Math 210B Lecture 2 Notes

Daniel Raban

January 9, 2019

1 Introduction to Field Theory

1.1 Field extensions

Definition 1.1. A field E is an **extension field** (or **extension**) of a field F if F is a subfield of E.

We often write E/F to denote that E is an extension of F. F is called the **ground field** of E/F. E is an F-vector space. If E is finite dimensional over F, we say that E/F is a finite extension.

Definition 1.2. Let E be finite dimensional over F. Then the **degree** $[E : F]$ is $\dim_F(E)$.

Definition 1.3. Let $S \subseteq E$. We say S **generates** E/F if E is the smallest subfield of E containing F and S.

If $S = \{\alpha_1, \dots, \alpha_n\}$, we write $E = F(\alpha_1, \dots, \alpha_n)$.

Lemma 1.1. *Every field F is an extension of $\mathbb{Q}$ if $\operatorname{char}(F) = 0$ and $\mathbb{F}_p$ if $\operatorname{char}(F) = p$.*

Proof. $\mathbb{Q}$ or $\mathbb{F}_p$ here is the subfield generated by 1. □

Definition 1.4. An **intermediate field** E' in E/F is a subfield of E containing F.

Example 1.1. $Q(i)$ and $Q(\sqrt{2})$ are intermediate fields of $\mathbb{C}/\mathbb{Q}$.

Note that $\mathbb{Q}(i) = \mathbb{Q}[i] \subseteq \mathbb{C}$ and $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}] \subseteq \mathbb{C}$. This is not always the case.

Example 1.2. Let $\mathbb{Q}(x) = \{f/g : f, g \in \mathbb{Q}[x], g \neq 0\}$. The field of rational functions is $\mathbb{Q}(\mathbb{Q}[x])$. $\mathbb{Q}(x) \neq \mathbb{Q}[x]$

Lemma 1.2. *Let E/F be an extension and $\alpha \in E$. Then $F(\alpha) = \mathbb{Q}(F[\alpha])$.*

Proof. $F(\alpha)$ is the smallest subfield containing $F \cup \{\alpha\}$. $F[\alpha]$ is the smallest subring containing $F \cup \{\alpha\}$. The inclusion $\iota : F[\alpha] \to F(\alpha)$ is injective and induces an isomorphism $Q(F[\alpha]) \to F(\alpha)$ of fields. □

1.2 Algebraic extensions, minimal polynomials, and splitting fields

Definition 1.5. If E/F is an extension and $\alpha \in E$, then α is **algebraic** (over F) if $F[\alpha] = F(\alpha)$ and **transcendental** otherwise. E/F is **algebraic** if every $\alpha \in E$ is algebraic over F and transcendental otherwise.

Proposition 1.1. *If $\alpha \in E$ is algebraic over F. then there exists a unique monic irreducible polynomial $f \in F[x]$ such that $f(\alpha) = 0$. Moreover, $F[x]/(f) \cong F(\alpha)$ by sending $g(x) \mapsto g(\alpha)$.*

This f is called the **minimal polynomial** of α over F.

Proof. Note that $1/\alpha = g(\alpha)$ for some $g \in F[x]$. Then $\alpha g(\alpha) - 1 = 0$. Set $h = xg(x) - 1$. There exists a monic irreducible $f \mid h$ such that $f(\alpha) = 0$. If $p \in F[x]$ satisfies $p(\alpha) = 0$ and $f \nmid p$, then $(f, p) = (1)$. But the ideal generated by α is not trivial. So $f \mid p$. The last statement follows. □

Corollary 1.1. *If α is algebraic over F, then $F(\alpha)/F$ is finite of degree equal to the degree of the minimal polynomial of α with basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$ over F.*

Proposition 1.2. *If E/F is finite and $\alpha \in E$, then α is algebraic.*

Proof. The set $\{1, \alpha, \ldots, \alpha^{[E:F]}\}$ is linearly depedent. The relation gives a polynomial with α as a root. □

Corollary 1.2. *If E/F is finite, then $E = F(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n \in E$.*

Theorem 1.1 (Kronecker)**.** *Given nonconstant $f \in F[x]$, there exists E/F such that E contains a root of F.*

Proof. Take $F[x]/(g)$, where g is monic, irreducible, and $g \mid f$. □

Definition 1.6. A **splitting field** for nonconstant $f \in F[x]$ is a field E in which f factors into a product of linear polynomials.

Corollary 1.3. *For any nonconstant $f \in F[x]$, there exists a splitting field for f over F.*

Example 1.3. A splitting field for $x^3 - 2$ (over $\mathbb{Q}$) in $\mathbb{C}$ is $\mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}) = \mathbb{Q}(\omega, \sqrt[3]{2})$, where $\omega = e^{2\pi i/3}$.

1.3 Degrees of extensions

Theorem 1.2. *If K/E and E/F are extensions, A is a basis of E/F, and B is a basis of K/E, then $AB \cong A \times B$ is a basis of K/F.*

Proof. If $\gamma \in K$, then $\gamma = \sum c_j \beta_j$, where $c_j \in E$. Then $c_j = \sum d_{i,j}\alpha_i$, where $\alpha_i \in f$. So $\gamma = \sum_i \sum_j d_{i,j}\alpha_i\beta_j$. So AB spans K. If $\sum(\sum a_{i,j}\alpha_i)\beta_j = 0$, then $\sum a_{i,j}\alpha_i = 0$ for all j. Then $a_{i,j} = 0$ for all i, j. □

Corollary 1.4. *If K/E and E/F are finite, then $[K : F] = [K : E][E : F]$.*

Definition 1.7. Let $E, E' \subseteq K$ be subfields. The **compositum** EE' is the smallest subfield of K containing E and E'.

Example 1.4. If E/F, then $E(\alpha) = EF(\alpha)$.

Example 1.5. $F(\alpha, \beta) := F(\alpha)(\beta) = F(\alpha)F(\beta)$.

Proposition 1.3. *If E, E' are finite over F and contained in K, A is a basis of E/F, and B is a basis of E'/F, teen AB spans EE'.*

Proof. Let $A = \{\alpha_1, \ldots, \alpha_m\}$ and $B = \{\beta_1, \ldots, \beta_n\}$. Then $EE' = F(\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n) = F[\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n]$. Note that $\alpha_1^{i_1} \cdots \alpha_m^{i_m} \in E$ is a linear combination over F of the α_is. Similarly for the β_js in E'. So the $\alpha_i\beta_j$s span EE'. □

Corollary 1.5.

$$[EE' : F] \leq [E : F][E' : F].$$

Corollary 1.6. *If $[E : F]$ and $[E' : F]$ are relatively prime, we get equality.*

Proof. $[E : F]$ and $[E' : F]$ divide $[EE' : F]$. □

Example 1.6. Consider $\mathbb{Q}(\sqrt[3]{2}, \omega^3\sqrt[3]{2})$, where $\omega^2 + \omega + 1 = 0$. Then

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}][\mathbb{Q}(\omega^3\sqrt[3]{2}) : \mathbb{Q}] = 9, \qquad [\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}][\mathbb{Q}(\omega) : \mathbb{Q}] = 6.$$

Proposition 1.4. *Let E_i be subfields of K containing F for all i in some index set I. The the compositum E of all E_i is $\bigcup F(\alpha_1, \ldots, \alpha_n)$, where $n \geq 0$, and each α_j is in some E_i.*