Integration Workshop 2003
Project on Constructing the p-adic Numbers

Douglas Ulmer

For each prime number p there is a field of p-adic numbers, denoted $\mathbb{Q}_p$, which is complete with respect to a certain absolute value. Essentially any question that makes sense for the real numbers also makes sense for $\mathbb{Q}_p$ and in particular one can develop a calculus of functions $f : \mathbb{Q}_p \to \mathbb{Q}_p$. One of the prevalent ideologies of modern number theory is that if one wants to study $\mathbb{Q}$, one should first study $\mathbb{R}$ and all the fields $\mathbb{Q}_p$ ($p = 2, 3, 5, \dots$) in parallel.

This project gives two constructions of $\mathbb{Q}_p$ and then proves that they give the same object.

1 Inverse limit construction

1.1

An *inverse system* of rings (groups, vector spaces, ...) is a collection of rings R_n for $n = 1, 2, 3, \dots$ together with ring homomorphisms $\phi_n : R_n \to R_{n-1}$. The *inverse limit* of such a system is by definition

$$R = \{(a_n)_{n\in\mathbb{Z}_+} | \phi_n(a_n) = a_{n-1} \text{ for all } n\} \subset \prod_n R_n.$$

In other words, it is the set of all compatible systems of elements $a_n \in R_n$, where "compatible" is determined by the ϕ_n.

We make R into a ring in the natural way: $(a_n) + (b_n) = (a_n + b_n)$ and $(a_n)(b_n) = (a_n b_n)$. Prove that this does indeed make R into a ring. There are natural homomorphisms $\psi_n : R \to R_n$ for all n; if you know about "universal properties" you can show that R and the homomorphisms ψ_n satisfy a certain universal property which characterizes them uniquely.

Two somewhat trivial examples: fix a ring R_0 and set $R_n = R_0$ for all $n \geq 1$. If $\phi_n = 0$ for all n, the inverse limit is 0; if we set $\phi_n = id$ for all n, then the inverse limit is just R_0. See below for a more interesting example.

1.2

Now assume that R_n is finite for all n. Define a topology on R by declaring that the sets $\psi_n^{-1}(a_n)$ for every $n \in \mathbb{Z}_+$ and every $a_n \in R_n$ are a basis for the

topology. Check that this is a legitimate definition. The resulting topology on R is called the *profinite topology*.

Prove that R with its profinitie topology is compact and totally disconnected (i.e., the connected components are points).

1.3

Let p be a prime number and apply the above with $R_n = \mathbb{Z}/p^n\mathbb{Z}$ and $\phi_n : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^{n-1}\mathbb{Z}$ the natural projection. The resulting ring R is denoted $\mathbb{Z}_p$ and is called the ring of p-adic integers. Prove that $\mathbb{Z}_p$ is an integral domain, in fact a principal ideal domain, and that every ideal in $\mathbb{Z}_p$ is of the form $p^e\mathbb{Z}_p$.

Where does p being prime matter?

1.4

Define $\mathbb{Q}_p$ by $\mathbb{Q}_p = \mathbb{Z}_p[1/p]$, or more formally, $\mathbb{Q}_p = \mathbb{Z}_p[x]/(xp-1)$. Topologize $\mathbb{Q}_p$ by requiring that the sets $a + p^e\mathbb{Z}_p$ ($a \in \mathbb{Q}_p$, $e \in \mathbb{Z}$) form a basis for the topology. Prove that $\mathbb{Q}_p$ is a topological field and that $\mathbb{Z}_p$ is its maximal compact subring.

2 Completion construction

2.1

Let X be a metric space, i.e., a set with a distance function $d(x, y)$. Recall that this means that $d(x, y) = 0 \Leftrightarrow x = y$, $d(x, y) = d(y, x)$ and $d(x, y) + d(y, z) \geq d(x, z)$. A *Cauchy sequence* in X is a sequence of points $x_1, x_2, x_3, \ldots$ such that for every $\epsilon > 0$ there exists an integer N such that $d(x_m, x_n) < \epsilon$ for all $m, n > N$.

