangle$ so $\dim_k(m/m^2) \geq \min \#$ of gens.

Thus $\dim(R) \leq \dim_k(m/m^2)$ (by C82 for example ; or $\boxed{\dim R = \text{codim}\, m} \underset{PIT}{\leq} d$)

DEF Let R be a Noetherian ring assume it is local with max ideal m. We say that R is regular (local) if $\dim R = \dim_k(m/m^2)$ (PIT says that if $\dim R = d$, then m can't be generated by less than d elmts. Regular: when it can be generated by exactly d.)

Examples i) $k[x_1, -, x_n]_{\langle x_1, -, x_n \rangle}$ local ✓ noeth ✓, max ideal is $\underset{\langle x_1, -, x_n \rangle}{\langle x_1, -, x_n \rangle} \overset{\text{wrong !!}}{\leq} k[x_1, -, x_n]_{\langle x_1, - x_n \rangle}$ can be generated by n elmts which is $\dim(k[x_1, -, x_n]_{\langle x_1, -, x_n \rangle})$ easily
(we can find chain of length n and dim loc $\underset{\text{by prop 8}}{\leq}$ dim not loc)

ii) $\mathbb{Z}_{\langle p \rangle}$ p prime. Kind of the same argument. ($\dim \mathbb{Z} = 1$)

We'll proof that regular $\overset{R}{\text{local}}$ ring → R domain. It is harder to show R regular local implies UFD (ch 19 Eis we did not get to it and apparently uses homological methods), thus by prop 50 R is normal. (So regular local are nice)

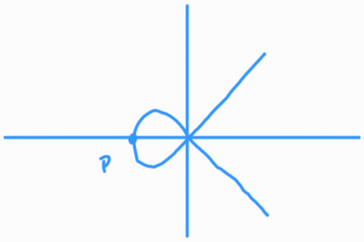
Geometry discussion Let $X \subseteq \mathbb{A}^n$ algebraic set $k = \bar{k}$, $x \in X$. Recall $\mathcal{O}_{X,x} = A(X)_{I(\{x\})}$ (identified with rational functions on X defined at x)

We define $x \in X$ to be nonsingular if $\mathcal{O}_{X,x}$ is regular. (note $\mathcal{O}_{X,x}$ local noeth)
Of course singular if $\mathcal{O}_{X,x}$ not regular.

PLAN:
- Do an example (concludes geometry discussion)
- Prove regular local → domain
- Make sense of nonsingular

/ Section ends

Example: $X = Z(\{y^2 - x^3 - x^2\}) \subseteq \mathbb{A}^2$. Now $A(X) = k[x,y] / \langle y^2 - x^3 - x^2 \rangle$



let $p = (-1, 0)$, $\mathcal{O}_{X,p} = A(X)_{\langle x+1, y \rangle}$. Claim $\langle y^2 - x^3 - x^2 \rangle$ prime (to do this you prove that $y^2 - x^3 - x^2 \in \mathbb{C}[x,y]$ is irreducible. To do so is easy to see that $y^2 - g(x)$ reducible iff $g(x)$ square in $\mathbb{C}[x]$.)

$A(X)$ is an affine domain so its dimension coincides with dim $A(X)_{\langle \overline{x+1}, \overline{y} \rangle}$ (take maximal chain of prime ideals ending at $\langle x+1, y \rangle$, that chain can be used to give a chain of same length in localization. Now by what we did not prove dim $A(X)$ is the length of that chain and the dimension after loc always is equal or lower, the result now follows). Now dim $A(X)$ = dim $(\langle y^2 - x^3 - x^2 \rangle) \underset{\substack{\downarrow \\ \text{affine} \\ \text{dom}}}{=}$ dim $K(x,y)$ - codim $(\langle y^2 - x^3 - x^2 \rangle)$

$= 2 - 1 = 1$. $\left(\begin{array}{l} \text{codim}(\langle y^2 - x^3 - x^2 \rangle) \leq 1 \ \text{PIT} \\ \phantom{\text{codim}(\langle y^2 - x^3 - x^2 \rangle)} > 0 \ \text{trivial, domain} \end{array} \right)$

Thus dim $\mathcal{O}_{X,p} = 1$

To prove that $\mathcal{O}_{X,p}$ is regular we want to see if its max ideal $\langle \overline{x+1}, \overline{y} \rangle_{\langle \overline{x+1}, \overline{y} \rangle}$ is principal

think of it as rational funct in X def in x.

But in $\mathcal{O}_{X,p}$ (abusively) $x+1 = \frac{x^3 - x^2}{x^2} = y^2/x^2$ thus the maximal ideal is generated by $\overline{y}$. So P is Nonsingular (satisfies intuition).

Maybe is better to write $\langle x+1, y \rangle \subseteq \mathcal{O}_{X,p}$ understanding that $x+1 \equiv \frac{x+1}{1}$, $y \equiv \frac{y}{1}$ and $x+1$, y represent equiv classes. (Many ways to think it and write it; if we understand all we can be more abusive)

If we take $q = (0,0)$, $\mathcal{O}_{X,q} = A(X)_{\langle x,y \rangle}$ again has dimension 1 (similar)

Consider the max ideal $m = \langle x, y \rangle \subseteq \mathcal{O}_{X,q}$. If this ideal m not principal, q singular.

We know that $\dim_k(m/m^2)$ is the minimal number of gens. Want to see $\dim_k(m/m^2) = 2$

$m/m^2 \underset{\substack{\downarrow \\ \text{loc properties}}}{=} M/M^2 = \text{span}_k\{x, y\}$ easy to see li (by the relations we mod out) so dim $\nearrow$.

not much detail, just ideas.

$M = \langle x,y \rangle \subseteq A(X)$ also vs as k vs (easy).

$\frac{\mathcal{O}_{X,q}}{m} \cong k$ as fields. (Very plausible; We did not argue)

Corollary 87 Let R be a regular local ring. Then R is a domain.

Proof/ We proceed by induction on $\dim(R)$. If $\dim(R) = 0$ since R is regular local we must or: ideal gen by zero elmts is zero ideal (smallest ideal containing empty set)

have $m = 0$ (otherwise if m would be gen minimally by a positive number of elmts so $\dim R > 0$) and in this case R is a field. Assume now $\dim(R) = d > 0$. Note $m \neq m^2$ by NAK (local, so we can apply it; if $m = m^2 \to m = 0$ so $\dim R = 0$ ↯). Let $P_1, \dots, P_t \subseteq R$ minimal prime ideals. We have that $m \not\subseteq P_i \; \forall i$ (otherwise m minimal so $\dim R = 0$) thus by prime avoidance ($m \not\subseteq m^2$) $\exists x \in m : x \notin m^2 \cup \bigcup_{i=1}^{t} P_i$. Consider $S = R/\langle x \rangle$. If we show that S is a domain we are done. (In that case $\langle x \rangle \subseteq R$ prime. Since $x \notin$ minimal primes $\exists Q \subsetneq \langle x \rangle$ $Q \in \operatorname{Spec}(R)$) now if $y \in Q$, $y = ax$ for $a \in R$. Since $x \notin Q$ $a \in Q$ thus $Q \underset{\supseteq \checkmark}{\subseteq} xQ \underset{\supseteq \checkmark}{\subseteq} mQ$ thus $Q = mQ$. So by NAK $Q = 0$, R/Q was a domain so R domain.)

So NTS S domain. Let $n = m/\langle x \rangle \subseteq S$ the maximal ideal in S. By corollary 84 $\dim S \geq \dim R - 1 = d - 1$. Take $x_2, \dots, x_d \in m$: $\bar{x}, \bar{x}_2, \dots, \bar{x}_d$ is a k-basis of m/m^2 (Prolongation, linear alg) where $k = R/m$. So $m = \langle x, x_2, \dots, x_d \rangle$ as an ideal in R (by another NAK as in the proof of the 1st claim of the section) Thus in S, $n = \langle x_2 + \langle x \rangle, \dots, x_d + \langle x \rangle \rangle \subseteq S$ thus $\dim S \leq d - 1$

↓

PIT (S local so $\dim S$ = codim n)

Thus $\dim S = d - 1$ and since n can be gen by $\dim S$ elmts, S regular local of dimension $d - 1$ so S domain as wanted. □

Now the section is essentially done with the section. However we will add one more geometry discussion trying to understand why we define nonsingular like that. So the following is motivation in which I will try to be as clear as possible; but motivation (so no proof, ... just interesting words)

(- apply thm 8
- apply concep
before L25)

Making sense of nonsingular. *(VIDEO : About nonsing explanation + Picturing local ring at p)

↳ chain of primes in local ring corresponds to....

Anders gives the following discussion for a manifold / $\mathbb{R}$. To avoid defining manifold (which is very easy but I do not have taken a course on it) I'll do this in the context of k-regular surfaces from Análisis 3.

Recall that if $X \subseteq \mathbb{R}^n$ is a k-regular surface (C^∞) we have a notion of tangent vector at a point p

$v \in \mathbb{R}^n$ is a tg vector if $\exists r > 0$ $\alpha : (-r, r) \to X$ diff at $t = 0$ with $\alpha(0) = p$, $\alpha'(0) = v$.

$T_X(p) = \{ v \in \mathbb{R}^n : v \text{ tg vector of } X \text{ at } p \}$ (v space). Now if we have $f : X \longrightarrow \mathbb{R}$ C^∞ (compose with

(change of notation wrt an 3)

chart and get usual C^∞). If you take

$$df_p : T_X(p) \longrightarrow \mathbb{R}$$
$$v \longmapsto \left.\frac{d}{dt}\right|_{t=0} f(\alpha(t))$$

, so $df_p \in T_X(p)^*$

Now if we work over $k = \bar{k}$, and take $p \in \mathbb{A}^n$. Set $T_{\mathbb{A}^n}(p) = k^n$ (there is a notion of tg space in alg geo)

Let $f \in A = k[x_1, -, x_n]$, define $df_p(v) = \sum_{j=1}^{n} \frac{\partial f}{\partial x_j}(p) v_j$, $v \in T_{\mathbb{A}^n}(p)$ (we are trying to do same thing as above)
$\hookrightarrow$ symbolically

Note $T_{\mathbb{A}^n}(p)^*$ the dual has basis $\{dx_1, -, dx_n\}$ where $dx_i : \mathbb{K}^n \to \mathbb{K}$, $(v_1, -, v_n) \mapsto v_i$. It follows That $df_p \in T_{\mathbb{A}^n}(p)^*$ defined by $df_p = \sum_{j=1}^{n} \frac{\partial f}{\partial x_j}(p) dx_j$.

If we take $M_p = I(\{p\}) \subseteq A$ the max ideal corresp to p, $M_p \overset{\text{know}}{=} \langle x_1 - a_1, -, x_n - a_n \rangle$ $p = (a_1, -, a_n)$

We now have a natural isom of k-vs (basis to basis)

$$\begin{tikzcd} T_{\mathbb{A}^n}(p)^* \arrow[r] & M_p / M_p^2 \\ dx_i \arrow[r, mapsto] & (x_i - a_i) + M_p^2 \end{tikzcd}$$

From PIT M_p can't be gen by less than n elmts since we already proved codim $M_p = n$. So dim $M_p/M_p^2 = n$ and $\{x_i - a_i\}$ is a basis by the proof of 1st claim in the section.

Under this isom, $df_p \longmapsto f - f(p) + M_p^2$

$\left(f \equiv f(p) + \sum_{j=1}^{n} \frac{\partial f}{\partial x_j}(p)(x_j - a_j) \mod M_p^2 \right)$

(easy exercise)

This motivates the following defn, $T_{\mathbb{A}^n}(p)^* := M_p / M_p^2$ and $T_{\mathbb{A}^n}(p) = (M_p/M_p^2)^*$

If $f \in A$, we write $df_p = f - f(p) + M_p^2 \in T_{\mathbb{A}^n}(p)^*$ (Everything is as before but very algebraic)

(Since the vs are finite dim the dual of $T_{\mathbb{A}^n}(p)$ is indeed $T_{\mathbb{A}^n}(p)^*$)

More generally if $X \subseteq \mathbb{A}^n$ $p \in X$ algebraic set, we define $T_X(p) = \{ v \in T_{\mathbb{A}^n}(p) : \overset{\text{can evaluate (worst case we ident.)}}{df_p(v)} = 0 \ \forall f \in I(X) \}$

the Zariski tangent space "If v looks like a tg vector to X at p and take f vanishing on X, if you take the derivative of f along v, should be 0"

Note : Recall from functional analysis that if E vspace with norm, E^* dual ; given $A \subseteq E^*$ we have $A^\perp := \{ x \in E : a(x) = 0 \ \forall a \in A \}$. Thus $T_X(p) = N^\perp \subseteq T_{\mathbb{A}^n}(p)$ where $N = \{ df_p : f \in I(X) \} \subseteq T_{\mathbb{A}^n}(p)^*$

Now he argued $T_X(p) \underset{\text{isom I guess}}{=} m_p / m_p^2$. $m_p \subseteq \mathcal{O}_{X,p}$ max ideal. (as what? ; I guess as v spaces)

(I did not fully get it but I don't care much, the steps were $\underset{\substack{\downarrow \\ \text{reasonable}}}{T_X(p) = T_{\mathbb{A}^n}^*(p)/N} \overset{\text{easy}}{=} M_p / M_p^2 + I(X) = m_p / m_p^2$ I think it is a lemma to prove this (Gathmann)

$N^\perp \oplus N \cong T_{\mathbb{A}^n}(p)^*$ (Idk but seems reasonable)

??

??

We now redefine : Let $X = \text{spec-m}(R)$, R affine domain over $k = \bar{k}$, $P \in \text{Spec-m}(R)$ let $T_X(P)^* = P/P^2$ call it cotangent space ; also $T_X(P) := (P/P^2)^*$ as a v space (same note as above)

In the case of $X = Z(y^2 - x^3 - x^2) \subseteq \mathbb{A}^2$ $p = (0,0)$ $\dim_k(m/m^2) = 2$ thus $T_X(p) = T_{\mathbb{A}^2}(p)$

so we see that if something is singular then it has too much dimension (the dimension of X near p (dim $T_X(p)$) is the expected dim (dim $(\mathcal{O}_{X,p})$))

This motivates $p \in X$ nonsingular iff dim $T_X(p) =$ dim $(\mathcal{O}_{X,p})$ (iff $\mathcal{O}_{X,p}$ regular)

expected dimension

<u>Jacobi criterion</u> $X \subseteq \mathbb{A}^n$ alg set, $p \in X$. We have $I(X) \xrightarrow{d} T_{\mathbb{A}^n}(p)^* \twoheadrightarrow T_X(p)^* \longrightarrow 0$ exact

$$f \longmapsto df_p$$

P nonsing iff dim $d(I(X)) = n -$ dim $\mathcal{O}_{X,p}$

(as a vs I guess) (as a ring)

He proves it but I prefer to wait for Gathmann.

24. DISCRETE VALUATION RINGS (~ II.1 E6)

DEF A DVR (discrete valuation ring) is a regular local ring of dim 1. If R DVR with m max ideal we know that m can be generated by one elmt; a generator $m = \langle t \rangle$ is called a regular or uniformizing parameter for R.
(of course $t \neq 0$, if $t = 0$ then $R = C$)

Prop 88 Let R be a DVR with max ideal m. Let $0 \neq f \in K(R)$ (R domain so ∃ quotient field) then $\exists !\ d \in \mathbb{Z}, u \in R^{\times} = R \setminus m$ unit of R st $f = ut^d$ $(m = \langle t \rangle)$

Note i) Of course $u \in R \setminus m$ iff u unit in R (unique ideal containing u is R since R is local)

ii) In particular every ideal of R is of the form $\langle t^d \rangle$ thus R PID and hence R is UFD (we already said that regular local → UFD but here is easy to prove).

Proof/ Existence: CASE 1 $f \in R$ (we are seeing $R \subseteq K(R)$).

