Lecture 29: Galois group of finite fields

Sunday, March 11, 2018 10:56 AM

Let $\overline{\mathbb{F}_p}$ be an algebraic closure of $\mathbb{F}_p$. We have seen that for any positive integer n, there is a unique subfield of $\overline{\mathbb{F}_p}$ that has order p^n and it is denoted by $\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^n} = \{\alpha \in \overline{\mathbb{F}_p} \mid \alpha^{p^n} = \alpha\}$.

$\mathbb{F}_{p^n}$ is a splitting field of $x^{p^n} - x$; and $x^{p^n} - x$ does not have multiple zeros. Hence $\mathbb{F}_{p^n}/\mathbb{F}_p$ is a Galois extension.

Let $\sigma_p : \overline{\mathbb{F}_p} \to \overline{\mathbb{F}_p}$, $\sigma_p(\alpha) := \alpha^p$. We have seen that σ_p is a field embedding.

<u>Claim</u>. $\sigma_p(\overline{\mathbb{F}_p}) = \overline{\mathbb{F}_p}$.

<u>Pf</u>. $\alpha \in \overline{\mathbb{F}_p} \Rightarrow x^p - \alpha$ has a zero in $\overline{\mathbb{F}_p}$ as $\overline{\mathbb{F}_p}$ is algebraically closed. Say $\beta^p - \alpha = 0$. So $\sigma_p(\beta) = \alpha$. And we have already pointed out that it is an embedding.

So $\sigma_p \in \mathrm{Aut}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$; since $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois, $\sigma_p|_{\mathbb{F}_{p^n}} \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$.

Let $\sigma_{p,n} := \sigma_p|_{\mathbb{F}_{p^n}}$. Suppose $d = |\langle \sigma_{p,n} \rangle|$. Then

$\forall \alpha \in \mathbb{F}_{p^n}$, $\sigma_{p,n}^d(\alpha) = \alpha \Rightarrow \alpha^{p^d} - \alpha = 0 \Rightarrow \mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^d}$.

$\Rightarrow n \mid d$. On the other hand, $\sigma_{p,n}^n(\alpha) = \alpha^{p^n} = \alpha$ $\forall \alpha \in \mathbb{F}_{p^n}$. And

Lecture 29: Absolute Galois group of F_p

Sunday, March 11, 2018 11:14 AM

So $|\langle \sigma_{p,n}\rangle| \,\big|\, n$. Hence $|\langle\sigma_{p,n}\rangle| = n = [\mathbb{F}_{p^n}:\mathbb{F}_p] = |\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)|$.

Therefore $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \sigma_{p,n}\rangle \simeq \mathbb{Z}/n\mathbb{Z}$.

Since $\overline{\mathbb{F}}_p = \bigcup_{\substack{E/\mathbb{F}_p \\ \text{finite norma}}} E$, we get $\overline{\mathbb{F}}_p = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$; and as we proved earlier: $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \simeq \varprojlim \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$.

Notice that

$$\begin{tikzcd} \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \arrow[r, two heads] \arrow[d, "\wr"] \arrow[dr, phantom, "\circlearrowleft"] & \mathrm{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p) \arrow[d, "\wr"] \\ \mathbb{Z}/n\mathbb{Z} \arrow[r, two heads] & \mathbb{Z}/m\mathbb{Z} \end{tikzcd} \qquad \text{if } m \mid n$$

$$\begin{tikzcd} \sigma_{p,n} \arrow[r, mapsto] \arrow[d, mapsto] & \sigma_{p,m} \arrow[d, mapsto] \\ 1+n\mathbb{Z} \arrow[r, mapsto] & 1+m\mathbb{Z} \end{tikzcd}$$

And so $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \simeq \varprojlim \mathbb{Z}/n\mathbb{Z} := \{ (a_k)_{k=1}^{\infty} \in \prod (\mathbb{Z}/k\mathbb{Z}) \mid m|n,\ a_n \equiv a_m \pmod{m} \}$.

(This is called the profinite closure of $\mathbb{Z}$, and it is denoted by $\hat{\mathbb{Z}}$.).

- Next we will study a splitting field $E \subseteq \mathbb{C}$ of x^n-1 over $\mathbb{Q}$.

Let $\zeta_n := e^{\frac{2\pi i}{n}}$. Then $x^n - 1 = (x-1)(x-\zeta_n)\cdots(x-\zeta_n^{n-1})$.

So $E = \mathbb{Q}[1,\zeta_n,\zeta_n^2,\ldots,\zeta_n^{n-1}] = \mathbb{Q}[\zeta_n]$. Since $\mathrm{char}(\mathbb{Q})=0$, $\mathbb{Q}[\zeta_n]/\mathbb{Q}$ is a Galois extension. For any $\sigma \in \mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q})$, $\sigma(\zeta_n)$ is a zero of x^n-1. Hence $\sigma(\zeta_n) = \zeta_n^i$ for some $0 \le i < n$.

Lecture 29: Cyclotomic fields

Sunday, March 11, 2018 11:31 AM

Since the multiplicative order $o(\zeta_n)$ is the same as $o(\sigma(\zeta_n))$,

and $o(\zeta_n^i) = \frac{i}{\gcd(i,n)}$; we deduce that $\gcd(i,n)=1$.

