Lecture 30: Cyclotomic polynomials

Monday, March 12, 2018 11:08 AM

In the previous lecture we proved that the splitting field $E \subseteq \mathbb{C}$ of x^n-1 over $\mathbb{Q}$ is $\mathbb{Q}[\zeta_n]$ where $\zeta_n = e^{\frac{2\pi i}{n}}$. We showed

$$\mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q}) \xrightarrow{\theta} (\mathbb{Z}/n\mathbb{Z})^{\times}, \quad \sigma \longmapsto i_\sigma \text{ where } \sigma(\zeta_n) = \zeta_n^{i_\sigma}$$

is an injective group homomorphism.

To show this is an isomorphism, we defined $\Phi_n(x) := \prod_{\substack{0<j<n \\ \gcd(j,n)=1}} (x-\zeta_n^j)$ (the n^{th} cyclotomic polynomial). We mentioned it is enough to prove $\Phi_n(x) \in \mathbb{Q}[x]$ and $\Phi_n(x)$ is irreducible to be able to deduce θ is an isomorphism.

Next we proved $\prod_{d|n} \Phi_d(x) = x^n-1$. And we were in the middle of proof of the following lemma:

<u>Lemma</u>. $\Phi_n(x) \in \mathbb{Z}[x]$.

<u>Pf.</u> We proceed by induction on n. $\Phi_1(x) = x-1 \in \mathbb{Z}[x]$. By strong induction hypothesis and the previous lemma, $\Phi_n(x)$ is the quotient of x^n-1 divided by $\prod_{\substack{d|n \\ d\neq n}} \Phi_d(x)$ and $\prod_{\substack{d|n \\ d\neq n}} \Phi_d(x)$ is a monic polynomial in $\mathbb{Z}[x]$. Hence $\Phi_n(x) \in \mathbb{Z}[x]$. ■

Lecture 30: Cyclotomic polynomials

Sunday, March 11, 2018 1:36 PM

<u>Theorem</u>. $\Phi_n(x)$ is irreducible in $\mathbb{Q}[x]$.

<u>Pf</u>. Suppose not. Since $\Phi_n(x) \in \mathbb{Z}[x]$, by Gauss's lemma

$\exists\, f, g \in \mathbb{Z}[x]$ s.t. $\deg f, \deg g \geq 1$ and $\Phi_n(x) = f(x)g(x)$.

<u>Claim</u>. If $f(\zeta) = 0$ and $p \nmid n$ is a prime, then $f(\zeta^p) = 0$.

<u>Pf of claim</u>. $f(\zeta) = 0 \Rightarrow \Phi_n(\zeta) = 0 \Rightarrow o(\zeta) = n$

$$\Rightarrow o(\zeta^p) = \frac{n}{\gcd(n,p)} = n \Rightarrow \Phi_n(\zeta^p) = 0.$$

So, if $f(\zeta^p) \neq 0$, then $g(\zeta^p) = 0$. Hence

$$m_{\zeta,\mathbb{Q}}(x) \mid f(x) \quad \text{and} \quad m_{\zeta,\mathbb{Q}}(x) \mid g(x^p). \qquad (*)$$

Since f and g are monic polynomials in $\mathbb{Z}[x]$, by means of Euclid's algorithm $\gcd(f(x), g(x^p))$ is monic and in $\mathbb{Z}[x]$. And so, by $(*)$,

$\exists\, h(x) \in \mathbb{Z}[x]$, monic, $\deg h \geq 1$ and $h(x) \mid f(x)$, $h(x) \mid g(x^p)$.

Therefore $\bar{h}(x)$ divides $\bar{f}(x)$ and $\bar{g}(x^p)$ where $\bar{h} = h \pmod p$
$(\dagger)$

$\bar{f} = f \pmod p$, and $\bar{g} = g \pmod p$. But in $\mathbb{F}_p[x]$, $\bar{g}(x^p) = \bar{g}(x)^p$,

and $\bar{f}(x)\bar{g}(x) = x^n - 1$.