If f is a unit ✓. Otherwise $f \in m$ thus $f = f_1 \cdot t$ $f_1 \in R$. If f_1 is a unit we are done, else $f_1 = f_2 t$ $f_2 \in R$ .... The claim is that this has to stop meaning that at some point f_n has to be a unit, therefore $f = \text{unit} \cdot t^d$. If not we get $\langle f \rangle \subsetneq \langle f_1 \rangle \subsetneq \cdots\cdots$

↓ if $f_1 \in f$ then $f_1 = fx = f_1 tx$
Now R domain so $tx = 1$ so $m = R$ ↯

which contradicts Noeth prop.

CASE 2 if $f = g/h \in K(R)$ $g, h \in R$ then $g = u_1 t^{d_1}$, $h = u_2 t^{d_2}$ then $f = u_1/u_2\, t^{d_1 - d_2}$

Uniqueness: $u_1 t^{d_1} = u_2 t^{d_2}$ WMA $d_1 \geq d_2$ then $t^{d_1 - d_2} = u_1/u_2 \in R \setminus m$ thus $d_1 - d_2 = 0$. and now $u_1 = u_2$ since we are in a domain. □

Remark This means we can define $\nu : K(R)^{\times} \longrightarrow \mathbb{Z}$ and this map satisfies
$$f = ut^d \longmapsto d$$

i) $\nu(st) = \nu(s) + \nu(t)$ (group hom). (discrete valuation)
ii) $\nu(s+t) \geq \min\{\nu(s), \nu(t)\}$

Note that $R = \{f \in K(R)^{\times} : \nu(f) \geq 0\} \cup \{0\}$.
↓
understood as $R \subseteq K(R)$

$\supseteq$) ✓

$\subseteq$) Let $f\in R$, $f=ut^d$; if $d<0$ then $t^d=u^{-1}f\in R$ now $t^{-d}\in m$ $(-d>0, m=\langle t\rangle)$

thus $t^d\cdot t^{-d}\in m$ so $1\in m$ ↯.

↱ I added this

DEF Let R be a domain, a valuation on R is a map $v: K(R)^* \longrightarrow G$, where G totally ordered group such that: i) v group hom
ii) $v(a+b)\geq \min(v(a),v(b))$

these are the ones people care because one can always normalize. If v not surj (nonzero; zero are excluded always) $\exists \pi\in K(R)^*$ with smallest valuation. Now define $v'(x)=\frac{v(x)}{v(\pi)}$. v' is onto.

When $G=\mathbb{Z}$ usual order, this is called a discrete valuation. (Also by defn discrete valuations are considered onto)

If you start with a valuation $\overset{S}{\overset{\shortparallel}{\{f\in K(R)^*: v(f)\geq 0\}\cup\{0\}}}$ is the valuation ring of v. It is quite clear that this is a ring, in fact is local with max ideal $\overset{M=}{}\{f\in K(R)^* \mid v(f)>0\}\cup\{0\}$ (it is an ideal with everything outside it a unit. This means it is maximal and the unique one). So from a valuation we get a local ring.

↳ Let $f\in S\setminus M$ then $f\neq 0$, $v(f)=0$. Since $f\in K(R)^*$ we can consider $f^{-1}\in K(R)^*$ note $v(f\cdot f^{-1})=v(1)=0$. Thus $f^{-1}\in S$ so f unit.

$v(f)+v(f^{-1})=v(f^{-1})$

Observation: Let R be a domain. R is a DVR iff $\exists\, v: K(R)^*\longrightarrow\mathbb{Z}$ discrete valuation st R is the valuation ring of v.

$\longrightarrow$) ✓ (Make sure it is onto: If not onto $t=0$ then $m=0$ so $\dim R=0$ ↯)

$\longleftarrow$) We know that R domain, local. $\left(\overset{R=}{m=}\{f\in K(R)^* \mid v(f)\overset{\geq}{>}0\}\cup\{0\}\right)$

·Noetherian: STEP 1: If $x,y\in R$ are st $v(x)=v(y)$ then $v(xy^{-1})=0$ so $xy^{-1}\in\{f\in K(R)^*: v(f)=0\}$ thus $xy^{-1}\in$ units of the valuation ring of v = Units of R. Thus $\langle x\rangle=\langle y\rangle$

STEP 2: If $I\subseteq R$ ideal $\exists$ least integer k st $v(x)=k$ for some $x\in I$. It follows by step 1 that if $y\in R$ $v(y)\geq k$, $y\in I$. So the only nonzero ideals in R are $m_k=\{y\in R: v(y)\geq k\}$. From this we easily see R noetherian.

· $\dim R=1$: Since $v: K(R)^*\longrightarrow\mathbb{Z}$ surjection $\exists x\in K(R)^*: v(x)=1$. Note that $x\in m$. Now $\langle x\rangle$ is an ideal and contains $x\in R$ so it follows (since we have a description of all the ideals) that $m=\langle x\rangle$ $(=m_1)$ and similarly $m_k=\langle x^k\rangle$ $k\geq 1$. Thus $\langle x\rangle$ only nonzero prime hence $\dim(R)=1$. (every nonzero ideal is a power of the maximal ideal) also is clearly regular since m gen by dim(R) elmts.

"The significance of this is: If we consider a $\overset{\text{(irred)}}{\text{curve}}$ (this is intuitively clear but at this point I can take it as alg set $\overset{\text{(irred)}}{\text{of}}$ dim 1) take a nonsingular point. The local ring $\mathcal{O}_{X,P}$ is a DVR (note is regular local and $\dim \mathcal{O}_{X,P}=\dim A(X)=1$ as in the example of Geom. discussion). The valuation of this will tell you the order of vanishing of the rational function; will tell you pole, zero..."

To argue this I needed A(X) domain (to use that maximal chains in affine domains all have same length) maybe it can be done without that assumption (if so I guess that would need more machinery)

literally the same proof

25. SERRE'S CRITERION FOR NORMALITY

This works for any $U \subseteq R$ mult closed with $0 \notin U$

Remark R domain, $K = K(R)$ let $P \in \operatorname{Spec}(R)$, $I \subseteq R$ ideal. We identify I_P with $\{ r/s \in K : r \in I,\ s \in R \setminus P \}$ as a subring of the fraction field (In part $R_P \subseteq K$ when P prime)

$$\begin{tikzcd} I_P \arrow[r] & K \\ \frac{a}{u} \arrow[r, mapsto] & a/u \end{tikzcd}$$ if $a/u \cdot$ then easily $a = 0$)

analogue but easier remark than Warning 2. we have to say that we identify (recall remark about identification) but they are "very" different even in how we denote elements they are equal but the nature is distinct.

Assume $r/s \in K \setminus R$ thus $r \notin \langle s \rangle$. Thus $\langle s \rangle \subsetneq \langle r, s \rangle$ so the ring $\langle r,s \rangle / \langle s \rangle \neq 0$. This means that $\operatorname{ann}\left(\langle r,s \rangle / \langle s \rangle \right)$ is not the unit ideal (obvious by contradiction) (see $\langle r,s \rangle / \langle s \rangle$ as an R-module then ann makes sense)

Thus $\operatorname{ann}\left(\langle r,s \rangle / \langle s \rangle \right) \subseteq Q$ some maximal ideal (of R). Therefore $\langle s \rangle_Q \subsetneq \langle r,s \rangle_Q$ by prop 11 iii. So $r/s \notin R_Q$

(if so $\exists\ r' \in R,\ s' \in R \setminus Q : r'/s' = r/s$ thus $r = \frac{sr'}{s'} \in \langle s \rangle_Q$ ↯)

no need to put $\frac{r}{1}$ because we are in a domain (I embedds in $U^{-1}I$)

So it follows that $R = \bigcap\limits_{P \in \operatorname{Spec-m}(R)} R_P$

$\subseteq$) ✓

$\supseteq$) Let $r/s \in \bigcap R_P$ (note $R_P \subseteq K$ so $r/s \in K$) if $r/s \notin R$ then $\exists Q \in \operatorname{Spec-m}(R) : r/s \notin R_Q$.) ↯

(Also $R \subseteq K(R)$ embedded as a subring $R \overset{\text{ident}}{\cong} \{ r/1 : r \in R \} \subseteq K(R)$.)

Geometry $X \subseteq \mathbb{A}^n$ $(k = \bar{k})$ irreducible alg set, $A(X) = R$ domain. $K(X) := K(R)$ field of rational functions. If $p \in X$ point, $P \subseteq A(X)$ corresponding max ideal $\mathcal{O}_{X,p} = A(X)_P \subseteq K(X)$

Then $A(X) = \bigcap\limits_{p \in X} \mathcal{O}_{X,p} \subseteq K(X)$.

Prop 89 Let R be a Noetherian domain then $R = \bigcap\limits_{\substack{P \text{ assoc to} \\ \text{principal ideal}}} R_P \subseteq K(R)$

$P \in \operatorname{Ass}_R\left(R/\langle a \rangle \right)$)

if P ass to $\langle 0 \rangle$ then $P = \langle 0 \rangle$, $R_P = K(R)$ so no problem !

Proof/ $\subseteq$) ✓

$\supseteq$) Let $r/s \in K(R) \setminus R$. Then as before $r \notin \langle s \rangle$ so $r + \langle s \rangle \neq 0 \in R/\langle s \rangle$. By Corollary 27 this means $\exists\ P \in \operatorname{Ass}\left(R/\langle s \rangle \right)$ such that $\frac{r + \langle s \rangle}{1} \neq 0 \in \left(R/\langle s \rangle \right)_P \underset{\text{canonic}}{\cong} R_P / \langle s \rangle_P$ so this is (image of $\frac{r+\langle s \rangle}{1}$ under the canonic iso)

$r/1 + \langle s \rangle_P \neq 0$ $R_P / \langle s \rangle_P$ so $r/1 \notin \langle s \rangle_P$ and now exactly as above we say that $r/s \notin R_P$. This (exactly as above) gives $\supseteq$.

VIDEO: FUNDAMENTAL IDEA

□

Recall $U \subseteq R$ mult closed. $R \subseteq S$ rings $U^{-1}\left(\overline{R}^S \right) = \overline{U^{-1}R}^{U^{-1}S} \subseteq U^{-1}S$. In part if R domain, $P \in \operatorname{Spec}(R)$

$\overline{R_P}^K = \left(\overline{R}^K \right)_P$ (localizing at $R \setminus P$; $\overline{R}$ R-module) (K identified with K_P of course)

$\overset{\shortparallel}{K = K(R)}$ we already embedded all loc. at mult closed (with no 0) in K .

Theorem 90 (Serre's criterion VS 1) Let R be a Noetherian domain. Then R normal iff $\forall P \subseteq R$ associated to a principal ideal R_P is a DVR or a field.

$\leftarrow$) DVR implies PID (go to the last Observation In the proof we see all ideals are principal) which implies UFD (alg qual) which implies normal (prop 50). Thus $R = \bigcap\limits_{\substack{P \text{ ass to} \\ \text{principal ideal}}} R_P$ is normal since all $R_P \subseteq K$ are normal.

$\rightarrow$) Assume R normal, let $P \subseteq R$ prime associated to $\langle a \rangle$.

Thus $\exists\, \bar{s} \in R/\langle a \rangle$ st $P = \operatorname{ann}(\bar{s}) = \{r \in R : rs \in \langle a \rangle\}$. Consider

$$\begin{tikzcd} R \arrow[r, "\text{ring hom, } R\text{-module hom}"] & R/\langle a \rangle \\ r \arrow[r, mapsto] & rs + \langle a \rangle \end{tikzcd}$$

the kernel is R/P; so

$$\begin{tikzcd} R/P \arrow[r] & R/\langle a \rangle \\ r+P \arrow[r, mapsto] & rs + \langle a \rangle \end{tikzcd}$$

1-1 ring hom, R-module hom

I reproved it but this is remark after defn of ass.

So R/P isomorphic to submodule of $R/\langle a \rangle$. NTS R_P is a DVR or a field. We may assume R local with max ideal P (If we prove it in this case and we have R ring P ass to principal ideal, then R_P is local and P_P associated to a principal ideal so $(R_P)_{P_P}$ is a DVR or field and easily $(R_P)_{P_P} \underset{\text{rings}}{\cong} R_P$)
easy ex.

It is expected and fairly easy to see that $R_P \cong R$ (univ property of loc). NTS R DVR or field.
If $P = 0$ then R field. Suppose $P \neq 0$. <u>Claim</u>: P is principal

(If we show this by PIT codim $P \leq 1$, but 0 prime since we are in a domain so codim $(P) = 1$
Thus since we are in a local ring $\dim R = \operatorname{codim} P = 1$ So R local Noeth domain
of dim 1 with max ideal principal. Hence R DVR ✓)

Now $P \subsetneq R \subseteq P^{-1} := \{r \in K(R) : rP \subseteq R\} \subseteq K$ R-submodule
We also define $P^{-1}P := \{\sum\limits_{i=1}^{n} q_i p_i : q_i \in P^{-1}, p_i \in P\}$ R-submodule
$P \subseteq P^{-1}P \subseteq R$ and since $P^{-1}P$ R-submodule it is an ideal in R
But P maximal so either $P^{-1}P = P$ or $P^{-1}P = R$

In general if R domain, $I \subset K(R)$; $I^{-1} := \{s \in K(R) : sI \subseteq R\}$
R seen inside $K(R)$ (embedded)
$I^{-1}I := \{\sum\limits_{i=1}^{n} s_i r_i : s_i \in I, r_i \in I^{-1}\}$
$(\overset{\shortparallel}{I I^{-1}})$

. Suppose $P^{-1}P = P$: <u>Claim</u> $P^{-1} = R$: Let $r \in P^{-1}$; then $P \xrightarrow{r\cdot} P$ is an R-homomorphism. P is fg R-module ideal) since R is Noetherian so by Cayley-Hamilton $r^n + c_1 r^{n-1} + \dots + c_n = 0$ for $c_i \in R$ so $r \in \bar{R}^{K(R)} = R$
(R-domain)

Now since $P \in \operatorname{Ass}_R(R/\langle a \rangle)$, $P = \operatorname{ann}(\bar{b})$, $\bar{b} = b + \langle a \rangle \in R/\langle a \rangle$ so $bP \subseteq \langle a \rangle$ thus
$b/a \cdot P \subseteq R$ so $b/a \in P^{-1} = R$ thus $b/a = r \in R$ so $b = ra \in \langle a \rangle$ so $\bar{b} = 0$ thus $\operatorname{ann}(\bar{b}) = R$ ↯
(operation in $K(R)$)
(technically $\frac{b}{1} = \frac{ar}{1}$ but we are in a domain...)

It follows $P^{-1}P = R$. So $\exists p \in P, q \in P^{-1} : pq \in R \setminus P$. Claim $P = \langle p \rangle$. Let $s \in P$, $qs \in R$

$s = \underbrace{qs(pq)^{-1}}_{\in K(R)} p \in \langle p \rangle$

↳ $qs \in R$, $pq \in R \setminus P$ so pq unit in R so $(pq)^{-1} \in R$.

Now we are done □

Corollary 91 If R noeth local domain of dimension 1 then R DVR iff R normal

→) Proof of 1st implication of thm 90

←) Let m be maximal ideal in R, R local so $\dim R \overset{=1}{=} \operatorname{codim} m$. Then let $a \in m \setminus \{0\}$

Since $\operatorname{codim}(m) = 1$ $\nexists$ primes between $0, m$ (R domain so 0 prime) thus m minimal over $\langle a \rangle$ so by thm 30 i) m minimal over $\langle a \rangle$ so by thm 90 R_m DVR but $R_m \underset{\text{ring}}{\cong} R$ as said before □

theorical (Buch did not do it)

We compilate this in the following result from Atiyah Mcdonald.

Cor 92 Compilation DVR   Let R be local Noeth domain $\dim(R) = 1$. Let m max ideal $k = R/m$.

