Example: the p-adic integers (Section 7.1)

The 10-adic integers

Decimal numbers are strings

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

? $\bullet$ 0 0 0 ...

10-adic integers are strings

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

Example

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

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

This was wrong

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

5 is a notation for 101

$5\,(\ldots 01101101) = 1$ ✗

001

$\frac{1}{5} = \ldots\overline{011}01101.$ ✗

It should be

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

Pre-class Warm-up!!

In the 2-adic integers, calculate

$\ldots 1111.000 + 1.000$ $= 0$

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)

$$
\begin{array}{rr}
 & \ldots 0101011 \\
\times & 11 \\
\hline
 & \ldots 10101011 \\
+ & 0101010110 \\
\hline
 & \ldots 000001
\end{array}
$$

First definition of completion

Let M be an R-module and consider a filtration

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

filtration = chain of submodules.

We define a pseudo-distance function on M.
Let $0 < \mu < 1$. We put, for $a, b \in M$

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

Proposition For all a, b in M we have

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

$d(a,c) \leq \max(d(a,b), d(b,c))$ the ultrametric inequality

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

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

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

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

$$\overset{\shortparallel}{B_{\mu^{i-1}}(a)}$$

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

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

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

Example: The powers of the ideal (p) in 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 $(0, 0, a_i p^i, \dots a_1 p, a_0)$

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 $a_i \to x$ 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: $(3, 3.1, 3.14, 3.141, 3.1415, \ldots)$ 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) $M \longrightarrow \hat{M}$

$m \longmapsto (m, m, m, m, \ldots)$

$\hat{M}$ 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

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

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

$$R[t]^{\wedge}_{\mathfrak{m}} =: R[[t]] = \{\sum_{i \geq 0} a_i t^i \mid a_i \in R\}$$

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

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 $R^{\wedge}_{\mathfrak{m}}$ generated by $\mathfrak{m}$ has

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

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

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

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 $R^{\wedge}_{\mathfrak{m}}$ 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 $R^{\wedge}_{\mathfrak{m}}$.
This means $R/\mathfrak{m}$ & $R^{\wedge}_{\mathfrak{m}}/(\mathfrak{m})$ are in bijection. $(\mathfrak{m}) \cap R = \mathfrak{m}$
= lists of elements of R belonging to $\mathfrak{m}$.
$R/\mathfrak{m} \longrightarrow R^{\wedge}_{\mathfrak{m}}/(\mathfrak{m})$ 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 $\mathcal{C}$:

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

Free(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

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

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 is a picture of R-modules

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

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

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

Their product is the inverse limit of this diagram.

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

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

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

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

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

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

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

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

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 $\hat{M} \longrightarrow \varprojlim F$

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

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

The maps $M/M_i \to M/M_{i-1}$ 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 $\varprojlim F$:

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

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

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

$*$ = object of $\mathcal{G}$.

because

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

$\rho = F(g)\rho$

$\rho(m) = F(g)\rho(m) \quad \forall m \in \varprojlim F$.

$\rho(m)$ is fixed.

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 $\mathcal{C} = G$ 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

Corollary. Inverse limit is left exact.

Proposition.
Let $\mathfrak{m}$ be an ideal of 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. Inverse limit is left exact, so we only need show that $\hat{B}_{\mathfrak{m}} \to \hat{C}_{\mathfrak{m}}$ is surjective.

We will use the fact that, $\forall i$,

$$A/\mathfrak{m}^i A \to B/\mathfrak{m}^i B \to C/\mathfrak{m}^i C \to 0$$

is exact, because $R/\mathfrak{m}^i \otimes_R -$ is right exact.

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). $\square$

Proposition.

$$\hat{M}_{\mathfrak{m}} \cong \hat{R}_{\mathfrak{m}} \otimes_R M .$$

<u>Proof</u>. It is true if M is free.

In general, take a free finite presentation $F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0$

Consider

$$\begin{tikzcd}
\arrow[r] & \hat{F}_{1\mathfrak{m}} \arrow[r] & \hat{F}_{0\mathfrak{m}} \arrow[r] & \hat{M}_{\mathfrak{m}} \arrow[r] & 0 \\
& \hat{R}_{\mathfrak{m}} \otimes F_1 \arrow[r] \arrow[u] & \hat{R}_{\mathfrak{m}} \otimes F_0 \arrow[r] \arrow[u] & \hat{R}_{\mathfrak{m}} \otimes M \arrow[r] \arrow[u] & 0
\end{tikzcd}$$

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 !

Corollary. Inverse limit is left exact.

Fact:
$\hat{R}_{\mathfrak{m}}$ is flat, so $M \mapsto \hat{M}_{\mathfrak{m}}$ is exact.

Hensel's lemma.
If $\mathfrak{m}$ is maximal prime? then $\hat{R}_{\mathfrak{m}}$ is a local ring.

Show $\hat{R}_{\mathfrak{m}}$ is complete
The image of $(\mathfrak{m}^r) \otimes M$ contains $\mathfrak{m}^r \cdot M$
Cauchy sequences in M are the images of Cauchy sequences in $\hat{R}_{\mathfrak{m}} \otimes M$. In $\hat{R}_{\mathfrak{m}} \otimes M$ they converge, so they do in the image also. Therefore $\hat{M}_{\mathfrak{m}} =$ image of $\hat{R}_{\mathfrak{m}} \otimes M$.