§2.5 Normal extentions

Related to the notion of a splitting field is that of a normal extention

Defn: An extention L/K is **normal** if every irreducible polynomial $f \in K[x]$ which has at least one zero in L splits in L.

ie if L has one zero then it has all zeros of f.

Example 1) $\mathbb{C} : \mathbb{R}$ is normal since every polynomial splits in $\mathbb{C}$.

2) If α is a real root of $x^3 - 2 \in \mathbb{Q}[x]$ then $\mathbb{Q}(\alpha) = \mathbb{Q}$ is not normal since $x^3 - 2$ has a root in $\mathbb{Q}(\alpha)$ but does not split in $\mathbb{Q}(\alpha)$.

The next thm shows the close connection between normal extentions and splitting fields

Thm 2.24. Let $L : K$ be an extention. Then $L : K$ is normal and finite $\Leftrightarrow$ L is a splitting field for some polynomial over K.

Proof (⇐) Let L be a splitting field of a polynomial $g(x) \in K[x]$

Then note $[L:K] \leq (\deg g)!$ is finite

let $f \in K[x]$ be an irreducible pdy with a zero $\alpha \in L$

w.t.s: f splits over L.

let $M \supseteq L$ be a splitting field of fg over K. Suppose θ_1, θ_2 are 2 zeroes of f in M.

Claim: $[L(\theta_1):L] = [L(\theta_2):L]$

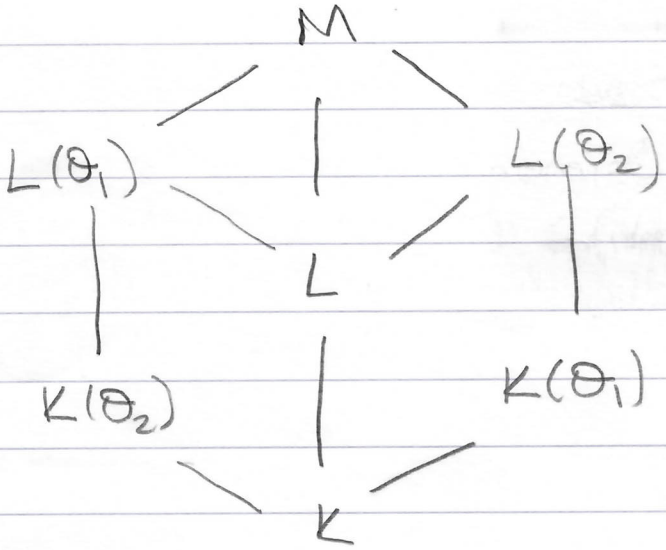
If the claim is true and if $\theta_1 \in L$ we then have $[L(\theta_1):L] = 1$, hence $[L(\theta_2):L] = 1$ by claim. Hence $\theta_2 \in L$.

Hence the claim implies that if one root of f is in L so does any other root, hence f splits in L

So to prove what we want, we want to prove the claim.

Pf of claim We will look at subfields of M and relate their degrees.

We have the following lattice of subfields of M, L, K.



For $j=1,2$ we have

$$[L(\theta_j) : L][L : K] = [L(\theta_j) : K]$$

$$= [L(\theta_j) : K(\theta_j)][K(\theta_j) : K]$$

Since θ_1, θ_2 are the roots of the some irred poly $f \in K[x]$, we have

$K(\theta_1) \cong K(\theta_2)$ and $[K(\theta_1) : K] = [K(\theta_2) : K]$
$= \deg f$

(Using Thm 2.6)

Since L is a splitting field for g over K
$L(\theta_j)$ is a splitting field for g over $K(\theta_j)$

Hence by Thm 2.19, the isom $\varphi : K(\theta_1) \to K(\theta_2)$ can be extented to an isom σ of splitting fields $\sigma : L(\theta_1) \to L(\theta_2)$

$[L(\theta_1) : K(\theta_1)] = [L(\theta_2) : K(\theta_2)]$ being the degree of isom extensions.

