MATH5725: Galois Theory (S2,2014)
Lecture 3

Here's an example of a splitting field and a field which splits:
The field $\mathbf{Q}(i,\sqrt{2})$ splits $X^2+1 \in \mathbf{Q}[X]$ but is not generated by the roots f X^2+1. However the field $\mathbf{Q}(i)$ is generated by the roots of X^2+1 and splits X^2+1. The field $\mathbf{Q}(\sqrt[3]{2})$ is not a splitting field for $X^3-2 \in \mathbf{Q}[X]$ as it does not contain all of the roots of $\mathbf{Q}(\sqrt[3]{2})$. The motto is "splitting fields contain all the roots of the polynomial they split and are generated by the roots of the polynomial they split".

In general the existence of splitting fields is a slightly subtle question of algebra. You should have already seen the

Proposition 1. *Let $f \in k[X]$. A splitting field for K/k exists.*

Proof. The proof is by induction on the degree n of f. If $n=1$, then f is linear and so k is a splitting field for f. We now assume the inductive hypothesis applies to $n-1$, i.e. given a polynomial $f' \in k'[X]$ of degree $n-1$ there exists a splitting field K'/k' for f'. Let f_1 be an irreducible factor of f and consider quotient ring $E = k[\beta]/(f_1(\beta))$. E is a field. Let $\psi : k \longrightarrow E$ be the ring homomorphism given by $\lambda \mapsto \lambda \cdot 1$. If we identify k with its image in E we have that E/k is a field extension and that f factors in $E[X]$ as

$$f(X) = (X-\beta)g(X)$$

where $g(X) \in E$ has degree $n-1$. Moreover $E = k(\beta)$. By the inductive hypothesis applied to g and E there is a splitting field E' for g, that is $E' = E(\alpha_1, \cdots, \alpha_{n-1})$ with $g(\alpha_i) = 0$ for each i. By construction $E = k(\beta, \alpha_1, \cdots, \alpha_n)$ is a splitting field for f.
This is the idea of the proof, however to be careful we should not identify k with its image in E. We construct a field extension k'/k by the following process: as a set $k' = k \cup E \backslash \psi(k)$; the field structure of k' is induced by the map ψ' given by

$$\psi'(x) = \begin{cases} x & \text{if } x \in E \\ \psi(x) & \text{if } x \in k. \end{cases}$$

Then $f(X)$ factors as $f(X) = (X-\beta)g(X)$ in $k'[X]$ and by the inductive hypothesis there is a splitting field K/k'. The rest of the argument is the same. □

Splitting fields are unique up to non-unique isomorphism (this is perhaps the core idea behind Galois theory). For example in the case of $\mathbf{Q}(\sqrt{D})$ with $D \in \mathbf{Q}$ non-square, there are two automorphisms of $\mathbf{Q}(\sqrt{D})/\mathbf{Q}$ namely the identity and the map given by $\sigma(\sqrt{D}) = -\sqrt{D}$ and $\sigma(a) = a$ if $a \in \mathbf{Q}$ (σ is "conjugation"). Thus if $K/\mathbf{Q}$ is any splitting field for $X^2 - D$ and if $\psi : \mathbf{Q}(\sqrt{D}) \longrightarrow K$ is a $\mathbf{Q}$-linear isomorphism we have a second isomorphism $\psi \circ \sigma$ which is distinct from ψ.

Here is another useful example:
the field $k = \mathbf{Q}(\sqrt[3]{2})$ and $k' = \mathbf{Q}(\sqrt[3]{2}e^{\pi i/3})$ are isomorphic; the polynomial $X^3 - 2$ can be considered an element of either $k[X]$ or $k'[X]$. The fields $K = k(e^{2\pi i/3})$ and $K' = k'(e^{2\pi i/3})$ are also isomorphic and split $X^3 - 2$. If we fix an isomorphism:

$$\psi : K \longrightarrow K' : \sqrt[3]{2} \mapsto \sqrt[3]{2}e^{2\pi i/3}, e^{2\pi i/3} \mapsto e^{2\pi i/3}$$

then ψ_k is an isomorphism between k and k'. Any other isomorphism ϑ which restricts to ψ_k has to send $e^{2\ pii/3}$ to a third root of unity. So there are exactly two possibilities for ϑ.

In general we have

Proposition 2. *1. Let K/k and L/k be splitting fields for $f \in k[X]$. Then there is a k-linear isomorphism $\psi : K \longrightarrow L$.*
2. Let K/k and K'/k' be splitting fields for $f \in k[X]$ and $f' \in k'[X]$ respectively. Assume given an isomorphism $\psi : k \longrightarrow k'$ such that $\psi(f) = f'$. Then there exists an isomorphism

$\Psi : K \longrightarrow K'$ *extending* ψ.
3. Let $\psi : k \longrightarrow k'$ *be as in 2 and let*

$$\mathrm{Iso}_\psi(K/k, K'/k') = \{\Psi : K \longrightarrow K' \mid \Psi(a) = \psi(a) \text{ for } a \in k\}$$

then $\mathrm{Iso}_\psi(K/k, K'/k')$ *is finite and has cardinality* n *such that* $1 \leq n \leq [K : k]$. *In particular*

$$\mathrm{Aut}(K/k) = \{\sigma : K \longrightarrow K \mid \sigma(a) = a \text{ for } a \in k\}$$

has cardinality $n \leq [K : k]$. *The cardinality* n *is equal to* $[K : k]$ *if the irreducible factors of* f *splits as a product of distinct linear factors in* $K[X]$.

