About the Yoneda Lemma

Instead of proving we prove the A.G. statement.

Input: R, R' rings $\underline{\underline{F_R \cong F_{R'}}}$

$\forall$ ring T we have a bijection

between points $Mor(R,T) \cong Mor(R',T)$

Satisfying: $\forall$ $f: T \to T'$ we have a commutative diagram

$$\begin{array}{ccc} Mor(R,T) & \cong & Mor(R',T) \\ \downarrow f\circ & & \downarrow f\circ \\ Mor(R,T') & \cong & Mor(R',T') \end{array}$$

Need: $R \cong R'$

use $T = R$:

obtain some $\varphi: R' \to R$

Similarly use $T' = R'$

to obtain $\psi: R \to R'$

$$\begin{array}{ccc} \underset{id_R}{Mor(R,R)} & \cong & \underset{\varphi}{Mor(R',R)} \\ \downarrow \psi\circ & & \downarrow \psi\circ \\ \underset{\psi}{Mor(R,R')} & \cong & \underset{id_{R'}}{Mor(R',R')} \end{array}$$

by $\downarrow \to$ id_R goes to $id_{R'}$

Therefore $\to\downarrow$ id_R should also go to $id_{R'}$

$\Rightarrow \psi \circ \varphi = id_{R'}$

Analogously $\varphi \circ \psi = id_R$ ∎

So the functor of points completely determines the ring.

Next question: Suppose we know R (secretly $R = \mathbb{Q}[x_1, \dots, x_n]/(f_1, \dots, f_m)$) we want to recover the set of solutions to $\begin{cases} f_1 = 0 \\ f_m = 0 \end{cases}$

Basic things about rings.

Defn: Noetherian rings

A ring R is called Noetherian if any of the following conditions hold:

Cond 1) Any increasing sequence of ideals $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \dots \subseteq R$ has to stop: $\exists N$: $\mathfrak{a}_N = \mathfrak{a}_{N+1} = \dots$

Cond 2) Any ideal $\mathfrak{a} \subseteq R$ is finitely generated, i.e. $\mathfrak{a} = (f_1, \dots, f_m)$ some $f_1, \dots, f_m \in R$.

Proof: 1) => 2) Pick $\mathfrak{a} \subseteq R$ suppose not f.g. Define a sequence $\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \dots$ of ideals by $\mathfrak{a}_0 = (0)$ $\mathfrak{a}_1 = (f_1)$ $f_1 \neq 0$ $f_1 \in \mathfrak{a}$
$\mathfrak{a}_2 = (f_1, f_2)$ $f_2 \in \mathfrak{a}$, $f_2 \notin \mathfrak{a}_1$, ... so on
$\mathfrak{a}_n = (f_1, f_2, \dots, f_n)$ $f_n \in \mathfrak{a}$, $f_n \notin \mathfrak{a}_{n-1}$
we obtain $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \dots$
this sequence does not stop $\times$.

2) => 1) Pick $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \dots$ consider $\bigcup_{n=1}^{\infty} \mathfrak{a}_n$. This is an ideal. So $\bigcup_{n=1}^{\infty} \mathfrak{a}_n = (f_1, \dots, f_m)$.
each f_i is in $\mathfrak{a}_{n_i}$. Let $N = \max(n_1, \dots, n_m)$ then $f_i \in \mathfrak{a}_N$. so $(f_1, \dots, f_m) \subset \mathfrak{a}_N \Rightarrow$
$\bigcup_{n=1}^{\infty} \mathfrak{a}_n = \mathfrak{a}_N \Rightarrow \mathfrak{a}_{N+1} = \mathfrak{a}_{N+2} = \dots = \mathfrak{a}_N$.

Main property 1) R Noetherian $\Rightarrow$ $R[X]$ is Noeth.
2) R Noetherian, $\mathfrak{a} \subset R$ ideal $\Rightarrow$ $R/\mathfrak{a}$ Noeth.

