

1 Homework 2.

1. Let $\Phi_n(x)$ be the n -th cyclotomic polynomial. Suppose p is an odd prime which does not divide n . Let $\Phi_{n,p} \in \mathbb{F}_p[x]$ be $\Phi_n(x) \pmod{p}$. Let $\overline{\mathbb{F}}_p$ be an algebraic closure of $\mathbb{F}_p$ and $E \subseteq \overline{\mathbb{F}}_p$ is a splitting field of $\Phi_{n,p}(x)$ over $\mathbb{F}_p$.

- (a) Suppose $\zeta \in E$ is a zero of $\Phi_{n,p}(x)$. Prove that ζ is not a zero of $\Phi_{d,p}(x)$ for any $d|n$ and $d \neq n$. Deduce that the multiplicative order $o(\zeta)$ of ζ is n .

(**Hint.** $x^n - 1$ does not have multiple zeros in $\overline{\mathbb{F}}_p$.)

- (b) Prove that $\Phi_{n,p}(x) = \prod_{1 \leq i \leq n, \gcd(i,n)=1} (x - \zeta^i)$ where $\zeta \in E$ is a zero of $\Phi_{n,p}(x)$. Deduce that $E = \mathbb{F}_p[\zeta]$ and

$$\theta : \text{Gal}(\mathbb{F}_p[\zeta]/\mathbb{F}_p) \rightarrow (\mathbb{Z}/n\mathbb{Z})^\times, \theta(\sigma) = a_\sigma \pmod{n}$$

is an injective group homomorphism where $\sigma(\zeta) = \zeta^{a_\sigma}$.

- (c) Suppose θ is as in the previous problem. Prove that

$$\theta(\text{Gal}(E/F)) = \langle p \rangle.$$

(**Hint.** Use the fact that $\text{Gal}(E/F) = \langle \sigma_p \rangle$, where $\sigma_p(a) = a^p$ is the Frobenius map.)

- (d) Prove that if $\Phi_{n,p}(x)$ has a zero in $\mathbb{F}_p$, then $n|p-1$.
 (e) Use the previous problem to show there are infinitely many primes of the form $\{nk+1\}_{k=1}^\infty$.

(**Hint.** Suppose $p_1, \dots, p_r$ are primes of the form $nk+1$. Consider

$$f(x) := \Phi_n((2n \prod_{i=1}^r p_i)x);$$

for some value of $a \in \mathbb{Z}$, $f(a)$ has a prime factor ℓ . Argue why $\ell \nmid n$ and $\ell \neq p_i$. Use the previous problem to deduce that $n|\ell-1$.)

- (f) Prove that $\Phi_{n,p}(x)$ is irreducible in $\mathbb{F}_p[x]$ if and only if $\langle p \rangle = (\mathbb{Z}/n\mathbb{Z})^\times$.

2. Suppose E/F is an algebraic extension. Let

$$E_{\text{sep},F} := \{\alpha \in E \mid m_{\alpha,F}(x) \text{ is separable}\}.$$

- (a) Prove that $E_{\text{sep},F}$ is a field and $E_{\text{sep},F}/F$ is a separable extension.
(Hint. For $\alpha, \beta \in E_{\text{sep},F}$, suppose L is a splitting field of $m_{\alpha,F}(x)m_{\beta,F}(x)$ over F . Argue that L/F is Galois; and so it is separable. Deduce that $\alpha \pm \beta, \alpha\beta^{\pm 1} \in E_{\text{sep},F}$.)

- (b) Prove that if $\text{char}(F) = p > 0$, then for every $\alpha \in E$, there exists $l \in \mathbb{Z}$ such that $\alpha^{p^l} \in E_{\text{sep},F}$ and $m_{\alpha, E_{\text{sep},F}}(x) = x^{p^l} - \alpha^{p^l}$.

(Hint. Argue that for $\alpha \in E$, there is a separable irreducible polynomial $g_\alpha(x) \in F[x]$ such that $m_{\alpha,F}(x) = g_\alpha(x^{p^k})$. Deduce that

$$\alpha^{p^k} \in E_{\text{sep},F};$$

and so order of $\alpha(E_{\text{sep},F})^\times$ is a power of p and $m_{\alpha, E_{\text{sep},F}}(x) | (x - \alpha)^{p^k}$. Use these results to deduce that $m_{\alpha, E_{\text{sep},F}}(x) = (x - \alpha)^{p^l} = x^{p^l} - \alpha^{p^l}$.)

