Pick $f_1, \dots, f_r \in \mathbb{Z}[X_1, \dots, X_n]$

If $R$ is a ring, set

$$M(R) := \{(x_1, \dots, x_n) \in R^n \mid f_i(x_1, \dots, x_n) = 0 \quad \forall i = 1, \dots, r\}$$

Obvious: If $M(\mathbb{Z}/m) = \emptyset$ for some $m \geq 2$

$\Rightarrow M(\mathbb{Z}) = \emptyset$

$(\exists M(\mathbb{Z}) \to M(\mathbb{Z}/m))$

$(M(R \times S) = M(R) \times M(S))$

What about the converse?

Assume $M(\mathbb{Z}/m) \neq \emptyset \quad \forall m \geq 2$.

Equiv: $M(\mathbb{Z}/p^i) \neq \emptyset \quad \forall$ primes $p$, $i \geq 1$

(CRT)

Is than $M(\mathbb{Z}) \neq \emptyset$ ?

Answer: No, e.g. $f(x,y) = x^2 + 23y^2 - 41$

(later, $M(\mathbb{Z}) = \emptyset$ here)

Note: $M(\mathbb{Z}) \to \varprojlim_i M(\mathbb{Z}/p^i)$ $\forall$ primes $p$ (in gen.)

inverse limit for trans. morph.

$\ldots \to M(\mathbb{Z}/p^{i+1}) \to M(\mathbb{Z}/p^i) \to \ldots$

Def: Let $(\mathbb{N}, \leq) = (\ \ldots \bullet \to \bullet \to \bullet\ )$

$\ldots \to M_{i+1} \xrightarrow{g_{i+1}} M_i \to \ldots \xrightarrow{g_1} M_0$

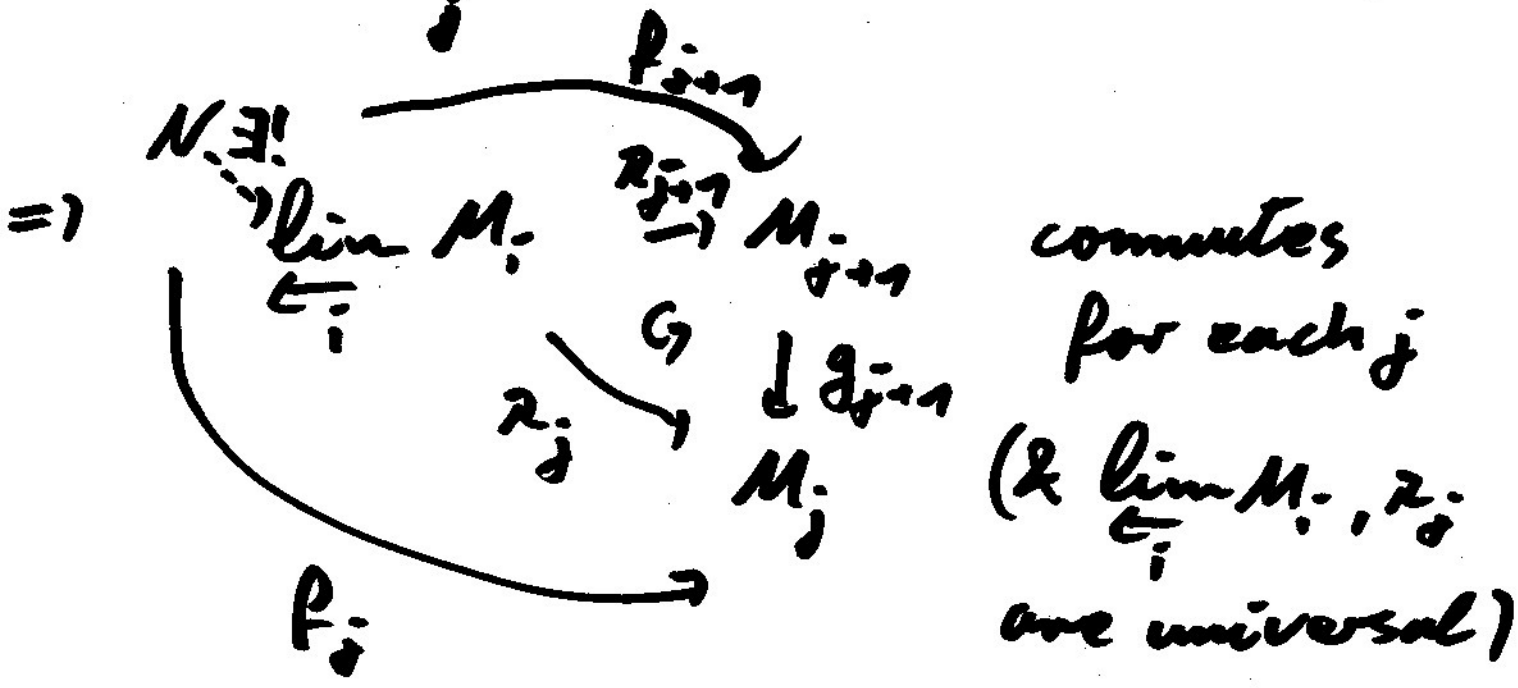
be ($\mathbb{N}$-indexed) inverse system of sets (rings, modules, ...)

