





## First definition of completion

Let  $M$  be an  $R$ -module and consider a filtration

$$\dots \subseteq M_i \subseteq \dots \subseteq M_1 \subseteq M_0 = M$$

filtration = chain of submodules.  
pseudo-

We define a distance function on  $M$ .

Let  $0 < \mu < 1$ . We put, for  $a, b \in M$

$$d(a, b) = \begin{cases} \mu^i & \text{if } a-b \in M_i - M_{i+1} \\ 0 & \text{if } a-b \in \bigcap_{i \geq 0} M_i \end{cases}$$

Proof of ultrametric  $\leq$

If  $a-b \in M_i - M_{i+1}$ ,  $b-c \in M_j - M_{j+1}$

with  $\mu^i \geq \mu^j$  then  $i \leq j$  so

$b-c \in M_i$ ,  $a-c = a-b + b-c \in M_i$

so  $d(a, c) \leq \mu^i$ .  $\square$

Proposition For all  $a, b$  in  $M$  we have

$$d(a, b) \geq 0, \quad d(a, b) = d(b, a)$$

$$d(a, c) \leq \max(d(a, b), d(b, c)) \quad \text{the ultrametric inequality}$$
$$\leq d(a, b) + d(b, c)$$

$$d(a, b) = 0 \Leftrightarrow a-b \in \bigcap_{i \geq 0} M_i$$

Definition (Krull topology) We put a topology on  $M$  with basic open sets the balls

$$B_\epsilon(a), \quad a \in M, \quad \epsilon > 0.$$

Open sets = unions of these balls.

Proposition / Exercise. This topology is Hausdorff if and only if  $\bigcap M_i = \{0\}$

The following is a collection of basic open sets:  $a + M_i$ ,  $i = 0, 1, 2, \dots$   $a \in M$ .  
"  $B_{\mu^{i-1}}(a)$

$M$  is a topological group under  $+$

## Representing elements of $M$ as sequences

Take a set of coset representatives

$x_{i,j}$  for  $M_{i+1}$  in  $M_i$ ,  $j$  varies

Each  $m \in M$  determines a list of these coset reps: Consider  $i=0$

$$M_0 \supseteq M_1 \dots m \equiv x_{0,j_0} \pmod{M_1}$$

$$m - x_{0,j_0} \equiv x_{1,j_1} \pmod{M_2}$$

$$m - x_{0,j_0} - x_{1,j_1} \equiv x_{2,j_2} \pmod{M_3}$$

We get a list  $(\dots, x_{2,j_2}, x_{1,j_1}, x_{0,j_0})$

We could call the elements of the list the 'digits of  $m$ '.

Example: The powers of the ideal  $(p)$  in  $\mathbb{Z}$ .

$M = \mathbb{Z}$ ,  $M_i = (p^i)$  Coset reps

$$\{x_{0,j}\} = \{0, \dots, p-1\}$$

$$\{x_{i,j}\} = \{0p^i, 1p^i, \dots, (p-1)p^i\}$$

Write  $m \in \mathbb{Z}$  as

$$m = a_i p^i + a_{i-1} p^{i-1} + \dots + a_1 p + a_0$$

$a_j \in \{0, \dots, p-1\}$ . List  $(0, a_i p^i, \dots, a_1 p, a_0)$

Proposition.

Elements  $m, m'$  in  $M$  produce the same list of coset representatives if and only if  $m - m' \in \bigcap M_i$

Thus  $\bigcap M_i = 0$  implies elements of  $M$  are determined by these lists of elements.

# Pre-class Warm-up!!

Given Cauchy sequences  $(a_i)$  and  $(b_i)$  in a metric space, in defining the completion of the space, which (if any) of the following means that the Cauchy sequences are equivalent?

- A There exists a point  $x$  in the space so that  $a_i \rightarrow x$  and  $b_i \rightarrow x$  as  $i \rightarrow \infty$ .
- B Given  $\epsilon > 0 \exists N$  so that  $i > N$  implies  $d(a_i, b_i) < \epsilon$
- C Given  $\epsilon > 0 \exists N$  so that  $i, j > N$  implies  $d(a_i, b_j) < \epsilon$
- D Given  $N, \exists \epsilon > 0$  so that  $i > N \Rightarrow d(a_i, b_i) < \epsilon$
- E None of the above.

Example:  $(3, 3.1, 3.14, 3.141, 3.1415, \dots)$   
In  $\mathbb{Q}$  is a Cauchy sequence with no limit.

Defn. A sequence  $(a_i)$  is Cauchy  
 $\Leftrightarrow \forall \epsilon > 0 \exists N$  so that  $i, j > N \Rightarrow d(a_i, a_j) < \epsilon$

Sequences  $(a_i)$   $(b_i)$  are equivalent  
 $\Leftrightarrow B$  or  $C$  opposite.

Defn. The completion of the metric space  $M$  is the set of equivalence classes of Cauchy sequences.

We have an embedding (metric, not pseudometric)  $M \rightarrow \hat{M}$

$m \mapsto (m, m, m, m, \dots)$   
 $\hat{M}$  acquires a metric  $\hat{d}$  extending  $d$ .  
 $M$  is complete.

2nd question: For what reason did we ever learn about Cauchy sequences in the first place?

Proposition.

A sequence  $(m_k)$  of elements of  $M$  is a Cauchy sequence if and only if

$$\forall \epsilon > 0 \exists N \text{ so that } i, j > N$$

$$\Rightarrow d(m_i, m_j) < \epsilon$$

In digit notation this means

$$\forall \epsilon > 0 \exists N, i, j > N \Rightarrow$$

first  $\frac{1}{\epsilon}$  digits of  $m_i, m_j$  are the same.

Proposition

A Cauchy sequence in  $M$  determines a single list of digits that coincides with arbitrarily long initial segments of the digits of terms in the sequence.

Two Cauchy sequences are equivalent if and only if they produce the same sequence of digits.

$$d(m, m') < \mu^i \Leftrightarrow \text{the first } i \text{ digits of } m, m' \text{ are the same.}$$

Definition. The completion  $\hat{M}$  of  $M$  (with respect to the filtration) is the set of equivalence classes of Cauchy sequences in  $M$ .

Usual situation. We take an ideal  $M \subseteq R$   
 $M = R, M_i = M^i$

$$R = \mathbb{Z} = M, M_i = (2^i)$$

Question. Let  $M_i = (2^i) \subseteq \mathbb{Z}$  and let  $\mu = 1/2$ .  
What is  $d(48, 96)$ ?

$$96 - 48 = 48 \in (2^4) - (2^5) \text{ so } i = 4$$

$$d(48, 96) = \left(\frac{1}{2}\right)^4 = \frac{1}{16}$$

Proposition. The completion is

- an  $R$ -module,
- a metric space
- the same as the completion of  $M / \bigcap_{i \geq 0} M_i$
- if  $M = R$  and the  $M_i$  are ideals, then it is a ring.

