Continuing the pre/review ...

Riemann's explicit formula, Gauss *Quadratic Reciprocity*, Lagrange resolvents for cyclotomic fields, factorization of Dedekind zeta functions, ...

Continuing: solving equations mod p^n ... and p-adic numbers. *Hensel's Lemma*, a version of *Newton-Raphson* in a different context. Both *completions* and *projective limits*.

Forgotten example: Cauchy's criterion is *sufficient*, p-adically.

Ultrametric inequality: All p-adic triangles are isosceles!!!
Stronger than *triangle inequality*:

$$|x \pm y|_p \;\leq\; \max\big(|x|_p, |y|_p\big) \qquad \text{(with } \textit{equality} \text{ unless } |x|_p = |y|_p\text{)}$$

Ring structure of $\mathbb{Z}_p$

All integers n *prime to* p become p-adic *units*

No zero divisors in $\mathbb{Z}_p$: use the p-adic norm...

Even on the *completion* $\mathbb{Q}_p^\times$ the p-adic norm *still* takes only the discrete values p^ℓ with $\ell \in \mathbb{Z}$ ... in contrast to the usual $| * |$'s values on $\mathbb{R}$ versus on $\mathbb{Q}$.

Each of these sets is *both open and closed.*

$$\begin{aligned} \mathbb{Z}_p &= \{\alpha \in \mathbb{Q}_p \,:\, |\alpha|_p \le 1\} &= \{\alpha \in \mathbb{Q}_p \,:\, |\alpha|_p < p\} \\ p\mathbb{Z}_p &= \{\alpha \in \mathbb{Q}_p \,:\, |\alpha|_p < 1\} &= \{\alpha \in \mathbb{Q}_p \,:\, |\alpha|_p \le \tfrac{1}{p}\} \\ \mathbb{Z}_p^\times &= \{\alpha \in \mathbb{Q}_p \,:\, |\alpha|_p = 1\} &= \{\alpha \in \mathbb{Q}_p \,:\, \tfrac{1}{p} < |\alpha|_p < p\} \end{aligned}$$

Proof: Discreteness of $|*|_p$...

$\mathbb{Z}_p$ and $\mathbb{Q}_p$ are totally disconnected. That is, given $\alpha \neq \beta$ in $\mathbb{Q}_p$, there are disjoint open-and-closed sets $U \ni \alpha$ and $V \ni \beta$ such that $U \cup V = \mathbb{Q}_p$ ...

Cauchy's criterion is necessary-and-sufficient: A p-adic infinite sum $a_o + a_1 + a_2 + \ldots$ is convergent if and only if $|a_n| \to 0$.

Proof: Ultrametric property: given $\varepsilon > 0$, let m_o be large enough so that $|a_m|_p < \varepsilon$ for $m \geq m_o$. Then, by the ultrametric property, for $m_o \leq m < n$, the tail between these two indices has size

$$|a_{m+1} + \ldots + a_n|_p \;\leq\; \max_{m<j\leq n} |a_j|_p \;<\; \varepsilon$$

Done.

Don't forget that in $\mathbb{R}$, Cauchy's criterion is *necessary*, but *not* sufficient: the harmonic series $1 + \frac{1}{2} + \frac{1}{3} + \ldots$ diverges.

Observe: The only non-zero proper *ideals* in $\mathbb{Z}_p$ are $p^\ell \cdot \mathbb{Z}_p$ with $\ell > 0$.

Proof: Given a proper, non-zero ideal I in $\mathbb{Z}_p$, let $\sigma = \sup_{x\in I} |x|_p$. By the discreteness of $|*|_p$, for $|x_j|_p \to \sigma \neq 0$, eventually $|x_i|_p = \sigma$.

Thus, we can choose *a* largest element x in I. For all $y \in I$, $|y/x|_p = |y|_p/|x|_p \leq 1$. That is, $y/x \in \mathbb{Z}_p$, and $I = x \cdot \mathbb{Z}_p$. ///

Another viewpoint: Even though the p-adic norm and metric succeed in making the sequences produced by Hensel's lemma *convergent*, there was no mandate to make metric spaces.

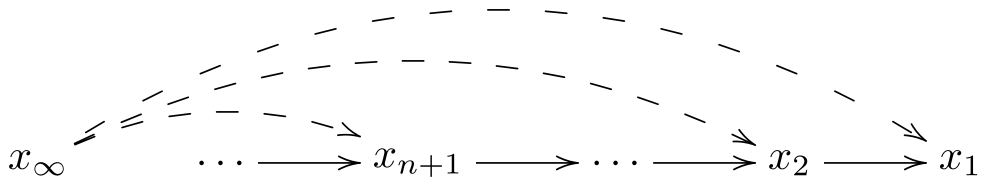
One ambiguity is that many different metrics can give the same topology.

