p-Adic Fields and the Isomorphism $\mathbb{Q}_p^* \simeq \mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$ for $p \neq 2$.

Juraj Milcak
University of Toronto
MAT477
Instructor: Prof. Milman

January 26, 2012

The ring of p-adic integers $\mathbb{Z}_p$, for a prime p:

$\forall n \in \mathbb{N}$, $A_n := \mathbb{Z}/p^n\mathbb{Z}$ and $\phi_n : A_n \to A_{n-1}$with $\ker(\phi_n) = p^{n-1}A_n$.

Def. $\mathbb{Z}_p := \varprojlim (A_n, \phi_n)$ is the 'projective limit' of the system

$$\cdots \to A_n \to A_{n-1} \to \cdots \to A_1 \ .$$

The story of $\mathbb{Q}_p$, the field of p-adic numbers

Also, write $x \in \mathbb{Q}$ as $x = p^n \frac{a}{b}$, $n \in \mathbb{Z}$, $p \nmid ab$. Define a *norm* on $\mathbb{Q}$

by $|x|_p := p^{-n}$. $\mathbb{Q}_p$ is a *completion* of $\mathbb{Q}$ with respect to $|.|_p$.

Any p-adic number α can be written in the form $\sum_{k=d}^{N} a_k p^k$,

and $\alpha \in \mathbb{Z}_p$ iff $d \geq 0$ and $\alpha \in \mathbb{Q}$ iff $N < \infty$.

Can view $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\},\ \mathbb{Q}_p = (\mathbb{Z}_p)$.

The remarkable *Ostrowski's theorem* (1916):

The only norms on $\mathbb{Q}$ are the absolute value and p-adic norms.

Thus $\mathbb{R}$ and $\mathbb{Q}_p$ for p a prime are the only completions of $\mathbb{Q}$

in which $\mathbb{Q}$ is locally compact.

Prop. 1: Sequences $0 \to \mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p \xrightarrow{\pi_n} A_n \to 0$ are exact.

Pf. Multiplication by p is injective in $\mathbb{Z}_p$; clearly $p^n\mathbb{Z}_p \subset \ker(\pi_n)$,

to show $p^n\mathbb{Z}_p = \ker(\pi_n)$: if $x \in \ker(\pi_n)$, construct y s.th. $x = p^n y$.

Thus we can make the identification $\mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p^n\mathbb{Z}$.

Prop. 2: $x \in U := \mathbb{Z}_p^* \Leftrightarrow p \nmid x$.

Remark A: $\forall x \in U \; \exists! \; x = p^n u$ for $u \in U, n \in \mathbb{Z}^+$.

Pf. of P2: Enough to show for $x_n \in A_n$: if $x_n \notin pA_n$, the image

of x_n in $A_1 = \mathbb{F}_p$ is $\neq 0$, so x_n is invertible $\Rightarrow \exists\ y, z \in A_n$ s.th.

$xy = 1 - pz \Rightarrow xy(1 + pz + \cdots + p^{n-1}z^{n-1}) = 1$, so $x \in U$. $\square$

Remark B: Define $v_p(x) := n$, clearly $v_p(.)$ is a valuation:

$v_p(xy) = v_p(x) + v_p(y)$, $v_p(x + y) \geq min\{v_p(x), v_p(y)\}$;

put $v_p(0) = \infty \Rightarrow \mathbb{Z}_p$ is an integral domain.

The field $\mathbb{Q}_p = \mathbb{Z}_p[p^{-1}]$

Write $x \in \mathbb{Q}_p^\times$ uniquely as $p^n u$ with $u \in U$ & $v_p(x) \geq 0$ iff $x \in \mathbb{Z}_p$.

Define a topology on $\mathbb{Q}_p$ by $d(x, y) = e^{-v_p(x-y)}$.

The metric d is *ultrametric*: $d(x, z) \leq max\{d(x, y), d(y, z)\}$.

A bit more about projective limits:

Lemma 1: Let $D := \lim\limits_{\leftarrow} [D_n \to D_{n-1}]_{n \geq 2}$, where D_i are sets.

If each D_n is finite and non-empty, then $D \neq \emptyset$.

Remark C. If each $D_n \to D_{n-1}$ is surjective $\Rightarrow$ $D \neq \emptyset$ is direct.

Proof: Let $D_{n,k}$ be the image of D_{n+k} in D_n $\Rightarrow$ $D_{n,k}$ is

independent of k for k large. Let $E_n = \lim_k D_{n,k}$.

$\Rightarrow$ $D_n \to D_{n-1}$ maps E_n *onto* E_{n-1},

$\Rightarrow$ $\varprojlim E_n \neq \emptyset$ $\Rightarrow$ $\varprojlim D_n \neq \emptyset$, by the remark. $\square$

p-Adic equations: equivalence of solutions in A_n^m and $\mathbb{Z}_p^m$

If $f \in \mathbb{Z}_p[\overrightarrow{x}]$, let $[f]_n \in A_n[\overrightarrow{x}]$ denote the reduction mod p^n of f.

Prop. 3: Let $f_i \in \mathbb{Z}_p[\overrightarrow{x}] \Rightarrow f_i$ have a common zero in $\mathbb{Z}_p^m$ iff

for all integers $n \geq 1$, $[f_i]_n$ have a common zero in A_n^m .

