Math 210B Lecture 8 Notes

Daniel Raban

January 25, 2019

1 Normal Extensions, Galois Extensions, and Galois Groups

1.1 The primitive element theorem

Let's complete the proof from last time.

Theorem 1.1 (primitive element theorem)**.** *Every finite, separable extension is simple.*

Proof. If $F = \mathbb{F}_q$, then $\mathbb{F}_{q^n}$, where $\mathbb{F}_q(\xi)$, where ξ is the primitive $(q^n - 1)$-th root of 1. Now we may assume that F is an infinite field. It suffices to show that any $F(\alpha, \beta)/F$ (with α, β algebraic) is simple. Look at $\gamma := \alpha + c\beta$ for $c \in F \setminus \{0\}$. Since F is infinite, we can choose $c \neq (\alpha' - \alpha)/(\beta' - \beta)$, where α' is a conjugate of α and same for β. Then $\gamma \neq \alpha' + c\beta'$ for all such α', β'. Let f be the minimal polynomial of α, and let $h(x) = f(\gamma - cx) \in F(\gamma)[x]$. Now $h(\beta) = f(\alpha) = 0$, and $h \in F(\gamma)[x]$. But $h(\beta') = f(\gamma - c\beta) \neq 0$ for all β' conjugate (but not equal) to β. If $g \in F[x]$ is the minimal polynomial of β, then since it and h share just one root, β, in $F(\gamma)$, the minimal polynomial of β is $x - \beta$. Then $\beta \in F(\gamma)$, which gives $\alpha \in F(\gamma)$. So $F(\gamma) = F(\alpha, \beta)$. $\square$

Remark 1.1. Where does separability come into play during the proof? We used that g is separable and α is not a double root of h.

1.2 Normal extensions

Definition 1.1. An algebraic extension E/F is **normal** if it is the splitting field of some set of polynomials in $F[x]$.

Example 1.1. $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not normal. The minimal polynomial of $\sqrt[4]{2}$, $x^4 - 2$, has roots not in $\mathbb{Q}(\sqrt[4]{2})$. However, the extension $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ is normal.

Lemma 1.1. *If K/F is normal, then so is K/E for any intermediate E.*

Theorem 1.2. *An algebraic extension E/F is normal if and only if every embedding $\Phi : E \to \overline{F}$ (where $\overline{F} \subseteq E$) fixing F satisfies $\Phi(E) = E$.*

Proof. Let E/F be normal, and say it is the splitting field of $S \subseteq F[x]$. Suppose $\Phi : E \to \overline{F}$ is an embedding fixing F. Let $\alpha \in E$. Then $\Phi(\alpha) = \beta$, where β is conjugate to α over F. So $\beta \in E$, so $\Phi(E) \subseteq E$. Then $\Phi(E) = E$.

Suppose that $\Phi(E) = E$ for all Φ, and let $\alpha \in E$ have minimal polynomial f. Given $\beta \in \overline{F}$ that is a root of f, there exists Φ such that $\Phi(\alpha) = \beta$. Therefore, $\beta \in E$. So in particular, E is the splitting field of all minimal polynomials in $F[x]$ with a root in E. $\square$

Corollary 1.1. *IF E/F is normal and $f \in F[x]$ has a root in E, then f splits in E.*

Proposition 1.1. *If $E, K \subseteq \overline{F}$ are normal over F, then so is the compositum EK.*

Proof. E is the splitting field of S. K is the splitting field of T. Then EK is the splitting field of $S \cup T$. $\square$

Here is an alternative proof.

Proof. If $\varphi \in \mathrm{Emb}_F(EK)$, then since $\varphi(E) = E$ and $\varphi(K) = K$, $\varphi(EK) = EK$. $\square$

1.3 Galois groups and extensions

Definition 1.2. The **Galois group** $\mathrm{Gal}(E/F)$ of a normal extension E/F is the group of field automorphisms $E \to E$ fixing F.

Sometimes, we may write $\mathrm{Gal}(E/F) = \mathrm{Aut}_F(E) \subseteq \mathrm{Aut}(E)$.

Remark 1.2. $|\mathrm{Gal}(E/F)| = [E : F]_s$. This equals the degree when E/F is separable.

Definition 1.3. An extensions E/F is **Galois** if it is normal and separable.

Remark 1.3. If E/F is finite, then E/F is Galois iff it is normal and $|\mathrm{Gal}(E/F)| = [E : F]$.