Proof: given $\mathfrak{a} \subset R[X]$

$c(x) = c_0 + c_1 X + \dots c_n X^n$ $\quad$ $(d_0 + d_1 X + \dots + d_m X^m = d(x)) \times X^{n-m}$
$n > m$

Idea: we have a sequence $d_0^{(1)} + \dots d_{m_1}^{(1)} X^{m_1} = d^{(1)}(x)$
$d_0^{(2)} + \dots d_{m_2}^{(2)} X^{m_2} = d^{(2)}(x)$
if we can reduce c_n modulo $d_{m_1}^{(1)}, d_{m_2}^{(2)}, \dots$
then you can reduce $c(x)$ modulo $d^{(i)}(x)$
and polynomials of degree $< n$.

Define ideals $\mathfrak{a}_n \subset R$ by
$\mathfrak{a}_n = \{ c_n \mid c_0 + \dots + c_n X^n \in \mathfrak{a} \}$.
$\mathfrak{a}_n$ is an ideal (clear)
Clearly $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \dots$. This sequence stops:
$\exists N$ $\mathfrak{a}_N = \mathfrak{a}_{N+1} \dots$.
Let $f_1^{(1)}, \dots f_{m_1}^{(1)}$ be generators of $\mathfrak{a}_1$,
$f_1^{(k)}, \dots f_{m_k}^{(k)}$ — || — $\mathfrak{a}_k$ $\quad k \leq N$.
Let $g_1^{(k)}, \dots g_{m_k}^{(k)} \in \mathfrak{a}$ so that
$g_i^{(k)} = f_i^{(k)} X^k + (\text{smaller degree terms})$
Claim: $\mathfrak{a}$ is generated by all these $g_i^{(k)}$
(by decreasing the degree) $\blacksquare$

Proof of 2) $\pi: R \to R/\mathfrak{a}$ Pick some ideal $\mathfrak{b} \subset R/\mathfrak{a}$, take $\pi^{-1}(\mathfrak{b}) \subset R$. This is an ideal, it is finitely generated by $f_1, \dots f_n$.
Since π is surjective $\pi(f_1), \dots, \pi(f_n)$ generate $\mathfrak{a}$.
Equivalently ideals in $R/\mathfrak{a}$ are in bijection with ideals in R containing $\mathfrak{a}$. (Using the Definition 1)

Corollary: Any finitely generated ring over a noetherian ring is noetherian.

Overview

ring

points corresponding to maximal ideals $\subset$ points with values in fields $\cong$ prime ideals.

Nullstellensatz

works well only over alg. closed fields.

More classical

more general

Usually don't need Nullstellensatz. More modern.

Fields

Prop R is a field $\iff$ $0 \neq 1$ and the only ideals are (0) and (1).

$\Updownarrow$

R has exactly 2 ideals.

Pf $\Leftarrow$ $x \in R$ $x \neq 0$

Let $\mathfrak{a} = (x)$

$\mathfrak{a} = (1) \Rightarrow$ $1 = xy$ (some $y \in R$)

$\Rightarrow x$ is invertible

$\Rightarrow R$ is a field.

$\Rightarrow$ clear

Let us understand points with coefficients in fields.

Fix R find $\{\varphi : R \to k \quad k \text{ field}\}$.

for such φ Consider $\varphi^{-1}(\{0\}) \subset R$. Claim $R/\varphi^{-1}(\{0\})$ is a domain

Pf

$xy = 0 \Rightarrow \varphi(xy) = 0$

$\varphi(x)\varphi(y) = 0 \Rightarrow \varphi(x)$ or $\varphi(y) = 0$.

domain:

$xy = 0 \Rightarrow x = 0$ or $y = 0$

Prop $R/\mathfrak{a}$ is a domain $\iff$ $\mathfrak{a}$ is a prime ideal.

