Math 210B Lecture 4 Notes

Daniel Raban

January 14, 2019

1 Möbius Inversion, Cyclotomic Polynomials, and Field Embeddings

1.1 Möbius inversion and cyclotomic polynomials

Definition 1.1. The **Möbius function** $\mu : \mathbb{Z}_{\geq 1} \to \{-1, 0, 1\}$ is given by

$$\mu(n) = \begin{cases} (-1)^k & n \text{ is a product of } k \text{ distinct primes} \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 1.1. *For $n \geq 2$,*

$$\sum_{d \mid n} \mu(d) = 0.$$

Proof. First,

$$\sum_{d \mid n} \mu(d) = \sum_{d \mid m} \mu(d),$$

where m is the product of the distinct primes dividing n. Say there are k of them. Then

$$\sum_{d \mid m} \mu(d) = 1 - k + \binom{k}{2} + \cdots + (-1)^k = (1-1)^k = 0. \qquad \square$$

Theorem 1.1 (Möbius inversion formula)**.** *Let A be an abelian group, and let $f : \mathbb{Z}_{\geq 1} \to A$. Define $g : \mathbb{Z}_{\geq 1} \to A$ by $g(n) = \sum_{d \mid n} f(d)$. Then*

$$f(n) = \sum_{d \mid n} \mu(d) g(n/d).$$

Proof. By the lemma,

$$\sum_{d \mid n} \mu(n/d) g(d) = \sum_{d \mid n} \sum_{k \mid d} \mu(n/d) f(k)$$

$$= \sum_{k|n} \sum_{\substack{d|n \\ k|d}} \mu(n/d) f(k)$$

$$= \sum_{k|n} \left(\sum_{c|n/k} \mu((n/k)/c) \right) f(k)$$

$$= f(n).$$

□

Corollary 1.1.

$$\Phi_n = \prod_{d|n} (x^d - 1)^{\mu(n/d)}.$$

Proof. Let $A = \mathbb{Q}(x)^x$, and let f send $d \mapsto \Phi_d$. Then

$$g(n) = \prod_{d\ midn} \Phi_d = x^n - 1.$$

Now apply the Möbius inversion formula. □

Example 1.1. $\Phi_1 = x - 1$, $\Phi_2 = x + 1$,and $\Phi_p = x^{p-1} + x^{p-2} + \cdots + x + 1$, where p is prime. If $p \mid n$, then $\Phi_{pn}(x) = \Phi_n(x^p)$. This also gives us that

$$\Phi_{p^n} = x^{p^{n-1}(p-1)} + \cdots + x^{p^{n-1}} + 1.$$

If $p \neq q$ are primes,

$$\Phi_{pq}(x) = \frac{\Phi_q(x^p)}{\Phi_q(x)}$$

$$\frac{(x^{pq} - 1)(x - 1)}{(x^p - 1)(x^q - 1)} = \frac{\Phi_q(x^p)}{\Phi_q(x)}.$$

$$\Phi_{15} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1.$$

Theorem 1.2. *Φ_n is irreduible in $\mathbb{Q}[x]$.*

Proof. Suppose $\Phi_n = fg$ with f a monic irreducible polynoimal, and let ζ be a root of f. For $p \nmid n$ prime, ζ^p is a root of Φ_n. If ζ^p is a root of g, then $g(x^p)$ has ζ as a root, so $f(x) \mid g(x^p)$. Reduce f and $g \pmod p$. We get $\overline{f}, \overline{g} \in \mathbb{F}_p[x]$. Then $\overline{g}(x^p) = \overline{g}(x)^p$. Then $\overline{f} \mid \overline{g}^p$, but $\overline{f}$ has no multiple roots in $\mathbb{F}_p$, so $\overline{f} \mid \overline{g}$. So Φ_n has multiple roots $\pmod p$¡ which is a contradiction. So ζ^p is a root of f. Therefore, ζ^a is a root of f for all $a \in \mathbb{Z}$ and $\gcd(a, n) = 1$, so $f = \Phi_n$. □

1.2 Field embeddings

Definition 1.2. If $E, E'/F$ and $\varphi : E \to E'$ is an isomorphism, we sat that φ **fixes** F if $\varphi|_F = \mathrm{id}_F$. Elements $\alpha \in E$ and $\beta \in E'$, are **conjugate** over F if there exists an isomorphism $\varphi : F(\alpha) \to F(\beta)$ fixing F with $\varphi(\alpha) = \beta$.

