Review exercise sheet

1. Show that $X^4 + 1 \in \mathbb{Q}[X]$ is irreducible. Show that $X^4 + 1$ is reducible in $\mathbb{F}_p[X]$ for every prime p.

2. For the polynomial $X^4 + 2X^3 + X^2 + 2X + 1 \in \mathbb{Q}[X]$ determine the Galois group of its splitting field over $\mathbb{Q}$.

3. Let $p > 2$ be a prime number and $\zeta := e^{\frac{2\pi i}{p}}$. Let $E = \mathbb{Q}(\zeta)$. Recall that $\mathrm{Gal}(E : \mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$.

(a) Show that there exists a unique subgroup H of $\mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q})$ of order 2. What is its generator? [*Hint:* It is an element of order 2]

(b) Prove that $\mathbb{Q}(\zeta + \zeta^{-1}) \subseteq E^H$ and that $[E : \mathbb{Q}(\zeta + \zeta^{-1})] \leqslant 2$.

(c) Deduce that $E^H = \mathbb{Q}(\zeta + \zeta^{-1})$.

4. Let $E : k$ be a finite Galois extension with Galois group $G = \mathrm{Gal}(E : k)$ of degree $n = [E : k]$. Define the *trace* $T : E \longrightarrow E$ by

$$T(x) = \sum_{\sigma \in G} \sigma(x).$$

(a) Prove that $\mathrm{im}(T) \subseteq k$ and that T is k-linear.

(b) Show that T is not identically zero and deduce that $\dim(\ker(T)) = n - 1$.

(c) Now suppose that $\mathrm{Gal}(E : k)$ is cyclic and generated by an automorphism σ. Consider the linear map $\tau = \sigma - \mathrm{id}_E$. Prove that

$$\ker(T) = \mathrm{im}(\tau) = \{\sigma(u) - u : u \in E\}.$$

5. Let p be an odd prime number. Let $\zeta = e^{\frac{2\pi i}{p}} \in \mathbb{C}$ and $E = \mathbb{Q}(\zeta)$. Recall that $\mathrm{Gal}(E : \mathbb{Q}) \cong \mathbb{F}_p^\times$. For $a \in \mathbb{F}_p^\times$, define the *Legendre symbol*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a square in } \mathbb{F}_p^\times \\ -1 & \text{if } a \text{ is a not square in } \mathbb{F}_p^\times. \end{cases}$$

Define the complex number

$$\tau = \sum_{a \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right) \zeta^a.$$

(a) Show that the map $\mathbb{F}_p^\times \to \{\pm 1\}$ sending $a \mapsto \left(\frac{a}{p}\right)$ is a group homomorphism.

(b) Prove that

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p,$$

and that this determines $\left(\frac{a}{p}\right) \in \{\pm 1\}$ uniquely.

(c) Show that $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \pmod 4$.

(d) For $b \in \mathbb{F}_p^\times$, let $\sigma_b \in \mathrm{Gal}(E : \mathbb{Q})$ be the automorphism $\sigma_b(\zeta) = \zeta^b$. Prove the equality $\sigma_b(\tau) = \left(\frac{b}{p}\right) \cdot \tau$.

(e) Prove that $\mathbb{Q}(\tau) : \mathbb{Q}$ is the unique quadratic intermediate extension of $E : \mathbb{Q}$.

We now want to determine the extension $\mathbb{Q}(\tau)$ by computing τ^2 explicitly.

(f) Let $c \in \mathbb{F}_p^\times$. Show that

$$\sum_{a \in \mathbb{F}_p^\times} \zeta^{a(1+c)} = \begin{cases} -1 & \text{if } c \neq p-1 \\ p-1 & \text{if } c = p-1 \end{cases}$$

(g) Write

$$\tau^2 = \sum_{a \in \mathbb{F}_p^\times} \sum_{b \in \mathbb{F}_p^\times} \left(\frac{ab}{p}\right) \zeta^{a+b}.$$

Substituting $b = ac$ with $c \in \mathbb{F}_p^\times$, deduce that

$$\tau^2 = -\sum_{c=1}^{p-2} \left(\frac{c}{p}\right) + \left(\frac{-1}{p}\right)(p-1).$$

(h) Conclude: if $p \equiv 1 \pmod 4$, then $\mathbb{Q}(\tau) = \mathbb{Q}(\sqrt{p})$; if $p \equiv 3 \pmod 4$, then $\mathbb{Q}(\tau) = \mathbb{Q}(i\sqrt{p})$.

6. Let $L : K$ be a finite Galois extension with Galois group G. Let G' denote the commutator subgroup $[G, G]$ generated by all commutators $xyx^{-1}y^{-1}$ in G. Show that $L^{G'} : K$ is a Galois extension with $\mathrm{Gal}(L^{G'} : K)$ abelian. Show that any Galois extension $E : K$ with $E \subset L$ and $\mathrm{Gal}(E : K)$ abelian is contained in $L^{G'}$.

7. For all ideals $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ and all elements x, y of a ring R show the formulas

(a) $(x)(y) = (xy)$

(b) $\mathfrak{a}(\mathfrak{b}\mathfrak{c}) = (\mathfrak{a}\mathfrak{b})\mathfrak{c}$

(c) $(x) \cdot ((y) \cdot \mathfrak{a}) = (xy) \cdot \mathfrak{a}$

8. Decide which of the following ideals of $\mathbb{Q}[X, Y, Z]$ are equal:

$$\begin{aligned} I_1 &:= (X, Y) & I_5 &:= (XZ, X - Y, X + Y) \\ I_2 &:= (X, Y, Z) & I_6 &:= (X^2 + Y^2, Z - Y^2, Z - X^2) \\ I_3 &:= (X^2, Y^2, Z) & I_7 &:= (XZ, Y^2 - 5X^2, X^2 - XZ) \\ I_4 &:= (XZ, X^2, Y^2) \end{aligned}$$

9. For $\omega = e^{\frac{2\pi i}{3}}$ consider the ring $R := \mathbb{Z}[\omega] \subset \mathbb{C}$ with the *field norm*

$$N\colon R \to \mathbb{Z}_{\geqslant 0},\ a + b\omega \mapsto a^2 - ab + b^2.$$

(a) Show that the field norm N is multiplicative.

(b) Prove that R is a Euclidean ring with respect to N.

(c) Determine the group of units $R^{\times}$. [*Hint:* Use part (b).]

(d) Write $5 + \omega$ as a product of prime elements from R.

(e) Prove that each prime element of R divides exactly one prime number $p \in \mathbb{Z}$.