PMATH 940: p-ADIC ANALYSIS NOTES

HEE-SUNG YANG

ABSTRACT. Electronic version of class notes for PMATH 940: p-adic Analysis.

1. Introduction

1.1. Introduction to valuation.

Definition 1. A map $|\cdot|$ from field K to $\mathbb{R}$ is said to be *a valuation* if

(i) (Positive-semidefinite) For all $a \in K$, $|a| \geq 0$, and $|a| = 0$ iff $a = 0$.
(ii) (Multiplicativity) For all $a, b \in K$, $|ab| = |a| \cdot |b|$.
(iii) There exists $C > 0$ such that for all $a \in K$ with $|a| \leq 1$, then $|1 + a| \leq C$.

Remark 2. (iii) is often replaced by the triangle inequality.

Example 3. The ordinary absolute value $|\cdot|$ on $\mathbb{C}$. In this case, we can take $C = 2$.

Example 4. The p-adic valuation $|\cdot|_p$ on $\mathbb{C}$ is defined in the following manner: Let p be a prime number. Let $\operatorname{ord}_p a$ (for $a \in \mathbb{Z}$) be the largest power of p dividing a. Extend this idea to $\mathbb{Q}$ by putting $\operatorname{ord}_p(a/b) = \operatorname{ord}_p a - \operatorname{ord}_p b$. Now define $|\cdot|_p$ on $\mathbb{Q}$ by letting $|0|_p = 0$ and $|a/b|_p = p^{-\operatorname{ord}_p(a/b)}$. In this case, we can take $C = 1$. Thus p-adic valuation is an example of *a non-Archimedean valuation*, which will be discussed in Section 1.3 in greater detail.

Example 5. Let k be a field and consider $K = k(T)$, where T is transcendental over k. Let $\lambda \in \mathbb{R}$ with $0 < \lambda < 1$. Let $p(T) \in k[T]$ be irreducible. Observe that every non-zero element of K has a representation of the form $h(T) = p(T)^q \frac{f(T)}{g(T)}$ where $q \in \mathbb{Z}$ and $(f, p) = (g, p) = 1$. Note that q is uniquely determined. Define $|\cdot|$ on K by $|0| = 0$ and $|h(T)| = \lambda^q$. Axioms 1(i) and (ii) are immediate. For (iii), note that if $|h| \leq 1$, then $q \geq 0$ so $|1 + h| = \left|1 + p(T)^q \frac{f(T)}{g(T)}\right| \leq 1$. We can take $C = 1$.

Example 6. Let K be any field, and put a valuation $|\cdot|_0$ known as *the trivial valuation*, i.e., $|0|_0 = 0$ and $|a|_0 = 1$ for all nonzero $a \in K$. We can (trivially) take $C = 1$.

Example 7. Let $K = k(T)$ as in Example 5. Let $\gamma \in \mathbb{R}$ with $\gamma > 1$. We define $|\cdot|$ first on $k[T]$. If

$$f(T) = a_0 + a_1 T + \cdots + a_n T^n \quad (a_n \neq 0)$$

and $a_i \in K$ for all i, we put $|f| = \gamma^n$.

Extend this to elements $f(T)/g(T)$ in K with $g \neq 0$ by putting $\left|\frac{f}{g}\right| = \frac{|f|}{|g|}$. As always, $|0| = 0$. One can check that $|\cdot|$ satisfies (iii) with $C = 1$.

Date: 25 November 2014.

1.2. **Properties of valuation.**

(1) $|1| = 1$ (Note that $|1| = |1 \cdot 1| = |1| \cdot |1|$.)
(2) If $|a^n| = 1$, then $|a| = 1$. Note that $|-1| = 1$ and $|-a| = a$ for all $a \in K$.
(3) If $K = \mathbb{F}_p$ then the only valuation on K is the trivial valuation, by (2).
(4) If $|\cdot|$ is a valuation on K and $\lambda \in \mathbb{R}^+$, then $|\cdot|_1$ defined by $|a|_1 := |a|^\lambda$ for all $a \in K$ is also a valuation of K: take $C_1 = C^\lambda$.

Definition 8. If $|\cdot|$ and $|\cdot|_1$ are valuations on a field K, then we say they are *equivalent* if there exists $\lambda \in \mathbb{R}^+$ such that $|a|^\lambda = |a|_1$ for all $a \in K$. This gives us an equivalence class on a field K of valuations, and such an equivalence class of valuations is known as *a place of K*.

Lemma 9. *A valuation $|\cdot|$ on K satisfies the triangle inequality if and only if for all $a \in K$ with $|a| \leq 1$, we have $|1 + a| \leq 2$.*

Proof. ($\Leftarrow$) Suppose $a_1, a_2 \in K$. If $a_1 = 0$ or $a_2 = 0$ then clearly $|a_1 + a_2| \leq 2\max(|a_1|, |a_2|)$. Suppose neither is zero, and without loss of generality, assume $|a_1| \geq |a_2|$. Then $|a_1 + a_2| = |a_1| \cdot |1 + a_2/a_1| \leq 2|a_1| = 2\max(|a_1|, |a_2|)$. Thus, we have $|a_1 + a_2| \leq 2\max(|a_1|, |a_2|)$ for any $a_1, a_2 \in K$. Now apply induction to $a_1, a_2, \dots, a_{2^n}$ to derive

$$|a_1 + a_2 + \cdots + a_{2^n}| \leq 2^n \max(|a_1|, |a_2|, \dots, |a_{2^n}|).$$

Given $a_1, a_2, \dots, a_N \in K$ where N is sufficiently large, we can choose n so that $2^{n-1} < N \leq 2^n$ and define $a_{N+1} = a_{N+2} = \cdots = a_{2^n} = 0$. Then for any $a_1, a_2, \dots, a_N \in K$,

$$|a_1 + a_2 + \cdots + a_N| \leq 2^n \max(|a_1|, |a_2|, \dots, |a_N|) \leq 2N \max_{1 \leq j \leq N}(|a_j|),$$

from which we can take $a_1 = a_2 = \cdots = a_N$ to derive $|N| \leq 2N$. Let $b, c\ inK$ and $n \in \mathbb{Z}_+$. Then

$$\begin{aligned}
|b + c|^n = |(b + c)^n| = \left|\sum_{r=0}^{n} \binom{n}{r} b^r c^{n-r}\right| &\leq 2(n+1)\max_r \left|\binom{n}{r} b^r c^{n-r}\right| \\
&\leq 4(n+1)\max_r \left|\binom{n}{r}\right| |b|^r |c|^{n-r} \quad (\text{since } |N| \leq 2N) \\
&\leq 4(n+1)\sum_{r=0}^{n} \binom{n}{r} |b|^r |c|^{n-r} \\
&\leq 4(n+1)(|b| + |c|)^n.
\end{aligned}$$

Thus, it follows that $|b + c| \leq (4(n+1))^{1/n}(|b| + |c|)$, and letting $n \to \infty$ gives us the triangle inequality.

($\Rightarrow$) This is immediate, since $|1 + a| \leq |1| + |a| \leq 2$. $\square$

Corollary 10. *Every valuation on K is equivalent to a valuation satisfying the triangle inequality.*

1.3. **Non-Archimedean valuation.**

Definition 11. A valuation $|\cdot|$ on a field K is said to be *non-Archimedean* if we can choose $C = 1$ in Definition 1(iii). Otherwise, it is called *Archimedean.*

Remark 12. Observe that *any* valuation equivalent to a non-Archimedean valuation is also non-Archimedean.

Lemma 13. *A valuation on K is non-Archimedean if and only if $|\cdot|$ satisfies the strong triangle inequality for all $a, b \in K$.*

Proof. ($\Rightarrow$) Without loss of generality, suppose $a, b \in K$ with $|a| \leq |b|$. Note that we have $|a+b| = |b(1+\frac{a}{b})| = |b||1+\frac{a}{b}| \leq |b| \cdot |1|$, according to Definition 11. Thus $|a+b| \leq |b| = \max(|a|, |b|)$, as required.

($\Leftarrow$) Again, we assume that $a, b \in K$ with $|a| \leq |b|$. Thus, by the strong triangle inequality, we have $|a+b| = |b||1+\frac{a}{b}| \leq |b|$. This implies that $|1+\frac{a}{b}| \leq 1$ for any $a, b \in K$, so we can choose $C = 1$. Therefore $|\cdot|$ is non-Archimedean. ☐

Lemma 14. *Let $|\cdot|$ be a valuation on a field K. Then $|\cdot|$ is non-Archimedean if and only if $|e| \leq 1$ for all $e \in R_K$, where R_K denotes the ring generated by 1 in K.*

Remark 15. We *cannot assume* that the ring generated by 1 in K is $\mathbb{Z}$, since that is no longer the case if K has a positive characteristic.

Proof. ($\Leftarrow$) Any non-Archimedean valuation is equivalent to a non-Archimedean valuation, and since any non-Archimedean valuation satisfies the triangle inequality, one can replace the original valuation to the one satisfying the triangle inequality. Suppose $e \in R_K$ and $|e| \leq 1$. Apply the triangle inequality:

$$|1+e|^n = |(1+e)^n| \leq \sum_{j=0}^{n} \left| \binom{n}{j} \right| |e| \leq \sum_{j=0}^{n} |a| \leq n+1.$$

Take the n-th root on both sides and let $n \to \infty$ to get $|1+e| \leq 1$ for any $e \in R_K$. Thus we can take $C = 1$, as required.

($\Rightarrow$) This is immediate, since $|1+1| \leq |1|$ by the triangle inequality. Apply induction to derive $|e| \leq 1$ for all multiples of 1. ☐

Corollary 16. *If K and k are fields with $k \subseteq K$, and $|\cdot|$ a valuation on K, then $|\cdot|$ is non-Archimedean on K if and only if its restriction to k is non-Archimedean also.*

Proof. Apply the previous lemma for the $\Leftarrow$ direction. The $\Rightarrow$ direction is immediate. ☐

Corollary 17. *If $|\cdot|$ is a valuation on a field K with* $\operatorname{char} K > 0$, *then $|\cdot|$ is non-Archimedean.*

Proof. This follows from the fact that the only valuation on the finite field $\mathbb{F}_p$ is the trivial valuation, and the trivial valuation is (trivially) non-Archimedean. ☐

2. Ostrowski's Theorem

Theorem 18 (Ostrowski's Theorem)**.** *All non-trivial valuations on $\mathbb{Q}$ is equivalent to either the ordinary absolute value or the p-adic valuation, where p is a prime.*

Proof. Let $|\cdot|$ be a valuation on $\mathbb{Q}$. By Corollary 10 we may assume that $|\cdot|$ satisfies the triangle inequality. Let $b > 1$ and $c > 0$ with $b, c \in \mathbb{Z}$. Write c in terms of b: $c = c_m b^m + c_{m-1} b^{m-1} + \cdots + c_0$, where $c_0, \ldots, c_m$ are taken from $\{0, 1, \ldots, b-1\}$ and where $c_m \neq 0$. Note that $m \leq \log c / \log b$. By the triangle inequality,

$$|c| \leq (m+1) \max_{0 \leq i \leq m} |c_i| \max(1, |b|^m) \leq (m+1) M \max(1, |b|^m)$$

where $M - \max(|1|, \ldots, |b-1|)$. Let $a \in \mathbb{Z}_+$ and put $c = a^n$ for $n \in \mathbb{Z}_+$. Then

$$|a|^n = |a^n| = \left(\frac{n \log a}{\log b} + 1\right) M \max(1, |b|^{\frac{n \log a}{\log b}}).$$

Take n-th roots and let $n \to \infty$:

$$|a| \leq \max(1, |b|^{\frac{\log a}{\log b}}). \tag{1}$$

Suppose first that there is some positive a with $|a| > 1$. Then from (1), we see that $|b| > 1$ for all $b > 1$ with $b \in \mathbb{Z}$. Interchanging the roles of a and b in (1), we see that

$$|a|^{1/\log a} = |b|^{1/\log b}.$$

Thus, there exists a real number λ with $\lambda > 1$ such that for all positive integers a, we have $|a| = a^\lambda$ and hence $|\cdot|$ is equivalent to the ordinary absolute value on $\mathbb{Q}$ (i.e., $|a/b| = |a/b|_\infty^\lambda$, where $|a/b|_\infty$ denotes the ordinary absolute value).

Now suppose that $|a| \leq 1$ for all positive integers a. If $|a| = 1$ for all positive integers a then $|\cdot|$ is the trivial valuation. Thus there is a smallest positive integer a for which $|a| < 1$. Notice that a is a prime by the multiplicative property of valuations.

Let c be an integer such that $p \nmid c$. We can write $c = up + v$ with $v \in \{1, 2, \ldots, p-1\}$. Then $|v| = 1$ since p is the smallest positive integer with valuation less than 1. Furthermore, $|up| = |u| \cdot |p| < 1$. Since $|a| \leq 1$ for all $a \in \mathbb{Z}_+$, we see that $|\cdot|$ is non-Archimedean. Therefore $|c| = |up + v| = |v|$. This means that the valuation on $\mathbb{Q}$ is determined once we know that its value on p. Thus it is equivalent to the p-adic valuation, as desired. $\square$

We will give a criterion for the two valuations on a field K to be equivalent.

Proposition 19. *Let K be a field and let $|\cdot|_1$ and let $|\cdot|_2$ be valuations in K. If $|\cdot|_1$ is not the trivial valuation and for $a \in K$*

$$|a|_1 < 1 \Rightarrow |a|_2 < 1,$$

then $|\cdot|_1$ and $|\cdot|_2$ are equivalent.

Proof. By taking inverse we see that $|a|_1 > 1$ implies $|a|_2 > 1$. Next suppose that $|a|_1 = 1$ and $|a|_2 > 1$. Since our valuation $|\cdot|_1$ is not a trivial valuation, these exists $c \in K \setminus \{0\}$ with $c \neq 0$ and $|c|_1 < 1$. Then for each $n \in \mathbb{Z}_+$ we have

$$|ca^n|_2 = |c|_2 |a^n|_2 > 1 \text{ for } n \text{ sufficiently large.}$$

But $|ca^n|_1 = |c|_1 |a|_1^n < 1$ for all $n \in \mathbb{Z}_+$ and this contradicts our assumption. We thus conclude that $|a|_1 < 1 \Rightarrow |a|_2 < 1$ and $|a|_1 > 1 \Rightarrow |a|_2 > 1$. Since $|\cdot|_1$ is non-trivial there exists a $c \in K$ with $c \neq 0, |c|_1 > 1$. Then $|c|_2 > 1$. Now let $a \in K, a \neq 0$ and define γ by $|a|_1 = |c|_1^\gamma$. Let $m, n \in \mathbb{Z}_+$ with $m/n > \gamma$. Then $|a|_1 < |c|_1^{m/n}$. Hence

$$\left|\frac{a^n}{c^m}\right|_1 < 1 \Rightarrow \left|\frac{a^n}{c^m}\right|_2 < 1.$$

Therefore $|a^n|_2 < |c^m|_2$ so $|a|_2 < |c|_2^{m/n}$.

Similarly if $m/n < \gamma$ we have

$$|a|_2 > |c|_2^{m/n}.$$

Therefore $|a|_2 = |c|_2^\gamma$. Thus $\gamma = \log|a|_1/\log|c|_1 = \log|a|_2/\log|c|_2$ and so

$$\frac{\log|a|_1}{\log|a|_2} = \frac{\log|c|_1}{\log|c|_2}$$

is equal to λ for some $\lambda \in \mathbb{R}, |\lambda| > 0$. Accordingly, $|a|_1 = |a|_2^\lambda$, completing the proof. □

Given any function $|\cdot|$ on a field K satisfying axioms (i) and (ii) in Definition 1 we can use it to define a topology on K. For each $\varepsilon > 0$ and $x_0 \in K$ we defined the fundamental basis of neighbourhoods of x_0 by the inequalities $|x - x_0| < \varepsilon$. Axiom (iii) in Definition 1 ensures that our space is Hausdorff. We can define a metric d on K by putting $d(a, b) = |a - b|$.

Remark 20. The induced topology is the discrete topology whenever $|\cdot|$ is the trivial valuation.

Proposition 21. *Let $|\cdot|_1$ and $|\cdot|_2$ be valuations on a field K. $|\cdot|_1$ and $|\cdot|_2$ induce he same topology on K if and only if they are equivalent.*

Proof. ($\Rightarrow$) We may suppose that both $|\cdot|_1$ and $|\cdot|_2$ are non-trivial valuations on K. Suppose that a in in K with $|a|_1 < 1$. Thus $|a|_1 < 1 \Rightarrow |a|^n|_1 \to 0$ as $n \to \infty$. Since $|\cdot|_1$ and $|\cdot|_2$ induce the same topology , $|a^n|_2 \to 0$. But then $|a|_2 < 1$. The result now follows by Proposition 19. □

Inequivalent valuations on a field K are independent in the following sense:

Proposition 22. *Let $|\cdot|_1, \ldots, |\cdot|_H$ are non-trivial valuations on a field K with pairwise non-equivalence. Then there exists $a \in K$ such that*

$$|a|_1 > 1 \textit{ while } |a|_j < 1$$

for all $2 \leq j \leq H$.

Proof. The proof is via induction on H. Let $H = 2$ (base case). Since $|\cdot|_1$ is not the trivial valuation and $|\cdot|_1$ and $|\cdot|_2$ are not equivalent, there exists some $b \in K$ with $|b|_1 < 1$ and $|b|_2 \geq 1$. Similarly, since $|\cdot|_2$ is non-trivial, there exists $c \in K$ such that $|c|_2 < 1$ and $|c|_1 \geq 1$. Then we can take $a = cb^{-1}$. Notice that $|a|_1 > 1$ and $|a|_2 < 1$.

Suppose that $H > 2$ and the result holds for $j = 2, \ldots, H-1$. Then there exists, by the inductive hypothesis, $b \in K$ with $|b|_1 > 1$ but $|b|_j < 1$ for all $j = 2, \ldots, H-1$. We can also consider $|\cdot|_1$ and $|\cdot|_H$, and by the inductive hypothesis one can find $d \in K$ such that $|d|_1 > 1$ while $|d|_H < 1$.

Notice that if $|b|_H < 1$ we are done, since we can take $a = b$. If $|b|_H = 1$ then we can take $a = b^n d$ for n sufficiently large. If $|b|_H > 1$ we can take $a = \frac{b^n}{1+b^n} d$. a works for sufficiently large n since

$$\frac{b^n}{1+b^n} = \frac{1}{1+b^{-n}} \to \begin{cases} 1 & (|\cdot|_1 \text{ and } |\cdot|_H) \\ 0 & \text{all other valuations} \end{cases}.$$

This completes the proof. □

3. September 25: Approximation theorem and completion

3.1. Approximation theorem.

Theorem 23 (Approximation theorem). *Let $|\cdot|_1, \ldots, |\cdot|_H$ be pairwise inequivalent, non-trivial valuations. Let $b_1, \ldots, b_H \in K$. Let $\varepsilon > 0$ be a positive real number. Then there exists an element $a \in K$ so that $|a - b_i|_i < \varepsilon$ for $i = 1, 2, \ldots, H$.*

Proof. By Proposition 22, there exist $c_j \in K (1 \le j \le H)$ with $|c_j|_j > 1$ and $|c_j|_i < 1$ for all $i \neq j$. Notice that for $j = 1, \ldots, H$,

$$\left|\frac{c_j^n}{1 + c_j^n}\right|_i \to \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j. \end{cases}$$

as $n \to \infty$. The result now follows from the triangle inequality by taking

$$a = \sum_{j=1}^{H} \frac{c_j^n}{1 + c_j^n} b_j.$$

□

Remark 24. This can be viewed as an analogue of the Chinese Remainder Theorem.