But then

$$\underbrace{[L(\theta_1) : K(\theta_1)][K(\theta_1) : K]}_{= [L(\theta_1) : K]} = \underbrace{[L(\theta_2) : K(\theta_2)][K(\theta_2) : K]}_{= [L(\theta_2) : K]}$$

But then

$$[L(\theta_1) : L][L : K] = [L(\theta_2) : L][L : K]$$

and hence $[L(\theta_1) : L] = [L(\theta_2) : L]$ which proves the claim and also

($\Leftarrow$) part of the pf of Thm 2.24

($\Rightarrow$) Suppose $L : K$ finite and normal

Since $L : K$ is finite, $L = K(\alpha_1 \cdots \alpha_n)$ for certain α_i, algebraic over K.

Let m_i be the min poly of α_i over K and $f = m_1 \cdots m_n$

Each m_i is irred over K and has a zero in L. By normality of $L : K$ m_i splits in L. But then f splits

in L. Since L is generated by K and the zeroes of f, it is a splitting field of f over K ∎

Example. 1) $\mathbb{Q}(e^{2\pi i/p}) : \mathbb{Q}$ is a normal extension since it is the splitting field $x^p - 1$.

2) We'll see later that any finite field of p^n elements, $\mathbb{F}_{p^n}$, is a normal extension of $\mathbb{F}_p$; as we'll see that it is a splitting field of $x^{p^n} - x \in \mathbb{F}_p[x]$

§2.6 Separable Extentions

We've seen in thm 2.19 that:
if $\varphi: F \to \tilde{F}$ an isom of fields, $f \in F[x]$
with K a splitting field of f over F
and $\tilde{K}$ " " " φf over $\tilde{F}$
Then $[K:F] = [\tilde{K}:\tilde{F}]$ and
φ extends to an isom $\sigma: K \to \tilde{K}$
and number of such extentions is at most $[K:F]$.
In the proof we took $\alpha \in F$, and
First extented φ to $\varphi': F(\alpha) \to \tilde{F}(\tilde{\alpha})$

where $\tilde{\alpha}$ is a root of φm, with
$m = \min$ poly α over F.
The choices for $\tilde{\alpha}$ are the roots of
φm. If $\deg m = \deg \varphi m = d$, then m has
at most d distinct roots (ie it can
have multiple roots)
And this leads to at most $[K:F]$
extentions of φ to an isom $\sigma: K \to \tilde{K}$.

If we could guarantee exactly d distinct
roots then we end up with maximal
number ie $[K:k]$ extentions of φ to
$\sigma: K \to \tilde{K}$.

$f \in F[x]$, K a splitting field of f so that

$f(x) = b(x-a_1)\cdots(x-a_n)$ in $K[x]$

It can happen that f has multiple roots

ie e.g $a_1 = a_2$

To avoid problems coming from multiple roots, the concept of separable polynomial and separable extention is introduced.

We'll see shortly that in char 0 all (irreducible) polynomials are separable and all alg. extentions are separable.

Galois did not recognize explicitly the concept of separability since he worked only over $\mathbb{C}$.

The concept is implicit in his proofs and must be invoked when studying fields of char p.

Recall $\mathrm{char}(R)$ = smallest positive n s.t $n \cdot 1 = 0$ if such n exists, otherwise ∞

If $R = F$ is a field $\mathrm{char} F = 0$ or p, prime

Prime subfield of F is either (isom to) $\mathbb{Q}$ or a finite field $\mathbb{F}_p$.

Defn (1) A polynomial $g(x) \in F[x]$ is called **separable over F**, if each of its irreducible factors has distinct roots in a splitting field. ie. it factors into distinct linear factors.

Otherwise $g(x)$ is called **inseparable**.

(2) If α is algebraic over F, then it is called **separable over F** if its minimal poly $m_{\alpha,F}(x) \in F[x]$ is separable.
If $m_{\alpha,F}(x)$ is **inseparable**, α is called inseparable.

