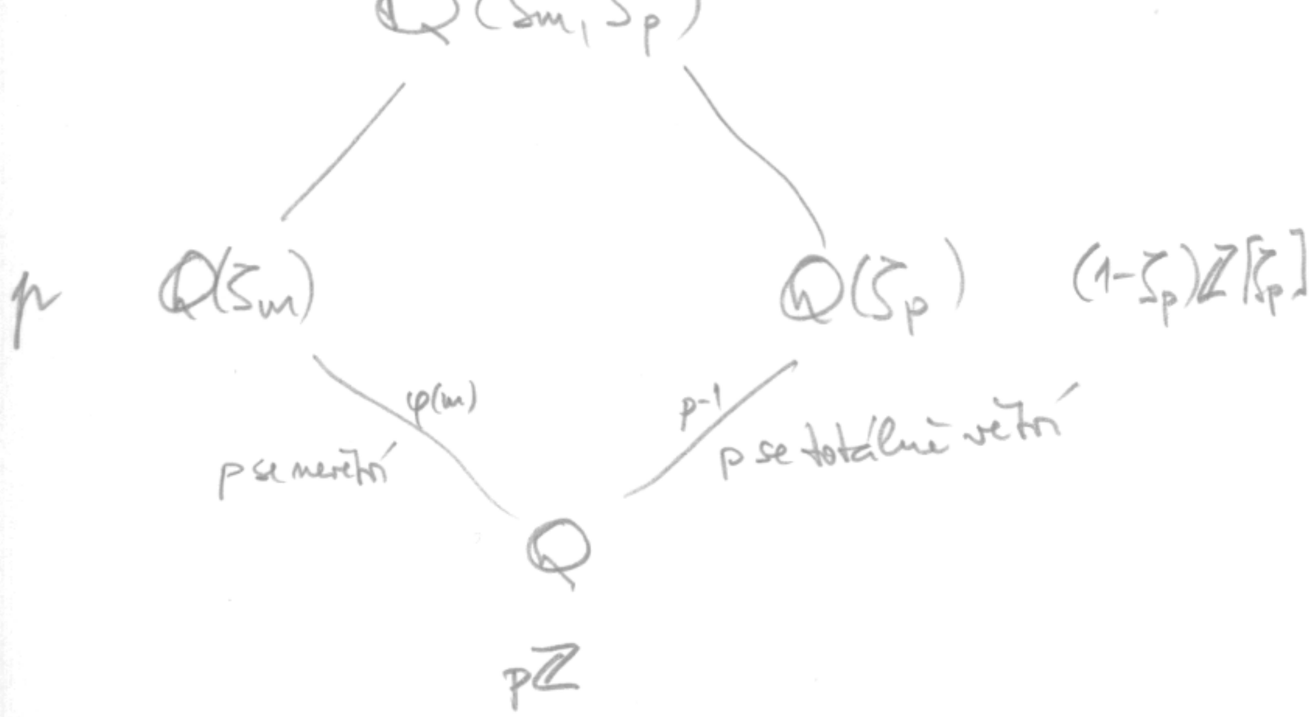
③ Faktorizace ideálu generovaného Gaussovou sumou

Mějme $\underbrace{m \mid q-1}_{m>1,\ \text{surjektivní charakter}}$, $\chi : \mathbb{F}_q^\times \longrightarrow \mu_m = \langle \zeta_m \rangle$ a Gaussovu sumu $g(\chi) \in \mathbb{Q}(\zeta_m, \zeta_p) = \mathbb{Q}(\zeta_{mp})$

$q = p^f$, přitom $m \mid q-1$



p se v $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ nevětví $\Longrightarrow$ $(1-\zeta_p)$ se nevětví v $\mathbb{Q}(\zeta_{mp})/\mathbb{Q}(\zeta_p)$.

$p\mathbb{Z}[\zeta_m] = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_k$, kde $\mathfrak{p}_1 = \mathfrak{p}$

$p\mathbb{Z}[\zeta_{mp}] = \mathfrak{P}_1^{p-1} \cdot \mathfrak{P}_2^{p-1} \cdots \mathfrak{P}_k^{p-1}$, kde $\mathfrak{P}_1 = \mathfrak{P}$

$\mathfrak{p}_i \mathbb{Z}[\zeta_{mp}] = \mathfrak{P}_i^{p-1}$ pro každé $i = 1, \ldots, k$.

Pro libovolné $\sigma \in Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ existuje $\hat{\sigma} \in Gal(\mathbb{Q}(\zeta_{mp})/\mathbb{Q})$ takové, že $res_{\mathbb{Q}(\zeta_{mp})/\mathbb{Q}(\zeta_m)} \hat{\sigma} = \sigma$.

Pro každé $\sigma \in Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ je $\mathfrak{p}_i^\sigma = \mathfrak{p}_j$ pro nějaké $j \in \{1, \ldots, k\}$.

Naopak pro každé $j \in \{1, \ldots, k\}$ existuje $\sigma \in Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ takové, že $\mathfrak{p}_j = \mathfrak{p}_1^\sigma$ (zde jsme využili toho, že pro Galoisova rozšíření konečných rozšíření $\mathbb{Q}$ platí, že každá valuace na větším tělese modulující danou valuaci na dolním tělese se získá z jedné zvolené aplikací Galoisovy grupy – to jsme dokazovali v seminární lomi)

$\mathfrak{p}_j \mathbb{Z}[\zeta_{mp}] = \mathfrak{p}_1^{\hat{\sigma}} \mathbb{Z}[\zeta_{mp}] = (\mathfrak{P}_1^{p-1})^{\hat{\sigma}} = (\mathfrak{P}_1^{\hat{\sigma}})^{p-1} \Longrightarrow \mathfrak{P}_j^{p-1} = (\mathfrak{P}_1^{\hat{\sigma}})^{p-1} \Longrightarrow \mathfrak{P}_j = \mathfrak{P}_1^{\hat{\sigma}}$

$\nu_{\mathfrak{P}_j}(g(\chi)) = \nu_{\mathfrak{P}_1^{\hat{\sigma}}}(g(\chi)) = \nu_{\mathfrak{P}_1}(g(\chi)^{\hat{\sigma}^{-1}})$