Homework 9

Friday, March 9, 2018 1:11 AM

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

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

(2) 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 $d \mid n$ and $d \neq n$. Deduce that $o(\zeta) = n$ as an element of $E^\times$.

(3) Use part (2), to show $\Phi_{n,p}(x) = \prod_{\substack{1 \le i \le n \\ \gcd(i,n)=1}} (x - \zeta^i)$. Deduce that $E = \mathbb{F}_p[\zeta]$, and $Gal(\mathbb{F}_p[\zeta]/\mathbb{F}_p) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$.
Use the fact that the Frob. map $x \longmapsto x^p$ generates $Gal(\mathbb{F}_p[\zeta]/\mathbb{F}_p)$ to deduce $Gal(\mathbb{F}_p[\zeta]/\mathbb{F}_p) \simeq \langle p \rangle$ where $\langle p \rangle \subseteq (\mathbb{Z}/n\mathbb{Z})^\times$.

(4) Prove, if $\Phi_{n,p}(x)$ has a zero in $\mathbb{F}_p$, then $n \mid p-1$.

Use this to show there are infinitely many primes of the form $\{nk+1\}_{k=1}^{\infty}$

Homework 9

Friday, March 9, 2018 1:46 AM

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

$\boxed{2}$ Suppose $\mathbb{Q}[\zeta_n] \subseteq F \subseteq \mathbb{C}$ is a tower of fields where $\zeta_n = e^{\frac{2\pi i}{n}}$.

(1) For $a_1, a_2 \in F^\times$, prove that

$$F[\sqrt[n]{a_1}] = F[\sqrt[n]{a_2}] \Leftrightarrow a_1 (F^\times)^n = a_2 (F^\times)^n$$

(Here $\sqrt[n]{a}$ means an element of $\mathbb{C}$ which is a zero of $x^n - a$.)

(2) Prove that $F[\sqrt[n]{a}]/F$ is a Galois extension for any $a \in F^\times$, and $\mathrm{Gal}(F[\sqrt[n]{a}]/F) \simeq \langle a(F^\times)^n \rangle \subseteq F^\times/(F^\times)^n$.

$\boxed{3}$ Suppose E/F is a finite extension. For any $a \in E$, let $l_a : E \to E$, $l_a(e) := ae$. View l_a as an element of $\mathrm{End}_F(E)$. Prove that E/F is separable if and only if $\forall a \in E$, l_a is diagonalizable over an algebraic closure $\overline{F}$ of F.

$\boxed{4}$ Let F be a field. Suppose for any finite extension E/F, $p \nmid [E:F]$, where p is an odd prime.

(1) Suppose E/F is a finite separable extension. Prove $[E:F] = p^n$ for some $n \in \mathbb{Z}^{\geq 0}$.

(2) Suppose F is not perfect. Prove $\mathrm{char}(F) = p$.

(3) Suppose E/F is any finite extension. Prove $[E:F] = p^n$.

Homework 9

Friday, March 9, 2018 2:27 AM

$\boxed{5}$ Suppose E/F is an algebraic extension. Let

$$F^{ab} := \{\alpha \in E \mid F[\alpha]/F \text{ is Galois } \underline{\text{and}} \; \mathrm{Gal}(F[\alpha]/F) \text{ is abelian}\}$$

(1) Suppose $F \subseteq K \subseteq E$, K/F is Galois, and $\mathrm{Gal}(K/F)$ is abelian. Prove that $K \subseteq F^{ab}$.

(2) Prove that F^{ab} is a field.

(3) Prove that F^{ab}/F is Galois and $\mathrm{Gal}(F^{ab}/F)$ is abelian.

$\boxed{6}$ Let $q = p^n$ where p is a prime and $n \in \mathbb{Z}^+$. Prove that any irreducible factor of $x^q - x + 1 \in \mathbb{F}_q[x]$ has degree p.

(Hint: Suppose α is a zero of $x^q - x + 1$ in a splitting field. Prove that $\alpha^{q^i} = \alpha - i$; and so $\alpha^{q^p} = \alpha$ and $\alpha^{q^i} \neq \alpha$ for $1 \leq i \leq p-1$.

Hence $\mathbb{F}_q[\alpha] = \mathbb{F}_{q^p}$.)

$\boxed{7}$. Suppose F is a field, $f(x) \in F[x]$ is irreducible, and E is a splitting field of $f(x)$ over F. Suppose $\exists \alpha \in E$ s.t. $f(\alpha) = f(\alpha+1) = 0$. Prove that

(1) $\mathrm{Char}\, F = p > 0$. (2) $\exists\, F \subseteq K \subseteq E$ s.t. E/K is Galois and $[E:K] = p$.

