MATH 552 NOTES – LECTURE 3

Splitting fields: If K is a field and $f \in K[t]$ is monic, a *splitting field* of f over K is an extension field F such that (i) in $F[x]$, $f(t)$ is a product of linear terms $t - r_i$, and (ii) F is generated over K by the roots r_i of f.

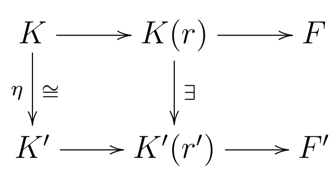
For example, $f(t) = t^3 - 1$ is the product $(t-1)(t-\omega)(t-\omega^2)$ in $\mathbb{C}[t]$, and $F = \mathbb{Q}(\omega)$ is a splitting field of f over $\mathbb{Q}$. However, $\mathbb{F}_3$ is already a splitting field for $t^3 - 1$ over $\mathbb{F}_3$, because $f(t) = (t-1)^3$ in $\mathbb{F}_3[t]$.

Proposition 1. *Every monic polynomial f in $K[t]$ has a splitting field F, and $[F : K] \leq n!$, $n = \deg(f)$.*

Proof. We proceed by induction on $d = \deg(f)$, the case $d = 1$ being clear. Factor f as a product of irreducible polynomials f_i, and form the field $E = K[t]/(f_1)$, with r_1 the image of t. The monic polynomial $g(t) = f(t)/(t - r_1)$ has degree $(d-1)$ so there is a splitting field F of g over E. Then $g = \prod_2^d (t - r_i)$ in $F[t]$ so $f = (t - r_1)g$ is a product of linear terms. Finally, $[F : K] = [F : E][E : K] \leq \deg(f_1)\deg(g) \leq \deg(f)!$. □

We now consider the following situation. Let $K \xrightarrow{\eta} K'$ be a field isomorphism; it induces a ring isomorphism $K[t] \to K'[t]$ sending $f(t) = \sum a_i t^i$ to $f'(t) = \sum \eta(a_i) t^i$. The following Lemma is elementary. (**why?**)

Lemma 2. *Let F and F' be field extensions of K and K', respectively. If $r \in F$ is algebraic over K, with minimum polynomial $f(t)$, then the extensions of η to a field map $K(r) \to F'$ are in 1–1 correspondence with the roots of $f'(t)$ in F'. In particular, an extension exists if and only if $f'(t)$ has a root in F'.*



Date: Feb. 4, 2025.

Theorem 3. *Let* $K \xrightarrow{\eta} K'$ *be a field isomorphism,* F *a splitting field of a monic polynomial* $f(t) \in K[t]$*, and* F' *a splitting field of the corresponding monic polynomial* $f'(t) \in K'[t]$*. Then* η *can be extended to an isomophism* $F \xrightarrow{\cong} F'$ *between the respective splitting fields* F *and* F'*.*

Proof. We proceed by induction on $[F : K]$. If $F = K$, $f = \prod(t - r_i)$ in $K[t]$ and $f' = \prod(t - \eta(r_i))$, so $F' = K'$ and $F \cong F'$ is just η. Otherwise, f has an irreducible monic factor $g(t)$ of degree ≥ 2, and f' has an irreducible monic factor $g'(t)$. By assumption, all the roots r_i of f are in F, and all the roots s_i of f' are in F'. By re-indexing the roots, g is the minimal polynomial of r_1 in $K[t]$ and g' is the minimal polynomial of s_1 in $K[t]$.

Set $E = K(r_1)$ and $E' = K'(s_1)$. Then $[E : K]$ is the number of roots of f in F, and $[E' : K']$ is the number of roots of f' in F'. By definition, F is a splitting field of f over E, and F' is a splitting field of f' over E'. By induction, $E \xrightarrow{\cong} E'$ extends to an isomorphism $F \xrightarrow{\cong} F'$. □

Porism. If all the roots of f in F are distinct, then the number of extensions of η to an isomorphism $F \cong F'$ is $[F : K]$, and is at most $\deg(f)!$. (**why?**) A careful study of the induction step in the proof shows that the number of extensions is at most the number of roots of f.

