3. Normal and separable field extensions

<u>Observation</u>: Over fields of characteristic $p>0$, it is possible for an irreducible polynomial to have multiple roots in an extension field.

<u>Example</u>: Let $F=\mathbb{Z}_2(t)$, and $f(x)=x^2+t\in F[x]$, which is irreducible by Eisenstein.

By Prop 1.8, $f(x)$ has a root (call it $\sqrt{t}$) in an extension field K. In $K[x]$, $(x-\sqrt{t})^2 = x^2-2\sqrt{t}\,x+t = x^2+t$, so $\sqrt{t}$ is a root of multiplicity 2.

<u>Remark</u>: This holds for any prime $p>0$. If char $F=p>0$, then:

(1) $(a+b)^p=a^p+b^p$ and $(a-b)^p=a^p-b^p$ for all $a,b\in F$.

(2) $f(x)\in x^p-t\in F(t)[x]$ has one root with multiplicity p in any splitting field.

<u>Pf</u>: Exercise.

<u>Def</u>: An irreducible polynomial $f(x)\in F[x]$ is <u>separable</u> if $f(x)$ has distinct roots in a splitting field.

A polynomial $f(x)\in F[x]$ is <u>separable</u> if each of its irreducible factors is separable.

If $f(x)=a_0+a_1x+\dots+a_nx^n\in F[x]$, then the <u>derivative</u> of $f(x)$ can be defined formally as $f'(x)=a_1+2a_2x+\dots+na_nx^{n-1}$.

<u>Exercise</u> (easy): The derivative of $f(x)+g(x)$ is $f'(x)+g'(x)$, and the derivative of $f(x)g(x)$ is $f(x)g'(x)+f'(x)g(x)$.

<u>Prop 3.1</u>: If $f(x) \in F[x]$ and $\deg f(x) > 0$, then $f'(x) = 0$ iff $\operatorname{char} F = p > 0$ <u>and</u> $f(x) = g(x^p)$ for some $g(x) \in F[x]$.

<u>Pf</u>: Exercise (easy).

<u>Prop 3.2</u>: Suppose $f(x) \in F[x]$ and $\deg f(x) > 0$. Then

(1) If $f'(x) = 0$, every root of $f(x)$ has multiplicity ≥ 2

(2) If $f'(x) \neq 0$ and $(f(x), f'(x)) = 1$, then $f(x)$ has no repeated roots in an extension field.

<u>Pf</u>: (1) Say $a \in K$ is a root of $f(x)$.

Write $f(x) = (x-a)\,g(x)$

$$f'(x) = g(x) + (x-a)\,g'(x) = 0$$

$$f'(a) = g(a) + (a-a)\,g'(a) = 0$$

$$\Rightarrow g(a) = 0 \Rightarrow (x-a) \mid g(x) \Rightarrow (x-a)^2 \mid f(x). \checkmark$$

(2) Suppose for sake of contradiction that $a \in K$ was a root of multiplicity ≥ 2.

Write $f(x) = (x-a)^2 g(x)$

$$f'(x) = 2(x-a)\,g(x) + (x-a)^2 g'(x) \Rightarrow a \text{ is a root of } f'(x).$$

Since $(f(x), f'(x)) = 1$, we can write

$$h(x)f(x) + k(x)f'(x) = 1 \text{ for some } h(x), k(x) \in F[x].$$

$$\Rightarrow 0 = h(a)f(a) + k(a)f'(a) = 1 \quad ↯ \quad \square$$

<u>Cor 1</u>: If $f(x) \in F[x]$ is irreducible, then $f(x)$ is separable iff $f'(x) \neq 0$.

<u>Cor 2</u>: If $\operatorname{char} F = 0$, then every polynomial in $F[x]$ is separable.

* <u>Cor 3</u>: If $f(x)$ is not separable, then $f(x) = h(x^{p^k})$ for some <u>separable</u> $h(x)$.

Def: If $a \in K$ is algebraic over F, then a is <u>separable</u> if its minimal polynomial $m_{a,F}(x)$ is separable. An extension K/F is separable if every $a \in K$ is separable over F.

Prop 3.3: Suppose K is a splitting field for some $\mathcal{F} \subseteq F[x]$, that $f(x) \in F[x]$ is separable and irreducible of degree $n > 0$, and that $f(x)$ splits over K.

(a) If $a \in K$ is a root of $f(x)$ and $G = Gal(K/F)$, then $\{\phi(a) : \phi \in G\}$ is the set of roots of $f(x)$.