Proof a. We can add Cauchy sequences, adding an equivalent sequence produces equivalent sequences

b. done

c. If  $m_i \in \bigcap_{i \geq 0} M_i$  then

$$a_1 + m_1, a_2 + m_2, \dots$$

is equivalent to  $(a_i)$ .

Every sequence  $(a'_i)$  with  $a'_i$  in the same coset of  $\bigcap M_i$  as  $a_i$  is in the same equivalence class as  $(a_i)$

the set of sequences  
 $(\dots, x_{2,j_2}, x_{1,j_1}, x_{0,j_0})$   
with  $x_{i,j_i} \in$  set reps of  $M_{i+1}$  in  $M_i$

because every equiv. class of Cauchy sequences produces such a list of set reps and is determined by this list.

Given such a list we construct a Cauchy sequence

$$x_{0,j_0}, x_{0,j_0} + x_{1,j_1}, x_{0,j_0} + x_{1,j_1} + x_{2,j_2}, \dots$$

Question: Is it obvious that the completion  $\hat{M}$  is an  $R$ -module?

A Yes, it is obvious.

B No, it is not obvious.



Question.

Is there any reason in normal high-school arithmetic that we work with the real numbers (rather than the algebraic numbers, for instance).

Is it anything more than notational convenience?

A Yes

B No

# Pre-class Warm-up!!

For each prime  $p$  we have constructed the  $p$ -adic integers.

Are the  $p$ -adic integers

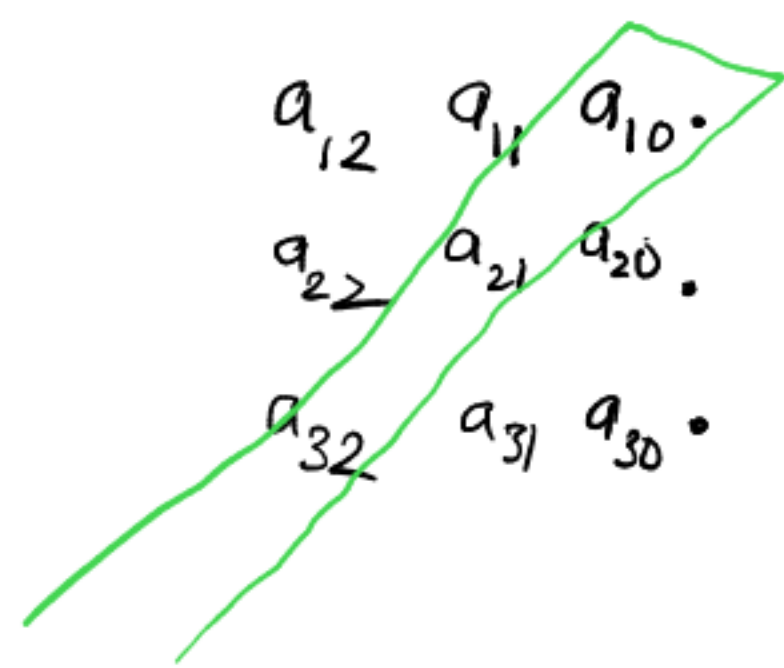
countable?

✓

$p$ -adic integers are lists

$\dots a_2 a_1 a_0 \bullet$

If we could enumerate such lists, make a table



Get a list different from the diagonal list in each place.

This expansion is not in the enumeration.

Notation and example. If  $\mathcal{M}$  is an ideal of  $R$ ,  $M$  is an  $R$ -module we get a filtration

$$\dots \subseteq \mathcal{M}^2 M \subseteq \mathcal{M} M \subseteq M$$

The limit is denoted  $\hat{M}_{\mathcal{M}} = \hat{M}_{\mathcal{M}}$ .  
In particular  $\hat{R}_{\mathcal{M}}$  or  $\hat{R}_{\mathcal{M}}$  is the completion of  $R$  at  $\mathcal{M}$ .

$$R[\hat{t}]_{\mathcal{M}} =: R[[t]] = \left\{ \sum_{i \geq 0} a_i t^i \mid a_i \in R \right\}$$

Get this description by taking coset reps  $a t^i$ ,  $a \in R$  for  $(t)^{i+1}$  in  $(t)^i$ .

Some more properties we have already seen:

Proposition

a. There is a homomorphism  $M \rightarrow \hat{M}$   
with kernel  $m \mapsto (m, m, m, \dots)$

b. The distance function on  $M_{\lambda}$  extends to a distance function on  $\hat{M}$  and  $\hat{M}$  is complete.

Proposition. Let  $\mathcal{M}$  be an ideal of  $R$ . Then the ideal  $(\mathcal{M})$  of  $\hat{R}_{\mathcal{M}}$  generated by  $\mathcal{M}$  has

$$\hat{R}_{\mathcal{M}} / (\mathcal{M}) \cong R / \mathcal{M},$$

$$\text{and } (\mathcal{M}) \cap R = \mathcal{M}$$

$$\text{Example: } \hat{\mathbb{Z}}_{(p)} / (p) \cong \mathbb{Z} / p\mathbb{Z}$$

Proof Elements of  $\mathcal{M}$  are represented by lists of coset reps  $(x_1, x_2, \dots, 0)$ .  
On completing,  $\mathcal{M}$  completes to all lists  $(\dots, \dots, \dots, 0)$ . This is the ideal of  $\hat{R}_{\mathcal{M}}$  generated by  $\mathcal{M}$ .

The lists  $(0, 0, \dots, 0, a)$ ,  $a$  is a coset rep for  $\mathcal{M}$  in  $R$  are coset reps for  $(\mathcal{M})$  in  $\hat{R}_{\mathcal{M}}$ .

This means  $R / \mathcal{M} \cong \hat{R}_{\mathcal{M}} / (\mathcal{M})$   
are in bijection.  $(\mathcal{M}) \cap R = \mathcal{M}$   
= lists of elements of  $R$  belonging to  $\mathcal{M}$ .  
 $R / \mathcal{M} \rightarrow \hat{R}_{\mathcal{M}} / (\mathcal{M})$  is an isomorphism.

## Categorical approach

Definition.

A diagram of  $R$ -modules is a functor

$F: \mathcal{C} \rightarrow R\text{-mod}$ , where  $\mathcal{C}$  is some category

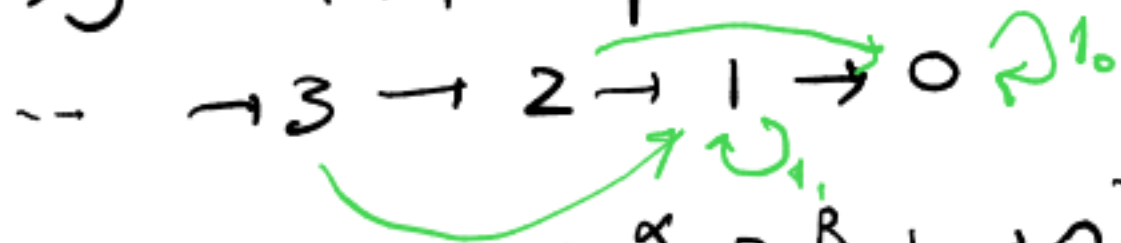
This is the same as a representation of  $\mathcal{C}$  over  $R$ .