Definition 25. Let K be a field and $|\cdot|$ be the valuation on K. We say that *a sequence $(a_1, a_2, \ldots)$ of elements of K converges to a limit b in K with respect to* $|\cdot|$ if given $\varepsilon > 0$ there exists $n_0(\varepsilon)$ such that for $n > n_0(\varepsilon)$ we have $|a_n - b| < \varepsilon$.

Remark 26. By axiom (i) of Definition 1, if the limit exists it is unique.

Definition 27. We define a *Cauchy sequence* $(z_1, z_2, \ldots)$ to be a sequence such that for each $\varepsilon > 0$ there exists $n_1(\varepsilon)$ such that whenever $m, n > n_1(\varepsilon)$ we have $|a_m - a_n| < \varepsilon$. Note that if $(a_1, a_2, \ldots)$ has a limit then it is a Cauchy sequence.

Definition 28. A sequence $(a_1, a_2, \ldots)$ is said to be a *null sequence* with respect to $|\cdot|$ if it has limit zero.

Definition 29. A field K is *complete with respect to* $|\cdot|$ if every Cauchy sequence in K has a limit in K.

Remark 30. $\mathbb{Q}$ is not complete with respect to $|\cdot|_\infty$ (the ordinary absolute value on $\mathbb{Q}$), since, for example, one can choose a Cauchy sequence which converges to $\sqrt{2}$.

So, what about $\mathbb{Q}$ and $|\cdot|_p$? Let $p = 5$. We now will construct a sequence with respect to the 5-adic valuation $|\cdot|_5$ which does *not* have a limit in $\mathbb{Q}$. Here, $|\cdot|_5$ is normalized so that $|5|_5 = 5^{-1}$. To show that $\mathbb{Q}$ is not complete with respect to $|\cdot|_5$, we construct a sequence of integers $(a_1, a_2, \ldots)$ satisfying $a_n^2 - 6 \equiv 0 \pmod{5^{n+1}}$ and $a_{n+1} \equiv a_n \pmod{5^n}$ for all $n \in \mathbb{N}$. Define $b_0, b_1, \ldots$ from $\{0, 1, 2, 3, 4\}$ inductively. Let $b_0 = 1$ and choose b_1 so that $(1 + b_1 5)^2 \equiv 1 + 2b_1 5 \equiv 6 \pmod{5^2}$. Thus $2_b 1 \equiv 1 \pmod 5$ so we can choose $b_1 = 3$. More generally suppose that $b_0, b_1, \ldots, b_n$ have been chosen hence determining $a_1, \ldots, a_n$. Then $a_n^2 = (b_0 + b_1 5 + \cdots + b_n 5^n)^2 \equiv 6 \pmod{5^{n+1}}$. Thus $(a_n + b_{n+1} 5^{n+1})^2 \equiv a_n^2 + 2b_{n+1} 5^{n+1} \equiv 6 + c5^{n+1} + 2b_{n+1} 5^{n+1} \equiv 6 + (c + 2b_{n+1}) 5^{n+1} \pmod{5^{n+2}}$ for some integer c. Thus it suffices to choose b_{n+1} so that $c + 2b_{n+1} \equiv 0 \pmod 5$. Observe that such b_{n+1} can be found. Thus $a_{n+1}^2 \equiv 6 \pmod{5^{n+2}}$. Further, we have $a_{n+1} \equiv a_n \pmod{5^{n+1}}$. This completes the inductive construction.

Notice that $(a_1, a_2, \dots)$ is a Cauchy sequence with respect to $|\cdot|_5$ since $a_{n+1} \equiv a_n \pmod{5^{n+1}}$ for $n = 1, 2, \dots$. If $(a_1, a_2, \dots)$ converged to a limit d in $\mathbb{Q}$, then since $|a_n^2 - 6|_5 \leq 5^{-n+1}$ we see that $|d^2 - 6|_5 = 0$. In other words, $d = \sqrt{6} \in \mathbb{Q}$ and this is a contradiction. One can show in a smilier manner that $\mathbb{Q}$ is not complete with respect to any p-adic valuation $|\cdot|_p$. Plainly, the sequence $(5^n)_{n=1}^{\infty}$ is a null sequence with respect to $|\cdot|_5$ but is not a Cauchy sequence with respect to $|\cdot|_\infty$ or any p-adic valuation $|\cdot|_p$ where $p \neq 5$.

Definition 31. Let K be a field with a valuation $|\cdot|$. Let L be a field containing K. A valuation $|\cdot|_1$ on L *extends* $|\cdot|$ *on* K if $|\alpha|_1 = \alpha$ for all $\alpha \in K$.

Definition 32. Let K be a field with a valuation on $|\cdot|$. We say that a field L together with a valuation $|\cdot|_1$ with extends on K is a *completion of* K if L is complete and L is the closure of K in the topology induced by $|\cdot|_1$.

Given a field K with valuation $|\cdot|$, how do we construct a completion of K with respect to $|\cdot|$? First suppose that $|\cdot|$ satisfies the triangle inequality. The Cauchy sequences of elements of K form a ring (call this ring R) under term-wise addition and multiplication, i.e. $(a_n) + (b_n) = (a_n + b_n)$ and $(a_n) \cdot (b_n) = (a_n b_n)$. Then the set of all null sequences of elements in K with respect to $|\cdot|$ (call this set N) forms a maximal ideal in the ring R. Thus $L := R/N$ formulates a field. We now define a valuation $|\cdot|_1$ on L in the following way. If $\alpha \in L$, then $\alpha = (a_1, a_2, \dots) + N$ where $(a_1, a_2, \dots)$ is a Cauchy sequence in K with respect to $|\cdot|$. Define $|\alpha|_1 = \lim_{n\to\infty} |a_n|$. However, we need to ensure that $|\cdot|_1$ is well-defined. We first check that the limit exists, and then that the limit does not depend on our choice of representative of the equivalence class we choose. We first check that $(|a_n|)_n$ is a Cauchy sequence. Notice by the triangle inequality that:

- $|a_n| \leq |a_n - a_m| + |a_m| \Rightarrow |a_n| - |a_m| \leq |a_n - a_m|$ and $|a_m| - |a_n| \leq |a_n - a_m|$. Hence, $||a_n| - |a_m||_\infty \leq |a_n - a_m|$. Thus we see that the sequence $(|a_n|)$ is Cauchy and so converges to a limit.
- Now we need to show that the choice of a representative does not matter (well-defined). Note that if $(a_1, a_2, \dots) \sim (b_1, b_2, \dots)$, then we must show that $\lim |a_n| = \lim |b_n|$. But then
$$||a_n| - |b_n||_\infty \leq |a_n - b_n|. \tag{2}$$
Since $(a_n - b_n)_n$ is a null sequence we see from (2) that $\lim |a_n| = \lim |b_n|$.

Finally, we must check that $|\cdot|_1$ is a valuation on L but this is routine. First, we can (naturally) embed K in L with the map $\varphi : K \to L$ by $\varphi(a) = (a, a, a, \dots) + N$. Then φ is an injective field homomorphism satisfying $|a| = |\varphi(a)|_1$. Let $K' = \varphi(K)$. Then K' is everywhere dense in L. For let $\alpha = (a_1, a_2, \dots) \in L$, then given $\varepsilon > 0$ there exists $n_0(\varepsilon)$ such that for all $n > n_0(\varepsilon)$, we have $|\alpha - \varphi(a_n)|_1 < \varepsilon$ since $(a_1, a_2, \dots)$ is a Cauchy sequence.

We now verify if L is complete. Let $(a_n)_n$ be a Cauchy sequence in L. Since K' is everywhere dense in L, there exists a sequence $(\varphi(a_n))_n$ such that $|\varphi(a_n) - a_n|_1 < \frac{1}{n}$. Thus, the sequence $(\varphi(a_n) - a_n))_n$ is a null sequence in L. Hence $(\varphi(a_n))_n$ is a Cauchy sequence in L. Thus $(a_n)_n$ is a Cauchy sequence in K. In particular, it determines an element β in L with
$$\lim_{n\to\infty} |\varphi(a_n) - \beta|_1 = 0.$$
Thus $\lim_{n\to\infty} |a_n - \beta|_1 = 0$ so $(a_n)_n$ converges to an element in L.

4. September 30

Let $|\cdot|_p$ be the p-adic valuation on $\mathbb{Q}$ normalized so that $|p|_p = p^{-1}$. We will denote by $\mathbb{Q}_p$ "the" completion of $\mathbb{Q}$ with respect to $|\cdot|_p$. We say "the" to refer to the construction described previously. Further, we will denote the valuation $|\cdot|_{1_p}$ on $\mathbb{Q}_p$ by $|\cdot|_p$.

Theorem 33. *Every $\alpha \in \mathbb{Q}_p$ with $\alpha_p \le 1$ has a* unique *representative Cauchy sequence $(a_n)_n$ such that:*

- *$a_n \in \mathbb{Z}$ for all $n = 1, 2, 3, \ldots$*
- *$0 \le a_i < p^i$ for $i = 1, 2, \ldots$*
- *$a_{i+1} \equiv a_i \pmod{p^i}$ for $i = 1, 2, 3, \ldots$.*

Proof. We first prove uniqueness. Suppose that $(a_n)_n$ and $(b_n)_n$ are two such sequences representing some $\alpha \in \mathbb{Q}_p$. If $(a_n)_n \ne (b_n)_n$ then for some integer i, we have $a_i \ne b_i$. But then for $n > i$, it is known that $a_n \equiv a_i \pmod{p^i}$ and $b_n \equiv b_i \pmod{p^i}$. Hence $a_n \not\equiv b_n \pmod{p^i}$ therefore $|a_n - b_n|_p \ge p^{-i}$. Thus $(a_n - b_n)$ is not a null sequence, hence a contradiction. It remains to show that each element in $\mathbb{Q}_p$ has such a representation. To do so, we will need the following result:

Lemma 34. *If $x \in \mathbb{Q}$ and $|x|_p \le 1$ then for any positive integer i there exists an integer c with $0 \le c < p^i$ such that $|x - c|_p \le p^{-i}$.*

Proof of Lemma. The result is immediate when $x = 0$. So suppose $x \ne 0$. Now write $x = a/b$ with $(a, b) = 1$. Since $|\frac{a}{b}|_p \le 1$, we see that $p \nmid b$. Thus there exist integers m and n such that $mb + np^i = 1$. Put $c_1 = am$. Then

$$\left|\frac{a}{b} - c_1\right|_p = \left|\frac{a}{b}\right|_p \left|1 - \frac{c_1 b}{a}\right|_p = |1 - mb|_p \le p^{-i}.$$

We now choose c with $0 \le c < p^i$ so that $c \equiv c_1 \pmod{p^i}$. $\square$

Now we are ready to prove existence. Suppose that $(b_n)_n$ a Cauchy sequence which represents α. Then for each positive integer j there exists an $N(j)$ such that $|b_i - b_k|_p \le p^{-j}$ whenever $i, k > N(j)$. We may suppose, without loss of generality, that $N(1) < N(2) < \cdots$ so $N(j) \ge j$. Further, $|b_i|_p \le 1$ for $i \ge N(1)$ since for all $k > N(1)$ we have (by the strong triangle inequality)

$$|b_i|_p = |(b_k) + (b_i - b_k)|_p \le \max(|b_k|_p, |b_i - b_k|_p) \le \max\left(|b_k|_p, \frac{1}{p}\right).$$

But $|\alpha|_p \le 1$ and $|b_k|_p \to |\alpha|_p$ as $k \to \infty$ hence $|b_i|_p \le 1$.

We now use Lemma 34 to find a sequence of integers $(a_n)_n$ with $0 \le a_j < p^j$ for $j = 1, 2, \ldots,$ and

$$|a_j - b_{N(j)}|_p \le p^{-j}.$$

We now show that $a_{j+1} \equiv a_j \pmod{p_j}$. We have

$$\begin{aligned} |a_{j+1} - a_j|_p &= |(a_{j+1} - b_{N(j+1)}) + (b_{N(j+1)} - b_{N(j)}) + (b_{N(j)} - a_j)|_p \\ &\le \max(|a_{j+1} - b_{N(j+1)}|_p, |b_{N(j+1)} - b_{N(j)}|_p, |b_{N(j)} - a_j|_p) \\ &\le \max(p^{-j+1}, p^{-j}, p^{-j}) \le p^{-j}. \end{aligned}$$

Therefore $a_{j+1} \equiv a_j \pmod{p^j}$. Further, $(a_i - b_i)_i$ is a null sequence since for each positive integer j we have, for $i > N(j)$,

$$\begin{aligned} |a_i - b_i|_p &= |(a_i - a_j) + (a_j - b_{N(j)}) + (b_{N(j)} - b_i)|_p \\ &\leq \max(|a_i - a_j|_p, |a_j - b_{N(j)}|_p, |b_{N(j)} - b_i|_p) \\ &\leq \max(p^{-j}, p^{-j}, p^{-j}) = p^{-j}. \end{aligned}$$

Thus $|a_i - b_i|_p \to 0$ as $i \to \infty$.

If $a \in \mathbb{Q}_p$ and $|a|_p > 1$ then for some integer k, $|p^k a|_p \leq 1$. We can find an appropriate representative for $p^k a$, say $(a_i)_i$. We then represent a by $(p^{-k} a_i)_i$. Now suppose that $\alpha \in \mathbb{Q}_p$ with $|\alpha|_p \leq 1$. Let $(a_i)_i$ be a sequence as in Theorem 33 which represents α. We can represent a_i in base p, i.e., $a_i = b_0 + b_1 p + \cdots + b_{i-1} p^{i-1}$ where $b_0, b_1, \ldots, b_{i-1} \in \{0, 1, \ldots, p-1\}$. Since $a_{i+1} \equiv a_i \pmod{p^i}$ we have $a_{i+1} = b_0 + b_1 p + \cdots + b_i p^i$. Thus we can view α has having the unique power series expansion $\alpha = b_0 + b_1 p + b_2 p^2 + \cdots$. Further, if $a \in \mathbb{Q}_p$ and $|\alpha|_p = p^k$ for $k \in \mathbb{Z}_+$ then α has the power series expansion $\alpha = b_{-k} p^{-k} + b_{-k+1} p^{-k+1} + \cdots + b_0 + b_1 p + b_2 p^2 + \cdots$. □

Remark 35. This is a natural representation in terms of digits $\{0, 1, 2, \ldots, p-1\}$. There are other "natural" representations, for instance the Teichmüller representation. It is worth noting that each element $\alpha \in \mathbb{Q}_p$ has a unique base p expansion. Contrast this with the base 10 expansion of elements $\mathbb{R}$. Then of course $1.0000\ldots$ and $0.999\ldots$ are both equal to 1.

Definition 36. $\mathbb{Z}_p$ is the set of p-adic integers and is defined by

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

Addition, subtraction, multiplication, and division can be performed as in $\mathbb{R}$ but with carrying taken from right to left instead of left to right.

Let k be a field and P an indeterminate over k. Let $k(T)$ be the field of rational functions in T with coefficients in k. Let γ be a real number with $0 < \gamma < 1$. For any $\alpha \in k(T)$, we can write

$$\alpha = T^a \frac{f(T)}{g(T)}$$

where $f, g \in k[T]$ with $f(0), g(0) \neq 0$ and $a \in \mathbb{Z}$. We define a valuation $|\cdot|$ on $k(T)$ by $|\alpha| = \gamma^a$.

Let $k((T))$ be the completion of $k(T)$ with respect to $|\cdot|$. Denote the expansion of $|\cdot|$ from $k(T)$ to $k((T))$ by $|\cdot|$. Let $N \in \mathbb{Z}_+$ and let $(f_N, f_{N+1}, \ldots)$ be a sequence of elements of k. Then put

$$f^{(m)} = \sum_{n=N}^{m} f_n T^n$$

for $m = N, N+1, \ldots$. Note that $f^{(m)} \in k[T]$ for $m = N, N+1, \ldots$. The sequence $(f^{(m)})_{m=N}^{\infty}$ is a Cauchy sequence of elements of $k(T)$ with respect to $|\cdot|$, since

$$|f^{(i)} - f(j)| \leq \gamma^{\min(i,j)+1}.$$

Denote the element of $k((T))$ of which $f^{(m)}$ for which $(f^{(m)})_{m=N}^{\infty}$ is a representative by

$$f(T) = \sum_{m=N}^{\infty} f_n T^n.$$

Recall that $k((T))$ is the completion of $k(T)$ with respect to $|\cdot|$. Let $f(T) = \sum_{n=N}^{\infty} f_n T^n$, $f_n \in k$. f is the limit of $(f^{(m)})_{m=N}^{\infty}$ where $f^{(m)}(t)$ is the partial sum from N to m. Conside the set S of all expressions

$$\sum_{n \gg -\infty} f_n t^n,$$

where $f_n \in k$. When we say $n \gg -\infty$, we mean that there exists some integer $N \in \mathbb{Z}$ such that $f_n = 0$ for $n < N$. S forms a commutative ring with identity under the usual rules for multiplying and adding the power series.

Let $f \in S \setminus \{0\}$. Then $f(T) = T^a b(1 + \sum_{n=1}^{\infty} g_n T^n)$ for $a \in \mathbb{Z}$ and $b \in k \setminus \{0\}$. Put

$$h(T) = T^{-a} b^{-1} \left(1 + \sum_{m=1}^{\infty} \left(- \sum_{n=1}^{\infty} g_n T^n \right) \right) = \sum_{n \gg -\infty} h_n T^n.$$

Further, $f(T)h(T) = 1$. Thus S is a field. Note that $k(T) \subseteq S$ and the closure of $k(T)$ with respect to $|\cdot|$ is contained in S Thus S is isomorphic to $k((T))$.

Definition 37. We define $k[[T]]$ to be the element of $k((T))$ with $|f| \leq 1$. Then $f \in k[[T]] \Leftrightarrow f = \sum f_n T^n$. $k[[T]]$ is a subring of $k((T))$. It is the ring of formal power series with coefficients in k.

Definition 38. $f \in \mathbb{Q}[[T]]$ with $f = \sum_{n=0}^{\infty} f_n T^n$ is said *to satisfy Eisenstein's condition* if there is a non-zero integer l such that $l^n f_n$ is an integer for all $n \geq 0$.