(b) If $L = F(a)$, and $H = \mathcal{G}L \leq G$, then $[G:H] = n$ and if $\{\phi_1, \dots, \phi_n\}$ is a complete set of coset representatives for H in G, then $\{\phi_1(a), \dots, \phi_n(a)\}$ are all the roots of $f(x)$.

Pf: (a) If $f(x) = \sum_{i=0}^{n} a_i x^i$, then $\phi(f(x)) = \sum_{i=0}^{n} a_i \phi(x^i) = \sum_{i=0}^{n} a_i \phi(x)^i = f(\phi(x))$

Thus $\phi f(c) = f\phi(c)$ for any $c \in K$, and so if $a \in K$ is a root of $f(x)$, so is $\phi(a)$.

(i.e, G acts on the set of roots of $f(x)$).

Let $b \in K$ be another root.

Cor to Prop 1.9 $\Rightarrow \exists\, \theta : F(a) \to F(b)$, $\theta(a) = b$

Thm 1.11 $\Rightarrow \theta$ extends to $\phi \in G$, $\phi(a) = \phi(b)$. ✓

(b) Clearly, $Stab_G(a) = \mathcal{G}L = H$, so $\exists\ [G:H]$ distinct roots of $f(x)$ (Orbit-Stabilizer thm).

$f(x)$ is separable & irreducible $\Rightarrow [G:H] = \deg f(x) = n$.

If $i \neq j$ then $\phi_i a = \phi_j a \Rightarrow \phi_j^{-1}\phi_i a = a$

$\Rightarrow \phi_j^{-1}\phi_i \in Stab_G(a) = H \Rightarrow \phi_i H = \phi_j H$. ↯ ✓ □

Thm 3.4: If K/F is algebraic, then the following are equivalent:

(a) K/F is Galois

(b) K is a separable splitting field for some $\mathcal{F}_1 \subseteq F[x]$.

(c) K is a splitting field for some set $\mathcal{F}_2 \subseteq F[x]$ of separable polynomials.

Pf: (a) $\Rightarrow$ (b): Put $\mathcal{F}_1 = \{ m_a(x) : a \in K \}$

Thm 2.8 $\Rightarrow$ each $m_a(x)$ splits & has distinct roots in K. ✓

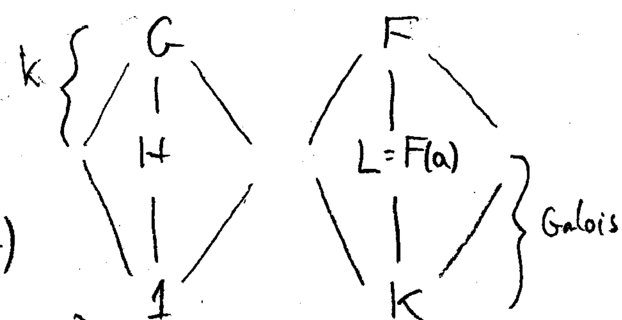
(b) $\Rightarrow$ (c): Let $\mathcal{F}_2 = \mathcal{F}_1$ ✓

(c) $\Rightarrow$ (a):

Case 1: $[K:F] < \infty$. Let $G = \mathrm{Gal}(K/F)$.

Pick $f(x) \in \mathcal{F}_2$ of $\deg f(x) = n > 0$ and let $g(x)$ be an irreducible factor with $\deg g(x) = k > 0$.

Let $a \in K$ be a root of $g(x)$.



Set $L = F(a)$, $H = \mathcal{G}L$.

Props 3.3 & 1.3 $\Rightarrow [G:H] = k = [L:F]$ $(*)$

Use induction on $[K:F]$ (Base case trivial)

Assume it holds for all fields of degree $< n$.

Since K is a splitting field for $\mathcal{F}_2$ over L, & $[K:L] < [K:F]$,

IHoP $\Rightarrow$ K/L is Galois.

$$\Rightarrow [K:L] = |\mathrm{Gal}(K/L)| = |\mathcal{G}L| = |H|. \quad (**)$$

$$\text{Lagrange} \Rightarrow |G| = |H|[G:H] = \underset{(**)}{[K:L]}\underset{(*)}{[L:F]} = [K:F].$$

Since $|G| = [K:F]$, K/F is Galois (by Cor to FTGT) ✓

Case 2: $[K:F] = \infty$.