Let  $\mathcal{C}$  be the category

with objects  $\{0, 1, 2, \dots\} = \mathbb{N}$

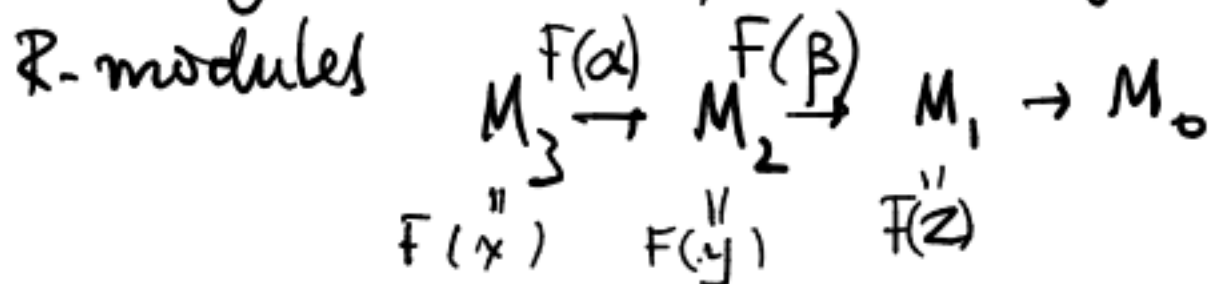
and a unique morphism  $i \rightarrow j$  whenever

$i \geq j$ . Picture of  $\mathcal{C}$ :

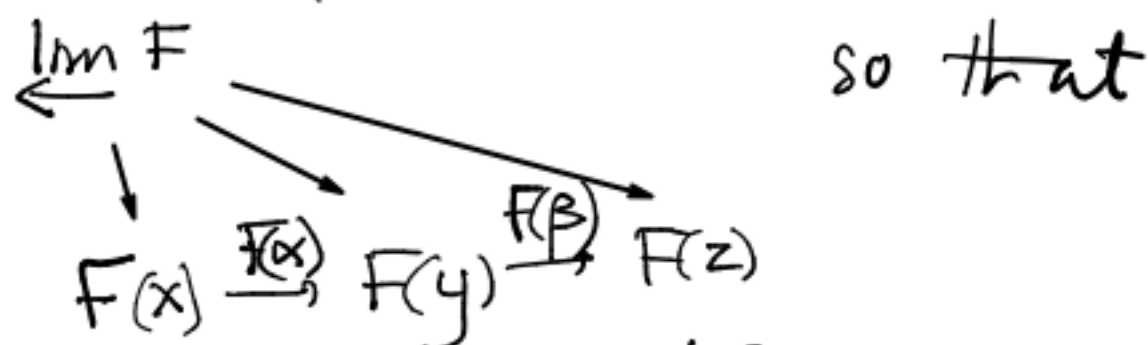


Free (quiver  $\dots \rightarrow 3 \xrightarrow{\alpha} 2 \xrightarrow{\beta} 1 \rightarrow 0$ ).

A diagram with shape  $\mathcal{C}$  is diagram of



The limit, or inverse limit of the diagram is a diagram of  $R$ -modules



- (1) All triangles commute
- (2) Given another such picture with  $N$  instead of  $\lim F$ ,  $\exists$  unique  $R$ -module hom  $N \rightarrow \lim F$  so that everything commutes.



Example. The pullback, the product.

Given  $\mathcal{C} = \bullet \rightarrow \bullet \leftarrow \bullet$  a diagram is a picture of  $R$ -modules.

The pullback is a module

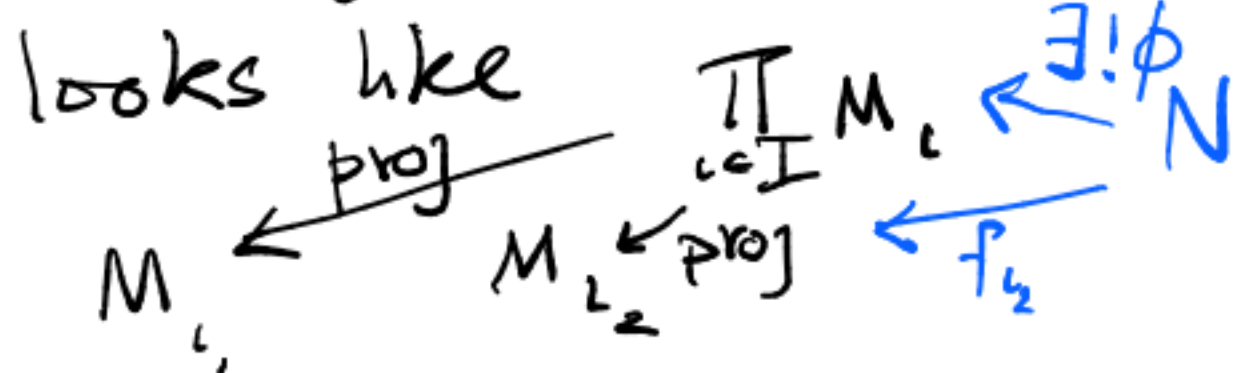
$P$  with morphisms as shown, so that (2) holds. The pullback is a limit.

The colimit, or direct limit of the diagram is similar, with arrows in the opposite direction.

The product of modules  $M_i, i \in I$ .

Take a category  $\mathcal{C}$  where the objects are the  $i$  in  $I$ , the only morphisms are identities.

A diagram  $F: \mathcal{C} \rightarrow R\text{-mod}$



Their product is the inverse limit of this diagram.

$$\prod M_i = (a_i) \quad a_i \in M_i.$$

$$\phi(n) = (f_i(n))$$

# Pre-class Warm-up!!!

Did we define what it means for a ring to be complete with respect to a certain ideal?