(we say $E/E_{\text{sep},F}$ is a purely inseparable extension.)

- (c) Suppose E/F is a normal extension. Prove that $E_{\text{sep},F}/F$ is a Galois extension.
- (d) Suppose $F \subseteq E \subseteq K$ is a tower of algebraic field extensions. Prove that K/F is separable if and only if K/E and E/F are separable.
(Hint. $(\Rightarrow)$ $m_{\alpha,E}(x) | m_{\alpha,F}(x)$. $(\Leftarrow)$ Argue that $E \subseteq K_{\text{sep},F}$. Deduce that for every $\alpha \in K$, $m_{\alpha, K_{\text{sep},F}}(x) | m_{\alpha,E}(x)$. On the other hand, $m_{\alpha, K_{\text{sep},F}}(x) = (x - \alpha)^{p^l}$ for some $l \in \mathbb{Z}$. Deduce that $l = 0$ and $\alpha \in K_{\text{sep},F}$.)

3. Suppose F is a field and $\mu_n(F) := \{\zeta \in F \mid \zeta^n = 1\}$ has n elements. Suppose E/F is a finite Galois extension and $a \in E$.

- (a) Prove that there exists a Galois extension E'/F with the following properties:
- For every $\tau \in \text{Gal}(E/F)$, E' contains a splitting field $E[\sqrt[n]{\tau(a)}]$ of $x^n - \tau(a)$ over E .
 - The field E' is generated by E and the elements $\sqrt[n]{\tau(a)}$ as τ ranges in $\text{Gal}(E/F)$.

(Hint. Suppose E is a splitting field of the separable polynomial $f(x) \in F[x]$. Let $\mathcal{O}_a := \text{Gal}(E/F) \cdot a$ be the orbit of the Galois group.

Recall that

$$m_{a,F}(x) = \prod_{a' \in \theta_a} (x - a').$$

Let E' be a splitting field of $f(x)m_{a,F}(x^n)$ over F .

- (b) Suppose E' is as above; prove that $\text{Gal}(E'/E)$ is solvable.

(Hint. Suppose $\text{Gal}(E/F) := \{\tau_1, \dots, \tau_m\}$; and let $E_0 := E$ and $E_k := E[\sqrt[n]{\tau_1(a)}, \dots, \sqrt[n]{\tau_k(a)}]$. Argue why E_{k+1}/E_k is a cyclic extension. Consider the chain of subgroups

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

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

4. Suppose F is a field of characteristic zero,

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

is a chain of fields such that $F_{i+1} = F_i[\sqrt[m_i]{a_i}]$ for some $a_i \in F_i^\times$. Prove that there exists a field extension F'/F_n such that F'/F is a Galois extension and $\text{Gal}(F'/F)$ is solvable.

(Hint. Let E_0 be a splitting field of $x^m - 1$ over F_0 where $m = \prod_{i=1}^n m_i$. Using the previous problem, show that there exists a field extension E_{i+1}/E_i such that $\sqrt[m_i]{a_i} \in E_{i+1}$, E_{i+1}/F_0 is a Galois extension, and $\text{Gal}(E_{i+1}/E_i)$ is solvable. Consider the chain of subgroups

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

Argue why $\text{Gal}(E_n/E_k)/\text{Gal}(E_n/E_{k+1}) \simeq \text{Gal}(E_{k+1}/E_k)$ and it is solvable. Argue why $\text{Gal}(E_n/F_0)/\text{Gal}(E_n/E_0) \simeq \text{Gal}(E_0/F_0)$ is abelian. Deduce that $\text{Gal}(E_n/F_0)$ is solvable. Argue why E_n contains a copy of F_n .)

5. 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 $\text{Gal}(E/\mathbb{Q}) \simeq S_p$.

(Hint. Since $E/\mathbb{Q}$ is a normal extension, restriction of complex conjugation gives us an element of $\text{Aut}(E/\mathbb{Q})$. Let $\alpha \in E$ be a zero of $f(x)$; then

$p = [\mathbb{Q}[\alpha] : \mathbb{Q}][E : \mathbb{Q}]$. Argue why $[E : \mathbb{Q}] = |\text{Aut}(E/\mathbb{Q})|$. Let $X \subseteq E$ be the set of zeros of $f(x)$. Argue why restriction to X gives us an embedding of $\text{Aut}(E/\mathbb{Q})$ 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 .)