Example: the p-adic integers (Section 7.1)

The 10-adic integers

Decimal numbers are strings

finite integers | $a_3 a_2 a_1 a_0 \bullet a_{-1} a_{-2}$ - - - - - -

~~? • 0 0 0 ;~~

10-adic integers are strings

$\cdots\cdots - a_3 a_2 a_1 a_0 \bullet 000$

Example
$$
\begin{array}{r}
\ldots 54321 \\
+ \;\; \ldots 41798 \\
\hline
- - - - \ldots 96119
\end{array}
$$

Let $p = 2$ and work to base 2.

This was wrong

$$
\begin{array}{r}
1\,?0\,?1\,?1\,?0\,?1. \\
\times \qquad\qquad 5. \\
\hline
0\,0\,0\,1. \\
1\,1\,1\,1\,1\,1\,0
\end{array}
$$

5 is a notation for 101

$5\,(\ldots 01101101) = 1$ ✗

001

$\frac{1}{5} = \ldots\overline{0110}11 0 1.$ ✗

It should be

$\frac{1}{5} = \ldots\overline{1100}11001101.$

Pre-class Warm-up!!

In the 2-adic integers, calculate

...1111.000 + 1.000 = 0

A 0

B 1

C -1

D 10

E 11

$-1 = \ldots 1111.$

Fact: The 2-adic integers are a group under +

Calculate also $\ldots\overline{10}101011.000 \times 3$
(where 3 is a notation for the 2-adic integer 11.000)

$$
\begin{array}{rr}
 & \ldots 01010111 \\
\times & 11 \\
\hline
 & \ldots 10101011 \\
+ & 01010110 \\
\hline
 & \ldots 000001 \\
 & 1\;1\;1\;1\;\;\;
\end{array}
$$

First definition of completion

Let M be an R-module and consider a filtration

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

filtration = chain of submodules.

We define a pseudo-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 ultrametic $\leq$

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

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

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

$$\leq d(a,b) + d(b,c)$$

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

Definition (Krull topology) We put a topology on M with basic open sets the balls $B_\epsilon(a)$, $a \in M$, $\epsilon > 0$.

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: $a + M_i$, $i = 0, 1, 2, \ldots$ $a \in M$.

$\quad = B_{\mu^{i-1}}(a)$

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

$j = 1, 2, 3, \ldots$

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

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

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

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

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

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

Example: The powers of the ideal (p) in Z.

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

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

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

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

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

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

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 $a_i \to x$ and $b_i \to x$ as $i \to \infty$.

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 $\hat{M}$ of the metric space M is the set of equivalence classes of Cauchy sequences.

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

$m \longmapsto (m, m, m, m, \dots)$

$\hat{M}$ acquires a metric $\hat{d}$ extending d.

$\hat{M}$ 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
$\forall \epsilon > 0 \ \exists N$ 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.
$d(m, m') < \mu^i \Leftrightarrow$ the first i digits of m, m' 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 $\mathfrak{m} \subseteq R$
$M = R, \ M_i = \mathfrak{m}^i$

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

Question. Let M_i = (2^i)⊊ Z and let μ = 1/2.
What is d(48,96)?

$96 - 48 = 48 \in (2^4) - (2^5)$ so $i = 4$
$d(48, 96) = \left(\frac{1}{2}\right)^4 = \frac{1}{16}$

Proposition. The completion is
a. an R-module,
b. a metric space
c. the same as the completion of $M / \bigcap_{i \geq 0} M_i$
d. 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

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

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

$(\ldots \ldots, x_{2,j_2}, x_{1,j_1}, x_{0,j_0})$

with $x_{i,j_i} \in$ coset reps of M_{i+1} in M_i

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

Given such a list we construct a Cauchy sequence

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

Quesion: 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

A countable?