TFAE
i) R is a DVR
ii) $\exists\, v : K(R)^* \to \mathbb{Z}$ discrete valuation st R is the valuation ring of v.
iii) R normal (integrally closed)
iv) m principal
v) $\dim_k(m/m^2) = 1$ (k-vsp)
vi) Every nonzero ideal is a power of m
vii) $\exists\, x \in R : \forall I \subseteq R$ nonzero ideal $I = \langle x^k \rangle$, $k \geq 0$

Proof/ $i \leftrightarrow ii$ obs ; $i \leftrightarrow iii$ 91 , $i \leftrightarrow iv$ $\underset{\leftrightarrow v}{}$ Clear (local noeth domain of dim 1 is DVR iff regular $\underset{\text{def}}{\text{iff}}$ $\dim_k(m/m^2) = 1$ iff m principal)
(claim starting sec 23)

Now $ii \to vi$) is clear by the proof of the observation (we described all the ideals)

$vi \to vii$) If $m = m^2$ by NAK $m = 0$ so $m^2 \neq m$. So $\exists x \in m$, $x \notin m^2$. Now $\langle x \rangle = m^r$
so it follows $r = 1$, $m = \langle x \rangle$, $\langle x^k \rangle = m^k$.

$vii \to i$) Max ideal is principal so iv holds and we know $iv \leftrightarrow i$ //

Geometry $X \subseteq \mathbb{A}^n$ alg set (irreducible) of dimension 1 (coord ring has dim 1 = curve) then $x \in X$ nonsingular iff $\mathcal{O}_{X,x}$ normal (of course we can relate normality

($\mathcal{O}_{X,x}$ as explained before is local noeth of dim $\mathcal{O}_{X,x} = \dim A(X) = 1$
so regular iff normal)

I needed $A(X)$ domain to argue this (maybe one can do it without but I guess that would need more machinery. Even this uses the result that we did not prove)

Corollary 93 (Reformulation): Let R be a Noeth domain. Then R normal iff

i) Every prime ideal associated to a principal ideal ($\neq 0$) has codim 1

ii) $P \in \operatorname{Spec}(R)$ of codim $(P) = 1$ then R_P is a DVR

Proof $\rightarrow$) If R normal, $\forall P \subseteq R$ associated to a principal ideal R_P is a DVR or a field. So if P prime ass to $\langle x \rangle \neq 0$ then R_P has dim 1 thus easily $\operatorname{codim} P = 1$

If $P \in \operatorname{Spec}(R)$ of $\operatorname{codim}(P) = 1$ then P minimal over any $\langle a \rangle : a \in P$ so $P \in \operatorname{Ass}_R(R/\langle a \rangle)$ so R_P DVR

$\leftarrow$) Clear.

Corollary 94 If R normal Noetherian domain $R = \bigcap\limits_{\substack{\operatorname{codim}(P)=1 \\ P \in \operatorname{Spec}(R)}} R_P \subseteq K(R)$.

Proof/ $R = \bigcap\limits_{\substack{P \text{ associated} \\ \text{to a principal} \\ \text{ideal}}} R_P = \bigcap\limits_{\substack{P \text{ ass to} \\ \text{principal ideal} \\ \neq 0}} R_P$.

If P ass to $\langle 0 \rangle$ $P = \{0\}$ so $R_P = K(R)$

Now $\{P \text{ ass to nonzero principal ideal}\} = \{P \in \operatorname{Spec}(R) : \operatorname{codim} P = 1\}$ when R normal
$\in \operatorname{Spec}(R)$

$\subseteq$) C. 93

$\supseteq$) P ass to $\langle a \rangle$ for any $a \in P \setminus \{0\}$ since it is minimal over it (thm 30) ☐

Geometry application Suppose $X \subseteq \mathbb{A}^n$ ($k = \bar{k}$) irreducible alg set, $Y \subseteq X$ closed irreducible

Let $\mathcal{O}_{X,Y} = A(X)_{I(Y)} \subseteq K(X)$. Note $A(X)$ domain $I(Y)$ prime ideal (as explained in the corresp before L25, $I(Y)$ here means poly functions in X vanishing at Y; so kind of abusive notation to mean $I(Y)/I(X)$ where $I(Y) = \{f \in k[x_1, \ldots, x_n] : f \text{ vanish at } Y\}$)

So $\mathcal{O}_{X,Y}$ noeth local domain. In the same way $A(X)$ can be identified with poly functions at X, $\mathcal{O}_{X,Y}$ can be identified with the ring $\{f \in K(X) = K(A(X)) : \exists p \in Y \text{ st } f \text{ defined at } p\}$ rational function is defined at p.

Assume X normal, $A(X)$ normal. Suppose $Z \subseteq X$ closed of codim $Z \geq 2$. Suppose $f \in K(X)$ and we know is defined on $X \setminus Z$. Claim f is actually defined in all X ($f \in A(X) \subseteq K(X)$)
(this of course can be translated to $\mathcal{O}_{X,\cdot}$ language)

$A(X) = \bigcap_{\substack{P \in \operatorname{spec}(A(X)) \\ \operatorname{codim} P = 1}} A(X)_P \subseteq k(X)$; under the usual correspondence

if $P \in \operatorname{Spec}(A(X))$ codim $P = 1$ $P = I(Y)^{\subseteq A(X)}$ for Y closed irreducible of codim 1

So $A(X) = \bigcap_{\substack{Y \subseteq X \\ \operatorname{codim} Y = 1}} \mathcal{O}_{X,Y}$. ($\mathcal{O}_{X,Y} \subseteq k(X)$ previous results) .

Now if Y has codim 1 I claim that $Y \cap (X \setminus Z) \neq \emptyset$ (Otherwise $Y \subseteq Z$ so codim $Y \geqslant$ codim $Z \geqslant 2$)

So f is defined at at least a point of Y thus $f \in A(X)$. □

At this point in the course we started thinking about what we should cover after we are done with this section. The options were: i) Fractional ideals, invertible modules fractional ideals, divisor theory

ii) Grobner basis

iii) Completions .

We ended up doing option 1 . So I mention a few words about the other two . ii) Grobner basis have already been mentioned and motivated through the course . Again, Grobner basis give ways to actually compute (at least in principle ; the algorithms become very slow) for affine rings most if not all of the things that we've been speaking about (prime ideals primary dec...) . The reason why we did not do it is because with the time remaining we would not probably get very far into understanding this algs .

iii) Completions studies the theory behind formal power series, p-adic integers etc . We decided not to study it because it would be a bit dull . The main references are ch 10 A&M and Ch 7 Eis . The first option contains inside the chapter things I already know so it will be easier (can skip things) . Also since dimension theory starts Eisenbud's book sporadically contains results about completions that we've been skipping . As well as ch 23 Isaacs alg this is smth I should do while/before as prerequisites for number theory .

Now we aim to prove the general version of Serre's criterion . Recall corollary 93, what if we drop domain?

Noticing when R product of rings

• Let $R = R_1 \times \cdots \times R_r$, R_i rings . We have that R_i also a ring and we denote $e_i = (0, -, \underset{i}{1}, 0, -, 0) \in R$ are called idempotents $e_i e_j = \delta_{ij} e_i$ ⊛

$e_1 + \cdots + e_n = 1 \in R$ (**)

• Conversely if R any (comm) ring and we have $e_1, -, e_n \in R$ st ⊛ and (**) hold set $R_i = \langle e_i \rangle = Re_i \subseteq R$. Note R_i is a ring with identity e_i . ($a e_i \cdot b e_i = ab e_i$)

We also have a projection $\begin{array}{l} \rho_i : R \to R_i \\ \quad a \mapsto ae_i \end{array}$ ring hom. And $\begin{array}{l} \varphi : R \to R_1 \times \cdots \times R_n \\ \quad a \mapsto (ae_1, \ldots, ae_n) \end{array}$

is surjective ring hom ($\forall (a_1, \ldots, a_n) \in R_1 \times \cdots \times R_n$, $\varphi(a_1e_1 + \cdots + a_ne_n) = (a_1, \ldots, a_n)$) also 1-1

(if $\varphi(a) = 0$ $ae_i = 0$ So $ae_1 + \cdots + ae_n = 0 = a(1) = a$.

- Note that if R any ring with $e_1, \ldots, e_n$ satisfying ⊛. If we let $e_{n+1} = 1 - (e_1 + \cdots + e_n)$ then $e_1, \ldots, e_{n+1}$ satisfy ⊛, $\boxed{**}$

So we realize that a ring is a product of rings when contains $e_1, \ldots, e_n$ satisfying ⊛, $\boxed{**}$

We want to speak about normality of Noeth rings that are not necessarily domains. We do not have the concept of field of fractions; we need an analogue (Recall that first we defined $R \subseteq S$, R normal IN S if ... ; then R domain normal if normal in field of fractions; we want to do the same (find appropriate over ring in which we speak about normality) for Noeth.

DEF Let R be a ring, $U = \{u \in R : u \text{ nzd}\}$ mult closed. Define $K(R) = U^{-1}R$ called the total ring of fractions (if R domain we get field of fractions so consistent notation)

Notes i) $\underset{\text{identify}}{R \subseteq K(R)}$ as a subring $\left(\begin{array}{l} R \to K(R) \\ r \mapsto r/1 \end{array} \right.$ if $r \in \ker$, $\underset{\text{nzd}}{\exists u \in U} : ru = 0$ so $r = 0$ $\Big)$

ii) If R $\overset{\sqrt{(0)} = 0}{\text{reduced}}$ Noeth then $\dim(K(R)) = 0$

Proof/ If R Noetherian and reduced K(R) is also Noetherian reduced (noetherian is corollary 9, reduced is easy). By prop 39 $\text{Ass}_R(R/0) = \{\text{minimal primes over } 0\}$

So if $P \in \text{Spec}(R)$ not minimal prime then $P \not\subseteq$ Union of minimal primes $\underset{\substack{\downarrow \\ \text{thm 30}}}{=} \{\text{zero divisors of } R\}$

Suppose $Q_1, Q_2 \in \text{Spec}(K(R))$ $Q_1 \subsetneq Q_2$ then by prop 8 $Q_1 \cap R \subsetneq Q_2 \cap R$ both in Spec(R) not intersecting U. Thus $Q_2 \cap R \in \text{Spec}(R)$ not minimal so $\exists r \in Q_2 \cap R$: r non zero div

but $(Q_2 \cap R) \subseteq R \setminus U = \{\text{zero divisors of } R\}$ ↯

iii) If R noeth NOT reduced then $\dim K(R)$ can be > 0. (not much details)

Let $R = k[x,y]/\langle x^2, xy \rangle$ We have $\dim R = 1$ $\left(\langle x^2, xy \rangle \subsetneq \underset{\substack{\downarrow \\ \text{prime}}}{\langle x \rangle} \subsetneq \langle x, y \rangle \right)$

(k any field)

(⟨x,y⟩ in R)

(all elts outside are nzd)

Now all elmts of $\langle x,y \rangle / \langle x^2, xy \rangle$ are zero divisors so $K(R) = R_{\langle x,y \rangle}$ (in R) thus $\dim K(R) = 1$

DEF let R be a Noetherian ring, $r \in R$, $P \in \operatorname{Spec}(R)$ we say that P is associated to r iff P associated to $R/\langle r \rangle$.

R subring of $K(R)$
so R_P is seen as subring of $K(R)_P$
(ident)

Prop 95 let R be a reduced noeth ring, $x \in K(R)$. Then $x \in R$ iff $\frac{x}{1} \in R_P \subseteq K(R)_P$ for all primes associated to nzd.

$\bigcap R_P$

↘ R-module

Note we do not write $R = \bigcap_{\substack{P \text{ ass to} \\ \text{nzd}}}$ because $R_P \subseteq K(R)_P$ and $K(R)_P \neq K(R)_Q$ in general.

Previously, everything was inside fraction field.

We could still try to make sense of identity but be careful and clear of what we mean.

Proof/ $\rightarrow$) Obvious

$\leftarrow$) let $x = a/u$, $u \in R$ nzd. Assume $x \notin R$.

Then $a \notin \langle u \rangle$ so $\bar{a} \neq 0 \in R/\langle u \rangle = R/uR$. Thus

$a \neq 0 \in R_P/uR_P$ for some $P \in \operatorname{Ass}_R(R/\langle u \rangle)$

($a = a/_1 + uR_P$) For this we are using corollary 27 i) and obs 2 in thm 19

Thus $a/_1 \notin uR_P \subseteq R_P$ thus $a/u \notin R_P$. With this and a bit of care one sees $\frac{x}{1} \notin R_P \subseteq K(R)_P$

(If $x/_1 \in R_P \subseteq K(R)_P$ $\exists\, b \in R, c \in R \setminus P$: $\frac{x}{1} = \frac{b/1}{c}$ thus $\exists d \in R \setminus P$: $d(c \cdot x - b/_1) = 0$

$\frac{x}{1}$ ↓ $R \subseteq K(R)$ as $\{r/_1 : r \in R\}$

d, c ↓ R-module mult ; $\in K(R)$

thus $d(c \cdot \frac{a}{u} - \frac{b}{1}) = 0$ so $\frac{dca}{u} - \frac{db}{1} = 0 \in K(R)$ so $\frac{dca - dbu}{u} = 0$ in $K(R)$ so $\frac{dca-dbu}{1} = 0$

$\exists u'$ nzd : .... Thus $dca - dbu = 0$. This is exactly $a/u \in R_P$.)

$\square$

Theorem 96 (Serre's Criterion) Let R Noetherian ring. Then R direct product of normal (isom to) domains iff

i) $P \in \operatorname{Spec}(R)$ associated to a nzd $\longrightarrow$ codim$(P) = 1$
$P \in \operatorname{Spec}(R)$ associated to 0 ideal $\longrightarrow$ codim$(P) = 0$

ii) $P \in \operatorname{Spec}(R)$: codim$(P) = 1 \longrightarrow R_P$ DVR.
codim$(P) = 0 \longrightarrow R_P$ field.

Note If R noeth, $R = R_1 \times \cdots \times R_n$ then R_i must be noeth because if $I \subseteq R_i$ ideal then $0 \times \cdots \times I_i \times 0 \cdots \times 0 \subseteq R$ ideal.

Proof/ $\longrightarrow$) $R = R_1 \times \cdots \times R_n$ R_i normal domain.

Let $P \subseteq R$ be a prime ideal then $P = R_1 \times \cdots \times R_{i-1} \times Q_i \times R_{i+1} \times \cdots \times R_n$; this is because if $f_j = (1, \ldots, 1, \underset{j}{0}, 1, \ldots, 1)$, $f_1 \cdots f_n = 0 \in P$ so one of them say $f_i \in P$. Therefore we see

$P = R_1 \times \cdots \times R_{i-1} \times Q_i \times R_{i+1} \times \cdots \times R_n$ and it easily follows that $Q_i \subseteq R_i$ prime.

Now P associated to $a=(a_1,\dots,a_n)\in R$ by the remark after defn of ass this is equivalent to R/p iso to submodule of $R/\langle a\rangle \underset{\substack{\downarrow \\ \text{easy, noether}}}{\cong} R_1/\langle a_1\rangle \times\dots\times R_n/\langle a_n\rangle$

$\overset{\displaystyle \cong}{0\times\dots\times R_i/Q_i \times 0 \dots 0}$

By composing we see that R_i/Q_i is iso to a submodule of $R/\langle a_i\rangle$ and again this means Q_i ass to $R/\langle a_i\rangle$ (iff)

Now this implies (by saying a bunch of easy words) via cor 93 (thm 90) that i), ii) hold.

. We now have primes in R one and the codim P is equal (thanks to knowing them) to the codim Q_i in R_i in the language above.

$\longleftarrow$) Assume i) ii)

<u>STEP 1</u> R is reduced. (expected; product of reduced is reduced)

Pf/ R is noetherian (picture $\boxed{}$ after thm 34)

$\underset{\substack{\uparrow \\ \text{minimal primary dec}}}{0=} I_1\cap\dots\cap I_n$ with I_j P_j-primary where $\{P_1,\dots,P_n\}=\mathrm{Ass}_R(R/0)$

Thus codim $P_j=0$ by i) and by ii R_{P_j} is a field. Notice that we always have $I_j\subseteq P_j$. Let us show the opposite. Suppose $r\in P_j$ then $r/1=0\in R_{P_j}$ (it belongs to the maximal ideal in a field. So $\exists\, s\in R\setminus P_j : rs=0$ (typical loc prop). So $rs\in I_j$, $s\notin P_j$ so by , $r\in I_j$.