Proposition 1.1. *Let $E, E'/F$. Elements $\alpha \in E$, $\beta \in E'$ are conjugate over F if and only if they have equal minimal polynomials in $F[x]$.*

Proof. Let α, β be conjugate over F. Then $\varphi(g(\alpha)) = g(\beta)$ for all $g \in F[x]$. Then α, β have the same minimal polynomial (α is a root of $g(x)$ iff β is a root of $g(x)$).

If α, β haeve the same minimal polynomial $f \in F[x]$, then $F[x]/(f) \cong F(\alpha)$ via $x\ mapsto\alpha$ and $F[x]/(f) \cong F(\beta)$ via $x\ mapsto\beta$. □

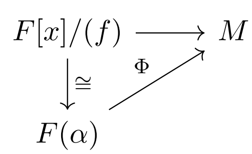
Example 1.2. The roots of $x^2 + 1$a re ± 1. There exists a field automorphism $\mathbb{C} \to \mathbb{C}$ $i \mapsto -i$ fixing $\mathbb{R}$, namely, complex conjugation.

Definition 1.3. A **field embedding** is a ring homomorphism of fields (necessarily injective). If $\varphi : F \to M$ is an embedding and E/F is an extension, then $\Phi : E \to M$ **extends** φ if $\Phi|_F = \varphi$.

Example 1.3. Let $\iota : \mathbb{Q} \to \mathbb{R}$ be the natural inclusion map. There are two field embeddings extending ι; these are $\mathbb{Q}(\sqrt{2} \to \mathbb{R}$ sending $\sqrt{2} \mapsto \sqrt{2}$. There are no extensions to $\mathbb{Q}(i) \to \mathbb{R}$.

Theorem 1.3. *Let E/F be an extension, and let $\alpha \in E$ be algebraic over F. Let $\varphi : F\ toM$ be an embedding, and let $\tilde{\varphi} : F[x] \to M[x]$ be the induced map. Let f be the minimal polynomial of α. Then the extensions $\Phi : F(\alpha) \to M$ of φ are in 1-1 correspondence with the roots of $\tilde{\varphi}(f)$ in M via $\Phi \mapsto \Phi(\alpha)$.*

Proof. If $\tilde{p}(f)$ has a root β in M, let ev_β be evaluation at β. Consider $e_\beta \circ \tilde{\varphi} : F[x] \to M$. Then $\ker(e_\beta \circ \tilde{\varphi}_{\supseteq}(f)$. Since we are working in a PID, this is equality. We get



where $\Phi(\alpha) = \beta$.

If $\Phi : F(\alpha) \to M$ extends φ, then write $f = \sum_{i=0}^n c_i x^i$, where $n = \deg(f)$. Then

$$\tilde{\varphi}(f)(\Phi(\alpha)) = \sum_{i=0}^n \varphi(c_i)\Phi(\alpha)^i = \Phi(\sum_{i=0}^n c_i \alpha^i) = \Phi(f(\alpha)) = 0.$$ □

Corollary 1.2. *Let E/F be finite, and let $\varphi : F \to M$ be a field embedding. The number of extensions of φ to $E \to M$ is $\leq [E : F]$.*

Proof. Induct on the degree. If $E = F(\alpha)$, then the number of roots of $\mathrm{irr}_F(\alpha)$ in M is $\leq [F(\alpha) : F]$. Then the number of extensions is $\leq [F(\alpha) : F]$ by the theorem. Consider extensions of these; the number for each is $\leq [E : f(\alpha)]$ by induction. So the number is $\leq [E : F]$. $\square$

Example 1.4. We can extend $\iota : \mathbb{Q} \to \mathbb{R}$ to $\varphi : \mathbb{Q}(\sqrt{2}, \sqrt{3}) \to \mathbb{R}$ in 4 ways. However, there is only one way to embed $\mathbb{Q}(\sqrt[3]{2}) \to \mathbb{R}$ because $x^3 - 2 = (x - \sqrt[3]{2}) \cdot (\deg(2))$ in $\mathbb{R}[x]$.

Proposition 1.2. *Let E/F be algebraic, and let $\sigma : E \to E$ be an embedding fixing F. Then σ is an isomorphism.*

Proof. For any $\beta \in E$, let f be its minimal polynomial. The restriction to the finite set of roots $\sigma : \{\text{roots of } f \text{ in } E\} \to \{\text{roots of } f \text{ in } E\}$ is a bijection (as it is injective). So $\beta \in \mathrm{im}(\sigma)$. $\square$