✓

p-adic integers are lists

$\ldots a_2 a_1 a_0 .$

If we could enumerate such lists, make a table

$$\begin{array}{ccc} a_{12} & a_{11} & a_{10}. \\ a_{22} & a_{21} & a_{20}. \\ a_{32} & a_{31} & a_{30}. \end{array}$$

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

This expansion is not in the enumeration.

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

$$\cdots \subseteq \mathfrak{m}^2 M \subseteq \mathfrak{m}M \subseteq M$$

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

$$R[t]^{\hat{}}_{\mathfrak{m}} =: R[[t]] = \left\{ \sum_{i \geq 0} a_i t^i \;\middle|\; a_i \in R \right\}$$

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

Some more properties we have already seen:

Proposition
a. There is a homomorphism $M \to \hat{M}$ with kernel $m \longmapsto (m, m, m, \dots)$

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

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

$$R^{\hat{}}_{\mathfrak{m}} / (\mathfrak{m}) \cong R/\mathfrak{m},$$

and $(\mathfrak{m}) \cap R = \mathfrak{m}$

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

Proof Elements of $\mathfrak{m}$ are represented by lists of coset reps $(\dots, x_2, x_1, 0)$
On completing, $\mathfrak{m}$ completes to all lists $(?, ?, \dots ?, 0)$. This is the ideal of $R^{\hat{}}_{\mathfrak{m}}$ generated by $\mathfrak{m}$.
The lists $(0, 0, \dots 0, a)$, a is a coset rep for $\mathfrak{m}$ in R are coset reps for $(\mathfrak{m})$ in $R^{\hat{}}_{\mathfrak{m}}$.
This means $R/\mathfrak{m}$ & $R^{\hat{}}_{\mathfrak{m}}/(\mathfrak{m})$ are in bijection. $(\mathfrak{m}) \cap R = \mathfrak{m}$
= lists of elements of R belonging to $\mathfrak{m}$.
$R/\mathfrak{m} \longrightarrow R^{\hat{}}_{\mathfrak{m}}/(m)$ is an isomorphism.

Categorical approach

Definition.
A diagram of R-modules is a functor $F: \mathcal{C} \to R\text{-mod}$, 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 $i \to j$ whenever $i \geq j$. Picture of $\mathcal{C}$:

$$\begin{tikzcd} \cdots \arrow[r] & 3 \arrow[r] \arrow[rr, bend right] & 2 \arrow[r] \arrow[rr, bend left] & 1 \arrow[r] \arrow[loop below, "1_1"] & 0 \arrow[loop right, "1_0"] \end{tikzcd}$$

$\text{Free}(\text{quiver } \cdots \to \underset{x}{3} \xrightarrow{\alpha} \underset{y}{2} \xrightarrow{\beta} \underset{z}{1} \to 0)$.

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

$$\underset{\substack{\parallel \\ F(x)}}{M_3} \xrightarrow{F(\alpha)} \underset{\substack{\parallel \\ F(y)}}{M_2} \xrightarrow{F(\beta)} \underset{\substack{\parallel \\ F(z)}}{M_1} \to M_0$$

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

$$\begin{tikzcd} \varprojlim F \arrow[d] \arrow[dr] \arrow[drr] & & \\ F(x) \arrow[r, "F(\alpha)"] & F(y) \arrow[r, "F(\beta)"] & F(z) \end{tikzcd}$$

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

$$\begin{tikzcd} N \arrow[r, "\exists!"] \arrow[dr] \arrow[drr] & \varprojlim F \arrow[d] \arrow[dr] & \\ & F(x) \arrow[r] & F(y) \end{tikzcd}$$

Example. The pullback, the product.

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

$$\begin{tikzcd} P \arrow[r] \arrow[d] \arrow[dr, phantom, "\text{comm uter}"] & N \arrow[d] \\ M \arrow[r] & L \end{tikzcd}$$

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 $F: \mathcal{C} \to R\text{-mod}$ looks like

$$\begin{tikzcd}
 & & \prod_{i \in I} M_i \arrow[dll, "\text{proj}"'] \arrow[dl, "\text{proj}"] & N \arrow[l, "\exists ! \phi"'] \arrow[dll, "f_{i_2}"] \\
M_{i_1} & M_{i_2} & &
\end{tikzcd}$$

Their product is the inverse limit of this diagram.