Proof. Clearly parts 1 and 2 are consequences of part 3.
We proceed by induction on the degree n of f. If $n = 1$ then f is a product of linear factors in $k[X]$, and in this case $K = K' = k$ and any such Ψ is in fact ψ.
Assume, by induction, that part 3 holds for $n-1$, i.e. that if L/E and L'/E' are splitting fields for polynomials $g \in E[X]$ and $g'E'[X]$ of degree $n-1$ and an isomorphism $\varphi : E \longrightarrow E'$ is given such that $\varphi'(g) = g'$ then the set $\mathrm{Iso}_\varphi(L/E, L'/E')$ has cardinality $n-1$.
Let f_1 be an irreducible factor of f of degree n_1. Let $\alpha \in K$ be a root of f_1. Then $\psi(f_1)$ is an irreducible factor of $\psi(f)$ and splits as a product of linear factors, $(X - \beta_1), \cdots, (X - \beta_{n_1})$ in $K'[X]$. For each β_i we have an extension φ_i of ψ to a map from $k(\alpha)$ to $k'(\beta_i)$ given by $\varphi_i(\alpha) = \beta_i$. Now the inductive hypothesis applies to $\mathrm{Iso}_{\varphi_i}(K/k(\alpha), K'/k'(\beta_i))$ which therefore has cardinality $[K : k]/n_1$ as $[K : k(\beta)][k(\beta) : k] = [K : k]$. There are at most n_1 different choices of lift φ_i and for each φ_i (with exactly n_1 if the β_i are distinct) and there are at most n/n_1 choices (with equality if the irreducible factors of f/f_1 splits as a product of distinct linear factors in $K[X]$) of lift to Ψ. Therefore $\mathrm{Iso}_\psi(K/k, K'/k')$ has cardinality $\leq [K : k]$, with equality if f splits as a product of distinct linear factors in $K[X]$. □

Remark[1]
In the proof above we constructed a $\varphi_i : k(\alpha) \longrightarrow k'(\beta_i)$, extending $\psi : k \longrightarrow k'$ and showed that φ_i extended to an isomorphism $\Psi : K \longrightarrow K'$ by induction. There were at most $\deg(f_1)$ choices for φ_i and by induction at most $[K : k]/\deg(f_1)$ choices for Ψ (with equality if the roots of the irreducible factors of f have distinct roots). So Ψ, φ_i and ψ all fit into a commutative diagram (where the vertical arrows are field inclusions):

$$\begin{array}{ccc} K & \xrightarrow{\Psi} & K' \\ \uparrow & & \uparrow \\ k(\alpha) & \xrightarrow{\varphi_i} & k(\beta_i) \\ \uparrow & & \uparrow \\ k & \xrightarrow{\psi} & k' \end{array}$$

Thus Ψ is really an element of $\mathrm{Iso}_\psi(K/k, K'/k')$ and moreover an element of this set defines an isomorphism φ_i between $k(\alpha)$ and $k(\beta_i)$ for some β_i (by restricting Ψ to $k(\alpha)$ because $\Psi(\alpha)$ has to be equal to one of the β_i) as well as an isomorphism $\mathrm{Iso}_{\varphi_i}(K/k(\alpha), K'/k'(\beta_i))$. In other words we have a bijection

$$\mathrm{Iso}_\psi(K/k, K'/k') \to \bigcup_{\varphi_i : k(\alpha) \longrightarrow k(\beta_i)} \mathrm{Iso}_{\varphi_i}(K/k(\alpha), K'/k'(\beta_i)).$$

Example where $\mathrm{Aut}(K/k)$ **is trivial but** $[K : k] > 1$ Let $\mathbf{F}_2$ be the field with 2 elements, i.e. $\mathbf{Z}/2$. Let $k = \mathbf{F}_2(u, v)$, i.e. the function field in two indeterminates u and v. Let $K = k(\sqrt{u}, \sqrt{v})$. Then if $\sigma : K \longrightarrow K$ is a field automorphism such that $\sigma(a) = a$ for $a \in k$ we have $\sigma(\sqrt{u})^2 = u$ and $\sigma(\sqrt{v})^2 = v$. Which means $\sigma(\sqrt{u}) = \sqrt{u}$ and $\sigma(\sqrt{v}) = v$ as $-1 = 1$!
However $k(\sqrt{u})$ has dimension 2 of k as $\sqrt{u} \notin k$ and likewise K has dimension 4 over $k(\sqrt{u})$ as $\sqrt{v} \notin k(\sqrt{u})$. I.e. $[K : k] = 4$.

[1]Not in the original lecture, but I'll mention it briefly next time.

The essential reason for failure is that K is the splitting field of the polynomial $(X^2 - u)(X^2 - v)$ which has degree 4 but only two distinct roots in K.

This example is particularly interesting as K/k has infinitely many intermediate quadratic subfields (in complete contrast to the example of lecture 1 where there were exactly 3 intermediate subfields all corresponding to subgroups of the Klein group). Indeed if $\lambda \in K$ then $\alpha_\lambda = \sqrt{u} + \lambda\sqrt{v}$ is quadratic as $\alpha_\lambda^2 = u + \lambda^2 v \in k$. And the fields $k(\alpha_{\lambda_0})$ and $k(\alpha_{\lambda_1})$ are equal only if

$$\sqrt{u} + \lambda_0\sqrt{v} = a + b(\sqrt{u} + \lambda_1\sqrt{v})$$

with $a, b \in k$. This implies that (by using the k-basis elements $1, \sqrt{u}, \sqrt{v}, \sqrt{uv}$ of K) $b = 1$ and $b\lambda_1 = \lambda_0$, i.e. $\lambda_1 = \lambda_0$.
We will revisit this example when proving the primitive element theorem.

Basically classical Galois theory can not do much for the the field K/k - $\mathrm{Aut}(K/k)$ is trivial but K/k has infinitely many intermediate subfields. So the subgroups of $\mathrm{Gal}(K/k)$ do not and can not classify the intermediate subfields of K/k.