Math 210B Lecture 5 Notes

Daniel Raban

January 16, 2019

1 Algebraic Closure

1.1 Algebraically closed fields

Definition 1.1. A polynomial **splits** in $L[x]$ if it factors in $L[x]$ as a product of linear polynomials.

Definition 1.2. A field L is **algebraically closed** if every nonconstant polynomial in $L[x]$ has a root in L.

Proposition 1.1. *If $L[x]$ is algebraically closed, then every (nonconstant) poltnomial in $L[x]$ splits over L.*

Corollary 1.1. *If M is an algebraic extension of an algebraically closed field L, then $M = L$.*

Theorem 1.1 (fundamental theorem of algebra)**.** *$\mathbb{C}$ is algebraically closed.*

Here is a proof that uses no algebra.

Proof. Let $f \in \mathbb{C}[x]$ have no roots in $\mathbb{C}$. Then $1/f$ is holomorphic on $\mathbb{C}$. Moreover, $1/f$ is bounded. So $1/f$ is constant by Liouville's theorem. Thus, f is constant. $\square$

Theorem 1.2. *Let E/F be algebraic, and let $\varphi : F \to M$ be a field embedding with M algebraically closed. Then there exists a field embedding $\Phi : E \to M$ extending φ.*

Proof. Let $X = \{(K, \sigma) : E/K/F, \sigma : K \to M \text{ is an embedding extending } \varphi\}$. Then $(K, \sigma) \leq (K', \sigma')$ if $K \subseteq K'$ and $\sigma'|_K = \sigma$ defines a partial order on X. Let $|mcC$ be a chain in X. Then $L = \bigcup_{K \in \mathcal{C}} K$ with $\tau : L \to M$ defined as $\tau|_K = \sigma$ for each $K \in \mathcal{C}$ is an upper bound for $\mathcal{C}$. By Zorn's lemma, we have a maximal element (Ω, Φ).

We want to show that $\Omega = E$. Let $\alpha \in E$, and let $f \in \Omega[x]$ be its minimal polynomial $f(x) = \sum_{i=1}^n a_i x^i$, where $n = \deg(f)$. Define $g := \sum_{i=1}^n \Phi(a_i) x^i \in M[x]$. M is algebraically closed, so g has a root $\beta \in M$. So there exists $\tilde{\Phi} : \Omega(\alpha) \to M$ with $\tilde{\Phi}|_\Omega = \Phi$ and $\alpha \mapsto \beta$. Then $(\Omega(\alpha), \tilde{\Phi}) \geq (\Omega, \Phi)$. So $\alpha \in \Omega$, as (Ω, Φ) is maximal. $\square$

Proposition 1.2. *The set of all algebraic elements over F in an extension E/F is a subfield of E, the largest intermediate field that is algebraic over F.*

Proof. Let M be the set of algebraic elements over F in E. Let $\alpha, \beta \in M$. Then $F(\alpha, \beta)/F$ is finite, so it contains $\alpha - \beta$ and α/β if $\beta \neq 0$, and $F(\alpha, \beta) \subseteq M$. $\square$

Corollary 1.2. *The set $\overline{\mathbb{Q}}$ of algebraic numbers in $\mathbb{C}$ is a subfield of $\mathbb{C}$.*

1.2 Algebraic closure

Definition 1.3. An **algebraic closure** of a field F is an algebraic, algebraically closed extension of F.

Proposition 1.3. *Let $K/E/F$. Then K/F is algebraic if and only if K/E and E/F are algebraic.*

Proof. ($\Longleftarrow$): Take $\alpha \in K$, and let $f \in E[x]$ be its minimal polynomial, $f = \sum_{i=0}^{n} a_i x^i$, where $a_i \in E$. Each of these a_i is algebraic over F. Then $F(a_0, \dots, a_n)(\alpha)$ is finite over F, so every element in it is algebraic over F, so α is algebraic over F. $\square$

Proposition 1.4. *If F is a field and M/F is algebraically closed, then M contains a unique algebraic closure of F, the maximal subfield $\overline{F}$ of M which is algebraic over F.*

Proof. Suppose $f \in \overline{F}[x]$, and look at E/F, generated by the coefficients of f. E/F is finite. If $\alpha \in M$ is a foot of f, then $E(\alpha)/F$ is algebraic by the previous proposition, so α is algebraic over F. Then $\alpha \in \overline{F}$. $\square$

Corollary 1.3. *$\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$.*

Example 1.1. $\overline{\mathbb{F}}_p := \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$ is an algebraic closure of $\mathbb{F}_p$. This union makes sense because $\mathbb{F}_{p^k}, F_{p^\ell} \subseteq F_{p^m}$, where $m = \operatorname{lcm}(k, \ell)$.

Theorem 1.3. *Every field F has an algebraic closure.*

Proof. Let F be a field, $\Omega = \coprod_f R_f$, where f runs over monic irreducible polynomials in $F[x]$ and R_f is a finite set with one element for each root of f in a splitting field. Then $F \subseteq \Omega$ because a is the unique root of $x - a$. Let $X = \{E/F \text{ algebraic} : E \subseteq \Omega, \alpha \in E\}$. Such an $\alpha \in R_f$, where f is in the minimal polynomial of α. $X \neq \varnothing$, since $F \in X$.

Let $\mathcal{C}$ be a chain in X, and let $K = \bigcup_{E \in \mathcal{C}} E \subseteq \Omega$. Check yourself that $K \in X$. So $\mathcal{C}$ has an upper bound. By Zorn's lemma, we have a maximal element $\overline{F} \in X$. Since $\overline{F} \in X$, it is algebraic. We claim that $\overline{F}$ is algebraically closed. Let $f \in F[x]$ and $g \in \overline{F}[x]$ be monic and irreducible with $g \mid f$. $E = \overline{F}[x]/(g) \subseteq \Omega$ as follows: if $h \in F[x]$ is monic and irreducible with a root in E, then the distinct roots of h in $E \setminus \overline{F}$ inject into elements of $R_h \setminus \overline{F}$. By maximality, $E = \overline{F}$. So $\overline{F}$ is algebraically closed. $\square$

Proposition 1.5. *If M, M' are algebraic closures of F then there exists an isomorphism $\Phi : M \to M'$ fixing F.*

Proof. We have an embedding $F \to M'$. There exists a $\Phi : M \to M'$ extending this inclusion. It suffices to show that $\mathrm{im}(\Phi)$ is algebraically closed. If $\alpha \in M$ is a root of $f \in F[x]$, it maps to a root of $\Phi(\alpha)$ of f in $\Phi(M) \subseteq M'$. So $\Phi(M)$ is algebraically closed, and hence $\Phi(M) = M$. $\square$