Math 332

Field Theory

Def. Let k and K be fields with $k \subseteq K$. Then K is called an **extension field** of k. We write $[K:k]$ for $\dim_k K$.

Prop. Let $E \subset F \subset K$ be fields. If $\{v_\alpha\}$ is an E-basis for F and $\{w_\beta\}$ is an F-basis for K. Then $\{v_\alpha w_\beta\}_{\alpha,\beta}$ is an E-basis for K.

Thus, $[K:E] < \infty$ iff $[F:E] < \infty$ and $[K:F] < \infty$, and in this case

$$[K:E] = [K:F][F:E].$$

Pf/ Exercise. $\square$

Def. Let $k \subseteq K$ be a field extension. An element $\alpha \in K$ is **algebraic** over k if $\exists$ nonzero $p \in k[x]$ such that $p(\alpha) = 0$.

Let $k \subseteq K$ be a field extension, and let $\alpha \in K$. We let $k[\alpha]$ denote the smallest ring in K containing α and k, and $k(\alpha)$ denote the

smallest field in K containing α and k.

Prop. $k \subseteq K$, $\alpha \in K$. If α is algebraic over k, then $k[\alpha] = k(\alpha)$.

Pf/ The ring homomorphism $\varphi : k[x] \longrightarrow k[\alpha]$, $f \longmapsto f(\alpha)$ is surjective and induces an isomorphism $k[x]/\ker\varphi \xrightarrow{\cong} k[\alpha]$. Since $k[x]$ is a PID, $\ker\varphi = (p)$ for some $p \in k[x]$ (and p is nonzero since α is algebraic). Then, since $k[\alpha] \subseteq K$ is a domain, we know (p) is prime. In a PID, nonzero prime ideals are maximal. Hence, $k[x]/(p) \cong k[\alpha]$ is a field. So $k[\alpha] = k(\alpha)$. □

Def. The polynomial p (taken to be monic, i.e. with leading coefficient equal to 1) is called the irreducible polynomial for α over k. (It's unique: $k[x]$ is a UFD and $(p) = (q) \Rightarrow p = qu$ for some unit u. If p, q both monic, then $p = q$.)

Example. $\mathbb{Q} \subseteq \mathbb{C}$, and $i \in \mathbb{C}$ is algebraic / $\mathbb{Q}$ with irreducible polynomial $p(x) = x^2 + 1$. Then $\mathbb{Q}[i] = \{a + bi : a, b \in \mathbb{Q}\} \cong \mathbb{Q}[x]/(x^2+1)$.

Prop. $k \subseteq K$. Then $\alpha \in K$ is algebraic over k iff $k(\alpha)$ is finite-dimensional over k.

Pf/ ($\Rightarrow$) Suppose α is algebraic over k. Let p be the irreducible polynomial for α so that $k(\alpha) \cong k[x]/(p)$. Let $d = \deg p$. By the division algorithm, each $f \in k[x]$ can be written $f = pq + r$ with $\deg r < d$. Since $f = r$ in $k[x]/(p)$, every element of $k[x]/(p)$ is represented by a polynomial of degree $< d$. Hence, $\{1, x, \ldots, x^{d-1}\}$ span $k[x]/(p)$. So $k(\alpha)$ is finite-dimensional over k, spanned by $\{1, \alpha, \ldots, \alpha^{d-1}\}$. [In fact, $\{1, \alpha, \ldots, \alpha^{d-1}\}$ is a basis. To see this, we show that $\{1, x, \ldots, x^{d-1}\}$ is a basis for $k[x]/(p)$ over k. Suppose $\sum_{i=0}^{d-1} a_i x^i = 0 \in k[x]/(p)$. Then $a_0 + a_1 x + \cdots + a_{d-1} x^{d-1} = pq$ in $k[x]$. But $\deg p = d > d-1$. Hence, $q = 0$. So $a_0 + a_1 x + \cdots + a_{d-1} x^{d-1} = 0$ as a polynomial in $k[x]$. Thus, $a_i = 0 \ \forall i$.]

($\Leftarrow$) Conversely, suppose $[k(\alpha) : k] = d < \infty$. Consider $\{1, \alpha, \alpha^2, \ldots\}$. By finite-dimensionality there is a relation $\sum_{i=0}^{e} a_i \alpha^i = 0$ for some e. Let $q = \sum a_i x^i \in k[x]$. Then $q(\alpha) = 0$. Hence, α is algebraic / k. $\square$

Note: As part of the above proof, we see that if $\alpha \in K$ is algebraic over k then $[k(\alpha) : k]$ is the degree of the irreducible polynomial for α over k.

Def. Let $k \subset K$ be an extension of fields. The **algebraic closure** of k in K is

$$F := \{\alpha \in K : \alpha \text{ algebraic over } k\}.$$

Prop. Let $k \subset K$ be an extension of fields and let F be the algebraic closure of k in K. Then F is a field.

