Math 5055

Recall: $\mathbb{K}$ is algebraically closed if $\forall f \in \mathbb{K}[x]$ has a root in $\mathbb{K}$.

If $\mathbb{F} \subset \mathbb{K}$ algebraic extension, and if $\forall f \in \mathbb{F}[x]$ has a root in $\mathbb{K}$, then $\mathbb{K}$ is algebraically closed.
In this case, $\mathbb{K}$ is called an algebraic closure of $\mathbb{F}$.

Thm (Assuming axiom of choice) Every field has an alg closure.
And it's unique up to iso — a version of uniqueness of splitting fields.

Pf (Artin): Consider the (massively) infinite polynomial ring

$$\mathbb{F}[\ldots, x_f, \ldots]$$

where there a generator x_f for every $f \in \mathbb{F}[x]$.

Let's look at the ideal $I \subset \mathbb{F}[\dots x_f \dots] = R$

generated by all of the $f(x_f)$

for each $f \in \mathbb{F}[x]$. $\quad I = (\dots f(x_f) \dots)_{f \in \mathbb{F}[x]}$.

$I \neq (0)$

If $\underbrace{I = (1)}_{\hookrightarrow \text{rule out.}}$? Or is $I \subsetneq R$?

Suppose $I = (1)$. i.e. $\exists$ finite set of generators of I and $g_1(\text{other } x_f\text{'s}) \dots g_r(\text{other } x_f\text{'s})$

$f_1(x_{f_1}), \dots, f_r(x_{f_r})$

s.t. $1 = \sum_{i=1}^{r} g_i(x_{f_1'} \dots x_{f_n'}) \cdot f_i(x_{f_i})$

i.e.: If $I = (1)$, then it would be true for some finitely many polys.

$$\begin{array}{ccc} I & \subset & \mathbb{F}[\dots x_f \dots] = R \\ \cup & & \cup \\ 1 \in I' = (\text{just finitely many}). & & \mathbb{F}[x_1, \dots, x_r] = R' \end{array}$$

Choose an extension $\mathbb{F} \subset \mathbb{E}$ in which these finitely many polys have roots.

Choose those roots. Then $R' \longrightarrow \mathbb{E}$

$x_f \longmapsto$ choice of root.

$I' \subseteq \ker(R' \to \mathbb{E})$. This map is nonzero, so $1 \notin I'$. So $1 \notin I$.

So $I \neq (1) \subset R$. $\exists$ maximal ideal $\mathfrak{m} \subset R$.

So, using choice: $I \subset \mathfrak{m} \subset R$

So look at $R/\mathfrak{m}$ some field.

In this field, $[x_f] \in R/\mathfrak{m}$ will solve $f(x_f)=0$.

because $I \subseteq \mathfrak{m}$.

$$\mathbb{F} \subset \underbrace{\qquad\qquad}_{\mathbb{K} := \text{all elts of } R/\mathfrak{m} \text{ algebraic over } \mathbb{F}.} \subset R/\mathfrak{m}$$

$\blacksquare$.

Idea of the pf:

R/I is the univ ring freely built by adding a new root for every poly

e.g.:
$\mathbb{F} = \mathbb{R}$, $\quad R/I \cong \mathbb{R}[x]/_{x^2=1}$.

$\longrightarrow$ either $R/I = 0$. [some inconsistency between freely adding roots] ✗

or R/I has a field among its quotients. ✓

$f \in \mathbb{F}[x]$ is <u>separable</u> if it has no repeated roots in its splitting field.

E.g. $x^2 + 1$ is sep'l over $\mathbb{F} = \mathbb{R}$.

x^2 is not.

Given $f(x)$, let's look in a splitting field $\mathbb{F} \subset \mathbb{E}$

factor $f(x) = \prod (x - a_i)^{d_i}$ in $\mathbb{E}[x]$

all the a_i's are distinct, d_i handles repeated roots.

$d f = \frac{d f(x)}{dx}$

$d(x^n) := n x^{n-1}$ extend linearly.

<u>Algebraic fact</u>: $d(f \cdot g) = df \cdot g + f \cdot dg$.

working in $\mathbb{E}$, if $f = \prod_{i=1}^{k} (x-a_i)^{d_i}$

$$df = \sum_{i=1}^{k} \left(\prod_{j \neq i} (x-a_j)^{d_j} \right) \cdot d_i \cdot (x-a_i)^{d_i - 1}.$$

$\Rightarrow$ iff f has a repeated root, e.g. $d_i \geq 2$ for some i,

then f and df have a common factor $(x-a_i)$

In other words:

f is separable iff $\gcd(f, df) = 1$.