A Yes

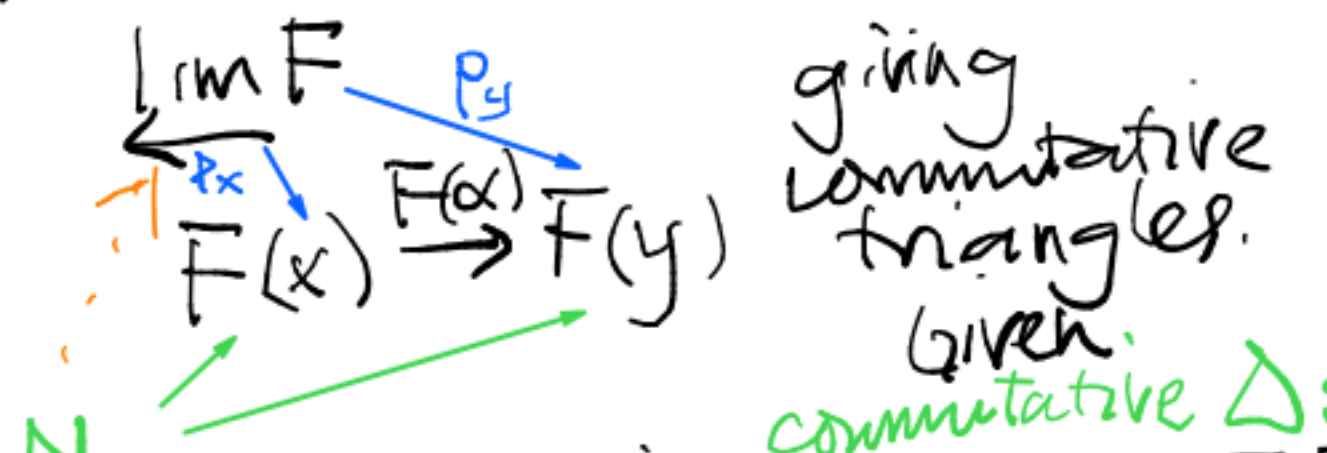
B No

Proposition. Limits of R-modules always exist and are unique.

Proof. Suppose we have a diagram  $F: \mathcal{C} \rightarrow R\text{-mod}$ . We construct

$$\lim F = \left\{ (a_x) \in \prod_{x \in \text{Ob}(\mathcal{C})} F(x) \mid \begin{array}{l} a_x \in F(x), \\ \forall \alpha: x \rightarrow y \text{ in } \mathcal{C} \\ F(\alpha)(a_x) = a_y \end{array} \right\}$$

The projections  $\prod F(x) \xrightarrow{p_x} F(x)$  restrict to maps



$\exists$  a unique homom.  $N \rightarrow \prod F(x)$  whose image lies in  $\lim F$

Corollary. Given a filtration of a module  $M$

$$\dots \subseteq M_2 \subseteq M_1 \subseteq M_0 = M$$

the completion of  $M$  is the same thing as the inverse limit of the diagram

$$\dots \rightarrow M/M_2 \rightarrow M/M_1 \rightarrow M/M_0 = 0$$

Proof. Each equivalence class of Cauchy sequences corresponds to a list of coset representatives  $\{ \dots, a_2, a_1, a_0 \}$  in  $M_i$ .

Define  $\hat{M} \rightarrow \lim F$   
 $(\dots, a_2, a_1, a_0) \rightarrow (a_{i-1} + a_{i+1} + \dots + a_0 + M_{i+1})_i$

$$a_{i-1} + \dots + a_0 + M_{i+1} \in M/M_i$$

The maps  $M/M_i \rightarrow M/M_{i-1}$  remove the top term in the partial sum. We get an isomorphism.  $\Delta$  comm

Question: How comprehensible  
was that

A I got it !! 😊

B

C Maybe

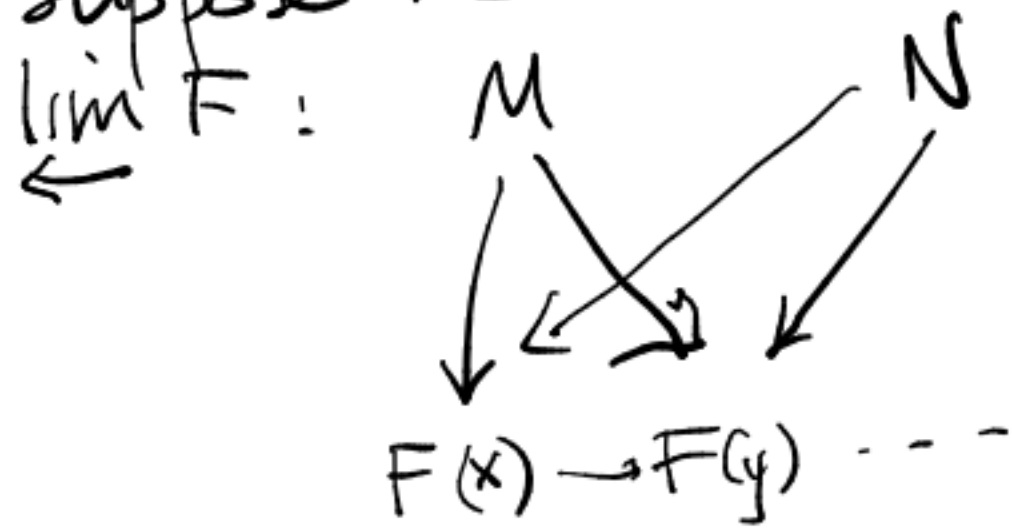
D

E I'm totally lost.



Proof of uniqueness of  $\varprojlim F$ .

Suppose we have two candidate



Because  $M$  is  $\varprojlim F$ ,  $\exists!$

$N \xrightarrow{\phi} M$  so that everything commutes

Similarly  $\exists!$   $M \xrightarrow{\theta} N$

$M \xrightarrow{\phi\theta} M$  is the unique

map  $M \rightarrow M$  so that everything commutes.  $1_M$  is such a map.

Therefore  $\phi\theta = 1_M$

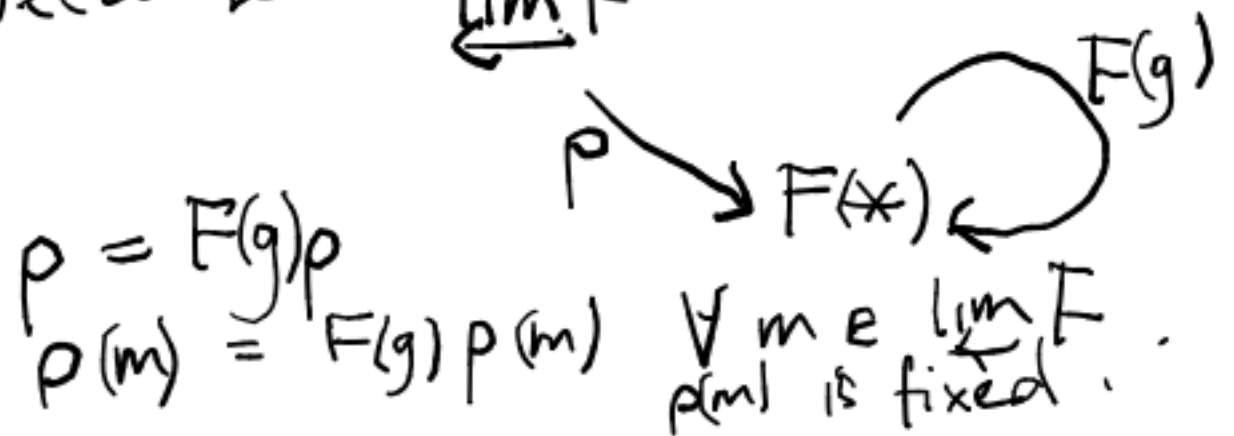
Similarly  $\theta\phi = 1_N$

$M \cong N$  via an isomorphism that commutes with everything.  $\square$

Example. Let  $G = \langle g \rangle$  be a group. A diagram  $F: G \rightarrow R\text{-mod}$  is a representation of  $G = \text{Mor}(G)$ .

