Krull Hauptidealsatz.

R ring $f \in R$

$(f) \subset p$ p minimal among primes containing f $\Rightarrow$ $ht(p) \leq 1$

Proof simplifications:

Assume • $R = R_p$ ($\Rightarrow$ p is a maximal ideal of R, no other maximal ideals = R is a local ring)

• Assume R is a domain

$(0) \subset R$ is a prime ideal

• $f \in R$ $rad(f) = p$ $\Leftrightarrow$ $p^n \subset (f)$

• q prime $\{0\} \subset q \subset p$, $q \neq \{0\}$, $q \neq p$.

We want to get a contradiction.

Tools (for local rings)

Def R is a local ring if it has a unique maximal ideal $p = m$; any $x \in R \setminus p$ is invertible

Prop 1 $\bigcap_{n=1}^{\infty} m^n = \{0\}$ (for R, m noetherian local ring)

Prop 2 Nakayama lemma

if $a \subset R$ is an ideal s.t. $ma = a$ then $a = 0$.

Clearly Prop 2 $\Rightarrow$ Prop 1

$x \in \bigcap m^n \Rightarrow x \in m \cdot \bigcap m^n$

$\Downarrow$

$\forall n$ $x \in m^n \Rightarrow x \in m \cdot m^{n-1}$

$\forall n$ $x = \sum a_i b_i$ $a_i \in m$ $b_i \in m^{n-1}$

Proof R noetherian local ring

$a \subset R$ satisfies $ma = a$:

Since R is noetherian, we can write $a = (f_1, \dots, f_n)$

$ma = a$ implies:

$\forall i$ $f_i = \sum_{j=1}^{n} c_{ij} f_j$ $c_{ij} \in m$.

trick: write as a matrix

$$\begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} = \begin{pmatrix} & c_{ij} & \end{pmatrix} \cdot \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix}$$

$f = C \cdot f$ in R^n

$\Downarrow$

$(1 - C) f = 0$ in R^n.

$1 - C$ is invertible! because $\det(1-C) = 1 \mod m$

$\Downarrow$

$\det(1-C)$ is invertible in R

$\Downarrow$

$1 - C$ is invertible (by linear algebra there is a formula for $1-C$ with denominators only containing $\det(1-C)$.) Kramer's rule.

Let M be s.t. $M(1-C) = I_n$

then we obtain $M(1-C) f = f \Rightarrow f = 0$

$\Rightarrow f_i = 0$ $\forall i \Rightarrow a = 0.$)

Prop 2 $\Rightarrow$ Prop 1:

Consider $\bigcap_n m^n$. This is an ideal generated by some $f_1, \dots, f_m$

$m. \bigcap m^n =$

$(\bigcap m^n : m) \subset (\bigcap m^n : m^2) \subset \dots$ must stabilize

$\{x : xm \subset \bigcap m^n\}$

$\bigcap_n m^n : m^k$

$\bigcap_n m^n = p_1 \cap \dots \cap p_k$

$m = (a_1, \dots, a_m)$

$f_i = \sum$ monomials in a_i - elements of R of length $\geq n$

$\bigcap_n m^n \cdot \bigcap_n m^n \subseteq \bigcap_n m^n$

$\bigcap_n m^n \subset rad(\bigcap m_n) \subset m$ $rad(m^n) = m$

$x \in a_1 m^k + a_2 m^k + \dots + a_n m^k$

$x \in a_1 m^k \mod a_2, \dots, a_n$

$x \in \bigcap m^n$

m $m \supset m^2 \supset m^3 \supset \dots$

Use Prop 2: Krull's theorem proof: $m^n \subset (x)$

Prop 3 Suppose (R, m) is a local ring, suppose $m^n = 0$ then R is Artinian, which means any decreasing chain of ideals stops.

$a_1 \supset a_2 \supset \dots$ then $a_N = a_{N+1} = \dots$ for some N.

