Algebraic Number Theory

Script

Prof. Dr. Preda Mihăilescu

LaTeX-version by Niklas Sennewald

Mathematisches Institut
Georg-August-Universität Göttingen
Winter semester 2020/21

Contents

This script does not represent any replacement for the lectures given by professor Mihăilescu and will not be proof-read by him or anyone else in charge, these are basically my personal notes. Therefore I can not guarantee for its completeness and I will probably not write down any proofs given for theorems (because that's simply no fun in LaTeX.) glhf

III. Valuations and completions

1. Equivalent valuations and the theorem of Ostrowski

Definition 3.1.1 (Valuation)
For $a \in \mathbb{Z}_{\geq 0}$ we define the *valuation of a* $v_p(a)$ as the largest power of p dividing a, that is

$$a = p^m \cdot n,\ (n,p) = 1 \implies v_p(a) = m.$$

From that we conclude $a \in \mathbb{Z} \implies v_p(a) = v_p(|a|)$ and $a = \frac{a_1}{a_2} \in \mathbb{Q} \implies v_p(a) = v_p(a_1) - v_p(a_2)$. We also define $v_p(0) = \infty$.

Definition 3.1.2 (p-adic absolute value)
We define the *p-adic absolute value* to be$|a|_p = p^{-v_p(a)}$. From this, it follows that

1. $|a|_p = 0 \iff a = 0$,
2. $|ab|_p = |a|_p|b|_p$ and
3. $|a+b|_p \leq |a|_p + |b|_p$, making $|\cdot|_p$ a metric. Since it also also satisfies $|a+b|_p \leq \max\{|a|_p, |b|_p\}$, it is an ultrametric.

We can endow $\mathbb{Q}$ with the p-adic metric and build Cauchy sequences. Let $\mathcal{C}$ be the space of Cauchy sequences on $\mathbb{Q}$ with respect to $|\cdot|_p$ and let $\mathcal{N} = \{z = (z_n)_{n\in\mathbb{N}} \mid z \in \mathcal{C},\ \lim_{n\to\infty}(z_n) = 0\}$. Then $\mathcal{C}$ ist an integral ring and $\mathcal{N}$ is a maximal ideal therein. Therefore $\mathcal{C}/\mathcal{N}$ is a field called $\mathbb{Q}_p$.

Example 3.1.3: $z = (1, p, p^2, \dots, p^n, \dots) \in \mathcal{N},\ |p^n|_p = p^{-n} \to 0$. Note that a power series $f(z) = \sum_{n\in\mathbb{N}} a_n z^n,\ |a_n + a_{n+1}| \leq \max\{a_n, a_{n+1}\}$ verifies $|\sum_{n\in\mathbb{N}} a_n z^n|_p \leq |a_n z^n|$ if $a_n z^n$ are falling to 0.

Definition 3.1.4 (Limits in $\mathbb{Q}_p$)
For $x \in \mathbb{Q}_p$ with $|x_n| \to x$ we define the absolute value of x as $|x|_p = \lim |x_n|_p$.
$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid v_p(x) \geq 0\} = \mathcal{C}(\mathbb{Z})/\mathcal{N}(\mathbb{Z})$ (valuation ring of $\mathbb{Q}_p$)

From these definitions we can show two facts:

i) $(\mathbb{Z}_p/p^n\mathbb{Z}_p) \cong (\mathbb{Z}/p^n\mathbb{Z})$

ii) Let $S \subset \mathbb{Z}$ be representatives of $\mathbb{F}_p$. Then $\mathbb{Z}_p = \left\{ x = \sum\limits_{\substack{n=0 \\ x_n \in S}}^{\infty} x_n p^n \right\}$.

