Existence of Roots

Two perspectives on $\mathbb{C}$:

Hamilton: $\mathbb{C} = \mathbb{R}^2$ with $(a,b)\cdot(c,d) = (ac-bd, ad+bc)$

Cauchy: $\mathbb{C} = \mathbb{R}[x]/(x^2+1)$. Mult'n law derives from taking remainder of $(a+bx)(c+dx)$ upon division by x^2+1. Field b/c $(x^2+1) \subseteq \mathbb{R}[x]$ is a maximal ideal:

Prop If F is a field and $f \in F[x]$ is nonconstant, then TFAE

(a) The poly f is irreducible over F.

(b) The ideal $(f) = \{fg \mid g \in F[x]\}$ is maximal.

(c) The quotient ring $F[x]/(f)$ is a field.

Pf (b) $\Leftrightarrow$ (c) is standard.

(a) $\Rightarrow$ (b). Suppose f irred, $(f) \subseteq \overset{\text{ideal}}{I} \subseteq F[x]$. Since $F[x]$ is a PID, $I = (g)$ for some $g \in F[x]$. Then $f \in (g)$ implies $f = gh$ for some $h \in F[x]$. Since f is irred, g or h must be constant. If g constant, $I = F[x]$. If h constant, $I = (f)$.

(b) $\Rightarrow$ (a). Suppose (f) max'l and let $f = gh$. Then $(f) \subseteq (g)$ so $(g) = (f)$ or $F[x]$. The former implies h constant, the latter g constant. Thus f irred. $\square$

Since x^2+1 irred$/\mathbb{R}$ (TPS: Why?) we deduce (x^2+1) max'l so $\mathbb{R}[x]/(x^2+1)$ is a field.

Defn Given a ring homomorphism of fields $\varphi: F \to L$, say L is a *field extension* of F via φ. Usually identify F with its image $\varphi(F) \subseteq L$, and write $F \subseteq L$.

HW φ is injective inducing $F \cong \varphi(F)$.

Notation Write L/F when L is a field extension of F.

<u>Prop</u> If $f \in F[x]$ is irreducible, then there exists L/F and $\alpha \in L$ s.t. $f(\alpha) = 0$.

<u>Pf</u> Let $L = F[x]/(f) \xleftarrow{\varphi} F$. Set $\alpha = x + (f)$.

$$a + (f) \longleftarrow a$$

Suppose $f = a_0 x^n + \cdots + a_n$ w/ $a_i \in F$. Then

$$f(\alpha) = (a_0 + (f))(x + (f))^n + \cdots + (a_n + (f))$$
$$= a_0 x^n + \cdots + a_n + (f)$$
$$= f + (f) = 0 + (f). \qquad \square$$

<u>Recall</u> $\alpha \in L$ is a root of $f \in L[x]$ iff $x - \alpha$ is a factor of f in $L[x]$.

A field L contains <u>all</u> roots of f means f factors

$$f = a_0 (x - \alpha_1) \cdots (x - \alpha_n)$$

where $\alpha_1, \ldots, \alpha_n \in L$. When this happens, we say f splits completely over L.

<u>Thm</u> Let $f \in F[x]$ be a poly of degree $n > 0$. Then $\exists\, L/F$ s.t. f splits completely over L.

<u>Pf</u> by induction on $n = \deg(f)$. If $n = 1$, $f = a_0 x + a_1$, $a_0 \neq 0$, $a_0, a_1 \in F$. Then $L = F$, $\alpha_1 = -a_1/a_0 \Rightarrow f = a_0(x - \alpha_1)$.

Now suppose $\deg(f) = n > 1$ & thm is true for $n-1$. Since $F[x]$ is a UFD, f has an irred divisor f_1. $\exists\, F_1/F$ and $\alpha_1 \in F_1$ s.t. $f_1(\alpha_1) = 0 \Rightarrow f(\alpha_1) = 0$ in F_1. Thus $f = (x - \alpha_1) g$ for some $g \in F_1[x]$ of deg $n-1$. Applying the induction hypothesis to g gives L/F_1 and $\alpha_2, \ldots, \alpha_n \in L$ s.t. $g = a_0 (x - \alpha_2) \cdots (x - \alpha_n)$.

Thus $f = a_0 (x - \alpha_1) \cdots (x - \alpha_n)$ so f splits completely over L. $\square$