Proof we have R/m, $m/m^2, \dots, m^{n-1}/m^n$

each of these is a finite dimensional vector space over R/m.

$m^i/m^{i+1} \times R/m \to m^i/m^{i+1}$ is well defined. R/m is a field, so m^i/m^{i+1} is a vector space. If it wasn't fin. dim, we have an infinite increasing sequence of subspaces $V_1 \subset V_2 \subset \dots \subset m^i/m^{i+1}$.

So $V_1 + m^{i+1} \subset V_2 + m^{i+1} \subset \dots$ is an infinite sequence of ideals X.

We can "think" $R = R/m + m/m^2 + \dots + m^{n-1}/m^n$ finite dimensional.

Example $\mathbb{Z}/p^2\mathbb{Z}$ we have

a s.e.s. $0 \to \mathbb{Z}/p\mathbb{Z} \xrightarrow{p} \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \to 0$

but $\mathbb{Z}/p^2\mathbb{Z} \neq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ as a ring.

Choose on each m^i/m^{i+1} a filtration, i.e. a sequence of subspaces $V_1^{(i)} \subset V_2^{(i)} \dots \subset V_{N_i}^{(i)} = m^i/m^{i+1}$ with $\dim V_j^{(i)} = j$.

Then we obtain a filtration of R by ideals

$R \supset m \supset m^2 + V_{N_1-1}^{(1)} \supset m^2 + V_{N_1-2}^{(1)} \supset$

$\supset m^2 + V_1^{(1)} \supset m^2 \supset m^3 + V_{N_2-1}^{(2)} \supset \dots$

so on. After renumbering we obtain a sequence of ideals

$R \supset a_1 \supset a_2 \supset \dots \supset a_N = 0$

s.t. $a_1 = m$ $a_i / a_{i+1} \cong R/m$ (is a 1-dimensional vector space)

$R = R/a_N \to R/a_{N-1} \to \dots \to R/a_1$

is a sequence of rings.

Let $b \subset R$ be arbitrary ideal.

$\Rightarrow$ we have a sequence of ideals

$b \cap a_1 \supset b \cap a_2 \dots \supset b \cap a_N = 0$.

$\forall i$ (1) $b \cap a_i = b \cap a_{i+1}$ or

(2) $b \cap a_i / b \cap a_{i+1} \cong R/m$.

Let's count the # of (2), is called the length of b.

Claim $b \supsetneq b' \Rightarrow length(b) > length$ of b'.

look at first i such that $b' \cap a_i \neq b' \cap a_{i+1}$ $\Rightarrow$

length of $(b' \cap a_{i+1}) + 1 = len(b')$

if $b \cap a_i \neq b \cap a_{i+1}$ then length of $(b \cap a_{i+1}) + 1 = len(b)$,

so we replace b, b' by $b \cap a_{i+1}, b' \cap a_{i+1}$

$$\begin{matrix} b \cap a_1 & = & b \cap a_2 & \dots = & b \cap a_i & \supset & b \cap a_{i+1} \\ \cup & & \cup & & \cup & & \cup \\ b' \cap a_1 & = & b' \cap a_2 & \dots = & b' \cap a_i & \supset & b' \cap a_{i+1} \end{matrix}$$

For $b \cap a_{i+1}, b' \cap a_{i+1}$ the number i will be larger use induction.

$b' \cap a_{i+1} \subset b \cap a_{i+1}$ 1) if they are not equal, then by induction assumption

$len(b' \cap a_{i+1}) < len(b \cap a_{i+1}) \Rightarrow$

$len(b') < len(b)$.

2) if $b' \cap a_{i+1} = b \cap a_{i+1}$:

quotient is R/m $b' \subset b$ the quotient is R/m

b/b' must be 0. Contradiction.