Definition 3.1.5 (Projective limits)
Let $\{R_i\}_{i\in\mathbb{N}}$ be a family of (integral) rings and suppose there are homomorphisms $\varphi_{m,n} : R_m \to R_n \ \forall m > n$, such that $\varphi_{n,k} \circ \varphi_{m,n} = \varphi_{m,k} \ \forall m > n > k$. There exists a ring R unique up to isomorphism together with maps $\varphi_n : R \to R_n$ with $\varphi_n = \varphi_{m,n} \circ \varphi_m$ and a universal property

$$\begin{tikzcd}
& & & & & A \arrow[rrr, "\rho"] \arrow[d, dashed, "\psi_n"] & & & R \arrow[dllllllll] \arrow[dlll, "\varphi_n"] \arrow[dl, "\varphi_m"] \arrow[d] \\
R_0 & R_1 \arrow[l] & \cdots \arrow[l] & R_k \arrow[l] & \cdots \arrow[l] & R_n \arrow[l] \arrow[ll, bend left, "\varphi_{n,k}"] & \cdots \arrow[l] & R_m \arrow[l] \arrow[ll, bend left, "\varphi_{m,n}"] \arrow[llll, bend left=50, "\varphi_{m,k}"] & \cdots \arrow[l]
\end{tikzcd}$$

If A is a ring with maps $\psi_n : A \to R_n$ and commuting diagrams, then there is a map $\rho : A \to R$, such that $\psi_n = \varphi_n \circ \rho$.

R is the projective limit of the R_n. The maps $\varphi_{m,n}$ are not required to be surjective in general (though they are in the case of p-adic numbers). In the case of p-adic numbers, we use $R_n = \mathbb{Z}/p^n\mathbb{Z}$ and $\varphi_{m,n} : R_m \to R_n$ as the reduction modulo p^n. This defines $\mathbb{Z}_p = \lim\limits_{\infty \leftarrow n} (\mathbb{Z}/p^n\mathbb{Z})$. The elements $z \in \mathbb{Z}_p$ are identified by the sequences $(z_n)_{n\in\mathbb{N}}$, where $z_n = \varphi_n(z)$.

Remark 3.1.6: For $z \in \mathbb{Z}_p$ as a projective limit, we have $z = \lim\limits_{n\to\infty} \varphi(z)$ in terms of the p-adic metric.

Example 3.1.7: $R_n = \mathbb{Z}/n\mathbb{Z}$. We have a lattice of homomorphisms $\varphi_{m,n} : R_m \to R_n$, which are surjective iff $n \mid m$. This gives us the projective limit $\hat{\mathbb{Z}} = \lim\limits_{\infty \leftarrow n} R_n$, which happens zo be $\hat{\mathbb{Z}} = Gal(\overline{F_p}/F_p) = Gal(\mathbb{Q}^{(ab)}/\mathbb{Q})$.

Lemma 3.1.8
If $(c_n)_{n\in\mathbb{N}} \subset \mathbb{Z}_p$ converges to 0, then $\sum_{n\in\mathbb{N}} c_n$ exists.

Theorem 3.1.9
Let $f \in \mathbb{Z}[x]$ be irreducible and $\bar{f} \in \mathbb{F}_p[x]$ be its image under reduction, and assume this image to be square-free. Then there is a $\varphi \mid n = \deg(f)$ and φ polynomials $g_i(x) = \mathbb{F}_p[x]$ of degree $\frac{n}{\varphi}$, such that

i) $\bar{f}(x) = \prod_{i=1}^{\varphi} g_i(x)$,

ii) $\mathbb{F}_p[x]/g_i(x)$ *are isomorphic.*

Hensel: $f(x) = \prod_{i=1}^{\frac{n}{\varphi}} g_i^H(x)$ with $g_i^H(x) \in \mathbb{Z}_p[x]$ and $g_i^H(x) \equiv g_i(x) \mod p\mathbb{Z}_p[x]$. Then we can define $K_i = \mathbb{Q}_p[x]/g_i^H(x)$. These are finite algebraic extensions over $\mathbb{Q}_p$.

Definitions