Take any $a \in K \setminus F$.

$[F(a):F] < \infty$, so a has a splitting field $M \subseteq K$ of some finite subset of $\mathcal{F}_2$.

Then $[M:F] < \infty$, and M/F is Galois (By Case 1).

Thus, $\phi(a) \neq a$ for some $\phi \in Gal(M/F)$.

Thm 1.11 $\Rightarrow$ ϕ extends to an elt $\theta \in Gal(K/F)$, $\theta(a) \neq a$. ✓ □

Cor: Suppose K/F is algebraic, and char $F = 0$. Then K/F is Galois iff K is the splitting field over F for some set of polynomials in $F[x]$.

Def: K/F is a normal extension if every irreducible polynomial that has a root in K splits over K.

Example: $\mathbb{Q}(\sqrt[3]{2})$ is not normal over $\mathbb{Q}$, since $m_{\sqrt[3]{2}}(x) = x^3 - 2$, but $x^3 - 2$ does not split in $\mathbb{Q}(\sqrt[3]{2})$ (it has 2 complex roots).

Thm 3.5: Suppose K/F is algebraic and $\overline{F}$ is an algebraic closure, $F \subseteq K \subseteq \overline{F}$. Then the following are equivalent:

(a) K/F is normal

(b) K is a splitting field for some $\mathcal{F} \subseteq F[x]$.

(c) If $\phi \in Gal(\overline{F}/F)$, then $\phi(K) \subseteq K$. (K is "stable").

Pf: (a) $\Rightarrow$ (b). Take $\mathcal{F} = \{m_a(x) : a \in K\}$. ✓

(b) $\Rightarrow$ (c): Let K be a splitting field for $\mathcal{F} = \{f_\alpha(x) : \alpha \in A\} \subseteq F[x]$.

Take $\phi \in Gal(\bar{F}/F)$ and $f_\alpha(x) \in \mathcal{F}$, and say $a \in K$ is a root of $f_\alpha(x)$.

Then $0 = \phi(f_\alpha(a)) = f_\alpha(\phi(a))$, so $\phi(a)$ is a root of $f_\alpha(x)$, and so $\phi(a) \in K$. Since K is generated by roots of polynomials in $\mathcal{F}$, $\phi(K) \subseteq K$. ✓

(c) $\Rightarrow$ (a): Let $f(x) \in F[x]$ be irreducible, $f(a) = 0$ for some $a \in K$.

Let $b \in \bar{F}$ be any other root of $f(x)$.

Then $\exists$ F-isomorphism $\phi : F(a) \longrightarrow F(b)$, $\phi(a) = b$ by the Cor to Prop 1.9, and ϕ extends to $\theta \in Gal(\bar{F}/F)$ by Thm 1.11.

Then, $\theta(K) \subseteq K$, so $\theta(a) = b \in K$, so $f(x)$ splits over K. ✓ $\square$

<u>Cor</u>: If K/F is algebraic, then K/F is Galois iff K is both normal and separable over F.

<u>Pf</u>: Thms 3.4 & 3.5.

<u>Def</u>: A <u>normal closure</u> of K/F is a field $L \supseteq K$ that is normal over F and minimal in that respect.

<u>Def</u>: A <u>Galois closure</u> of K/F is a field $L \supseteq K$ that is Galois over F and minimal in that respect.

Thm 3.6: Let K/F be an algebraic extension:

(a) K has a normal closure L over F, unique up to isomorphism.

(b) If $[K:F] < \infty$, then $[L:F] < \infty$.

(c) If K/F is separable, then L is a Galois closure.

Pf: (a) Say $K = F(S)$ for some $S = \{a_i : i \in I\}$.

Put $\mathcal{F} = \{m_{a_i,F}(x) : i \in I\} \subseteq K[x]$.

Let L be a splitting field for $\mathcal{F}$ over K, which is also a splitting field for $\mathcal{F}$ over F.