Thus $I_j=P_j$. Now by cor 15, $\sqrt{0}=\bigcap_{P\in\mathrm{Spec}(R)} P \subseteq \bigcap_{j=1}^{n} P_j \subseteq \bigcap_{j=1}^{n} I_j = 0 \subseteq \sqrt{0}$. So $\sqrt{0}=0$. //

<u>STEP 2</u>. R($\subseteq K(R)$) is normal/integrally closed in K(R). (R reduced)

Pf/ Let $x\in \overline{R}^{K(R)}$ we need to show $x\in R$. By the proposition we need to show $\frac{x}{1}\in R_P\subseteq K(R)_P$ $\forall$ P ass to nzd. By i) this means codim (P) = 1 so by ii R_P is DVR

Now DVR → PID → UFD → Normal. It is fairly obvious that $K(R)_P \underset{\text{embedded}}{\subseteq}$ field of fractions of R_P

Thus $\overline{R_P}^{K(R)_P}=R_P$. Now $x/1\in \overline{R_P}^{K(R)_P}=R_P$ so $x\in R$ thus $\overline{R}^{K(R)}=R$.

(x satisfies $f(y)\in R[y]$ monic !! So $\frac{x}{1}$ will satisfy a monic poly in $K(R)_P$ missing details)

<u>STEP 3</u> R noeth, normal in K(R) and reduced ⟶ R product of normal domains. (perhaps excessively rigorous)

Pf/ We proved R reduced noeth → dim K(R) = 0 and also K(R) noeth, reduced. By thm 20 noetherian of dim 0 (every prime is maximal) implies K(R) artinian.

By corollary 22 $K(R)\cong K_1\times\dots\times K_n$ with K_i reduced (otherwise K(R) not reduced) local Artinian. Now K_i is a field (by C23 if m_i maximal in K_i, $m_i^n\in \mathrm{Ann}(R)=\{0\}$ thus $m_i\subseteq\sqrt{(0)}=0$. So 0 is max ideal hence K_i field; Anders gave different arg using NAK) formal count

($R \subseteq K(R)$ already identified; anyway in $K(R)$ if we want; or the elements of R are $r/1$ from now on; whatever)

We now look at

$$\begin{tikzcd} R \arrow[r, "i"] \arrow[rr, bend right, "\varphi_i"'] & K(R) \arrow[r, "proj"] & K_i \\ r \arrow[r, mapsto] & r & \end{tikzcd}$$

this is a ring hom, call $P_i := \ker(\varphi_i)$.
ideal of R

Note $R/P_i \cong$ subring of a field so R/P_i domain and P_i is prime. Let $e_i = (0,\dots,\overset{i}{1},\dots 0) \in K_1 \times \dots \times K_n$

Let $e_i \in K(R)$ the corresponding element in $K(R)$ thus (as an) $e_i^2 - e_i = 0$ so $e_i \in \overline{R}^{K(R)} = R$ $\forall i$
($R \subseteq K(R)$)

Thus $R \underset{rings}{\cong} Re_1 \times \dots \times Re_n$ by a previous observation (external, but $Re_i \subseteq R$)

Note $Re_i \cong R/P_i$:

$$\left(\begin{array}{c} \underbrace{R \xrightarrow{i} K(R) \xrightarrow{\cong} K_1 \times \dots \times K_n \xrightarrow{e_i \cdot} 0 \times \dots \times K_i \times \dots 0}_{P_i \text{ kernel}} \underbrace{\xrightarrow{\cong^{-1}} e_i R}_{1-1} \\ r \longmapsto r \longrightarrow \cong(r) \longrightarrow e_i \cdot \cong(r) \longmapsto e_i \cdot r \\ \cong^{-1}(e_i \cdot \cong(r)) = e_i r \end{array} \right)$$

so this map has P_i kernel and just by looking at it we see is surj; thus $R/P_i \cong e_i R$

so domain.

So NTS Re_i integrally closed (in its field of frac). Note $Re_i \subseteq K(R)e_i \overset{\text{clear (just see } K(R) \text{ above)}}{\cong} K_i$ field so $K(R)e_i$ contains quotient field of Re_i. Thus enough to see integrally closed in $K(R)e_i$. But if $x \in \overline{Re_i}^{K(R)e_i}$ then

x satisfies $e_i y^n + a_{n-1} e_i y^{n-1} + \dots + a_0 e_i \in Re_i[y]$ monic (1 in the ring is e_i)
$a_j \in R$

Now $e_i^2 = e_i$ so $e_i^n y^n = e_i y^n$, thus xe_i satisfies a monic poly in $R[y]$ thus $xe_i \in R$ since
$\in K(R)$

$\overline{R}^{K(R)} = R$. But $x \in K(R)e_i$ so $x = te_i$ thus $\underset{\substack{\uparrow \\ R}}{xe_i} = te_i^2 = te_i = x$ $\square$

//

<u>Note</u> We have proved; R noeth : Normal in $\overset{total}{\text{ring}}$ of fractions and reduced

$\longleftrightarrow$ R product of normal domains $\longleftrightarrow$ cond then.
(follows these domains are normal)

VIDEO : What we've done (Serre)

- Fanxin asked about applications of Serre's general then, Anders gave 2 applications.

(No proofs, in fact to prove what we're saying we need a precise statement; this statement contains defs that I dk yet)

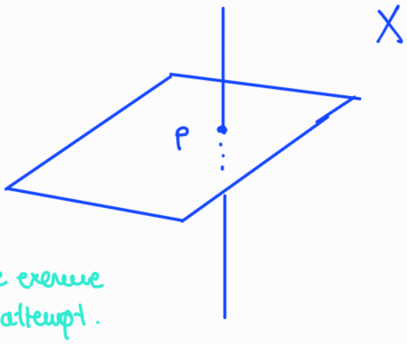
- Let A affine reduced k-alg, $X = \text{Spec-m}(A)$ (we saw this "is" an alg set). Suppose A normal in its total ring of fractions. (Corresponds to $X \overset{\subseteq \mathbb{A}^n}{} $ alg set, $A(X) = A$ reduced and normal in $K(A)$ total ring of fractions). Then by the theorem A is a direct product of finitely many normal $\overset{\text{(noeth)}}{\text{domains}}$ $R_1 \times \cdots \times R_n$. Now since we know how spec-m $(R_1 \times \cdots \times R_n)$ works (see start of proof of 96) it is very plausible that X is a disjoint union of irred alg sets

This needs more theory of varieties in general but I guess it means union of varieties.

- The other application he talked about was something like $p \in X$ alg set $\mathcal{O}_{X,p}$ normal in its ring of total fractions, reduced. Then p belongs to only one irreducible comp of X.

(I did not stop to think about it so to prove it one might need to throw in some extra hypothesis or maybe less. But good to know that 96 is applied in this kind of things)

So if



then $\mathcal{O}_{X,p}$ will not be normal in its ring of fractions

Nice exercise to attempt.

VIDEO : Course done ?

Until now we have what Anders wanted to cover 100 %. From now on we start what we described as option 1. Before we continue to fractional ideals we need to cover some basics. This does not correspond to any section of these notes.

Some basics before we move on.

In the algebra qual "Group thy notes" we gave a definition of finitely presented group. We now give an analogue defn to finitely presented module.

(defined in p17 Eis, 795 D&F)

DEF Let M be an R-module. We say M is finitely presented if there exist an exact sequence

$$R^n \longrightarrow R^m \longrightarrow M \longrightarrow 0 \quad \text{of } R\text{-homs.}$$

"M cokernel of a matrix in R"

Note i) An equivalent condition is that M fg by m elements and the kernel of the corresponding R-hom $R^t \to M$ (send e_i to ith generator) can be generated by s elements.

ii) Note that the definition is quite similar to the one in alg qual notes for Groups

Recall that if M, N are R-modules, $\mathrm{Hom}_R(M,N)$ is an R-module (alg qual). I state some easy properties (2.2 Eis)

i) $\mathrm{Hom}_R(R,N) \cong N$

$$\varphi \longmapsto \varphi(1)$$

ii) Hom is functorial: If $\alpha: M \to M'$, $\beta: N \to N'$ R-homs then there is a induced R-hom

$$\mathrm{Hom}_R(M,N) \longrightarrow \mathrm{Hom}_R(M',N')$$
$$\varphi \longmapsto \beta \circ \varphi \circ \alpha$$

iii) $\mathrm{Hom}_R(\oplus_i M_i, N) \underset{\text{can. iso}}{\overset{\text{alg qual}}{=}} \prod_i \mathrm{Hom}_R(M_i, N)$; $\mathrm{Hom}_R(M, \prod_j N_j) = \prod_j \mathrm{Hom}_R(M, N_j)$

iv) $0 \to A \to B \to C$ exact then $0 \to \mathrm{Hom}_R(M,A) \to \mathrm{Hom}_R(M,B) \to \mathrm{Hom}_R(M,C)$ exact
(natural induced)

$A \to B \to C \to 0$ exact then $\mathrm{Hom}_R(C,N) \to \mathrm{Hom}_R(B,N) \to \mathrm{Hom}_R(A,N) \to 0$ exact.

(this gives S R-mod structure)

Now let $R \longrightarrow S$ ring hom. M, N R-modules then the following is an S-hom.

$$\alpha : \mathrm{Hom}_R(M,N) \otimes_R S \longrightarrow \mathrm{Hom}_S(M \otimes_R S, N \otimes_R S)$$

$$\varphi \otimes_R s \longmapsto \text{map sending} : m \otimes s' \longrightarrow \varphi(m) \otimes ss'$$

When is it an isom?

Prop If M finitely presented and $R \to S$ flat then $\mathrm{Hom}_R(M,N) \otimes_R S \underset{S\text{-module}}{\cong} \mathrm{Hom}_S(M \otimes_R S, N \otimes_R S)$ via α. In particular if M finitely presented for any $U \subset R$ mult closed there is a natural isom (with α)

$$\mathrm{Hom}_{U^{-1}R}(U^{-1}M, U^{-1}N) \cong U^{-1}(\mathrm{Hom}_R(M,N))$$

This is prop 2.10 in Eis and seems to be well detailed. So read from there. We now move on to ex 4.13

DEF A ring R is said to be semilocal if it has finitely many maximal ideals.

Lemma (ex 4.13) Let R be semilocal, M, N R-modules $M_P \underset{(R_P \text{ modules})}{\cong} N_P$ $\forall P$ max ideal of R. If M is finitely presented then $M \cong N$. (R-modules)

↳ see next stupid remark.

This is also fairly clear from Eisenbud's solutions.

26. INVERTIBLE MODULES, FRACTIONAL IDEALS (~ 11.3 Eis)

This also appears in number theory; so some of this is commutative alg with a view towards nthy (and alg geo)

DEF Let R be a ring, the R-module I is invertible if I fg R-module and $I_P \cong R_P$ $\forall P \in \mathrm{Spec}(R)$

Suppose that $I_P \cong R_P$ $\forall P \in \mathrm{Spec\text{-}m}(R)$ then if $Q \in \mathrm{Spec}(R)$ $Q \subseteq P \underset{\text{Max}}{\subsetneq} R$ thus

$$I_Q \underset{\substack{\text{clear}\\ Q \subseteq P}}{\cong} (I_P)_Q \underset{\substack{\text{easy}\\ (\text{localising } R\text{-module})}}{\cong} (R_P)_Q \underset{\text{same}}{\cong} R_Q$$. So enough to check for max ideals.

Stupid remark $I_P \xrightarrow{\varphi} M_P$ hom of R-modules iff hom of R_P modules | M_P, I_P R-module. I_P, M_P R_P-module. | M, I as R-modules juxtapos.

$\longrightarrow$) We have that $\varphi(r \cdot \frac{1}{u}) = r \cdot \varphi(\frac{1}{u}) = \frac{r}{1} \cdot \varphi(\frac{1}{u})$. Now $\varphi(\frac{r}{u'} \cdot \frac{1}{u}) =$

$= \varphi\left(\frac{r1}{u'u}\right) = \varphi(r \cdot \frac{1}{u'u}) = r \cdot \varphi\left(\frac{1}{u'u}\right) = \frac{ru'}{u'} \cdot \varphi\left(\frac{1}{u'u}\right) = \left(\frac{r}{u'} \frac{u'}{1}\right) \cdot \varphi\left(\frac{1}{u'u}\right) = \frac{r}{u'} \cdot \left(u' \cdot \varphi\left(\frac{1}{u'u}\right)\right)$

$= \frac{r}{u'} \cdot \varphi\left(\frac{1}{u}\right)$

$\frac{ra}{b} = \frac{ru'a}{u'b}$

product in R_P

$\longleftarrow$) We have $\varphi(\frac{r}{u'} \cdot \frac{1}{u}) = \frac{r}{u'} \cdot \varphi(\frac{1}{u})$. Now $\varphi(r \cdot \frac{1}{u}) = \varphi\left(\frac{r1}{u}\right) = \varphi(\frac{r}{1} \cdot \frac{1}{u}) = \frac{r}{1} \varphi(\frac{1}{u}) =$

$= r \cdot \varphi(\frac{1}{u})$

(Now is more clear to me when the book says I locally free of rk 1.

Examples i) Let $I = R$ then I invertible

ii) $I = \langle x \rangle \subseteq R$. I is invertible iff x nzd

$\leftarrow$) Let $P \in \text{spec-m}(R)$. Consider $I \xrightarrow{\varphi} R$; this is well defined if $rx = sx$ $r = s$ since x is a nzd
$x \longmapsto 1$ and easily is a 1-1 R-module homomorphism
$rx \longmapsto r$

Now the ex after prop 10 then $I_P \xrightarrow{\varphi_P} R_P$ is 1-1 hom. But clearly surj. Thus iso.
$\frac{rx}{u} \longmapsto \frac{r}{u}$

of R-modules (R_P mod)

$\rightarrow$) Suppose x is a zero divisor $\exists y \in R \setminus \{0\} : yx = 0$ thus if we take $\text{ann}(y)$ (proper ideal) is contained in $P \in \text{Spec-m}(R)$. Now $\frac{y}{1} \neq 0 \in R_P$ (if 0 $\exists u \in R \setminus P : uy = 0$ so $u \in \text{ann}(y)$ ↯)

But $y \cdot I_P = 0$, $y \cdot R_P \neq 0$. This implies $I_P \ncong R_P$ (easily ; $R_P \xrightarrow{\varphi} I_P$ iso
let $1 \in R_P$, $\varphi(y \cdot 1) = y \cdot \varphi(1) = 0$
So $y \cdot 1 = 0$ So $y \cdot R_P = 0$ ↯)

R - , R_P - see stupid mark.

iii) We can give example of nonprincipal invertible ideal. Let $R = \mathbb{Z}[\sqrt{-5}]$, $I = \langle 2, 1+\sqrt{-5} \rangle \subseteq R$
$\mathbb{Z}[\sqrt{-5}]$ is sums and products of $\sqrt{-5}$ and $\mathbb{Z}$. So $R = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$.
(algebraic gen by)

We can note $I = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}, a+b \text{ even}\}$ little ex. So not the unit ideal

Also $(1+\sqrt{-5})(1+\sqrt{-5}-2) = -6 \in I^2$. Thus $6 - 2^2 = 2 \in I^2$

If $P \in \text{Spec}(R)$: • $I \nsubseteq P \longrightarrow I_P = R_P$ easy
• $I \subseteq P$ then $2 \in P \cdot I$ so $I = PI + \langle 1+\sqrt{-5} \rangle$ now by localising at
(just a bit hand wavy) P, $I_P = P_P I_P + \langle 1+\sqrt{-5} \rangle_P$. Thus $I_P/\langle 1+\sqrt{-5} \rangle_P \cdot P_P = I_P/\langle 1+\sqrt{-5} \rangle_P$
so by NAK $I_P = \langle 1+\sqrt{-5} \rangle_P$ from this we see is free of rk 1 so
$I_P \cong R_P$

