# 6370-001 - FALL 2021 - WEEK 8 (10/19, 10/21)

**Exercise 0.**

(1) Show any $x \in \mathbb{Q}_p$ can be expressed uniquely as $\sum_{k=-N}^{\infty} a_k p^k$ for $a_k \in \{0, 1, \dots, p-1\}$.
(2) Express $-1$ in this way.

**Exercise 1.** Let $K$ be a field with an absolute value $|\cdot|$. Recall that $|\cdot|$ is called *non-archimedean* if there exists $C > 0$ such that $|m| \le C$ for all $m \in \mathbb{Z}$ (using the natural map $\mathbb{Z} \to K$).

(1) Show that $|\cdot|$ is non-archimedean if and only if the *strong triangle inequality* holds:
$$|x + y| \le \max(|x|, |y|)$$
(2) Show that $|\cdot|$ is non-archimedean and $|x| \ne |y|$ then
$$|x + y| = \max(|x|, |y|).$$
(3) Generalize (1) and (2) to $|\sum_{i=1}^{N} x_i|$.

**Exercise 2 (Similar to Milne 7-2).** Let $K$ be a field with a non-archimedean absolute value $|\cdot|$.

(1) Show that the set of elements in $K$ of absolute value $\le 1$ is a subring (called the valuation ring of $|\cdot|$). Why doesn't this hold for an archimedean absolute value?
(2) We can define a norm on the vector space $K^n$ by $\|(a_1, \dots, a_n)\| = \max(|a_1|, \dots, |a_n|)$. Show that "any point in a ball in $K^n$ is its center." (part of the exercise is to make sense what this means! This is already interesting when $n = 1$, so feel free to treat just that case).
(3) *The freshman's dream.* If $K$ is complete, then for $a_n$ a sequence in $K$, show that the series $\sum_{n=0}^{\infty} a_n$ converges if and only if $\lim_{n\to\infty} a_n = 0$.

**Exercise 3.** Let $K$ be complete with respect to a non-archimedean absolute value $|\cdot|$ and $\mathrm{char} K = 0$.

(1) What are the possible restrictions of $|\cdot|$ to $\mathbb{Q} \subseteq K$? (Hint: Ostrowski's theorem).
(2) For which $x \in K$ does $\log(1 + x)$ converge, where
$$\log(1 + x) := x - \frac{x^2}{2} + \frac{x^3}{3} + \dots$$
(3) For which $x \in K$ does $\exp(x)$ converge, where
$$\exp(x) := 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots$$
(4) Show that exp and log are inverse functions when they are defined, i.e.
$$\exp(\log(s)) = s \text{ and } \log(\exp(t)) = t.$$
for values of $s$ and $t$ where these make sense (what values are these?).

**Exercise 4.** If you know a little bit of functional analysis, prove that if $\mathbb{C} \subseteq K$ and $K$ is complete for an absolute value extending the standard absolute value on $\mathbb{C}$, then $\mathbb{C} = K$. *Hint: $K$ is a Banach space; what do you know about the spectrum of a bounded operator on a complex Banach space?.*
(No analogous statement holds for non-archimedean absolute values – in particular, there is no "biggest" complete algebraically closed field containing $\mathbb{Q}_p$. This fact is one reason that $p$-adic analytic geometry behaves like a mixture of complex analytic geometry and algebraic geometry).

**Exercise 5.** Consider the following result:

**Theorem** (Weak Approximation). *Let $|\cdot|_1, |\cdot|_2, \dots, |\cdot|_n$ be nontrivial inequivalent absolute values on a field $K$, and let $a_1, \dots, a_n$ be elements of $K$. For any $\epsilon > 0$, there is an element $a \in K$ such that $|a - a_i|_i < \epsilon$ for all $1 \le i \le n$.*

(1) (Similar to Milne 7-1) Suppose $A$ is a Dedekind domain, $K = \mathrm{Frac}(A)$, and $|\cdot|_i$ are all absolute values that come from distinct primes of $A$. Prove the weak approximation theorem in this case by using the Chinese Remainder Theorem.
(2) Prove the Weak Approximation theorem (if you get stuck this follows a section in Milne):
  (a) First show there is an element $a$ such that $|a|_1 > 1$ and $|a|_i < 1$ for $i \neq 1$.
  (b) Use this to construct an element $a$ with $|a-1|_1$ close to 0 and $|a|_i$ close to zero for $i \neq 1$.
  (c) Conclude.

