MATH200C, LECTURE 4

GOLSEFIDY

Cyclotomic polynomials

In the previous lecture we proved that

$$\theta : \mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times, \theta(\sigma) := a_\sigma + n\mathbb{Z},$$

where $\theta(\zeta_n) = \zeta_n^{a_\sigma}$ is an injective group homomorphism. And in order to show it is an isomorphism, we defined the n-th cyclotomic polynomial:

$$\Phi_n(x) := \prod_{1\le a\le n, \gcd(a,n)=1} (x - \zeta_n^a) \in \mathbb{C}[x].$$

Lemma 1.

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

Proof.

$$\begin{aligned} x^n - 1 &= \prod_{i=0}^{n-1} (x - \zeta_n^i) \\ &= \prod_{d|n} \prod_{\gcd(i,n)=d, 0\le i\le n} (x - \zeta_n^i) \\ &= \prod_{d|n} \prod_{0\le j\le n/d, \gcd(j,n/d)=1} (x - \zeta_n^{dj}) \\ &= \prod_{d|n} \prod_{0\le j\le n/d, \gcd(j,n/d)=1} (x - \zeta_{n/d}^{j}) \\ &= \prod_{d|n} \Phi_{n/d}(x). \end{aligned}$$

□

Lemma 2. $\Phi_n(x) \in \mathbb{Z}[x]$.

Proof. We proceed by strong induction on n. We have that $\Phi_1(x) = x - 1 \in \mathbb{Z}[x]$, which gives us the base of induction. By the previous lemma, we have that

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n, d \neq n} \Phi_d(x)}.$$

Therefore by the strong induction hypothesis, $\Phi_n(x)$ is the quotient of a long division of two monic integer polynomials; and so $\Phi_n(x) \in \mathbb{Z}[x]$. □

Theorem 3. *$\Phi_n(x)$ is irreducible in $\mathbb{Q}[x]$.*

Proof. We assume to the contrary that $\Phi_n(x)$ is reducible in $\mathbb{Q}[x]$. Since $\Phi_n(x)$ is monic integer polynomial, we deduce that there are integer polynomials $f(x), g(x) \in \mathbb{Z}[x]$ such that $\deg f, \deg g > 0$ and $\Phi_n(x) = f(x)g(x)$. Since ζ_n is a zero of $\Phi_n(x)$, it should be a zero of $f(x)$ or $g(x)$. W.L.O.G. we can and will assume that $f(\zeta_n) = 0$.

Claim. Suppose p is prime and $p \nmid n$. Then if $f(\zeta) = 0$, then $f(\zeta^p) = 0$.

Proof of Claim. Suppose to the contrary that $f(\zeta^p) \neq 0$. Since ζ is a zero of $f(x)$, it is a zero of $\Phi_n(x)$; hence $o(\zeta) = n$. As $p \nmid n$, $o(\zeta^p) = n$; and so $\Phi_n(\zeta^p) = 0$; and so $g(\zeta^p) = 0$. Hence

$$m_{\zeta,\mathbb{Q}}(x)|f(x), \text{ and } m_{\zeta,\mathbb{Q}}(x)|g(x^p).$$

Since $f(x)$ and $g(x^p)$ are monic integer polynomials, using Euclid's algorithm we can deduce that $h(x) := \gcd(f(x), g(x^p))$ is a monic integer polynomial. Since $m_{\zeta,\mathbb{Q}}(x)|h(x)$, we have that $\deg h > 0$. Thus there are polynomials $r, s \in \mathbb{Z}[x]$ such that

$$f(x) = h(x)r(x), \text{ and } g(x^p) = h(x)s(x).$$

Let's view both sides modulo p. So we get

$$\overline{f}(x) = \overline{h}(x)\overline{r}(x), \text{ and } \overline{g}(x)^p = \overline{h}(x)\overline{s}(x).$$

This implies that $\gcd(\overline{f}, \overline{g}) \neq 1$; and so $\overline{f}(x)\overline{g}(x)$ has multiple zeros in $\overline{\mathbb{F}}_p$. So $\Phi_n(x) \pmod{p}$ should have multiple zeros in $\overline{\mathbb{F}}_p$. But $\Phi_n(x)$ divides $x^n - 1$ and $x^n - 1$ does not have multiple zeros in $\overline{\mathbb{F}}_p$ as $\gcd(x^n - 1, nx^{n-1}) = 1$ (we have this as $p \nmid n$), which gives us a contradiction. □

Claim. $f(\zeta_n^a) = 0$ if $\gcd(a, n) = 1$.

