# Extension Fields

<u>Def</u>: An <u>extension field</u> $E$ of a field $F$ is a field $E$ which contains $F$.

$$\begin{tikzcd}[arrows=dash]
\mathbb{C} \arrow[d] & & \mathbb{C}(x,y) & \\
\mathbb{R} \arrow[d] & \mathbb{C}(x) \arrow[ur] & & \mathbb{C}(y) \arrow[ul] \\
\mathbb{Q} & & \mathbb{C} \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

We all know the <u>Fundamental Theorem of Algebra</u> that a nonconstant polynomial $f(x) \in \mathbb{R}[x]$ has at least one (and hence $n = \text{degree}(f)$ many) root in $\mathbb{C}$.

<u>Quest</u>: What about other fields?

<u>Ex</u>: $F = \mathbb{Z}_2$, $f(x) = x^2 + x + 1$

$f(0) = 1$ and $f(1) = 1$ so no roots

Maybe it has roots over some larger field (extension field)?

**Theorem:** Let $F$ be a field and $f(x) \in F[x]$ be a polynomial which is not constant. Then there exists an extension field $F \subseteq E$ and $\alpha \in E$ with $f(\alpha) = 0$.

Ex: $x^2+x+1 \in \mathbb{Z}_2[x]$ has a root in $F_4$.

Ex: $x^2+x+1 \in \mathbb{Q}[x]$ has a root in $\mathbb{C}$.

Basic idea: Choose $p(x)$ irreducible in $F[x]$ with $p(x) \mid f(x)$. Then $\langle p(x) \rangle = I$ is a maximal ideal so $(n = \deg p)$

$$E = F[x]/I$$
$$= \{a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + I \mid a_0, \ldots, a_{n-1} \in F\}$$
$$= \operatorname{span}_F \{1, x, x^2, \ldots, x^{n-1}\} \text{ is a field!}$$

Obviously $x + I \in E$ satisfies $f(x+I) = 0 + I$.

## Algebraic and Transcendental Elements

Def: An element $\alpha \in E \supseteq F$ is algebraic over $F$ if $\exists$ nonzero polynomial $f(x) \in F[x]$ with $f(\alpha) = 0$. An element which is not algebraic is called transcendental.

Special case: $\alpha \in \mathbb{C}$ which is algebraic / $\mathbb{Q}$ is called an algebraic number.

Ex: $\sqrt{2}$, $\sqrt{2}+\sqrt{3}$, $i$ are algebraic #'s

Ex: $\pi, e$ are not algebraic numbers

Open problem: are $\pi+e$, $\pi-e$, or $\pi e$ algebraic?

Let $E$ be an extension field of $F$ and $\alpha \in E$.
If $\alpha$ is algebraic, $\exists f(x) \in F[x]$ with $f(\alpha)=0$.
Let

$$I = \{ f(x) \in F[x] \mid f(\alpha) = 0 \}$$

← maximal ideal!

by Euclidean algorithm, $I = \langle p(x) \rangle$.

Def: If $\alpha$ is algebraic, we define the minimal polynomial of $\alpha$ to be the unique polynomial $p(x) \in F[x]$ satisfying

- $p(x)$ is monic
- $p(\alpha) = 0$
- if $q(x) \in F[x]$ satisfies $q(\alpha)=0$, then $p(x) \mid q(x)$

Notation: $\operatorname{irr}(\alpha, F)$

Ex: $\operatorname{irr}(2, \mathbb{Q}) = x-2$

$\operatorname{irr}(i, \mathbb{Q}) = x^2+1$

$\operatorname{irr}(\sqrt{2}+\sqrt{3}, \mathbb{Q}) = (x^2-5)^2-24$

__Theorem:__ If $\alpha \in E$ is algebraic, then

$$F[\alpha] = \operatorname{img}(\phi_\alpha) = \{ f(\alpha) \mid f(x) \in F[x] \}$$

is a field.

__Proof:__ $I := \ker(\phi_\alpha) = \langle \operatorname{irr}(\alpha, F) \rangle$ so the evaluation morphism descends to the quotient to an isomorphism

$$\begin{tikzcd} F[x] \arrow[r] \arrow[d, "q"'] & F[\alpha] \\ F[x]/I \arrow[ur, "\cong"'] & \end{tikzcd}$$

Thus $F[\alpha] \cong F[x]/I$ and since $I$ is maximal, $F[\alpha]$ is a field.

$\square$

__Def:__ The __subextension field__ $F(\alpha)$ by $\alpha \in E$ is the smallest subfield of $E$ containing $F$ and $\alpha$.

__Theorem:__