1 Lesson 5, 20/10/13 - P-adic numbers

1.1 Defining p-adic numbers

P-adic number are different from "regular" numbers first of all by their absolut value. While $\mathbb{R}$ is constructed as a completion of $\mathbb{Q}$ with respect to the usual absolut value, P=adic numbers are created from $\mathbb{Q}$ with respect to another absolut value. Let us recall what absolut value is.
Given a field F, absolut value is a function $|\ | : F \to \mathbb{R}^+$ that applies:

1. The triangle inequality : $|x+y| \leq |x| + |y|$
2. $|x||y| = |xy|$
3. $|x| = 0 \Leftrightarrow x = 0$

Examples for absolut values can be:

- The trivial absolut value, as we know it - $|\ |_\infty$
- The standard absolut value: $|\ |_0 = \begin{cases} 0 & 0 \\ 1 & not\ 0 \end{cases}$
- The p-adic absolut value $|\ |_p$

First, we shall explain the p-adic absolut value on prime numbers.
For a prime number p, $|p|_p = \frac{1}{p}$
For two different prime numbers p, q, $|q|_p = 1$.
For $|m|_p = |q_1^{r_1} q_2^{r_2} \cdots q_k^{r_k} p^{r_p}| = \frac{1}{p^{r_p}}$
For (a,p)=(b,p) = 1 (greatest common divisor) $|p^n \frac{a}{b}|_p = p^{-n}$
Let's check the triangle inequality - for (a,p)=(b,p)=(c,p)=(d,p)=1, and assuming $n \leq k$, then
$|p^n \frac{a}{b} + p^k \frac{c}{d}|_p = |p^n|_p|\frac{a}{b} + p^{k-n}\frac{c}{d}|_p = p^{-n}|\frac{ad+p^{k-n}cd}{bd}|_p = p^{-n}|ad + p^{k-n}cd|_p = p^{-n}|\frac{ad+p^{k-n}cd}{ad}|_p = p^{-n}|1 + p^{k-n}\frac{c}{a}|_p \leq p^{-n}$, as the g.c.d's of a,b,c,d and p are 1, and as $k \geq n$.
Actually, what we found is another character of the p-adic absolut value - it is a non-Archimedean absolut value, meaning $|x+y|_p \leq max(|x|_p, |y|_p)$ which means, in turn, that $|x|_p \neq |y|_p \Rightarrow |x+y|_p = max(|x|_p, |y|_p)$
In Arcimedean absolut values, for some given x,y, there exists some n for which $|x + x + ... + x|(n\ times) \geq |y|$, and that character does not apply in non-Archimedean absolut values. As those characters do not cover all options, we might find some absolut values which are not Archimedean and not non-Archimedean.

- $Ex1^*$: Prove the Ostrowsky(?) theorem - For a given absolut value $|\ |_\alpha$ **over** $\mathbb{Q}$, one of the following occurs:
  - $|\ |_\alpha \sim |\ |_\infty$

- $| \ |_\alpha \sim | \ |_p$
- $| \ |_\alpha \sim | \ |_0$

where $\sim$ means space topology equivalence.

- $Ex2$: The following exists generally:
  $| \ |_\alpha \sim | \ |_\beta \Leftrightarrow \exists c : | \ |_\alpha^c = | \ |_\beta$
  ($| \ |_\alpha^c$ means $| \ |_\alpha$ to the power of c)

Definition : This completion is denoted by $\mathbb{Q}_\mathbf{p} = \widehat{\mathbb{Q}_{| \ |_p}}$
Notice, that just like $\mathbb{R}$, this completion is not algebraicly closed.

We can write p-adic numbers based on a p-adic absolut value, where $n \neq 2$, and we'll get numbers with finite number of digits to the right of the point, and infinite number of digits to the left of the point, like that:

- $Ex3$: Prove that $\mathbb{Q}_p = \{...x_{-n}...x_0.x_1...x_k | x_i \in \{0, 1, ..., p-1\}\}$. (You should show that the sum $x_k p^{-k} + ... + x_1 p^{-1} + x_0 + x_{-1} p + ... + x_{-n} p^n ...$ converges into that number according to the $| \ |_p$ absolute value)

Therefore, when you replace p with some other prime number, you'll get different results. It should be noted that by choosing p=2, we encounter the "problem" of the lack of a single result, meaning, each number can be displayed by more than one p-adic number. This also happens in $mathbbR$ but do not in other than 2 p-adic numbers.