Pf/ Let $\alpha, \beta \in F$. Then α algebraic over $k \Rightarrow [k(\alpha):k] < \infty$, and

β algebraic over $k \Rightarrow \beta$ algebraic over $k(\alpha) \Rightarrow [k(\alpha)(\beta):k(\alpha)] < \infty$

(note: $k(\alpha)(\beta) = k(\alpha,\beta) =$ smallest field in K containing k, α, and β).

Therefore, $[k(\alpha,\beta):k] = [k(\alpha,\beta):k(\alpha)][k(\alpha):k] < \infty$. Hence, if $\gamma \in k(\alpha,\beta)$, then $k(\alpha,\beta) \supseteq k(\gamma) \supseteq k \Rightarrow [k(\gamma):k] < \infty \Rightarrow \gamma$ algebraic over k. Therefore, $\alpha+\beta$, $-\alpha$, $\alpha\beta$ are algebraic over k, hence elements of F. $\square$

Prop. With notation as in the preceding proposition, suppose L is a field with $F \subseteq L \subseteq K$ and $[L:F] < \infty$. Then $L = F$.

Pf/ Let $\alpha \in L$. Then $F(\alpha)$ is finite-dimensional over F, hence α is algebraic

over F. Take $p \in F[x]$ such that $p(\alpha) = 0$. Let $a_i \in F$ be the coefficients of p. Then α is algebraic over $k(a_1, \dots, a_n)$. We have a chain of finite extensions: $k \subseteq k(a_1) \subseteq k(a_1, a_2) \subseteq \cdots \subseteq k(a_1, \dots, a_n) \subseteq k(a_1, \dots, a_n, \alpha)$. Hence, $k(a_1, \dots, a_n, \alpha)$ is finite-dimensional over k. Therefore, so is $k(\alpha)$ since $k \subseteq k(\alpha) \subseteq k(a_1, \dots, a_n, \alpha)$. Hence, α is algebaic over k, an element of L. $\square$

Def Let $k \subseteq K$ be an extension of fields. Then K is an algebraic extension of k if each $\alpha \in K$ is algebraic over k.

Def A field E is algebraically closed if it has no algebraic extensions.

Prop. The following are equivalent

(1) E is algebraically closed.
(2) E has no non-trivial finite extensions.
(3) Every non-constant polynomial in $E[x]$ has a root in E.
(4) Every irreducible polynomial in $E[x]$ has degree 1.
(5) Every non-constant polynomial in $E[x]$ is a product of linear polynomials in $E[x]$.

Pf/ (1) $\Rightarrow$ (2) If $F \supseteq E$ is finite and $\alpha \in F$ then $[F:E] = [F:E(\alpha)][E(\alpha):E] \Rightarrow$ $[F(\alpha):F] < \infty \Rightarrow \alpha$ algebraic / F. Hence, F is alg. over E, implying $F = E$.

(2) $\Rightarrow$ (1) Suppose $F \supsetneq E$ is an algebraic extension. Then $E(\alpha) > E$ is a nontrivial finite extension.

(2) $\Leftrightarrow$ (3) $\Leftrightarrow$ (4) is clear from the division algorithm.

(2) $\Rightarrow$ (3) If $p \in E[x]$ is irreducible, then $E[x]/(p)$ is a finite extension of E and we seen $[E[x]/(p) : E] = \deg(p)$. Thus, (3) $\Rightarrow \deg p = 1$.

(3) $\Rightarrow$ (2). Suppose F is a finite extension of E and let $\alpha \in F$. Then α is algebraic over E. Let $p \in E[x]$ be the minimal polynomial for α. Then (3) $\Rightarrow p = x - \alpha$. Hence, $\alpha \in E$. $\square$

Cor If Ω is algebraically closed, and k is a subfield, let $\bar{k}$ be the algebraic closure of k in Ω. Then $\bar{k}$ is algebraically closed.

Pf/ Suppose $p \in \bar{k}[x]$ is irreducible. Then p has a root $\alpha \in \Omega$. Then $[\bar{k}(\alpha):\bar{k}] < \infty$ Since $\bar{k}$ is algebraic over k, so is α. [Let $\{a_i\} \subseteq \bar{k}$ be the coefficients

of p and consider the chain of fields $k(a_1,\dots,a_n,\alpha) \supseteq k(a_1,\dots,a_n) \supseteq k(a_1,\dots,a_{n-1}) \supseteq \cdots \supseteq k$.

Each step is finite since each a_i is algebraic $/k$ an α is algebraic $/ k(a_1,\dots,a_n)$.]

Hence, $\alpha \in k$. $\square$

Def / Example The algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$ is an algebraically closed, infinite extension of $\mathbb{Q}$ called the field of algebraic numbers.