Homework 9

Friday, March 9, 2018 8:13 AM

$\boxed{8}$ Suppose F is a field and $\mathrm{char}(F) \neq 2$. Let $a_1, \ldots, a_n \in F^\times$,

$H := \langle a_1 (F^\times)^2, \ldots, a_n (F^\times)^2 \rangle \leq F^\times/(F^\times)^2$, and $E := F[\sqrt{a_1}, \ldots, \sqrt{a_n}]$.

(1) Prove that E/F is a Galois extension.

(2) Let $G := \mathrm{Gal}(E/F)$. Prove that G is an elementary abelian 2-group; that means $G \simeq (\mathbb{Z}/2\mathbb{Z})^m$ for some $m \in \mathbb{Z}^{\geq 0}$.

(3) Prove that H is an elementary abelian 2-group.

(4) Let $T : G \times H \longrightarrow \{\pm 1\} \simeq (\mathbb{Z}/2\mathbb{Z})$ be

$$T(\sigma, a(F^\times)^2) := \sigma(\sqrt{a})/\sqrt{a}.$$

Prove that T is a non-degenerate bilinear form; that means $T(\sigma_1\sigma_2, \bar{a}) = T(\sigma_1, \bar{a})\, T(\sigma_2, \bar{a})$,

$T(\sigma, \bar{a}\,\bar{a}') = T(\sigma, \bar{a})\, T(\sigma, \bar{a}')$, and

$$\begin{cases} \forall \sigma \in G, & T(\sigma, \bar{a}_0) = 1 \Rightarrow \bar{a}_0 = \bar{1} \\ \forall \bar{a} \in H, & T(\sigma_0, \bar{a}) = 1 \Rightarrow \sigma_0 = \mathrm{id}_E \end{cases}$$

(5) Deduce that $\mathrm{Gal}(F[\sqrt{a_1}, \ldots, \sqrt{a_n}]/F) \simeq \langle a_1 (F^\times)^2, \ldots, a_n (F^\times)^2 \rangle$.

Homework 9

Friday, March 9, 2018 12:01 PM

$\boxed{9}$ (1) In class we proved that $\mathrm{Aut}(\overline{F}/F) \simeq \varprojlim_{\substack{E/F \\ \text{finite, normal}}} \mathrm{Aut}(E/F)$. And so

$\mathrm{Aut}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \simeq \varprojlim_n \mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. Deduce that

$\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \simeq \varprojlim \mathbb{Z}/n\mathbb{Z} := \{(a_m) \in \prod (\mathbb{Z}/m\mathbb{Z}) \mid \forall d \mid m, a_m \overset{d}{\equiv} a_d\}$.

(2) Prove that $\varprojlim \mathbb{Z}/n\mathbb{Z}$ has no non-trivial torsion element.

(3) Suppose $E \subseteq \overline{\mathbb{F}}_p$ is a subfield and $[\overline{\mathbb{F}}_p : E] < \infty$.

Prove that $E = \overline{\mathbb{F}}_p$.

$\boxed{10}$ Suppose E/F is a finite Galois extension. Suppose

$\mathrm{Gal}(E/F) = \langle \sigma \rangle$. View σ as an element of $\mathrm{End}_F(E)$.

Let $n := [E:F]$. For $a \in E^\times$, let $l_a : E \to E$, $l_a(e) = ae$.

view l_a as an element of $\mathrm{End}_F(E)$; and let $\tau_a := l_a \circ \sigma$.

(1) Prove that $\tau_a^i = l_{a\sigma(a)\cdots\sigma^{i-1}(a)} \circ \sigma^i$.

(2) Prove that the minimal polynomial of τ_a (as an element of $\mathrm{End}_F(E)$) is $x^n - N_{E/F}(a)$ where $N_{E/F}(a) = \prod_{i=0}^{n-1} \sigma^i(a)$.

(3) Find rational canonical form of τ_a.

Homework 9

Friday, March 9, 2018 12:21 PM

(4) Suppose, for $a \in E^{\times}$, $N_{E/F}(a) = 1$. Show τ_a has eigenvalue one, and deduce $\exists\, b \in E$ s.t. $a = b/\sigma(b)$.

(5) Prove that $N_{E/F} : E^{\times} \longrightarrow F^{\times}$ is a group homomorphism and

$$\ker(N_{E/F}) = \{ b/\sigma(b) \mid b \in E^{\times} \}.$$

(6) Prove $\exists\, \alpha \in E$ s.t. $\{\alpha, \sigma(\alpha), \sigma^2(\alpha), \dots, \sigma^{n-1}(\alpha)\}$ is an F-basis of E. (Hint. Use part (3) for $a=1$.)