So I invertible. Now we show I is not principal. If $\exists x \in R : I = \langle x \rangle$ $2 \in \langle x \rangle^2$ so $\exists u \in R : 2 = ux^2$. Let $N(a + b\sqrt{-5}) = a^2 + 5b^2$; $N(2) = 4 = N(ux^2) = N(u)N(x)^2$ ($N(xy) = N(x)N(y)$ easy ; complex norm) Thus we must have $N(x) = \pm 2$ but $a^2 + 5b^2 \neq \pm 2$

Notation ; if I R-module $I^* = \text{Hom}_R(I, R)$. Note that we have a natural

R-hom
$$\begin{tikzcd} I^* \times I \arrow[r] \arrow[dr] & R \\ & I^* \otimes_R I \arrow[u] \end{tikzcd}$$
$(\varphi, a) \longmapsto \varphi(a)$ R-bilinear

$I^* \otimes_R I \longrightarrow R$
$\varphi \otimes_R a \longmapsto \varphi(a)$

DEF Let R be a ring, consider $K(R)$ its total ring of fractions. An R-submodule $I \subseteq K(R)$ is called a fractional ideal if $\exists\, u \in R$ nzd $u \in R$: $\underbrace{u \cdot I}$ $\subseteq \underbrace{R \text{ (inside } K(R)\text{)}}_{R \subseteq K(R) \text{ subring; we identified.}}$

(Slightly different to Eisenbud; if R domain both agree and that is the def on wikipedia)

This will now be an ideal in R (is iso to; but we are identifying so; an ideal in R)
So I fract ideal $\to$ I iso to an ideal in R as an R-module

Notes i) $I \subseteq K(R)$ fg as an R-module then its frac. ideal (multiply by the product of denominators of the generators)

ii) If R is noetherian, $I \subseteq K(R)$ R-submodule. I frac ideal iff I fg R-module
(so if $I \subseteq K(R)$ inv, then fract. ideal) R-module

$\longleftarrow$) ✓

$\longrightarrow$) $u \cdot I \subseteq R$ is an ideal of R noeth so gen by $r_1, \dots, r_n$. $r_j = u \cdot i_j$ $i_j \in I$. Easy to see i_j generate I as an R-module

If $I \subseteq K(R)$ any R-submodule we define $I^{-1} = \{s \in K(R) : s \cdot I \subseteq R\}$

and for $I, J \subseteq K(R)$; $IJ = \{\sum_{i=1}^{n} p_i q_i : p_i \in I, q_i \in J\} \subseteq K(R)$
$\downarrow$ subsets

(expected; but since we only defined this for ideals of R we have to make sure)

(I^{-1} R-submodule and if I, J frac then so is IJ.)

Theorem 97 (Picard) Let R be a Noeth ring, then

i) Let I be an R-module. I invertible iff $I^* \otimes_R I \xrightarrow{\mu} R$ is an iso
$\varphi \otimes_R a \longmapsto \varphi(a)$

ii) Every invertible R-module (R-mod) is isomorphic to a fractional ideal of $K(R)$

Also if I fractional ideal which is invertible contains a nzd of R (embedded in $K(R)$)

iii) If $I, J \subseteq K(R)$ invertible then $I \otimes_R J \xrightarrow{\cong} IJ$ $\quad$ $I^{-1} J \xrightarrow{\cong} \mathrm{Hom}_R(I, J)$
$s \otimes t \longmapsto st$ $\quad$ $t \longmapsto \underset{t}{\mathrm{map}} : a \mapsto at$

In part $I^{-1} \cong I^*$ (so fractional by the notes)

iv) If $I \subseteq K(R)$ any R-submodule it is invertible iff $I^{-1} I = R$ ($\subseteq K(R)$)
(reason why its called invertible)

Proof/ i) $\longrightarrow$) Let $P \in \mathrm{Spec}(R)$, we know that $I_P \overset{\theta}{\cong} R_P$. Now we consider

$$(I^* \otimes_R I)_P \xrightarrow[\substack{\text{canonically} \\ \text{see ex in} \\ \text{the 48}}]{\cong} (I^*)_P \otimes_{R_P} I_P \xrightarrow[\substack{\text{via } \theta \text{ on} \\ \text{right}}]{\cong} (I^*)_P \otimes_{R_P} R_P \xrightarrow{\cong} (R_P)^* \otimes_{R_P} R_P \xrightarrow{\cong} R_P$$

($(I^*)_P = (\mathrm{Hom}_R(I,R))_P$
$= \mathrm{Hom}_{R_P}(I_P, R_P) = (I_P)^* =$
$\downarrow$ canonical
$= (R_P)^*$
using θ, not exactly but clear that there are iso.)

$R_P^* \cong R_P$ by note i) of Hom ($\tilde{\varphi} \mapsto \tilde{\varphi}(1)$)
$R_P \otimes_{R_P} R_P \cong R_P$
$\downarrow$
Prop 10

This iso works as follows (reading the description on each step)

$$\frac{\varphi \otimes_R a}{u} \longmapsto \varphi \otimes_{R_P} \frac{a}{u} \longrightarrow \varphi \underset{R_P}{\otimes} \frac{\theta(a)}{u} \longrightarrow \tilde{\varphi} \otimes_{R_P} \frac{\theta(a)}{u} \longrightarrow \varphi(\theta^{-1}(1)) \otimes_{R_P} \frac{\theta(a)}{u} \longrightarrow \frac{\varphi(\theta^{-1}(1))\,\theta(a)}{u} = \frac{\varphi(a)}{u}$$

where $\tilde{\varphi} : R_P \longrightarrow R_P$
$r/v \longmapsto \frac{\varphi(\theta^{-1}(r))}{v}$

So what we've proved is that μ_p is iso $\forall\, P \in \operatorname{Spec}(R)$ thus φ iso by Corollary 12*.

$\longleftarrow$) Assume μ iso. Then $\exists \sum_{i=1}^{n} \varphi_i \otimes a_i \in I^* \otimes_R I : \mu\left(\sum_{i=1}^{n} \varphi_i \otimes a_i\right) = 1 \in R \quad = \sum_{i=1}^{n} \varphi_i(a_i)$

Let $P \in \operatorname{Spec}(R)$, then $\exists\, i : \varphi(a_i) \notin P$ (of course)

Set $a = \varphi_i(a_i)^{-1} a_i \in I_p$. Now $(I^*)_p \otimes_{R_p} I_p \xrightarrow[\text{}]{\overset{\text{canonic}}{\cong}} (I^* \otimes_R I)_p \xrightarrow[\substack{\text{iso}\\ \text{by } 12^*}]{\mu_p} R_p$ is an iso

under this iso $\frac{\varphi_i}{1} \otimes_{R_p} a \longrightarrow \varphi_i \otimes_R \frac{a_i}{\varphi_i(a_i)} \longrightarrow \frac{\varphi_i(a_i)}{\varphi_i(a_i)} = 1$

Then note that $(\varphi_i)_p : I_p \longrightarrow R_p$ is onto since I_p is an R_p-module, thus is R_p module hom and $(\varphi_i)_p(a) = (\varphi_i)_p\left(a_i/\varphi_i(a_i)\right) = 1 \in R_p$. Thus $I_p = a \cdot R_p \oplus \operatorname{Ker}((\varphi_i)_p)$
(direct; easy)

Now, $\underset{\binom{\text{apply}}{a} \equiv a}{(I^*)_p \longrightarrow R_p}$ is again surj $\left(\frac{\varphi_i}{1} \mapsto 1\right)$ thus similarly $(I^*)_p = R_p \cdot \frac{\varphi_i}{1} \oplus \ker(a)$

$\frac{\theta}{u} \mapsto \frac{\theta(a)}{u}$

Thus $R_p \underset{\mu_p}{\cong} (I^* \otimes_R I)_p \underset{\text{knew}}{\cong} (I^*)_p \otimes_{R_p} I_p = \left(\frac{\varphi_i}{1} \cdot R_p \oplus \ker(a)\right)) \otimes_{R_p} (a \cdot R_p \oplus \operatorname{Ker}((\varphi_i)_p))$

$= \left[\frac{\varphi_i}{1} \cdot R_p \otimes_{R_p} a \cdot R_p\right] \oplus \underbrace{\left[\frac{\varphi_i}{1} \cdot R_p \otimes_{R_p} \operatorname{Ker}((\varphi_i)_p)\right]} \oplus \left[\ker(a) \otimes_{R_p} a \cdot R_p\right] \oplus \left[\ker(a) \otimes_{R_p} \ker((\varphi_i)_p)\right]$

Prop 10
but note
we can make
sense so that this
is actually equal

(if we do not want
this, we argue
there that it goes
to zero under triple
comp)

This part under the iso (inverse) maps to 0 easily (we will end up doing φ_i evaluated at smth in the kernel)

Since we have an iso we conclude $\frac{\varphi_i}{1} \overset{\times 0}{\cdot} R_p \otimes_{R_p} \ker((\varphi_i)_p) = 0$ thus $\operatorname{Ker}((\varphi_i)_p) = 0$

Hence $(\varphi_i)_p$ 1-1 also onto thus $(\varphi_i)_p$ iso. Thus $I_p \cong R_p$

Finally, since μ iso and $\mu\left(\sum_{i=1}^{n} \varphi_i \otimes a_i\right) = 1$ it easily follows that I generated by $a_1, \dots, a_n$. Thus I invertible //

Before we keep going we have an observation:

i) R semilocal, I invertible R-module then $I \underset{R\text{-modules}}{\cong} R$ (Lemma ex 4.13)

ii) R Noeth reduced then $\underbrace{\text{total ring of fr. } K(R)}$ artinian so $K(R)$ semilocal.

$\dim(K(R)) = 0$
so every prime is
maximal

now apply thm 20.

---

ii) Let I be an invertible R-module (we want I isom to fractional ideal)

Note that $I \otimes_R K(R)$ is an invertible $K(R)$-module.
(total ring..)

First, let $Q \in \mathrm{Spec}(K(R))$ note $P := Q \cap R \in \mathrm{Spec}(R)$ and its members are all zerodivisors

Also $Q = P\,K(R)$ $\left(\begin{array}{l} \text{i) prop 8 part 1} \\ \text{ii) we see } R \subseteq K(R) \text{ so this is also an operation in } K(R) \end{array}\right)$

<u>Claim</u> $R_P \cong K(R)_Q$ $\left(= K(R)_{PK(R)}\right)$ as rings, so as $K(R)$-modules

To be rigorous I think we have to use prop 7. But seems very reasonable; we first have U in the denominators and then $R \setminus P \supseteq U$. | (Also for this reason R_P is a $K(R)$ module) — maybe ex in NAK

write what we think the isom is $\frac{r}{v} \longrightarrow \frac{r/u}{v/u}$ and prove it with that

Now $(I \otimes_R K(R))_Q \cong$

$$\cong (I \otimes_R K(R)) \otimes_{K(R)} K(R)_Q \cong I \otimes_R \left(K(R) \otimes_{K(R)} K(R)_Q\right) \cong I \otimes_R K(R)_Q \cong$$

↓ ex after prop 10 ↓ proof of 48

(to review!
It is very trivial but nice to do it via universal prop that if A, B, C R-mod $A \cong B$. Then $A \otimes_R C \cong B \otimes_R C$

$$\cong I \otimes_R R_P \cong I_P \cong R_P \cong K(R)_Q$$

But $K(R)$ semilocal so by the observation $I \otimes_R K(R) \cong K(R)$ as a $K(R)$-module

Notice $I \xrightarrow[\varphi]{R\text{-hom}} I \otimes_R K(R)$ is injective: To prove so it is enough to see that when we localize
$a \longmapsto a \otimes_R 1$

at $P \in \text{Spec-m}(R)$ $\overset{\varphi_P}{\text{is injective}}$. But

(easy)
$R_P \otimes_R K(R) \cong U^{-1} R_P$
$U = \{\text{n.z.d of } R\}$

$$\begin{tikzcd}
I_P \arrow[r, "\varphi_P"] \arrow[dd] & (I\otimes_R K(R))_P \arrow[r, phantom, "\cong"] & I_P \otimes K(R) \arrow[r, phantom, "\cong"] & R_P \otimes_R K(R) \arrow[r, phantom, "\cong"] & K(R_P) \\
a/u \arrow[r, mapsto] & \frac{a\otimes_R 1}{u} \arrow[r] & \frac{a}{u}\otimes_R 1 \arrow[r] & \theta(a/u)\otimes_R 1 \arrow[r] & \theta(a/u) \in K(R_P) \\
R_P \arrow[urrrr, bend right, "1-1"'] & & & & \\
\theta(a/u) & & & &
\end{tikzcd}$$

$\theta : I_P \to R_P$ isom

(note $R_P \subseteq K(R_P)$)
we already discussed this

$(I \otimes_R K(R))_P \overset{\text{can}}{\cong} (I \otimes_R K(R)) \otimes_R R_P$
$\cong (I \otimes_R R_P) \otimes_R K(R)$
$\cong I_P \otimes_R K(R)$
everything canonic.

the diagram commutes thus φ_P is 1-1 so we conclude by 12* that φ 1-1

Therefore I is an R-module isomorphic to a submodule of $K(R)$. But it is invertible so f.g so by note ii we see that indeed I is isomorphic to a fractional ideal.

Now suppose $I \subseteq K(R)$ fractional ideal. Assume $R \cap I$ consists of zero divisors. NTS I not inv.

↳ since $R \subseteq K(R)$ this can be treated as a legit intersection of sets.

We know that $\exists u \in R$ nzd such that $uI \subseteq R \cap I$. Thus $uI \subseteq R$ is an ideal of zero divisors. By Thm 30 $uI \subseteq P$ for some $P \in \mathrm{Ass}_R(R/0)$. So $P = \mathrm{ann}(b)$ for some $b \in \underset{\neq 0}{R}$. So $ubI = 0$ and $ub \neq 0 \in R$ then $\mathrm{ann}(ub) \subseteq Q$ prime (since it is a proper ideal) so $\frac{ub}{1} \neq 0 \in R_Q$ but also $ub \cdot I_Q = 0$ thus $I_Q \not\cong R_Q$ as R-modules so I not inv.

(write iso; get contradiction using ub easily

iii) Suppose $I, J \subseteq K(R)$ invertible (note they are fractional)

<u>Claim</u> $I \otimes_R J \xrightarrow{\varphi} IJ$ natural is 1-1 (of course surjective hom)

. Remark : $P \subseteq R$ prime then $R_P \cong I_P \subseteq K(R)_P$ so in that iso $R_P \to I_P$ $1 \in R_P$ will be sent to some $x \in I_P \subseteq K(R)_P$ and by the last stupid remark this is also R_P-hom so $I_P = R_P \cdot x \subseteq$ $\subseteq K(R)_P$

R-mod

nzd (in $K(R)_P$ which is easily seen to be a ring)

(R_P-module)

We can do the same thing with J; $J_P = R_P \cdot y$ for some $y \in K(R)_P$ nzd.

We now look at

$$\begin{tikzcd}
R_P \arrow[r, "\cong"'] & R_P \otimes_{R_P} R_P \arrow[r, "\cong"] & I_P \otimes_{R_P} J_P \arrow[r, dash] & (IJ)_P \subseteq K(R)_P \\
r/s & r/s \otimes_{R_P} 1 \arrow[l, mapsto, "(\text{prop }20)"'] \arrow[r] & r/s \cdot x \otimes_{R_P} y \arrow[r] & r/s \cdot \underset{\text{nzd}}{xy}
\end{tikzcd}$$

(so 1-1

So in particular $I_P \otimes_{R_P} J_P \longrightarrow (IJ)_P$ natural map is 1-1. But $I_P \otimes_{R_P} J_P$ is canonically iso (ex in proof of NAK) to $(I \otimes_R J)_P$ as R-modules or R_P-modules

↳ that ex justifies $I_P \otimes_{R_P} J_P$ R-module .... and more.

