Thm Let $f \in K[x]$ be irreducible. Then $K' := K[x]/(f)$ is a field extension of K and f has a root in K'. (More precisely the image of f under $K[x] \to K'[x]$ the inclusion)

Cor Given a polynomial $f \in K[x]$ there is some extension $E \supseteq K$ over which f factors into a product of linear polynomials.

Proof of thm (f) maximal $\Rightarrow K' := K[x]/(f)$ is a field

- The map $i : K \to K[x]/(f)$, $a \mapsto a + (f)$ is injective. Indeed $i(a) = 0 \Rightarrow a + (f) = 0$
  $\Rightarrow a \in (f)$.
  But a is a constant & $\deg f \geq 1 \Rightarrow a = 0$.
- $\bar{x}$ is a root of $i(f)$. Indeed,
  $i(f)(\bar{x}) = f(\bar{x}) = \overline{f(x)} = \bar{0}$. ∎

We will prove the corollary after we give a concrete description of $K[x]/(f)$.

Our goal is to prove a general theorem that implies things such as $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$

$$\mathbb{Q}[x]/(x^2-2) \cong \mathbb{Q}[\sqrt{2}]$$

Defn A **field extension** is an injective map of fields $K \to L$ (L is said to be a field extension of K, denoted $K \subseteq L$)

Ex
- $\mathbb{R} \subseteq \mathbb{C}$, $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{2}] \subseteq \mathbb{R}$.
- We can define the field of rational functions $\mathbb{Q}(x) = \left\{ \frac{f(x)}{g(x)} : g \neq 0 \right\}$ (we threw in the inverse of all non-zero elements in $\mathbb{Q}[x]$.)

On Hwk 5, we saw $\mathbb{Q}[\sqrt{2}] = \{ p(\sqrt{2}) : p \in \mathbb{Q}[x] \}$ is a field. Thus $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2}) := \left\{ \frac{p(\sqrt{2})}{q(\sqrt{2})} : q \neq 0 \right\}$

we will prove this more generally

Defn Let $K \subseteq L$ be a field extension and $\alpha \in L$. We define $K(\alpha)$ to be the smallest subfield of L containing K and α (it's the intersection of all subfields of L containing α and K). This is called the **field extension of K generated by α.** We can of course generalize to $K(A)$ for any subset $A \subseteq L$.

Remark Thus $K(\alpha) \supseteq \left\{ \frac{p(\alpha)}{q(\alpha)} : p, q \in K[x],\ q(\alpha) \neq 0 \right\}$. Since the latter is a field (we only need to worry about inverses) we have equality!

Important Exercise If $K \to L$ is a field extension, then L is a K-vector space

Defn $K \subseteq L$ be a field extension. The degree of the extension, denoted $[L:K]$, is the dimension of L as a K-vector space.
We say L is a finite extension if $[L:K] < \infty$, or infinite otherwise.

Ex.
- $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$ because $\{1, \sqrt{2}\}$ is a basis.
- $[\mathbb{C}:\mathbb{R}] = 2$ because $\{1, i\}$ is a basis.

* Let $\omega = e^{\frac{2\pi i}{3}}$ be a cube root of unity.
Then $[\mathbb{Q}(\omega):\mathbb{Q}] = 2$ because $\{1, \omega\}$ is a basis

- First note $\mathbb{Q}(\omega) = \mathbb{Q}[\omega] = \{a + b\omega + c\omega^2 : a, b, c \in \mathbb{Q}\}$ using $\omega^3 = 1$
- Then note $x^3 - 1 = (x-1)(x^2+x+1) \Rightarrow 1 + \omega + \omega^2 = 0$ i.e. $\{1, \omega, \omega^2\}$ is dependent.

- (Non-trivial) $[\mathbb{R}:\mathbb{Q}] = \infty$
- $[K(x):K] = \infty$ as $1, x, x^2, \ldots$ are linearly independent

Thm K a field and $f \in K[x]$ irreducible. Then $L = K[x]/(f)$ is a finite extension of K and $[L:K] = \deg f$.

Pf
- L being a field follows from $(f(x))$ being maximal (HwK 6).
- $K \subseteq L$ because $a \in K \Rightarrow a + (f) \in L$.

- Given $g(x) \in K[x]$, use the division algorithm to write $g = fq + r$ with $r = 0$ or $\deg r < \deg g$.
In $K[x]/(f)$ this becomes $g + (f) = r + (f)$.
But $r(x) = a_0 + a_1 x + \dots + a_r x^r$ with $r < \deg g$.
Thus $K[x]/(f) = \text{span}_K \{1 + (f), x + (f), \dots, x^{n-1} + (f)\}$.
Check that this is a linearly independent set to conclude $\dim_K L = n$ ∎

Defn
- Let $K \subseteq L$ be a field extension and $\alpha \in L$. Then α is said to be algebraic over K if $\exists\, f \in K[x] - \{0\}$ such that $f(\alpha) = 0$.
- If not α is said to be transcendental.
- If every $\alpha \in L$ is algebraic over K, we say $K \subseteq L$ is an algebraic extension.

Ex
- $\alpha \in K$ is algebraic over K (take $x - \alpha$).
- i, ω are algebraic over $\mathbb{R}$ (take x^2+1, x^2+x+1).
- [Non trivial] $\mathbb{Q} \subseteq \mathbb{R}$, π is transcendental over $\mathbb{Q}$.

Thm If $K \subseteq L$ is finite, then $K \subseteq L$ is algebraic.

Pf Since $[L:K] = n < \infty$, for any $\alpha \in L$, the set of $n+1$ elements $\{1, \alpha, \dots, \alpha^n\}$ is linearly dependent. Thus $\exists\, a_i$ not all zero such that $a_0 \cdot 1 + a_1 \alpha + \dots + a_n \alpha^n = 0$. Taking $f(x) = a_n x^n + \dots + a_1 x + a_0$ we see that α is algebraic over K as $f(\alpha) = 0$ and $f \in K[x] - \{0\}$ ∎

HwK $K \subseteq L$ algebraic $\not\Rightarrow$ $K \subseteq L$ finite (See HwK 7).

Defn Let $K \subseteq L$ be a field extension and $\alpha \in L$ algebraic. The minimal polynomial of α over K is $f \in K[x] - \{0\}$ of minimal degree satisfying

① f is monic ($f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$)

② $f(\alpha) = 0$

It's unique.

Ex. • $\mathbb{Q} \subseteq \mathbb{R}$, $\sqrt{2}$ has min. poly. $x^2 - 2$

• $\mathbb{R} \subseteq \mathbb{C}$, i has min. poly $x^2 + 1$

Thm Let $K \subseteq L$ a field extension and $\alpha \in L$ algebraic over K. Let f be the minimal polynomial of α

① f is irreducible

② If $g \in K[x]$ s.t. $g(\alpha) = 0 \Rightarrow f \mid g$.

Pf • ② follows from the division algorithm and the fact that the min. poly is irreducible.

• Assume $f = gh$ with g, h not units. Then $g(\alpha)h(\alpha) = f(\alpha) = 0$. Since K is a domain $\Rightarrow g(\alpha) = 0$ or $h(\alpha) = 0$. But $\deg g, \deg h < \deg f$, contradicting the minimality assumption of f (we may scale g, h by a unit to get g', h' monic and $g'(\alpha) = 0$ or $h'(\alpha) = 0$). Thus f is irreducible ■