Zvolíme $m > 1$, k tomu libovolné prvočíslo $p \nmid m$.
Nechť f je nejmenší přirozené číslo splňující $p^f \equiv 1 \pmod m$,
tj f je řád $[p]_m$ v $\mathbb{Z}_m^\times$. Položme $q = p^f = |\mathbb{Z}[\zeta_m]/\mathfrak{p}|$, kde
$\mathfrak{p}$ je libovolný prvoideál $\mathbb{Z}[\zeta_m]$ dělící p. Nechť $\tilde{\mathfrak{p}}$ je libovolný
prvoideál $\mathbb{Z}[\zeta_{q-1}]$ nad $\mathfrak{p}$

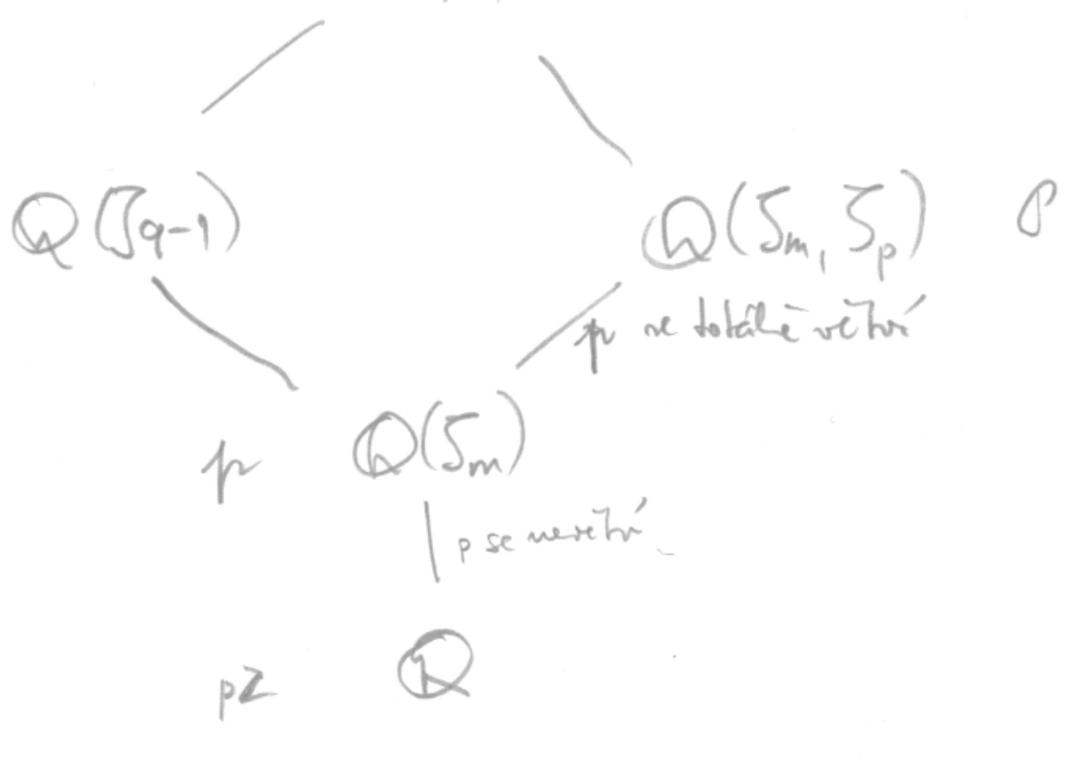
Platí

$$q = |\mathbb{Z}[\zeta_{q-1}]/\tilde{\mathfrak{p}}| = |\mathbb{Z}[\zeta_{(q-1)p}]/\tilde{\mathfrak{P}}|$$

neboť ideál $p\mathbb{Z}$ má v každém rozšíření

$\mathbb{Q}(\zeta_m)/\mathbb{Q}$, $\mathbb{Q}(\zeta_{q-1})/\mathbb{Q}$, $\mathbb{Q}(\zeta_{(q-1)p})/\mathbb{Q}$

stejný stupeň inercie.



Definujme $\mathbb{F}_q := \mathbb{Z}[\zeta_{(q-1)p}]/\tilde{\mathfrak{P}}$,
na tomto tělese zavedeme multiplikativní charakter ω řádu $q-1$ takto:

$$\omega : \mathbb{F}_q^\times \to \mu_{q-1} = \langle \zeta_{q-1} \rangle$$

předpisem: pro každé $a \in \mathbb{Z}[\zeta_{(q-1)p}]/\tilde{\mathfrak{P}}$ je $\omega(a)$ ta $(q-1)$-tá odmocnina
z jedné, která leží ve třídě a, tj $a = \omega(a) + \tilde{\mathfrak{P}}$. Abychom věděli, že
tato definice je korektní, stačí uhádnout, že v každé nenulové třídě
leží právě jedna taková odmocnina, což vzhledem k tomu, že $|\mathbb{F}_q^\times| = |\langle \zeta_{q-1} \rangle|$,
bude plynout z toho, že dvě různé $(q-1)$-té odmocniny z jedné nemohou
ležet ve stejné třídě modulo $\tilde{\mathfrak{P}}$. Ale to ať přímo.