Candidly, Hensel's recursion produces a sequence x_n fitting into a picture

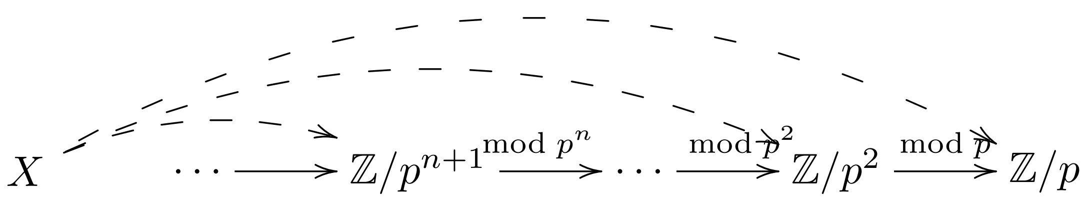
$$\cdots \longrightarrow x_{n+1} \longrightarrow \cdots \longrightarrow x_2 \longrightarrow x_1$$

$$\cdots \longrightarrow \mathbb{Z}/p^{n+1} \xrightarrow{\text{mod } p^n} \cdots \xrightarrow{\text{mod } p^2} \mathbb{Z}/p^2 \xrightarrow{\text{mod } p} \mathbb{Z}/p$$

What we want is not so much a metric something-something, but an object X *behind* all the $\mathbb{Z}/p^n$'s, and $x_\infty \in X$,



making a *commutative diagram* (meaning that the outcome doesn't depend on what route is traversed)



We should tell how this X is to *interact* with other things, probably *topological rings*, meaning rings with topologies so that addition and multiplication are continuous. *Hausdorff*, for sanity.

Warm-up: characterizations versus constructions:

The *ordered pair* formation (a, b) is *characterized* by the property that $(a, b) = (a', b')$ if and only if $a = a'$ and $b = b'$. Straightforward intent!

In contrast, the set-theory *construction* is $(a, b) = \{\{a\}, \{a, b\}\}$. In the early 20th century, this was interesting. The construction is irrelevant to the *use* of ordered pairs.

Or, what is an indeterminate? We tell calculus students that x is a *variable real number*. Or *is arbitrary*. Not bad intuition, but what does that *mean?* This viewpoint is stressed beyond hope in the Cayley-Hamilton theorem: a linear map T on a finite-dimensional real vectorspace V has characteristic polynomial $\chi_T(x) = \det(x \cdot 1_V - T)$. The CH theorem says $\chi_T(T) = 0$.

We are substituting a *matrix* for x.

The CH theorem helps illustrate that x has the property that we can *substitute anything* for it... within reason.

One way to say this: working over $\mathbb{C}$, for example, the polynomial ring $\mathbb{C}[x]$ should have the property that, for every ring R containing a copy of $\mathbb{C}$, and for every $r_o \in R$, there is a unique ring hom $\mathbb{C}[x] \to R$ mapping $x \to r_o$ (and mapping $\mathbb{C}$ to the copy inside R).

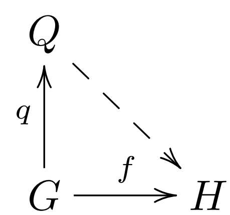
That is, $\mathbb{C}[x]$ is the *free* $\mathbb{C}$-*algebra on one generator*.

Set-maps $\{x\} \to R$ become $\mathbb{C}$-*algebra* maps $\mathbb{C}[x] \to R$.

(The functor $\{x\} \dashrightarrow \mathbb{C}[x]$ is *adjoint to* the forgetful functor taking R to its underlying set.)

Quotient groups:

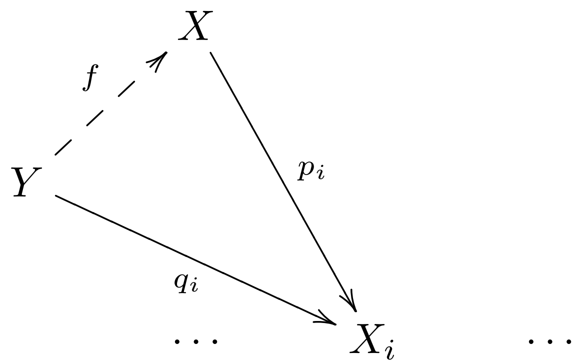
The *quotient* G/N of a group G by a normal subgroup N is usually *defined* to be the set of cosets gN. This is easy to say, but conceals the *purpose*. With hindsight, the real purpose is to make a group Q with a group hom $q : G \to Q$ such that every group hom $f : G \to H$ with $\ker f \supset N$ *factors through* $q : G \to Q$, in the sense of giving a commutative diagram



Existence of Q is proven by the usual *construction* by cosets.

