LECTURE 12, WEDNESDAY 17.03.04

FRANZ LEMMERMEYER

1. p-adic Numbers

At the end of the 19th century, Hensel invented p-adic numbers as a number theoretical analogue of power series in complex analysis. It took more than 25 years before p-adic numbers were taken seriously by number theorists: this was when Hasse, around 1920, proved the Local-Global Principle for quadratic forms over $\mathbb{Q}$: a quadratic form in n variables with rational constants represents 0 nontrivially if and only if the quadratic form represents 0 nontrivially in each p-adic completion of $\mathbb{Q}$. The point is that checking representability in p-adic fields is something that can be done easily, and in a finite number of steps.

So what are p-adic numbers? Actually there are several ways of introducing them.

The Naive Approach. Fix a prime number p and consider formal power series in p:

$$a = a_0 + a_1 p + a_2 p^2 + \dots, \tag{1}$$

where $0 \le a_i \le p-1$. The key word here is *formal*, that is, you negelct things like convergence. Now you can clearly add, subtract and multiply such power series; for example, let us add the 5-adic numbers

$$\begin{array}{ccccccccc} 3 & + & 2\cdot 5 & + & 0\cdot 5^2 & + & 4\cdot 5^3 & + \dots \\ 1 & + & 4\cdot 5 & + & 2\cdot 5^2 & + & 2\cdot 5^3 & + \dots \\ \hline 4 & + & 6\cdot 5 & + & 2\cdot 5^2 & + & 6\cdot 5^3 & + \dots . \end{array}$$

Now observe that $6 = 1 + 5$, hence $6 \cdot 5 = 1 \cdot 5 + 1 \cdot 5^2$, hence we carry 1 and find

$$4 + 6\cdot 5 + 2\cdot 5^2 + 6\cdot 5^3 + \dots = 4 + 1\cdot 5 + 3\cdot 5^2 + 1\cdot 5^3 + \dots,$$

where we have carried another 1 at the coefficient of 5^3. Clearly we can also multiply p-adic numbers this way, so we get a ring $\mathbb{Z}_p$, the ring of p-adic integers, whose neutral element is $0 = 0 + 0\cdot p + 0\cdot p^2 + \dots$ and whose unit element is $1 = 1 + 0\cdot p + 0\cdot p^2 + \dots$. Note that $\mathbb{Z}_p$ contains $\mathbb{Z}$ as a subring: every natural number a actually has a *finite* expansion into a p-adic series. What about -1?. Well,

$$\begin{aligned} -1 &= p - 1 - 1\cdot p \\ &= p - 1 + (p-1)\cdot p - p^2 \\ &= p - 1 + (p-1)\cdot p + (p-1)\cdot p^2 - p^3 \\ &= \dots \\ &= p - 1 + (p-1)\cdot p + (p-1)\cdot p^2 + (p-1)\cdot p^3 + \dots \end{aligned}$$

Actually, this is not too surprising: consider the geometric series $\frac{1}{1-x} = 1 + x + x^2 + \ldots$ and plug in p: then $\frac{1}{1-p} = 1 + p + p^2 + \ldots$, and multiplying through by $p-1$ gives you the p-adic expansion of -1 above. Actually, the "equation"

$$-1 = 1 + 2 + 4 + 8 + \ldots$$

can be found in Euler's work (where, of course, it didn't make too much sense).

It is a simple exercise to show that the ring $\mathbb{Z}_p$ has no zero divisors, hence it is an integral domain; its quotient field $\mathbb{Q}_p$ is called the field of p-adic numbers.

How do p-adic numbers (as opposed to p-adic integers) look like? You might know that in the ring of formal power series, an element is a unit if and only if its constant term is nonzero. The same works here: every p-adic integer of the form (1) is a unit if $a_0 \neq 0$ (or, more generally, if $p \nmid a_0$). In particular, the prime p is a nonunit, and

$$\frac{a_0 + a_1 p + a_2 p^2 + \ldots}{p} = a_0 p^{-1} + a_1 + a_2 p + \ldots;$$

thus p-adic numbers are something like Laurent series in p: power series in p with at most finitely many negative exponents.

Projective Systems. In order to get a more satisfying definition of p-adic numbers, let us "cut off" such a power series at some exponent. This seems to give us an integer, namely

$$a_0 + a_1 p + a_2 p^2 + \ldots + a_{n-1} p^{n-1}.$$

But remember that we are allowed to carry and borrow; if we borrow 1 from p^n and cut off at exponent n, we get

$$a_0 + a_1 p + a_2 p^2 + \ldots + (a_{n-1} + p) p^{n-1}.$$

Thus cutting off does not seem to be a well defined process; fortunately, not all is lost: if we interpret the element after cutting off as an element of $\mathbb{Z}/p^n\mathbb{Z}$, then carrying or borrowing does not do any harm.