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

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

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 $F : \mathcal{C} \to R\text{-mod}$. We construct

$$\varprojlim F = \left\{ (a_x) \in \prod_{x \in Ob(\mathcal{C})} F(x) \;\middle|\; a_x \in F(x), \ \forall\, \alpha : x \to y \text{ in } \mathcal{C} \ \ F(\alpha)(a_x) = a_y \right\}$$

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

$$\begin{tikzcd}
 & \varprojlim F \arrow[d, "p_x"] \arrow[dr, "p_y"] & \\
 & F(x) \arrow[r, "F(\alpha)"] & F(y) \\
N \arrow[ur] \arrow[urr] \arrow[uur, dashed] & &
\end{tikzcd}$$

giving commutative triangles.

Given commutative Δs $\exists$ a unique homom. $N \to \prod F(x)$ whose image lies in $\varprojlim F$

Corollary. Given a filtration of a module M

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

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

$$\cdots \to M/M_2 \to M/M_1 \to M/M_0 = 0$$

Proof. Each equivalence class of Cauchy sequences corresponds to a list of coset representatives for M_{i+1} in M_i: $(\cdots, a_2, a_1, a_0)$

Define $\hat{M} \to \varprojlim F$

$$(\cdots, a_2, a_1, a_0) \longmapsto (a_{i-1} + a_{i+1} + \cdots + a_0 + M_{i+1})_i$$

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

The maps $M/M_i \to M/M_{i-1}$ remove the top term in the partial sum, Δs commute. We get an isomorphism.

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 $\varprojlim F$:

$$\begin{tikzcd} M \arrow[d] \arrow[dr] & N \arrow[dl] \arrow[d] \\ F(x) \arrow[r] & F(y) \cdots \end{tikzcd}$$

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 $M \to M$ 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 $\mathcal{C} = G$ be a group. A diagram $F : G \to R\text{-mod}$ is a representation of $G = \mathrm{Mor}(G)$.

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

$*$ = object of G.

because

$$\begin{tikzcd} \varprojlim F \arrow[r, "p"] & F(*) \arrow[loop right, "F(g)"] \end{tikzcd}$$

$p = F(g)p$

$p(m) = F(g)\,p(m)$ $\forall m \in \varprojlim F$.

$p(m)$ is fixed.

Pre-class Warm-up!!!

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

Which of the following seems likely to be true?

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

✓ B Inverse limit is a functor $\mathrm{Fun}(\mathcal{C}, R\text{-mod}) \to R\text{-mod}$

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

D Inverse limit is a natural transformation.

E None of the above.

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

The inverse limit is the information

$$\begin{tikzcd} & \varprojlim F \arrow[d] \arrow[dr] & & \\ \cdots & F(x) \arrow[r, "F(\alpha)"] & F(y) & \cdots \end{tikzcd}$$

$\forall \ \alpha : x \to y$.

Limits in terms of the constant diagram

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

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

Example: If $\mathcal{C} = \mathcal{G}$ 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 : C -> R-mod, we have

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

The functor R-mod -> Fun(C,R-mod) given by

$$N \longrightarrow \underline{N}$$

<u>Proof</u> A natural transfn $\theta : \underline{N} \to F$ is pictured

$$\begin{tikzcd}
N \arrow[r, "1"] & N \\
\cdots \quad \underline{N}(x) \arrow[u, phantom, "\parallel"] \arrow[d, "\theta_x"'] & \underline{N}(y) \arrow[d, "\theta_y"] \quad \cdots \\
F(x) \arrow[r, "F(\alpha)"] & F(y)
\end{tikzcd}$$

and bijects with a diagram

$$\begin{tikzcd}
 & & \varprojlim F \arrow[dll] \arrow[d] \\
N \arrow[urr] \arrow[r, "\theta_x"'] \arrow[rr, bend left, "\theta_y"] & F(x) \arrow[r, "F(\alpha)"] & F(y)
\end{tikzcd}$$