A form of simplest *isomorphism theorem* is really the *characterization* of the quotient.

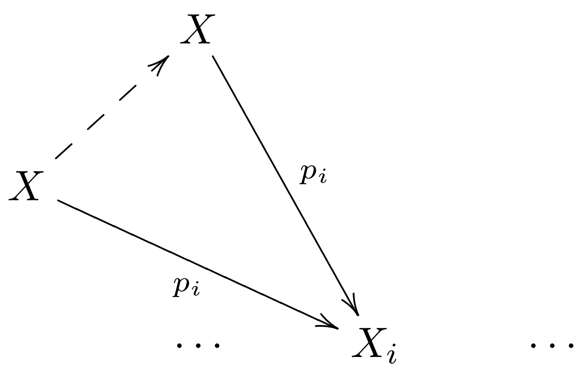
Simple example: products: A *product* $X = \prod_i X_i$ of objects X_i has maps $p_i : X \to X_i$ such that, for every object Y with maps $q_i : Y \to X_i$, there is a *unique* $f : Y \to X$ such that $q_i = p_i \circ f$. A picture:



This characterization explains why the *product topology* of an infinite collection of topological spaces is coarser than we might expect: the following general fact (proven just below) shows that there is *no choice* of how to make a sensible product object!

This diagrammatic characterization determines the product $\prod_i X_i$ *uniquely up to unique isomorphism.*

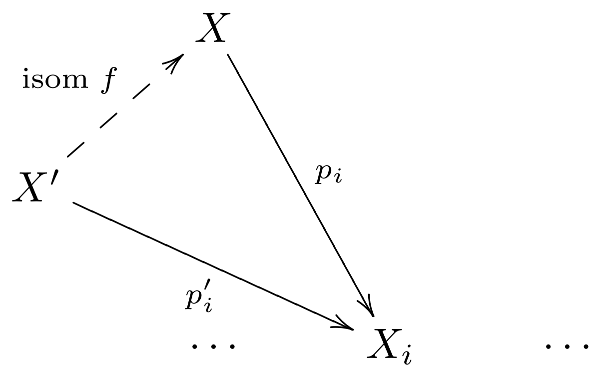
Proof: First, show that the only map $X \to X$ compatible with the diagram



is the *identity* map. Indeed, the identity map fits, and the assertion that there is *only one* map fitting into the diagram finishes it.

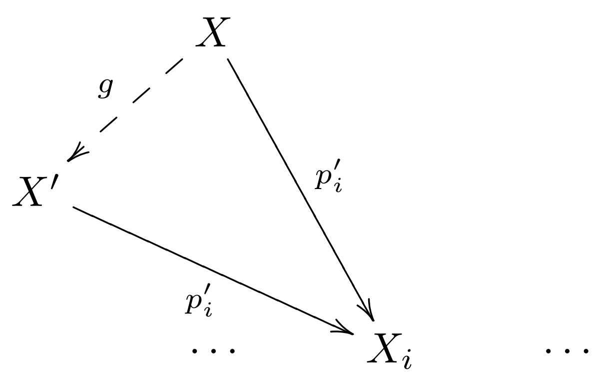
Next, ...

... show that, given two products X, X' with projections p_i, p'_i to X_i, there is a unique isomorphism $X' \to X$ fitting into the diagram



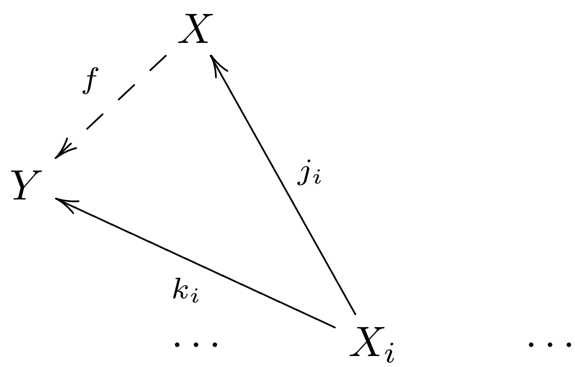
First, since X is a product, in any case there is a *unique* map f fitting into the diagram. We must prove it is an isomorphism.