Recall: $f(x) \in F[x]$ a poly with

$$f(x) = a(x-a_1)^{n_1} \cdots (x-a_r)^{n_r}$$ in a splitting field K.

with $a, a_i \in K$. a_i is called a
multiple root if $n_i > 1$
simple root if $n_i = 1$

(3) An **alg extention** K/F is called **separable** if every $\alpha \in K$ is separable
ie $m_{\alpha,F}(x)$ has only simple roots in its splitting field

We note the following simple lemma

lemma 2.25 : Let $L \supseteq K$ be a separable algebraic extension and M an intermediate field. Then $M \supseteq K$ and $L \supseteq M$ are separable.

Proof Clearly $M \supseteq K$ is separable.

Let $\alpha \in L$, let $m_{\alpha,K}$, $m_{\alpha,M}$ be its min. polys over K and M resp.

We've seen that $m_{\alpha,M} \mid m_{\alpha,K}$ in $M[x]$

But α is separable over K, hence $m_{\alpha,K}$ is separable, ie has distinct roots

but then $m_{\alpha,M}$ must also have distinct roots since $m_{\alpha,M} \mid m_{\alpha,K}$. Therefore $L \supseteq M$ is also a separable extension.

Next we give simple examples of separable and inseparable polynomials.

Example (1) $\Phi_p(x) = x^{p-1} + \dots + 1 \in \mathbb{Z}[x]$

is irreducible, and has zeroes $e^{\frac{2\pi i k}{p}}$ $k=0,\dots p-1$ all distinct hence $\Phi_p(x)$ is separable.

(2) $f(x) = x^p - t \in \mathbb{Z}_p(t)[x]$ is irred over $\mathbb{Z}_p(t)$ and inseparable.

We first show that all zeroes of f are equal to each other, hence f is inseparable

Indeed if α is a zero of f then $\alpha^p = t$

But $(x-\alpha)^p = x^p - \binom{p}{1} x^{p-1}\alpha + \dots + (-\alpha)^p$

$= x^p - \alpha^p = x^p - t$ (*)

since we are in char p and $\binom{p}{k}$ are divisible by p, for $k = 1, \dots, p-1$.

Now if β is any other root of f then

$0 = (\beta^p - t) = (\beta - \alpha)^p$ by (*)

but then since we're in a field $\beta - \alpha = 0$

$\beta = \alpha$.

To see f is irred:

Suppose $f = gh$, with $g, h \in \mathbb{Z}_p(t)[x]$

with $\deg f > \deg g, \deg h$.

Since $g \mid f$ and $f(x) = x^p - t = (x-\alpha)^p$

by (*) in some splitting field $K \supset \mathbb{Z}_p(t)$

we have that $g(x) = (x-\alpha)^s$ for some $0 < s < p$

by uniqueness of factorization.

Hence the constant coef of $g(x) = \alpha^s \in \mathbb{Z}_p(t)$

Since $s < p$, p prime, $\exists\ a, b \in \mathbb{Z}$ s.t

$as + bp = 1$

Hence $\alpha^{as+bp} = \alpha$, now $\alpha^{as} \in \mathbb{Z}_p(t)$

since $\alpha^s \in \mathbb{Z}_p(t)$, $\alpha^{bp} \in \mathbb{Z}_p(t)$ since $\alpha^p = t$

Hence $\alpha^{as+bp} = \alpha \in \mathbb{Z}_p(t)$

That means $\alpha = \dfrac{u(t)}{v(t)}$ with $u(t), v(t) \in \mathbb{Z}_p[t]$.

But then $\alpha^p = t \Rightarrow u(t)^p - t\,v(t)^p = 0$

But note this cannot happen since the terms with highest degree in $u'(t)$ and $t v^p(t)$ has to cancel and that cannot happen, since they have different degrees.

Hence our assumption abot f being irred. is wrong ##.

Remark. Recall from analysis that for a poly $f(x) \in \mathbb{R}[x]$, we can detect if f has a multiple root using its derivative.