Thm 3.5 $\Rightarrow$ L/F is normal. ✓

Minimality: Suppose $K \subseteq M \subseteq L$, and M/K normal. K contains one root of each $m_{a_i,F}(x)$, thus M does as well. But since M/K is normal, each $m_{a_i,F}(x)$ splits in M $\Rightarrow$ M is a splitting field for $\mathcal{F}$ over K $\Rightarrow$ $M = L$. ✓

Uniqueness: Suppose L' is a normal closure for K/F. Then L' is a splitting field for $\mathcal{F}$ over K $\Rightarrow$ $L' = L$. ✓

(b) If $[K:F] < \infty$, then we can pick S to be finite, thus $[L:F] < \infty$. ✓

(c) If K/F is separable, then Thm 3.4 $\Rightarrow$ L/F is Galois. ✓ $\square$

Example: Let $K = \mathbb{Q}(\sqrt[4]{2})$. The min'l poly is $m(x) = x^4 - 2$, which has roots $\{\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}\}$, so the Galois closure is the splitting field of $m(x)$, i.e, $\mathbb{Q}(\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i)$.

<u>Lemma 3.7</u> If G is a finite subgroup of the multiplicative group $F \setminus \{0\}$, then G is cyclic.

<u>Pf:</u> Since $G \cong P_1 \times \cdots \times P_k$ for its Sylow subgroups, we need to show that each Sylow subgroup P is cyclic.

Set $m = \max\{|a| : a \in P\}$, and pick $b \in P$ with $|b| = m$.

Then $1, b, b^2, \ldots, b^{m-1}$ are distinct roots of $f(x) = x^m - 1 \in F[x]$.

Prop 1.7 $\Rightarrow$ They are the only roots of $f(x)$.

If $c \in P$, then $c^m = 1$ $\Rightarrow$ c is a root of $f(x)$

$\Rightarrow c = b^k$ for some $k \Rightarrow P = \langle b \rangle$. $\square$

<u>Thm 3.8</u>: If K/F is finite, then K/F is simple iff there are only finitely many intermediate fields between K and F.

<u>Pf</u>: ($\Rightarrow$) Say $K = F(a)$, and let $m(x) = m_{a,F}(x)$.

If $F \subseteq L \subseteq K$, set $f(x) = m_{a,L}(x)$. (<u>Note</u>: $f(x) \mid m(x)$ in $K[x]$).

If $f(x) = b_0 + b_1 x + \cdots + b_{k-1}x^{k-1} + x^k$, let $M = F(b_0, b_1, \ldots, b_{k-1}) \subseteq L$.

Clearly, $m_{a,M}(x) = f(x)$ and $K = M(a)$.

Therefore $[K : M] = \deg f(x) = [K : L] \Rightarrow M = L$.

Thus, $f(x)$ determines L, and there are only finitely many factors of $m(x)$ ✓.

($\Leftarrow$) If $|F| < \infty$, Prop 3.7 $\Rightarrow K \setminus \{0\} = \langle b \rangle \Rightarrow K = F(b)$. ✓

Assume $|F| = \infty$. Pick $a, b \in K$, $b \neq 0$ and set $L = F(a, b)$.

Consider all elts of the form $c = a + bd$, $d \in F$.

Since $|F| = \infty$, but $\exists$ finitely many intermediate fields,

$\exists$ $c_1 = a + bd_1 \neq a + bd_2 = c_2$ s.t. $F(c_1) = F(c_2) = E \subseteq L$.

Claim: $F(a,b) = F(c_1)$.

Consider $c_1 - c_2 = b(d_1 - d_2) \in E$.

Since $d_1 - d_2 \neq 0$, $b \in E$. Also, $a = c_1 - bd_1 \in E \Rightarrow E = L$ ✓

Pick $a \in K$ s.t. $[F(a):F]$ is maximal.

If $F(a) \neq K$, then $\exists$ $b \in K$ s.t. $F(a,b) \supsetneq F(a)$, but

then we can find $c_1 \in K$ s.t $F(a,b) = F(c_1)$. ↯

Therefore, $F(a) = K$. □

Thm 3.9: If K/F is finite & separable, then K/F is simple.

Pf: Let L be a Galois closure for K/F.

Then $Gal(L/F)$ is finite, and has finitely many subgroups.

By FTGT, there are finitely many L s.t. $F \subseteq L \subseteq K$.

Thm 3.8 $\Rightarrow$ K/F is simple. □

Thm 3.10: (Fundamental Theorem of Algebra): $\mathbb{C}$ is algebraically closed.

Pf: Pick $f(x) \in \mathbb{C}[x]$ and let a be a root in an ext. field.

Let K be a Galois closure of $\mathbb{C}(a)$ over $\mathbb{R}$, and let

$G = Gal(K/\mathbb{R})$.

Let H be a 2-Sylow subgroup of G and let $L = \mathcal{F}H$.

FTGT $\Rightarrow$ $[L:\mathbb{R}] = [G:H]$ is odd.

