Alg. Zth.

17.1.2024

Wiederholung

$v_p(K^\times) = \frac{1}{e}\mathbb{Z}$

$$\begin{array}{ccccccc} K & \supseteq & \mathcal{O} = \mathcal{O}_K & \supseteq & \mathfrak{p} = (\pi) \\ | & & | & & \\ \mathbb{Q}_p & \supseteq & \mathbb{Z}_p & \supseteq & p\mathbb{Z}_p \end{array} \qquad v_p$$

$e v_p = v_K = v_\mathfrak{p}$

wobei $p\mathcal{O}_K = \mathfrak{p}^e$

Es gilt: $ef = [K : \mathbb{Q}_p]$

$f = [\mathcal{O}/\mathfrak{p} : \mathbb{F}_p]$

$$\mathcal{U}_K^{(1)} = \mathcal{U}^{(1)} = 1 + \mathfrak{p}$$
$$= \{ \alpha \in \mathcal{O} \mid \alpha \equiv 1 \pmod{\mathfrak{p}} \} \leq \mathcal{O}^\times.$$

Dies ist ein $\mathbb{Z}_p$-Modul vermöge:

$$u \in \mathcal{U}_K^{(1)}, \quad \alpha = \sum_{\nu=0}^{\infty} a_\nu p^\nu, \quad 0 \leq a_\nu < p$$

$$s_n := \sum_{\nu=0}^{n-1} a_\nu p^\nu$$

$$u^\alpha := \lim_{n\to\infty} (u^{s_n}) \in \mathcal{U}_K^{(1)} \qquad \text{(Übung)}$$

<u>ZIEL:</u> $K^\times \simeq \mathbb{Z} \times \mu_{q-1} \times \mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}_p^{[K:\mathbb{Q}_p]}$

wobei $q = |\mathcal{O}/\mathfrak{p}| = p^f$, $a \geq 0$ geeignet

Bislang: $K^\times = \pi^\mathbb{Z} \times \mu_{q-1} \times \mathcal{U}_K^{(1)}$

Bislang gezeigt:

$$\log(1+x) = -\sum_{\nu=1}^{\infty} (-1)^\nu \frac{x^\nu}{\nu}$$

konvergiert für $|x|_p < 1$, d.h. $x \in \mathfrak{p}$.

Es gilt:

$$\log((1+x)(1+y)) = \log(1+x) + \log(1+y),$$
$$\forall x, y \in \mathfrak{p}$$

Also ist

$$\log : U_K^{(1)} \longrightarrow K$$

ein Homom.

Wir werden zeigen: $\log(\underbrace{U_K^{(n)}}_{1+\mathfrak{p}^n}) \subseteq \mathfrak{p}^n$

<u>Übung</u>: log ist stetig auf $U_K^{(1)}$

<u>Ziel</u>: Setze log auf $K^\times$ fort.

Schreibe dazu

$$K^\times \ni \alpha = \pi^{v_K(\alpha)} \omega(\alpha) \langle \alpha \rangle$$

mit $\omega(\alpha) \in \mu_{q-1}$, $\langle \alpha \rangle \in U_K^{(1)}$

$$\Longrightarrow \log(\alpha) = v_K(\alpha) \log(\pi) + \log(\omega(\alpha)) + \log(\langle \alpha \rangle)$$

$$\log\left(\omega(\alpha)^{q-1}\right) = \log(1) = 0 \Longrightarrow \log(\omega(\alpha)) = 0$$

Also ist noch $\log(\pi)$ zu bestimmen.
Betrachte dazu:

$$p = \pi^e \omega(p) \langle p \rangle$$

$$\Rightarrow \quad 0 = \log(p) = e \log(\pi) + \log(\langle p \rangle)$$

$$\Rightarrow \quad \log(\pi) = -\frac{1}{e} \log(\langle p \rangle).$$

Noch zu zeigen: Unabhängigkeit von π.
Sei $\pi' \in \mathcal{O}$ ein weiteres Primelement. Schreibe

$$\alpha = (\pi')^{v_K(\alpha)} \omega'(\alpha) \langle \alpha \rangle'$$

Z.z. $v_K(\alpha) \log(\pi) + \log(\langle \alpha \rangle) = v_K(\alpha) \log(\pi') + \log(\langle \alpha \rangle')$

wobei $\log(\pi') = -\frac{1}{e} \log(\langle p \rangle')$

$\log(\pi) = -\frac{1}{e} \log(\langle p \rangle)$.