So we get a map $\mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q}) \xrightarrow{\theta} (\mathbb{Z}/n\mathbb{Z})^\times$,

$$\sigma \longmapsto i_\sigma$$

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

Claim. θ is a group homomorphism; and θ is an embedding.

Pf. • $\forall\, \sigma_1, \sigma_2 \in \mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q})$,

$$\sigma_1 \circ \sigma_2(\zeta_n) = \sigma_1(\zeta_n^{i_{\sigma_2}}) = \sigma_1(\zeta_n)^{i_{\sigma_2}} = (\zeta_n^{i_{\sigma_1}})^{i_{\sigma_2}} = \zeta_n^{i_{\sigma_1} \cdot i_{\sigma_2}}.$$

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

• Since $\sigma(\zeta_n)$ uniquely determines σ, θ is an embedding. ∎

We would like to prove θ is an isomorphism.

A different proof was presented during lecture

Proposition. Suppose $F[\alpha]/F$ is a Galois extension. Then

$$m_{\alpha,F}(x) = \prod_{\sigma \in \mathrm{Gal}(F[\alpha]/F)} (x - \sigma(\alpha)).$$

① Pf $\forall\, \sigma \in \mathrm{Gal}(F[\alpha]/F)$, $\sigma(\alpha)$ is a zero of $m_{\alpha,F}(x)$. Since $\sigma(\alpha)$ uniquely determines σ, $\{x - \sigma(\alpha)\}_{\sigma \in \mathrm{Gal}(F[\alpha]/F)}$ is a set of distinct factors of $m_{\alpha,F}(x)$. Hence $g_\alpha(x) \mid m_{\alpha,F}(x)$ where $g_\alpha(x) = \prod_{\sigma \in \mathrm{Gal}(F[\alpha]/F)} (x - \sigma(\alpha))$.

Lecture 29: Cyclotomic fields

Sunday, March 11, 2018 11:56 AM

On the other hand, $\sigma(g_\alpha(x)) = g_\alpha(x)$ for any $\sigma \in Gal(F[\alpha]/F)$.

And so $g_\alpha(x) \in Fix(Gal(F[\alpha]/F))[x] = F[x]$. As $g_\alpha(x) \mid m_{\alpha,F}(x)$,

g_α and $m_{\alpha,F}$ are monic in $F[x]$, and $m_{\alpha,F}$ is irred. in $F[x]$,

claim follows. ■

So θ is an isomorphism if and only if $m_{\zeta_n,\mathbb{Q}}(x) = \prod_{\substack{1\le i\le n\\ \gcd(i,n)=1}} (x-\zeta_n^i)$.

Def. Let $\Phi_n(x) := \prod_{\substack{1\le i\le n\\ \gcd(i,n)=1}} (x-\zeta_n^i)$. It is called the n^{th} cyclotomic polynomial.

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

Pf. $$x^n - 1 = \prod_{1\le i\le n} (x-\zeta_n^i) = \prod_{d\mid n} \prod_{\substack{1\le i\le n\\ \gcd(i,n)=d}} (x-\zeta_n^i)$$

$$= \prod_{d\mid n} \prod_{\substack{1\le i'\le n/d\\ \gcd(n/d,i')=1}} (x-\zeta_n^{di'}) = \prod_{d\mid n} \prod_{\substack{1\le i'\le n/d\\ \gcd(n/d,i')=1}} (x-\zeta_{n/d}^{i'})$$

$$= \prod_{d\mid n} \Phi_{n/d}(x) = \prod_{d\mid n} \Phi_d(x). \quad ■$$

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

Pf. We proceed by induction on n. $\Phi_1(x) = x - 1 \in \mathbb{Z}[x]$. (We cont. in the next lecture)

Lecture 29: Different proof about minimal poly

Monday, March 12, 2018 11:35 AM

Pf ② of proposition (this was presented during lecture)

Let α' be a zero of $m_{\alpha,F}(x)$. Then $\exists\, \sigma: F[\alpha] \xrightarrow{\sim} F[\alpha']$ s.t. $\sigma|_F = id_F$. Since $F[\alpha]/F$ is normal, $\alpha' \in F[\alpha]$. Comparing degrees we deduce that $F[\alpha] = F[\alpha']$. Hence $\sigma \in Gal(F[\alpha]/F)$. Since $F[\alpha]/F$ is separable, all zeros of $m_{\alpha,F}(x)$ are distinct. Hence $m_{\alpha,F}(x) = \prod_{i=1}^{n}(x-\alpha_i)$ for some $\alpha_i \in F[\alpha]$, $\alpha_i \neq \alpha_j$ if $i \neq j$. And $\exists\, \sigma_i \in Gal(F[\alpha]/F)$ s.t. $m_{\alpha,F}(x) = \prod_{i=1}^{n}(x - \sigma_i(\alpha))$ and $\sigma_i \neq \sigma_j$ if $i \neq j$.

On the other hand,

$$\begin{array}{c} \deg m_{\alpha,F} = [F[\alpha]:F] = |Gal(F[\alpha]/F)| \\ \| \\ |\{\sigma_1, \dots, \sigma_n\}|. \end{array}$$

Therefore $Gal(F[\alpha]/F) = \{\sigma_1, \dots, \sigma_n\}$; and claim follows. ∎