Claim  $\varprojlim F = \text{fixed points of } G \text{ acting on } F(*)$

$*$  = object of  $G$ .  
because



# Pre-class Warm-up!!!

Consider the operation of inverse limit that takes a diagram  $F$  (of shape  $C$ ) and returns the inverse limit  $\varprojlim F$

Which of the following seems likely to be true?

A Inverse limit is a functor  $R\text{-mod} \rightarrow \text{Fun}(C, R\text{-mod})$

B Inverse limit is a functor  $\text{Fun}(C, R\text{-mod}) \rightarrow R\text{-mod}$

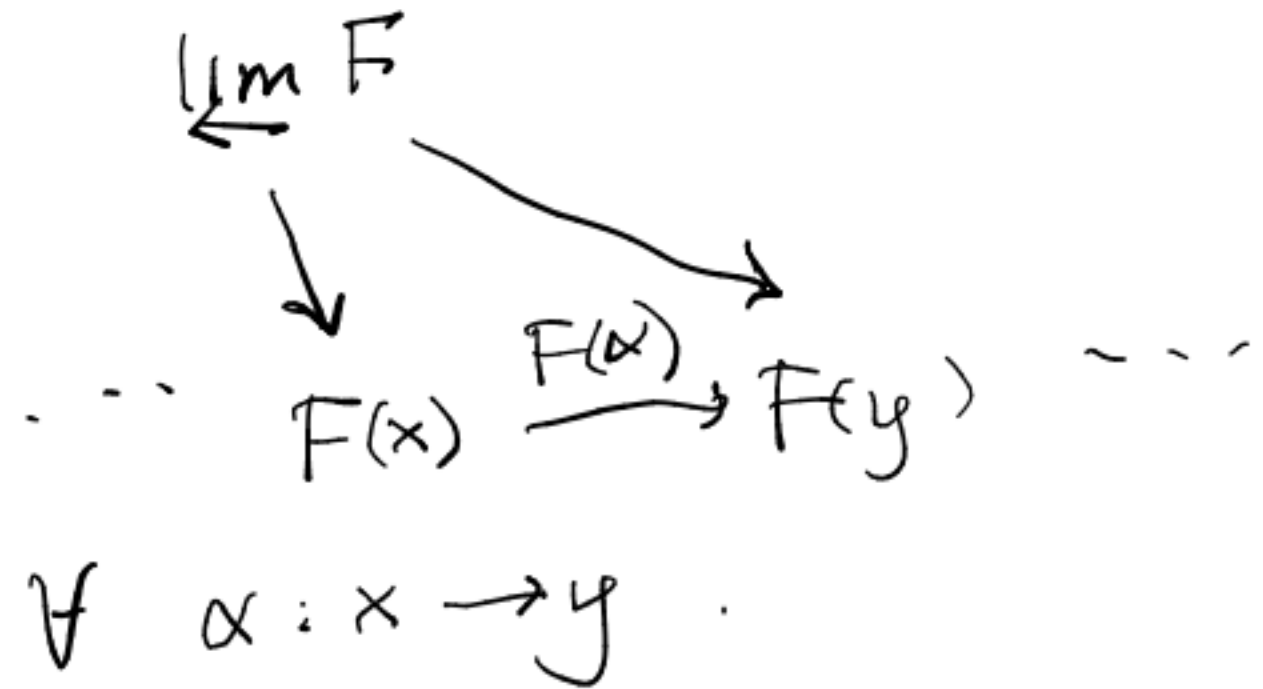
C Inverse limit is a functor  $\text{Fun}(C, R\text{-mod}) \rightarrow R\text{-mod}^{\text{op}}$

D Inverse limit is a natural transformation.

E None of the above.

$F: C \rightarrow R\text{-mod}$   
is a functor.

The inverse limit is the information



## Limits in terms of the constant diagram

Definition. Given an  $R$ -module  $N$  and a category  $\mathcal{C}$ , the constant functor (or diagram) is the functor  $F: \mathcal{C} \rightarrow R\text{-mod}$  with  $F(x) = N \quad \forall$  objects  $x$

$$F(\alpha) = 1_N \quad \forall \alpha: x \rightarrow y \text{ in } \mathcal{C}.$$

Example: If  $\mathcal{C} = G$  is a group  $F(g) = 1_N$ .  $F$  is a direct sum of copies of the trivial representation of  $G$ .

Notation  $\underline{N}$  is the constant functor with value  $N$ .

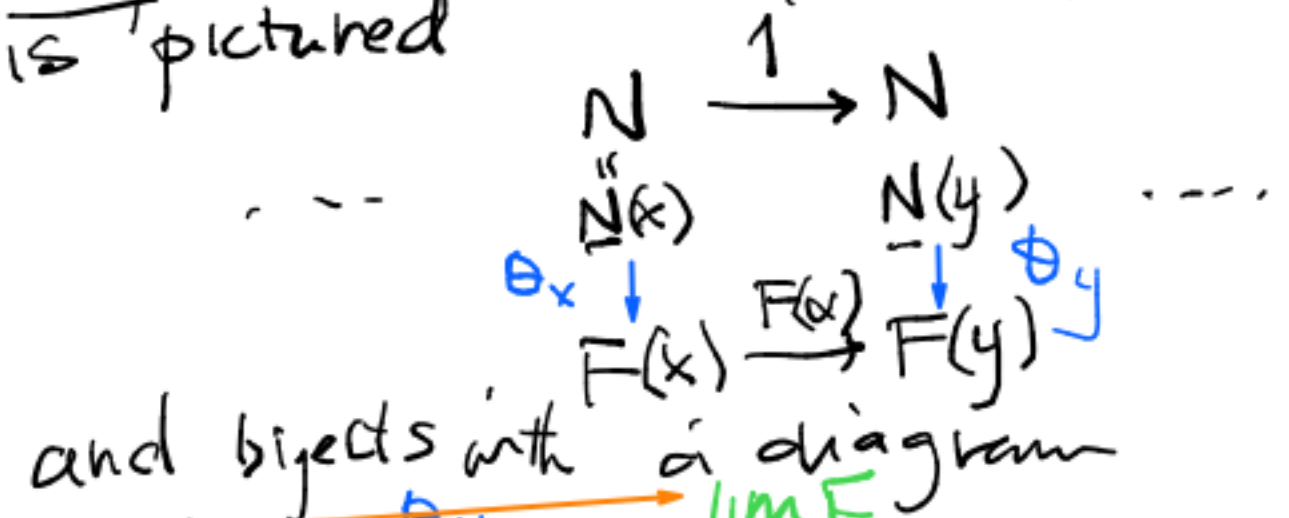
Proposition. Given a diagram  $F: \mathcal{C} \rightarrow R\text{-mod}$ , we have

$$\text{Hom}_{\text{Fun}(\mathcal{C}, R\text{-mod})}(\underline{N}, F) \cong \text{Hom}_{R\text{-mod}}(N, \varprojlim F)$$