This method generalizes to arbitrary fields by defining the derivative of $f \in F[x]$ in a formal way and will allow to describe the separability condition without leaving $F[x]$ (ie without going to a splitting field)

Defn Let $f(x) = \sum_{i=0}^{n} a_i x^i \in F[x]$

the derivative Df of f, denoted by $f'(x) \in F[x]$ is the polynomial

$$f' := Df := \sum_{i=1}^{n} i a_i x^{i-1}$$

It is straightforward to check

$$D(f+g) = Df + Dg$$

$$D(fg) = (Df)g + f(Dg).$$

We then have

Proposition 2.26 A non-zero poly $f \in F[x]$ has a multiple root α in a splitting field if and only if α is a root of f and Df.

Proof ($\Rightarrow$) Suppose α is a multiple root of f in a splitting field K

Then $f(x) = (x-\alpha)^n g(x) \in K[x]$ with $n \geq 2$. Then $Df(x) = n(x-\alpha)^{n-1} g(x) + (x-\alpha)^n (Dg)(x)$

Hence if $n \geq 2$ Then

$$(Df)(x) = (x-\alpha)\left[n(x-\alpha)^{n-2} g(x) + (x-\alpha)^{n-2}(Dg)(x)\right]$$

hence $x-\alpha \mid (Df)(x)$ and α is also a root of Df.

($\Leftarrow$) Conversely suppose α is a root of f and Df. Then if we write

$$f(x) = (x-\alpha)h(x) \quad \text{then}$$

$$(Df)(x) = h(x) + (x-\alpha)(Dh)(x)$$

Since α is a root of Df, $(x-\alpha) \mid Df$

$(x-\alpha)$ also divides $(x-\alpha)Dh$ hence $(x-\alpha) \mid h(x)$.

But then $f(x) = (x-\alpha)(x-\alpha)g(x)$

for some $g(x)$ and α is at least a double root of f.

∎

Rmk ① Since α is a root of $f \in F[x]$ $\iff m_{\alpha,F}(x) \mid f(x)$

We have that if α is a multiple root of f then $m_{\alpha,F} \mid f$ and Df. Hence α is a multiple root $\iff$ f, Df has a common factor of degree ≥ 1.

② In particular if f is irreducible then

Cor 2.27 of $f(x)$ is seperable $\iff \gcd(f, Df) = 1$ (f irreducible)

Next thm shows that over char 0 every irred. poly is separable and also gives a condition for an irred poly to be separable over a field of char p.

Thm 2.28 For any field F, an irreducible non-constant polynomial $f(x) \in F[x]$ is separable if and only if $f'(x) \neq 0$ in $F[x]$.

In particular, when F has characteristic 0 every irred poly is separable and when $\text{char } F = p$, $f(x) \in F[x]$ is separable if and only if it is not a polynomial in x^p.

Proof: Let $f(x) \in F[x]$ be irreducible.

f is separable $\iff \gcd(f, f') = 1$ by Cor 2.27

If f, and f' are not relatively prime then since f is irreducible $f \mid f'$ But $\deg f' < \deg f$ hence f' must be zero

Conversly if $f' = 0$ then $\gcd(f, f') = f$ is non-constant, hence $f(x)$ is inseparable again by cor 2.27.

If $\text{Char } F = 0$ and f is not a constant poly,

then $f' \neq 0$. Hence all irreducible polynomials over a field F of char 0 are separable.

Now assume $\text{char } F = 0$. If $f(x) \in F[x]$ is not separable then $f' \equiv 0$

If $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$

$$f'(x) = a_n n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + a_1 = 0$$

$$\Rightarrow \quad i a_i = 0 \quad \text{in } F \quad \text{for} \quad 1 \leq i \leq n-1$$

If $p \nmid i$ then $a_i = 0$ in F.
and hence f has the form

$$f(x) = a_{mp} x^{mp} + a_{p(m-1)} x^{(m-1)p} + \cdots + a_p x^p + a_0$$

$$= g(x^p)$$

where $g(x) = a_{mp} x^m + \cdots + a_p x + a_0$

so $f(x) \in F[x^p]$

Conversely if $f(x) = g(x^p)$ then $f'(x) = g'(x^p) p x^{p-1} = 0$

Since $\text{char } F = 0$, Hence f is separable. by the first part.