Math 210B Lecture 3 Notes

Daniel Raban

January 11, 2019

1 Finite Fields and Cyclotomic Fields

1.1 Finite fields

Proposition 1.1. *Let F be a field and $n \geq 1$. Let $\mu_n(F)$ be the n-th roots of unity in F. Then $\mu_n(F)$ is cyclic of order dividing n.*

Proof. Let m be the exponent of $\mu_n(F)$. Then $x^m - 1 = 0$ for all $x \in \mu_n(F)$. So $|\mu_n(F)| \leq m$. Then $|\mu_n(F)| = m$. □

Lemma 1.1. *Let F be a finite field. Then $|F|$ is a power of* $\operatorname{char}(F)$.

Proof. Let $p = \operatorname{char}(F)$. Then F is a vector space over $\mathbb{F}_p$. Then $|F| = p^{[F:\mathbb{F}_p]}$. □

Corollary 1.1. *If $|F| = p^n$, then $F^\times$ is cyclic with $F^\times = \mu_{p^n-1}(F)$.*

Corollary 1.2. $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$.

Lemma 1.2. *Let* $\operatorname{char}(F) = p$ *and $\alpha, \beta \in$. Then $(\alpha+\beta)^{p^k} = \alpha^{p^k} + \beta^{p^k}$.*

Proof. This follows from the Binomial theorem. □

Theorem 1.1. *Let $n \geq 1$. Then there exists a unique extension $\mathbb{F}_{p^n}$ of $\mathbb{F}_p$ of degree n up to isomorphism. If $E/\mathbb{F}_p$ is a finite extension of degree a multiple of n, then E contains a unique subfield isomorphic to $\mathbb{F}_{p^n}$. Moreover, $\mathbb{F}_{p^n} \subseteq \mathbb{F}_p^m \iff n \mid m$.*

Proof. Let $\mathbb{F}_{p^n}$ be the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$. Let $F = \{\alpha \in \mathbb{F}_{p^n} L \alpha^{p^n} = \alpha\}$. Note that F is closed under addition by the lemma and is closed under multiplication and taking inverses of nonzero elements. So F is a field. In fact, F is a splitting field of the polynomial, so $F = \mathbb{F}_{p^n}$.

We know that $|\mathbb{F}_{p^n}| \leq p^n$ because the polynomial $x^{p^n} - x$ has at most p^n roots; we want equality. Let $a \in \mathbb{F}_{p^n}^\times$. Consider the polynomial $g(x) = (x^{p^n} - x)/(x-a)$. Then $g(x) = \sum_{i=1}^{p^n-1} a^{i-1} x^{p^n-i}$. Then

$$g(a) = \sum_{i=1}^{p^n-1} a^{p^n-1} = (p^n-1)a^{p^{n-1}} = (0-1)1 = -1 \neq 0.$$

So $x^{p^n} - x$ has p^n distinct roots, giving us $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$.

Let E have degree m, where $n \mid m$. Then $E \cong \mathbb{F}_{p^m}$, so $E^\times = \mu_{p^m-1}(E)$. Since $\mu_{p^n-1}(E) \subseteq \mu_{p^m-1}(E)$, we have $F \subseteq E$ with $F \cong \mathbb{F}_{p^n}$. □

Example 1.1. $[\mathbb{F}_9 : \mathbb{F}_3] = 2$. We can compute that x^2+1, x^2+x-1, and x^2-x-1 are the quadratic irreducible polynomials over $\mathbb{F}_3$. $\mathbb{F}_9$ is the splitting field of each. We get

$$x^9 - x = (x^2+1)(x^2+x-1)(x^2-x-1)x(x+1)(x-1).$$

Proposition 1.2. *Let q be a power of p. Let $m \geq 1$, and let ζ_m be a primitive m-th root of unity in an extension of $\mathbb{F}_q$. Then $[\mathbb{F}_q(\zeta_m) : \mathbb{F}_q]$ equals the order of q in $(\mathbb{Z}/m\mathbb{Z})^\times$.*

Proof.

$$\begin{aligned} \ell = [\mathbb{F}_q(\zeta_m) : \mathbb{F}_q] &\iff \mathbb{F}_q(\zeta_m) = \mathbb{F}_{q^\ell} \\ &\iff m \mid q^\ell - 1 \text{ and } m \nmid q^{j-1} \text{ for all } j < \ell \\ &\iff q \text{ has order } \ell \text{ in } (\mathbb{Z}/m\mathbb{Z})^\times. \end{aligned}$$ □

Proposition 1.3. *Let $m \geq 1$ and $m = p_1^{r_1} \cdots p_k^{r_k}$, where the p_i are distinct primes. THen $(\mathbb{Z}/m\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{r_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{r_k}\mathbb{Z})\times$, and*

$$(\mathbb{Z}/p^r\mathbb{Z})^\times \cong \begin{cases} \mathbb{Z}/p^{r-1}\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} & p \text{ odd} \\ \mathbb{Z}/2^{r-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & p = 2, r \geq 2. \end{cases}$$

Proof. The map $(\mathbb{Z}/p^r\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ has kernel

$$\frac{1+p\mathbb{Z}}{1+p^r\mathbb{Z}} \subseteq (\mathbb{Z}/p^r\mathbb{Z})^\times.$$

If p is odd,

$$(1+p^k)^p = 1 + p^{k+1} + \cdots + (p^k)^p.$$

Then $kp > k+1 \iff k(p-1) > 1 \iff k \geq 2$ or $p \geq 3$. So if p is odd, then $(1+p^k)^p \cong 1 + p^{k+1} \pmod{p}^{k+2}$. This argument gives us that $1+p$ has order p^{r-1} in $(\mathbb{Z}/p^r\mathbb{Z})^\times$.

For $p = 2$, look at

$$\frac{1+4\mathbb{Z}}{1+2^r\mathbb{Z}}.$$

Then $(1+4)^{2^i} \cong 1 + 2^{i+2} \pmod{2}^{i+3}$. So $1+4$ has order 2^{r-2}. This gives us that $\mathbb{Z}/2^r\mathbb{Z} = \langle -1 \rangle + (1+4\mathbb{Z})/(1+2^r\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{r-2}\mathbb{Z}$. □

1.2 Cyclotomic fields and polynomials

Let ζ_n be a primitive n-th root of 1 in an extension of $\mathbb{Q}$ (e.g. $\zeta_n = 2^{\pi i/n} \in \mathbb{C}$) such that $\zeta_n^{n/m} = \zeta_m$ for all $m \mid n$.

Definition 1.1. $\mathbb{Q}(\zeta_n)$ is the n-th **cyclotomic field** over $\mathbb{Q}$.

Remark 1.1. $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\mu_n)$, where μ_n is the set of n-th roots of unity in $\mathbb{C}$.

Definition 1.2. The n-th **cyclotomic polynomial** Φ_n is the unique monic polynomial in $\mathbb{Q}[x]$ with roots the primitive n-th roots of 1.

Note that

$$\Phi_n = \prod_{\substack{i=1 \\ (i,n)=1}}^{n} (x - \zeta_n^i),$$

$$x^n - 1 = \prod_{\substack{d \mid n \\ d \geq 1}} \Phi_d.$$

So $\Phi_n \in \mathbb{Q}[x]$ by induction. The degree of Φ_n is $\varphi(n) = |\{1 \leq i \leq n : (i,n) = 1\}|$.