Set $\varprojlim_i M_i := \{ (x_{n_i})_i \in \prod_i M_i \mid$

set (ring, ...) $g_{i+1}(m_{i+1}) = m_i \ \forall i \}$

"compatible system of elements"
↖
w.r.t. $g_i$

Let $\pi_j : \varprojlim_i M_i \to M_j$, $(m_i)_i \mapsto m_j$




commutes for each $j$

(& $\varprojlim_i M_i, \pi_j$ are universal)

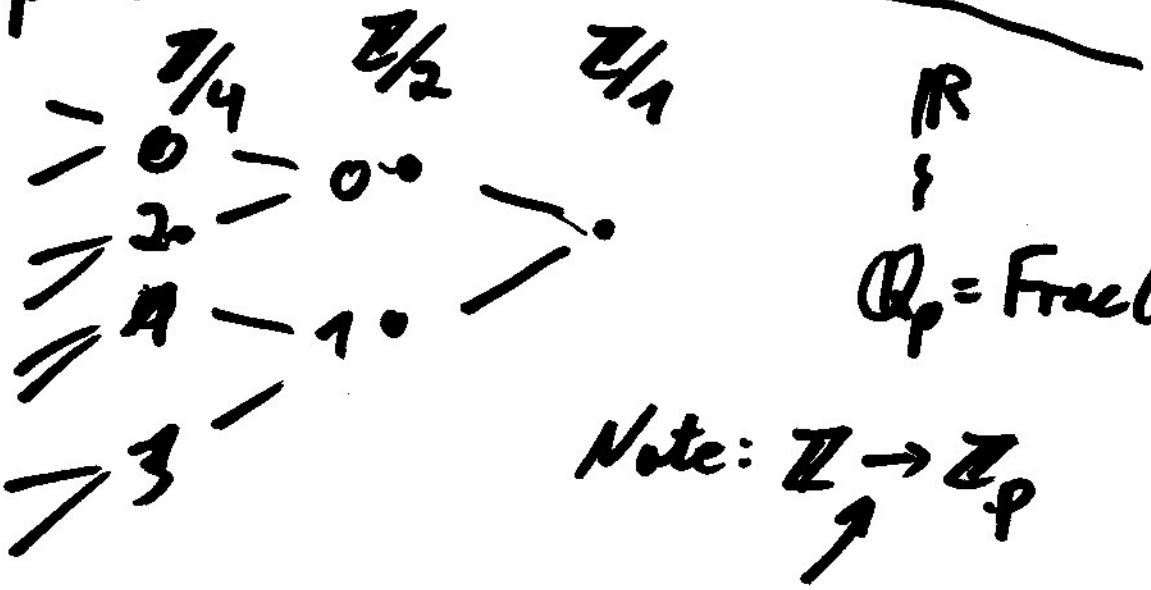
Def: Let $p$ be a prime

⚠ $\mathbb{Z}_p := \varprojlim_i \mathbb{Z}/p^i$ ring of

$p$-adic integers

↖ via componentwise mult.

Ex: $p=2$




$\mathbb{Q}_p = \mathrm{Frac}(\mathbb{Z}_p)$

Note: $\mathbb{Z} \to \mathbb{Z}_p$ injective

$(\ker = \bigcap_i p^i\mathbb{Z} = \{0\}$

Clear: $M(\mathbb{Z}_p) = M \varprojlim_i M(\mathbb{Z}/p^i)$

Claim: $M(\mathbb{Z}/p^i) \neq \emptyset \ \forall i \iff M(\mathbb{Z}_p) \neq \emptyset$

In other words, if solutions exist modulo any $p^i$, then there exists a compatible system of solutions

La: Assume $\to M_{i+1} \xrightarrow{g_{i+1}} M_i \to \dots \to M_0$ is an inverse system of sets

1) If each $g_i$ is surj., then

$$\pi_j : \varprojlim_i M_i \to M_j \text{ is surj.}$$

for each $j$.