Def $\mathfrak{a} \subset R$ is prime if

$xy \in \mathfrak{a} \Rightarrow x \in \mathfrak{a}$ or $y \in \mathfrak{a}$

Prop Fix R. ideals appearing as $\operatorname{Ker}\varphi$ for $\varphi : R \to k$, k field are precisely the prime ideals.

Pf $\Rightarrow$ clear

$\Leftarrow$ Suppose $\mathfrak{a} \subset R$ is prime.

we need to construct k.

Step 1 take $R/\mathfrak{a}$. This is a domain.

Construction Field of fractions:

R is a domain $\Rightarrow$ $F(R) = \left\{ \dfrac{x}{y} \;\middle|\; \begin{array}{l} x \in R \\ y \in R \setminus \{0\} \end{array} \right\} \Big/ \sim$

$\dfrac{x}{y} \sim \dfrac{x'}{y'}$ if $xy' = x'y$.

$F(R)$ is a field.

$R \to F(R)$ is given by

$x \mapsto \dfrac{x}{1}$ is injective

R is a domain $\Rightarrow$ $\dfrac{x}{y} \sim \dfrac{x'}{y'}$, $\dfrac{x'}{y'} \sim \dfrac{x''}{y''}$

$\Rightarrow xy' = x'y \quad x'y'' = y'x''$

need $xy'' = x''y$

$xy'' \cdot y' = x'yy'' = yy'x''$

$\Rightarrow (xy'' - yx'')y' = 0$, since $y' \neq 0$

we get $xy'' = yx''$.

So $\mathfrak{a} \subset R$ prime then $F(R/\mathfrak{a})$ is a field

then $\operatorname{Ker}\left(R \to R/\mathfrak{a} \to F(R/\mathfrak{a})\right) = \mathfrak{a}$.

R ring (prime ideal is assumed $\neq R$)

Def $\operatorname{Spec}(R) = \{p \mid p \subset R \text{ prime}\}$

For each p we had $R \to F(R/p)$ a points with values in a field.

Prop $\operatorname{Spec}(R) \neq \{\emptyset\}$ if $R \neq \{0\}$.

Defn Ideal $m \subset R$ is *maximal* if $m \neq R$, and there is no ideal $m \subsetneq a \subsetneq R$.

Prop m is maximal $\Leftrightarrow$ R/m is a field.

Prop maximal $\Rightarrow$ prime (because $m = \ker(R \to R/m)$)

Prop maximal ideals exist.

(Zorn lemma: Consider the set of ideals $a \subset R$ $(a \neq R)$.

Any chain has an upper bound because Suppose Λ is a linearly ordered set $\{a_\lambda\}_{\lambda \in \Lambda}$ is an increasing collection of ideals. Then $\bigcup_{\lambda \in \Lambda} a_\lambda$ is an ideal.

and $1 \notin \bigcup_{\lambda \in \Lambda} a_\lambda$, so it is an upper bound.

$\Rightarrow$ 1) maximal ideals exist

2) any ideal $a \subsetneq R$ is contained in a maximal ideal.

Corollary $\operatorname{Spec}(R) \neq \emptyset$.

Remark

$\varphi: R \to R'$ $\quad p \subset R'$ prime $\Rightarrow \varphi^{-1}(p)$ is prime

Pf $p = \ker(\psi: R' \to k) \Rightarrow$

$\varphi^{-1}(p) = \ker(\psi \circ \varphi)$ is prime.

But $m \subset R'$ maximal $\Rightarrow \varphi^{-1}(m)$ doesn't have to be maximal.

So for $f: R \to R'$ we can define $f^*: \operatorname{Spec}(R') \to \operatorname{Spec}(R)$ by $p \to f^{-1}(p)$.

Question For R Consider $\bigcap_{p \in \operatorname{Spec} R} p$ What is it?

$x \in \bigcap_{p \in \operatorname{Spec} R} p$

Prop $\bigcap_{p \in \operatorname{Spec} R} p = \{x \in R \mid x^n = 0 \text{ some } n\} =: Nil(R)$ "nil-radical"

Proof $x \in Nil(R) \Rightarrow x \in \ker \varphi$ $\forall \varphi: R \to k$, k field.

