MAT 250B HW10

[add your name here]

Due Friday, 3/15/24 at 11:59 pm on Gradescope

Exercise 1

Let σ_p denote the Frobenius map $a \mapsto a^p$ on the finite field $\mathbb{F}_{p^n}$. Verify that σ_p is an automorphism of $\mathbb{F}_{p^n}$, and that the order of σ_p is n.

Exercise 2

Let $\mu_n \subset \mathbb{C}$ denote the set of nth roots of unity. The n-th cyclotomic polynomial is

$$\Phi_n(x) = \prod_{\text{primitive } \zeta \in \mu_n} (x - \zeta).$$

Fact $\Phi_n(x)$ is an irreducible monic polynomial in $\mathbb{Z}[x]$. Hence $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$.

Unfortunately, we don't have time to talk about the proof of this in class. You can find the proof in various textbooks, and already have the tools to understand the proof.

Observations

1. $x^n - 1 = \prod_{\zeta \in \mu_n} (x - \zeta) = \prod_{d \mid n} \prod_{\text{primitive } \zeta \in \mu_d} (x - \zeta) = \prod_{d \mid n} \Phi_d(x)$
2. $\deg \Phi_n(x) = \phi(n)$, where ϕ is Euler's totient function.

Over $\mathbb{F}_p$ Let p be a prime. The splitting field of $x^n - 1$ contains all the n-th roots of unity $\mu_n \subset \overline{\mathbb{F}}_p$. The observations above still hold, since we are just taking the coefficients of polynomials mod p.

If $a \in \mathbb{F}_{p^n}^\times$ and $|a| = m$, then we still have $\Phi_m(a) = 0$. But also, for all $d < m$, $\Phi_d(a) \neq 0$ since a is not a dth root of $1 \in \mathbb{F}_p$. So $\Phi_m(x) = m_{a,\mathbb{F}_p}(x)$ still holds.

(a) Determine $\Phi_p(x) \in \mathbb{Z}[x]$. Then, for p prime, show that $\Phi_p(x) \equiv (x-1)^{p-1} \mod p$. *This should be a fairly short explanation.*

(b) Prove that if $d \mid (p^n - 1) = |\mathbb{F}_{p^n}^\times|$, then $\Phi_d(x) \in \mathbb{F}_p[x]$ has exactly $\phi(d)$ roots in $\mathbb{F}_{p^n}^\times$.

Hint: These roots are precisely the primitive dth roots of unity over $\mathbb{F}_p$. *Use the fact that* $|\mathbb{F}_{p^n}^\times| = p^n - 1 = \sum_{d \mid p^n - 1} \phi(d)$.

(c) Prove that n divides $\phi(p^n - 1)$. *Hint: Think about* $\operatorname{Aut}(\mathbb{F}_{p^n}^\times)$.

Exercise 3

Let $d, n \in \mathbb{N}$.

(a) Prove that $d \mid n$ if and only if $x^d - 1$ divides $x^n - 1$.

Hint: If $n = qd + r$, then $x^n - 1 = (x^{qd+r} - x^r) + (x^r - 1)$.

(b) Prove that for any $a \in \mathbb{N}$,

$$d \mid n \qquad \text{if and only if} \qquad a^d - 1 \mid a^n - 1.$$

(c) Conclude that $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$ if and only if $d \mid n$.

Exercise 4

Compute the Galois groups of the following polynomials over the given fields.

(a) $x^8 - x$ over $\mathbb{Q}$

(b) $x^8 - x$ over $\mathbb{F}_2$

(c) $x^4 - 1$ over $\mathbb{F}_7$

Exercise 5

Let p be a prime. Determine the elements of the Galois group of $x^p - 2 \in \mathbb{Q}[x]$.