Lecture 26 3/12/2021

Review:

$F \subseteq K$ is an algebraic closure if K is alg. closed and K/F is algebraic.

Last time: for any F, K exists.

Thm. Let $\phi: F \to F'$ be an iso of fields, let $F \subseteq K$ and $F' \subseteq K'$ be alg. closures. Then there is an iso $\theta: K \to K'$ s.t. $\theta|_F = \phi$.

Pf. Take the set of all triples (E, E', ψ)

$F \subseteq E \subseteq K$, $F' \subseteq E' \subseteq K'$, $\psi: E \to E'$ an iso s.t. $\psi|_F = \phi$.

$$\begin{tikzcd}
K \arrow[r, dashed, "\theta"] \arrow[d, dash] & K' \arrow[d, dash] \\
L \arrow[r, "e"] \arrow[d, dash] & L' \arrow[d, dash] \\
E \arrow[r, "\psi"] \arrow[d, dash] & E' \arrow[d, dash] \\
F \arrow[r, "\phi"'] & F'
\end{tikzcd}$$

Put an order on this set where $(E, E', \psi) \leq (L, L', e)$ if $E \subseteq L$, $E' \subseteq L'$, $e|_E = \psi$.

Apply Zorn - note given any chain $\{(E_\alpha, E_\alpha', \psi_\alpha) \mid \alpha \in I\}$ an upper bound is

$(\bigcup E_\alpha, \bigcup E_\alpha', \psi)$. So there is a maximal element (L, L', ρ).

Suppose $L \subsetneq K$. Pick $\alpha \in K / L$ and if $f = \text{minpoly}_L(\alpha) \in L[x]$ take $\rho(f) \in L'[x]$, let α' be a root of $\rho(f)$.

There is an isomorphism

$$L(\alpha) \xrightarrow{\delta} L'(\alpha') \quad \text{s.t.} \quad \delta|_L = \rho.$$

$$\begin{tikzcd} L(\alpha) \arrow[r, "\delta"] & L'(\alpha') \\ L \arrow[u, dash] \arrow[r, "\rho"'] & L' \arrow[u, dash] \end{tikzcd}$$

contradicting maximality since $(L, L', \rho) < (L(\alpha), L'(\alpha'), \delta)$.

So. $L = K$ Now $\rho : K \to L' \subseteq K'$ is an isomorphism. Note L' is alg. closed since K is. Since K'/F' is algebraic, K'/L' is algebraic. Since L' is alg. closed, this forces $K' = L'$.

So $\rho = \theta : K \to K'$ is an isomorphism and $\theta|_F = \phi$.

Cor. if $F \subseteq K$ and $F \subseteq K'$ are alg. closure, then there is an iso $\theta : K \to K'$ s.t. $\theta|_F = 1_F$.

Notation: the alg closure of F is written $\overline{F}$.

Ex. Consider $\overline{\mathbb{F}_p}$ where p is prime.

for each $n \geq 1$ we have a field $\mathbb{F}_{p^n}$

if we consider $\mathbb{F}_p \subseteq \mathbb{F}_{p^n} \subseteq \overline{\mathbb{F}_{p^n}}$

Note $\overline{\mathbb{F}_{p^n}} / \mathbb{F}_p$ is algebraic and $\overline{\mathbb{F}_{p^n}}$ is alg. closed. So $\mathbb{F}_p \subseteq \overline{\mathbb{F}_{p^n}}$ is an alg. closure so $\overline{\mathbb{F}_{p^n}} = \overline{\mathbb{F}_p}$.

So $\mathbb{F}_p \subseteq \mathbb{F}_{p^n} \subseteq \overline{\mathbb{F}_p}$ for all n.

Claim $\overline{\mathbb{F}_p} = \bigcup_n \mathbb{F}_{p^n}$.

Since if $\alpha \in \overline{\mathbb{F}_p}$, if $f = \text{minpoly}_{\mathbb{F}_p}(\alpha)$ has degree n then $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^n}$.

Note $\mathbb{F}_{p^n} = \{\alpha \in \overline{\mathbb{F}_p} \mid \alpha^{p^n} = \alpha\}$.

So $\alpha \in \mathbb{F}_{p^n}$.

Last topic: $\mathbb{C}$.

Fact: $\mathbb{C}$ is alg. closed – many proofs.

This is the most "algebraic" proof.

It uses only.

<u>Lemma.</u>

① If $f \in \mathbb{R}[x]$ and f has odd degree, then f is a root in $\mathbb{R}$.