$$\alpha = \pi^{v_K(\alpha)} \omega(\alpha) \langle \alpha \rangle, \quad \pi' = \pi\, \omega(\pi') \langle \pi' \rangle$$

$$\Rightarrow \alpha = (\pi')^{v_K(\alpha)} \underbrace{\left(\omega(\pi')^{-v_K(\alpha)} \omega(\alpha) \right)}_{\omega'(\alpha)} \underbrace{\langle \pi' \rangle^{-v_K(\alpha)} \langle \alpha \rangle}_{\langle \alpha \rangle'}$$

Rest: Einsetzen und Nachrechnen. $\blacksquare$

Satz: Sei $K|\mathbb{Q}_p$ ein p-adischer Zahlkörper. Sei $p\mathcal{O} = \mathfrak{p}^e$. Dann liefern die Potenzreihen

$$\exp(x) = \sum_{\nu=0}^{\infty} \frac{x^\nu}{\nu!} \quad \text{und} \quad \log(1+z) = -\sum_{\nu=1}^{\infty} (-1)^\nu \frac{z^\nu}{\nu}$$

für $n > \frac{e}{p-1}$ zueinander inverse Isomorphismen

$$\mathfrak{p}^n \underset{\log}{\overset{\exp}{\rightleftarrows}} U_K^{(n)}$$

Lemma: Sei $\nu \in \mathbb{N}$ und $\nu = \sum_{i=0}^{r} a_i p^i$ mit $0 \leq a_i < p$. Dann ist

$$v_p(\nu!) = \frac{1}{p-1} \sum_{i=0}^{r} a_i (p^i - 1).$$

ohne Beweis (siehe Neukirch).

Beachte: $v_K = e v_p \Rightarrow$

$$\left(v_p(\alpha) > \frac{1}{p-1} \iff v_K(\alpha) > \frac{e}{p-1} \right)$$

Beweis des Satzes:

Zeige zuerst: $\log(U_K^{(n)}) \subseteq \mathfrak{p}^n$.

Dazu zeigt man: $v_p\left(\frac{z^\nu}{\nu}\right) - v_p(z) > 0$ für $\nu \geq 2$.

Dann folgt: $v_p\left(\log(1+z)\right) = v_p(z)$

$$\Rightarrow \quad v_K\left(\log(1+z)\right) = v_K(z) \geq n \quad \text{für } z \in \mathfrak{p}^n.$$

<u>Dazu:</u> $v_p\left(\frac{z^\nu}{\nu}\right) - v_p(z) = \nu\, v_p(z) - v_p(\nu) - v_p(z)$

$$= (\nu-1)\underbrace{v_p(z)}_{> \frac{1}{p-1}} - v_p(\nu) > \frac{\nu-1}{p-1} - v_p(\nu)$$

$$= (\nu-1)\underbrace{\left(\frac{1}{p-1} - \frac{v_p(\nu)}{\nu-1}\right)}_{\geq 0,\ \underline{\text{denn:}}}$$

$$\frac{v_p(\nu)}{\nu-1} = \frac{a}{p^a\nu_0 - 1} \leq \frac{a}{p^a-1} = \frac{1}{p-1}\cdot\underbrace{\frac{a}{p^{a-1}+\ldots+1}}_{\leq 1}$$

$\nu = p^a\nu_0\,,\ (\nu_0, p) = 1$

$$\leq \frac{1}{p-1}.$$

<u>Konvergenz von exp:</u>

$$v_p(\nu!) = \frac{1}{p-1}\sum_{i=0}^{r} a_i\,(p^i - 1)$$

$$= \frac{1}{p-1}\left(\nu - \underbrace{(a_0 + a_1 + \ldots + a_r)}_{=:\, S_\nu}\right)$$

$$\Longrightarrow \quad v_p\left(\frac{x^\nu}{\nu!}\right) = \nu\, v_p(x) - \frac{\nu - s_\nu}{p-1}$$

$$= \nu\left(v_p(x) - \frac{1}{p-1}\right) + \underbrace{\frac{s_\nu}{p-1}}_{\geq 0}$$

Falls also $v_p(x) > \frac{1}{p-1}$, so folgt

$$v_p\left(\frac{x^\nu}{\nu!}\right) \xrightarrow{\nu \to \infty} \infty, \quad \text{und}$$

exp konvergiert.

<u>Noch zu zeigen:</u> $\exp(\mathfrak{p}^n) \subseteq U^{(n)}$

<u>Dazu:</u>

$$v_p\left(\frac{x^\nu}{\nu!}\right) - v_p(x) = (\nu - 1)\, v_p(x) - \frac{\nu - s_\nu}{p-1}$$

$$= \underbrace{(\nu - 1)\, v_p(x) - \frac{\nu - 1}{p-1}}_{>0,\ \text{falls } \nu > 1} + \frac{s_\nu - 1}{p-1} > \frac{s_\nu - 1}{p-1} \geq 0$$

Also gilt: $v_K(\exp(x) - 1) = v_K(x)$.

