

1 Homework 4.

1. Suppose n is a positive integer and $\zeta_n := e^{2\pi i/n} \in \mathbb{C}$. Prove that $\mathbb{Q}[\sqrt[3]{2}]$ is not a subfield of $\mathbb{Q}[\zeta_n]$ for every n .

(**Hint.** Argue that $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ is not a normal extension and get a contradiction using the main theorem of Galois theory.)

2. Prove that $\mathbb{Q}[\cos(2\pi/n)]/\mathbb{Q}$ is a Galois extension, and

$$\text{Gal}(\mathbb{Q}[\cos(2\pi/n)]/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times / \pm 1.$$

(**Hint.** Argue why $[\mathbb{Q}[\zeta_n] : \mathbb{Q}[\cos(2\pi/n)]] = 2$. Notice that the complex conjugation gives us an element $\tau \in \text{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q})$ and $\mathbb{Q}[\cos(2\pi/n)] \subseteq \text{Fix}(\tau)$; deduce that $\mathbb{Q}[\cos(2\pi/n)] = \text{Fix}(\tau)$. Use the concrete isomorphism $\text{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ and the main theorem of Galois theory to finish the proof.)

3. Suppose p is a prime number and $\overline{\mathbb{F}}_p$ is an algebraic closure of $\mathbb{F}_p$. Let $\sigma_0 : \overline{\mathbb{F}}_p \rightarrow \overline{\mathbb{F}}_p$, $\sigma_0(x) = x^p$.

- (a) Argue why $\overline{\mathbb{F}}_p/\mathbb{F}_p$ is Galois, and prove that $\sigma_0 \in \text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$.
- (b) Prove that $\text{Fix}(\sigma_0^n) =: \mathbb{F}_{p^n}$ is a finite field of order p^n , and

$$\overline{\mathbb{F}}_p = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}.$$

- (c) Prove that

$$\text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \simeq \varprojlim (\mathbb{Z}/n\mathbb{Z})$$

where

$$\varprojlim (\mathbb{Z}/n\mathbb{Z}) := \{(x_n)_n \in \prod_n \mathbb{Z}/n\mathbb{Z} \mid \forall m|n, x_n \equiv x_m \pmod{m}\}.$$

- (d) Prove that $\varprojlim (\mathbb{Z}/n\mathbb{Z})$ is torsion-free.
- (e) Suppose F is a subfield of $\overline{\mathbb{F}}_p$ and $[\overline{\mathbb{F}}_p : F] < \infty$. Prove that $F = \overline{\mathbb{F}}_p$.

(**Hint.** For part (d), suppose $k(x_n)_n = 0$ for some positive integer k ; then for every positive integer n , we have $kx_{kn} \equiv 0 \pmod{kn}$. Hence

$$x_{kn} \equiv 0 \pmod{n}.$$

Because $x_n \equiv x_{kn} \pmod{n}$, deduce that $x_n \equiv 0 \pmod{n}$. Therefore $(x_n)_n = 0$.)

4. Suppose $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$, and $\alpha_0 \in \overline{\mathbb{Q}} \setminus \mathbb{Q}$.

(a) Let $\Sigma_{\alpha_0} := \{F \in \text{Int}(\overline{\mathbb{Q}}/\mathbb{Q}) \mid \alpha_0 \notin F\}$. Prove that Σ_{α_0} has a maximal element with respect to the ordering given by $\subseteq$.

(b) Suppose F is a maximal element of Σ_{α_0} and $E \in \text{Int}(\overline{\mathbb{Q}}/\mathbb{Q})$ is a finite Galois extension of F . Prove that $\text{Gal}(E/F)$ is cyclic.

(**Hint.** For part (b), argue that for every $K \in \text{Int}(E/F)$ which is not F , $F[\alpha_0] \subseteq K$. Use the main theorem of Galois theory and deduce that every proper subgroup of $\text{Gal}(E/F)$ is a subgroup of $\text{Gal}(E/F[\alpha_0])$. Deduce that for every $\sigma \in \text{Gal}(E/F) \setminus \text{Gal}(E/F[\alpha_0])$, $\text{Gal}(E/F) = \langle \sigma \rangle$.)

5. Suppose $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$ and $\hat{\sigma} \in \text{Aut}_{\mathbb{Q}}(\overline{\mathbb{Q}})$. Let F be the field $\text{Fix}(\hat{\sigma})$. Suppose $E \in \text{Int}(\overline{\mathbb{Q}}/\mathbb{Q})$ is a finite Galois extension of F . Prove that $\text{Gal}(E/F)$ is cyclic.

