Extension Fields

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

$$\begin{tikzcd} \mathbb{C} \arrow[d, dash] \\ \mathbb{R} \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd} \qquad\qquad \begin{tikzcd} & \mathbb{C}(x,y) \arrow[dl, dash] \arrow[dr, dash] & \\ \mathbb{C}(x) \arrow[dr, dash] & & \mathbb{C}(y) \arrow[dl, dash] \\ & \mathbb{C} & \end{tikzcd}$$

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 $(n = \deg p)$

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

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

Algebraic and Transcendental Elements

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

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: π, e are <u>not</u> algebraic numbers

<u>Open problem</u>: are $\pi+e$, $\pi-e$, or πe algebraic?

Let E be an extension field of F and $\alpha \in E$.
If α is algebraic, $\exists\, f(x) \in F[x]$ with $f(\alpha)=0$.
By well-ordering, we can choose $p(x)$ monic with $p(\alpha)=0$ and

$$\deg p(x) = \min\{\deg f(x) \mid f(x) \in F[x],\ f(\alpha)=0\}$$

<u>Def</u>: If α is algebraic, we define the <u>minimal polynomial</u> of α 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 $q(x)=0$ or $\deg q \geq \deg p$.

<u>Notation</u>: $\operatorname{irr}(\alpha, F)$

<u>Ex</u>:

$$\operatorname{irr}(2,\mathbb{Q}) = x-2$$
$$\operatorname{irr}(i,\mathbb{Q}) = x^2+1$$
$$\operatorname{irr}(\sqrt{2}+\sqrt{3},\mathbb{Q}) = (x^2-5)^2-24$$

<u>Theorem</u>: If $\alpha \in E$ is algebraic, then

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

is a field.