Elements of Extension Fields

Defn Extension L/F, $\alpha \in L$. Then α is *algebraic* over F if there is a nonconstant polynomial $f \in F[x]$ s.t. $f(\alpha) = 0$. If α is not algebraic over F, then α is *transcendental* over F.

e.g.
- $\sqrt{2} \in \mathbb{R}$ is algebraic over $\mathbb{Q}$ since $\sqrt{2}$ is a root of $x^2 - 2 \in \mathbb{Q}[x]$
- $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$ is algebraic over $\mathbb{Q}$ since it's a root of $x^n - 1 \in \mathbb{Q}[x]$.
- π, e are transcendental over $\mathbb{Q}$ [hard!]
- $\sqrt{2} + \sqrt{3}$ is a root of $(x - \sqrt{2} - \sqrt{3})(x - \sqrt{2} + \sqrt{3})(x + \sqrt{2} - \sqrt{3})(x + \sqrt{2} + \sqrt{3})$ $= x^4 - 10x^2 + 1$ so is algebraic over $\mathbb{Q}$.
- Next Monday: If $\alpha, \beta \in L$ are alg over F, then so are $\alpha + \beta$, $\alpha\beta$, $\frac{1}{\alpha}$. Thus $\{\alpha \in L \mid \alpha \text{ alg } /F\}$ is a subfield of L.

Lemma If $\alpha \in L$ alg $/F$, then $\exists!$ nonconst monic poly $p \in F[x]$ s.t.
(a) $p(\alpha) = 0$, and
(b) if $f \in F[x]$ with $f(\alpha) = 0$, then $p \mid f$.

Defn Such p is called the *minimal polynomial* of α over F.

Pf of Lemma Among nonconstant $f \in F[x]$ w/ α as a root, there is (at least) one with minimal degree. Dividing by leading coeff, call this p. Clearly $p(\alpha) = 0$. Now suppose $f(\alpha) = 0$. Then $f = qp + r$ for some $q, r \in F[x]$ with $r = 0$ or $\deg(r) < \deg(p)$. Eval'n at α gives $0 = f(\alpha) = q(\alpha)p(\alpha) + r(\alpha) = r(\alpha)$. By minimality of $\deg(p)$, we conclude $r = 0$.

Uniqueness: ~~Say~~ Suppose $\tilde{p}$ also satisfies (a), (b). We get $p \mid \tilde{p}$ & $\tilde{p} \mid p$. Since both are monic, $p = \tilde{p}$. □

Prop $\alpha \in L$ alg $/F$, p = min poly of α $/F$. If $f \in F[x]$ is a nonconstant monic polynomial, then $f = p$ iff f is a poly of min'l degree with $f(\alpha) = 0$ iff f is irred $/F$ with $f(\alpha) = 0$.

Pf First equiv is in the proof of the lemma. Now show min poly is irred: if not, one of its factors has lower degree & α as root, contradicting first criterion. Now suppose $f(\alpha)=0$ with f irred. Then $p \mid f \Rightarrow p = f$ since both monic, f irred. □

e.g. · $p_{\sqrt{2},\mathbb{Q}} = x^2-2$

· $p_{\sqrt{2}+\sqrt{3},\mathbb{Q}} = x^4-10x^2+1$

· $p_{\zeta_n,\mathbb{Q}} = \Phi_n$, nth cyclotomic poly of degree $\phi(n) = \#$divisors of n. $(1 \le k \le n)$

Adjoining elts Given $\alpha_1, \dots, \alpha_n \in L$, define $F[\alpha_1, \dots, \alpha_n] := \{ h(\alpha_1, \dots, \alpha_n) \mid h \in F[x_1, \dots, x_n] \}$, $F(\alpha_1, \dots, \alpha_n) := \mathrm{Frac}\left(F[\alpha_1, \dots, \alpha_n]\right)$

Lemma $F(\alpha_1, \dots, \alpha_n)$ is the smallest subfield of L containing F and $\alpha_1, \dots, \alpha_n$.

Pf Must show that if K/F, $\alpha_1, \dots, \alpha_n \in K$, then $F(\alpha_1, \dots, \alpha_n) \subseteq K$.
Obvious since $F[\alpha_1, \dots, \alpha_n] \subseteq K$ & K is a field. □

Cor $F(\alpha_1, \dots, \alpha_n) = F(\alpha_1, \dots, \alpha_r)(\alpha_{r+1}, \dots, \alpha_n)$. □

Lemma L/F, $\alpha \in L$ alg over F with min poly $p \in F[x]$. Then $\exists!$ ring iso $F[\alpha] \cong F[x]/(p)$ which is the identity on F & $\alpha \mapsto x+(p)$.

Pf Take $\varphi: F[x] \longrightarrow L$ ($x \longmapsto \alpha$) which has image $F[\alpha]$. Remains to show $\ker(\varphi) = (p)$. Since $p(\alpha)=0$, $p \in \ker\varphi$ so $(p) \subseteq \ker\varphi$. If $f \in \ker\varphi$, $f(\alpha)=0$ so $p \mid f$ so $\ker\varphi \subseteq (p)$.
Uniqueness: ring hom defined on $F[\alpha]$ is determined by its values on F, α. □

Prop L/F, $\alpha \in L$. Then α is algebraic over F iff $F[\alpha] = F(\alpha)$.

Pf Lemma + $F[x]/(p)$ a field for p irred gives $\Rightarrow$.

($\Leftarrow$) Assume $\alpha \neq 0$. Then $\frac{1}{\alpha} \in F(\alpha) = F[\alpha]$ implies

$$\frac{1}{\alpha} = a_0 + a_1\alpha + \cdots + a_m\alpha^m.$$

for some $a_i \in F$. Thus $0 = -1 + a_0\alpha + a_1\alpha^2 + \cdots + a_m\alpha^{m+1}$ so α alg/F. □

Prop $F \subseteq L \ni \alpha_1, \ldots, \alpha_n$ alg/F. Then $F[\alpha_1, \ldots, \alpha_n] = F(\alpha_1, \ldots, \alpha_n)$.

Pf by induction on n. □