<u>SubClaim</u>. $x^n - 1$ does not have multiple zeros in $\overline{\mathbb{F}_p}$ if $p \nmid n$.

Pf of Subclaim. Its derivative is $n x^{n-1}$ and $\gcd(n x^{n-1}, x^n-1)=1$.

SubClaim. $\gcd(\bar{f}(x), \bar{g}(x))=1$.

Pf of Subclaim. Otherwise $\bar{f}(x)\bar{g}(x)=x^n-1$ has multiple zeros in $\overline{\mathbb{F}}_p$.

Since $\gcd(\bar{f},\bar{g})=1$, we deduce $\gcd(\bar{f}(x),\bar{g}(x^p))=1$;

which contradicts (†) that asserts $\exists\, \bar{h}$, $\deg \bar{h}\geq 1$, $\bar{h}\mid\bar{f}$ and $\bar{h}(x)\mid\bar{g}(x^p)$. ∎

Claim. If $f(\zeta)=0$ and $\gcd(a,n)=1$, then $f(\zeta^a)=1$.

Pf. Write $a=\prod_{i=1}^{m} p_i$ as product of not necessarily distinct primes.

We prove the claim by induction on m. Base of induction is proved in the previous Claim. By induction hypothesis, we have

$f(\zeta^{\prod_{i=1}^{m-1} p_i})=0$. So again by the previous claim we get

$f((\zeta^{\prod_{i=1}^{m-1} p_i})^{p_m})=0$, which means $f(\zeta^a)=0$. ∎

Hence $f(x)=\prod_{a\in(\mathbb{Z}/n\mathbb{Z})^\times}(x-\zeta^a) \Rightarrow \deg f=\deg\Phi_n \Rightarrow \deg g=0$ ⁂ ∎

($\mathbb{Q}[\zeta_n]$ is called a cyclotomic field.)

So overall we get:

Lecture 30: Cyclotomic fields; solvability of polynomials

Sunday, March 11, 2018 2:12 PM

<u>Theorem</u>. Let $\zeta_n = e^{\frac{2\pi i}{n}}$. Then

(1) $m_{\zeta_n,\mathbb{Q}}(x) = \Phi_n(x) \in \mathbb{Z}[x]$. In particular, $\deg m_{\zeta_n,\mathbb{Q}}(x) = \varphi(n)$.

(2) $\mathbb{Q}[\zeta_n]/\mathbb{Q}$ is Galois; and $\mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times$,

$$\sigma \longmapsto i_\sigma + n\mathbb{Z},$$

if $\sigma(\zeta_n) = \zeta_n^{i_\sigma}$.

Let F be a field that contains all the zeros of x^n-1, where either $\mathrm{char}(F)=0$ or $\gcd(\underbrace{\mathrm{char}(F)}_{p},n)=1$. So in either case x^n-1 has n distinct zeros $1,\zeta,\zeta^2,\dots,\zeta^{n-1}$.

Suppose $a\in F^\times\setminus(F^\times)^n$. We would like to study the splitting field E of x^n-a.

Let's denote one of its zeros by $\sqrt[n]{a}$. Then

$$x^n-a = a\left(\left(\frac{x}{\sqrt[n]{a}}\right)^n-1\right) = a\left(\frac{x}{\sqrt[n]{a}}-1\right)\left(\frac{x}{\sqrt[n]{a}}-\zeta\right)\cdots\left(\frac{x}{\sqrt[n]{a}}-\zeta^{n-1}\right)$$

$$= (x-\sqrt[n]{a})(x-\zeta\sqrt[n]{a})\cdots(x-\zeta^{n-1}\sqrt[n]{a}).$$

And so $E = F[\sqrt[n]{a},\zeta\sqrt[n]{a},\dots,\zeta^{n-1}\sqrt[n]{a}] = F[\sqrt[n]{a}]$

$\boxed{\zeta^i\in F}$

Lecture 30: Solvability of polynomials

Sunday, March 11, 2018 2:18 PM

and $x^n - a$ does not have multiple zeros. Hence E/F is Galois.