Proof of Claim. One can easily deduce this by induction on the number of prime factors of a and using the previous Claim. □

The above claim implies that $\deg f = \phi(n) = \deg \Phi_n$; and so $\deg g = 0$, which is a contradiction. □

Overall we get

Theorem 4. *$\mathbb{Q}[\zeta_n]/\mathbb{Q}$ is a Galois extension, and*

$$\theta : \mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times, \theta(\sigma) := a_\sigma + n\mathbb{Z}$$

where $\sigma(\zeta_n) = \zeta_n^{a_\sigma}$ is a group isomorphism.

Proof. We have already proved that θ is an injective group homomorphism. By the previous Theorem we have $m_{\zeta_n,\mathbb{Q}}(x) = \Phi_n(x)$; and so

$$|\mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q})| = [\mathbb{Q}[\zeta_n] : \mathbb{Q}] = \deg m_{\zeta_n,\mathbb{Q}}(x) = \deg \Phi_n(x) = \phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|.$$

This implies that θ is onto; and claim follows. □

Solvability by radicals

Long ago we mentioned that a lot of algebra had been developed to find zeros of polynomials. For a given polynomial $f(x) \in F[x]$, people tried to find its zeros using $+, -, \times, /$, and $\sqrt[n]{\cdot}$. In modern language we say $f(x)$ is solvable by radicals over F if there is a chain of fields

$$F =: F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$$

such that $F_{k+1} = F_k[\sqrt[m_k]{a_k}]$ for some $a_k \in F_k$ and F_n has a zero of $f(x)$. Suppose the characteristic of F is zero and F' is the normal closure of F_n over F. Then by a result that you have proved in your HW assignment we have that $\mathrm{Gal}(F'/F)$ is solvable. This is proved by Galois; he proved the converse of this statement as well and these were his main motivations to work on field theory.

Theorem 5. *Suppose $\mathrm{char}(F) = 0$, $f(x) \in F[x]$ is irreducible, and E is a splitting field of $f(x)$ over F; then $f(x)$ is solvable by radicals over F if and only if $\mathrm{Gal}(E/F)$ is solvable.*

For the remaining part of this lecture we focus on proving the "if" part of this Theorem. The following is an important result that has many applications.

Proposition 6 (Independence of characters)**.** *Suppose G is a group, F is a field, and $\chi_1, \ldots, \chi_n : G \to F^\times$ are distinct group homomorphisms. Then χ_i's are F-linearly independent; that means $\sum_{i=1}^n c_i\chi_i = 0$ for some $c_i \in F$ implies that $c_i = 0$ for any i.*

(A group homomorphism $\chi : G \to F^\times$ is called a character of G.)

Proof of Proposition 6. Suppose χ_i's are linearly dependent and take a non-trivial linear relation with smallest number of non-zero coefficients. After relabelling, if necessary, we can and will assume that

$$c_1\chi_1 + \cdots + c_m\chi_m = 0 \tag{1}$$

and $c_i \neq 0$ for any i. Since $\chi_1 \neq \chi_2$ (notice that m cannot be 1), there is $g_0 \in G$ such that $\chi_1(g_0) \neq \chi_2(g_0)$. By (1), for any $g \in G$, we have

$$\begin{cases} c_1\chi_1(g) + \cdots + c_m\chi_m(g) = 0 & \times\chi_1(g_0) \\ c_1 \underbrace{\chi_1(g_0g)}_{\chi_1(g_0)\chi_1(g)} + \cdots + c_m \underbrace{\chi_m(g_0g)}_{\chi_m(g_0)\chi_m(g)} = 0 & \end{cases}$$

which implies

$$c_1(\chi_1(g_0)\chi_1(g) - \chi_1(g_0)\chi_1(g)) + \cdots + c_m(\chi_1(g_0)\chi_m(g) - \chi_m(g_0)\chi_m(g)) = 0.$$

Therefore

$$c_2(\chi_1(g_0) - \chi_2(g_0))\chi_2 + \cdots + c_m(\chi_1(g_0) - \chi_m(g_0))\chi_m = 0,$$

which means we have found a non-trivial linear relation with smaller number of non-zero coefficients; and this is a contradiction. $\square$

Theorem 7 (Hilbert's Theorem 90)**.** *Suppose E/F is a finite Galois extension and $\mathrm{Gal}(E/F) = \langle\sigma\rangle$. Let $N_{E/F}(\alpha) := \prod_{\tau\in\mathrm{Gal}(E/F)} \tau(\alpha)$. Then*

$$N_{E/F}(\alpha) = 1 \Leftrightarrow \exists\beta \in E, \alpha = \frac{\sigma(\beta)}{\beta}.$$

