Homework 1

Songyu Ye

September 29, 2025

Problem 1 Let ζ_n denote a primitive n-th root of unity (so that powers of ζ_n give all n-th roots of unity). Consider

$$L = \mathbb{Q}(\zeta_n) \quad \text{over} \quad K = \mathbb{Q}.$$

This is a Galois extension and there is an isomorphism ("canonical")

$$i : \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times$$

characterized by the equation that $\sigma(\zeta_n) = \zeta_n^{i(\sigma)}$ for all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

Now let p be a prime number coprime to n. You may accept that p is unramified in $\mathbb{Q}(\zeta_n)/\mathbb{Q}$.

(i) Prove that the Frobenius element

$$(p, \mathbb{Q}(\zeta_n)/\mathbb{Q})$$

maps to $p \in (\mathbb{Z}/n\mathbb{Z})^\times$ under the map i.

(ii) Using (i) show that p splits completely in $\mathbb{Q}(\zeta_n)$ if and only if $p \equiv 1 \pmod{n}$.

* Bonus: Can you describe the condition for p to be inert in $\mathbb{Q}(\zeta_n)$?

Problem 2 Assume that $n = q$ is a prime such that $q \equiv 1 \pmod 4$. Recall there is a canonical isomorphism

$$i : \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/q\mathbb{Z})^\times$$

sending the Frobenius element $(p, \mathbb{Q}(\zeta_q)/\mathbb{Q})$ to $p \in (\mathbb{Z}/q\mathbb{Z})^\times$ for every $p \neq q$. Take on faith that $\mathbb{Q}(\sqrt{q}) \subset \mathbb{Q}(\zeta_q)$. Now fix an **odd** prime $p \neq q$.

(i) Verify that p is a square modulo q if and only if $(p, \mathbb{Q}(\zeta_q)/\mathbb{Q})$ fixes the subfield $\mathbb{Q}(\sqrt{q})$ elementwise.

(ii) Check that $(p, \mathbb{Q}(\zeta_q)/\mathbb{Q})$ fixes the subfield $\mathbb{Q}(\sqrt{q})$ elementwise if and only if p splits completely in $\mathbb{Q}(\sqrt{q})$.

(iii) Deduce from (i), (ii), and Problem Set 03 #3 that p is a square modulo q if and only if q is a square modulo p, namely

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1.$$

Note: Please refrain from using quadratic reciprocity since the point is to give a Galois-theoretic proof of quadratic reciprocity.

* Bonus: When $q \equiv 3 \pmod 4$, a similar argument with $\mathbb{Q}(\sqrt{-q})$ in place of $\mathbb{Q}(\sqrt{q})$ shows that

$$\left(\frac{p}{q}\right)\left(\frac{-q}{p}\right) = 1.$$

Problem 3 Do Lang's Algebra, Exercises VI.46, VI.47, and VI.48, pp. 330–331. Submit your solutions only for VI.47 and VI.48.

(Please do VI.46 but it's a private exercise. Note: These exercises will prepare us for the Witt vectors section [S] VI.6.)