Theorem 39 (Eisenstein's theorem). *Let $f \in \mathbb{Q}[[T]]$. If f satisfies a non-trivial polynomial equation with coefficients in $\mathbb{Q}[T]$ then f satisfies Eisenstein's condition.*

Proof. We may suppose that f satisfies $g_0(T) + g_1(T)f(T) + \ldots g_J(T)f(T)^J = 0$. Not all of the g_j's are the zero polynomial and $g_j \in \mathbb{Q}[T]$ for $j = 0, 1, \ldots, J$. Let us suppose that J is minimal. For indeterminates X and Y, put

$$H(X) = \sum_{j=0}^{J} g_j(T) X^j \in \mathbb{Q}[T, X],$$

and $H(X + Y) = H(X) + H_1(X)Y + \cdots + H_J(X)Y^J$ where $H_j(X) \in \mathbb{Q}[T, X]$. Since J is minimal, we have $H_1(f) \neq 0$. Of course $H(f) = 0$. Now define the integer m as follows: $|H_1(f)| = \gamma^m$. Obviously we have $m \geq 0$. Put

$$f(T) = u(T) + T^{m+1} v(T),$$

where $u(T) = f_0 + f_1 T + \cdots + f_{m+1} T^{m+1} \in \mathbb{Q}[T]$ and $v(T) = 0 + f_{m+2} T + f_{m+3} T^2 + \cdots \in \mathbb{Q}[[T]]$. Notice that it suffices to show that $v(T)$ satisfies Eisenstein's condition. Since $H(f) = 0$, we have

$$0 = H(u + T^{m+1} v) = H(u) + T^{m+1} H_1(u) v + \sum_{j \geq 2} T^{(m+1)j} H_j(u) v^j. \qquad (3)$$

We have $H(u), H_1(u), \ldots, H_j(u)$ are in $\mathbb{Q}[T]$. Since $|H_1(f)| = \gamma^m$ we see that T^{2m+1} divides $H(u)$ and so divide the terms in (3) by T^{2m+1} to get

$$0 = h + h_1 v + h_2 v^2 + \cdots + h_J v^J \tag{4}$$

where $h, h_1, \ldots, h_J$ are in $\mathbb{Q}[T], h_1(0) \neq 0, h_j(0) = 0$ for $2 \leq j \leq J$. Without loss of generality, we may suppose that $h, h_1, \ldots, h_J$ are in $\mathbb{Z}[T]$ by multiplying both sides of (4) by an appropriate non-zero integer. Let $l = h_1(0)$ so l is a non-zero integer. Recall that $v(0) = 0$. Write $v(T) = 0 + v_1 T + v_2 T^2 + \cdots$ and re-label f_{m+2} as v_1, etc. We prove via induction on n that $l^n v_n$ is an integer. To see this it suffices to examine the coefficients on T^n in the expansion (4). In particular, from (4),

$$\begin{aligned}
&0 = (a_0^{(0)} + a_1^{(0)} T + \cdots + a_{N_0}^{(0)} T^{N_0}) \\
&+(a_0^{(1)} + a_1^{(1)} T + \cdots + a_{N_1}^{(1)} T^{N_1})(v_1 T + v_2 T^2 + \cdots) \\
&\vdots \\
&+(a_0^{(J)} + a_1^{(J)} T + \cdots + a_{N_J}^{(J)} T^{N_J})(v_1 T + v_2 T^2 + \cdots)^J.
\end{aligned}$$

Note that $a_0^{(i)} = 0$ for all $i = 1, 2, \ldots, J$. Therefore, $l v_n$ is a sum of terms of the form $a \prod_{m<n} v_m^{r_m}$, where $a \in \mathbb{Z}$ and $\sum_{m<n} m r_m < n$ since $h_i(0) = 0$ for all $2 \leq i \leq J$. Then the result follows by induction. □

Notice that, for example, $f(T) = \sum \frac{T^n}{n} \in \mathbb{Q}[[T]]$ does not satisfy non-trivial a polynomial expansion over $\mathbb{Q}(T)$ by Eisenstein's theorem. Therefore it is not algebraic over $\mathbb{Q}(T)$.

Remark 40. The natural question to ask is what the value of l will look like. Quantitative results refining the theorem have been given by Coates, Schmidt, Dwork, and van der Poorten.

6. October 7

Theorem 41 (Ostrowski's theorem). *Let k be a field which is complete with respect to an* archimedean *valuation $|\cdot|$ on k. Then k is isomorphic to $\mathbb{C}$ or $\mathbb{R}$, and the valuation is equivalent to $|\cdot|_\infty$, the ordinary absolute value.*

Proof. k is of characteristic 0 (since otherwise the valuation must be non-archimedean), so it contains the rationals. Thus there exists the valuation induced on $\mathbb{Q}$ by $|\cdot|$, and $|\cdot|$ is archimedean and equivalent to the ordinary absolute values $|\cdot|_\infty$ on $\mathbb{Q}$. Since k is complete it contains the completion of $\mathbb{Q}$ with respect to $|\cdot|$. This completion is $\mathbb{R}$ and $|\cdot|$ restricted to $\mathbb{R}$. Clearly $|\cdot|$ is equivalent to $|\cdot|_\infty$ on $\mathbb{R}$. We now distinguish two cases:

(1) k contains a solution to $i^2 + 1 = 0$
(2) k does not contain a solution to $i^2 + 1 = 0$

We shall now prove some technical propositions. Our aim is to reduce the proof to the case when k is an extension of $\mathbb{C}$. We shall show that if k is different from $\mathbb{C}$ we get a contradiction.

Lemma 42. *Any archimedean valuation $|\cdot|$ on $\mathbb{C}$ is equivalent to the ordinary absolute value $|\cdot|_\infty$ on $\mathbb{C}$.*

Proof of Lemma 42. Without loss of generality we may suppose that $|\cdot|$ on $\mathbb{C}$ satisfies the triangle inequality. Since $|\cdot|$ induces an archimedean valuation on $\mathbb{Q}$ it is equivalent to $|\cdot|_\infty$ on $\mathbb{Q}$ and hence to $|\cdot|_\infty$ on $\mathbb{R}$. Thus there exists some $\lambda > 0$ such that for all $a \in \mathbb{R}$, we have $|a| = |a|_\infty^\lambda$. Let $\alpha = a + ib$ with $a, b \in \mathbb{R}$. We have $|a|_\infty \leq |\alpha|_\infty$ and $|b|_\infty \leq |\alpha|_\infty$. Thus

$$|\alpha| = |a + ib| \leq |a| + |ib| \leq |a| + |b| \leq |a|_\infty^\lambda + |b|_\infty^\lambda \leq 2|\alpha|_\infty^\lambda. \tag{5}$$

If $|\cdot|$ and $|\cdot|_\infty$ are inequivalent, then given $\varepsilon > 0$ we can find $\beta \in \mathbb{C}$ such that $|\beta|_\infty < \varepsilon$ and $|\beta| \geq 1$. But this contradicts (5) when ε is sufficiently small. The result follows. □

We will now show that if k does not contain i, in other words $T^2 + 1$ is irreducible over k then we can extend our valuation to $k(i)$.

Lemma 43. *Let k be a field which is complete with respect to an archimedean valuation $|\cdot|$. Suppose that $T^2 + 1$ is irreducible over k. Then there is a positive real number θ such that for all $a, b \in k$, we have*

$$|a^2 + b^2| \geq \theta \max(|a|^2, |b|^2) \tag{6}$$

Proof. Again suppose $|\cdot|$ satisfies the triangle inequality. We shall show that we can take $\theta = \frac{|4|}{1+|4|}$. Observe that we may suppose that $a, b \neq 0$. By homogeneity of (6), it suffices to show that if there exists $c_1 \in k$ with $|c_1| \leq 1$ and $|c_1^2 + 1| < \theta$ then $T^2 + 1$ is reducible over k. Put $\delta_1 = |c_1^2 + 1|$. By the triangle inequality,

$$1 = |1| = |c_1^2 + 1 - c_1^2| \leq |c_1^2 + 1| + |c_1|^2,$$

so $|c_1|^2 \geq 1 - \delta_1 > 1 - \theta$. Put $c_2 = c_1 + h_1$ where $h_1 \in k$ and to be chosen. Then $c_2^2 + 1 = c_1^2 + 2c_1 h_1 + h_1^2$. We choose $h_1 = -\frac{c_1^2+1}{2c_1}$ and put $\delta_2 = |c_2^2 + 1|$. We have

$$\delta_2 = |c_2^2 + 1| = |h_1^2| = \frac{|c_1^2 + 1|^2}{|4||c_1|^2} = |c_1^2 + 1| \frac{|c_1^2 + 1|}{|4||c_1|^2} = \delta_1 \gamma,$$

where $\gamma = \frac{|c_1^2+1|}{|4||c_1|^2} < \frac{\theta}{|4|(1-\theta)} \leq 1$.

Having constructed c_2 now we can repeat this process to construct $c_3, c_4, \ldots,$ with $\delta_3 = |c_3^2 + 1| \leq \delta_2 \gamma \leq \delta_1 \gamma^2$ and more generally, $\delta_n = |c_n^2 + 1| < \theta \gamma^{n-1}$ for $n = 2, 3, \ldots$. Further,

$$|c_{n+1} - c_n|^2 = |h_n|^2 = \delta_{n+1} \leq \theta \gamma^n.$$

Therefore, $|c_{n+1} - c_n| < \sqrt{\theta \gamma^n}$. Notice that then $(c_n)_{n=1}^\infty$ is a Cauchy sequence with respect to $|\cdot|$ and since k is complete with respect to $|\cdot|$ we see that the sequence converges to an element $c \in k$. But then $|c^2 + 1| = \lim_{n\to\infty} |c_n^2 + 1| = 0$ so $c^2 + 1 = 0$. Thus $T^2 + 1$ is reducible over k. □

Lemma 44. *Let k be complete with respect to an archimedean valuation $|\cdot|$. Suppose that $T^2 + 1$ is irreducible in $k[T]$. Then there is an extension of $|\cdot|$ to $k(i)$ where $i^2 = -1$.*

Proof. We define the function $|\cdot|_1$ on $k(i)$ by $|a + ib|_1 = |a^2 + b^2|^{1/2}$, for all $a, b \in k$. We now check that $|\cdot|_1$ is a valuation on $k(i)$ which extends $|\cdot|$ on k. First, note that $|\cdot|_1$ agrees with $|\cdot|$ on k. It remains to show that $|\cdot|_1$ is a valuation on $k(i)$.

Note that since $i \notin k$ we see that property (i) of Definition 1 holds for $|\cdot|_1$. Property (ii) is immediate. For property (iii) suppose $|a + ib| \leq 1$ with $a, b \in k$. Then by Lemma 43,

$$|a|, |b| \leq \theta^{-1/2},$$

and so

$$|1+a+ib|_1^2 \le |(1+a)^2+b^2| = |1+2a+a^2+b^2| \le 1+|2||a|+|a|^2+|b|^2$$
$$\le 1+2\theta^{-1/2}+2\theta^{-1} = C^2,$$

as required. □

We are now able to conclude the proof of Ostrowski's theorem. By Lemma 44, we may suppose that k contains $\mathbb{C}$ and observe that our valuation $|\cdot|$ on k is equivalent to $|\cdot|_\infty$ when restricted to $\mathbb{C}$. Suppose then that $\mathbb{C} \subsetneq k$. We shall show that this is impossible. Accordingly, let $\alpha \in k \setminus \mathbb{C}$. Consider the map $f : \mathbb{C} \to \mathbb{R}$ given by $f(a) = |\alpha - a|$. Observe that f is continuous. Considering f on the compact subset of $\mathbb{C}$ given by a with $|a| \le 3|\alpha|$ we see that f achieves on absolute minimum at some element $b \in \mathbb{C}$. Put $\beta = \alpha - b$. Notice that $|\beta| > 0$ since $\alpha \notin \mathbb{C}$. Now pick a non-zero element $c \in \mathbb{C}$ with $0 < |c| < |\beta|$. Next let n be a positive integer. Then

$$\frac{\beta^n - c^n}{\beta - c} = \prod_{\substack{\zeta^n=1 \\ \zeta\neq 1}} (\beta - \zeta c).$$

Observe $\beta - \zeta c| \ge |\beta|$ hence

$$\left|\frac{\beta^n - c^n}{\beta - c}\right| \ge |\beta|^{n-1}.$$

Thus

$$\frac{\beta - c}{\beta} \le \frac{|\beta^n - c^n|}{|\beta|^n} = \left|1 - \left(\frac{c}{\beta}\right)^n\right| \le 1 + \left|\frac{c}{\beta}\right|^n \le 1 + \left(\frac{|c|}{|\beta|}\right)^n.$$

Since $|c| < |\beta|$ we see on letting $n \to \infty$ that $|\beta - c| \le \beta$. Therefore $|\beta - c| = |\beta|$. We can repeat this argument now with $\beta - c$. in this way we find that for each $m \in \mathbb{Z}_+$, we have $|\beta - mc| = |\beta$. Thus, now apply the triangle inequality on mc:

$$m|c| = |m||c| = |mc| \le |\beta| + |\beta - mc| \le 2|\beta|,$$

for all $m \in \mathbb{Z}_+$. But $|c| > 0$ and this is a contradiction. Hence, we can't extend this valuation beyond $\mathbb{C}$. □

7. October 9: Focus on non-archimedean valuation

Let $|\cdot|$ be a non-archimedean valuation on a field k. We denote by

$$\theta = \{a \in k : |a| \le 1\},$$

and the ring of $|\cdot|$-integers. The set

$$\mathfrak{p} = \{a \in k : |a| < 1\}$$

is a maximal ideal in θ, since if we add any element $a \in \theta \setminus \mathfrak{p}$ with $|a| = 1$ then $a^{-1} \in \mathfrak{p}$ so $1 \in \mathfrak{p}$.

Definition 45. We call $\theta/\mathfrak{p}$ the *residue class field*. The set of values $\{|a|, a \in k\}$ assumed by elements of a under the valuation is known as the valuation group.

Definition 46. We say that the valuation is *discrete* if the valuation group is a discrete subset of $\mathbb{R}^+$ under the usual topology on $\mathbb{R}$.

Remark 47. Note that the valuation group is a subgroup of $\mathbb{R}^+$. Observe that the valuation group of k under $|\cdot|$ is the same as the valuation group of $\overline{k}$ under $|\cdot|$ where $|\cdot|$ denotes the extension of $|\cdot|$ to $\overline{k}$ since if $|b| < |c|$ then $|b+c| = |c|$. This is discrete if there exists a $\delta > 0$ such that $1-\delta < |a| < 1+\delta$ implies $|a| = 1$.

Lemma 48. *A non-archimedean valuation $|\cdot|$ is discrete if and only if the maximal ideal $\mathfrak{p}$ is principal.*

Proof. ($\Leftarrow$) Since $\mathfrak{p}$ is principal there is an element $\pi \in k$ such that $\mathfrak{p} = (\pi)$. Suppose that $a \in k$ with $|a| < 1$. Then we have $a = \pi b$ for some $b \in \mathbb{Q}$. Therefore $|a| = |\pi b| = |\pi| \cdot |b| \leq |\pi| < 1$. Similarly, if $a \in k$ with $|a| > 1$ then $|a^{-1}| < 1$ so $|a^{-1}| \leq |\pi|$. Thus $|a| \geq |\pi|^{-1}$. Accordingly, if $a \in k$ with $|\pi| < |a| < |\pi|^{-1}$ then $|a| = 1$ as required.

($\Rightarrow$) If the valuation $|\cdot|$ is discrete, then the set $\{|a| : a \in k, |a| < 1\}$ attains its maximum for some $\pi \in k$. Then if $a \in k$ with $|a| < 1$ we have $a = \pi b$ with $|b| \leq 1$ hence $\mathfrak{p} = (\pi)$. □

Definition 49. Let $|\cdot|$ be a discrete non-archimedean valuation on a field k .Then an element π for which $\mathfrak{p} = (\pi)$i said to be a *prime element for the valuation*. Then for any element $b \in k$ with $b \neq 0$ we have that $|b| = |\pi^n| = |\pi|^n$ for some integer n. n is known as *the order of* b and denoted by $\operatorname{ord}_{\mathfrak{p}} b$.

Definition 50. Suppose that $a_1, a_2, \ldots$ are in k. Then the infinite sum $\sum a_n$ *converges to* s *with respect to the valuation* $|\cdot|$ if

$$s = \lim_{N\to\infty} \sum_{n=1}^{N} a_n.$$

Since

$$\left|\sum_{n=1}^{N} a_n\right| \leq \max_{1\leq n\leq N} |a_n|,$$

we have

$$\left|\sum_{n=1}^{\infty} a_n\right| \leq \max_{\pi} |a_n|.$$

Lemma 51. *Suppose that k is complete. Then*

$$\sum_{n=1}^{\infty} a_n \textit{ converges} \Leftrightarrow \lim_{n\to\infty} |a_n| = 0.$$

Proof. ($\Rightarrow$) $\lim_{n\to\infty} a_n = \lim_{n\to\infty} s_{n+1} - s_n = \lim_{n\to\infty} s_{n+1} - \lim_{n\to\infty} s_n = s - s = 0$.

($\Leftarrow$) Suppose $|a_n| \to 0$. Let $M > N$. Then

$$|S_M - S_N| = |a_{N+1} + \cdots + a_M| \leq \max_{N+1\leq i\leq M} |a_i|.$$

Given $\varepsilon > 0$ we can find $N_0(\varepsilon)$ such that for $M, N > N_0(\varepsilon)$, we have $|S_M - S_N| < \varepsilon$. Thus (s_n) is a Cauchy sequence in k. Since k is complete it converges to a element s in k. □

Lemma 52. *Let k be complete with respect to a discrete valuation $|\cdot|$ and let π be a prime. Let $A \subset \theta$ be a set of representatives for $\theta/\mathfrak{p}$. Then every element a in θ has a unique representative in the form $a = \sum a_n \pi^n$ where $a_n \in A$ for $n = 0, 1, 2, \ldots$. Further, every infinite sum of this form converges to an element a with $a \in \theta$.*

Proof. The last assertion follows since $|a_n| \leq 1$ and $|\pi| < 1$. Thus $\lim_{n\to\infty} |a_n\pi^n| = 0$ and k is complete.

For our first claim, note that the valuation of she differences of two distinct elements of A is 1 hence for any $a \in \theta$ there is at most one element $a_0 \in A$ for which $|a - a_0| < 1$ by the strong triangle inequality. There is at least one such a_0 since A is a full set of representatives. Then $a - a_0 = \pi b_1$ for some $b_1 \in \theta$. Similarly, there is precisely one element $a_1 \in A$ such that $|b_1 - a_1| < 1$. So we have $b_1 = a_1 + \pi b_2$ for $b_2 \in \theta$. Thus for every positive integer N we have

$$a = a_0 + a_1\pi + a_2\pi^2 + \cdots + a_N\pi^N + b_{N+1}\pi^{N+1}$$

with $b_{N+1} \in \theta$ and $a_i \in A$ for $i = 0, 1, \ldots, N$. Since $|b_{N+1}\pi^N| \to \infty$ as $N \to \infty$ the result follows. □

Remark 53. The p-adic case is a special case of Lemma 52, with $\mathbb{Z}_p$ with the valuation $|\cdot|_p$ and $\pi = p, A = \{0, 1, \ldots, p-1\}$.

Remark 54. Also note that we can extend this result to k since every non-zero element $a \in k$ has $\pi^N a \in \theta$ for some $N \in \mathbb{Z}$.

Lemma 55. *Let k be complete with respect to a discrete valuation. If the residue class field $\theta/\mathfrak{p}$ is finite then θ is compact.*

Proof. Since $|\cdot|$ induces a metric on θ compactness is equivalent to sequential compactness. Thus it is enough to show that every sequence $(a^{(j)})$ has a convergent subsequence. For each j consider the representation

$$a^{(j)} = \sum_{n=0}^{\infty} a_{j,n}\pi^n \quad (a_{j,n} \in A).$$

Since A is finite then there exists an element $a_0 \in A$ for which $a_{j,0} = a_0$ for infinitely many positive integers j. We can then find infinitely many integers j for which $a_{j,0} = a_0$ and for which $a_{j,1} = a_1$ for some $a_1 \in A$. Continuing in this way we find an element $a = a_0 + a_1\pi + \cdots$ in θ which is the limit of a convergent subsequence. □

8. October 14

Lemma 56 (Hensel's Lemma)**.** *Let k be a field complete with respect to a discrete, non-archimedean valuation $|\cdot|$, and let $f \in \theta[X]$. Let $a_0 \in \theta$ which satisfies*

$$|f(a_0)| < |f'(a_0)|^2. \tag{7}$$

Then there exists an $a \in \theta$ for which $f(a) = 0$.

Example 57. In $\mathbb{Z}_5$ we showed that $f(X) = x^2 - 6$ has a root. By Lemma 56, it is enough to note that $\frac{1}{5} = |f(1)|_5 < |f'(1)|^2 = 1$.