**Exercise 6.** We have the following important results on roots and factorization:

**Theorem** (Simple Hensel's lemma for roots). *Let $A$ be a complete DVR with residue field $\kappa$ (e.g. $A = \mathbb{Z}_p$ or $A = \kappa[[t]]$). For $f \in A[x]$, write $\overline{f}$ for the image in $\kappa[x]$ by reducing all the coefficients modulo the maximal ideal. Show that if there is an $\overline{a} \in \kappa$ such that $\overline{f}(\overline{a}) = 0$ and $\overline{f}'(\overline{A}) \neq 0$, then there is a unique $a \in A$ with reduction $\overline{a}$ such that $f(a) = 0$. In other words, simple roots in $\kappa$ lift uniquely to simple roots in $A$.*

**Theorem** (Strong Hensel's lemma for roots). *Let $K$ be complete for a non-archimedean absolute value $|\cdot|$, and let $A \subset K$ be the valuation subring / unit ball consisting of $k \in K$ with $|k| \le 1$. Suppose $f(x) \in A[x]$ and $a_0 \in K$ is such that $|f(a_0)| < |f'(a_0)|^2$. Show there is a unique root $a$ of $f(x)$ with $|a - a_0| \le |f(a_0)/f'(a_0)|$.*

**Theorem** (Hensel's lemma for factorization). *Let $A$ be a complete DVR with residue field $\kappa$. Suppose $f \in A[x]$ is monic and $\overline{f}(x) = \overline{g}_1(x) \dots \overline{g}_m(x)$ where the $\overline{g}_i(x)$ are pairwise coprime in $\kappa[x]$. Then the factorization lifts uniquely to a factorization $f(x) = g_1(x) \dots g_m(x)$ in $A[x]$.*

(1) What is the relation between these three results? (I.e. which imply which?)
(2) Compute $\mu(\mathbb{Q}_p)$, the group of roots of unity in $\mathbb{Q}_p$. *Hint: Hensel's lemma will do most of the job, but you'll also need an earlier computation for pth roots. Pay attention when $p = 2$!.*
(3) Show that $(x^2-2)(x^2-17)(x^2-34)$ has a root in $\mathbb{Z}_p$ for all $p$ and in $\mathbb{R}$, but has no root in $\mathbb{Q}$.
(4) Prove strong Hensel's lemma for roots (*Hint: use Newton's method.*).
(5) Show that $5x^3 - 7x^2 + 3x + 6$ has a root $\alpha \in \mathbb{Z}_7$ with $|\alpha - 1|_7 < 1$. Find $a \in \mathbb{Z}$ such that $|\alpha - a|_7 < 7^{-4}$.
(6) Prove Hensel's lemma for factorization, or read the proof in Milne (Theorem 7.33).

**Exercise 7.**

(1) Show that for $p$ odd, $\mathbb{Q}_p^\times \cong \mathbb{Z}_p^\times \times p^{\mathbb{Z}} \cong (1 + p\mathbb{Z}_p) \times \mu(\mathbb{Q}_p) \times p^{\mathbb{Z}}$.
(2) What happens for $p = 2$? *Hint: the first identity still holds, but what about the second one?*
(3) Compute $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$. *Hint: use Hensel's lemma or the exponential/logarithm, but pay attention when $p = 2$!.*
(4) How many quadratic extensions of $\mathbb{Q}_p$ are there?
(5) Show $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^n$ is finite for any $p$ and $n$ – in particular, if $\mathbb{Q}_p$ contains the $n$th roots of unity, deduced that there are only finitely many cyclic degree $n$ extensions of $\mathbb{Q}_p$. *Next week we will see that there are only finitely many extensions of any fixed degree of $\mathbb{Q}_p$.*