1.11 Tutorial 9 MAST30005 Semester I Year 2024

1. Let $K = \mathbb{Q}[\sqrt[p]{n}, \zeta]$ where n is a positive integer that is not a p-th power, p is a prime, and $\zeta = e^{\frac{2\pi i}{p}}$.

   (a) Find $[K : \mathbb{Q}]$ (Hint: What are the degrees of the intermediate field extensions?).

   (b) Show that $|\mathrm{Aut}_{\mathbb{Q}}(K)| \le p(p-1)$.

   (c) Let $\alpha = \sqrt[p]{n} + \zeta$. Prove that $K = \mathbb{Q}[\alpha]$ (if it makes it simpler, assume n is large relative to p).

   (d) Write $K = E[\zeta]$ and $K = F[\sqrt[p]{n}]$ for some appropriate subfields E and F. Deduce the existence of automorphisms σ_i and τ of K such that
$$\sigma_i(\sqrt[p]{n}) = \sqrt[p]{n}, \quad \sigma_i(\zeta) = \zeta^i$$
   and
$$\tau(\sqrt[p]{n}) = \zeta\sqrt[p]{n}, \quad \tau(\zeta) = \zeta.$$

   (e) Show that the automorphism group of K is isomorphic to the group of invertible matrices of the form $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$ where the entries are in $\mathbb{F}_p$.

2. Let $F = \mathbb{C}(w)$. Let $f(x) = x^4 - 4x^2 + 2 - w$.

   (a) Prove that $f(x)$ is irreducible in $F[x]$.

   (b) Let $K = F[x]/(f(x))$. Prove that K is not a splitting field of f.
   [Hint: It may be easier to identify $w = t^4 + t^{-4}$ and identify F with the corresponding subfield of $\mathbb{C}(t)$, as here you can compute the roots of f explicitly]

3. (a) Show that $\mathrm{Aut}(\mathbb{Q})$ is the trivial group.

   (b) Show that $\mathrm{Aut}(\mathbb{R})$ is the trivial group.

4. Let F be a field and $\delta \in F$ an element that is not a square in F. Show that
$$K = \left\{ \begin{pmatrix} a & \delta b \\ b & a \end{pmatrix} \mid a, b \in F \right\} \subset M_{2\times 2}(F) \qquad \text{is a field isomorphic to} \quad F[\sqrt{\delta}] = \frac{F[x]}{(x^2 - \delta)}.$$

5. Let $F \subseteq \mathbb{C}$ be a field and suppose that $f \in F[x]$ is an irreducible (monic) quadratic polynomial. Let the roots of f be $\alpha, \beta \in \mathbb{C}$. Show that

   (a) $F(\alpha) = F(\alpha, \beta)$

   (b) $|\mathrm{Gal}(F(\alpha)/F)| = 2$, $F(\alpha)$ is a Galois extension of F, and the non-trivial element in $\mathrm{Gal}(F(\alpha)/F)$ permutes α and β.

6. (a) Show that if a and b are rational numbers with $(a+b\sqrt{2})^2 = 1+\sqrt{2}$, then $(a-b\sqrt{2})^2 = 1-\sqrt{2}$. Use this to show that $1+\sqrt{2}$ is not a square in $\mathbb{Q}[\sqrt{2}]$.

   (b) Let $K = \mathbb{Q}[\sqrt{1+\sqrt{2}}]$. Find $[K : \mathbb{Q}]$.

   (c) Show that $K/\mathbb{Q}$ is not Galois. [Hint: If it were Galois, then the minimal polynomial of $\sqrt{1+\sqrt{2}}$ would have four roots in K. Find those roots. Are they real?] [Comment: $K/\mathbb{Q}[\sqrt{2}]$ is Galois and $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$ is Galois. This example shows that being Galois is not a transitive property of field extensions.]

7. The n-th cyclotomic polynomial is defined by

$$\Phi_n(x) = \prod_{1 \le k \le n, \gcd(n,k)=1} (x - e^{2\pi i k/n}).$$

   (a) If p is prime, show that

   $$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1.$$

   Can you find a similar formula for Φ_n when n is a power of a prime?

   (b) Prove that

   $$\prod_{d|n} \Phi_d(x) = x^n - 1,$$

   and use this to show by induction on n that $\Phi_n(x) \in \mathbb{Q}[x]$.

   (c) Factor $\Phi_{12}(x)$ into irreducibles in $\mathbb{R}[x]$.

   (d) Prove that $\Phi_{12}(x)$ is irreducible in $\mathbb{Q}[x]$. (A more general fact is that $\Phi_n(x)$ is always irreducible in $\mathbb{Q}[x]$)

   (e) Show that the Galois group of $\Phi_{12}(x)$ over $\mathbb{Q}$ is the Klein Four group.

8. Let $F = \mathbb{Q}(\sqrt[4]{2}, i)$.

   (a) Prove that F is a Galois field extension of $\mathbb{Q}$

   (b) Compute $[F : \mathbb{Q}]$.

   (c) Show that there exists $\tau \in \mathrm{Gal}_{\mathbb{Q}}(F)$ such that $\tau(\sqrt[4]{2}) = i\sqrt[4]{2}$ and $\tau(i) = i$.

   (d) Show that the Galois group $\mathrm{Gal}_{\mathbb{Q}}(F)$ is isomorphic to the dihedral group D_4.

   (e) Find the intermediate fields between $\mathbb{Q}$ and F.