This shows $I \otimes_R J$ invertible!!

Thus we see that $(I \otimes_R J)_P \xrightarrow{\varphi_P} (IJ)_P$ is 1-1 so by 12* φ is 1-1. Inportant iso.

For the second one we want $I^{-1}J \longrightarrow \mathrm{Hom}_R(I, J)$ to be an iso. ((Clearly hom)

$$t \longmapsto \underset{a \mapsto at}{\text{map}: I \to J} := \varphi_t.$$

We have already proved that $\exists v \in I \cap R$ nzd. If $0 \neq t \in I^{-1}J$ then $tv \overset{\neq 0}{\in} J$ this means that $\varphi_t(v) \neq 0$ so $\varphi_t \neq 0$ hence our map is 1-1

(a bit careful we are not in localization but $R \subseteq K(R)$ embedded.

Now we work towards surjectivity. Let $\varphi \in \mathrm{Hom}_R(I, J)$. <u>Claim</u> $v^{-1}\varphi(v) \in I^{-1}J$ (if so clearly this element maps to φ by our map so surj ✓).

↳ $a/s \in I$, $a, s \in R$ s nzd. $v^{-1}\varphi(v)\frac{a}{s} \underset{(R\text{-hom})}{=} v^{-1}\varphi(va)\frac{1}{s} = v^{-1}v\,\varphi(a)\frac{1}{s} = \varphi(a/s) \in J$

(see everything in $K(R)$ as the beginning)

The above calculation shows $v^{-1}\varphi(v) \cdot I \subseteq J$

$v^{-1}\varphi(v) \in K(R)$; if we consider $I^{-1}J \subseteq K(R)$ as a R-submodule

$a/s \in I$ so $\varphi(a/s)$ makes sense.
Now $\frac{\varphi(a)}{s} = \varphi(a/s)$ since
$s \cdot \varphi(a)/s - s\varphi(a/s) = 0$

and we prove that $\frac{v^{-1}\varphi(v)}{1} \in (I^{-1}J)_P$ $\forall P \subseteq R$ max ideal, by Lemma 12 (applied to the quotient, $(K(R)/I^{-1}J)_P = K(R)_P/I^{-1}J_P$) we would have $v^{-1}\varphi(v) \in I^{-1}J$

So ETS $\frac{v^{-1}\varphi(v)}{1} \in (I^{-1}J)_P = (I^{-1})_P J_P \subseteq K(R)_P$ $\forall P \subseteq R$ prime

For a fixed $P \in \operatorname{Spec}(R)$ we had $J_P = R_P \cdot y$ for some $y \in K(R)_P$ nzd.

(By Ex 3.15 ii $K(R_P) \underset{\text{canonically iso}}{=} K(K(R)_P)$)

Now $\frac{v^{-1}\varphi(v)}{1} \cdot I_P \subseteq R_P \cdot y$ thus $\underbrace{\frac{v^{-1}\varphi(v)}{y} \cdot I_P \subseteq R_P}_{\text{this happens in } K(R_P)}$. So $\frac{v^{-1}\varphi(v)}{y} \in (I_P)^{-1} \subseteq K(R_P)$

$\downarrow$
$v^{-1}\varphi(v) I \subseteq J$

Now $(I_P)^{-1} \overset{(\supseteq \text{ also true})}{\subseteq} (I^{-1})_P \subseteq K(R)_P \subseteq K(R_P)$: I is fg R-module $a_1, \dots, a_n \in K(R)$ generators

let $\lambda \in (I_P)^{-1}$, this is $\lambda \in K(R_P)$, $\lambda \cdot I_P \subseteq R_P$. Thus $\frac{\lambda a_i}{1} \in R_P$.

$\exists s_i \in R \setminus P$: $s_i \lambda a_i \in R$. Let $s = s_1 \dots s_n \in R \setminus P$ $s \lambda a_i \in R$ so $s \lambda I \subseteq R$ thus $s\lambda \in I^{-1}$ thus $\lambda \in (I^{-1})_P$ ($s\lambda a_i \in R$ so from this, knowing that one of the a_i can be taken to be a nzd by ii) Note $I \subseteq K(R)$ inv so frac. $\subseteq$, $K(R_P)$) thus $s\lambda \in K(R)$ as needed.)

So $\frac{v^{-1}\varphi(v)}{y} \in (I^{-1})_P \subseteq K(R)_P$ Thus $v^{-1}\varphi(v) \in (I^{-1})_P \cdot R_P y \subseteq (I^{-1})_P J_P$ // in part.

iv) $\rightarrow$) If $I \subseteq K(R)$ invertible R-submodule. Note $I^* = \operatorname{Hom}(I, R) \underset{iii)}{\cong} I^{-1}R = I^{-1}$

Thus $I^{-1}I \overset{iii}{\cong} I^{-1} \otimes_R I \cong I^* \otimes_R I \overset{i)}{\cong} R$

and the composition is just inclusion so $I^{-1}I = R$

$\leftarrow$) If $I^{-1}I = \underset{\subseteq K(R)}{R}$ take $g_i \in I^{-1}$, $a_i \in I$ st $1 = \sum_{i=1}^{n} g_i a_i = 1$.

<u>Claim</u> $I = \langle a_1, \dots, a_n \rangle$ and $I_P \cong R_P$ $\forall P$ prime.

Suppose we prove it when we have local ring. In general consider R_P, we know that $I^{-1}_P I_P = R_P$ so $\underset{(R_P\text{-module}}{I_P}$ fg and $\underset{I_P \cong}{(I_P)_{P_P}} \cong \underset{\cong R_P}{(R_P)_{P_P}}$. Thus I fg R-module...

So WMA R local with max ideal P. NTS $R \cong I$ ($R_P \overset{R\text{-mod}}{\cong} R$ dividing by units
$I_P \cong I$)

Since $1 = \sum_{i=1}^{n} g_i a_i$, $\exists i$: $g_i a_i \in R \setminus P$ and hence it is a unit.

Thus $\underset{\subseteq I^{-1}I = R}{q_i I}$ contains a unit hence as an R-module contains all R. Thus $q_i I = R$

Now $I \xrightarrow[\cdot q_i]{} R$ surjective.

If $i \cdot q_i = 0$ then $\underbrace{i q_i a_i}_{\text{unit}} = 0$ so $i = 0$. thus inj as wanted □

Rmk If I invertible, I^{-1} is invertible ($I^{-1} \cong I^*$ and now read purple underlined part of proof of i)

Moreover if $I \subseteq K(R)$ inv R-submodule, $(I^{-1})^{-1} = I$: $(I^{-1})^{-1} \underset{\text{R-module}}{=} (I^{-1})^{-1} R = (I^{-1})^{-1} \cdot I^{-1} I = R \cdot I = I$.

DEF Let R be a Noetherian ring, we define $\mathrm{Pic}(R) = \{\text{Invertible R-modules}\}/\cong$ we consider this set with the following operation $\mathrm{Pic}(R) \times \mathrm{Pic}(R) \longrightarrow \mathrm{Pic}(R)$

$$([I],[J]) \longmapsto [I \otimes_R J]$$

inv. see the proof of iii.

Buch writes $(I,J) \sim I \otimes_R J$.

(abelian; see prop 10) (Well defined is obvious; univ prop of tensor if you want)

This is a mult. group (tensor is associative, the inverse class of the class of I is the class of I^* and the identity is the class of R). We call this Pic(R) ≡ Picard Group of R

Note if $I, J \subseteq K(R)$ invertible R-module $[I][J] = [IJ]$ so when we write IJ in the sense defined above the thm, this is also a rep of the class resultant of taking the product in Pic(R)

Moreover,

(same if we say inv R-submodules of K(R); see notes before thm)

Let $C(R) = \{\text{invertible fractional ideals } I \subseteq K(R)\}$. We give a group operation by setting the product of I, J to be IJ. (the inverse of I is I^{-1} and the identity R). This group is called (abelian)

C(R), the group of Cartier divisors.

As we mentioned above IJ, I^{-1} are invertible and $(I^{-1})^{-1} = I$ so everything clear and consistent.

Now $(IJ)^{-1}$? It is the inverse of IJ, and $(IJ)(J^{-1}I^{-1}) = R$ thus since I^{-1}, J^{-1} inv. $I^{-1}J^{-1}$ inv it follows $IJ^{-1} = J^{-1}I^{-1}$. Also could prove using defn

What is the difference between Pic(R), C(R)?

Corollary 98 Let R be a Noetherian ring. Then

i) $$0 \to R^{\times} \xrightarrow{\text{(units)}} K(R)^{\times} \longrightarrow C(R) \longrightarrow \mathrm{Pic}(R) \longrightarrow 0$$ is exact.

(total ring of fr.)

$0 \mapsto 0$

$r \longmapsto r/1$

$u \longmapsto Ru$ "Principal divisor"

$I \longmapsto [I]$

ii) C(R) is gen as a group by the set of invertible ideals in R ($I \subseteq R$ ideal invertible as an R-module)

Proof/ i) $C(R) \to \mathrm{Pic}(R)$, $I \mapsto [I]$ is onto by (iii) of last thm.

Note $Ru \in C(R)$ (We easily see $(Ru)^{-1} = Ru^{-1}$ and $Ru^{-1} Ru = R$)

Claim $\ker(C(R) \to \operatorname{Pic}(R)) = \{Ru : u \in K(R)^\times\}$.

$\subseteq$)

If $I \in C(R)$, $[I] = [R]$ we have that $I \cong R$ R-modules so $I = R \cdot u$ where u is the image of 1 under the isom $\left(\begin{matrix} R \xrightarrow{f} I \\ 1 \mapsto u \end{matrix} \right)$ If we consider $g : f^{-1} \in \operatorname{Hom}_R(I, R)$ so it $\overset{(ii)}{\text{}}$ must be related by mult by some $v \in I^{-1}$. Thus mult by uv is the identity on I

Since $\exists\, c \in I$ nzd we see $uvc = c \to uv = 1$ so $u \in K(R)^\times$.

We easily see u is a nzd otherwise not isom)

$\supseteq$) ✓.

Claim $\ker(K(R)^\times \to C(R)) = R^\times$: If $u \in K(R)^\times$ and $Ru = R$, $u \in R$.
and easily $u \in R^\times$ ($\exists\, v \in R : vu = 1$).

ii) Let $I \in K(R)$ invertible $\overset{R\text{-sub}}{\text{module}}$, then by ii $\exists\, a \in I^{-1}$ which is in R and nzd
so $aI \subseteq I^{-1}I = R$. So $I = aI \; (aR)^{-1}$ □

Note

i) $\operatorname{Pic}(R) \cong C(R) \big/ \text{Principal divisors}$ (reminds ideal class group). Also Principal div $\cong \frac{K(R)^\times}{R^\times}$ ← very nice invariant.

ii) If R is a PID recall that M fg R-module then $M \cong R^n \oplus T$, T has nonzero annihilator
so if I invertible it follows $I \cong R$ so in case of R PID the Picard group is trivial

GEOMETRY DIGRESSION

Now Anders spent about 1 and a half lectures trying to explain why we are looking at these things (geometric motivation). So this is not from the book and I have already said enough words about these type of discussions. In this digression we introduce new defn that are good to know.
I will mark with { whatever I feel that I should take as imprecise/do not worry now...

I am not sure if all we say is said in the standard way it is usually presented (this first observation I'm sure yes) but I am sure this would be instructive.

Glimpse of locally free modules, presheafs, sheafs

DEF Let R be a Noeth ring, M fg R-module. We say M is **locally free** if M_p free $\forall\, P \in \operatorname{Spec}(R)$ R_p-mod.
As above, enough to check for maximal.

(Review free modules from Alg qual if needed)

Note M is locally free iff $\forall\, P \in \operatorname{Spec}(R)$ $\exists\, f \in R \setminus P$: M_f free R_f-module

$\leftarrow$) $M_p = (M_f)_p$ (see proof of the 19 to see how M_f being $\overbrace{R_f \oplus \cdots \oplus R_f}^{n}$ implies M_p is $\overbrace{R_p \oplus \cdots \oplus R_p}^{n}$

$\rightarrow$) $M_p \cong R_p \oplus \cdots \oplus R_p$ (here direct sum may be seen as internal or external)

Choose $m_1, \dots, m_n \in M$: $\{\frac{m_1}{1}, \dots, \frac{m_n}{1}\}$ basis of M_p

We have a map $\begin{array}{ccc} R^n & \xrightarrow{\varphi} & M \\ e_i & \longmapsto & m_i \end{array}$. Note φ_P is an iso.

Let $K = \ker\varphi$, $C := \operatorname{Coker}\varphi$ so $0 \to K \to R^n \xrightarrow{\varphi} M \to C \to 0$ exact so after localizing is again exact with middle map an isomorphism so $K_P = C_P = 0$ so $\exists\ f \in R \setminus P : K_f = C_f = 0$ [think; you can't take f to be an arbitrary element; also we need K, C fg (from R Noeth; if M finite pres ✓)]

So again $R_f \xrightarrow{\varphi_f} M_f$ iso (Localize at $U = \{f^n\}$, get exact but you get zero's ...)

take gen $\frac{k_1}{1}, \dots, \frac{k_s}{1}$, $\exists\ p_i \in P : p_i k_i = 0$ ... multiply all ..

(easy)

So we care about invertible because more generally we care about locally free. And why we care about locally free in Geometry?

DEF Let X be a topological space; a presheaf (denoted by $\mathcal{F}$) of ab groups/rings consists of

- $\forall\ U \in X$ open we have an abelian group/ring $\mathcal{F}(U)$ (think of it as ring of functions in U) (differentiable if we want)
- $\forall\ U \subseteq V$ open subsets we have a group/ring hom $\rho_{V,U} : \mathcal{F}(V) \to \mathcal{F}(U)$

(think of this as restriction of function to a subset)

Such that:
- $\mathcal{F}(\emptyset) = 0$
- $\rho_{U,U}$ identity on $\mathcal{F}(U)$ $\forall\ U \subset X$ open
- For any inclusion $U \subset V \subset W$

$$\begin{tikzcd} \mathcal{F}(W) \arrow[r, "\rho_{W,V}"] \arrow[rr, bend right, "\rho_{W,U}"'] & \mathcal{F}(V) \arrow[r, "\rho_{V,U}"] & \mathcal{F}(U) \end{tikzcd} = \rho_{W,U}$$

It is convenient (and common) to write this defn with category thy language (Now that I thought about classes I can for sure understand it but I might wait a bit to define category in my notes; maybe when I do Hom. alg)

Notation: $\varphi_i \in \mathcal{F}(U)$ are called sections of $\mathcal{F}$ over U; $\rho_{U,V} : \mathcal{F}(V) \to F(U)$, $\varphi \longmapsto \varphi|_U$ meaning $\rho_{V,U}(\varphi)$ is denoted by $\varphi|_U$

A presheaf of ab groups/rings is called a sheaf of ab groups/rings if it satisfies the following "gluing property": if $U \subset X$ open, $\{U_i : i \in I\}$ arbitrary open cover of U and $\varphi_i \in \mathcal{F}(U_i)$ $\forall\ i \in I$ st $\varphi_i|_{U_i \cap U_j} = \varphi_j|_{U_i \cap U_j}$ $\forall\ i, j \in I$ then $\exists!\ \varphi \in \mathcal{F}(U) : \varphi|_{U_i} = \varphi_i\ \forall\ i \in I$.