Corollary 4. *If* F *is a splitting field of* f *over* K*, then* $\mathrm{Gal}(F/K)$ *has at most* $[F : K]$ *elements. If the roots of* f *are distinct and* f *is irreducible, then* $|\mathrm{Gal}(F/K)| = [F : K]$*.*

Proof. Take $K = K'$, $F = F'$, and use the Porism. □

Example 5. (i) $\mathbb{C}$ is the splitting field of $t^8 - 1$ over $\mathbb{R}$, and $[\mathbb{C} : \mathbb{R}] = 2$. This shows that $|\mathrm{Gal}(F/K)|$ can be less than $\deg(f)$.
(ii) If $\mathrm{char}(K) = p$ and $f(t) = t^p - 1 = (t-1)^p$, then $F = K$.

Separable and inseparable extensions: The previous porism and example show that multiple roots are problematic.

Definition 6. A monic polynomial $f(t)$ is *separable* (over K) if it has distinct roots in some (hence any) splitting field. An element u in some finite exension of K is *separable* over K if its minimal polynomial is separable. We say F/K is separable if every element of F is separable over K.

If $f(t) = \sum a_i t^i$, the *derivative* $f'(t) = \sum i a_i t^{i-1}$ makes sense and satisies the usual product rule. If $(t-a)^2$ divides f then $(t-a)$ also divides $f'(t)$. Conversely, if $(t-a)$ divides both f and f' then $(t-a)^2$ divides f. (**why?**)

Theorem 7. *Let $f(t) \in K[t]$ be irreducible and F its splitting field. Then the following are equivalent:*
1) f is separable over K;
2) f factors into distinct linear factors in $F[t]$
3) $f' \neq 0$ in $K[x]$.

Proof. That 1) is equivalent to 2) is a tautology. If $f' = 0$ and a is a root of f, then $f(a) = f'(a) = 0$ so $t - a$ divides f and f'. Hence 2) implies 3). To see that 3) implies 2), notice that, because f is irreducible, if $f' \neq 0$ then $\deg(f') < \deg(f)$ and hence $\gcd(f, f') = 1$. Thus $(t-a)^2$ cannot divide f in $F[t]$; otherwise $(t - a)$ would divide both f and f'. □

Remark 8. If $\mathrm{char}(K) = 0$, every field extension is separable, because f' is never zero (unless f is constant). If $\mathrm{char}(K) = p$, $f' = 0$ iff $f(t) = g(t^p)$ for some polynomial $g(t)$. Thus inseparability is only a problem in characteristic $p > 0$.

Perfect fields: A field K is said to be *perfect* if every polynomial in $K[t]$ is separable. Every field of characteristic 0 is perfect.

Lemma 9. *A field K of characteristic $p > 0$ is perfect iff the Frobenius $\varphi : K \to K$ is an isomorphism.*

Proof. If $a \notin \varphi(K)$ then $f(t) = t^p - a$ is irreducible (**why?**), and inseparable because $f' = 0$, so K is not perfect. If φ is an isomorphism and $f(t) \in K[t]$ is irreducible and inseparable then $f(t) = \sum a_n t^{np}$; but $a_n = \varphi(b_n)$ for some $b_n \in K$ and hence $f(t) = (\sum b_n t^n)^p$, a contradiction. □

Corollary 10. *Every finite field K is perfect.*

Indeed, $\varphi : K \to K$ is an injection, hence a bijection.

Example 11. Since K is obtained from K^p by adjoining all p^{th} roots of elements, it makes sense to write $K^{p^{-1}}$ for the field obtained from K by adjoining all p^{th} roots of elements. Thus $K \subseteq K^{p^{-1}}$, and the Frobenius is an isomorphism $K^{p^{-1}} \xrightarrow{\wp} K$.

The *perfect closure* of K is the union $K^{p^{-\infty}}$ of the sequence of fields

$$K \subseteq K^{p^{-1}} \subseteq K^{p^{-2}} \subseteq \cdots \subseteq K^{p^{-n}} \subseteq \cdots$$

By construction, $K^{p^{-\infty}}$ is a perfect field.