Thm 3.9 $\Rightarrow L = \mathbb{R}(b)$ for some $b \in L$ with $\deg m_{b,\mathbb{R}}(x)$ odd.

But $m_{b,\mathbb{R}}(x)$ has a real root (Intermediate value theorem), so WLOG assume it's b. Thus, $L = \mathbb{R}$. $\Rightarrow [G:H] = 1$

Therefore $|G| = 2^k$, so every subgroup of G is a 2-group. Suppose $k > 0$.

Pick $G_2 \leq G$ s.t. $[G_2 : Gal(K/\mathbb{C})] = 2$

(Recall that p-groups always have a subgroup of index p^i. See HW 3, #5)

$$\begin{tikzcd}
Gal(K/\mathbb{R}) \arrow[r, "\mathcal{F}"] \arrow[d, dash] & \mathbb{R} \arrow[d, dash] \\
Gal(K/\mathbb{C}) \arrow[d, dash] & \mathbb{C} \arrow[d, dash] \\
Gal(K/K) & K = \mathbb{C}(a) \arrow[l, "\mathcal{G}"]
\end{tikzcd}$$

Now, $[\mathcal{F}G_2 : \mathbb{C}] = [G_2 : Gal(K/\mathbb{C})] = 2.$

But every degree-2 polynomial over $\mathbb{C}$ has roots in $\mathbb{C}$ (by the quadratic formula!), thus $\mathcal{F}G_2$ can't exist.

We conclude that $|G| = 2^0 = 1 \Rightarrow K = \mathbb{C} \Rightarrow a \in \mathbb{C}$. $\square$

<u>Application</u>: Finite fields:

<u>Def</u>. If $|F| = p^n$, then the monomorphism $\phi_p : a \mapsto a^p$ is the <u>Frobeneius map</u> on F.

<u>Prop 3.11</u> If F is a finite field with q elements and prime field $F_p \cong \mathbb{Z}_p$, then $q = p^n$ where $n = [F : F_p]$ and F is a splitting field over F_p for $f(x) = x^q - x$.

Pf: F is a $\mathbb{Z}_p$-vector space of dimension $n = [F : \mathbb{Z}_p]$, thus $|F| = p^n$. ✓

The multiplicative group $F \setminus \{0\}$ has order $q-1$, thus each $a \neq 0$ is a root of $x^{q-1} - 1$, so each $a \in F$ is a root of $f(x) = x^q - x$.

Thus, F is a splitting field for $f(x)$ over $\mathbb{Z}_p$. ✓ $\square$

Prop 3.12: If $0 < n \in \mathbb{Z}$, and p is prime, then there is a field F of order $q = p^n$, unique up to isomorphism. The Galois group $G(F/\mathbb{Z}_p) = \langle \phi_p \rangle$ has order n, and ϕ_p is the Frobenius map.

Pf: Let F be a splitting field for $f(x) = x^q - x \in \mathbb{Z}_p[x]$ over $\mathbb{Z}_p$.

Since $f'(x) = -1 \neq 0$, $f(x)$ has q distinct roots.

Since $(a+b)^p = a^p + b^p$, if $a, b \in F$ are non-zero roots, then $a \pm b$, ab, and a/b are roots.

Thus, the roots of $f(x)$ form a field, over which $f(x)$ splits.

Therefore, $|F| = q$, and uniqueness follows from uniqueness of splitting fields. ✓

Note: $\phi_p \in Gal(F/\mathbb{Z}_p)$, and $\phi_p^k(a) = a^{p^k}$ $\forall a \in F$, $k \geq 0$.

Therefore $\phi_p^n = 1 \Rightarrow |\phi_p| \mid n$.

If $|\phi_p| = k < n$, then all elements of F would be roots of $g(x) = x^{p^k} - x$ $\lightning$ (Prop 1.7).

Thus, $Gal(F/\mathbb{Z}_p) = n$ and $|\phi_p| = n \Rightarrow Gal(F/\mathbb{Z}_p) = \langle \phi_p \rangle$ $\square$

<u>Cor</u>: If F and K are finite fields with $F \subseteq K$, then K/F is Galois.

<u>Pf</u>: If $|K| = q$, let $f(x) = x^q - x \in F[x]$.
Since $f(x)$ has distinct roots, it is separable, and K is a splitting field for $f(x)$ over F.
By Thm 3.4 (c) $\Rightarrow$ (a), K/F is Galois.