Math200c, homework 1

Golsefidy

April 2019

Algebraic closure of a finite field.

Suppose $\overline{\mathbb{F}}_p$ is an algebraic closure of $\mathbb{F}_p$. Let $\sigma : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$, be the Frobenius map; that means $\sigma(\alpha) := \alpha^p$.

1. Prove that $\sigma \in \mathrm{Aut}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$.

2. Prove that $\{\alpha \in \overline{\mathbb{F}}_p | \, \sigma^n(\alpha) = \alpha\} \simeq \mathbb{F}_{p^n}$. (We will identify $\mathbb{F}_{p^n}$ with this set of fixed points of σ^n.)

3. Prove that $\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle r_{\mathbb{F}_{p^n}}(\sigma)\rangle$ where $r_{\mathbb{F}_{p^n}} : \mathrm{Aut}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \to \mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is the the restriction homomorphism. **(Hint.**

Show that $\mathbb{F}_{p^n}$ is a splitting field of a separable polynomial; and deduce that $|\operatorname{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = n$.)

4. Prove that $\operatorname{Aut}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \simeq \widehat{\mathbb{Z}}$ where

$$\widehat{\mathbb{Z}} := \{\{a_n + n\mathbb{Z}\}_n \in \prod_{n=2}^{\infty} \mathbb{Z}/n\mathbb{Z} | \; m|n \text{ implies } m|a_n - a_m\}.$$

5. Prove that $\widehat{\mathbb{Z}}$ is torsion free. (**Hint.** Suppose $k\{a_n + n\mathbb{Z}\}_n = 0$. This implies that $n|ka_n$ for any $n \in \mathbb{Z}^+$. Deduce that $n|a_{nk}$ for any n. Since $n|a_{nk} - a_n$, deduce that $n|a_n$; and so $a_n + n\mathbb{Z} = 0$ for any n.)

6. Suppose $\overline{\mathbb{F}}_p/E$ is a finite field extension. Prove that $E = \overline{\mathbb{F}}_p$. (**Hint.** Prove that $\overline{\mathbb{F}}_p$ is a splitting field of a separable polynomial over E. Deduce that $|\operatorname{Aut}(\overline{\mathbb{F}}_p/E)| = [\overline{\mathbb{F}}_p : E]$.)

Splitting fields.

1. Suppose F is a field and $x^n - 1$ has n distinct zeros in F. Suppose $a \in F^{\times}$.

   (a) Prove that $F[\sqrt[n]{a}]$ is a splitting field of a separable polynomial.

(b) Prove that $\{\alpha \in F | \alpha^n = 1\}$ is a cyclic group of order n. (**Hint.** Use problem 4, HW 4, math200a.)

(c) Prove that $\mathrm{Aut}(F[\sqrt[n]{a}]/F)$ can be embedded into $\mathbb{Z}/n\mathbb{Z}$. (**Hint.** Show that $\sigma(\sqrt[n]{a})/\sqrt[n]{a}$ is a zero of $x^n - 1$.)

2. Suppose F is a field of characteristic zero and E is a splitting field of $x^n - 1$ over F. Prove that $\mathrm{Aut}(E/F)$ can be embedded into $(\mathbb{Z}/n\mathbb{Z})^\times$. (**Hint.** Suppose $\{\alpha \in E | \alpha^n = 1\} = \langle \zeta \rangle$ (using 1(b)). Show that $E = F[\zeta]$ and prove that for any $\sigma \in \mathrm{Aut}(E/F)$ there is $i_\sigma \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that $\sigma(\zeta) = \zeta^{i_\sigma}$.)

3. Suppose F is a field and $x^n - 1$ has n distinct zeros in F. Suppose E/F is a finite Galois extension and $a \in E$.

(a) Prove that a Galois closure E' of $E[\sqrt[n]{a}]$ over F is

$$E[\sqrt[n]{\tau(a)} | \tau \in \mathrm{Gal}(E/F)].$$

(**Hint**. Suppose E is a splitting field of the separable polynomial $f(x) \in F[x]$. Show that the above field is a splitting field of $f(x) \prod_{\tau \in \mathrm{Gal}(E/F)}(x^n - \tau(a))$ over F. Use this to show E' is contained in the above field. To get the other direction, notice that any $\tau \in \mathrm{Gal}(E/F)$ can be extended to $\widehat{\tau} \in \mathrm{Gal}(E'/F)$. And $(\widehat{\tau}(\sqrt[n]{a}))^n - \tau(a) = 0$.)