2) If all $M_i$ are finite & $\varprojlim_i M_i = \emptyset$, then $M_i = \emptyset$ for some $i$

Proof: 1) induction

2) For each $j$, set $N_j = \bigcap_{i \geq j} \operatorname{Im}(M_i \xrightarrow{g_{ij}} M_j)$ (comp. of $g_i$)

$\Rightarrow g_j(N_j) = N_j \subseteq N_{j-1}$

In fact, $g_j(N_j) = N_{j-1}$

(as $N_{j-1} = \operatorname{Im}(M_i \to M_{j-1})$ for $i \gg 0$)

$M_j$ finite

If $\varprojlim_i M_i = \emptyset \Rightarrow \varprojlim_i N_i = \emptyset$

(as $\varprojlim_i N_i \subseteq \varprojlim_i M_i$)

$\Rightarrow N_i = \emptyset \ \forall i \Rightarrow M_i = 0, i >> 0$.

1)

We will see: arithmetic of $\mathbb{Z}_p$ is much simpler than for $\mathbb{Z}$ (or $\mathbb{Z}_{(p)}$)

Reason: $\mathbb{Z}_p$ is a <u>complete</u> topological ring (arithmetic of $\mathbb{R}$ is much simpler than the arithmetic of $\mathbb{Q}$)

Abstract situation:

$R$ any ring, $I \subsetneq R$ any ideal

(In our sit., $R = \mathbb{Z}$, $I = (p)$, $p$ prime)

Def: The $I$-adic topology on $R$ is top. gen. by $r + I^n$ with $r \in R$, $n \geq 1$

Then $R$ is a top. ring for its $I$-adic topology (i.e. add. / mult. are cont.)

(e.g. $(r+I^n)\cdot(s+I^m) \subseteq r\cdot s + I^{n+m}$

$\Rightarrow$ mult. cont.

$m(r+I^n \times s+I^m)$ $r+I^n + s+I^m \subseteq r+s+I^{\min(n,m)}$ )

Fund. sys. of opens of $0 = \{I^n\}_{n \geq 1}$

$m: R \times R \to R$

$a: R \times R \to R$

**Def:** $\hat{R} := R_I := \varprojlim_n R/I^n \subseteq \prod_n R/I^n$

(trs. maps $\simeq$ $R/I^{n+1} \twoheadrightarrow R/I^n$)

**Then:** $\hat{R}$ is a top. ring for inverse limit topology with each $R/I^n$ discrete

**Expl.**

$$\begin{array}{ccc} r+I^n & \to & \bar{r} \\ \| & & \| \\ \hat{r} & \to & R/I^n \end{array}$$

let $J_n := \ker(\hat{R} \twoheadrightarrow R/I^n)$ $\nwarrow \nearrow$ $R$

$\Rightarrow (J_n)_n$ fund. syst. of nbhds of $0$ in $\hat{R}$

Have can. cont. morph.

$$\begin{array}{ccc} R & \to & \hat{R} \\ \downarrow & & \downarrow \\ I\text{-adic} & & \text{inverse limit top.} \end{array} \qquad \begin{array}{l} (\text{as } I^n \to J_n) \\ \ker(R \to \hat{R}) \\ \| \\ \bigcap_{n \geq 1} I^n \end{array}$$

**Def:** Let $S$ be a top. ring

1) A sequence $(s_i)_{i\in\mathbb{N}}$ is Cauchy if for all nbhds $U$ of $0$, there exists $i_0 \in \mathbb{N}$, s.t. $s_i - s_j \in U \ \forall i,j \geq i_0$

2) $S$ complete if each Cauchy sequence has a unique limit

**Prop:** 1) $\hat{R}$ is complete for its inverse limit top.

2) If $I$ is f.g., then $J_n = \ker(\hat{R} \to R/I^n)$ $= I^n \cdot \hat{R}$ $\forall n$, i.e. inverse limit on $\hat{R}$ is the $I\cdot\hat{R}$-adic top.

**Proof:** 1) Each $R/I^n$ is discrete

$\Rightarrow$ it is complete

$\Rightarrow$ can construct limit componentwise

2) Stacks Project, Tag 05GG

We only prove relevant case:

$I = (r)$, $r \in R$ non-zero divisor

In this case, for $m \geq n$

$$0 \to R/I^{m-n} \xrightarrow{\cdot r^n} R/I^m \to R/I^n \to 0$$

Let $a \in J_n$, i.e. $a = (\ldots, a_{m+1}, a_n = 0, a_{n-1}, \ldots)$ with $a_{m+1} \in R/I^{m+1}$, $a_n \in R/I^n$

$\Rightarrow \forall m \geq n$ ex. unique

$$b_m \in R/I^{m-n} \text{ s.t. } r^n \cdot b_m = a_m$$

Uniqueness implies

$$b_{m+1} \equiv b_m \bmod I^{m-n}$$

$\Rightarrow b := (\ldots, b_{m+1}, b_m) \in \hat{R}$

and $r^n \cdot b = a \Rightarrow I^n \cdot \hat{R} = J_n$

Note: If $I=(r)$, $r \in R$ non-zero divisor

$\Rightarrow 0 \to \hat{R} \xrightarrow{r} \hat{R} \to R/I^n \to 0$ exact $\forall n$

(pass use $\varprojlim_m R/I^{m-n} \cong \varprojlim_m R/I^m$)

$\Rightarrow$ $r$ non-zero div. in $\hat{R}$

$\varprojlim : Fun(\mathbb{N}, \mathcal{C}) \to \mathcal{C}$

$\Delta(c)(n)=c$ ($\Delta$ left adjoint to $\varprojlim$)

const. diag.