$\Rightarrow x \in \bigcap p$

($\Leftarrow$) Suppose $x \in \bigcap p$ suppose $x^n \neq 0$ $\forall n$.

Consider $\{a \mid a \subset R : \forall n \ x^n \notin a\} = S$

1) $S \neq \emptyset$. $(S \ni (0))$

2) Every chain has upper bound

$\{a_\lambda\}_{\lambda \in \Lambda} \to \bigcup a_\lambda \in S$.

by Zorn $\exists$ $a \in S$ maximal (as an element of S)

Let's prove a is prime.

$\alpha\beta \in a$ $\quad \alpha \notin a$ $\quad \underbrace{(a, \alpha)}_{\notin S} \subset R$

$x^n = \alpha c \mod a$

$\beta \notin a \Rightarrow$ $x^m = \beta c' \mod a$

$\Rightarrow x^{m+n} = \underbrace{\alpha\beta}_{=0} cc' \mod a$ $\cancel{\ }$

So a is prime $\quad x \notin a \Rightarrow x \notin \bigcap_{p \in \operatorname{Spec} R} p$

$\cancel{\ }$.

Note: x such that $x^n = 0$ is called nilpotent.

If R is such that $Nil(R) = (0)$ we say R is reduced.

More generally.

Suppose $R \supset a$, consider

$\operatorname{Spec}(R/a) = \{p \in \operatorname{Spec} R \mid p \supset a\}$

(Proof: we have a map $\pi^*: \operatorname{Spec}(R/a) \to \operatorname{Spec} R$

π^* is injective

any element in $\operatorname{image}(\pi^*)$ contains a.

Conversely if $p \supset a$ p prime then $(R/a)/(p/a) \cong R/p$ is a domain

$\Rightarrow p/a$ is prime.

Corollary $\bigcap_{\substack{p \in \operatorname{Spec}(R) \\ p \supset a}} = \operatorname{rad}(a) = \{x \in R \mid x^n \in a, \text{ some } n\}$

$\left(\bigcap / a = \bigcap p/a = nil(R/a) = \{x \mid x^n = 0_{R/a}\} \right)$

Correspondence between closed subsets and ideals.

$\{a \mid a \subset R \text{ ideal}\} \to$ Subsets of $\operatorname{Spec}(R)$

$a \to \operatorname{Spec}(R/a) \subset \operatorname{Spec}(R)$

$\bigcap_{p \in S} p \leftarrow S \subset \operatorname{Spec}(R)$

Geometrically

System of equations $\to$ set of solutions

functions which vanish on S. $\leftarrow$ subset of points S

---

1). Sets of the form $Z(a) = \operatorname{Spec}(R/a) = \{\text{prime ideals } p \supset a\}$ are called closed

2) we have ideals of the form $I(S) = \bigcap_{p \in S} p$ $S \subset \operatorname{Spec}(R)$.

Are precisely the radical ideals

Def $a \subset R$ is radical if $\operatorname{rad}(a) = a$

Proof $a = \operatorname{rad}(a) \Rightarrow a = \bigcap_{p \in Z(a)} p = I(Z(a))$

Conversely $a = \bigcap_{p \in S} p \Rightarrow \operatorname{rad}(a) = I(Z(a)) \subset a$

because $Z(a) \supset S$

$I(Z(a)) \subset \underbrace{I(S)}_{=a}$

$\Rightarrow \operatorname{rad}(a) = a$.

3) I, Z form a bijection between radical ideals and closed sets.

Zariski topology.

Geometry R ring $\qquad$ $Spec(R)$

points are prime ideals p, come with maps

$R \to F(R/p)$

$f \in R$ $\to$ image in $F(R/p)$ for all p.

This is like evaluating f at p.

so values of f are in different fields for different points.