Proof. ($\Leftarrow$) is true for any finite Galois extension:

$$N_{E/F}(\alpha) = \prod_{\tau\in\mathrm{Gal}(E/F)} \tau\left(\frac{\sigma(\beta)}{\beta}\right) = \frac{\prod_{\tau\in\mathrm{Gal}(E/F)}(\tau\circ\sigma)(\beta)}{\prod_{\tau\in\mathrm{Gal}(E/F)}\tau(\beta)} = 1.$$

($\Rightarrow$) Let $T_\alpha : E \to E, T_\alpha(a) := \alpha\sigma(a)$. Since $\sigma \in \mathrm{Gal}(E/F)$, T_α is an F-linear map. We want to find the minimal polynomial of T_α; so we start with computing T_α^k. Notice that

$$T_\alpha^2(a) = T_\alpha(T_\alpha(a)) = T_\alpha(\alpha\sigma(a)) = \alpha\sigma(\alpha\sigma(a)) = (\alpha\sigma(\alpha))\sigma^2(a).$$

Following the same idea, we can prove by induction on k that

$$T_\alpha^k(a) = \underbrace{(\alpha\sigma(\alpha)\cdots\sigma^{k-1}(\alpha))}_{\alpha_k}\sigma^k(a). \tag{2}$$

In particular, we have $T_\alpha^n(a) = N_{E/F}(\alpha)a$ where $n = [E : F]$. Hence T_α satisfies $x^n - N_{E/F}(\alpha)$. Notice that, for any $\tau \in \mathrm{Gal}(E/F)$,

$$\tau(N_{E/F}(\alpha)) = \prod_{\sigma\in\mathrm{Gal}(E/F)} (\tau\circ\sigma)(\alpha) = \prod_{\sigma\in\mathrm{Gal}(E/F)} \sigma(\alpha) = N_{E/F}(\alpha);$$

and so $N_{E/F}(\alpha) \in \mathrm{Fix}(\mathrm{Gal}(E/F)) = F$. Therefore T_α satisfies $x^n - N_{E/F}(\alpha) \in F[x]$.

Claim. The minimal polynomial of T_α is $x^n - N_{E/F}(\alpha)$ if $\alpha \neq 0$.

Proof of Claim. Since T_α satisfies this polynomial, it is enough to show that it does not satisfy a smaller degree polynomial in $F[x]$; and this is equivalent to saying that $I, T_\alpha, \ldots, T_\alpha^{n-1}$ are F-linearly independent. Notice by (2) $T_\alpha^k(a) = \alpha_k\sigma^k$. So if $\sum_{i=0}^{n-1} f_i T_\alpha^i = 0$, then $\sum_{i=0}^{n-1} \underbrace{(f_i\alpha_i)}_{\in E}\sigma^i = 0$. Since $I, \sigma, \ldots, \sigma^{n-1} : E^\times \to E^\times$ are distinct group homomorphisms, by the previous lemma they are E-linearly independent. Hence $f_i\alpha_i = 0$, which implies $f_i = 0$ as $\alpha_i \neq 0$ (since $\alpha \neq 0$, we have $\alpha_i \neq 0$); and claim follows.

If $N_{E/F}(\alpha) = 1$, then the minimal polynomial of T_α is $x^n - 1$; hence it has eigenvalue 1. Therefore there is $\beta' \in E$ such that $T_\alpha(\beta') = \beta'$; this means

$$\alpha\sigma(\beta') = \beta'.$$

Thus for $\beta := \beta'^{-1}$ we have $\alpha = \sigma(\beta)/\beta$. □

The next lemma gives us the connection between Hilbert's theorem 90 and Galois's theorem.

Proposition 8. *Suppose* $\mu_n := \{\zeta \in F \mid \zeta^n = 1\}$ *has* n *distinct elements,* $\mathrm{Gal}(E/F) \simeq \mathbb{Z}/n\mathbb{Z}$. *Then there is* $a \in F$ *such that* $E = F[\sqrt[n]{a}]$.

Proof. As we have mentioned earlier μ_n is a cyclic group of order n. Suppose $\mu_n = \langle \zeta_n \rangle$. Then $N_{E/F}(\zeta_n) = \zeta_n^n = 1$. Hence by Hilbert's Theorem 90, there is $\beta \in E$ such that $\zeta_n = \frac{\sigma(\beta)}{\beta}$; this means $\sigma(\beta) = \zeta_n \beta$. we will continue next time. □