Proof. Let $f_j(x)\,(j = 1, 2, \ldots)$ be defined by the identity

$$f(x + y) = f(x) + f_1(x)y + f_2(x)y^2 + \cdots \tag{8}$$

Observe that $f'(x) = f_1(x)$. Now by (7), $|f'(a_0)| > 0$ hence $f'(a_0) \neq 0$ and

$$\frac{|f(a_0)|}{|f'(a_0)|} < |f'(a_0)| \leq 1.$$

Thus there exists $b_0 \in \theta$ such that

$$f(a_0) + b_0 f_1(a_0) = 0.$$

Therefore by (8),

$$|f(a_0+b_0)| = |f_2(a_0)b^2 + f_3(a_0)b^3 + \cdots| \le \max_{j\ge 2} |f_j(a_0)b^j|.$$

Since $f_j \in \theta[X], a_0 \in \theta$ then $|f_j(a_0)| \le 1$. Therefore

$$|f(a_0+b_0)| \le |b_0|^2 = \frac{|f(a_0)|^2}{|f'(a_0)|^2} \le \left(\frac{|f(a_0)|}{|f'(a_0)|^2}\right) \cdot |f(a_0)| < |f(a_0)|.$$

Also, we can expand $f_i(x+y)$ as we did for f to conclude that

$$|f_1(a_0+b_0) - f_1(a_0)| \le |b_0| = \frac{|f(a_0)|}{|f'(a_0)|} < |f'(a_0)| = |f_1(a_0)|.$$

By the ultrametric inequality,

$$|f_1(a_0+b_0)| = |f_1(a_0)|.$$

We now put $a_1 = a_0 + b_0$ and repeat the process. Observe that

$$|f(a_1)| < |f(a_0)| < |f'(a_0)|^2 = |f'(a_1)|^2.$$

In this way we generate a sequence $a_0, a_1, a_2, \ldots$ and $b_0, b_1, b_2, \ldots$ of elements on θ. We have that $a_n = a_{n-1} + b_{n-1}$ for $n = 1, 2, \ldots$ and that

$$|f_1(a_n)| = |f_1(a_0)|$$

for $n = 1, 2, \ldots$. Further, $|f(a_n)| < |f(a_{n-1})|$ for $n = 1, 2, \ldots$. And since the valuation is discrete we see that

$$\lim_{n\to\infty} |f(a_n)| = 0.$$

Furthermore,

$$|a_{n+1} - a_n| = |b_n| = \frac{|f(a_n)|}{|f_1(a_n)|} = \frac{|f(a_n)|}{|f_1(a_0)|}$$

tends to 0 a $n \to \infty$. Thus $(a_n)_{n=1}^{\infty}$ is a Cauchy sequence and since k is complete it has a limit a in k. Since $|a_n| \le 1$ for $n = 0, 1, 2, \ldots$ we see that $a \in \theta$. Finally,

$$\lim_{n\to\infty} |f(a_n)| = |f(a)| = 0,$$

so $f(a) = 0$. □

Example 58. Let $p \neq 3$, and let $b \in \mathbb{Z}_p$ with $|b|_p = 1$ (i.e., b is a p-adic unit). If $b \equiv c^3 \pmod{p}$ for some integer c then $b = a^3$ for some a in $\mathbb{Z}_p$.

Proof. Let $f(x) = x^3 - b$ so $f'(x) = 3x^2$. Then $|f(c)|_p < |f'(c)|^2 = 1$. The result now follows by Hensel. □

Lemma 59. *Let k be complete with respect to a non-archimedean valuation $|\cdot|$. Let $b_{ij} \in k$ for $i, j \in \{0, 1, 2, \ldots\}$. Suppose that for each $\varepsilon > 0$, there exists a $\tau(\varepsilon)$ such that for $\max(i,j) > \tau(\varepsilon)$ we have $|b_{ij}| < \varepsilon$. Then the series*

$$\sum_i \left(\sum_j b_{ij}\right) \text{ and } \sum_j \left(\sum_i b_{ij}\right)$$

both converge and the sums are equal.

Proof. For each i with $1 \leq i \leq \tau(\varepsilon)$, $\sum_j b_{ij}$ converges since $|b_{ij} \to 0$ as $j \to \infty$. Further, for $i > \tau(\varepsilon)$,

$$\left|\sum_j b_{ij}\right| \max_j |b_{ij}| < \varepsilon.$$

Thus $\sum_i (\sum_j b_{ij})$ converges, and one can use the similar argument to prove that $\sum_j (\sum_i b_{ij})$ converges. Finally,

$$\left|\sum_{i=0}^{\tau(\varepsilon)} \sum_{j=0}^{\tau(\varepsilon)} b_{ij} - \sum_{i=0}^{\infty} \left(\sum_{j=0}^{\infty} b_{ij}\right)\right| < \varepsilon$$

and

$$\left|\sum_{j=0}^{\tau(\varepsilon)} \sum_{i=0}^{\tau(\varepsilon)} b_{ij} - \sum_{j=0}^{\infty} \left(\sum_{i=0}^{\infty} b_{ij}\right)\right| < \varepsilon.$$

Hence

$$\left|\sum_{i=0}^{\infty} \left(\sum_{j=0}^{\infty} b_{ij}\right) - \sum_{j=0}^{\infty} \left(\sum_{i=0}^{\infty} b_{ij}\right)\right| < \varepsilon,$$

as required (since the inequality holds for any arbitrary ε). □

Let $a_i \in k$ for $i = 0, 1, 2, \ldots$, and define the power series f by

$$f(x) := a_0 + a_1 x + a_2 x^2 + \cdots .$$

Write

$$R^{-1} = \limsup_n |a_n|^{1/n},$$

so $0 \leq R \leq \infty$. For $b \in k$, the series $\sum_{n=0}^{\infty} a_n b^n$ converges if and only if $|a_n b^n| \to 0$ as $n \to \infty$. Let D be the domain of convergence of the series $\sum a_n x^n$. Then:

- if $R = 0$ then $D = \{0\}$.
- if $R = \infty$ then $D = k$.
- if $0 < R < \infty$ and $|a_n| R^n \to 0$ then $D = \{b \in k : |b| \leq R\}$
- if $0 < R < \infty$ and $|a_n| R^n \not\to 0$ then $D = \{b \in k : |b| < R\}$.

Lemma 60. *Let $f(x) = \sum_{n=0}^{\infty} a_n x^n$ be a power series with coefficients in k, a field which is complete with respect to a non-archimedean valuation $|\cdot|$. Let D be the domain of convergence of f. Let $c \in D$. For $m = 0, 1, 2, \ldots,$ put*

$$g_m = \sum_{n \geq m} \binom{n}{m} a_n c^{n-m}.$$

Then the series

$$g(x) = \sum_{m=0}^{\infty} g_m x^m$$

has domain of convergence D and $f(b + c) = g(b)$ for all $b \in D$.

Proof. Observe that the series defining g_m converges since $|\binom{n}{m}| \leq 1$ and $c \in D$. Now let $b \in D$. Then

$$f(b+c) = \sum_n a_n(b+c)^n = \sum_n \sum_{m \leq n} \binom{n}{m} a_n c^{n-m} b^m.$$

This sum converges and by Lemma 59 we can rearrange so that

$$f(b+c) = \sum_{m=0}^{\infty} \left(\sum_{n \geq m} \binom{n}{m} a_n c^{n-m} \right) b^m = \sum_{m=0}^{\infty} g_m b^m = g(b).$$

Thus the domain of convergence of g includes D.

Reversing this argument we see that if b is in the domain of convergence of g and $c \in D$, then $b + c$ is in D. Thus $b \in D$ and the domain of convergence of g equals that of f. □

Corollary 61. *A function f defined by a power series is continuous in its domain of convergence.*

Proof. We have $f(b + c) = g(b)$ and g is continuous at 0. The result follows. □

9. October 16

Theorem 62 (Strassman's theorem)**.** *Let k be complete with respect to a non-archimedean valuation $|\cdot|$, and let*

$$f(x) = \sum_{n=0}^{\infty} a_n x^n.$$

Suppose that $|a_n| \to 0$ as $n \to \infty$ with not all a_n's zero. Then there is at most a finite number of $b \in \theta$ such that $f(b) = 0$. In fact, there are at most N such b where N satisfies

$$|a_N| = \max_n |a_n| \text{ and } |a_n| < |a_N| \text{ for } n > N.$$

Proof. We prove by induction on N. Suppose first that $N = 0$. Then notices that $b \in \theta$ with $f(b) = 0$. We have

$$0 = \sum_{n=0}^{\infty} a_n b^n,$$

hence

$$a_0 = -\sum_{n=1}^{\infty} a_n b^n. \tag{9}$$

Observe that

$$\left| -\sum_{n=1}^{\infty} a_n b^n \right| \leq \max_{n \geq 1} |a_n b^n| \leq \max_{n \geq 1} |a_n| < |a_0|$$

which contradicts (9).

Suppose then that $N > 0$ and $f(b) = 0$ with $b \in \theta$. Let $c \in \theta$. Then

$$\begin{aligned} f(c) = f(c) - f(b) &= \sum_{n=0}^{\infty} a_n(c^n - b^n) \\ &= (c-b) \sum_{n \geq 1} \sum_{j<n} a_n c^j b^{n-1-j}. \end{aligned}$$

By Lemma 59, we can sum over powers of c, hence $f(c) = (c-b)g(c)$, where $g(x) = \sum_{j=0}^{\infty} g_j x^j$ and $g_j = \sum_{r\geq 0} a_{j+1+r} b^r$. Now we observe that

$$|g_j| \leq \max_r |a_{j+1+r}| \leq |a_N|.$$

Further, $|g_{N-1}| = |a_N|$ and $|g_n| < |a_N|$ for $n > N-1$. Thus by our inductive hypothesis, g has at most $N-1$ zeroes in θ and thus f has at most N zeroes in θ. The result follows. □

Corollary 63. *Suppose f and g are power series over k which both converge in θ, and that $g(b) = f(b)$ for infinitely many $b \in \theta$. Then $f \equiv g$.*

Proof. $f(x) - g(x)$ has infinitely many zeroes in θ. If not $f \not\equiv g$, then $f - g$ can only have finitely many zeroes in θ, a contradiction, by Starssman's theorem. The result follows. □

Corollary 64. *Suppose that k has characteristic zero. Let $f(x)$ be a power series over k which converges in θ. If $f(x) = f(x+d)$ foursome $d \in \theta$, then f is constant.*

Proof. Apply Strassman's theorem upon recognizing $f(x) = f(x+d) = f(x+2d) = \cdots$. □

For any $n \in \mathbb{Z}_+$ and any prime p, we have $|n!|_p = p^{-N}$, where

$$N = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots.$$

Thus since

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots < \frac{n}{p} + \cdots = \frac{n}{p-1}.$$

So we have

$$|n!|_p > p^{-\frac{n}{p-1}}.$$

Lemma 65. *Let p be a prime. Let $b \in \mathbb{Q}_p$ with $|b|_p \leq p-1$ for $p \neq 2$ and with $|b|_w \leq 2^{-2}$. Then there is a power series*

$$\Phi_b(x) = \sum_{n=0}^{\infty} \gamma_n x^n$$

with $\gamma_n \in \mathbb{Q}_p$ for which $|\gamma_n|_p \to 0$ as $n \to \infty$ and such that

$$(1+b)^r = \Phi_b(r)$$

for all $r \in \mathbb{Z}$.

Proof. We will first consider the case when $r \geq 0$. Then

$$(1+b)^r = \sum_{s=0}^{r} \binom{r}{s} b^s = \sum_{s=0}^{\infty} r(r-1)(r-2)\cdots(r-s+1)\frac{b^s}{s!}.$$

Observe that

$$\left|\frac{b^s}{s!}\right|_p \leq \frac{|b|_p^s}{p^{-\frac{s}{p-1}}} = |b|_p^s p^{\frac{s}{p-1}} \to 0 \text{ as } s \to \infty.$$

Thus the power series converges and we may express it as

$$\sum_{s=0}^{\infty} \left(\sum_{j=1}^{s} \theta_j r^j \right) \frac{b^s}{s!},$$

and so by Lemma 59 we may rearrange it to get

$$(1+b)^r = s\sum_{s=0}^{\infty} r(r-1)\cdots(r-s+1)\frac{b^s}{s!} = 1 + \left(\theta_1^{(s)}\sum_{s=1}^{\infty}\frac{b^s}{s!}\right)r + \left(\theta_2^{(s)}\sum_{s=2}^{\infty}\frac{b^s}{s!}\right)r^2 + \cdots .$$

Put $\gamma_0 = 1$ and $\gamma_j = \theta_j \sum\limits_{s=j}^{\infty} \frac{b^s}{s!}$ for $j = 1, 2, \ldots$, and then

$$(1+b)^r = \sum_{j=0}^{\infty} \gamma_j r^j$$

where $\gamma_j \in \mathbb{Q}_p$ and $|\gamma_j|_p \to 0$ as $j \to \infty$. Suppose that $r \in \mathbb{Z}_-$. Observe that for some positive integer m, we have $r + p^m > 0$. Furthermore, since $(a+b) = \sum\limits_{j=0}^{\infty} \gamma_j r^j$ we see that for $m \in \mathbb{Z}_+$,

$$\lim_{m\to\infty}(1+b)^{p^m} = 1.$$

Note that since $r + p^m > 0$ we have

$$(1+b)^{r+p^m} = \sum_{j=0}^{\infty} \gamma_j (r+p^m)^j.$$

Letting $m \to \infty$ we see that

$$(1+b)^{r+p^m} \to (1+b)^r,$$

and

$$\sum_{j=0}^{\infty} \gamma_j (r+p^m)^j \to \sum_{j=0}^{\infty} \gamma_j r^j$$

because $\sum \gamma_j r^j$ is continuous in its domain of convergence, and $|p^m|_p \to 0$ as $m \to \infty$. □

Let r and s be integers and u_0 and u_1 be integers. Suppose $u_n = ru_{n-1} + su_{n-2}$ for $n = 2, 3, \ldots$. The sequence $(u_n)_{n=0}^{\infty}$ is a binary recurrence sequence with initial terms u_0, u_1. Suppose $s \neq 0$ and $r^2 + 4s \neq 0$. Also suppose that u_0, u_1 not both 0. Let α, β be the roots of the associated polynomial $x^2 - rx - s$. By induction one can show that $u_n = a\alpha^n + b\beta^n$ for all $n \geq 0$, where

$$a = \frac{u_0\beta - u_1}{\beta - \alpha}, b = \frac{u_1 - u_0\alpha}{\beta - \alpha}.$$

Observe that if $|\alpha| > |\beta$ then $|u_n| \to \infty$ as $n \to \infty$. If $|\alpha| = |\beta|$ and α/β is not a root of unity then again $|u_n| \to \infty$ as $n \to \infty$ but this is not as obvious.

Consider the sequence $(u_n)_n$, where $u_n = u_{n-1} - 2u_{n-2}$ for $n = 2, 3, \ldots$, and $u_0 = 0, u_1 = 1$. Then

$$(u_n)_{n=0}^{\infty} = (0, 1, 1, -1, -3, -1, 5, 7, -3, -17, -11, 23, 45, -1, -91, -89, \ldots).$$

Write

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \text{ where } \alpha = \frac{1+\sqrt{-7}}{2}, \beta = \frac{1-\sqrt{-7}}{2}.$$

10. October 21

Let $\alpha = \frac{1+\sqrt{-7}}{2}, \beta = \frac{1-\sqrt{-7}}{2}$. Put $u_n = \frac{\alpha^n-\beta^n}{\alpha-\beta}$ for $n = 1, 2, \ldots$. Then the characteristic polynomial of the binary recurrence sequence $(u_n)_n$ is $x^2 - x + 2$.

Theorem 66 (Nagell)**.** *Let (u_n) be as above. Then $u_n = \pm 1$ only for $n = 1, 2, 3, 5, 13$.*

Proof. Put $f(x) = x^2 - x + 2$. Observe that

$$11^{-1} = |22|_{11} = |f(5)|_{11} < |f'(5)|_{11} = |9|_{11} = 1$$
$$11^{-1} = |44|_{11} = |f(7)|_{11} < |f'(7)|_{11} = 1.$$

By Hensel's lemma, there exist α and β in $\mathbb{Q}_{11}$ which are roots of $f(x)$ with

$$\alpha \equiv 5 \pmod{11}, \beta \equiv 7 \pmod{11}.$$

Further by the proof of Hensel's Lemma we have $f(5) + b_0 9 = 0$, so $22 + b_0 9 = 0$, so $b_0 \equiv 11 \pmod{11^2}$. Thus $\alpha \equiv a_0 + b_0 \equiv 16 \pmod{11^2}$. Also, $f(7) + b_0 \cdot 13 = 0$ hence $\beta = 7 + 99 \pmod{11^2}$. We wish to apply Lemma 65. Accordingly by Fermat's little theorem, we have $\alpha^{10} \equiv 1 \pmod{11}$ and $\beta^{10} \equiv 1 \pmod{11}$.

Put $A = \alpha^{10}$ and $B = \beta^{10}$. We write $n = r + 10s$ with $0 \le r \le 9$. So

$$u_{r+10s} = \frac{\alpha^r A^s - \beta^r B^s}{\alpha - \beta}.$$

First note that $u_{r+10s} \equiv u_r \pmod{11}$ for $s = 1, 2, \ldots$. By considering the first 10 values of our sequence we se that we can restrict our attention to $r = 1, 2, 3, 5$. Put $\alpha^{10} = A = 1 + a$ and $\beta^{10} = B = 1 + b$ so that $a \equiv 99 \pmod{11^2}$ and $b \equiv 77 \pmod{11^2}$. In fact, we have

r	$\alpha^r \pmod{11^2}$	$\beta^r \pmod{11^2}$
1	16	106
2	14	104
3	103	13
5	111	21
10	100	78

We now use Lemma 65 to develop

$$(\alpha - \beta)(u_{r+10s} \mp 1) = \alpha^r(1 + a)^s - \beta^r(1 + b)^s \mp \alpha - \beta \tag{10}$$

as a power series in s. Say $c_0 + c_1 s + c_2 s^2 + \cdots$, where $\mp$ in (10) indicates that we take -1 for $r = 1, 2$ and $+1$ for $r = 3, 5$. Notice that for $1, 2, 3, 5$, we have $c_0^{(r)} = 0$. We shall now suppress the index r and write $c_n^{(r)}$ as c_n for $n = 0, 1, 2, \ldots$. We now recall from the proof of Lemma 65 that

$$(1 + b)^r = \sum_{n=0}^{\infty} \gamma_n r^n$$

with $\gamma_n = \sum_{s=n}^{\infty} \theta_s \frac{b^s}{s!}$ where $\theta_s \in \theta$. Thus if $|b|_{11} \le 11^{-1}$ then

$$|\gamma_n|_{11} \le 11^{-2} \text{ for } n \ge 2$$
$$|\gamma_n|_{11} \le 11^{-3} \text{ for } n \ge 3.$$

Thus $|c_n|_{11} \le 11^{-2}$ for $n \ge 2$, and $|c_n|_{11} \le 11^{-3}$ for $n \ge 3$. Thus it remains to estimate c_1 and c_2.

We have

$$\begin{aligned}c_1 &= \alpha^r \left(\sum_{s=1}^{\infty} (-1)^{s-1} \frac{a^s}{s!} \right) - \beta^r \left(\sum_{s=1}^{\infty} (-1)^{s-1} \frac{b^s}{s!} \right) \\ &\equiv \alpha^r a - \beta^r b \pmod{11^2}.\end{aligned}$$

For $r = 1$ we have

$$\begin{aligned}c_1 &\equiv \alpha a - \beta b \pmod{11^2} \\ &\equiv 16 \cdot 99 - 106 \cdot 77 \pmod{11^2} \\ &\equiv 11(16 \cdot 9 - 106 \cdot 7) \pmod{11^2},\end{aligned}$$

but $16 \cdot 9 - 106 \cdot 7 \equiv 7 \pmod{11}$, so $|c_1|_{11} = 11^{-1}$. Thus by Strassman, the function defined by power series expansion (10) has at most one zero in $\mathbb{Q}_{11}$. In fact, it has *exactly* one zero for $r = 1$ given by $s = 0$.

