Lecture 26  3/12/2021

Review:

- \( F \subseteq K \) is an algebraic closure if
- \( K \) is algebraically closed and \( K/F \) is algebraic.

Last time: for any \( F, K \) exists.

Thus, let \( \varphi: F \to F' \) be an iso of fields

Let \( F \subseteq K \) and \( F' \subseteq K' \) be alg. closures.

The claim is an iso \( \Theta: K \to K' \) s.t.

\[ \Theta \varphi = \varphi. \]

Pf: Take the set of all triplets \((E, E', \psi)\)

\( E \subseteq E' \subseteq K \), \( E' \subseteq E' \subseteq K' \), \( \psi: E \to E' \)

an iso s.t. \( \psi|_{F} = \varphi. \)

\( k \rightarrow k' \)

Put an order on this set where

\( (E, E', \psi) \leq (E, E', \psi') \) if

\( E \subseteq L, E' \subseteq L', E|_{L} = \psi. \)
Apply Ben - not given any claim $\{(E_k, E'_k, \psi_k) \mid k \in I\}$ a upper bound is $\{UE_k, UE'_k, \psi\}$. So there is a maximal element $(L, L', \psi)$.

Suppose $L \neq L'$. Pick $k \in \mathbb{L}/\mathbb{L}$ and if $\mathfrak{m} \in \mathfrak{m}(L' \cap k) \neq \emptyset$ take $\mathfrak{m} \in L' \cap k$, let $p'$ be a root of $\mathfrak{m}(L')$. There is an isomorphism $L \xrightarrow{\psi} L'$ s.t. $p' \in L' \cap L$.

Contradicting maximality since $L \rightarrow \mathfrak{m}(L') \xrightarrow{\psi} L' \cap \mathfrak{m}(L')$. So $L = L'$. Now $E : K \rightarrow L' \subseteq K'$ is an isomorphism. Note $L'$ is alg. dom. since $K'$ is. Since $K'/P'$ is algebraic, $K'/L'$ is algebraic. Since $L' \subseteq K'$ is alg. dom., this forces $K' = L'$.

So $E = \Theta : K \rightarrow K'$ is an isomorphism.
and $\mathfrak{B} \mid F = \mathfrak{F}$.

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

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

Ex. Consider $\overline{F_p}$ where $p$ is prime.

for each $n \geq 1$, we have a field $\overline{F_p}$

if we consider $\overline{F_p} \leq \overline{F_p^n} \leq \overline{F_p}$

Note $\overline{F_p^n} / \overline{F_p}$ is algebraic and $\overline{F_p^n}$
is alg. closed. So $\overline{F_p} \leq \overline{F_p^n}$ is an alg. closure to $\overline{F_p^n} = \overline{F_p}$.

So $\overline{F_p} \leq \overline{F_p^n} \leq \overline{F_p}$ for all $n$. 
Claim $\mathbb{F}_p = \bigcup_{n} \mathbb{F}_{p^n}$.

Since if $x \in \mathbb{F}_p$, if $f(x)$ is in every $\mathbb{F}_p(d)$ has degree $n$, then $\mathbb{F}_p(d) = \mathbb{F}_{p^n}$.

Note $\mathbb{F}_{p^n} = \{x \in \mathbb{F}_p \mid x^{p^n} = x^3\}$.

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

---

**Last topic: $\mathbb{C}$**

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

This is the most "algebraic" proof.

It uses only.

**Lemma.**

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 $\mathbb{C}$. 
Ps. If \( D \) is closed, let \( f \) by \(-f\) if necessary

\[ f = a_n x^n + \ldots + a_0 \text{ with } a_n > 0 \]

The limit \( \lim_{x \to -\infty} f = \infty \), \( \lim_{x \to \infty} f = -\infty \).

Use intermediate value thm.

\[ \exists \] if \( f: a x^2 + b x + c \in C(x) \),

\[ f = a(x - r_1)(x - r_2) \]

where \( r_1, r_2 \) are \( -b \pm \sqrt{b^2 - 4ac} \) \( \frac{2a}{2a} \)

where every \( z \in C \) has a square root.

since if \( t = r e^{i\theta} \) with \( r > 0 \)

then \( \sqrt{t} = \sqrt{r} e^{i\theta/2} \).

Next: positive reals have a square root.

Then, \( C \) is alg. closed.

Ps: Let \( C \subseteq \mathbb{L} \) be an extension with \( C_1 : C \subseteq \infty \). We'll prove \( L = C \).
$R \leq G \leq L$.

Look at $L/R$. Maybe not locally, but it is separable. Let $L/E$ be a locally algebraic to $E/R$ is locally.

$R \leq G \leq L \leq E$. $6 = \text{Gal}(E/R)$.

Let $P$ be the second $2$-subgroup. So $[6; P]$ is odd. Let $K = \text{Fix}(P)$.

$R \leq K \leq G$. $[K : R] = [6 ; P]$ is odd.

If $x \in K$, uniquely $\alpha(x)$ has odd degree because it divides $[K : R]$.

So it is a root in $R$, and it is invertible over $R$, so it has degree $1$. So $K = R$. And $P = G$.

So $|6|$ is a power of $2$. 
\[ R \leq G \leq E \] now \( [E:C] = [E:N]/2 \) is also a power of 2.

\( \text{mod}(E/C) \) is a 2-group so it has a subgroup of index 2. \( H \).

The \( \text{Fix}(H) = M \leq C \) and \( [C:G] = \left[ \text{mod}(E/C): H \right] = 2 \).

\[ G \subseteq M \] now if \( d \in M \) then

\[ \text{index}(C(d)) \text{ has degree } 1 \text{ or } 2 \]

but it splits by the lemma. So \( d \in G \). So \( H = C \), a contradiction.

So \( G \) is algebraically closed.

\[ \text{An interesting fact about } G. \]
\[ \text{Aut}(R) = 1 \) (exercise) \]

But \( \text{Aut}(G) \) is huge!
This was the idea of a transcendental basis:

Given any field extension \( F \subseteq K \), you can find a set \( \{ y_a | a \in \mathbb{I} \} \subseteq K \) which is a transcendental basis:

\( \{ y_a \} \) is algebraically independent:

\[ T = F(\{ y_a \}_{a \in \mathbb{I}}) \supseteq \text{field of fractions of } F[\{ y_a \}_{a \in \mathbb{I}}], \text{ and } T \subseteq K \]

is algebraic.

(Left as an exercise)

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

Apply this to \( \mathbb{Q} \subseteq \mathbb{C} \).

So \( \mathbb{Q} \subseteq T = \mathbb{Q}(\{ y_a | a \in \mathbb{I} \}) \subseteq \mathbb{C} \).
Now give a permutation of \( I \), we get an automorphism of \( T \) that permutes the \( \mathbb{I} \) in this way. Then since \( C \) is the alg. closure of \( T \) this extends to an aut. of \( C \).

6. \( \text{Sym}(I) \) embeds in \( \text{Aut}(C) \).

And \( I \) is uncountable.

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

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