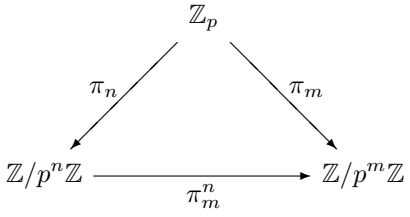
This means that for every $n \geq 1$ there is a natural map

$$\pi_n : \mathbb{Z}_p \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$$

defined by cutting off the expansion of a p-adic number at the exponent n. These maps actually respect the ring structure, i.e., the π_n are ring homomorphisms. In addition, they are "compatible" in the following sense: if we cut off at the exponent n and then reduce the result modulo p^m for some $m \leq n$, then we get the same number as if we had cut off at m right away. This means that

$$\pi_m^n \circ \pi_n = \pi_m,$$

where $\pi_m^n : \mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathbb{Z}/p^m\mathbb{Z}$ is the canonical projection.



Thus the ring $\mathbb{Z}_p$ of p-adic integers provides us with a projective system of rings.

A collection of sets (groups, rings, ...; this makes sense in pretty general categories) R_n and, for every pair $i < j$, maps (group homomorphisms, ring homomorphisms, morphisms in a category) $\pi_i^j : R_j \longrightarrow R_i$ is called a projective system if $\pi_i^j \circ \pi_j^k = \pi_i^k$ whenever $i < j < k$ (if you throw in identity maps $\pi_i^i : R_i \longrightarrow R_i$, you have these morphisms whenever $i \leq j$).

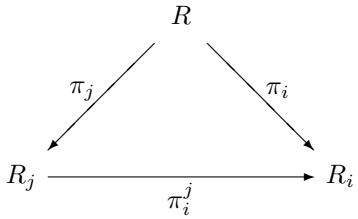
Now given such a projective system consisting of groups $\mathbb{Z}/p^n\mathbb{Z}$ and the corresponding natural projections, how can we get back our ring $\mathbb{Z}_p$? Remember that a p-adic number gave us cut-offs in every ring $\mathbb{Z}/p^n\mathbb{Z}$; but not every collection $(\alpha_n)_n$ of elements in these rings (or, in other words, an element in the direct product of the $\mathbb{Z}/p^n\mathbb{Z}$) will come from a p-adic number: those that do will satisfy the compatibility condition $\pi_m^n \alpha_n = \alpha_m$.

This suggests that given a projective system (R_i, π_i^j) of rings we should form the direct product $\prod R_i$ and then look for compatible sequences of elements: the subset

$$R = \{(r_1, r_2, \ldots) \in \prod R_i : \pi_i^j r_j = r_i \text{ for all } i < j\}$$

of the direct product $\prod R_i$ actually forms a ring: it contains the sequences $0 = (0, 0, 0, \ldots)$ and $1 = (1, 1, 1, \ldots)$, and it is closed with respect to addition and multiplication inherited from the direct product; in fact, if $r = (r_i)$ and $s = (s_i)$ are compatible sequences, then so are $r + s = (r_i + s_i)$ and $rs = (r_i s_i)$: this is because e.g. $\pi_i^j(r_j + s_j) = \pi_i^j(r_j) + \pi_i^j(s_j) = r_i + s_i$ etc.

The ring R constructed above from the projective system (R_i, π_i^j) is called the projective limit of the R_i, and we write $R = \varprojlim R_i$. This construction allows you to think of elements of the projective limit as compatible sequences of elements of the R_i. Moreover, we get the mprphisms $\pi_i : R \longrightarrow R_i$ for free: just take the projection on the i-th component. With these morphisms, the following diagrams commute:



In the case we are interested in, the $R_i = \mathbb{Z}/p^i\mathbb{Z}$ can be interpreted as discrete compact rings; thus the product $\prod R_i$ is compact by Tychonov, and since it can be shown that R is a closed subset of $\prod R_i$, the limit $R = \mathbb{Z}_p$ is a compact ring. The induced topology is called the profinite topology.

A very important case of projective limits are profinite groups: projective limits of finite groups. These play a major role in Galois theory: consider the field $\mathbb{Q}$ and its set of finite normal extensions $K/\mathbb{Q}$; each such extension has its Galois group $\mathrm{Gal}\,(K/\mathbb{Q})$. Moreover, if $K \subseteq L$, then there is a canoncial projection $\mathrm{res}_K^L : \mathrm{Gal}\,(L/\mathbb{Q}) \longrightarrow \mathrm{Gal}\,(K/\mathbb{Q})$ defined by restriction of automorphisms. The system of all such finite normal extensions together with the restriction maps from a projective system that is slightly more general than those considered above: the index set is not the set $\mathbb{N}$; the groups are indexed by the fields K. We can make the index set into a directed set by defining $K \leq L$ if $K \subseteq L$.

Note that a directed set is a partially ordered set (we have a relation $\le$ with the property that $i \le j$ and $j \le k$ imply $i \le k$) such that for any pair i, j there exists an index k such that $i \le k$, $j \le k$.