For $r = 2$, note that

$$\begin{aligned}c_1^{(2)} = c_1 &\equiv \alpha^2 a - \beta^2 b \pmod{11^2} \\ &\equiv 14 \cdot 99 - 104 \cdot 77 \pmod{11^2},\end{aligned}$$

so $|c_1|_{11} = 11^{-1}$. By Strassman, this is exactly one zero given by $s = 0$.

For $r = 5$, we have

$$c_1 = \alpha^5 a - \beta^5 b \equiv 111 \cdot 99 - 21 \cdot 77 \pmod{11^2}$$

so $|c_1|_{11} = 11^{-1}$. Again by Strassman, there is exactly one zero of the power series in $\mathbb{Q}_{11}$ given by $s = 0$. Finally if $r = 3$ we have $c_1 \equiv \alpha^3 a - \beta^3 b \equiv 0 \pmod{11^2}$, so we need to look into c_2 as well. We have

$$\gamma_2 = \sum_{s \geq 2} \left(\sum_{i=1}^{s-1} \frac{(-1)^s (s-1)!}{i} \right) \frac{b^s}{s!}$$

in the notation of Lemma 65. Thus $\gamma_2 \equiv \frac{b^2}{2} \pmod{11^3}$ hence $c_2 \equiv \alpha^3 \frac{a^2}{2} - \beta^3 \frac{b^2}{2} \pmod{11^3}$. Computation of α and β by Hensel's lemma yields $\alpha \equiv 137 \pmod{11^3}$ and $\beta \equiv 1195 \pmod{11^3}$. Once we have computed α we can determine β mod 11^3 immediately since $\alpha + \beta = 1$.

Next observe that $\alpha^{10} \equiv (137)^{10} \equiv 1189 \pmod{11^3}$. So $a \equiv 1188 \pmod{11^3}$. Further $\beta^{10} \equiv 199 \pmod{11^3}$, so $b \equiv 198 \pmod{11^3}$. Now since $2c_2 \equiv \alpha^3 a^2 - \beta^4 b^2 \pmod{11^3} \not\equiv 0 \pmod{11^3}$. Thus $|c_2|_{11} = 11^{-2}$. Therefore by Strassman's theorem, the power series at most has two zeroes. In fact it has actually 2 zeroes given by $s = 0, 1$. These zeroes correspond to $u_3 = -1$ and $u_{13} = -1$. Now that we dealt with all the possible arithmetic progressions, the proof is complete. □

11. October 23 & October 28

Theorem 67. *The only solutions to*

$$x^2 + 7 = 2^m \tag{11}$$

for integers x and m are those with $m = 3, 4, 5, 7, 15$. The equation (11) *is known as* the Ramanujan-Nagell equation.

Proof. Plainly, for any solution of (11), x is an odd integer. Put $x = 2y - 1$. Then (11) becomes $y^2 - y + 2 = 2^{m-2}$. Let $\alpha = \frac{1+\sqrt{-7}}{2}$ and $\beta = \frac{1-\sqrt{-7}}{2}$ so

$$y^2 - y + 2 = (y - \alpha)(y - \beta). \tag{12}$$

Let $K = \mathbb{Q}(\alpha)$. Then $\mathcal{O}_K$ (the ring of integers of K) is a Euclidean domain with respect to the norm map. Thus $\mathcal{O}_K$ is a UFD. The only units in $\mathcal{O}_K$ are ± 1. From (12), if we have a solution then

$$(y - \alpha)(y - \beta) = (\alpha\beta)^{m-2}.$$

Then since $\alpha + \beta = 1$ we see the α and β are coprime in $\mathcal{O}_K$. Thus either $y - \alpha = \pm\alpha^{m-2}$ or $y - \alpha = \pm\beta^{m-2}$. Consider the first situation. Then we have $y - \beta = \pm\beta^{m-2}$ and so $-(\alpha - \beta) = (y - \alpha) - (y - \beta) = \pm\alpha^{m-2} - (\pm\beta^{m-2})$ hence

$$\frac{\alpha^{m-2} - \beta^{m-2}}{\alpha - \beta} = \pm 1. \tag{13}$$

But by our previous result, we only have $m - 2 = 1, 2, 3, 5, 13$. Then similarly, in the second situation, we again recover (13). This completes the proof. □

11.1. Quick historical detour.

Ramanujan in 1913 asked if $m = 3, 4, 5, 7, 15$ give the complete set of solutions of the Ramanujan-Nagell equation. The first proof was given by Nagell in 1948. Later, Beukers proved using the hypergeometric method that if D is a positive odd integer, then the equation

$$x^2 + D = 2^m$$

has two or more solutions in positive integers x and n if and only if $D = 7, 23$, or $2^k - 1$ for $k \geq 4$. For $D = 23$, $(x, n) = (3, 5), (45, 11)$. For $D = 2^k - 1$ ($k \geq 4$), we have $(x, n) = (1, k)$ or $(2^{k-1}, 2k - 2)$.

11.2. Back to our main aim.

Our aim is to construct $\overline{\mathbb{Q}_p}$ – but note that we can already define many familiar functions over $\mathbb{Q}_p$. First, let us define the analogues of the exponential and logarithm functions over $\mathbb{R}$, but now over $\mathbb{Q}_p$. We have

$$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!} \text{ for } x \in \mathbb{R}$$

and

$$\log(1 + x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n} \text{ for } |x| < 1.$$

We will define $\exp_p(x)$ and $\log_p(1+x)$ over $\mathbb{Q}_p$ by means of these power series. For what regions in $\mathbb{Q}_p$ do they converge? Recall that

$$\left|\frac{1}{n!}\right|_p = p^{\lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \cdots} < p^{\frac{n}{p-1}}.$$

Thus $\exp_p(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$ converges for x in $\mathbb{Q}_p$ with $|x|_p < p^{-\frac{1}{p-1}}$. Further, $\log_p(1+x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n}$ converges for $|x|_p < 1$. Notice that we have

$$\log(1+x) + \log(1+y) = \log((1+x)(1+y)) = \log(1+x+y+xy)$$

as an equality of (formal) power series and so

$$\log_p(1+x) + \log_p(1+y) = \log_p(1+x+y+xy)$$

for $|x|_p < 1$ and $|y|_p < 1$. Also, as an equality of formal power series,

$$\exp(x)\exp(y) = \exp(x+y),$$

and

$$\exp(\log(1+x)) = 1+x, \quad \log(1+(\exp(x)-1)) = x.$$

Thus:

- $\exp_p(x+y) = \exp_p(x)\exp_p(y)$ for $|x|_p, |y|_p < p^{-\frac{1}{p-1}}$
- $\exp_p(\log_p(1+x)) = 1+x$ for $|x|_p < p^{-\frac{1}{p-1}}$
- $\log_p(1+(\exp_p(x)-1)) = x$ for $|x|_p < p^{-\frac{1}{p-1}}$.

Similarly, we can define

$$\sin_p x = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n+1}}{(2n+1)!}$$
$$\cos_p x = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n}}{(2n)!}$$

for $|x|_p < p^{-\frac{1}{p-1}}$.

Remark 68. Notice that $|-2|_2 < 1$. This tells us that if we look at

$$\log_2(1-2) + \log_2(1+2) = \log_2(1) = 0.$$

Thus $2\log_2(-1) = 0$ so $\log_2(-1) = 0$. But

$$\log_2(-1) = \log_2(1-2) = \sum_{n=1}^{\infty} -\frac{2^n}{n}.$$

Thus if $S_N = \sum_{1 \le n \le N} \frac{2^n}{n} = \frac{p_N}{q_N}$ with $(p_N, q_N) = 1$. Then $2^{K_N} \mid p_N$ for some K_N, where $k_N \to \infty$ as $N \to \infty$.

Lemma 69. *Let $F := \mathbb{F}_q$, and let $f := [F : \mathbb{F}_p]$. Let K be an algebraic closure of $\mathbb{F}_p$ which contains F. Then $q = p^f$, and F is the only field of q elements contained in K. And F is the set of roots of $x^q - x = 0$. Conversely, for any power of $q = p^f$ of p, the roots of $x^q - x$ in K form a field of q elements.*

Proof. ($\Rightarrow$) Since F is an f-dimensional vector space over $\mathbb{F}_p$, we see that $q = p^f$. Next, any field of q elements has $q-1$ non-zero elements. The non-zero elements form a multiplicative group of order $q-1$. Thus for any x in the group, the order of x divides the order of the group, so $x^{q-1} = 1$ hence $x^q = x$ for all $x \in F$. But there can be at most q solutions of $x^q - x = 0$ in F so we are done. In particular, F is the set of roots of $x^q - x$ in K.

($\Leftarrow$) Conversely, given any $q = p^f$, the set of elements in K such that $x^q - x = 0$ is a subfield S of K for it is closed under addition since if $a, b \in S$ then $a + b \in S$ because $(a+b)^q = a^q + b^q$. Similarly, S is closed under multiplication, i.e., $a, b \in S \Rightarrow ab \in S$. Hence S is a field and it remains to show that S has q elements. All the roots of $x^q - x$ are distinct in K since the formal derivative of $qx^{q-1} - 1 = -1$ is coprime with $x^q - x$. Since any two algebraic closures of $\mathbb{F}_p$ are isomorphic, any two fields of $q = p^f$ elements are isomorphic. We let $\mathbb{F}_q$ denote one of these fields. Note that $\mathbb{F}_q^\times$, the subgroup of non-zero elements of $\mathbb{F}_q$, has $q-1$ elements. In fact, it is a cyclic group of order $q-1$. To see this, observe that if $x \in \mathbb{F}_q^\times$ then the order of x, say d, divides $q-1$. Thus $x^d - 1 = 0$. The polynomial $x^d - 1$ has at most d roots in $\mathbb{F}_q$ and they are given by $x, x^2, \ldots, x^d = 1$. Of these roots, $\varphi(d)$ of them have order d. But $\sum_{d|q-1} \varphi(d) = q-1$. Since $\mathbb{F}_q^\times$ has exactly $q-1$ elements there are precisely $\varphi(d)$ elements of order d in $\mathbb{F}_q^\times$ hence $\varphi(q-1)$ elements of order $q-1$. Since $\varphi(q-1) \geq 1$ we see there is one elements of order $\mathbb{F}_q^\times$ of order $q-1$. Thus $\mathbb{F}_q^\times$ is cyclic. □

Definition 70. Recall that if X is a metric space then we say that X is *locally compact* if every point $x \in X$ has a neighbourhood which is compact.

Example 71. $\mathbb{R}$ is locally compact but not compact. Similarly, $\mathbb{Q}_p$ with the metric given by $|\cdot|_p$ is also locally compact but not compact.Too see this, note that $\{y : |y-x|_p \leq 1\} = x + \mathbb{Z}_p$ is compact since $\mathbb{Z}_p$ is compact.

Let F be a field with a non-archimedean valuation $|\cdot|$. Assume that F is locally compact, with respect to the metric induced by the valuation. Let V be a finite-dimensional vector space over F. By a valuation $|\cdot|$ on V which extends $|\cdot|$ on F we mean a map $|\cdot| : V \to \mathbb{R}^{\geq 0}$ such that:

(1) $|x| = 0 \Leftrightarrow x = 0$
(2) $|ax| = |a||x|$ for all $a \in F$ and for all $x \in V$
(3) $|x + y| \leq |x| + |y|$ for all $x, y \in V$.

Remark 72. If V is a field K which is a finite-dimensional extension of F and $|\cdot|$ is a valuation on K which extends $|\cdot|$ on F, then certainly $|\cdot|$ is a valuation on K as a vector space over F. The converse, however, is *not* true. To see this, consider the example given by $K = \mathbb{Q}_p(\sqrt{p})$. Then $\{1, \sqrt{p}\}$ forms a basis for K over $\mathbb{Q}_p$. If we define $|x|_p = |a + b\sqrt{p}|_p = \sup\{|a|_p, |b|_p\}$ then we can check that this is a vector space valuation but it is not a field valuation since $|\sqrt{p}|_p \cdot |\sqrt{p}|_p \neq p^{-1} = |p|_p$.

We say that the two valuations $|\cdot|_1$ and $|\cdot|_2$ on a vector space V are equivalent if a sequence of vectors from V is Cauchy with respect to $|\cdot|_1$ if and only if it is Cauchy with respect to $|\cdot|_2$. This is true if and only if there exist positive real numbers c_1 and c_2 such that for all $x \in V$, we have $c_1|x|_1 \leq |x|_2 \leq c_2|x|_1$.

Theorem 73. *If V is a finite-dimensional vector space over a locally compact field F with valuation $|\cdot|$ then all valuations on V extending $|\cdot|$ on F are equivalent.*

Proof. Let $\{v_1, \ldots, v_n\}$ be a basis for V over F. Define the sup valuation $|\cdot|_{\text{sup}}$ on V by

$$|x|_{\text{sup}} = |a_1v_1 + \cdots + a_nv_n|_{\text{sup}} := \max\{|a_1|, \ldots, |a_n|\}.$$

One can check that $|\cdot|_{\text{sup}}$ is a vector space valuation on V which extends $|\cdot|$ on F. We now show that if $|\cdot|$ is another valuation on V which extends $|\cdot|$ on F then there exist positive real numbers c_1 and c_2 such that

$$c_1|x| \leq |x|_{\text{sup}} \leq c_2|x|$$

for all $x \in V$. Thus any valuation is equivalent to the sup valuation and so any two valuations are equivalent. Notice that for $v \in V$,

$$\begin{aligned} |v| = |a_1v_1 + \cdots + a_nv_n| &\leq |a_1v_1| + |a_2v_2| + \cdots + |a_nv_n| \\ &\leq \sum_{i=1}^{n} |a_i||v_i| \leq n\left(\max_i |a_i|\right) \cdot \max_i |v_i| \\ &= n \max |v_i| \cdot |v|_{\text{sup}}. \end{aligned}$$

Now take $c_1 = \left(n \max_i |v_i|\right)^{-1}$ and we see that $|v|_{\text{sup}} \geq c_1|v|$ for all $v \in V$. To prove that $|\cdot|_{\text{sup}} \leq c_2|v|$ for some $c_2 > 0$, we first let

$$U := \{x \in V : |x|_{\text{sup}} = 1\}.$$

We claim that U is compact with respect to the metric induced by $|\cdot|_{\text{sup}}$, since V is finite-dimensional over a locally compact space. It suffices to remark that every sequence of elements in U has a convergent subsequence in U. The idea is to find a coordinate which has infinitely many tuples such that $|\cdot| = 1$. Next, assume that there is no $\tilde{c_2} > 0$ such that $\tilde{c_2} < |x|$ for all x in U. Then we can find a sequence $(x_i)_i$ with $x_i \in U$ such that $|x_i| \to 0$. Since U is compact, we can find a subsequence x_{i_j} which converges in the sup valuation to some $x \in U$. For every j we have $|x| \leq |x - x_{i_j}| + |x_{i_j}| \leq c_1^{-1}|x - x_{i_j}|_{\text{sup}} + |x_{i_j}|$. But $x_{i_j} \to x$ in the sup valuation and $x_{i_j} \to 0$ with respect to $|\cdot|$ as $j \to \infty$. Thus $|x| \leq 0$ so $|x| = 0$ hence $x = 0$. But $x \in U$ hence $x \neq 0$. Thus these exists $\tilde{c_2} > 0$ such that $|x| > \tilde{c_2}$ for all $x \in U$. Let $v \in V$. Then $v = a_1v_1 + \cdots + a_nv_n$. Note that $|v|_{\text{sup}} = |a_i|$ for some i with $1 \leq i \leq n$. Then $|\frac{v}{a_i}|_{\text{sup}} = 1$, so $|\frac{v}{a_i}| > \tilde{c_2}$ so $|v| > \tilde{c_2}|a_i| = \tilde{c_2}|v|_{\text{sup}}$, hence $\tilde{c_2}^{-1}|v| > |v|_{\text{sup}}$. Take $c_2 = \tilde{c_2}^{-1}$ and the result follows. □

Corollary 74. *Let $V = K$ be a field. Then there is at most one field valuation $|\cdot|$ on K which extends $|\cdot|$ on F.*

Proof. By Theorem 73, any two field valuations on K ar equivalent. Suppose that we have two such valuations $|\cdot|_1$ and $|\cdot|_2$ on K. If they are distinct then there exists an $x \in K$ with $|x|_1 \neq |x|_2$. We may suppose that $|x|_1 < |x|_2$. Then since the valuations are equivalent there is a positive number c_1 such that $|y|_1 > c_1|y|_2$, for all $y \in K$. But notice that for $N \in \mathbb{Z}_+$ sufficiently large, we have $|x^N|_1 = |x|_1^N < c_1|x|_2^N = c_1|x^N|_2$, which is a contradiction. Thus $|x|_1 = |x|_2$ for all $x \in K$. □

12. October 30

Suppose that K is a finite extension of a locally compact field F with a valuation $|\cdot|$ on F. We have already seen that there is at most one (field) valuation on K which extends $|\cdot|$ on F. Suppose also that $K = F(\alpha)$ and that the minimal polynomial of α over K is $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ with $a_i \in F$. We may suppose that the characteristic polynomial of F is zero and so the roots of f are distinct (say $\alpha = \alpha_1, \ldots, \alpha_n$). So $f(x) = \prod_{i=1}^{n}(x - \alpha_i)$. We define the norm from K to F of α, denoted $N_{K/F}(\alpha)$, by

$$N_{K/F}(\alpha) := \prod_{i=1}^{n} \alpha_i = (-1)^n a_0.$$

Observe that K is an n-dimensional vector space over F and multiplication by α is a F-linear map from K to K. Consider the basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$. We can represent multiplication by α with respect to this basis by the matrix A_α

$$A_\alpha = \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{bmatrix}$$

Notice that, by expanding by the first row,

$$\det(A_\alpha) = (-1)^{n+2} a_0 = (-1)^n a_0 = N_{K/F}(\alpha).$$

The determinant is unchanged if we pick a different basis. Suppose next that $\beta \in K$ but $F(\beta) \subsetneq K$. We wish to define $N_{K/F}(\beta)$. Define

$$N_{K/F}(\beta) := \left(N_{F(\beta)/F}(\beta)\right)^{[K:F(\beta)]}.$$

We claim that with this definition that the determinant of the matrix A_β which represents the map from K to K given by multiplication by β is $N_{K/F}(\beta)$. To see this first, let B_β be the matrix associated with the multiplication by β map on $F(\beta)$ with respect to the basis $\{1, \beta, \beta^2, \ldots, \beta^{d_1}\}$ where $d_1 = [F(\beta) : F]$. Next put $d_2 = [K : F(\beta)]$. Let γ be a primitive element for K over $F(\beta)$, so $K = F(\beta)(\gamma)$. Then

$$1, \beta, \beta^2, \ldots, \beta^{d_1-1}, \gamma, \gamma\beta, \ldots, \gamma\beta^{d_1-1}, \ldots, \gamma^{d_2-1}, \gamma^{d_2-1}\beta, \ldots, \gamma^{d_2-1}\beta^{d_1-1}$$

forms a basis for K over F. The matrix A_β given by multiplication by β with respect to the above basis is

$$A_\beta = \begin{bmatrix} B_\beta & & & \\ & B_\beta & & \\ & & \ddots & \\ & & & B_\beta \end{bmatrix}.$$

Thus $\det(A_\beta) = (\det B_\beta)^{d_2} = N_{K/F}(\beta)$. We now observe that $N_{K/F}(\_)$ is a multiplicative map on K since, for any α, β in K,

$$N_{K/F}(\alpha\beta) = \det A_{\alpha\beta} = \det(A_\alpha A_\beta) = \det(A_\alpha)\det(A_\beta) = N_{K/F}(\alpha)N_{K/F}(\beta).$$

Our problem is to figure out how to extend $|\cdot|_p$ on $\mathbb{Q}_p$ to a valuation on $\overline{\mathbb{Q}_p}$, the algebraic closure of $\mathbb{Q}_p$. Let α be algebraic over $\mathbb{Q}_p$ and suppose that $K = \mathbb{Q}_p(\alpha)$ is a finite Galois extension of $\mathbb{Q}_p$ and let $\alpha \in K$. What should $|\alpha|_p$ be? If $\|\cdot\|$ is a valuation extending $|\cdot|_p$ on K and σ is an automorphism of K which fixes $\mathbb{Q}_p$ then we can define another valuation $\|\cdot\|'$ on K which extends $|\cdot|_p$ on $\mathbb{Q}_p$ by defining for x in K,

$$\|x\|' = \|\sigma(x)\|.$$

It is a valuation since for all $x, y \in K$ we have:

(1) $\sigma(xy) = \sigma(x)\sigma(y)$
(2) $\sigma(x) = 0 \Leftrightarrow x = 0$
(3) $\sigma(x+y) = \sigma(x) + \sigma(y)$.