② If $g \in \mathbb{C}[x]$ and $\deg g = 2$ then g splits over $\mathbb{C}$.

Pf. ① Replace f by $-f$ if necessary

so $f = a_n x^n + \cdots + a_0$ with $a_n > 0$

Then $\lim_{x\to\infty} f = \infty$, $\lim_{x\to -\infty} f = -\infty$.

Use intermediate value thm.

② if $f = ax^2 + bx + c \in \mathbb{C}[x]$.

$f = a(x - r_1)(x - r_2)$

where r_1, r_2 are $\dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$

where every $z \in \mathbb{C}$ has a square root

since if $z = re^{i\theta}$ with $r \geq 0$

then $\sqrt{z} = \sqrt{r}\, e^{i\frac{\theta}{2}}$.

Need: positive reals have a square root.

Thm. $\mathbb{C}$ is alg. closed.

Pf. Let $\mathbb{C} \subseteq L$ be an extension

with $[L : \mathbb{C}] < \infty$. We'll prove $L = \mathbb{C}$.

$\mathbb{R} \subseteq \mathbb{C} \subseteq L$.

Look $L/\mathbb{R}$. Maybe not Galois, but it is separable. Let $L \subseteq E$ be a Galois closure so $E/\mathbb{R}$ is Galois.

$\mathbb{R} \subseteq \mathbb{C} \subseteq L \subseteq E$. $\quad G = \mathrm{Gal}(E/\mathbb{R})$.

Let P be Sylow 2-subgroup. So $[G:P]$ is odd. Let $K = \mathrm{Fix}(P)$.

$\mathbb{R} \subseteq K \subseteq E \quad [K:\mathbb{R}] = [G:P]$

is odd.

If $\alpha \in K$, $\mathrm{minpoly}_{\mathbb{R}}(\alpha)$ has odd degree because it divides $[K:\mathbb{R}]$. So it is a root in $\mathbb{R}$, and it is irreducible over $\mathbb{R}$, so it has degree 1. So $K = \mathbb{R}$. And $P = G$.

So $|G|$ is a power of 2.

$\mathbb{R} \subseteq \mathbb{C} \subseteq E$ now $[E:\mathbb{C}] = [E:\mathbb{R}]/2$ is also a power of 2.

$\mathrm{Gal}(E/\mathbb{C})$ is a 2-group so it has a subgroup of index 2. H.

Then $\mathrm{Fix}(H) = M$ has $[M:\mathbb{C}] = [\mathrm{Gal}(E/\mathbb{C}):H] = 2$.

$\underbrace{\mathbb{C} \subseteq M}_{2}$ now if $\alpha \in M$ then

$\mathrm{minpoly}_{\mathbb{C}}(\alpha)$ has degree 1 or 2 but it splits by the lemma. So $\alpha \in \mathbb{C}$. So $M = \mathbb{C}$, a contradiction.

So $\mathbb{C}$ is algebraically closed.

An interesting fact about $\mathbb{C}$.

$\mathrm{Aut}(\mathbb{R}) = 1$ (exercise)

But $\mathrm{Aut}(\mathbb{C})$ is huge!

This uses the idea of a transcendence basis:

Given any field extension $F \subseteq K$ you can find a set $\{y_\alpha \mid \alpha \in I\} \subseteq K$ which is a transcendence basis:
$\{y_\alpha\}$ is algebraically independent:
$T = F(y_\alpha \mid \alpha \in I) \cong$ field of fractions of $F[y_\alpha \mid \alpha \in I]$. and $T \subseteq K$ is algebraic.
(exists by Zorn)

Note: the cardinality of a transcendence basis is uniquely determined.

Apply this to $\mathbb{Q} \subseteq \mathbb{C}$.

So $\mathbb{Q} \subseteq T = \mathbb{Q}(y_\alpha \mid \alpha \in I) \subseteq \mathbb{C}$.

Now given a permutation of I, we get an automorphism of T that permutes the y_α this way. Then since $\mathbb{C}$ is the alg. closure of T this extends to an aut. of $\mathbb{C}$.

So $\mathrm{Sym}(I)$ embeds in $\mathrm{Aut}(\mathbb{C})$

And I is uncountable.

$|\mathrm{Sym}(I)|$ has an even bigger cardinality than I.

One can show: any such automorphism is discontinuous and sends $\mathbb{R}$ to a dense subset of $\mathbb{C}$.