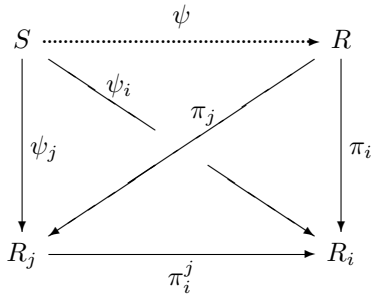
The index set of all finite normal extensions of $\mathbb{Q}$ is directed: if K and L are normal extensions, then so is the compositum KL, and we clearly have $K \le KL$ and $L \le KL$. The projective limit of this system is called the Galois group $G_{\mathbb{Q}} = \mathrm{Gal}\,(\overline{\mathbb{Q}}/\mathbb{Q})$ of the algebraic closure of $\mathbb{Q}$, or the absolute Galois group of $\mathbb{Q}$; the profinite topology on $G_{\mathbb{Q}}$ is called the Krull topology, and the main theorem of Galois theory also holds for infinite Galois extension if only *closed* subgroups of $G_{\mathbb{Q}}$ are used (in other words, the Galois correspondence is an inclusion reversing bijection between subfields of $\overline{\mathbb{Q}}$ and closed subgroups of $G_{\mathbb{Q}}$).

Finally, let us also give the definition of projective limits using the universal property: a projective system in a category C sonsists of a directed set I, a collection $(R_i)_{i\in I}$ of objects, together with morphisms $\pi_i^j : R_j \longrightarrow R_i$ for each pair $i \le j$ such that

- $\pi_i^i = \mathrm{id}_{R_i}$,
- $\pi_i^j \circ \pi_j^k = \pi_i^k$ whenever $i \le j \le k$

An object R together with morphisms $\pi_i : R \longrightarrow R_i$ is called a projective limit of the projective system if the following conditions are satisfied:

- $\pi_i = \pi_i^j \circ \pi_j$ whenever $i \le j$;
- if there is an object S and morphisms ψ_i such that $\psi_i = \pi_i^j \circ \psi_j$ whenever $i \le j$, then there exists a unique morphism $\psi : S \longrightarrow R$ such that $\psi_i = \pi_i \circ \psi$.



Projective limits exist in the categories of abelian groups, of R-modules, and of rings.

Completions. We have seen above that the ring $\mathbb{Z}_p$ of p-adic integers carries a profinite topology. With respect to this topology, the sequence $1, p, p^2, p^3, \ldots$ is a null sequence: it converges to 0. This observation gives us yet another way of constructing p-adic numbers, and this construction has the advantage of showing that the fields $\mathbb{Q}_p$ and $\mathbb{R}$ have a lot in common (note that $\mathbb{R}$ does not contain a subring which is a projective limit of finite rings).

Recall the construction of the real numbers from $\mathbb{Q}$: consider the ring C of Cauchy sequences of rational numbers; the set N of null sequences is an ideal in C, and, as a matter of fact, a maximal ideal; the quotient ring $\mathbb{R} = C/N$ is therefore a field.

The same construction gives us the p-adic numbers $\mathbb{Q}_p$: all we have to do is replace the absolute value $|\cdot|$ you know from calculus by the p-adic valuation defined as follows: if you fix a prime p, then every rational number $r \ne 0$ can be

written uniquely in the form $r = p^a s$, where s is a fraction whose numerator and denominator are coprime to p. Now define $|r|_p = p^{-a}$, and $|0|_p = 0$. This has all the properties of the usual absolute value; as a matter of fact, not only is the triangle inequality $|r + s|_p \leq |r|_p + |s|_p$ true (which is essential for proving that Cauchy sequences form a ring), it actually holds in the stronger form

$$|r + s|_p \leq \max\{|r|_p, |s|_p\}.$$

Note that the sequence $1, p, p^2, p^3, \ldots$ is a null sequence with respect to $|\cdot|_p$ because $|1|_p = 1$, $|p|_p = \frac{1}{p}$, $|p^2|_p = \frac{1}{p^2}$, etc. Cauchy sequences of rational numbers form a ring C, and the set N of null sequences is a maximal ideal. Thus the ring $\mathbb{Q}_p = C/N$ is a field, the field of p-adic numbers. It has a subring $\mathbb{Z}_p$ formed of Cauchy sequences of integers modulo null sequences.

Note that we can embed $\mathbb{Q}$ into $\mathbb{Q}_p$ by sending $a \in \mathbb{Q}$ to the Cauchy sequence $a, a, a, \ldots$; this embedding respects the ring structure, so $\mathbb{Q}$ is a subfield of $\mathbb{Q}_p$, and $\mathbb{Z}$ is a subring of $\mathbb{Z}_p$.

A nice feature of the p-adic topology is the fact that a sequence $\sum a_n$ converges in $\mathbb{Q}_p$ if and only if (a_n) is a null sequence with respect to $|\cdot|_p$: this is a consequence of the stronger version of the triangle inequality.

Note that the p-adic absolute value $|\cdot|_p$ can be extended to the completion $\mathbb{Q}_p$ by setting

$$|a_{-N}p^{-N} + \ldots + a_0 + a_1 p + \ldots|_p = p^N;$$

this clearly agrees with $|\cdot|_p$ on $\mathbb{Q}$.

The elements $u \in \mathbb{Z}_p$ with $|u|_p = 1$ are exactly the units; the set of elements divisible by p form a maximal ideal $p\mathbb{Z}_p$ in $\mathbb{Z}_p$, and we have $\mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{Z}/p\mathbb{Z}$.