But since there is at most one possible extension of $|\cdot|_p$ to K we see that $\|\cdot\|$ is the same as $\|\cdot\|'$. Thus

$$|N_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)|_p = \|N_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)\| = \prod_{\sigma \in \mathrm{Aut}(K/\mathbb{Q}_p)} \|\sigma(\alpha)\| = \|\alpha\|^n$$
$$\|\alpha\| = |N_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)|_p^{1/n} = |N_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)|^{[\mathbb{Q}_p(\alpha):\mathbb{Q}_p]^{-1}}$$

More generally, if K is a finite extension of $\mathbb{Q}_p(\alpha)$ then

$$\|\alpha\| = |N_{K/\mathbb{Q}_p(\alpha)}|_p^{[K:\mathbb{Q}_p]^{-1}}.$$

Theorem 75 (Hensel's Lemma II)**.** *Suppose $f \in \mathbb{Z}_p[x]$, and let $\overline{f}$ be the reduction of f mod p to an elements of $\mathbb{Z}_p/p\mathbb{Z}_p[x]$. Suppose also that $\overline{f}$ is not identically zero. If $g_0, h_0 \in \mathbb{Z}_p[x]$ with $\overline{g_0}, \overline{h_0}$ relatively prime in $\mathbb{Z}_p/p\mathbb{Z}_p[x]$ such that*

$$f(x) \equiv g_0(x)h_0(x) \pmod{p},$$

then there exist polynomials $g(x), h(x) \in \mathbb{Z}_p[x]$ such that $f(x) = g(x)h(x)$ with $g(x) \equiv g_0(x)$ $\pmod{p}$, $h(x) \equiv h_0(x) \pmod{p}$ and $\deg(g) = \deg(g_0)$.

Proof. We may assume that $\overline{g_0}$ is a monic polynomial of degree r since if

$$\overline{g_0}(x) = ax^r + \cdots \text{ with } a \neq 0,$$

we can replace $\overline{g_0}$ by $a^{-1}\overline{g_0}$ and $\overline{h_0}$ by $a\overline{h_0}$. Further, without loss of generality, we may suppose that $\deg(g_0) = \deg(\overline{g_0})$. We now construct two sequences of polynomials (g_i) and (h_i) in $\mathbb{Z}_p[x]$ with the g_i's of degree r and such that

$$f \equiv g_t h_t \pmod{p^{t+1}}, \tag{14}$$

and

$$g_t \equiv g_{t-1} \pmod{p^t} \text{ and } h_t \equiv h_{t-1} \pmod{p^t}.$$

If we make this construction, then we can take $g = \lim_{t\to\infty} g_t$ and $h = \lim_{t\to\infty} h_t$. Further,

$$g \equiv g_0 \pmod{p} \text{ and } h \equiv h_0 \pmod{p}.$$

Having constructed g_t and h_t, how do we product g_{t+1} and h_{t+1}? Put

$$\begin{aligned} g_{t+1} &= g_t + p^{t+1}u \\ h_{t+1} &= h_t + p^{t+1}v, \end{aligned} \tag{15}$$

where $u, v \in \mathbb{Z}_p[x]$ are to be chosen. Now by (14), $f - g_t h_t = p^{t+1} z$ with $z \in \mathbb{Z}_p[x]$. By (15),

$$g_{t+1}h_{t+1} - f = (g_t h_t - f) + p^{t+1}(h_t u + g_t v) + p^{2t+2}uv.$$

Thus we need to choose u and v so that

$$h_0 u + g_0 v \equiv z \pmod{p}. \tag{16}$$

Hence so that $-z + h_t u + g_t v \equiv 0 \pmod{p}$. Since $h_t \equiv h_0 \pmod{p}$ and $g_t \equiv g_0 \pmod{p}$, it suffices to choose u and v so that $h_0 u + g_0 v \equiv z \pmod{p}$. Since $\overline{h_0}$ and $\overline{g_0}$ are coprime in $\mathbb{Z}_p/p\mathbb{Z}_p[x]$, there exist l and m in $\mathbb{Z}_p[x]$ for which $lh_0 + mg_0 \equiv 1 \pmod{p}$ hence $lh_0 z + mg_0 z \equiv z \pmod{p}$. Write $\overline{l_z} = \overline{k}\overline{g_0} + u^*$ where $\deg u^* < \deg \overline{g_0} = r$. Let u be a polynomial in $\mathbb{Z}_p[x]$ such that $\overline{u} = u^*$ and such that $\deg u = \deg u^*$. Further,

$$h_0 u + (h_0 k + mz) g_0 \equiv z \pmod{p}$$

and we see that if $v = h_0 k + mz$, then (16) holds and the result follows. □

13. November 4

Corollary 76. *If $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Q}_p[x]$ with $a_n \neq 0$ and f is* irreducible, *then*

$$\max_i(|a_i|_p) \le \max(|a_0|_p, |a_n|_p).$$

Proof. Suppose $\max_i(|a_i|_p) = |a_j|_p$ where $0 \le j \le n$ and j is chosen to be maximal. Then $|a_j|_p = p^{-N}$. Put $t(x) := p^{-N} f(x)$, so that $t(x) = b_0 + b_1 x + \cdots + b_n x^n$. Notice that $b_j \not\equiv 0 \pmod{p}$. Then put

$$g_0(x) = b_0 + b_1 x + \cdots + b_j x^j,$$

and $h_0(x) = 1$. Notice that $\bar{g_0}$ and $\bar{h_0}$ are coprime in $\mathbb{Z}_p/p\mathbb{Z}_p[x]$. By Hensel's Lemma II, there exist $g(x), h(x) \in \mathbb{Q}_p[x]$ with $t(x) = g(x)h(x)$ so $f(x) = p^N g(x)h(x)$. Since f is irreducible we see that $j = 0$ or $j = n$. Thus the claim follows, as desired. □

Theorem 77. *Let K be a finite extension over $\mathbb{Q}_p$. The map $|\cdot|_p : K \to \mathbb{R}_{\ge 0}$ given by $|\alpha|_p = |\operatorname{N}_{K/\mathbb{Q}_p}(\alpha)|_p^{1/n}$ where $n = [K : \mathbb{Q}_p]$ is the* unique *valuation which extends $|\cdot|_p$ on $\mathbb{Q}_p$.*

Proof. Certainly $|\cdot|_p$ extends the valuation on $\mathbb{Q}_p$. Further, it suffices to show that $|\cdot|_p$ is a valuation on K since we have already proved that there can be at most one such valuation on K. Plainly, $\alpha_p = 0 \Leftrightarrow \alpha = 0$. Furthermore $|\cdot|_p$ is multiplicative on K since $\operatorname{N}_{K/\mathbb{Q}}$ is multiplicative. Thus it remains to check that for all $\alpha, \beta \in K$, we have $|\alpha + \beta|_p \le \max\{|\alpha|_p, |\beta|_p\}$.

We may assume α and β are non-zero. On dividing through by β we see that it suffices to prove that if $\gamma \in K$ then

$$|\gamma + 1|_p \le \max(|\gamma|_p, 1).$$

Let $x^m + a_{m-1}x^{m-1} + \cdots + a_0$ be the minimal polynomial for γ over $\mathbb{Q}_p$. Then $|\gamma|_p = |a_0|_p^{1/m}$. Further, the irreducible polynomial of $\gamma + 1$ over $\mathbb{Q}_p$ is

$$(x-1)^m + a_{m-1}(x-1)^{m-1} + \cdots + a_0,$$

and so

$$|\gamma + 1|_p = |(-1)^m + a_{m-1}(-1)^{m-1} + \cdots + a_0|_p^{1/m}.$$

By Corollary 76, we have

$$|\gamma+1|_p \le \max(1,|a_0|_p)^{1/m} \le \max(1,|a_0|_p^{1/m}) = \max(1,|\gamma|_p).$$

Therefore, $|\cdot|_p$ is indeed a valuation on K, as required. ☐

Recall that the algebraic closure $\overline{\mathbb{Q}_p}$ over $\mathbb{Q}_p$ is a union of the finite extensions of $\mathbb{Q}_p$. Also, if α is algebraic over $\mathbb{Q}_p$ we have that $|\alpha|_p$ does not change when we pass to field extensions of $\mathbb{Q}_p(\alpha)$. By virtue of these two facts, we see that $|\cdot|_p$ extends to a valuation on $\overline{\mathbb{Q}_p}$. Hence if $\alpha \in \overline{\mathbb{Q}_p}$ with minimal polynomial $x^m + a_{m-1}x^{m-1} + \cdots + a_0$ then

$$|\alpha|_p = |a_0|_p^{1/m}.$$

Let K be a finite extension of $\mathbb{Q}_p$ with $[K:\mathbb{Q}_p]=n$. For $\alpha in K$ we define $\operatorname{ord}_p \alpha$ by

$$\operatorname{ord}_p \alpha := -\frac{\log|\alpha|_p}{\log p} = -\frac{\log|\operatorname{N}_{K/\mathbb{Q}_p}(\alpha)|^{1/n}}{\log p} = -\frac{1}{n}\cdot\frac{\log|\operatorname{N}_{K/\mathbb{Q}_p}(\alpha)|_p}{\log p}.$$

The image of K under the map ord_p is a subset of $\frac{1}{n}\mathbb{Z}$. Even better, this is not just a subset, but is a *subgroup*. For any $\alpha,\beta \in K$ we have $\operatorname{ord}_p \alpha\beta = \operatorname{ord}_p \alpha + \operatorname{ord}_p \beta$, so the image is a subgroup of $\frac{1}{n}\mathbb{Z}$ and has the form $\frac{1}{e}\mathbb{Z}$ for the smallest positive integer e.

Definition 78. The integer e as defined above is called the *index of ramification of K over $\mathbb{Q}_p$*. if $e=1$ we say that K is *unramified over $\mathbb{Q}_p$*. If $e=n$ then we say that K is *totally ramified over $\mathbb{Q}_p$*.

Remark 79. If $\pi \in K$ with $\operatorname{ord}_p \pi = \frac{1}{e}$ then any $x \in K$ with $x \neq 0$ we can write it *uniquely* in the form $\pi^m u$ with $m \in \mathbb{Z}$ and u such that $|u|_p = 1$. Then $e \cdot \operatorname{ord}_p x = m$.

Definition 80. Let

$$f(x) = x^e + a_{e-1}x^{e-1} + \cdots + a_0, \tag{17}$$

with $a_i \in \mathbb{Z}_p$ and $a_i \not\equiv 0 \pmod p$ for $i=0,1,\dots,e-1$ and $a_0 \not\equiv 0 \pmod{p^2}$. Then f is an *Eisenstein polynomial* and by Eisenstein's criterion f is irreducible.

Lemma 81. *If K is a totally ramified finite extension of $\mathbb{Q}_p$ and $\pi \in K$ with $\operatorname{ord}_p \pi = \frac{1}{e}$ then π satisfies an Eisenstein equation. Conversely, if α is a root of an Eisenstein polynomial as in* (17) *over $\mathbb{Q}_p$ then $\mathbb{Q}_p(\alpha)$ is a totally ramified extension of $\mathbb{Q}_p$.*

Proof. Since the coefficients a_i of the minimal polynomial of π over $\mathbb{Q}_p$ are elementary symmetric polynomials in the conjugates of π, we see that $|a_i|_p < 1$ for $i=0,1,\dots,e-1$. Further, since $\operatorname{ord}_p \pi = \frac{1}{e}$, we see that $|a_0|_p = p^{-1}$.

Now conversely, suppose that α is a root of an Eisenstein polynomial as in (17). Then α is of degree e over $\mathbb{Q}_p$ since f is irreducible over $\mathbb{Q}_p$. Further, $|\pi|_p^e = |a_0|_p = p^{-1}$. Thus, $|\alpha|_p = p^{-1/e}$ and so $\mathbb{Q}_p(\alpha)$ is totally ramified. ☐

Definition 82. We say a totally ramified extension of $\mathbb{Q}_p$ is *tame* if $p \nmid e$ and *wild* if $p \mid e$.

Lemma 83. *Let K be a finite extension of $\mathbb{Q}_p$. K is complete with respect to $|\cdot|_p$.*

Proof. Let $w_1, w_2, \ldots, w_n$ be a basis for K over $\mathbb{Q}_p$. Let $(\gamma_i)_{i=1}^{\infty}$ be a Cauchy sequence of elements of K. Then we have $\gamma_i = a_{1i}w_1 + \cdots + a_{ni}w_n$ with $a_{1i}, \ldots, a_{ni} \in \mathbb{Q}_p$. Since $|\gamma_i - \gamma_j|_p \to 0$ as $\min(i,j) \to \infty$ and since all finite-dimensional vector space valuations over $\mathbb{Q}_p$ are equivalent, we see by the sup vector space valuation on K that $(a_{ji})_{i=1}^{\infty}$ is a Cauchy sequence in $\mathbb{Q}_p$ for $j = 1, 2, \ldots, n$. Since $\mathbb{Q}_p$ is complete, there exists $A_j \in \mathbb{Q}_p$ such that $A_j = \lim_{i\to\infty} a_{ij}$ for $j = 1, 2, \ldots, n$. Therefore $(\gamma_i)_{i=1}^{\infty}$ converges to $A_1w_1 + \cdots + A_nw_n$ which is in K. □

Notation. Let K be a finite extension of $\mathbb{Q}_p$. Define $A := \{x \in K : |x|_p \leq 1\}$ and $M := \{x \in K : |x|_p < 1\}$.

Remark 84. Consider the quotient A/M consisting of elements $a + M$ with $a \in A$. There is a natural inclusion of $\mathbb{Z}_p/p\mathbb{Z}_p$ into A/M given by $\varphi(a + p\mathbb{Z}_p) = a + M$. We will now show that A/M is of finite degree over $\mathbb{F}_p$. If $n = [K : \mathbb{Q}]$ then in fact $[A/M : \mathbb{F}_p] \leq n$. For any element $a \in A$, let $\overline{A}$ be the element $a + M$ in A/M. To see why $[A/M : \mathbb{F}_p] \leq n$, we will show that if $\overline{a_1}, \ldots, \overline{a_{n+1}} \in A/M$ then they are linearly dependent over $\mathbb{F}_p$.

Then for any $a_1, a_2, \ldots, a_{n+1} \in K$, for which the reductions are $\overline{a_1}, \ldots, \overline{a_{n+1}} \in A/M$, respectively, we have since $[K : \mathbb{Q}_p] = n$ that there exist $b_1, b_2, \ldots, b_{n+1} \in \mathbb{Q}_p$ such that $a_1b_1 + \cdots + a_{n+1}b_{n+1} = 0$. By multiplying through by p^N for an appropriate integer N we can suppose that b_i's are in $\mathbb{Z}_p$ and at least one has p-adic order zero. Then we have

$$\overline{a_1}\overline{b_1} + \cdots + \overline{a_{n+1}}\overline{b_{n+1}} = 0.$$

Since not all of the $\overline{b_i}$'s are zero, we see that $\overline{a_1}, \ldots, \overline{a_{n+1}}$ are linearly dependent over $\mathbb{F}_p$. Thus $[A/M : \mathbb{F}_p] \leq n$.

Definition 85. THe degree of $[A/M : \mathbb{F}_p]$ is called the *residue field degree* and is denoted by f.

Lemma 86. *Let K be a finite extension of $\mathbb{Q}_p$ with ramification index e and residue field degree f. Let A and M be as defined in Notation 14. Let $(\pi_i)_{i=-\infty}^{\infty}$ be a sequence of elements in K with $\operatorname{ord}_p \pi_i = \frac{i}{e}$ for $i \in \mathbb{Z}$. Let $0, c_1, \ldots, c_{p^f-1}$ be elements of A such that $0 + M, c_1 + M, \ldots, c_{p^f-1} + M$ are distinct in A/M. Let $\alpha \in K$ with $\operatorname{ord}_p \alpha = \frac{n}{e}$. Then there exists a* unique *representation α of the form*

$$\sum_{t=n}^{\infty} c_{i_t}\pi_t,$$

where c_{i_t} is chosen from $\{0, c_1, c_2, \ldots, c_{p^f-1}\}$.