(b) Suppose E' is as above; prove that $\mathrm{Gal}(E'/E)$ is solvable. (**Hint.** Suppose $\mathrm{Gal}(E/F) := \{\tau_1, \ldots, \tau_m\}$; and let $E_0 := E$ and $E_k := E[\sqrt[n]{\tau_1(a)}, \cdots, \sqrt[n]{\tau_k(a)}]$. Use problem 1 to show, E_{k+1}/E_k is a cyclic extension; that means it is a Galois extension with cyclic Galois group. Consider the chain of subgroups

$$1 \subseteq \mathrm{Gal}(E'/E_{m-1}) \subseteq \mathrm{Gal}(E'/E_{m-2}) \subseteq \cdots \subseteq \mathrm{Gal}(E'/E).$$

Argue why $\mathrm{Gal}(E'/E_k)/\mathrm{Gal}(E'/E_{k+1}) \simeq \mathrm{Gal}(E_{k+1}/E_k)$; and deduce that $\mathrm{Gal}(E'/E)$ is solvable.)

4. Suppose F is a field of characteristic zero,

$$F =: F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n$$

is a chain of fields such that $F_{i+1} = F_i[\sqrt[m_i]{a_i}]$ for some $a_i \in F_i^{\times}$. Suppose F' is a Galois closure of F_n over F. Prove that $\mathrm{Gal}(F'/F)$ is solvable. (**Hint.** Let E_0 be a splitting field of $x^m - 1$ over F_0 where $m = \prod_{i=1}^{n} m_i$. Let E_{i+1} be a

Galois closure of $E_i[\sqrt[m_i]{a_i}]$ over F_0. Consider the chain of subgroups

$$1 \subseteq \mathrm{Gal}(E_n/E_{n-1}) \subseteq \cdots \subseteq \mathrm{Gal}(E_n/E_0) \subseteq \mathrm{Gal}(E_n/F_0).$$

Argue why $\mathrm{Gal}(E_n/E_k)/\mathrm{Gal}(E_n/E_{k+1}) \simeq \mathrm{Gal}(E_{k+1}/E_k)$ and it is solvable. Argue why $\mathrm{Gal}(E_n/F_0)/\mathrm{Gal}(E_n/E_0) \simeq \mathrm{Gal}(E_0/F_0)$ is abelian. Deduce that $\mathrm{Gal}(E_n/F_0)$ is solvable. Argue why F' can be viewed as a subfield of E_n; and deduce that $\mathrm{Gal}(F'/F)$ is solvable.

5. Suppose p is prime and $E \subseteq \mathbb{C}$ is a splitting field of $x^p - 2$ over $\mathbb{Q}$. Prove that $\mathrm{Aut}(E/\mathbb{Q}) \simeq \mathbb{Z}/p\mathbb{Z} {}_{\phi}\!\rtimes (\mathbb{Z}/p\mathbb{Z})^{\times}$ where $\phi : (\mathbb{Z}/p\mathbb{Z})^{\times} \to \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$, $(\phi(a))(b) := ab$. (**Hint.** In the previous HW assignment you have showed that $E = \mathbb{Q}[\zeta_p, \sqrt[p]{2}]$ and $[E : \mathbb{Q}] = p(p-1)$. Argue why $|\mathrm{Aut}(E/\mathbb{Q})| = p(p-1)$. For $\sigma \in \mathrm{Aut}(E/\mathbb{Q})$ investigate what the possibilities of $(\sigma(\zeta_p), \sigma(\sqrt[p]{2}))$ are.)

6. Suppose $f(x) \in \mathbb{Q}[x]$ is irreducible, $\deg f = p$ is prime, f has $p-2$ real and 2 non-real zeros in $\mathbb{C}$. Let $E \subseteq \mathbb{C}$ be a splitting field of $f(x)$ over $\mathbb{Q}$. Prove that $\mathrm{Aut}(E/\mathbb{Q}) \simeq S_p$. (**Hint**. Since $E/\mathbb{Q}$ is a normal extension, restriction of

complex conjugation gives us an element of $\mathrm{Aut}(E/\mathbb{Q})$. Let $\alpha \in E$ be a zero of $f(x)$; then $p = [\mathbb{Q}[\alpha] : \mathbb{Q}] | [E : \mathbb{Q}]$). Argue why $[E : \mathbb{Q}] = |\mathrm{Aut}(E/\mathbb{Q})|$. Let $X \subseteq E$ be the set of zeros of $f(x)$. Argue why restriction to X gives us an embedding of $\mathrm{Aut}(E/\mathbb{Q})$ into the symmetric group S_X of X which is isomorphic to S_p. Get a subgroup of S_p that contains a transposition and a cycle of length p. Use problem 7(b), HW 4, math200a.)

7. Suppose F is a field, $f(x) \in F[x]$ is irreducible, and E is a splitting field of $f(x)$ over F. Suppose there is $\alpha \in E$ such that $f(\alpha) = f(\alpha + 1) = 0$. Prove that

   (a) Characteristic of F is a prime number p.

   (b) Show that $\mathrm{Aut}(E/F)$ has a subgroup of order p.