(as in discussion of sec II)

Examples i) $X = \text{Spec-m}(A)$, A reduced affine k alg $k = \bar{k}$. $\forall U \subset X$ open we assign $\mathcal{O}_X(U) = \{ f : U \to k \text{ regular} \}$ together with the usual restriction of maps of functions forms a sheaf $\mathcal{O}_X$ (structure sheaf ; sheaf of regular functions on X) (sheaf of rings)

This, as we saw in is a more general approach to taking X alg set, f locally rational on g $A = A(X)$ ... clear.

ii) $X = \mathbb{R}^n$ usual topology, set $\mathcal{F}(U) = \{ \varphi : U \to \mathbb{R} \text{ continuous} \}$ for $U \subset \mathbb{R}^n$ open forms a sheaf $\mathcal{F}$ on X with usual restrictions. (We could substitute cont by diff, analytic, arbitrary..)
C^∞

iii) Let M be a top space, E top space $\pi : E \to M$ cont st 1) $\forall p \in M$, $\overset{= E_p}{\pi^{-1}(\{p\})} \subset E$ is endowed with a k-dim real vs pace structure . 2) $\forall p \in M$ $\exists$ U nbgh of p in M and $\Phi : \pi^{-1}(U) \to U \times \mathbb{R}^k$ homeo st

$$\begin{tikzcd}
\pi^{-1}(U) \arrow[rr, "\Phi"] \arrow[dr, "\pi"'] & & U \times \mathbb{R}^k \arrow[dl, "\pi_1\ (\text{proj})"] \\
& U &
\end{tikzcd}$$

commutes and $\forall q \in U$, $\Phi|_{E_q} : E_q \to \{q\} \times \mathbb{R}^k \cong \mathbb{R}^k$ iso of vs.

(E together with π satisfying that)

This is called a real vector bundle of rank k ; if the vs are complex then complex v.bundle ;
if M, E smooth manifolds and the Φ can be chosen to be diffeomorphism then it is called smooth vector bundle
(see Lee, but intl. clear)

Rank 1 $\equiv$ line bundle

Tangent Bundle : M manifold, $E = \bigsqcup_{p \in M} T_p M = \{ (p, X) : p \in M, X \in T_p M \}$, π proj . (Ex of v. Bundle)

think k-regular surf
or read def from Lee
This is not a course in manifolds

(needs details, prop 5.3 Lee S.M)

Whenever we have a smooth vector bundle we have a sheaf of sections. $\forall U \subseteq M$ open $\mathcal{F}(U) = \{ s : U \to E : \pi \circ s = id_U \}$ with usual restrictions. (note $s(p) \in E_p$

(Fact : If you know the sheaf of sections you know the vector bundle up to iso)

this fact requires defns but good to have the idea .

(He mentioned that $\mathcal{F}|_U$ is locally free but I didn't quite get it ; a section about local and Global frames of Lee seems to be connected to this) . He also said that the advantage of sheaves of sections is that you can generalise them to quasi coherent sheaves . (I guess that here one should define vector bundle in the alg geo sense)

(take it as locally free appears here and more generally, below) ↳ replace manifold by variety
(alg var, scheme ...)

Glimpse of quasicoherent sheaves

DEF A ringed space $(X, \mathcal{G})$ is a pair where X top space, $\mathcal{G}$ sheaf of rings on X. A sheaf of $\mathcal{O}_X$-modules is a sheaf $\mathcal{F}$ on X such that for each open set $U \subseteq X$ the group $\mathcal{F}(U)$ is an $\mathcal{G}(U)$-module and for each $V \subseteq U$ open the hom $\mathcal{F}(U) \longrightarrow \mathcal{F}(V)$ is compatible with the module structures via the ring hom $\mathcal{G}(U) \to \mathcal{G}(V)$.

Let $X = \text{Spec-m}(A)$ (if you drop m, affine scheme; we think affine variety. I will assume A reduced affine k-alg $k = \bar{k}$ for consistency with sec II; he didn't say anything)

Let $f \in A$, $X_f = \text{Spec}(A_f) = \{P \in X : f \notin P\}$ open subset of X. If M is an A-module it is a fact that $\exists!$ sheaf $\tilde{M}$ of "$\mathcal{O}_X$-modules" defined by $\tilde{M}(X_f) := M_f$ (I guess this determines sheaf of $\mathcal{O}_X$-modules seems reasonable)

{with restriction maps .... (he just did a case $X_f \subseteq X_g$, $f = gh$)

Example i) Let $M = A$, then $\tilde{A}(X_f) = \mathcal{O}_X(X_f)$ (Comes from the obs that $\mathcal{O}_X(X_f) = A_f$ similar if not exactly what we did before in sec II.)

ii) A line bundle corresponds to an invertible A-module. So $\text{Pic}(X) := \{\text{line bundles}\}/_{\cong}$ with op the tensor product of line bundles

Honestly I do not know exactly what he means but it seems good reason to study inv. modules.

Idk what quasicoherent sheaf is in all of this. (I think that the sheaf from the fact is what it is called quasicoherent; see Hartshorne for def).

I think that so far this part of the discussion is to justify why we study invertible modules (geom. motivation) now we talk about divisors. It is more natural to start talking about Weil divisors first

---

Divisors in Geometry.

Let $X \subseteq \mathbb{A}^n$ irreducible alg set (in my head I'm taking $k = \bar{k}$) (he took spec-m(A) of course), by definition a prime divisor is $Y \subseteq X$ closed irred with $\dim Y = \dim X - 1$ $\left(\begin{array}{l}\dim X := \dim A(X) \\ \dim Y := \dim A(Y)\end{array}\right)$ $\left(\text{if we say } \dim Y = \dim(\overset{\text{in } A(X)}{I(Y)}) \text{ makes sense since } \dim(I(Y)) = \dim(A(X)/I(Y)) = \dim\left(\dfrac{k[x_1, \dots, x_n]/I(X)}{I(Y)/I(X)}\right) = \dim(A(Y))\right)$

This is equivalent to $I(Y) \subseteq A(X)$ being a codim 1 prime.

(as we've said before $I(Y) \subseteq A(X)$ is $I(Y)/I(X)$ ← sense of being of the course)

($\dim A = \dim I + \text{codim } I$ A affine domain)

We define the group of Weil Divisors of X to be the free abelian group generated by prime divisors. As a set we denote it by

$$\left\{ \sum_{\substack{Y\subseteq X\\ \text{prime}}} m_Y [Y] \;:\; m_Y \in \mathbb{Z} \text{ all } 0 \text{ but finitely many} \right\}$$

(sum is clear; formally these are formal sums.... ... ✓.)

we write this to make diff between divisor and generator.

The point of Weil divisors is that we can keep track of zeroes and poles of a function.

Let $0 \neq f \in K(A(X))$, let $Y \subseteq X$ prime divisor. There is a well defined integer called
(field of fractions; so nonzero rational function)

"order of vanishing of f along $Y = v_Y(f)$" Given this we define $\operatorname{div}(f) = \sum_{\substack{Y\subseteq X\\ \text{prime}}} v_Y(f)[Y] \in \operatorname{Div}(X)$
(Principal Weil divisor of f)
(ass to)

I will say some things about $v_Y(f)$:

i) In the general thy of schemes this is only defined when you have a normal scheme or a variety

ii) It works as follows: Recall that if f rational function on X so defined in all but finitely many pts of X thus defined in all but finitely many points of Y.
1) If f defined at all points of Y, $v_Y(f) \geq 0$
2) If 0 everywhere at Y where it is defined $v_Y(f) > 0$
3) $f = h/g$, $v_Y(f) = v_Y(h) - v_Y(g)$ $h, g \in A(X)$ (well def)

iii) Importantly is a finite sum for the next reason:

Let $f \in A(X)$, if $v_Y(f) > 0$ (f defined everywhere) f is zero in all Y so $f \in I(Y) \subseteq A(X)$ and this holds iff $I(Y)$ minimal prime over $\langle f \rangle$. So there are finitely many such Y
$(I(Y)/I(X))$
Y codim 1

now with principle 3) follows for rational func.

iv) If f defined at some point of Y then $f \in \mathcal{O}_{X,Y}$ (see geometry disc after C94) we let (this works in this case; affine)
$\in K(A(X)) \setminus \{0\}$

$$v_Y(f) = \text{length}\left(\mathcal{O}_{X,Y} / \langle f \rangle \right)$$

we are taking the length of this as a ring (module over itself). Why finite?

$\mathcal{O}_{X,Y} = A(X)_{I(Y)}$ local ring, codim $I(Y) = 1$ $(\subseteq A(X))$. A chain of primes in this ring corresponds to a chain of primes in $I(Y)$ so the dim of this ring is 1

But $A(X) = k[x_1, -, x_n]/\text{Prime}$ so domain, (X irred) $I(Y) \ni 0$ so $\mathcal{O}_{X,Y}$ domain

thus 0 prime hence in $\mathcal{O}_{X,Y}$ $0 \subsetneq m$ where m is the max ideal is a max chain

clearly $\mathcal{O}_{X,Y}/\langle f \rangle$ has dim 0 so every prime is maximal so Art. Thus finite length.

(easier to say $\mathcal{O}_{X,Y} \subseteq K(A(X))$ field.)

v) Now one needs to prove 1, 2, 3

vi) If $f \notin \mathcal{O}_{X,Y}$ we need more work (Andras said not too hard; but referred to Fulton int thy...)

vii) When X normal, $A(X)$ normal so by C93 $\mathcal{O}_{X,Y}$ DVR so m_Y the max ideal of $\mathcal{O}_{X,Y}$

is $<t>$, $f\in\mathcal{O}_{X,Y}$ then $f=ut^d$ $u\in\mathcal{O}_{X,Y}^*$ unit, $d\in\mathbb{Z}$. Now with a lot of work $v_Y(f)=d$.

This gives good information about principal Weil divisors. (I guess that if X has dim 1 to start or other specific conditions it is easier to define directly)

Assume now $X\subseteq\mathbb{A}^n$ normal $\overset{\text{irred}}{\text{alg}}$ set (He wrote spec-m(A) normal)

$A(X)$ is normal domain (noeth) so $A(X) \underset{\substack{\downarrow\\94}}{=} \bigcap_{\substack{\operatorname{codim}(P)=1\\ P\in\operatorname{Spec}(A(X))}} A(X)_P \subseteq K(A(X))$

But $\{P\in\operatorname{Spec}(A(X))\ \operatorname{codim} 1\}$ corresponds bijectively to $\{Y\subseteq X \text{ prime divisors}\}$ so

$$\underset{\substack{\downarrow\\ \text{geom}\\ \text{due sec 11}}}{\mathcal{O}_X(X)}=A(X)=\bigcap_{\substack{Y\subseteq X\\ \text{prime div}}}\mathcal{O}_{X,Y}=\{f\in K(A(X))\setminus\{0\}:\ \operatorname{div}(f)\geq 0\}\cup\{0\}$$

(this follows from the def; here our def applies)

{Slightly more generally (think) $U\subseteq X$ open, $\mathcal{O}_X(U)=\{f\in K(A(X))\setminus\{0\}:\ \forall Y\overset{\text{prime}}{\subseteq} X\ \ Y\cap U\neq\emptyset$ then $v_Y(f)\geq 0\}\cup\{0\}$.

I didn't check.

In this situation we define the class group of X, $Cl(X)=\operatorname{Div}(X)/$subgroup of principal divisors

This group is smaller and tells nice things about the algebra and geometry of X.

Example i) $Cl(\mathbb{A}^n)=0$.

We need to show that every prime divisor $Y\subseteq X$ satisfies $[Y]=\operatorname{div}(f)$ for some $f\in K(A(X))^*$

But $I(Y)$ is a codim 1 prime in $k[x_1,\dots,x_n]$ so by corollary 81 is principal thus $I(Y)=<f>$, $f\in k[x_1,\dots,x_n]$ irreducible. So $\operatorname{div}(f)=Y$

{ a bit unsure; I would need to think a bit

ii) More generally we notice that the thing we are using about $k[x_1,\dots,x_n]$ is C81, i.e. that it is a UFD so with a bit more details but essentially same argument X $\overset{\text{irred}}{\text{alg}}$ set $A(X)$ normal

A UFD iff $Cl(X)=0$ (he did it for spec-m(A), A normal affine domain; same thing)

(iff all codim 1 prime are princ)

(I could try to make sure about and then try to prove this more general case. Ask Anders if needed) keep photo just in case.

(Photo 1)

(At the beginning of the lecture of April 18th (Tues) he gave two examples; I'll keep the notes of that as Photo 2 but I'll not say much here)

(an elliptic curve appears)

I'm sure very instructive but I prefer to keep going now

So far the divisors that we've discussed in Geometry terms are not the ones we've seen in comm alg.

Now Anders discussed Cartier Divisors in Geometry.

I mention the defn; $X \subseteq \mathbb{A}$ normal irred alg set $D \in Div(X)$ we say that D is a **Cartier Divisor** if it is locally principal ($\forall x \in X, \exists x \in U$ open st $D_{|U} = 0 \in Cl(U)$)

?? U should be named

He talked (18th April) about how to restrict divisors, he gave examples and did a bit more; at the end these things are related to line bundles on variety and they have a fractional ideal associate (he redefined Cartier divisor); one of the last sentences is that D cartier iff $I(D)$ invertible

(spoke about local equations, strongly locally factorial...)

needs defn.

(I'll keep the notes of the rest of this doc as Foto3, but I will stop now for many reasons, for example I have many stupid questions that stop me a bit, better things to look at etc...)

Connects with comm alg !!

I end this divisors discussion here; the Goal was to see that this divisor/frac ideals are important in alg geo and we've at least said something. Now I'll go back to comm alg, where Weil divisors will appear and the defn will be "motivated" thanks to this discussion.

(the relation will be more clear than with Cartier).

. One possibility of my relation with divisors is : Current status : I know comm alg version; have some idea of Geo

then (
learn from Gathmann (easy version of divisors, goal: gain intuition and fully understand easy case)

then (
Go back to Photo 2, Photo 3, examples and see if more clear — see what Lev discussed

then (
learn divisors in an alg geo II class (Hartshorne ch 2)

End of digression.

(video: Last Geom digression)

Back to comm. alg

(≈ 11.4 Eb)

27. UNIQUE FACTORIZATION OF CODIM 1 IDEALS, DEDEKIND DOMAINS.

DEF let R be a Noetherian domain we say that R is **locally factorial** if R_P is a UFD $\forall P \in Spec(R)$

Again enough to prove it for max ideals, similar details.

Note If R UFD $\longrightarrow$ R locally factorial (noeth) —— R normal (deeper proof of the known fact UFD → Normal)

It is not hard to see that if R UFD, U mult closed $0 \notin U$ then $U^{-1}R$ is

(easy as expected; if doubts see math exchange)

$R = \bigcap_{P \in Spec(R)} R_P \subseteq K(R)$ frac. field ($R_P \subseteq K(R)$) see start of sec 25)

with R_P UFD so normal

It follows is normal.

DEF let R be a ring, $I \subseteq R$ ideal. We say that I has pure codimension C if codim $P = C$ $\forall P \in \mathrm{Ass}_R(R/I)$
(By convention $I = \langle 1 \rangle = R$ has pure codim C $\forall c \in \mathbb{N}$.)

- Geometrically $I \subseteq k[x_1, -, x_n]$, I has pure codim C iff all irreducible components of $\overset{X}{\overset{\shortparallel}{Z(I)}}$ (in $\mathbb{A}^n$) have dimension $n-c$ and there are no embedded components. (Not trying to write a formal proof but quite clear at least intuitively; formally easy exercise)

this depends on I, not on X. If I radical no embedded case as we saw. And in general $Z(I) = Z(\sqrt{I})$.

note that if you have an embedded comp that comp will be higher

As an example, $I = \langle x^2, xy \rangle \subseteq k[x,y]$ has no pure codim.

Theorem 99 Let R be a locally factorial noeth domain, then

i) $I \subseteq R$ ideal, I invertible R-module iff I has pure codim 1. (R empty product)

ii) $I \subseteq K(R)$ invertible fractional ideal. Then I can be uniquely expressed as product of powers of codim 1 primes $\subseteq R$. In particular $C(R)$ free abelian group gen by codim 1 primes of R (isom to)

Proof/ The in particular is obvious.

i) If $I = R$ trivial; $\rightarrow$) $I \subsetneq R$ ideal. Assume it is an invertible ideal. Let $P \in \mathrm{Ass}(R/I)$, since I invertible $I_P \cong R_P$ so $I_P = \langle x \rangle \subseteq R_P$ x nonzero divisor of R_P.
We have that $P_P \in \mathrm{Ass}(R_P/I_P)$. Now R locally factorial so R normal, thus R_P normal.