Pf. Let D and D_n be the set of common zeroes of the f_i and $[f_i]_n$

$\Rightarrow D_n$ are finite and we have $D = \varprojlim D_n \overset{Lemma}{\Rightarrow} D \neq \emptyset$ iff $D_n \neq \emptyset$.

Lemma 2: $0 \to A \to E \to B \to 0$, exact seq. of comm.

groups; $|A| = a, |B| = b$, $(a, b) = 1$. Let $B' = \{x \in E : bx = 0\}$.

Then $E = A \oplus B'$ and $B' \simeq B$ is the only such subgroup of E.

Pf. $(a, b) = 1 \Rightarrow \exists r, s \in \mathbb{Z}$ s.th. $ar + bs = 1$. Let $x \in A \cap B' \Rightarrow$

$ax = bx = 0 \Rightarrow (ar + bs)x = x = 0 \Rightarrow A \cap B' = 0$.

For $x \in E$ write $x = arx + bsx$. $bB' = 0 \Rightarrow bE \subset A \Rightarrow bsx \in A$

$abE = 0 \Rightarrow arx \in B' \Rightarrow E = A \oplus B'$ and $E \to B \Rightarrow B' \simeq B$. $\square$

The group $U := \mathbb{Z}_p^*$:

For $n \geq 1$, put $U_n = 1 + p^n\mathbb{Z}_p = \ker(\pi_n : U \to A_n^*)$.

The map $(1 + p^n x) \to x \pmod{p}$ is an isom. $U_n/U_{n+1} \to \mathbb{Z}/p\mathbb{Z}$

(follows from $(1 + p^n x)(1 + p^n y) \equiv 1 + p^n(x + y) \pmod{p^{n+1}}$).

Then by induction on n, one can show that U_1/U_n has order p^{n-1}.

Prop. 3: $U = V \times U_1$ where $V = \{x \in U | x^{p-1} = 1\}$

Proof. We apply the lemma to the exact sequences:

$$1 \to U_1/U_n \to U/U_n \to \mathbb{F}_p^* \to 1 \ .$$

$\Rightarrow$ U/U_n contains a unique subgroup V_n isomorphic to $\mathbb{F}_p^*$.

The projection $U/U_n \to U/U_{n-1}$ takes V_n to V_{n-1}.

By passing to the limit, $\exists!$ subgroup $V \in U$ s.th $V \simeq \mathbb{F}_p^*$. $\square$

Corollary. The field $\mathbb{Q}_p$ contains the $(p-1)$-th roots of unity.

Lemma 3: $x \in U_n - U_{n+1} \Rightarrow x^p \in U_{n+1} - U_{n+2}$.

Let $x = 1 + kp^n$ with $k \not\equiv 0 \pmod p$ $\xrightarrow{\textit{Binomial formula}}$

$$x^p = 1 + \binom{p}{0} kp^n + \cdots + k^p p^{np}.$$

The exponents in the not written terms are $\geq 2n+1$, thus $\geq n+2$.

$\Rightarrow x^p \equiv 1 + kp^{n+1} \pmod{p^{n+2}} \Rightarrow x^p \in U_{n+1} - U_{n+2}$. $\square$

Remark D. The proof works for $p = 2$ as long as $n \geq 2$, in what follows the the case $p = 2$ requires a slight modification.

Prop. 4: $p \neq 2 \Rightarrow U_1 \simeq \mathbb{Z}_p$.

Let $\alpha \in U_1 - U_2 \overset{Lemma}{\Rightarrow} \alpha^{p^i} \in U_{i+1} - U_{i+2}$.

Let α_n be the image of α in $U_1/U_n \Rightarrow (\alpha_n)^{p^{n-2}} \neq 1$, $(\alpha_n)^{p^{n-1}} = 1$.

Since $|U_1/U_n| = p^{n-1}$, it is cyclic $\Rightarrow \langle \alpha_n \rangle = U_1/U_n$.

Define $\theta_{n,\alpha} : \mathbb{Z}/p^{n-1}\mathbb{Z} \to U_1/U_n$ by $z \mapsto \alpha_n^z$. The diagram:

$$\begin{tikzcd}
\mathbb{Z}/p^n\mathbb{Z} \arrow[r, "\theta_{n+1,\alpha}"] \arrow[d] & U_1/U_{n+1} \arrow[d] \\
\mathbb{Z}/p^{n-1}\mathbb{Z} \arrow[r, "\theta_{n,\alpha}"] & U_1/U_n
\end{tikzcd}$$

is commutative. The $\theta_{n,\alpha}$ define an isomorphism $\theta : \mathbb{Z}_p \xrightarrow{\sim} U_1$. $\square$

Finally, as a result of Prop. 3 and Prop. 4 we get:

Theorem. $\mathbb{Q}_p^* \simeq \mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$ for $p \neq 2$.

Any $x \in \mathbb{Q}_p^*$ can be written as $x = p^n u$ with $n \in \mathbb{Z}, u \in U$.

$\Rightarrow \mathbb{Q}_p^* \simeq \mathbb{Z} \times U \overset{Prop.3}{\Rightarrow} U \simeq V \times U_1$ where V is cyclic of order $p-1$.

By Prop. 4, $U_1 \simeq \mathbb{Z}_p$, and the theorem follows. $\square$