$\mathbb{F}[x]$ $\Downarrow$

Euclid algorithm: $\gcd(f, df)$ is calculable without leaving $\mathbb{F}$.

E.g.: Suppose $f(x) \in \mathbb{F}[x]$ is primitive over $\mathbb{F}$.

Look at:

$\gcd(f, df)$

$\deg(df) < \deg(f)$

Find: If f is primitive, then either

- f is separable

or

- $\underbrace{df = 0}_{}$.

$\hookrightarrow$ possible in positive char.

$f(x) = x^n +$ lower order.

Looks like $df = n x^{n-1} + \dots \overset{?}{\neq} 0$.

Let $\mathbb{F} \subset \mathbb{E}$ be a field extension.

The <u>Galois</u> gp of this extension is

$$\mathrm{Gal}(\mathbb{E}/\mathbb{F}) := \left\{ \begin{array}{l} \text{field autos } \varphi : \mathbb{E} \to \mathbb{E} \\ \text{s.t. } \varphi|_{\mathbb{F}} = id. \end{array} \right\}.$$

Last time: $\mathrm{Gal}(\mathbb{R}/\mathbb{Q}) = \text{triv.}$ $\quad \mathrm{Gal}(\mathbb{Q}[\sqrt{2}, \sqrt{3}]/\mathbb{Q})$

$$\cong (\mathbb{Z}/2)^2.$$

Splitting fields of sep'le polys have larger Galois gps than non-splitting fields.

Given $\mathbb{F} \subset \mathbb{E}$ and given $G < Gal(\mathbb{E}/\mathbb{F})$

can look at the fixed subfield $\mathbb{E}^G := \{ e \in \mathbb{E} \text{ s.t. } ge = e \ \forall g \in G \}$.

$$\begin{array}{c} \mathbb{E}^G \\ \cup\!/ \\ \mathbb{F} \end{array}$$

$$\begin{array}{ccc} \text{subgps of } Gal(\mathbb{E}/\mathbb{F}) & \longrightarrow & \text{subextensions } \mathbb{F} \subset \mathbb{K} \subset \mathbb{E} \\ G & \longmapsto & \mathbb{E}^G. \\ Gal(\mathbb{E}/\mathbb{K}) & \longleftarrow\!\shortmid & \mathbb{K} \end{array}$$

$$
\begin{array}{ccccl}
\mathrm{Gal}(\mathbb{E}/\mathbb{F}) & & & & \\
\cup & & & & \\
G & \longmapsto & \mathbb{E}^G & & \text{fixed for all of } G \\
\cup & & \cap & & \\
H & \longmapsto & \mathbb{E}^H & & \text{fixed just by } H. \\
\cup & & \cap & & \\
\{1\} & \longmapsto & \mathbb{E} & &
\end{array}
$$

In other words, $G \mapsto \mathbb{E}^G$ is an $\overbrace{\text{antimap}}^{\text{contravariant map.}}$ of posets

$$\{\text{subgps of Gal}\} \to \{\text{subfields of } \mathbb{E}\}$$

$$\begin{array}{ccc}
\mathrm{Gal}(\mathbb{E}/\mathbb{F}) & \longleftarrow\!\!\shortmid & \mathbb{F} \\
\cup & & \cap \\
\mathrm{Gal}(\mathbb{E}/\mathbb{K}) = \text{autos of } \mathbb{E} \text{ that fix } \mathbb{K}. & \longleftarrow\!\!\shortmid & \mathbb{K} \\
\cup & & \cap \\
\text{autos of } \mathbb{E} \text{ that fix } \mathbb{L} & \longleftarrow\!\!\shortmid & \mathbb{L} \\
\cup & & \cap \\
\{1\} & \longleftarrow\!\!\shortmid & \mathbb{E}
\end{array}$$

. . . . if $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ is "large" (e.g. $\mathbb{E}$ is a splitting field of a set of sep'le polys) then this will be an equiv contravariant.

So we have contravariant maps

$$\left\{ \begin{array}{c}\text{subgps of} \\ \mathrm{Gal}(\mathbb{E}/\mathbb{F})\end{array} \right\} \rightleftarrows \left\{ \begin{array}{c}\text{sub extensions} \\ \text{of } \mathbb{F} \subset \mathbb{E}\end{array} \right\}.$$