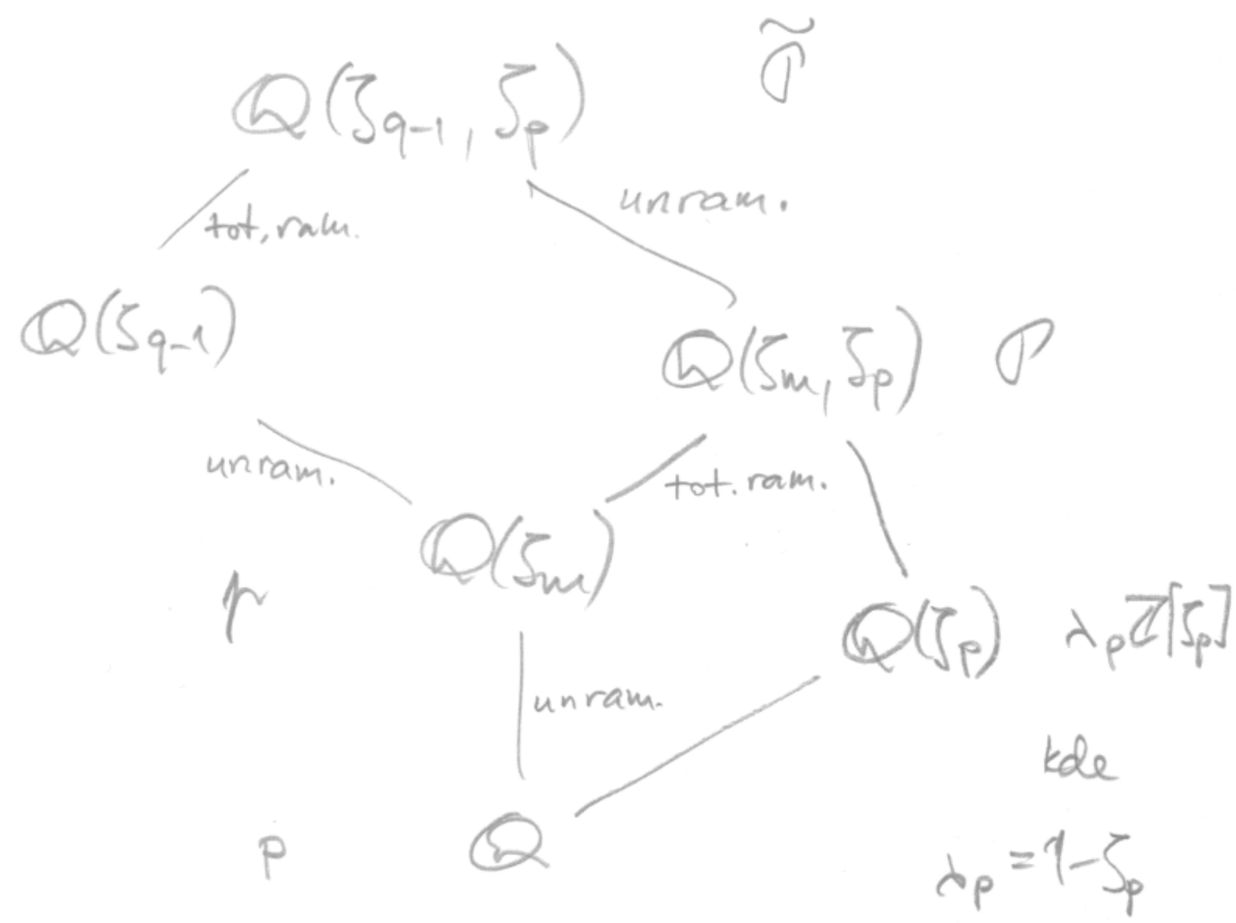
Zvolíme $m \in \mathbb{N}$ a prvočíslo $p \nmid m$.

Nechť p je libovolný pevně zvolený prvoideál $\mathbb{Z}[\zeta_m]$ obsahující p.

Pak $\mathbb{Z}[\zeta_m]/p$ je těleso mající $q = p^f$ prvků, kde f je řád $[p]_m$ v grupě $\mathbb{Z}_m^\times$, neboť je to řád Frobenia σ_p v $Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$.

Nechť $\tilde{p}$ je prvoideál $\mathbb{Z}[\zeta_{q-1}]$ nad p.

V $\mathbb{Z}[\zeta_{mp}]$ (resp. $\mathbb{Z}[\zeta_{(q-1)p}]$) existuje jediný prvoideál $\mathcal{P}$ (resp. $\tilde{\mathcal{P}}$), který je nad p (resp. $\tilde{p}$).



Platí

$$|\mathbb{Z}[\zeta_{q-1}]/\tilde{p}| = q = |\mathbb{Z}[\zeta_m]/p),$$

neboť řád $[p]_{q-1}$ v $\mathbb{Z}_{q-1}^\times$ je také f. Podobně

$$\left|\mathbb{Z}[\zeta_{p(q-1)}]/\tilde{\mathcal{P}}\right| = q = |\mathbb{Z}[\zeta_{mp}]/\mathcal{P}|.$$

Označme

$$\mathbb{F}_q := \mathbb{Z}[\zeta_{p(q-1)}]/\tilde{\mathcal{P}}$$

Ukažme, že různé $(q-1)$-té odmocniny z jedné leží v různých třídách tohoto faktorokruhu. Nechť tedy $0 \le i < j < q-1$ platí $\zeta_{q-1}^i - \zeta_{q-1}^j \in \tilde{\mathcal{P}}$, tj. $v_{\tilde{\mathcal{P}}}(\zeta_{q-1}^i - \zeta_{q-1}^j) = 0$. Zřejmě

$$\zeta_{q-1}^i - \zeta_{q-1}^j = \zeta_{q-1}^i\left(1 - \zeta_{q-1}^{j-i}\right),$$

přičemž

$$\prod_{a=1}^{q-1}(X - \zeta_{q-1}^a) = \frac{X^{q-1}-1}{X-1} = X^{q-2} + X^{q-3} + \ldots + X + 1,$$

a tedy

$$\prod_{a=1}^{q-1}(1 - \zeta_{q-1}^a) = q-1.$$

Protože $1 - \zeta_{q-1}^a$ je celé algebraické, tak $v_{\tilde{\mathcal{P}}}(1-\zeta_{q-1}^a) \ge 0$. Protože $v_{\tilde{\mathcal{P}}}(q-1) = 0$, neboť $\tilde{\mathcal{P}} \cap \mathbb{Z} = p\mathbb{Z}$, dostaneme dokazované.