The functor  $R\text{-mod} \rightarrow \text{Fun}(\mathcal{C}, R\text{-mod})$  given by

$$N \rightarrow \underline{N}$$

Proof A natural transfn  $\theta: \underline{N} \rightarrow F$  is pictured



and bijects with a diagram

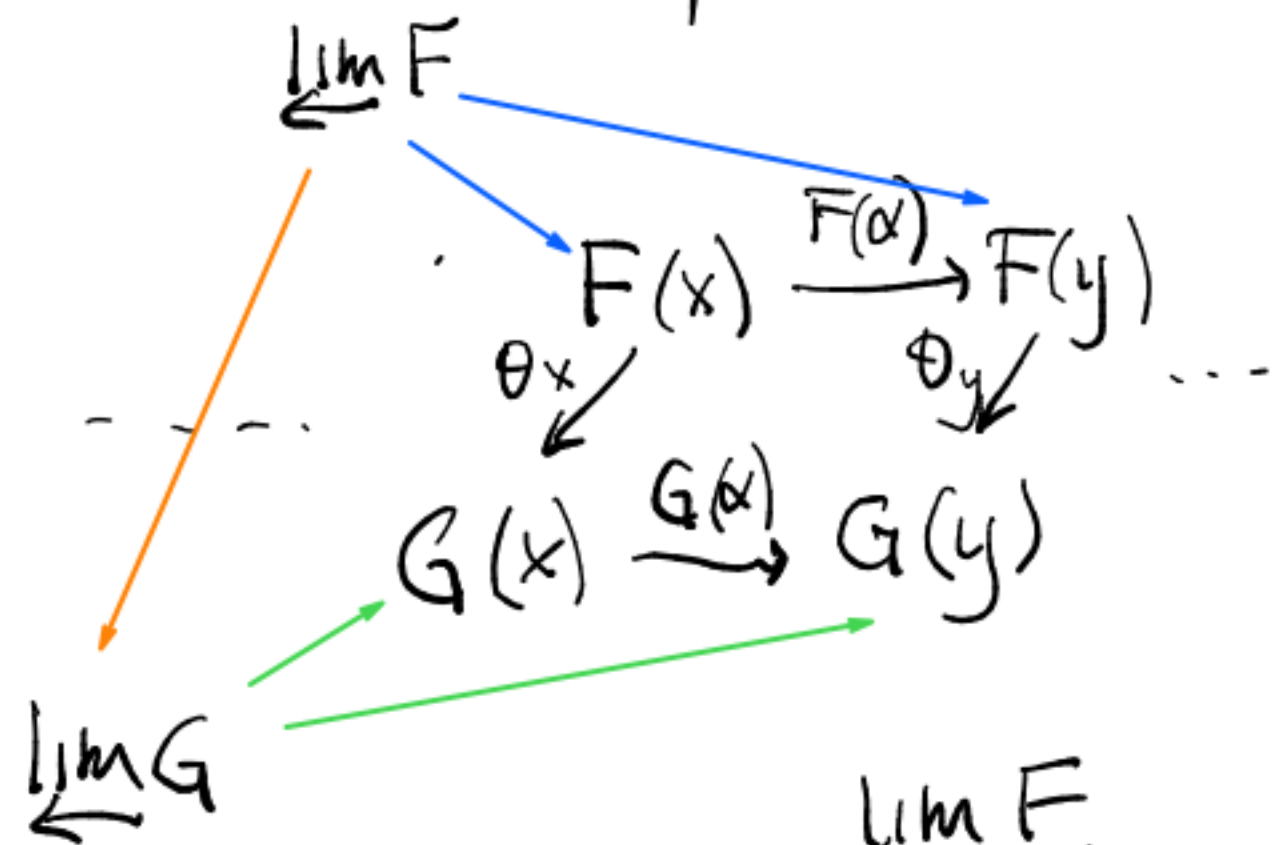
$$\begin{array}{ccc} N & \xrightarrow{\theta_y} & \varprojlim F \\ \theta_x \downarrow & \searrow & \uparrow \\ F(x) & \xrightarrow{F(\alpha)} & F(y) \end{array}$$

Such a diagram determines a  $! R\text{-mod}$  hom  $N \rightarrow \varprojlim F$ , and is determined by it.  $\square$

Functoriality of inverse limit

$\varprojlim : \text{Fun}(\mathcal{C}, R\text{-mod}) \rightarrow R\text{-mod}$   
 is a functor

A morphism of diagrams is  
 a natural transformation  $\theta : F \rightarrow G$



Because the  $\Delta$ s commute,  $\exists!$  unique map.

Corollary. Inverse limit is left exact on short exact sequences of functors.

Did we ever do s.e.s. of functors  $\mathcal{C} \rightarrow R\text{-mod}$

Fact  $0 \rightarrow F \xrightarrow{\theta} G \xrightarrow{\psi} H \rightarrow 0$

is a s.e.s.  $\iff \forall x \in \text{Ob}(\mathcal{C})$   
 the sequence  $0 \rightarrow F(x) \xrightarrow{\theta_x} G(x) \xrightarrow{\psi_x} H(x) \rightarrow 0$   
 is a s.e.s. of  $R$ -modules.

Proof:  
 Right adjoints are always left exact  $\square$

Proposition.

Let  $\mathfrak{m}$  be an ideal of a Noetherian ring  $R$  and  $0 \rightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \rightarrow 0$  be a short exact sequence of  $R$ -modules. Then

$0 \rightarrow A_{\mathfrak{m}}^{\wedge} \rightarrow B_{\mathfrak{m}}^{\wedge} \rightarrow C_{\mathfrak{m}}^{\wedge} \rightarrow 0$  is exact.

Proof.

We start by showing  $B_{\mathfrak{m}}^{\wedge} \rightarrow C_{\mathfrak{m}}^{\wedge}$  is onto

The rest of the argument is on the next page.

We represent elements of  $C_{\mathfrak{m}}^{\wedge}$  by sequences of cosets  $c_i + \mathfrak{m}^i C$ ,  $c_i \in C$ .