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

Functoriality of inverse limit

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

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

$$\begin{tikzcd}
\varprojlim F \arrow[r] \arrow[rr, bend left] \arrow[d] & F(x) \arrow[r, "F(\alpha)"] \arrow[d, "\theta_x"'] & F(y) \arrow[d, "\theta_y"] \\
\varprojlim G \arrow[r] \arrow[rr, bend right] & G(x) \arrow[r, "G(\alpha)"] & G(y)
\end{tikzcd}$$

$$\begin{tikzcd}
 & \varprojlim F \arrow[dl] \arrow[dr] & \\
G(x) \arrow[rr, "G(\alpha)"] & & G(y)
\end{tikzcd}$$

Because the Δs commute, $\exists !$ orange map.

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

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

Fact $0 \to F \xrightarrow{\theta} G \xrightarrow{\psi} H \to 0$ is a s.e.s. $\iff$ $\forall\, x \in \mathrm{Ob}(\mathcal{C})$ the sequence $0 \to F(x) \xrightarrow{\theta_x} G(x) \xrightarrow{\psi_x} H(x) \to 0$ 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
$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ be a short exact sequence of R-modules. Then
$0 \to \hat{A}_{\mathfrak{m}} \to \hat{B}_{\mathfrak{m}} \to \hat{C}_{\mathfrak{m}} \to 0$ is exact.

Proof.
We start by showing $\hat{B}_{\mathfrak{m}} \to \hat{C}_{\mathfrak{m}}$ is onto

The rest of the argument is on the next page.

We represent elements of $\hat{C}_{\mathfrak{m}}$ 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 $b_i \in B$ with $\beta(b_i) + \mathfrak{m}^i C = c_i + \mathfrak{m}^i C$

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

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

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

so $\exists\, a \in A$ with

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

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

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

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

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

We now show most of the argument that

$$0 \to A^{\wedge}_{m} \to B^{\wedge}_{m} \to C^{\wedge}_{m}$$

is exact.

The sequence of diagrams with terms

$$0 \to \frac{A}{A \cap m^i B} \to \frac{B}{m^i B} \to \frac{C}{m^i C}$$

is exact and so

$$0 \to \varprojlim \frac{A}{A \cap m^i B} \to \varprojlim \frac{B}{m^i B} \to \varprojlim \frac{C}{m^i C}$$

is exact.

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

$$\frac{A}{m^i A} \longrightarrow \frac{A}{A \cap m^i B}$$

gives an isomorphism on taking $\varprojlim$.

$$\varprojlim \frac{B}{m^i B} = B^{\wedge}_{m}$$

Proposition. Let R be a Noetherian commutative ring.

$$\hat{M_{\mathfrak{m}}} \cong \hat{R_{\mathfrak{m}}} \otimes_R M.$$

Proof. It is true if M is free.

$$(\hat{R_{\mathfrak{m}}})^d \cong \hat{R_{\mathfrak{m}}} \otimes_R R^d$$

In general, take a free finite presentation $F_1 \to F_0 \to M \to 0$ exact.

free

Consider

$$\begin{tikzcd}
\arrow[r] & \hat{F_{1\mathfrak{m}}} \arrow[r] & \hat{F_{0\mathfrak{m}}} \arrow[r] & M_{\mathfrak{m}} \arrow[r] & 0 \\
& \hat{R_{\mathfrak{m}}} \otimes F_1 \arrow[r] \arrow[u] & \hat{R_{\mathfrak{m}}} \otimes F_0 \arrow[r] \arrow[u] & \hat{R_{\mathfrak{m}}} \otimes M \arrow[r] \arrow[u] & 0
\end{tikzcd}$$

where the two rows are exact.