3) $b = b \cap a_i \supset b \cap a_{i+1}$.

b' $b' \cap a_i \supset b' \cap a_{i+1}$

$b = b \cap a_i = b \cap a_{i+1} \Rightarrow b \subset a_{i+1}$

$\Rightarrow b' \subset b \subset a_{i+1}$

so $b' \cap a_i = b' \cap a_{i+1}$.

So if $b \cap a_i \neq b \cap a_{i+1}$ $\Rightarrow$

2 cases: $b' \cap a_i = b' \cap a_{i+1}$ or $b' \cap a_i \neq b' \cap a_{i+1}$

so remaining case is

$b' \cap a_i = b' \cap a_{i+1}$ $b \cap a_i \neq b \cap a_{i+1}$

$b = b \cap a_i \supsetneq b \cap a_{i+1}$

$b' = b' \cap a_i = b' \cap a_{i+1}$

Replace b, b' by $b \cap a_{i+1}, b' \cap a_{i+1}$

By induction assumption

$\ell(b \cap a_{i+1}) \geq \ell(b' \cap a_{i+1})$

$\Rightarrow \ell(b \cap a_i) = \ell(b \cap a_{i+1}) + 1 > \ell(b' \cap a_{i+1})$.

R local ring s.t. $m^n = 0$ some n.

$\Rightarrow$ any ideal $a \subset R$ has an invariant called length $len(a)$,

$a \subseteq b \Rightarrow len(a) \leq len(b)$

$a \subsetneq b \Rightarrow len(a) < len(b)$.

Corollary any decreasing sequence must stop. Such rings are called Artinian.

Conversely, if a noetherian local ring is Artinian then

$m \supset m^2 \supset \dots$ must stop $\Rightarrow$

$m^k = m^{k+1} \Rightarrow m \cdot m^k = m^k \Rightarrow$ by Nakayama lemma $m^k = 0$.

$\dim(R) = \max_{p \subset R \text{ prime}} ht(p)$

if R is local $\Rightarrow \dim(R) = ht(m)$

($\dim R = 0 \Leftrightarrow m$ is minimal $\Leftrightarrow$ $rad(0) = m \Leftrightarrow m^k = 0$ (some k)).

Let's prove Krull's theorem.

(R, m) f $m^k \subset (f)$

$\{0\} \subsetneq q \subsetneq m$ consider R_q

if we prove that R_q is artinian, we are done. ($\Rightarrow ht(q) = 0$).

R_q is artinian $\Leftrightarrow$ $q_q^n = 0$

Consider the sequence of ideals

$R \cap q_q \supset R \cap q_q^2 \supset \dots$

$\pi : R \to R_q$

$\pi^{-1}(q_q) \supset \pi^{-1}(q_q^2) \dots \supset$.

Using Artinianity of $R/(f)$ we have

$\pi^{-1}(q_q) + (f) \supset \dots$ stops $\Rightarrow$

$\pi^{-1}(q_q^k) + (f) = \pi^{-1}(q_q^{k+1}) + (f)$

$\Rightarrow \pi^{-1}(q_q^k) \subset \pi^{-1}(q_q^{k+1}) + (f)$

Look at $\pi^{-1}(q_q^k) / \pi^{-1}(q_q^{k+1}) \subset R / \pi^{-1}(q_q^{k+1})$

any $x \in \pi^{-1}(q_q^k)$

$x = af + x'$ $x' \in \pi^{-1}(q_q^{k+1})$

Consider $af \subset \pi^{-1}(q_q^k)$

$\pi(a)\pi(f) \in q_q^k$ $\pi(f)$ is invertible

$\Rightarrow \pi(a) \in q_q^k \Rightarrow a \in \pi^{-1}(q_q^k)$

modulo $\pi^{-1}(q_q^{k+1})$ we have

$f \cdot \pi^{-1}(q_q^k) = \pi^{-1}(q_q^k) \Rightarrow$

$m \cdot \pi^{-1}(q_q^k) = \pi^{-1}(q_q^k)$ (mod $\pi^{-1}(q_q^{k+1})$)

Nak. $\Rightarrow$ $\pi^{-1}(q_q^k) = \pi^{-1}(q_q^{k+1})$

$\Rightarrow q_q^k = q_q^{k+1} \Rightarrow q_q \supset q_q^2 \supset$ stops

$\Rightarrow q_q^k = 0$ (by Nak.).