On the other hand, reversing the roles of X, X', using the fact that X' is a product, there is *some* map g fitting into the diagram



Then $g \circ f : X' \to X'$ and $f \circ g : X \to X$ respect the projections, so must be the respective identity maps, and are isomorphisms. ///

Coproducts are characterized by reversing the arrows: A *coproduct* $X = \coprod_i X_i$ of objects X_i has maps $j_i : X_i \to X$ such that, for every object Y with maps $k_i : X_i \to Y$, there is a *unique* $f : X \to Y$ such that $q_i = f \circ p_i$. A picture:



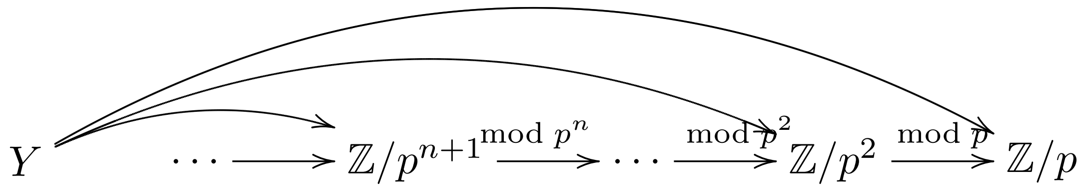
The same argument shows this diagrammatic characterization determines the coproduct *uniquely up to unique isomorphism.*

Note: In *concrete* categories, where objects more-or-less are constructible as *sets* with additional structure, *products* are typically constructible as *set*-products with the corresponding additional structure.

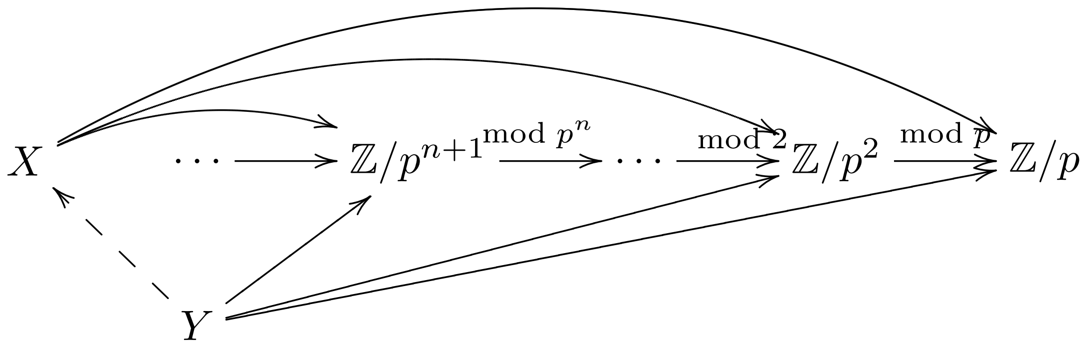
Product groups' underlying sets are product sets, as are topological spaces, vector spaces, etc .

In contrast, set-*coproducts* are *disjoint unions*, which is *not* the underlying set for coproducts of groups or vector spaces.

Back to projective limits: *map* means *continuous ring hom.* Require that, for every topological ring Y with compatible maps



there is a *unique* map $Y \to X$ giving a commutative diagram



A topological ring $X = \lim \mathbb{Z}/p^n$ meeting these conditions is the *(projective) limit* of the $\mathbb{Z}/p^n$'s, and is provably the same $\mathbb{Z}_p$!!!

Note: each finite ring $\mathbb{Z}/p^n$ has a unique Hausdorff topology!!!

Prove *existence* of projective limits by a *construction*. Here, as is typical, $\lim_n X_n$ is a *subset* of the (topological) product $\prod_n X_n$. Specifically, with

$$\ldots \longrightarrow X_{n+1} \xrightarrow{\varphi_{n+1}} \ldots \xrightarrow{\varphi_3} X_2 \xrightarrow{\varphi_2} X_1$$

a projective limit $X = \lim_n X_n$ can be constructed as

$$X = \{\{x_n\} : x_n \in X_n \text{ such that } \varphi_n(x_n) = x_{n-1} \text{ for all } n\}$$