Proof. We will first show that α has such representation. Note that $|\frac{\alpha}{\pi^n}|_p = 1$. Thus

$$\frac{\alpha}{\pi^n} \equiv c_{i_n} \pmod{M}.$$

Further, we have $M = \pi A$, and we have

$$\left|\frac{\alpha}{\pi^n} - c_{i_n}\right|_p < 1.$$

Put $\alpha_1 = \frac{\alpha}{\pi^n} - c_{i_n}$. If $\alpha_1 = 0$ we are done. Otherwise, let $\text{ord}_p\, \alpha_1 = \frac{b_1}{e}$ for some positive integer b_1. Thus

$$\alpha = c_{in}\pi_n + \alpha_1\pi_n.$$

Then $\text{ord}_p\, \alpha_1\pi_n = \frac{n+b_1}{e}$. We have

$$\left|\frac{\alpha_1\pi_n}{\pi_{n+b_1}}\right|_p = 1$$

so there exists a representative $c_{i_{n+b_1}}$ such that

$$\left|\frac{\alpha_1\pi_n}{\pi_{n+b_1}} - c_{i_{n+b_1}}\right| < 1.$$

We now put $\alpha_2 = \frac{\alpha_1\pi_n}{\pi_{n+b_1}} - c_{i_{n+b_1}} \in M$. We have

$$\alpha_1\pi_n = \alpha_2\pi_{n+b_1} + c_{i_{n+b_1}}\pi_{n+b_1}$$

with $\text{ord}_p\, \alpha_2\pi_{n+b_1} > \frac{n+b_1}{e}$. Thus

$$\alpha = c_{i_n}\pi)n + c_{i_{n+b_1}}\pi_{n+b_1} + \alpha_2\pi_{n+b_1}.$$

Containing in this way we obtain a Cauchy sequence of partial sums which converges to α, and this gives us the representation. It is immediate to check that this representation is unique. □

Lemma 87. *Let $[K : \mathbb{Q}_p] = n$. Suppose that the index of ramification of K is e and the residue field degree is f. Then $n = ef$.*

Proof. Let π be an element of K with $\text{ord}_p\, \pi = \frac{1}{e}$. Let $w_1, \ldots, w_f$ be elements of A such that $w_1 + M, \ldots, w_f + M$ form a basis for A/M over $\mathbb{F}_p$. Then $\{u_1w_1 + \cdots + u_fw_f + M : 0 \le u_i < p \text{ for } i = 1, 2, \ldots, f\}$ is just A/M. Let the c_i's in the previous proposition be the elements $u_1w_1 + \cdots + u_fw_f$. Then for any $\alpha \in K$ we have a unique representative of the form

$$\alpha = \sum_{t=m}^{\infty} c_{i_t}\pi_t,$$

where $\pi_t = p^{\left\lfloor \frac{t}{e} \right\rfloor}\pi^{t-e\left\lfloor \frac{t}{e} \right\rfloor}$. Put $r_t = t - e\left\lfloor \frac{t}{e} \right\rfloor$ so that $0 \le r_t \le e-1$. Then

$$\alpha = \sum_{t=m}^{\infty}(u_{1_t}w_1 + \cdots + u_{f_t}w_f)\pi^{r_t}p^{\left\lfloor \frac{t}{e} \right\rfloor}.$$

Therefore (note that we can rearrange the terms since the sum is convergent)

$$\alpha = \sum_{j=1}^{f}\sum_{s=0}^{e-1}\left(\sum_{l=\left\lfloor \frac{m}{e} \right\rfloor}^{\infty} i_{j,s,l}p^l\right) w_j\pi^s,$$

for $i_{j,s,l}$ chosen appropriately. Thus $\{w_j\pi^s : j = 1, 2, \ldots, f, s = 0, 1, \ldots, e-1\}$ spans K over $\mathbb{Q}_p$. In particular, we see that $n \le ef$. Note, however, that if we have

$$\sum_{j,s} a_{j,s}w_j\pi^s = 0,$$

with $a_{j,s} \in \mathbb{Q}_p$ not all zero, then we can first suppose that the terms $a_{j,s}$ are in $\mathbb{Z}_p$ by multiplying by an appropriate power of p with some $|a_{j,s}|_p = 1$. Since $w_1 + M, \dots, w_f + M$ are linearly independent over $\mathbb{F}_p$, we see that

$$\left| \sum_{a_{j,s}} \pi^s \right|_p \leq p^{-1}$$

for $j = 1, 2, \dots, f$. But for some pair j, s we have $|a_{j,s}|_p = 1$ and so

$$|a_{j,s}\pi^s|_p = p^{-\frac{s}{e}} \geq p^{-\frac{e-1}{e}}$$

since $0 \leq s \leq e-1$. But then

$$\left| \sum a_{j_s} \pi^s \right|_p = p^{-\frac{e-1}{e}},$$

but this is a contradiction. □

15. November 11

Proposition 88. *Let K be a finite-degree extension of $\mathbb{Q}_p$ with residue field degree f. Then K contains all of the $p^f - 1$ roots of unity. In particularly, K contains a primitive $p^f - 1$-th root of unity.*

Proof. As usual, put $A = \{x \in K : |x|_p \leq 1\}$ and $M = \{x \in K : |x|_p < 1\}$. SInce the residue field degree is f, we have $A/M \cong \mathbb{F}_{p^f}$. Recall that $\mathbb{F}_{p^f}^\times$ is a cyclic group. Then there exists $a_0 \in A$ such that $\overline{a_0}$ generates A/M. Thus $\overline{\alpha_0}, \overline{\alpha_0}^2, \dots, \overline{\alpha_0}^{p^f-1}$ are all distinct in A/M. Let $\pi \in K$ with $\mathrm{ord}_p\, \pi = e^{-1}$ where e is the index of ramification of K. Then $M = \pi A$. We claim that there exists $\alpha \in K$ with $\alpha \equiv \alpha_0 \pmod{\pi}$ for which $\alpha^{p^f-1} = 1$. Since $\overline{\alpha_0}, \overline{\alpha_1}, \dots, \overline{\alpha_0}^{p^f-1}$ are all distinct in A/M we see that α is a primitive $p^f - 1$-th root of unity.

We now will construct inductively as in the proof of Hansel's lemma (Theorem 75). Note that we have $\alpha_0^{p^f-1} \equiv 1 \pmod{\pi}$. Consider $\alpha_0 + \alpha_1\pi$. We have

$$(\alpha_0 + \alpha_1\pi)^{p^f-1} \equiv (\alpha_0^{p^f-1} - 1) + \binom{p^f-1}{1}\alpha^{p^f-2}\alpha_1\pi \pmod{\pi^2}.$$

Since $\alpha_0^{p^f-1} \equiv 1 \pmod{\pi}$ there exists a β_0 such that $\alpha^{p^f-1} - 1 \equiv \beta_0\pi \pmod{\pi^2}$. Thus

$$\begin{aligned}(\alpha_0 + \alpha_1\pi)^{p^f-1} - 1 &\equiv \beta_0\pi + (p^f-1)\alpha_0^{p^f-2}\alpha_1\pi \pmod{\pi^2} \\ &\equiv \beta_0\pi - \alpha_0^{p^f-2}\alpha_1\pi \pmod{\pi^2}.\end{aligned}$$

We now choose α_1 so that

$$\beta_0 - \alpha_0^{p^f-2}\alpha_1 \equiv 0 \pmod{\pi}.$$

That is, take α_1 so that

$$\alpha_1 \equiv \frac{\beta_0}{\alpha_0^{p^f-2}} \pmod{\pi}.$$

Therefore, $(\alpha_0 + \alpha_1\pi)^{p^f-1} \equiv 1 \pmod{\pi^2}$. Next, we need to choose α_2 appropriately so that

$$(\alpha_0 + \alpha_1\pi + \alpha_2\pi^2)^{p^f-1} \equiv 1 \pmod{\pi^3}.$$

Continuing in this way, we find a sequence $\alpha_1, \alpha_2, \dots \in A$ such that the sequence $\alpha_0, \alpha_0 + \alpha_1\pi, \alpha_0 + \alpha_1\pi + \alpha_2\pi^2 + \cdots$ is a Cauchy sequence which converges to an element $\alpha \in K$ with the property that

$$\alpha^{p^f-1} \equiv 1 \pmod{\pi} \text{ and } \alpha \equiv \alpha_0 \pmod{\pi}.$$

We can preform the same construction for $\overline{\alpha_0}, \dots, \overline{\alpha_0}^{p^f-1}$ to get all the $p^f - 1$-th roots of unity. □

Proposition 89. *For each positive integer f there is* exactly one *unramified extension of $\mathbb{Q}_p$ of residue field degree f. It can be obtained by adjoining a primitive $p^f - 1$-th root of unity to $\mathbb{Q}_p$.*

Proof. Let $\overline{\alpha_0}$ be a generator of $\mathbb{F}_{p^f}$ over $\mathbb{F}_p$ with minimal polynomial $\overline{g}(x) = x^f + \overline{\alpha_{f-1}}x^{f-1} + \cdots + \overline{\alpha_0}$ where we may suppose that $\overline{\alpha_{f-1}}, \dots, \overline{\alpha_0}$ are such that $a_{f-1}, \dots, a_0$ are elements of $\mathbb{Z}_p$. Put $g(x) = x^f + a_{f-1}x^{f-1} + \cdots + a_0$. Notice that $g(x) \in \mathbb{Z}_p[x]$ is irreducible over $\mathbb{Q}_p$ since $\overline{g}$ is irreducible. Let α be a root of $g(x)$ and put $K = \mathbb{Q}_p(\alpha)$. Note that $[K : \mathbb{Q}_p] = f$. Then the residue field of K contains a root of $\overline{g}$ and so $[A/M : \mathbb{F}_p] \geq f$. But then $[A/M : \mathbb{F}_p] \leq [K : \mathbb{Q}_p]$ hence $f = [K : \mathbb{Q}_p] = [A/M : \mathbb{F}_p]$. In particular, we see that $K = \mathbb{Q}_p(\alpha)$ is unramified over $\mathbb{Q}_p$. Thus for each positive f there is an unramified extension of $\mathbb{Q}_p$ of degree f over $\mathbb{Q}_p$. By Proposition 88 every unramified extension K of $\mathbb{Q}_p$ of degree f contains a primitive $p^f - 1$-th root of unity (say β). Then $\mathbb{Q}_p(\beta) \subseteq K$. But $[\mathbb{Q}_p(\beta) : \mathbb{Q}_p] = f$ and so $K = \mathbb{Q}_p(\beta)$ since the powers of β are distinct mod p. Thus the uniqueness follows. □

Notation. For any positive integer f, let K_f^{unram} denote the field $\mathbb{Q}_p(\beta)$ where β is a primitive $p^f - 1$-th root of unity.

Proposition 90. *Let K be a degree n extension of $\mathbb{Q}_p$ with index of ramification e and residue field degree f. Then $K = K_f^{\text{unram}}(\pi)$ where π is the root of an Eisenstein polynomial with coefficients in K_f^{unram}.*

Proof. We have $[K : \mathbb{Q}_p] = n = ef$. Let π be an element of K with $\operatorname{ord}_p \pi = e^{-1}$. Plainly K contains K_f^{unram} since the residue field degree is f. Let $g(x)$ be the minimal polynomial of π over K_f^{unram}. Then

$$g(x) = \prod_{i=1}^{t}(x - \pi_i),$$

where $\pi = \pi_1$. But we know that $|\pi_i|_p = |\pi|_p$ for $i = 1, 2, \dots, t$. Then

$$g(x) = x^t + a_{t-1}x^{t-1} + \cdots + a_0$$

with $a_0, \dots, a_{t-1}$ in K_f^{unram}. Note that $a_0 = \pi_1 \dots \pi_t$, and so $\operatorname{ord}_p a_0 = e^{-1} + \cdots + e^{-1} = te^{-1}$. But $a_0 \in K_f^{\text{unram}}$ so te^{-1} is an integer hence t is a positive multiple of e. Since $[K : \mathbb{Q}_p] = ef$ and $[K : \mathbb{Q}_p] = [K : K_f^{\text{unram}}] \cdot [K_f^{\text{unram}} : \mathbb{Q}_p] = [K : K_f^{\text{unram}}] \cdot f$, it follows that $t = e$. Furthermore, $|a_0|_p = p^{-1}$ and $|a_i|_p < 1$ for $i = 0, 1, \dots, p-1$ since the a_i's are elementary symmetric functions in the π_i's. Thus g is an Eisenstein polynomial. □

Corollary 91. *Let $[K : \mathbb{Q}_p] = n = ef$, and let $\pi \in K$ with $\operatorname{ord}_p \pi = e^{-1}$. Then every non-zero $\alpha \in K$ has a* unique *representation of the form*

$$\alpha = \sum_{i=m}^{\infty} a_i \pi^i, \tag{18}$$

where $m = e \cdot \operatorname{ord}_p \alpha$*, and the set of* a_i*'s is the set of roots of* $x^{p^f} - x$ *in* K*.*

Proof. This follows from the fact that there are p^f a_i's and they are representatives of distinct cosets mod M. □

Definition 92. The a_i's in (18) is known as the *Teichmüller digits*.

Remark 93. $\mathbb{Q}_p^{\text{unram}}$ is the union of all unramified extensions of $\mathbb{Q}_p$. Then $\mathbb{Z}_p^{\text{unram}}$ is the integral closure of $\mathbb{Z}_p$ in $\mathbb{Q}_p^{\text{unram}}$.

16. November 13

Lemma 94 (Krasner's lemma)**.** *Let* $a, b \in \overline{\mathbb{Q}_p}$ *and let* $a = a_1, a_2, \dots, a_n$ *be the conjugates of* a *over* $\mathbb{Q}_p$*. If*

$$|a - b|_p < |a - a_i|_p$$

for $i = 2, 3, \dots, n$*, then* $\mathbb{Q}_p(a) \subseteq \mathbb{Q}_p(b)$*.*

Proof. Assume that $a \notin \mathbb{Q}_p(b)$. Let σ be a non-trivial isomorphism of $\mathbb{Q}_p(a, b)$ into $\overline{\mathbb{Q}_p}$ which fixes $\mathbb{Q}_p(b)$. Suppose, without loss of generality, that $\sigma(a) = a_2$. Then for all $x \in \mathbb{Q}_p(a, b)$, we have $|x|_p = |\sigma(x)|_p$. Therefore

$$\begin{aligned} |b - a|_p &= |\sigma(b - a)|_p = |\sigma(b) - \sigma(a)|_p \\ &= |\sigma(b) - a_2|_p = |b - a_2|_p. \end{aligned}$$

Then

$$|a_2 - a|_p = |(a_2 - b) + (b - a)|_p \le \max(|a_2 - b|_p, |b - a|_p) = |b - a|_p.$$

This is a contradiction, so the claim follows. □

Theorem 95. $\overline{\mathbb{Q}_p}$ *is not complete with respect to* $|\cdot|_p$*.*

Proof. We will give a Cauchy sequence of elements of $\overline{\mathbb{Q}_p}$ which does not converge to an element of $\overline{\mathbb{Q}_p}$. Since any finite extension K of $\mathbb{Q}_p$ is complete with respect to $|\cdot|_p$, our sequence will have to run through elements of arbitrarily large degree. First, we remark that if i and j are positive integers with $j < i$ then $p^{2^j - 1} \mid p^{2^i} - 1$. This follows, since $y - 1 \mid y^{2^{i-j}} - 1$ on taking $y = 2^j$. Let b_i be a primitive $p^{2^i} - 1$-th root of unity for $i = 0, 1, 2, \dots$. Observe that if $j < i$ then $b_j^{p^{2^i} - 1} = 1$, since $p^{2^j} - 1 \mid p^{2^i} - 1$. Put $N_0 = 0$ and $a_0 = b_0 p^{N_0}$. We define N_i and a_i inductively by the following rule. Assume that N_i and

$$a_i = \sum_{j=0}^{i} b_j p^{N_j}$$

have been determined. Then we choose N_{i+1} so that a_i does not satisfy any congruence of the form

$$\alpha_n a_i^n + \cdots + \alpha_0 \equiv 0 \pmod{p^{N_{i+1}}},$$

with $\alpha_i \in \mathbb{Z}_p$ for $i = 0, 1, \dots, n$ and such that not all $\alpha_i \equiv 0 \pmod p$ for any non-negative integer n with $n < 2^i$. Such an integer N_{i+1} exists since otherwise a_i would be a root of a polynomial of degree less than 2^i over $\mathbb{Q}_p$. To see this, note that if there is no such N_{i+1} then for each integer j with $j > N_i$, then a_i satisfies a congruence

$$\alpha_{n,j} a_i^n + \cdots + \alpha_{0,j} \equiv 0 \pmod{p^j}$$

with $\alpha_{k,j} \in \mathbb{Z}_p$ for $k = 0, \ldots, n$ not all $\alpha_{k,j} \equiv 0 \pmod p$. Then there exists an infinite subsequence with

$$(\alpha_{n,j_t}, \ldots, \alpha_{0,j_t})$$

a fixed vector mod p^j. Within this subsequence we can find a further infinite (sub)subsequence with a fixed vector mod p^{j+1}. In the limit, this gives us a polynomial of degree less than 2^i which has a_i as a root. This cannot be the case, however, since the degree of a_i over $\mathbb{Q}_p$ is 2^i. To see this, we argue as follows.

First, observe that $\mathbb{Q}_p(a_i) \subseteq \mathbb{Q}_p(b_i)$ since $b_j \in \mathbb{Q}_p(b_i)$ for $j = 0, 1, \ldots, i$. Secondly, we note that $\mathbb{Q}_p(a_i) = \mathbb{Q}_p(b_i)$: otherwise, there exists a non-trivial embedding σ of $\mathbb{Q}_p(b_i)$ into $\overline{\mathbb{Q}_p}$ which fixes $\mathbb{Q}_p(a_i)$. Thus

$$\sum_{j=0}^{i} b_j p^{N_j} = a_i = \sigma(a_i) = \sum_{j=0}^{i} \sigma(b_j) p^{N_j}.$$

Notes that $\operatorname{ord}_p p = 1 = e^{-1}$ with can apply Corollary 91 with $\pi = p$ to see that our representation of a_i is unique. In particular, $b_j = \sigma(b_j)$ for $j = 1, 2, \ldots, i$. Hence $b_i = \sigma(b_i)$. But σ is *non-trivial*, so $\sigma(b_i) \neq b_i$. Thus $\mathbb{Q}_p(a_i) = \mathbb{Q}_p(b_i)$, so the degree of a_i over $\mathbb{Q}_p$ is 2^i. We then have

$$a_{i+1} = \sum_{j=0}^{i+1} b_j p^{N_j}.$$

The sequence $(a_j)_j$ is a Cauchy sequence since $|b_j|_p \leq 1$ for $j = 1, 2, \ldots$. Thus it converges to $a \in \overline{\mathbb{Q}_p}$. Then a is the root of a polynomial of degree t over $\mathbb{Q}_p$. Thus $\alpha_t a^t + \cdots + \alpha_0 = 0$, with α_j's in $\mathbb{Z}_p$ not all $\alpha_j \equiv 0 \pmod p$. Take $2^i > t$. Ceratinly, $a \equiv a_i \pmod{p^{N_{i+1}}}$. Thus

$$\alpha_t a_i^t + \cdots + \alpha_0 \equiv 0 \pmod{p^{N_{i+1}}},$$

which contradicts our choice of N_{i+1}. The claim follows. $\square$

17. November 18

Second proof of Theorem 95. We define b_i as a primitive $p^{2^{i^2}} - 1$-th root of unity and put

$$c_i = \sum_{j=0}^{i} b_j p^j.$$

The sequence (c_i) is clearly a Cauchy sequence of elements of $\overline{\mathbb{Q}_p}$. Suppose that the sequence converges to an element $c \in \overline{\mathbb{Q}_p}$. Let d be the degree of c over $\mathbb{Q}_p$, i.e., $d = [\mathbb{Q}_p(c) : \mathbb{Q}_p]$. Recall that $[\mathbb{Q}_p(b_i) : \mathbb{Q}_p] = 2^{i^2}$, and that $\mathbb{Q}_p(b_j) \in \mathbb{Q}_p(b_{j+1})$ for $j = 0, 1, 2, \ldots$. Thus $[\mathbb{Q}_p(b_{j+1}) : \mathbb{Q}_p(b_j)] = \frac{2^{(j+1)^2}}{2^{j^2}} = 2^{2j+1}$. Consider

$$c_{d+1} = \sum_{j=0}^{d+1} b_j p^j.$$

Since

$$c - c_{d+1} = \sum_{j \geq d+2} b_j p^j,$$

and further $|b_j|_p = 1$ for all j, it follows that $|c - c_{d+1}|_p = p^{-(d+2)}$. Let σ be an automorphism of $\overline{\mathbb{Q}_p}$ which fixes $\mathbb{Q}_p$. Then

$$|c - c_{d+1}|_p = |\sigma(c - c_{d+1})|_p = |\sigma(c) - \sigma(c_{d+1})|_p = p^{-(d+2)}.$$

Note that $2^{2d+1} \geq d + 1$. Since the degree of $\mathbb{Q}_p(b_{d+1})$ over $\mathbb{Q}_p(b_d)$ is 2^{2d+1} we can find $d+1$ automorphisms $\sigma_1, \ldots, \sigma_{d+1}$ of $\overline{\mathbb{Q}_p}$ which fixes $\mathbb{Q}_p(b_d)$ and for which $\sigma_1(b_{d+1}), \ldots, \sigma_{d+1}(b_{d+1})$ are distinct. Then if $i \leq l$ we have $\sigma_i(c_{d+1}) - \sigma_l(c_{d+1}) = (\sigma_i(b_{d+1}) - \sigma_l(b_{d+1}))p^{d+1}$. Since $\sigma_i(b_{d+1})$ and $\sigma_l(b_{d+1})$ are distinct $p^{2(d+1)^2-1}$-th roots of unity, we have $|\sigma_i(b_{d+1}) - \sigma_l(b_{d+1})|_p = 1$ hence

$$|\sigma_i(c_{d+1}) - \sigma_l(c_{d+1})|_p = p^{-(d+1)}.$$

Therefore,

$$\begin{aligned}|\sigma_i(c) - \sigma_l(c)|_p &= |(\sigma_i(c_{d+1}) - \sigma_l(c_{d+1})) - (\sigma_i(c_{d+1}) - \sigma_i(c)) + (\sigma_l(c_{d+1}) - \sigma_l(c))|_p \\ &= p^{-(d+1)}.\end{aligned}$$

Thus we see that $\sigma_i(c) \neq \sigma_l(c)$ whenever $l \neq i$. In particular, c has at least $d+1$ conjugates contradicting the fact that the degree of c over $\mathbb{Q}_p$ is d. □

Note that c is transcendental over $\mathbb{Q}_p$. The construction can be modified to give uncountably many such c. For example, for each sequence $(\varepsilon_1, \varepsilon_2, \ldots)$ with $\varepsilon_i \in \{0, 1\}$ we can associate to $c_{(\varepsilon)} = c_{(\varepsilon_1, \varepsilon_2, \ldots)}$, where we put

$$c_{(\varepsilon)} = \sum_{i=0}^{\infty} \widehat{b_i} p^i,$$

where

$$\widehat{b_i} = \begin{cases} b_i & (i \equiv 0 \pmod 2) \\ \varepsilon_{\frac{i+1}{2}} b_i & (i \equiv 1 \pmod 2). \end{cases}$$

We see that $c_{(\varepsilon)}$ is transcendental over $\mathbb{Q}_p$.