La: Assume $R$ $I$-adically complete ($R \to \hat{R}_I$), e.g. $I$ nilpotent

~~$R \hat{\otimes} S$ F.g.~~

or $R = \hat{\mathbb{Z}}_J$, Smirnof, $J \subseteq S$ f.g.
& $I = J \cdot R$

(e.g. $\mathbb{Z}_p$)

$\Rightarrow$ $R^\times = \{ r \in R \mid \bar{r} \in (R/I)^\times \}$

Proof: „$\subseteq$"

„$\supseteq$" Can construct $r^{-1}$
componentwise in $R = \hat{R} = \varprojlim R/I^n$
(by uniqueness of inverses)

$\Rightarrow$ Wlog $I$ nilpotent
(i.e. $I^n = 0$ for some $n \gg 0$)

Pick $s \in R$, s.t. $s \cdot r - 1 \in I$

$\Rightarrow$ $\frac{1}{r} = \frac{s}{1-(1-s\cdot r)} = s \cdot \underbrace{\sum_{i=0}^{\infty} (1-sr)^i}_{\text{makes sense as } I \text{ nilp.}} \in R$

$r = (\ \ldots, r_2, r_1, r_0\ )$

$\uparrow \quad \uparrow \quad \uparrow$

$R/I^2 \quad R/I \quad R/R$

STP

If $r_1 \in (R/I)^\times \Rightarrow r_n \in (R/I^n)^\times \ \forall n$

Now, replace $R$ by $R/I^n$ □

In part,

If $p$ prime, $\Rightarrow$ each $n \in \mathbb{Z}$ with $(n,p)=1$ is invertible in $\mathbb{Z}_p$

~~$(n \in (\mathbb{Z}/p\mathbb{Z})^\times)$~~

Back to: $f(x,y) = x^2 + 3y^2 - 47$

Get $f(\frac{1}{3}, \frac{4}{3}) = f(\frac{9}{4}, \frac{5}{4}) = 0$

$\Rightarrow f(x,y)$ solvable in $\mathbb{Z}_p$ for each prime $p$

La: $R$ Ring, $I=(r)$, $r \in R$ non-zero div.

1) $r$ non-zero div. in $\hat{R}$

2) If $R/I$ int. dom. $\Rightarrow$ $\hat{R}$ int. domain

3) If $S \subseteq R$ is a system of repr. for $R/I$, then $S \xrightarrow{1:1} R/I$

each $a \in \hat{R}$ can uniquely be written as

$$a = \sum_{i=0}^{\infty} s_i \cdot r^i \text{ with } s_i \in S$$

& conversely, bij. of sets

$$S^{\mathbb{N}} \xrightarrow{\sim} \hat{R}$$

$$(s_i)_{i\geq 0} \mapsto \sum_{i=0}^{\infty} s_i r^i$$

E.g: $\mathbb{Z}_p = \{ \sum_{i=0}^{\infty} s_i \cdot p^i \mid s_i \in \{0, \dots, p-1\} \}$

"power series in $p$"

2) $\mathbb{Z}_p$ int. dom.

$$\mathbb{Q}_p = \mathrm{Frac}(\mathbb{Z}_p) = \mathbb{Z}_p[\tfrac{1}{p}]$$

$$= \left\{ \sum_{i \gg -\infty}^{\infty} s_i \cdot p^i \mid s_i \in \{0, \dots, p-1\} \right\}$$

$A \xrightarrow{f} B$ , $a \in A$, $b \in B$

$a \cdot b = f(a) \cdot b$ $f_i \in$ ~~$\mathbb{Z}[x_1 \dots$~~

$\mathcal{M}(R) = \{ \dots$ $\mid \underline{f_i(x_1, \dots, x_n) = 0}$

~~$A \to$~~ $R$

$\mathrm{Spec}\left(\mathbb{Z}[x_1, \dots, x_n] / (f_1, \dots, f_r)\right)$

$\mathbb{Z}_{(p)}$ $\mathbb{Z}_{(p)}$ $= \mathbb{Z}_p$

$\downarrow$

$\mathbb{Z}/p^k$