Given a sequence  $(c_i)$  in  $C$  for which

$$c_{i+1} + \mathfrak{m}^i C = c_i + \mathfrak{m}^i C \quad \forall i$$

we construct inductively

$$b_i \in B \text{ with } \beta(b_i) + \mathfrak{m}^i C = c_i + \mathfrak{m}^i C$$

$$\text{and also } b_i + \mathfrak{m}^{i-1} B = b_{i-1} + \mathfrak{m}^{i-1} B$$

Given such  $b_i$ , take any  $b'_{i+1} \in B$  with

$$\beta(b'_{i+1}) + \mathfrak{m}^{i+1} C = c_{i+1} + \mathfrak{m}^{i+1} C.$$

$$\text{Now } \beta(b'_{i+1} - b_i) + \mathfrak{m}^i C = \mathfrak{m}^i C$$

so  $\exists a \in A$  with

$$b'_{i+1} - b_i + \mathfrak{m}^i B = \alpha(a) + \mathfrak{m}^i B$$

$$\text{Put } b_{i+1} = b'_{i+1} - \alpha(a).$$

$$\text{Then } b_{i+1} + \mathfrak{m}^i B = b_i + \mathfrak{m}^i B$$

$$\text{and } \beta(b_{i+1}) + \mathfrak{m}^{i+1} C = c_{i+1} + \mathfrak{m}^{i+1} C.$$

The sequence  $(b_i)$  maps on to the sequence  $(c_i)$ .  $\square$

We now show most of the argument that

$$0 \rightarrow A_{\mathcal{M}}^{\wedge} \rightarrow B_{\mathcal{M}}^{\wedge} \rightarrow C_{\mathcal{M}}^{\wedge}$$

is exact.

The sequence of diagrams with

terms

$$0 \rightarrow \frac{A}{A \cap \mathcal{M}^i B} \rightarrow \frac{B}{\mathcal{M}^i B} \rightarrow \frac{C}{\mathcal{M}^i C}$$

is exact and so

$$0 \rightarrow \varprojlim \frac{A}{A \cap \mathcal{M}^i B} \rightarrow \varprojlim \frac{B}{\mathcal{M}^i B} \rightarrow \varprojlim \frac{C}{\mathcal{M}^i C}$$

is exact.

The Artin-Rees lemma shows that the map of diagrams with

$$\frac{A}{\mathcal{M}^i A} \rightarrow \frac{A}{A \cap \mathcal{M}^i B}$$

gives an isomorphism on taking  $\varprojlim$ .

$$\varprojlim \frac{B}{\mathcal{M}^i B} = B_{\mathcal{M}}^{\wedge}$$



# Pre-class Warm-up!!

True or False (in general)?

If the ring  $R$  is complete with respect to the ideal  $I$  then

$$\bigcap_{j \geq 0} I^j = \{0\}$$

A True ✓

B False

Approach 1: If  $x \in \bigcap_{j \geq 0} I^j$  then the Cauchy sequence  $(x, x, x, \dots)$  is equivalent to  $0$ , so equals  $0$ .

Approach 2:  $R = \varprojlim (R/I^j \rightarrow R/I^{j-1})$

$$\bigcap_{j \geq 0} I^j = 0.$$

Another true or false question:

If  $I$  is a maximal ideal of a ring  $R$  and the radical  $\text{rad}(0) = 0$  then

$$\bigcap_{j \geq 0} I^j = \{0\}.$$

Consider  $R = k \times k$

$k$  a field.

$k \times 0$  is a maximal ideal.

$$(k \times 0)^j \quad \forall j.$$

$$\bigcap_{j \geq 0} (k \times 0)^j \neq 0.$$



Proposition.

Let  $\mathfrak{m}$  be a maximal ideal of  $R$ . Then  $\hat{R}_{\mathfrak{m}}$  is a local ring.

Proof. We show: every  $x \in \hat{R}_{\mathfrak{m}}$   $x \notin (\mathfrak{m})$  is invertible.

We have seen  $\hat{R}_{\mathfrak{m}}/(\mathfrak{m}) \cong R/\mathfrak{m}$  which is a field. The image  $\bar{x}$  of  $x$  is  $\neq 0$ , so  $\exists y \in \hat{R}_{\mathfrak{m}}$  with  $\bar{x}\bar{y} = 1 \in \hat{R}_{\mathfrak{m}}/(\mathfrak{m})$ ,

$$xy - 1 = a \in \mathfrak{m}$$

$$xy = 1 + a \text{ so}$$

$$(xy)^{-1} = 1 - a + a^2 - a^3 + \dots \in \hat{R}_{\mathfrak{m}}$$

$$x[y(xy)^{-1}] = 1 \text{ and } x \text{ is invertible.}$$

□

Corollary

If  $\mathfrak{m}$  is a maximal ideal and  $\bigcap_{i \geq 0} \mathfrak{m}^i = 0$  there is an inclusion

$R \longrightarrow R_{\mathfrak{m}} \hookrightarrow \hat{R}_{\mathfrak{m}}$   
of rings.

Proof. The map  $R \longrightarrow \hat{R}_{\mathfrak{m}}$   
 $x \longmapsto (x, x, \dots)$   
is 1-1. Every element of  $R$  not in  $\mathfrak{m}$  is invertible in  $\hat{R}_{\mathfrak{m}}$  so  $R_{\mathfrak{m}} \subseteq \hat{R}_{\mathfrak{m}}$ . □

We used:

Lemma. If  $u$  is in  $\mathfrak{I}$  then  $1 + u$  is invertible in  $\hat{R}_{\mathfrak{I}}$

Krull's intersection theorem.

Let  $I$  be a proper ideal in a Noetherian ring  $R$ .

If  $R$  is a domain or a local ring then

$$\bigcap_{j \geq 0} I^j = \{0\}$$

Theorem (Hensel's Lemma).

Let  $R$  be a ring that is complete with respect to an ideal  $\mathfrak{I}$ , and let  $f(x)$  in  $R[x]$  be a polynomial. If  $a$  in  $R$  is an approximate root of  $f$  in the sense that

$$f(a) \in f'(a)^2 \mathfrak{I}$$

then there is a root  $b$  of  $f$  near  $a$  in the sense that  $b - a \in f'(a) \mathfrak{I}$

This is most often used when  $f'(a)$  is a unit, so the condition is  $f(a) \in \mathfrak{I}$

Definition. The formal derivative  $f'$  of a polynomial  $f$  is given by  $(x^m)' := m x^{m-1}$

$\mathbb{R}$ ,  
extended linearly. to all polynomials

Proposition.