We now define Ω_p to be the completion of $\overline{\mathbb{Q}_p}$ with respect to $|\cdot|_p$. Ω_p is the set of equivalence classes of Cauchy sequences of elements of $\overline{\mathbb{Q}_p}$. Two sequences (a_i) and (b_i) are said to be equivalent if and only if $\lim |a_i - b_i|_p = 0$. Ω_p is in fact a field under the usual definition of $+$ and $\cdot$. Further we can extend $|\cdot|_p$ by putting $|[(a_i)]|_p = \lim |a_i|_p$. Note that the limit exists since the sequence is Cauchy, and $a = [(a_i)]$ does not depend on the choice of representative. Further, we define ord_p on Ω_p by

$$\mathrm{ord}_p\, a := -\frac{\log |a|_p}{\log p}.$$

Theorem 96. *Ω_p is algebraically closed.*

Proof. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ with $a_i \in \Omega_p$. It suffices to show that f has a root in Ω_p. For $i = 0, 1, \ldots, n-1$, let $(a_{i,j})_j$ be a Cauchy sequence of elements of $\overline{\mathbb{Q}_p}$ which converges to a_i or equivalently which represents a_i. Put

$$g_j(x) = x^n + a_{n-1,j}x^{n-1} + \cdots + a_{0,j}$$

for $j = 1, 2, \ldots$. Let $(r_{i,j})_{i=1}^n$ be the roots of g_j for $j = 1, 2, \ldots$. We will prove that for each j we can find an integer i_j with $1 \le i_j \le n$ so that $(r_{i_j,j})_{j=1}^n$ is a Cauchy sequence. Let $r = [(r_{i_j,j})_{j=1}^\infty]$. Then

$$f(r) = \lim_{j\to\infty} f(r_{i_j,j}) = \lim_{j\to\infty} g_j(r_{i_j,j}) = 0,$$

as required. Now it remains to show that we can actually find a Cauchy sequence that works.

Note that if $\theta \in \overline{\mathbb{Q}_p}$ and satisfies some equation, say,

$$\theta^n + b_{n-1}\theta^{n-1} + \cdots + b_0 = 0$$

with $b_i \in \mathbb{Q}_p$. Then $|\theta^n|_p = |-(b_{n-1}\theta^{n-1} + \cdots + b_0)|_p$, and since $|\cdot|_p$ is non-archimedean we have

$$|\theta|_p^n \le \max_{0\le j\le n-1}(|b_j|_p|\theta|_p^j).$$

Therefore, we have

$$|\theta|_p \le \max_{0\le j\le n-1}(1, |b_j|_p),$$

from which it follows

$$|\theta^n|_p \le \max_{0\le j\le n-1}(1, |b_j|_p^n).$$

Thus if $g \in \mathbb{Q}_p[x]$ and $g(\theta) = 0$ then $|\theta^n|_p \le C(g)$, where $C(g)$ is a positive number which depends on g only. We now show that we can choose the i_j's so that $(r_{i_j,j})_{j=1}^\infty$ is Cauchy. Suppose that the first j terms r_{i_j} have been chosen. Consider

$$|g_{j+1}(r_{i_j,j}) - g_j(r_{i_j,j})|_p = |g_{j+1}(r_{i_j,j})|_p = \prod_{i=1}^n |(r_{i,j+1} - r_{i_j,j})|_p,$$

and

$$|g_{j+1}(r_{i_j,j}) - g_j(r_{i_j,j})|_p \le \delta_j \max(1, |r_{i_j,j}|_p)^n \le \delta_j C(g_j) \le \delta_j C,$$

for some fixed positive number C and $\delta_j = \max\limits_{0\le i\le n-1} |a_{i,j+1} - a_{i,j}|_p$. But $\delta_j \to 0$ as $j \to \infty$. At each stage choose $r_{i,j+1}$ to be the closest p-adically to $r_{i_j,j}$. Since $\delta_j \to 0$ as $j \to \infty$ the resulting sequence is indeed Cauchy, as required. □

Definition 97. Ω_p is sometimes denoted by $\mathbb{C}_p$.

18. November 20

Consider extending $|\cdot|_p$ on $\mathbb{Q}$ to a finite extension K of $\mathbb{Q}$. Suppose $[K : \mathbb{Q}] = n$ and that $\alpha \in \mathbb{C}$ for which $K = \mathbb{Q}(\alpha)$. Let f be the minimal polynomial for α over $\mathbb{Q}$. Suppose that

$$f(x) = \prod_{i=1}^n (x - \alpha_i),$$

where we may take $\alpha \in \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$. We may order the roots α_i of f so that $\alpha_1, \ldots, \alpha_r$ are real and so that $\alpha_{r+1}, \ldots, \alpha_{r+2s}$ are not real with $\alpha_{r+i} = \overline{\alpha_{r+s+i}}$ for all $i = 1, 2, \ldots, s$. There are n embeddings of K in $\mathbb{C}$ which fix $\mathbb{Q}$ (say $\sigma_1, \sigma_2, \ldots, \sigma_n$) where $\sigma_i(\alpha) = \alpha_i$ for all $1 \le i \le n$. We define $r + s$ archimedean valuations on K given by

$$|\gamma|_i = |\sigma_i(\gamma)|$$

for all $\gamma \in K$ where $|\cdot|$ refers to the ordinary absolute value on $\mathbb{C}$. This gives the complete list of archimedean valuations of K up to equivalence. Note that these $r+s$ valuations on K extend $|\cdot|$ on $\mathbb{Q}$.

As for non-archimedean valuations, there is the trivial valuation. Also we can consider the extensions of $|\cdot|_p$. Let $\mathcal{O}_K$ be the ring of algebraic integers of K. There is unique factorization (up to ordering) of ideals of $\mathcal{O}_K$ into prime ideals. Each prime ideals of $\mathcal{O}_K$ divides (p), the principal ideal generated by a prime element p. We have

$$(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_t^{e_t},$$

where $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ are distinct prime ideals and $e_1, \ldots, e_t$ are positive integers. For any prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, we define the $\mathrm{ord}_\mathfrak{p}$ function for $\gamma \in \mathcal{O}_K \setminus \{0\}$ to be the exponent of $\mathfrak{p}$ in the prime ideal factorization of the principal ideal generated by γ in $\mathcal{O}_K$. We can then extend $\mathrm{ord}_\mathfrak{p}$ to $K \setminus \{0\}$ by writing an element $\theta \in K \setminus \{0\}$ as $\gamma_1\gamma_2^{-1}$ where $\gamma_1, \gamma_2 \in \mathcal{O}_K \setminus \{0\}$ and putting $\mathrm{ord}_\mathfrak{p}\theta = \mathrm{ord}_\mathfrak{p}\gamma_1 - \mathrm{ord}_\mathfrak{p}\gamma_2$. On scan check that ord_p is well-defined since the definition does not depend on the choice of γ_1 and γ_2.

For any prime $\mathfrak{p}$ of $\mathcal{O}_K$, we define the norm of $\mathfrak{p}$, say $N\mathfrak{p}$, to be the cardinality of $\mathcal{O}_K/\mathfrak{p}$. Then $N\mathfrak{p} = p^{f_\mathfrak{p}}$ for some positive integer $f_\mathfrak{p}$. Further we have the norm is multiplicative so

$$N(p) = (N\mathfrak{p}_1)^{e_1} \cdots (N\mathfrak{p}_t)^{e_t},$$

so

$$p^n = p^{e_1 f_1 + \cdots + e_t f_t},$$

hence $n = e_1 f_1 + \cdots + e_t f_t$. We define $|\cdot|_\mathfrak{p}$ for each prime ideal in $\mathcal{O}_K$ by

$$|\gamma|_\mathfrak{p} = N\mathfrak{p}^{-\frac{\mathrm{ord}_\mathfrak{p}(\gamma)}{e_\mathfrak{p} f_\mathfrak{p}}} = p^{-\frac{\mathrm{ord}_\mathfrak{p}(\gamma)}{e_\mathfrak{p}}}.$$

This defines a valuation on K. To gather with the trivial valuation, this gives us the complete collection of non-archimedean valuations of K, up to equivalence. Notice that $|\cdot|_{\mathfrak{p}_i}$ extends $|\cdot|_p$ on $\mathbb{Q}$, for $i = 1, 2, \ldots, t$. Recall that for $x \in \mathbb{Q} \setminus \{0\}$ we have

$$|x| \prod_p |x|_p = 1.$$

This is the product formula for $\mathbb{Q}$. But this doesn't work for K! To recover the product formula for K, we need a different way of normalization. We now put, for $x \in K \setminus \{0\}$,

$$\|x\|_i = |x|_i^{g(i)}$$

for $i = 1, 2, \ldots, r+s$ where

$$g(i) = \begin{cases} 1 & (i = 1, 2, \ldots, r) \\ 2 & (i = r+1, \ldots, r+s). \end{cases}$$

further we put, for $x \in K \setminus \{0\}$,

$$\|x\|_{\mathfrak{p}_i} = |x|_{\mathfrak{p}_i}^{e_{\mathfrak{p}_i} f_{\mathfrak{p}_i}}$$

for $i = 1, 2, \ldots, t$. Then for all $x \in K \setminus \{0\}$,

$$\prod_{i=1}^{r+s} \|x\|_i \cdot \prod_{\mathfrak{p} \in \mathcal{O}_K} \|x\|_\mathfrak{p} = 1. \tag{19}$$

Definition 98. The formula (19) is known as *the product formula for K*. The $r+s$ valuations $\|\_\|_i$ for $i = 1, 2, \dots, r+s$ are said to be valuations with the prime at infinity. Note that

$$\prod_{i=1}^{r+s} \|x\|_i = |N_{K/\mathbb{Q}}(x)|.$$

18.1. **A setting where p-adic analysis arises.**

Definition 99. A *quadratic form in n variables $x_1, \dots, x_n$* is a homogeneous polynomial in $x_1, x_2, \dots, x_n$ of degree 2.

There is a vast literature surrounding quadratic forms. First, consider forms over $\mathbb{Z}$. One might ask if the form represents every positive integer. This is not the case for $x_1^2 + x_2^2$ or $x_1^2 + x_2^2 + x_3^2$. But this can be done in four squares, as Lagrange showed in 1770.

Theorem 100 (Lagrange's four-square theorem)**.** *Every positive integer is represented by $x_1^2 + x_2^2 + x_3^2 + x_4^2$.*

Ramanujan considered the question for forms $ax_1^2 + bx_2^2 + cx_3^2 + dx_4^2$ with a, b, c, d positive integer. He found 54 triples (a, b, c, d) for which $ax_1^2 + bx_2^2 + cx_3^2 + dx_4^2$ represents all positive integers. For instance, $(a, b, c, d) = (1, 2, 5, 6)$ works. Recently, Bhargava and Hanke proved a conjecture of Conway:

Theorem 101 (Bhargava, Hanke)**.** *A positive-definite integral quadratic form represents all positive integers, provided that it represents all the integers up to* 290*, and* 290 cannot *be replaced by a smaller number.*

19. November 25 – the final lecture

MInkowski proved that if $q(x_1, x_2, \dots, x_n)$ is a quadratic form with rational coefficients and q represents 0 with $x_1, x_2, \dots, x_n \in \mathbb{R}$ and q represents 0 with $x_1, x_2, \dots, x_n$ in $\mathbb{Q}_p$ for each prime p then q represents 0 with $x_1, x_2, \dots, x_n \in \mathbb{Q}$. Therefore, "local" solutions imply "global" solutions. Hasse extended this result to finite extensions of $\mathbb{Q}$.

In general, the idea that one can pass from local to global solutions is known as the *Hasse principle.* However, it does not always apply.

Theorem 102 (Selmer)**.** $3x^3 + 4y^3 + 5z^3 = 0$ *has a solution in $\mathbb{R}$ and in $\mathbb{Q}_p$ for each prime p but does* not *have a solution in $\mathbb{Q}$.*

Proof. $(x, y, z) = (0, 0, 0)$ is a solution, so a solution is indeed in $\mathbb{R}$. But the $\mathbb{Q}_p$ case is less trivial. For $p = 3$, take $(x, z) = (0, -1)$. Then it suffices to show that $4y^3 - 5 = 0$ has a solution in $\mathbb{Q}_3$. Put $f(y) = 4y^3 - 5$. Then $|f(2)|_3 = 3^{-3}$ and $|f'(2)|_3 = 3^{-1}$. Thus by Hensel's lemma there is a solution in $\mathbb{Q}_3$. For $p = 5$, take $x = 1$ and $z = 0$ and then we look for a solution too $g(y) = 4y^3 + 3$ in $\mathbb{Q}_5$. Then $|g(2)|_5 = 5^{-1}$ and $|g'(2)|_5 = 1$, so the result follows by Hensel. Suppose now that $p \neq 3, 5$. If 3 is a cubic residue in $(\mathbb{Z}/p\mathbb{Z})^\times$ then take $(x, y, z) = (\theta, 1, -1)$ where θ is a root of $3x^3 \equiv 1 \pmod{\mathbb{Q}_p}$, and apply Hensel's lemma. If 3 is not a cube in $(\mathbb{Z}/p\mathbb{Z})^\times$ ten there are three possibilities. Either 5 is a cube in $(\mathbb{Z}/p\mathbb{Z})^\times$ in which case there is a cube root of 5 in $\mathbb{Q}_p$ and we take $(x, y, z) = (\theta, -\theta, 1)$. If not, then we have $5 \equiv 3t^3 \pmod{p}$ or $5 \equiv 3^2 t^3 \pmod{p}$ for some integer t. In the first case we can use Hensel to lift to a valuation θ of $\left(\frac{5}{3}\right)^{1/3}$ in $\mathbb{Q}_p$ and then $(x, y, z) = (\theta, 0, -1)$ is a solution. In the second case, we use Hensel to show that there is an element $\theta_1 = \left(\frac{5}{9}\right)^{1/3}$ in $\mathbb{Q}_p$ and then $(\theta_1, 0, -1)$ is a solution. This shows that there are local solutions always.

To show that there are no solutions over $\mathbb{Q}$, Selmer showed that the given cubic form defines an elliptic curve of rank 0 over $\mathbb{Q}$ and there are no rational points. □

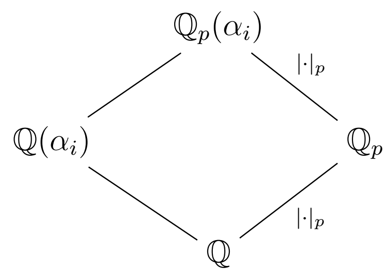
Let us return to our construction of Ω_p. Instead of completing $\mathbb{Q}$ to $\mathbb{Q}_p$ and then taking the algebraic closure extending $|\cdot|_p$ to $|\cdot|_p$ on $\overline{\mathbb{Q}_p}$ what if we first extend $|\cdot|_p$ to $\overline{Q}$ then complete? We consider a finite extension K of $\mathbb{Q}$? Let f be the monic irreducible polynomial defining K over $\mathbb{Q}$. Consider $f \in \mathbb{Q}_p[x]$ and let

$$f(x) = f_1(x)f_2(x)\cdots f_r(x),$$

where $f_1, f_2, \ldots, f_r$ are irreducibles in $\mathbb{Q}_p[x]$ of degree e_i for $i = 1, 2, \ldots, r$. Then the f_i's are distinct since f has no repeated roots in $\overline{\mathbb{Q}_p}$. To see this, note that f and f' are in $\mathbb{Q}[x]$ and $\mathbb{Q}$ is of characteristic zero and f is irreducible, so f is separable.

Let $\alpha_1, \ldots, \alpha_n$ be the roots of f in $\overline{\mathbb{Q}_p}$. Then there is an embedding σ_i of K in $\overline{\mathbb{Q}_p}$ for $i = 1, 2, \ldots, n$ given by $\sigma_i : K = \mathbb{Q}[x]/f \to \overline{\mathbb{Q}_p}$ where σ_i fixes $\mathbb{Q}$ and sends $x + (f) \mapsto \alpha_i$. Suppose that we have an embedding σ of K into $\overline{\mathbb{Q}_p}$ and $\sigma(K) = \mathbb{Q}(\alpha)$. If $\|\_\|$ is a valuation on K, which extends $|\cdot|_p$ on $\mathbb{Q}$, then under σ, $\|\_\|$ is a valuation on $\mathbb{Q}(\alpha)$ which extends $|\cdot|_p$ on $\mathbb{Q}$. Then we may complete $\mathbb{Q}(\alpha)$ with respect to $|\cdot|$ to a field K' and extend this valuation to K'. Notice that K' contains $\mathbb{Q}_p$ with the valuation $\|\_\|$ on $\mathbb{Q}_p$ the same as the valuation $|\cdot|_p$ on $\mathbb{Q}_p$. Also it contains α. But there is a unique way of extending $|\cdot|_p$ from $\mathbb{Q}_p$ to $\mathbb{Q}_p(\alpha)$ (actually, to $\overline{\mathbb{Q}_p}$) and $\mathbb{Q}_p(\alpha)$ is complete under $|\cdot|_p$. Therefore $K' = \mathbb{Q}_p(\alpha)$ and $\|\_\|$ is $|\cdot|_p$ on $\mathbb{Q}_p(\alpha)$.

But α is a root of $f(x)$ and the possible valuations are determined by the irreducible polynomials $f_1, f_2, \ldots, f_r \in \mathbb{Q}_p[x]$. Therefore there are at most r distinct valuations on K which extend $|\cdot|_p$ on $\mathbb{Q}$. To see that we get r distinct valuations, let α be a root of f_i in $\overline{\mathbb{Q}_p}$ for $i = 1, 2, \ldots, r$. Then we have



The above diagram determines a valuation on $\mathbb{Q}(\alpha_i)$ which extends $|\cdot|_p$ on $\mathbb{Q}$. But there are r distinct valuations on K given by the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ which divide (p) in $\mathcal{O}_K$. This gives them all the valuations. Therefore, we arrive at $\overline{\mathbb{Q}_p}$ or a field isomorphic to it, with valuation $|\cdot|_p$ whether we first complete and then take the algebraic closure or vice versa.

Department of Pure Mathematics, University of Waterloo, 200 University Avenue West, Waterloo, ON, Canada N2L 3G1

E-mail address: hsyang@uwaterloo.ca