# MATH200C, HOMEWORK 2

GOLSEFIDY

## Cyclotomic extensions.

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 $\mathbb{F}_p$.

(1) Suppose $\zeta \in E$ is a zero of $\Phi_{n,p}(x)$. Prove that $\zeta$ 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 $\zeta$ is $n$. (**Hint**. $x^n - 1$ does not have multiple zeros in $\overline{\mathbb{F}}_p$.)

(2) Prove that $\Phi_{n,p}(x) = \prod_{1\le i\le n, \gcd(i,n)=1}(x - \zeta^i)$ where $\zeta \in E$ is a zero of $\Phi_{n,p}(x)$. Deduce that $E = \mathbb{F}_p[\zeta]$ and $\theta : \mathrm{Gal}(\mathbb{F}_p[\zeta]/\mathbb{F}_p) \to (\mathbb{Z}/n\mathbb{Z})^\times, \theta(\sigma) = a_\sigma \pmod{n}$ is an injective group homomorphism where $\sigma(\zeta) = \zeta^{a_\sigma}$.

(3) Suppose $\theta$ is as in the previous problem. Prove that $\theta(\mathrm{Gal}(E/F)) = \langle p \rangle$. (**Hint**. Use the fact that $\mathrm{Gal}(E/F) = \langle \sigma_p \rangle$, where $\sigma_p(a) = a^p$ is the Frobenius map.)

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

(5) Use the previous problem to show there are infinitely many primes of the form $\{nk+1\}_{k=1}^\infty$. (**Hint**. Suppose $p_1, \ldots, p_r$ 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 $\ell$. Argue why $\ell \nmid n$ and $\ell \neq p_i$. Use the previous problem to deduce that $n|\ell - 1$.)

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

## Separable and purely inseparable extensions.

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

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

*Date*: April 2019.

(1) Prove that $E^{\text{sep}}$ is a field and $E^{\text{sep}}/F$ is a separable extension. (**Hint**. For $\alpha, \beta \in E^{\text{sep}}$, 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 $\alpha \pm \beta, \alpha\beta^{\pm 1} \in E^{\text{sep}}$.)

(2) Prove that if $\text{char}(F) = p > 0$, then for any $\alpha \in E$ there is $l \in \mathbb{Z}$ such that $\alpha^{p^l} \in E^{\text{sep}}$ and $m_{\alpha,E^{\text{sep}}}(x) = x^{p^l} - \alpha^{p^l}$. (**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 $\alpha^{p^k} \in E^{\text{sep}}$; and so order of $\alpha(E^{\text{sep}})^\times$ is a power of $p$ and $m_{\alpha,E^{\text{sep}}}(x)|(x-\alpha)^{p^k}$. Use these results to deduce that $m_{\alpha,E^{\text{sep}}}(x) = (x-\alpha)^{p^l} = x^{p^l} - \alpha^{p^l}$.)

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

(3) Suppose $E/F$ is a normal extension. Prove that $E^{\text{sep}}/F$ is a Galois extension.

(4) 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 $E \subseteq K^{\text{sep}}$, where $K^{\text{sep}} := \{\alpha \in K | m_{\alpha,F}(x) \text{ is separable}\}$. Deduce that for any $\alpha \in K$, $m_{\alpha,K^{\text{sep}}}(x)|m_{\alpha,E}(x)$. On the other hand $m_{\alpha,K^{\text{sep}}}(x) = (x-\alpha)^{p^l}$ for some $l \in \mathbb{Z}$. Deduce that $l = 0$ and $\alpha \in K^{\text{sep}}$.)

## Kummer theory

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

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

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

(Here $\sqrt[n]{a}$ means an element of $\mathbb{C}$ which is a zero of $x^n - a$.) (**Hint.** ($\Rightarrow$) Recall that $\psi_1 : \text{Gal}(F[\sqrt[n]{a_1}]/F) \to \{1, \zeta_n, \ldots, \zeta_n^{n-1}\} \simeq \mathbb{Z}/n\mathbb{Z}$, $\psi_1(\sigma) := \sigma(\sqrt[n]{a_1})/\sqrt[n]{a_1}$ is an injective group homomorphism. Similarly one can define $\psi_2$. Since $\mathbb{Z}/n\mathbb{Z}$ has a unique subgroup of order $[F[\sqrt[n]{a_1}] : F]$, we have that $\text{Im}(\psi_1) = \text{Im}(\psi_2)$. Suppose $\sigma_0$ is a generator of $\text{Gal}(F[\sqrt[n]{a_1}]/F)$; then $\sigma_0(\sqrt[n]{a_1})/\sqrt[n]{a_1} = (\sigma_0(\sqrt[n]{a_2})/\sqrt[n]{a_2})^i$ for some $i$. This implies that $\sigma_0(\sqrt[n]{a_1}/\sqrt[n]{a_2}^i) = \sqrt[n]{a_1}/\sqrt[n]{a_2}^i$; deduce that $a_1(F^\times)^n \in \langle a_2(F^\times)^n \rangle$.)

(2) Prove that $\mathrm{Gal}(F[\sqrt[n]{a}]/F) \simeq \langle a(F^\times)^n\rangle$ for any $a \in F^\times$. (**Hint**. Suppose $\sigma_0$ is a generator of $\mathrm{Gal}(F[\sqrt[n]{a}]/F)$. Then by the above argument

$$\sigma_0^d = \mathrm{id} \Leftrightarrow (\sigma_0(\sqrt[n]{a})/\sqrt[n]{a})^d = 1 \Leftrightarrow \sqrt[n]{a}^d \in F^\times \Leftrightarrow a^d \in (F^\times)^n.)$$