1.2 Another Differences between p-adic numbers and real numbers

Another differences between real and p-adic numbers will be shown in the following exercises:

- $Ex4$: Prove: for a sequence $\{a_i\} \subseteq \mathbb{Q}_p$, $|a_i|_p \to 0 \Leftrightarrow \Sigma a_i \ conv.$
- $ex5$: Prove that in p-adic numbers, balls do not have centers - $B(x, r) = B(y, r) \forall y \in B(x, r)$.
- $Ex6$: Prove that $\forall r \exists r'$ and $\forall r' \exists r$ such that $B_o(x, r) = B_c(x, r')$ where B_o means an open ball (all the points with distance up to r without r) and B_c mean a closed one (all points up to r and r included).
- $Ex7$: Prove that for each two p-adic balls, if they are not distinct, then one of them contains the other: $B(x, r) \cap B(x', r') \neq \emptyset \Rightarrow (B(x, r) \in B(x', r') \ or \ B(x', r') \in B(x, r))$

Def: $\mathbb{Z}_p = B_{\mathbb{Q}_p}(0,1)$. Meaning - all the numbers with no digits to the right of the point are in the unit circle.
Notice, that unlike real numbers, $\forall x, y \in \mathbb{Z}_p,\ x + y \in \mathbb{Z}_p$.
In the case of $p = 2$ we'll get $B_o(0,1) = B_c(0, \frac{1}{2})$. In this case, we'll have the unit ball, which is constructed out of two balls - the one where the last digit to the left of the point is 0. and the other, where that digit is 1. Each of these balls is made of two other balls, one with the digit previous to the last is 0, and the other where this digit is 1. In other p's, there are p balls within each balls. In that sense, the p-adic integers are homomorphic to the Cantor set.

- $Ex8$: $\mathbb{Z}_p \approx Cantor\ set$ where $\mathbb{Z}_p$ has the topology induced from $\mathbb{Q}_p$ and the Cantor set has the topology induced by the real numbers.

Conclusion - $\mathbb{Z}_p$ is a compact set.

1.3 Inverse limits

Let $A_1 \leftarrow A_2 \leftarrow A_3 \leftarrow ...$ equiped with homomorphisms
Def: Inverse limit of Abelian groups is defined by:

$$\varprojlim_{i \in i} A_i = \{\overrightarrow{a} \in \prod_{i \in I} A_i | a_i = f_{ij}(a_j)\ \forall i \leq j\ in\ I\}$$

Where f_{ij} is a homomorphism from A_j to A_i, where $j > i$, and $f_{ik} = f_{ij} \circ f_{jk}\ \forall i \leq j \leq k$.

- $Ex9$: Prove that $\varprojlim \mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p$
- $Ex10$: Prove that $\mathbb{Q}_p \simeq$ Cantor set - $\{1\}$ (topologically homomorphisms)
- $Ex11a$: Prove that $\mathbb{Q}_p^n \simeq \mathbb{Q}_p$
- $Ex11b$: For an open set $U \subset \mathbb{Q}_p^n$ then either $U \simeq$ Cantor set, or $U \simeq$ Cantor set-$\{1\}$ (topologically homomorphism).

1.4 Haar measure and local fields

For every group G - locally compact, there is a unique measure, invariant to translations up to a scalar multipliction.
Haar Thm: $\forall G$ locally compact
(1) $\forall g \in G,\ \ \exists \mu \in C_c(G)^* - 0\ s.t.\ < \mu, gf > = < \mu, f >\ where\ gf(x) = f(g^{-1}x)$
(2) If μ, μ' are as in (1), then $\exists \alpha\ s.t.\ \mu = \alpha\mu'$

- $Ex12$: Prove Haar theorem for $G = \mathbb{Q}_p$

hint: first define μ on basic open sets - balls. Define $\mu(B(0,1)) \equiv 1$ and get that $\mu(B(x,p)) = p$, since $B(0,p)$ can be covered distinctivly by p unit balls. In addition, you need to show that if μ is a Haar measure and $\mu(B(0,1)) = 0$ then $\mu = 0$.