1. If  $f$  is a polynomial then

$$f(a+t) = f(a) + f'(a)t + g(a,t)t^2$$

2. Leibniz rule holds.

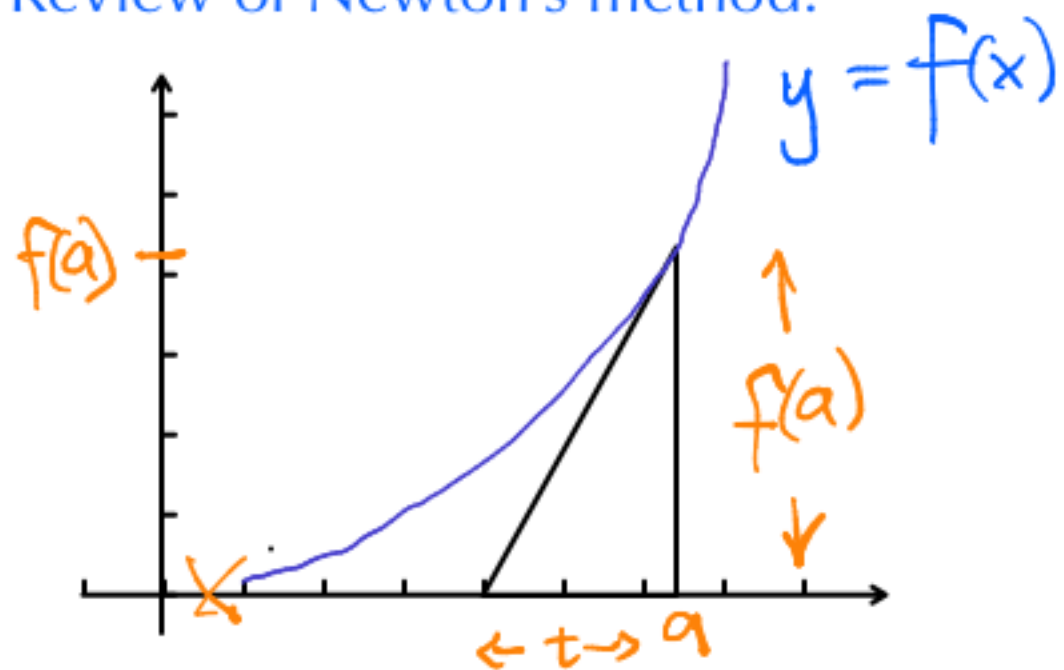
Proof. We check these hold for

$$f(x) = x^m$$

$$(a+t)^m = a^m + ma^{m-1}t + \binom{m}{2}a^{m-2}t^2 + \dots$$
$$= f(a) + f'(a)t + g(a,t)t^2.$$

□

## Review of Newton's method.



$$f'(a) = \frac{f(a)}{t} \quad , \quad t = \frac{f(a)}{f'(a)}$$

$a - \frac{f(a)}{f'(a)}$  might be

a closer approximation to  
a solution of  $f(x) = 0$ .

Theorem.

Suppose the ring  $R$  is complete with respect to the ideal  $I$ ,

let  $f$  in  $R[x]$  be a polynomial,  
 $n \geq 1$  a natural number.

Suppose  $a_n \in R$  satisfies

$$f(a_n) \in f'(a_n)^2 I^n$$

Then there exists  $a_{n+1} \in R$  with

$$a_{n+1} - a_n \in f'(a_n) I^n$$

$$f(a_{n+1}) \in f'(a_{n+1})^2 I^{n+1} \quad \text{and}$$

$f'(a_{n+1})$  lies in the same power of  $I$

as  $f'(a_n)$ .

Proof. Write  $f(a_n) = f'(a_n)^2 u$

for some  $u \in I^n$

Put  $\delta = -f'(a_n)u$  (so  $\delta = -\frac{f(a_n)}{f'(a_n)}$ )

$$a_{n+1} = a_n + \delta$$

Then

$$\begin{aligned} f(a_{n+1}) &= f(a_n + \delta) \\ &= f(a_n) + f'(a_n)\delta + g(a_n, \delta)\delta^2 \\ &= g(a_n, \delta)\delta^2 \\ &\in f'(a_n)^2 I^{2n} \end{aligned}$$

Also

$$\begin{aligned} f'(a_{n+1}) &= f'(a_n + \delta) \\ &= f'(a_n) + \delta h(a_n, \delta) \\ &\quad \text{for some polynomial } h \\ &= f'(a_n) (1 - u h(a_n, \delta)) \end{aligned}$$

Because  $u \in I$ ,  $(1 - u h(a_n, \delta))$  is invertible, so  $f'(a_{n+1})$  and  $f'(a_n)$  lie in the same power of  $I$  and

$$\begin{aligned} f(a_{n+1}) &\in f'(a_n)^2 I^{2n} = f'(a_{n+1})^2 I^{2n} \\ &\subseteq f'(a_{n+1})^2 I^{n+1} \quad \square \end{aligned}$$

Theorem (Hensel's Lemma).

Let  $R$  be a ring that is complete with respect to an ideal  $\mathfrak{I}$ , and let  $f(x)$  in  $R[x]$  be a polynomial. If  $a$  in  $R$  is an approximate root of  $f$  in the sense that

$$f(a) \in f'(a)^2 \mathfrak{I}$$

then there is a root  $b$  of  $f$ , near  $a$  in the sense that

$$b - a \in f'(a) \mathfrak{I}$$

If  $f'(a)$  is a unit then  $b$  is uniquely determined. *Not done.*

*Proof.* Start with  $a_1 = a$  in the last theorem and construct

$$a_1, a_2, a_3 \dots \text{ with } a_{n+1} - a_n \in f'(a_n) \mathfrak{I}^n$$

$$f(a_n) \in f'(a_n)^2 \mathfrak{I}^n \subseteq \mathfrak{I}^n$$

The sequence is Cauchy: let  $b = \lim_{n \rightarrow \infty} a_n$ .

Polynomials are continuous wrt the metric

$$\lim_{n \rightarrow \infty} f(a_n) = f(b) \in \bigcap_{n \geq 1} \mathfrak{I}^n = \{0\}$$

$$\begin{aligned} \text{We have } a_{n+1} - a_n &\in f'(a_n) \mathfrak{I}^n \\ &= f'(a) \mathfrak{I}^n \end{aligned}$$

$$\text{so } b - a \in f'(a) \mathfrak{I}.$$

## Applications

1. Roots of unity

2. When  $p$  is an odd prime, square roots of integers prime to  $p$  lie in  $\mathbb{Z}_p$  if and only if their images in  $\mathbb{F}_p$  have square roots.

Question. Determine whether each of  
2, 3, 6 have a square root in  $\mathbb{Z}_5$



- Compute the completion of  $\mathbb{Z}$  at the ideal  $0$ .

- at  $4\mathbb{Z}$ ? Is it the same as  $\mathbb{Z}_2$ ? Is  $\mathbb{Z}_2$  complete w.r.t  $4\mathbb{Z}$ .

- When  $I = \circ \rightarrow \circ \leftarrow \circ$ . Show that  $\varprojlim$  is not exact, but that when  $I = \circ \rightarrow \circ \rightarrow \circ$  then  $\varinjlim$  is exact.

---

If  $N \subset M$  is a submodule  
 $\downarrow$  natural map  
 $\hat{M}$

then  $\hat{N}$  is the closure of  $N$  in the topology on  $\hat{M}$

Show the  $a + M_n$  are a base for the topology on  $M$ .

---

Describe the  $p^{\text{th}}$  roots of 1 in  $\mathbb{Z}_p$ .

---