Replace $\hat{F_{1\mathfrak{m}}}$ by its image in $\hat{F_{0\mathfrak{m}}}$

Use the snake lemma!

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 $(x, x, x \cdots)$ is equivalent to 0, so equals 0. $x = 0$

Approach 2: $R = \varprojlim \left(\to R/I^j \to R/I^{j-1} \to \cdots \right)$

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

Another true or false question:
If I is a maximal ideal of a ring R and the radical 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.

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

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

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 $\bar{x}\bar{y} = 1 \in \hat{R}_{\mathfrak{m}}/(\mathfrak{m})$,

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

$xy = 1 + a$ so

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

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

$\square$

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 $R_{\mathfrak{m}} \subseteq \hat{R_{\mathfrak{m}}}$. $\square$

We used:
Lemma. If u is in I then 1 + u is invertible in $\hat{R_I}$

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

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

Theorem (Hensel's Lemma).
Let R be a ring that is complete with respect to an ideal 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

$$f(a) \in f'(a)^2 I$$

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

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

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

extended R-linearly. to all polynomials

Proposition.
1. If f is a polynomial then

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

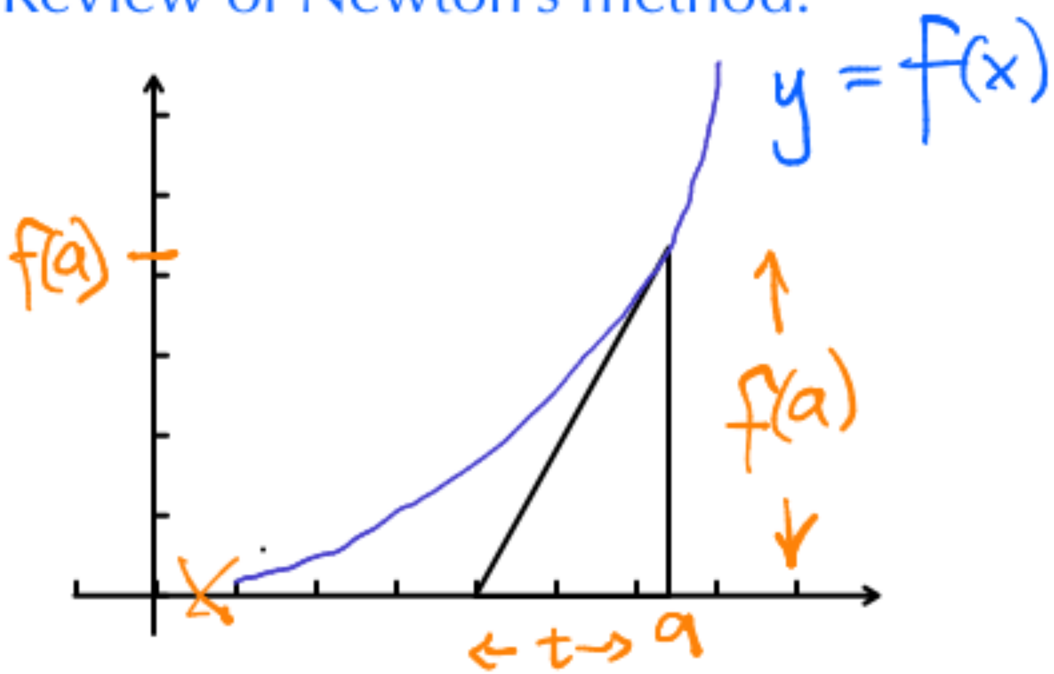
2. Leibniz rule holds.

Proof. We check these hold for $f(x) = x^m$.

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

$\square$

Review of Newton's method.