(**Hint.** Argue why the restriction of $\hat{\sigma}$ to E gives us an F -automorphism σ of E . Argue why $\text{Fix}(\langle \sigma \rangle) = F$, and deduce that $\text{Gal}(E/F) = \langle \sigma \rangle$.)

6. Suppose F is a field of characteristic zero and $\overline{F}$ is an algebraic closure of F . Let

$$F^{\text{ab}} := \{\alpha \in \overline{F} \mid F[\alpha]/F \text{ is Galois, } \text{Gal}(F[\alpha]/F) \text{ is abelian}\}.$$

(a) Prove that F^{ab}/F is Galois.

(b) $\text{Gal}(F^{\text{ab}}/F)$ is abelian.

(c) If E/F is a finite Galois extension and $\text{Gal}(E/F)$ is abelian, then $E \subseteq F^{\text{ab}}$.

(**Hint.** For part (a), argue that for every $\alpha \in F^{\text{ab}}$, $F[\alpha]$ is a splitting field of $m_{\alpha,F}$ over F . Deduce that for $\alpha, \beta \in F^{\text{ab}}$, $F[\alpha, \beta]$ is a splitting field of $m_{\alpha,F}m_{\beta,F}$ over F . Hence, $F[\alpha, \beta]/F$ is a normal extension. Argue why the restriction maps give us an embedding

$$\text{Gal}(F[\alpha, \beta]/F) \rightarrow \text{Gal}(F[\alpha]/F) \times \text{Gal}(F[\beta]/F).$$

Deduce that $\text{Gal}(F[\alpha, \beta]/F)$ is an abelian group. Use this to obtain that for every $E \in \text{Int}(F[\alpha, \beta]/F)$, E/F is Galois and $\text{Gal}(E/F)$ is abelian. Conclude that $\alpha \pm \beta, \alpha\beta^{\pm 1}$ are in F^{ab} . Therefore, F^{ab} is a subfield of $\overline{F}$. Argue that for every $\alpha \in F^{\text{ab}}$ and every $\sigma \in \text{Gal}(\overline{F}/F)$, $\sigma(\alpha) \in F[\alpha]$ and $F[\sigma(\alpha)] = F[\alpha]$. Deduce that F^{ab}/F is a normal extension. Argue why the restriction maps give us an embedding

$$\text{Gal}(F^{\text{ab}}/F) \rightarrow \prod_{\alpha \in F^{\text{ab}}} \text{Gal}(F[\alpha]/F),$$

and deduce that $\text{Gal}(F^{\text{ab}}/F)$ is abelian. For the last part, use the primitive element theorem.)

7. Suppose $\mathfrak{a}, \mathfrak{b} \trianglelefteq A$; then $(\mathfrak{a} : \mathfrak{b}) := \{x \in A \mid x\mathfrak{b} \subseteq \mathfrak{a}\}$. Convince yourself that $(\mathfrak{a} : \mathfrak{b})$ is an ideal of A . Prove the following properties:

- (a) $\mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b})$.
- (b) $(\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subseteq \mathfrak{a}$.
- (c) $((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) = (\mathfrak{a} : \mathfrak{b}\mathfrak{c}) = ((\mathfrak{a} : \mathfrak{c}) : \mathfrak{b})$.
- (d) $(\bigcap_i \mathfrak{a}_i : \mathfrak{b}) = \bigcap_i (\mathfrak{a}_i : \mathfrak{b})$.
- (e) $(\mathfrak{a} : \sum_j \mathfrak{b}_j) = \bigcap_j (\mathfrak{a} : \mathfrak{b}_j)$.

8. Suppose k is a field and x, y , and z are indeterminants.

- (a) Let $A := k[x, y, z]/\langle xy - z^2 \rangle$ and $\mathfrak{p} := \langle \overline{x}, \overline{z} \rangle$, where for every polynomial $f \in k[x, y, z]$, $\overline{f} := f + \langle xy - z^2 \rangle \in A$. Prove that $\mathfrak{p} \in \text{Spec}(A)$ and $\mathfrak{p}^2$ is not primary.
- (b) Let $\mathfrak{q} := \langle x, y^2 \rangle \trianglelefteq k[x, y]$. Prove that $\mathfrak{m} := \sqrt{\mathfrak{q}}$ is a maximal ideal of $k[x, y]$. Deduce that $\mathfrak{q}$ is $\mathfrak{m}$ -primary. Prove that $\mathfrak{q} \neq \mathfrak{m}^n$ for any $n \in \mathbb{Z}^+$.
- (c) Let $\mathfrak{a} := \langle x^2, xy \rangle \trianglelefteq k[x, y]$. Show that $\mathfrak{a}$ has at least two reduced primary decompositions.