So, let us define
Def: $\mu_a(B) = \mu(aB)$ for μ a Haar measure.

By the exercise $\mu_a = \alpha(a)\mu$ and $\alpha(a)$ does not depend on the original measure.

- $Ex13$: Show that $\alpha(a) = |a|_p$

hint: Choose B to be the unit ball. and compare measures (we know that this is enough since μ, μ_α) are Haar measures and therefore one is a scalar multipliction of the other).

Def: Local Field Local field is a topological field which is locally compact and non-descrete.
Examples for such fields may be $\mathbb{Q}_p$, $\mathbb{R}$, $\mathbb{C}$ and another one is the formal Laurent series over the p-adics - $L_q((t)) = \{\sum_{n=-m}^{\infty} a_n t^n\}$ where q may be some power of p.
There is a complex theorem which states that those are all the options for locally field. We shall not go all over it, but the main points are as follows:
(1) - Define the measure on G using $\mu \in C_c(g)^*$
use the Haar thm - you can define absolut value, up to scalar multipliction - $\exists\alpha(a),\ \mu_a = \alpha(a)\mu \to |a| \equiv \alpha(a)$
(2) - prove that every local field has a norm, which defined as a scalar multipliction of Haar measure (notice - $\mathbb{R}, \mathbb{C}$ have it a bit differently due to differnt volumes of unit balls)
(3) - prove that every compact metric space is complete
(4) - every local field includes $\mathbb{Q}$ and its completion
(5) - for $char(F) \neq 0$ show that there exists a transendental element, name it t, and show that it is $F_q((t))$.
(6) - show this field is an algebraic extension of finite dimension.

- $BigBonusEx$!! - prove this theorem completely and get up to 5 points to the course's grade!!

1.5 l-spaces

Our goal here is to reach the notion of distributions over varieties. The closest object in the p-adic theory for a valiety is an element called l-space.
Def: l-space: A topological space X will be called a l-space if:

1. X is Hausdorff
2. X has a basis of open compact sets

Here, open sets tend to be closed as well, hence, we can talk about open compact sets.
therefore, the p-adic line, and spaces based on $\mathbb{Q}_p$ are l-spaces.
Example - every non-Archimedean local field is a l-space.

- $Ex14$: open/closed subset of a l-space, is a l-space itself

Def: locally closed set: $U \subseteq X$ is locally closed, if $\forall p \in U,\ \exists V \subset X\ \ p \in V s.t.\ U \cap V$ is a closed set in X.
Example - an open set in the regular topology is locally closed.
Example - every affine variety over $\mathbb{Q}_p$ is a l-space.

Def: Refinement of a cover $\bigcup U_i = X$ is $\{V_j :\ \forall j \exists i,\ V_j \subseteq U_i\}$ and $\bigcup V_i = X$
Thm: Every cover has a compact disjoint open refinement.
We'll prove over 2 sets, from there, inductively, applies to the whole cover - let U_1, U_2 be open compact sets. The set $U_1 - U_2$ is open compact set itself. $U_1 - U_2$ and U_2 form a distinct cover.

- $Ex15^*(half\ star)$: find a l-space X which is countable at ∞ and an open subset $U \subset X$ that is not countable at ∞.

hint: X is not metrizable.

- $Ex16$: let us have 2 more axioms: 1. X is a metrizable l-space, 2. X is countable at ∞. Then for every open/closed subset in X is also metrizable and countable at ∞

- $Ex17^*(half\ star)$: every l-space metrizable and countable at ∞ space X, is isomorphic to 1 of the 3 spaces:

  1. Cantor set
  2. Cantor set-$\{1\}$
  3. X is a discrete set and - $\begin{cases} |X| < \infty \\ or \\ |X| = \aleph_0 \end{cases}$