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

$a - \dfrac{f(a)}{f'(a)}$ 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

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

$$f(a_{n+1}) \in f'(a_{n+1})^2 I^{n+1}$$ 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 "$\delta = -\dfrac{f(a_n)}{f'(a_n)}$")

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

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

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

Theorem (Hensel's Lemma).
Let R be a ring that is complete with respect to an ideal 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

$$f(a) \in f'(a)^2 I$$

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

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

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

The sequence is Cauchy: let $b = \lim_{n\to\infty} a_n$.
Polynomials are continuous wrt the metric

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

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

$$= f'(a) I^n$$

so $b - a \in f'(a) I$.

Pre-class Warm-up!!

When we work modulo 5, is 14 the square of a number?

A Yes

B No

i.e. Can we solve $x^2 \equiv 14 \pmod 5$

$$14 \equiv 4 \equiv -1 \pmod 5 ?$$

$$2^2 \equiv 4 \equiv 14 \pmod 5$$

The congruence classes of squares mod 5 are

$$\begin{array}{ccccc} 0^2 & 1^2 & 2^2 & 3^2 & 4^2 \\ \| & \| & \| & \| & \\ 0 & 1 & 4 & 4 & 1 \end{array}$$

Notice for later that the 4^{th} powers are

0, 1.

We will see in class that $\mathbb{Z}_5^\wedge$ has four 4^{th} roots of unity, including two square roots of -1.

Applications

1. Roots of unity in $\hat{\mathbb{Z}}_p$. Solve $X^t - 1 = 0$ in $\hat{\mathbb{Z}}_p$, where $p \nmid t$.

$f(X) = X^t - 1$, $f'(X) = tX^{t-1}$.

If $a \in \mathbb{Z}$ is a root of $X^t - 1 \equiv 0 \pmod p$ then $f'(a) = t a^{t-1}$ is a unit.

$f(a) \in f'(a)^2 p \hat{\mathbb{Z}}_p$.

Hensel says: $\exists\, b \in \hat{\mathbb{Z}}_p$ with $b \equiv a \pmod p$, $b^t = 1$.

Definition $\mu_t(R)$ is the set of t^{th} roots of 1 in R.

We have a ring homomorphism $\hat{\mathbb{Z}}_p \to \hat{\mathbb{Z}}_p / p\hat{\mathbb{Z}}_p \cong \mathbb{Z}/p\mathbb{Z}$

It takes roots of 1 to roots of 1.

Theorem If $p \nmid t$ the map $\mu(\hat{\mathbb{Z}}_p) \to \mu(\mathbb{Z}/p\mathbb{Z})$ is a bijection.

<u>Proof</u>. Hensel $\Rightarrow$ the map is surjective.

$f(X) = X^t - 1$ is separable over $\hat{\mathbb{Z}}_p$ and $\mathbb{Z}/p\mathbb{Z}$

$f'(X) = tX^{t-1} \neq 0$.

The roots of f are distinct in $\hat{\mathbb{Z}}_p$, and map to distinct roots in $\mathbb{Z}/p\mathbb{Z}$.

Therefore the map is 1-1.

2. When p is an odd prime, square roots of integers prime to p lie in Z^_p if and only if their images in F_p have square roots.

Theorem. An integer t prime to p (odd) has a square root in $\hat{\mathbb{Z}}_p$ $\Leftrightarrow$ it has a square root in $\mathbb{Z}/p\mathbb{Z}$.

Proof. Here $f(X) = X^2 - t$

$f'(X) = 2X$

If $a^2 \equiv t \pmod p$ then

$f'(a) = 2a$ is a unit (p odd).

so if $f(a) \in p\hat{\mathbb{Z}}_p$

$\exists\ b \in \hat{\mathbb{Z}}_p$ with $b^2 = t$. $\square$

Conversely ...

Question. Determine whether each of 2, 3, 6 have a square root in Z^_5

$$\shortparallel$$

$$\mathbb{Z}_5^{\wedge}.$$

Which of the following has a square root.