Example 1.2. Last time, we showed that $\mathbb{F}_{q^n}/\mathbb{F}_q$ is separable. $\mathbb{F}_{q^n}$ is the splitting field of $x^{q^n} - x$, which is separable, so $\mathbb{F}_{q^n}$ is Galois. The **Frobenius element** $\varphi_q \in \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is defined by $\varphi_q(\alpha) = \alpha^q$. This is a field homomorphism; it is an additive homomorphism because we are in characteristic q. What are the other elements of $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$?

Proposition 1.2. $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \langle \varphi_q \rangle \cong \mathbb{Z}/n\mathbb{Z}$.

Proof. The automorphism $\varphi_q^k(\alpha) = \alpha^{q^k}$ fixes $\mathbb{F}_{q^n}$ iff $n \mid k$. So its order is n. The Galois group has order n, so this must be a cyclic group. $\square$

Example 1.3. $\mathbb{F}_p(t^{1/p})/\mathbb{F}_q(t)$ is purely inseparable. If $\sigma \in \mathrm{Aut}_{\mathbb{F}_q(t)}(\mathbb{F}_q(t^{1/p}))$, then $\sigma(t) = t$. So $\sigma(t^{1/p})^p = \sigma(t) = t$. Then $\sigma(t^{1/p}) = t^{1/p}$. That is, $\mathrm{Aut}_{\mathbb{F}_q(t)}(\mathbb{F}_q(t^{1/p}))$ is trivial.

Example 1.4. Recall that the cyclotomic polynomial Φ_n is irreducible. Then $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$. Let K be a field of characteristic $\nmid n$. Define the n-th **cyclotomic character** $\chi_n : \mathrm{Gal}(K(\zeta_n)/K) \to (\mathbb{Z}/n\mathbb{Z})^\times$ sending $\sigma \mapsto a \pmod{n}$, where $\sigma(\zeta_n) = \zeta_n^a$. We can also say it like this: $\sigma(\zeta_n) = \zeta_n^{\chi_n(\sigma)}$. This is a homomorphism because

$$\zeta_n^{\chi_n(\sigma\tau)} = \sigma(\tau(\zeta_n)) = \sigma(\zeta_n^{\chi_n(\tau)}) = \sigma(\zeta_n)^{\chi_n(\tau)} = \zeta_n^{\chi_n(\sigma)\chi_n(\tau)}.$$

This is injective because χ_n is determined on σ by what power σ raises ζ_n to.

Proposition 1.3. *The map $\chi_n : \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$ is an isomorphism.*

Proof. The Galois group has order $\varphi(n)$, the same as the order of $(\mathbb{Z}/n\mathbb{Z})^\times$. We already showed that χ_n is injective. □

1.4 Fixed fields

Definition 1.4. The **fixed field** of a field E by a subgroup G of $\mathrm{Aut}(E)$ is the field $E^G = \{\alpha \in E : \sigma \cdot \alpha = \alpha \, \forall \sigma \in G\}$.

Proposition 1.4. *If if K/F is Galois, then $K^{\mathrm{Gal}(K/F)} = F$.*

Proof. ($\supseteq$): F is fixed by every $\sigma \in \mathrm{Gal}(K/F)$.

($\subseteq$): If $\alpha \in K^{\mathrm{Gal}(K/F)}$, then for all $\sigma \in \mathrm{Gal}(K/F)$, $\sigma \cdot \alpha = \alpha$. But this means that α is the only root of its minimal polynomial in K by normality. Separability gives us that the minimal polynomial is $x - \alpha$. Therefore, $\alpha \in F$. □

Let K/F is finite and Galois, let E be intermediate, and let $\sigma \in \mathrm{Gal}(K/F)$. We can consider the restriction $\sigma|_E : E \to \sigma(E)$. If E is normal over F, then this gives a map $\mathrm{Gal}(K/F) \to \mathrm{Gal}(E/F)$.

Lemma 1.2. *Let K/F be Galois and E be intermediate. The restriction map $\mathrm{res}_E : \mathrm{Gal}(K/F)/\mathrm{Gal}(K/E) \to \mathrm{Emb}_F(E)$ is a bijection. If E/F is Galois, then this is an isomorphism of groups.*

Proof is left as an exercise.[1]

[1] Why, Professor Sharifi? Why?