$\Rightarrow R_q$ is artinian $ht(q) = 0$ ∎.

So we have $ht(p) = g(p)$

$ht = \max(\dots)$

$g(p) = \min\{n \mid p$ is among minimal primes containing $(f_1, \dots, f_n)\}$.

Theorem $\dim\left(k[\underbrace{x_1, \dots, x_n}_{R}]\right) = n$ for any field k.

Proof $(0) \subset (x_1) \subset (x_1, x_2) \subset \dots \subset (x_1, \dots, x_n)$

these are prime ideals because

$$k[x_1, \dots, x_n]/(x_1, \dots, x_i) = k[x_{i+1}, \dots, x_n]$$ is a domain.

$\Rightarrow ht(x_1, \dots, x_n) \geq n \Rightarrow$

$\dim(R) = \max_p ht(p) \geq n$.

Conversely $\dim(R) = \max_{m \subset R \text{ maximal}} ht(m)$

Let's prove $g(m) \leq n$.

Consider $m \subset k[x_1, \dots, x_n]$ maximal.

By Nullstellensatz

R/m is a finite field extension of k.

So $\pi: R \to R/m$ gives (algebraic) elements $\pi(x_1), \dots, \pi(x_n)$ in R/m

Let p_i be a minimal polynomial of $\pi(x_i)$. This is an irreducible polynomial in $k[x]$.

Consider the ideal

$$a = (p_1(x_1), \dots, p_n(x_n)).$$

Claim m is among minimal primes containing a.

Example $k = \mathbb{R}$, $n = 2$

(i, i)

$\mathbb{R}[x, y] \to \mathbb{C}$

$m = \ker(f \to f(i, i))$

$Z(m) \subset \mathbb{C}^2$ (• (i,i), • $(-i,-i)$)

$p_1(x) = x^2 + 1$

$p_2(x) = x^2 + 1$

(p_1, p_2) in $\mathbb{C}^2$ has 4 points over $\mathbb{R}$:

$x^2 + 1 = 0 \quad y^2 + 1 = 0$

$\Rightarrow (x - y)(x + y) = 0$

$\Rightarrow x = y$ or $x = -y$ in any field

$\Rightarrow$ we have 2 prime ideals containing (p_1, p_2):

$(x^2 + 1, y^2 + 1, x - y)$ and $(x^2 + 1, y^2 + 1, x + y)$.

Let's prove the claim.

$a = (p_1(x_1), \dots, p_n(x_n))$

m is among minimal primes.

we have

$$R/a \cong k[x_1]/(p_1(x_1)) \otimes k[x_2]/(p_2(x_2)) \dots$$

if we have a homomorphism

$R/a \to K$, K field, then the image of R is contained in an algebraic extension of k $L \subset K$.

$R/a \to L$ is surjective $\Rightarrow$

$\ker R/a \to L$ is a maximal ideal

$\Rightarrow$ in R/a any prime ideal is maximal. $\Rightarrow$ any maximal ideal is a minimal prime, in particular m is. ∎

Next step Suppose R_1, R_2 rings

$Spec(R_2)$ $Spec(R_1)$ corresponding spaces.

$\varphi: R_1 \to R_2$ corresponds to

map $\varphi^*: Spec(R_2) \to Spec(R_1)$

we want to understand $im(\varphi^*)$

take $\overline{im\varphi^*} \subset Spec(R_1)$

$Spec(R_2) \to \overline{im\varphi^*}$

we will show $\dim Spec(R_2) \geq \dim \overline{im\varphi^*}$

and other things.

Exercise: is it true that $\bigcap m^n = \{0\}$ in a noetherian local domain?