A 2

B 3

C 6 ✓

D more than one of the above

E None of the above.

Lifting idempotents, the Krull-Schmidt theorem.

Proposition.
Let R be a commutative ring complete with respect to an ideal I.
Let A be an R-algebra, finitely generated as an R-module.
Any expression
1 = e_1 + … + e_n
as a sum of orthogonal idempotents in A/IA lifts to an expression
1 = f_1 + … + f_n
as a sum of orthogonal idempotents in A.
The e_i are primitive if and only if the f_i are primitive.

Meaning

$e \in A$ is idempotent $\Leftrightarrow e^2 = e$

e_1, e_2 are orthogonal $\Leftrightarrow$

$$e_1 e_2 = 0 = e_2 e_1$$

e is primitive $\Leftrightarrow$ ($e = e_1 + e_2$ orthogonal idempotents $\Rightarrow e_1 = 0$ or $e_2 = 0$)

Proposition.
Let R be a commutative ring complete with respect to an ideal I.
Let A be an R-algebra, finitely generated as an R-module.
Any expression
1 = e_1 + … + e_n
as a sum of orthogonal idempotents in A/IA lifts to an expression
1 = f_1 + … + f_n
as a sum of orthogonal idempotents in A.
The e_i are primitive if and only if the f_i are primitive.

Uses.
– Projective modules.
If $e^2 = e \in A$ then $A = Ae \oplus A(1-e)$
Ae is a projective left A-module.

Fact: Ae is indecomposable
$\Leftrightarrow$ e is primitive.
($\Leftrightarrow$ not possible to write $Ae = M_1 \oplus M_2$)
See my book on rep'n theory!

Projective modules ~~for~~ A/IA
are the reductions modulo I
of projective A-modules.

More on ures:

Fact: an A-module M is indecomposable $\iff$ $\mathrm{End}_A(M)$ only has one (non-zero) idempotent: 1_M.

(Another idempotent $e \in \mathrm{End}(M)$ gives $1_M = e + (1_M - e)$, a sum of ~~orthog.~~ idempotents, $M = eM \oplus (1-e)M$ as A-modules)

Conclude

M is indecomposable $\iff$ M/IM is an indecomposable A/IA-module.

Proposition.
Let R be a commutative ring complete with respect to an ideal I.
Let A be an R-algebra, finitely generated as an R-module.
Any expression

$$1 = e_1 + e_2$$

as a sum of orthogonal idempotents in A/IA lifts to an expression

$$1 = f_1 + f_2.$$

Proof.

Proof 2. We construct successive idempotents g_i in $A / I^i A$, lifting each other. Given g_{i-1} in $A / I^{i-1}A$ let a in A/I^i map onto g_{i-1}, so $a^2 - a$ is in I^{i-1} / I^i
Now $(a^2 - a)^2 = 0$ in A/I^i.
Let $g_i = 3a^2 - 2a^3$.
This lifts g_{i-1} and
$g_i^2 - g_i = -(3-2a)(1+2a)(a^2-a)^2 = 0$.

We take $f = \lim g_i$

Krull-Schmidt Theorem.

let R be a complete local Noetherian ring with maximal ideal I and let A be an R-algebra finite over R.

- 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 wrt $4\mathbb{Z}$.
- When $\mathcal{I} = \bullet \to \bullet \leftarrow \bullet$ Show ~~that~~ $\varprojlim$ is not exact, but ~~that~~ when $\mathcal{I} = \bullet \to \bullet \to \bullet$ then $\varprojlim$ is exact.

If
$$\begin{array}{c} N \subset M \text{ is a submodule} \\ \big\downarrow \text{natural map} \\ \hat{M} \end{array}$$
then $\hat{N}$ is the closure of N in the topology on $\hat{M}$

Show the $a + M_\lambda$ are a base for the topology on M.

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

Show that polynomial functions are continuous on $\hat{R}_{\mathfrak{m}}$