Let's introduce a topology on $Spec(R)$ by declaring closed sets the sets $Z(a)$ $a \subset R$.

Axioms: 1) $\emptyset$, $Spec(R)$ are closed ($\emptyset = Z(1)$, $Spec(R) = Z(0)$)

2) arbitrary intersections:

$$\bigcap_{\lambda \in \Lambda} Z(a_\lambda) = Z\left(\sum a_\lambda\right)$$

ideal generated by all a_λ.

3) finite unions.

$Z(a) \cup Z(b)$ $\qquad$ $\left.\begin{matrix} Z(ab) \\ \text{or} \\ Z(a \cap b) \end{matrix}\right\}$ both work.

Discussion

ab = ideal generated by fg $f \in a$, $g \in b$.

$ab \subset a \cap b \subset a$
$\subset b$

$Z(a) \subset$
$Z(b) \subset$ $Z(a \cap b) \subset Z(ab)$

Let $p \in Z(ab)$ $\qquad$ $\varphi: R \to k$
$p = \ker \varphi$.

$ab \subset p$.

$fg \subset p$ $\quad \forall f \in a$ $g \in b$.

suppose $a \not\subset p$ then $\exists f \in a \setminus p$

$\forall g \in b$ $\quad fg \in p \Rightarrow g \in p$

$\Rightarrow b \subset p$.

$\Rightarrow$ $p \in Z(a) \cup Z(b)$.

$\Rightarrow$ $Z(ab) = Z(a) \cup Z(b) = Z(a \cap b)$.

Cor $\quad rad(a \cap b) = rad(ab)$.

Cor $\quad$ We have a well-defined topology called Zariski topology.

For Noetherian rings R any closed set is $Z(f_1, .., f_m)$ $\quad f_i \in R$

$S = \{x \mid f_i(x) = 0 \ \forall i\}$

complement is $\{x \mid f_i(x) \neq 0 \text{ some } i\}$.

Open sets look like $\bigcup U_{f_i}$, where

$U_{f_i} = \{x \mid f_i(x) \neq 0\}$.

Terminology $\Rightarrow$ Open sets U_f form a basis of topology

called affine open sets.

Because

Spaces of the form $Spec\, R$ are called affine spaces.

It turns out U_f is of this form:

$U_f = \{p \in Spec\, R \mid f \notin p\}$.

Consider a ring $R[x]/(fx-1) = R_f$

clearly maps $R_f \to k$ are in bijection with maps $R \to k$ s.t. f goes to $\neq 0$.

$R \to R_f$ induces $Spec(R_f) \to Spec(R)$

this is inclusion with image U_f.

Examples

$R = \mathbb{Z}$ elements n

prime ideals $\supset$ maximal ideals

Any ideal looks like (n) quotient is $\mathbb{Z}/n\mathbb{Z}$

is a domain if n is prime or $n=0$.

is a field if n is prime

fields n prime $n=p$ $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ field

$n=0$ $\mathbb{Z} \to \mathbb{Q}$

$\operatorname{Spec} \mathbb{Z} = \{\text{prime numbers}\} \cup \{\infty\}$

$n \in \mathbb{Z}$ "function" at p it is $n \bmod p$

at ∞ it is $n \in \mathbb{Q}$.

$R =$ field not interesting $\operatorname{Spec} R =$ point

$R = k[X]$.

ideals are of the form (f) $f \in R$.

prime ideals : monic irreducible $f \in R$, or 0.

k alg. closed $\iff$ irreducible polynomials are $X - \alpha$ $(\alpha \in k)$.

maximal ideals : $f \neq 0$ irreducible.

fields: f irreducible $k[X]/f$ is a field.

if $k = \bar{k}$ $\Rightarrow$ maximal ideals correspond to points of k.

$(0) \rightarrow F(k[X]) = k(X)$ rational functions.

f polynomial $\rightarrow$ values are $f(x)$ for all x in all extensions of k.

"at ∞" f itself $f \in k(X)$.