Thus by Serre Vs 1 $((R_P)_{P_P} \underset{\text{rings}}{\cong})R_P$ is a DVR or a field (if field then $I_P = 0$ ↯ or $I_P = R_P$ but in this case there are no ass primes)

So R_P DVR hence $\dim R_P = 1 \underset{\substack{\downarrow \\ R_P \text{ local}}}{=} \mathrm{Codim}(P_P) \underset{\text{thus}}{=} \mathrm{codim}(P)$. So I has pure codim 1.

$\leftarrow$)

Claim Let $P \subseteq R$ prime of codimension 1, then it is invertible as an R-module.

Let $m \in \text{Spec-m}(R)$ a) $P \not\subseteq m$ then $P_m = R_m$ (r/u, $r \in R$, $u \in R \setminus m$ take $u' \in P \setminus m$ then $r/u = ru'/uu' \in P_m$)

b) $P \subseteq m$ then $P_m \subseteq R_m$ UFD (R locally factorial) so normal.
$P_m \in \mathrm{Spec}(R_m)$ and codim$(P_m) =$ codim $P = 1$. By corollary 81 P_m principal.
Now easy $P_m \cong R_m$ (generator to 1; as R_m modules, R-modules ...)

Claim Let I be an ideal of R of pure codimension 1, then it is a finite product of codim 1 primes (since the product of invertible ideals is invertible we will be done with ←; this will also help to prove ii)

Pf: If false (thanks to R being noeth) let I be $\overset{\text{pure}}{\text{codimension}}$ 1 ideal maximal wrt the property of not being expressable as (finite) product of codim 1 primes of R. Note $I = R$ is by convention the empty product of prime ideals so wma $I \subsetneq R$. Let P be minimal prime over I (R Noeth) by thm 30 $P \in \mathrm{Ass}_R(R/I)$ so $\operatorname{codim} P = 1$. Since P invertible by the previous claim, by thm 97 $P^{-1}P = R \subseteq K(R)$ field of fractions thus $R \subsetneq P^{-1}$! else $R=P$ Assume $I = P^{-1}I$ let $t \in P^{-1}$ by Cayley Hamilton $M = I, J = R$ and $\varphi : I \xrightarrow{t} I$ $\exists\ x^n + a_1 x^{n-1} + \dots + a_0 \in R[x] : \varphi^n + a_1\varphi^{n-1} + \dots + a_0 = 0 \in \mathrm{End}_R(I)$

So the image of 1 is 0, $t^n + a_1 t^{n-1} + \dots + a_0 = 0$ thus $t \in \bar{R}$ but R locally factorial so normal thus $t \in R$ so $P^{-1} \subseteq R$ ↯. Hence $R = P^{-1}P \supseteq P^{-1}I \underset{(1 \in P^{-1})}{\supsetneq} I$.

Now we want to see $P^{-1}I$ as an ideal of R has pure codim 1. Let $Q \in \mathrm{Ass}_R(R/P^{-1}I)$

We want to see that $Q \in \mathrm{Ass}_R(R/I)$ so that $\operatorname{codim} Q = 1$.

Note $Q \in \mathrm{Spec}(R)$ and P invertible so $P_Q \cong R_Q$ thus $P_Q = \langle x \rangle \subseteq R_Q$ for some $x \in R_Q$ (image of 1 and inv in R_Q) Consider $R_Q \xrightarrow{x\cdot} R_Q/I_Q$ the kernel is

$x^{-1}I_Q = (P^{-1}I)_Q$ ($x^{-1}I_Q$ is the kernel and clearly $x^{-1}I_Q \subseteq (P^{-1}I)_Q$ but $P^{-1}I)_Q$ easily seen to be in the kernel.)

wrong !! in mind.

(as we noted in last stupid rmk it does not matter R_Q has / R has)

So $R_Q/(P^{-1}I)_Q$ iso to submodule of R_Q/I_Q (remk 2 after def of ass). Thus $\overset{\cong\ R_Q/(P^{-1}I)_Q}{(R/P^{-1}I)_Q}$ iso to a submodule of $(R/I)_Q$. Now $Q_Q \in \mathrm{Ass}_{R_Q}((R/P^{-1}I)_Q)$ by 30 iii

So R_Q/Q_Q iso to submodule of ↗ so iso to submodule of $(R/I)_Q$

Thus $Q_Q \in \mathrm{Ass}_{R_Q}((R/I)_Q)$ and thus by thm 30 ii (and prop 8 probably) $Q \in \mathrm{Ass}_R(R/I)$

By maximality $P^{-1}I = P_1 \cdots P_e$ all P_i codim 1, thus $I \underset{\text{easy}}{=} P P_1 \cdots P_e$ product of codim 1 primes ↯

ii) $I \subseteq K(R)$ invertible fractional ideal, then $\exists\ u \in R$ nzd : $uI \subseteq R \subseteq K(R)$. I has pure codim 1, uI ideal in R iso as an R module to I thus uI has pure codim 1 hence product of codim 1 primes. Now $\langle x \rangle$ invertible so product of codim 1 primes $I = \langle x \rangle^{-1}(xI)$. ($\langle x \rangle^{-1}$ = invert the primes) so I is product of powers of codim 1 primes in R

already defined how to mult. 2 thus we can multiply 1000 ; also consistent because of ring axioms.

Finally uniqueness; suppose $\prod_{i=1}^{m} P_i^{d_i} = \prod_{j=1}^{n} Q_j^{e_j} \subseteq K(R)$ $\underset{\subseteq R}{P_i, Q_j}$ codim 1 primes $d_i, e_i \in \mathbb{Z}$

Multiplying both sides by primes that appear with negative powers WMA $d_i, e_i \geq 0$. Induct on $d = \sum_{i=1}^{m} d_i$. If $d=0$, $I=R$, $n=0$ ✓. Suppose $d \geq 1$ $\prod P_i^{d_i} \subseteq Q_1$. Since Q_1 prime $P_i \subseteq Q_1$ for some i. Since they have codim 1, $P_1 = Q_1$. Q_1 invertible so we mult by Q_1^{-1} both sides (so $Q_1^{-1} Q_1 (*) = R(*) = (*)$) and apply induction □

DEF A Dedekind domain is a normal Noetherian domain of dimension 1.

These objects are important in Number Theory.

Examples i) $\mathbb{Q} \subseteq L$ finite ext. Let $R = \mathbb{Z}^L$. Then R normal, domain. Since dim $\mathbb{Z} = 1$ by Going up and incomparability we see dim $R = 1$. By Finiteness of integral Closure R is fg as a $\mathbb{Z}$-module. So Noetherian $\mathbb{Z}$-module ; ideals of R are $\mathbb{Z}$ submodules so R is Noeth hence Dedekind.

ii) Anders' notes in danish have a few more

iii) $\underset{\text{dom.}}{R \text{ Dedekind}} \longrightarrow R$ locally factorial. Let $P \in \operatorname{Spec}(R)$ consider R_P noeth local domain and normal. Dim $R_P = 0, 1$. If R_P has dim 0 since it is a domain, R_P field so UFD. If R_P has dim 1, by C91 R_P DVR – UFD.

We translate the last result to Dedekind domains

Corollary 100 (Dedekind) Let R be a Dedekind domain. Every $0 \neq I$ ideal is invertible and every factorial ideal $0 \neq I \subseteq K(R)$ is invertible. Finally $C(R)$ is a free abelian group generated by maximal ideals.

(isom to ... language)

Proof/ Codim 1 prime in R ≡ max ideals in R ≡ nonzero primes in R.

If $\underset{\subseteq R}{I \neq 0}$, $P \in \operatorname{Ass}_R(R/I)$ then $\underset{\in \operatorname{Spec}(R)}{P \neq 0}$ so codim 1. By the last theorem I inv.

If I nonzero fractional ideal ($I \subseteq K(R)$) I is isomorphic as an R-module to a nonzero ideal of R so invertible. □

(It is known that every abelian group appears as the Picard Group of some Dedekind domain.

28. WEIL DIVISORS

(in 11.5 Eis)

DEF Let R be a ring we define $\operatorname{Div}(R)$ to be the free abelian group generated by codimension 1 primes and we refer to its elements as Weil Divisors (makes sense)

Formal linear combos of codim 1 primes with integer coeff

Note Suppose R noeth, $\dim R = 1$, $a \in R$ nzd then $\dim(R/\langle a\rangle) = 0$ so finite length (thm 20.)

The correspondence thm also bijects primes containing I with primes in R/I $(P \to P/I)$. Thus the primes in $R/\langle a\rangle$ are $P/\langle a\rangle$ with $P \in \operatorname{Spec}(R)$. If we have a chain $P_1/I \subsetneq P_2/I$ of primes this gives $P_1 \subsetneq P_2$ prime in R so P_1 minimal over 0 so P_1 contains only zero divisors by thm 30.
Thus $\dim(R/\langle a\rangle) = 0$.

Theorem 101 Let R be a Noetherian ring, then (this and proof remind a lot to the geo div.)

i) $\exists$ (unique) group hom $\varphi : C(R) \longrightarrow \operatorname{Div}(R)$

$$\underset{\text{inv ideal}}{\underset{\subseteq R}{I}} \longmapsto \sum_{\substack{\operatorname{codim}(P)=1 \\ P \in \operatorname{Spec} R}} \operatorname{length}(R_P/I_P) \cdot P$$

ii) If $\dim(R) = 1$ $\exists$ (unique) group hom $C(R) \longrightarrow \mathbb{Z}$

$$\underset{\text{inv ideal}}{I \subseteq R} \longmapsto \operatorname{length}(R/I)$$

as a ring or R-module, same I did a rmk about this

Remarks i) R_P one dimensional Noeth since P has codim 1 (loc of Noeth, noeth) thm 8). I invertible so ideal so $I_P \cong R_P$ and thus I_P contains nzd of R_P so by the (proof of the) note above $\operatorname{length}(R_P/I_P) < \infty$.

ii) By 98 $C(R)$ is generated by $\{I \subseteq R \text{ ideal, invertible as } R\text{-modules}\}$.
If G, H abelian groups and G gen by S. $\varphi : S \to H$ any function st if $a_i, b_j \in S$ $\prod_{i=1}^{n} a_i = \prod_{j=1}^{m} b_j$ then $\prod_{i=1}^{n} \varphi(a_i) = \prod_{j=1}^{m} \varphi(b_j)$) defines a (unique) group hom $\varphi : G \to H$ extending φ (a bit more details in E.s p263; but suff clear). So we know what we need to check.

Proof / Suppose $I \subseteq R$ inv ideal. We already know that $\operatorname{length}(R_P/I_P) < \infty$ but to make sure we land in $\operatorname{Div}(R)$ we need to see that only for finitely many P the length is nonzero. Let P be of codim 1, if $I \not\subseteq P$ (*) it is easy to see that $\operatorname{length}(R_P/I_P) = 0$ (the ring is 0 I think)
If $I \subset P$ since I contains nzd (97.ii) and P has codim 1 P must be minimal over I
(If $Q \subsetneq P$ $Q \in \operatorname{Spec}(R)$ minimal over I, since P has codim 1 Q minimal over 0 so the elements of Q are zero divisors by thm 30 so I can't be in Q). and there are finitely many of these.

To finish i) we need to show that φ respects products. To do so suppose $I = \prod_{j=1}^{n} I_j$ $I_j \subseteq R$ invertible ideals. Then NTS $\operatorname{length}(R_P/I_P) = \sum_{j=1}^{n} \operatorname{length}(R_P/(I_j)_P)$ $\forall P$ prime of codim 1.

WMA R local with max ideal P (so one dimensional) P has codim 1 (easy).

I_j is invertible ideal in R; So $R \cong \underset{\text{(all elmts outside } P \text{ are units)}}{R_P \cong I_{jP}} \cong I_j$ thus I_j is necessarily principal gen by nzd (the image of 1 under iso)

So $I_j = \langle \underset{\text{in } R}{\overset{}{a_j}} \rangle$ $a_j \in R$ nzd. We NTS that length $(R/\langle \prod a_j \rangle) = \sum_{j=1}^{n}$ length $(R/\langle a_j \rangle)$

Consider $R \supset \langle a_1 \rangle \supset \langle a_1 a_2 \rangle \dots \supset \langle \prod_{j=1}^{n} a_j \rangle$. Of course to prove equality NTS

$\langle \prod_{j<i} a_j \rangle / \langle \prod_{j \leq i} a_j \rangle \cong R/\langle a_i \rangle$ (easy ex. See E.s p264 details)

ii) Suppose $\dim R = 1$, $I \subseteq R$ invertible so contains a nzd. Thus $\dim(R/I) = 0$ (similar argument as note above). Thus finite length (thm 20). See the note in the proof of thm 19

$R/I \cong \bigoplus_{P \text{ max ideal of } R} \overset{= R_P/I_P}{(R/I)_P}$; now if codim $P = 0$ P is minimal over 0 so all the elmts are zero divisors

thus $I \not\subseteq P$ and as above, $R_P = I_P$ so $(R/I)_P = 0$. If codim $P = 1$ arguing as above

$R_P/I_P \neq 0 \to P$ minimal over I. Thus $(R/I)_P \neq 0 \to P$ codim 1 prime containing I.

Thus length $(R/I) = \sum_{\substack{P \text{ codim 1 prime} \\ \text{containing } I}}$ length (R_P/I_P). Now the comp of $\varphi : C(R) \to Div(R)$

and then $Div(R) \to \mathbb{Z}$ (which is a group hom; comp of 2) is when restricted to I invertible

$\sum_{\substack{P \text{ codim } 1 \\ \text{prime}}} n_P P \longmapsto \sum n_P$

ideal of R the map $I \to$ length (R/I). Now ii follows (by remark ii and knowing $\exists$ such hom) $\square$

Recall that we had $K(R)^\times \xrightarrow{\theta} C(R)$ hom. Well then $\varphi(Ra) \in Div(R)$ is called a principal divisor.
$a \longmapsto Ra$ $\quad$ $a \in K(R)^\times$ $\quad$ (now yes)

And also we define $\underset{\text{class group of } R}{Cl(R)} \equiv \underset{\text{Chow group of } R}{Chow(R)} = Div(R) / \underset{\text{group of principal divisors} \equiv PD}{\varphi(\theta(K(R)^\times))}$ (R any Noeth ring)

The map $\varphi : C(R) \longrightarrow Div(R)$ induces a hom $\Psi : Pic(R) \longrightarrow Chow(R)$
$[I] \longrightarrow \varphi(I) + PD$.

(this is because $\frac{C(R)}{\theta(K(R)^\times)} \longrightarrow Pic(R)$ iso ; see 98)
$I + \theta(K(R)^\times) \longmapsto [I]$

Note: If R locally factorial then by 9.9, $\mathrm{Div}(R) \cong C(R)$ (Both free abelian same set of gen but written differently)

it is an easy exercise to see that ψ iso in this case

In general ψ not inj nor onto. We have the diagram (commutative)

$$\begin{tikzcd}
0 \arrow[r] \arrow[d, equal] & R^\times \arrow[r] \arrow[d, equal] & K(R)^\times \arrow[r, "\theta"] \arrow[d, equal] & C(R) \arrow[r, "\pi"] \arrow[d, "\varphi"] & \mathrm{Pic}(R) \arrow[r] \arrow[d, "\psi"] & 0 \arrow[d, equal] \\
0 \arrow[r] & R^\times \arrow[r] & K(R)^\times \arrow[r, "\varphi \circ \theta"'] & \mathrm{Div}(R) \arrow[r, "\pi"] & \mathrm{Chow}(R) \arrow[r] & 0
\end{tikzcd}$$

Fact: If R Normal Noeth ring then φ, ψ 1-1 (We proved this on the first 10 min of the lecture of April 25th). I leave it as reading (prop 11.11 Eis).
Danish notes ... many sources

(There were 2 extra lectures; VIDEO Extra lectures)