That is, X consists exactly of *compatible sequences*

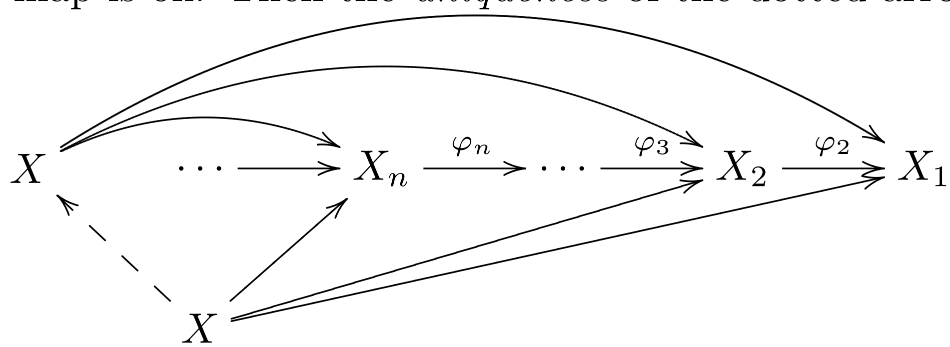
$$\ldots \longrightarrow x_{n+1} \xrightarrow{\varphi_{n+1}} \ldots \xrightarrow{\varphi_3} x_2 \xrightarrow{\varphi_2} x_1$$

as produced by Hensel. For continuous φ_n and *compact* X_n's, *Tychonoff's theorem* says the product is *compact*. The limit is a *closed* subset of a compact Hausdorff space, so is *compact*. This proves compactness of $\mathbb{Z}_p$!!!

Uniqueness (up to unique isomorphism) of projective limits

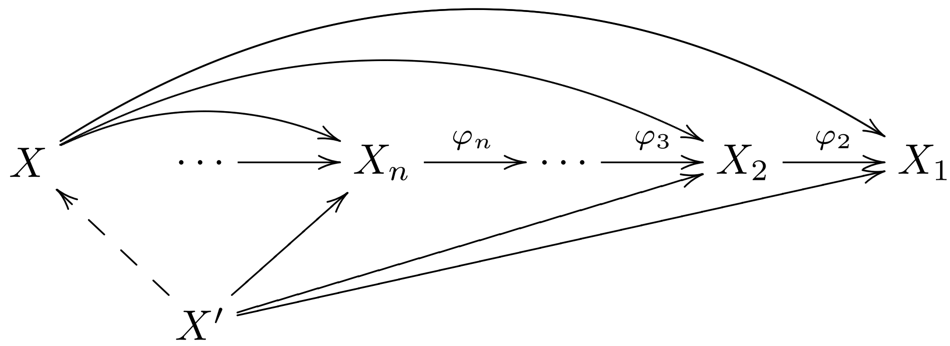
The diagrammatic characterization can be used to assure that there's *no ambiguity* in what $\mathbb{Z}_p$ is, as long as it functions as a projective limit:

First, claim the only map of $X = \lim_n X_n$ to *itself*, compatible with the maps of it to the X_n, is the *identity*. Certainly the identity map is ok. Then the *uniqueness* of the dotted arrow

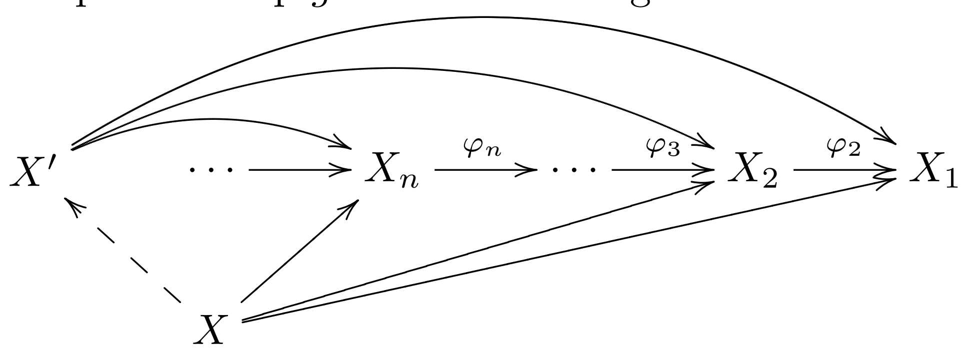


proves that the identity is the *only* compatible map. Next, ...

Suppose X and X' were *two* projective limits. On one hand, there is a unique $f : X' \to X$ giving commutative diagram



On the other hand, reversing the roles of X and X', there is a unique compatible map $g : X \to X'$ fitting into



The composites $f \circ g : X \to X$ and $g \circ f : X' \to X'$ are also compatible, so must be the identities on X and X', by the first part. Thus, f, g are mutual inverses. ///