For any $\sigma \in Gal(E/F)$, $\sigma(\sqrt[n]{a})$ is a zero of $x^n - a$. Hence

$\exists\, i_\sigma \in \mathbb{Z}/n\mathbb{Z}$ s.t. $\sigma(\sqrt[n]{a}) = \zeta^{i_\sigma} \sqrt[n]{a}$.

<u>Claim</u>. $Gal(E/F) \xrightarrow{\theta} \mathbb{Z}/n\mathbb{Z}$, is an injective group homomorphism.

$\sigma \longmapsto i_\sigma$

<u>Pf</u>. Since $E = F[\sqrt[n]{a}]$, $\sigma(\sqrt[n]{a})$ uniquely determines σ; and so θ is injective.

$$\sigma_1 \circ \sigma_2(\sqrt[n]{a}) = \sigma_1(\zeta^{i_{\sigma_2}} \sqrt[n]{a}) = \zeta^{i_{\sigma_2}} \sigma_1(\sqrt[n]{a}) = \zeta^{i_{\sigma_2}} \cdot \zeta^{i_{\sigma_1}} \sqrt[n]{a}$$
$$= \zeta^{i_{\sigma_1} + i_{\sigma_2}} \sqrt[n]{a}.$$

Hence $i_{\sigma_1 \circ \sigma_2} \equiv i_{\sigma_1} + i_{\sigma_2} \pmod{n}$. ■

<u>Corollary</u>. $Gal(F[\sqrt[n]{a}]/F) \hookrightarrow \mathbb{Z}/n\mathbb{Z}$ and so it is cyclic if $\mathrm{char}(F) \nmid n$ and n^{th} roots of unity are in F.

<u>Def</u>. We say a polynomial $f(x) \in F[x]$ is <u>solvable in radicals</u> if $\exists\ F =: F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_m$ s.t. $\forall i$, $F_{i+1} = F_i[\alpha_{i+1}]$ and $\alpha_{i+1}^{m_{i+1}} \in F_i$ for some $m_{i+1} \in \mathbb{Z}^+$.

Lecture 30: Solvability of poly's implies solvability of gps

Monday, March 12, 2018 8:50 AM

<u>Theorem</u>. Suppose $\mathrm{char}(F)=0$, $f(x)\in F[x]$, $\overline{F}$ is an algebraic closure of F, and $E\subseteq\overline{F}$ is a splitting field of $f(x)$ over F. Then, if $f(x)$ is solvable in radicals, then $\mathrm{Gal}(E/F)$ is solvable.

<u>Pf</u>. Suppose $f(x)$ is solvable in radicals. Then $\exists$

$$F_0\subseteq F_1\subseteq \cdots\subseteq F_m \text{ s.t. } F_{i+1}=F_i[\alpha_{i+1}] \text{ where } \alpha_{i+1}^{k_{i+1}}\in F_i.$$

Let $E_0\subseteq\overline{F}$ be a splitting field of $x^{\prod_{i=1}^m k_i}-1$ over F_0;

$E_{i+1}\subseteq\overline{F}$ be a splitting field of $x^{k_{i+1}}-\alpha_{i+1}^{k_{i+1}}$ over E_i;

hence by induction $F_i\subseteq E_i$; and so $E\subseteq E_m$.

- $\mathrm{Gal}(E_0/F_0)\hookrightarrow(\mathbb{Z}/n\mathbb{Z})^\times$ where $n=\prod_{i=1}^m k_i$

  (Similar to the first part of proof of $\mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q})\simeq(\mathbb{Z}/n\mathbb{Z})^\times$.)