Two Cauchy sequences (x_n) and (y_n) are *equivalent* if for every $\epsilon > 0$ there exists an integer N such that $d(x_n, y_n) < \epsilon$ for all $n > N$. Note that this is indeed an equivalence relation.

The *completion* of X (with respect to d) is by definition the set of equivalence classes of Cauchy sequences in X. Prove that d induces a natural distance function on the completion and that the map which sends an element of X to the "constant" Cauchy sequence gives an isometric embedding of X into its completion.

2.2

Suppose that X is a field (ring, group ,...) and the distance function comes from an absolute value on X (so $d(x, y) = |x - y|$ where $|\cdot|$ satisfies $|x| = 0 \Leftrightarrow x = 0$, $|x + y| \leq |x| + |y|$, and $|xy| = |x||y|$). Show that the completion is a field too and the map from X to its completion is a field homomorphism.

2.3

The completion of $\mathbb{Q}$ with respect to the usual absolute value is the real numbers. But there are other interesting possibilities for $|\cdot|$. Define the *p-adic absolute value* on $\mathbb{Q}$ by

$$\left|\frac{a}{b}\right| = p^{v_p(b)-v_p(a)}$$

where for an integer n, $v_p(n)$ is the power to which p divides n. In other words, $n = p^{v_p(n)}n'$ where $n' \in \mathbb{Z}$ and p does not divide n'.

Prove that the p-adic absolute value is indeed an absolute value. In fact, it satisfies a strong form of the triangle inequality, namely $|x+y| \leq \max(|x|,|y|)$, with equality if $|x| \neq |y|$. This is called the non-archimedean triangle inequality.

The non-archimedean triangle inequality has some strange consequences. For example, any point in a ball can serve as the center and every triangle is isoceles.

It is a theorem that up to a natural notion of equivalence the only absolute values on $\mathbb{Q}$ are the usual one and the p-adic ones.

2.4

Applying the general machinery of completions to $X = \mathbb{Q}$ with its p-adic distance, we get a field $\mathbb{Q}_p$ together with an absolute value satisfying the non-archimedean triangle inequality. Prove that $\mathbb{Q}_p$ is totally disconnected.

$\mathbb{Q}_p$ is a fun place to do calculus. For example, you can check that a series converges in $\mathbb{Q}_p$ if and only if its terms tend to 0!

Define $\mathbb{Z}_p$ to be the closure of $\mathbb{Z}$ in $\mathbb{Q}_p$ with respect to the metric topology. Prove that $\mathbb{Z}_p$ is the maximal compact subring of $\mathbb{Q}_p$ and that $\mathbb{Z}_p = \{x \in \mathbb{Q}_p | \, |x| \leq 1\}$.

3 Comparing the constructions

3.1

Prove that there is a (unique) field isomorphism between the two versions of $\mathbb{Q}_p$ such that the profinite topology on the inverse limit construction corresponds to the metric topology on the completion construction. Also, the two definitions of $\mathbb{Z}_p$ agree.

Either construction can be used to show that $\mathbb{Q}_p$ is a locally compact topological field. It's a theorem that the only locally compact topological fields are finite extensions of $\mathbb{R}$ (i.e., $\mathbb{R}$ and $\mathbb{C}$) and finite extensions of $\mathbb{Q}_p$. (Extensions of $\mathbb{Q}_p$ come in all degrees though.)

3.2

Just as one rarely thinks of real numbers as equivalence classes of Cauchy sequences, one rarely thinks of p-adic numbers that way or in terms of inverse

limits. Here is a convenient way to think of them:

Prove that every p-adic number can be written uniquely as a series of the form $\sum_n a_n p^n$ where $a_n \in \{0, 1, \ldots, p-1\}$ for all $n \in \mathbb{Z}$ and $a_n = 0$ for $n \ll 0$.

(Note that every real number can be written in a similar way, but where $a_n = 0$ for all $n \gg 0$. Also for reals, there is no need for p to be prime ... $p = 10$ is the standard choice for humans!)

3.3

There are also useful "Cantor set type" ways to think about the p-adics. Ask Fred Leitner about the Sierpinski triangle and $\mathbb{Z}_3$.