Beachte die formalen Identitäten

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

$\blacksquare$

SATZ: $$K^\times \simeq \mathbb{Z} \oplus \mathbb{Z}/_{q-1} \oplus \mathbb{Z}/_{p^a\mathbb{Z}} \oplus \mathbb{Z}_p^d$$

wobei $a \in \mathbb{Z}_{\geq 0}$, $d := [K:\mathbb{Q}_p]$.

Beweis: Bekannt

$$K^\times = \pi^{\mathbb{Z}} \times \mu_{q-1} \times \mathcal{U}_K^{(1)}.$$

Sei n groß genug $\Longrightarrow$

$$\log : \mathcal{U}_K^{(n)} \xrightarrow{\simeq} \mathfrak{p}^n = \pi^n \mathcal{O} \simeq \mathcal{O}$$

Dies ist ein Isomorphismus von $\mathbb{Z}_p$-Moduln, denn:

$$\log\left(\left(1+z\right)^\alpha\right) = \alpha \log(1+z).$$

für $\alpha \in \mathbb{Z}_p$.

Da $\mathbb{Z}_p$ ein HIR ist, besitzt $\mathfrak{p}^n$ eine $\mathbb{Z}_p$-Basis, d.h.

$$\mathfrak{p}^n = \mathbb{Z}_p \alpha_1 \oplus \dots \oplus \mathbb{Z}_p \alpha_d, \quad \alpha_i \in \mathfrak{p}^n$$
$$\simeq \mathbb{Z}_p^d$$

Es gilt: $$\left| \mathcal{U}_K^{(1)} / \mathcal{U}_K^{(n)} \right| \overset{!}{=} \left| \mathfrak{p} / \mathfrak{p}^n \right| < \infty$$

und eine p-Potenz.

Dann folgt: $\mathcal{U}_K^{(1)} \simeq \mathcal{U}_{K,\mathrm{tors}}^{(1)} \oplus \mathbb{Z}_p^d$

Noch zu zeigen: $\mathcal{U}_{K,\mathrm{tors}}^{(1)}$ = Gruppe der p-Potenz-einheitswurzeln in K.

<u>Beachte:</u> Die Gruppe der p-Potenzeinheitswurzeln in K ist von der Form μ_{p^a} für ein eindeutig bestimmtes $a \in \mathbb{N}_0$.

Sei $\varepsilon \in \mathcal{U}_K^{(1)}$ und $\varepsilon^\alpha = 1$ für $\alpha \in \mathbb{Z}_p$

Schreibe $\alpha = p^m u$ mit $m = v_p(\alpha)$, $u \in \mathbb{Z}_p^\times$

$$\Rightarrow \varepsilon^\alpha = (\varepsilon^u)^{p^m} = 1 \Rightarrow \varepsilon^u \in \mu_{p^a}$$

$$\Rightarrow \varepsilon = (\varepsilon^u)^{u^{-1}} \in \mu_{p^a}$$

<u>Zum !:</u> Betrachte die Filtrierungen

$$\mathfrak{y}^n \subseteq \mathfrak{y}^{n-1} \subseteq \dots \subseteq \mathfrak{y}^2 \subseteq \mathfrak{y}$$

$$1+\mathfrak{y}^n \subseteq 1+\mathfrak{y}^{n-1} \dots \subseteq 1+\mathfrak{y}^2 \subseteq 1+\mathfrak{y}$$

Es gilt: $$\mathfrak{y}^i / \mathfrak{y}^{i+1} \underset{\text{Isom. von abelschen Gruppen}}{\simeq} 1+\mathfrak{y}^i / 1+\mathfrak{y}^{i+1}$$

$$x + \mathfrak{y}^{i+1} \longmapsto (1+x) \bmod (1+\mathfrak{y}^{i+1})$$

<u>Denn:</u> $(1+x+y) \equiv (1+x)(1+y) \pmod{\mathfrak{y}^{i+1}}$

Dazu: $(1+x)(1+y) = 1 + x + y + \underbrace{xy}_{\in \mathfrak{g}^{2i} \subseteq \mathfrak{g}^{i+1}}.$

Beachte noch:

$$0 \to \mathfrak{g}^{n-1}/\mathfrak{g}^{n} \longrightarrow \mathfrak{g}/\mathfrak{g}^{n} \longrightarrow \mathfrak{g}/\mathfrak{g}^{n-1} \to 0 \quad \text{exakt.}$$

$$\mathfrak{g}^{n-1}/\mathfrak{g}^{n} \cong U_K^{(n-1)}/U_K^{(n)}$$

Rest: Induktion.

∎