- $\mathrm{Gal}(E_{i+1}/E_i)\hookrightarrow\mathbb{Z}/k_{i+1}\mathbb{Z}$.

$$\Rightarrow \quad 1\lhd \mathrm{Gal}(E_m/E_{m-1})\lhd\cdots\lhd\mathrm{Gal}(E_m/E_0)\lhd\mathrm{Gal}(E_m/F)$$

is a normal series of $\mathrm{Gal}(E_m/F)$; and all the factors are abelian:

$$\mathrm{Gal}(E_m/E_i)\,/\,\mathrm{Gal}(E_m/E_{i+1})\simeq\mathrm{Gal}(E_{i+1}/E_i).$$ Therefore

$\mathrm{Gal}(E_m/F)$ is solvable. Since $F\subseteq E\subseteq E_m$ and E/F is Galois,

Lecture 30: Dirichlet's independence of char

Monday, March 12, 2018 11:38 PM

$$\left.\begin{array}{l} \mathrm{Gal}(E/F) \simeq \mathrm{Gal}(E_m/F)/\mathrm{Gal}(E_m/E) \\ \mathrm{Gal}(E_m/F) \text{ is solvable} \end{array}\right\} \Rightarrow \mathrm{Gal}(E/F) \text{ is solvable.}$$

■

Converse of the above theorem is true as well. The following is nice result which is useful in other places as well.

<u>Proposition</u>. Let G be a group and $\chi_1, \dots, \chi_n : G \to E^\times$ are distinct group homomorphisms where E is a field. Then χ_i's are E-linearly independent; that means

$$\sum_{i=1}^{n} c_i \chi_i(g) = 0 \quad (\forall g \in G) \quad \Rightarrow \quad c_1 = \dots = c_n = 0.$$

<u>Pf</u>. Suppose $\exists\, \vec{c} \neq 0$ s.t. $\sum_{i=1}^{n} c_i \chi_i = 0$; and among all such $\vec{c}$'s take a solution with smallest possible non-zero terms. After reindexing, assume $c_1\chi_1 + \dots + c_m\chi_m = 0$ and $c_i \neq 0$.

After multiplying by c_1^{-1}, we have $\chi_1 + c_2'\chi_2 + \dots + c_m'\chi_m = 0$.

$\forall g_0 \in G$, $\chi_1(g_0)\chi_1(g) + c_2'\chi_2(g_0)\chi_2(g) + \dots + c_m'\chi_m(g_0)\chi_m(g) = 0$.

Hence $\underbrace{c_2'(\chi_1(g_0) - \chi_2(g_0))}\chi_2 + \dots + \underbrace{c_m'(\chi_1(g_0) - \chi_m(g_0))}\chi_m(g) = 0$

at most $m-1$ non-zero coeff. $\Rightarrow$ all should be zero by minimality of

Lecture 30: Hilbert's theorem 90

Monday, March 12, 2018 11:55 PM

we get $\chi_0(g_0)=\chi_1(g_0)=\cdots=\chi_m(g_0)$. Since g_0 is arbitrary, we deduce

$\chi_0=\cdots=\chi_m$ which is a contradiction. ∎

<u>Theorem.</u> (Hilbert's theorem 90)

Suppose E/F is a finite Galois extension; and $\mathrm{Gal}(E/F)=\langle\sigma\rangle$

is cyclic. Then $N_{E/F}(\alpha)=1 \iff \alpha=\sigma(\beta)/\beta$ for some $\beta\in E^\times$

where $N_{E/F}(\alpha)=\prod_{i=0}^{m-1}\sigma^i(\alpha)$ and $[E:F]=m$.

- We will prove this in the next lecture.

- Notice that $\forall\sigma\in\mathrm{Gal}(E/F)$,

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

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

$$\Rightarrow N_{E/F}(\alpha)\in\mathrm{Fix}(\mathrm{Gal}(E/F))=F.$$