Content:

Definition	Normal Extension
Example	If α is a primitive 5^{th} root of unity, then $\mathbb{Q} \triangleleft \mathbb{Q}(\alpha)$.
Theorem	Let $F \triangleleft E$, $p(x)$ be an irreducible polynomial in $F[x]$, and suppose E contains at least one root of p. Then E contains all roots of $p(x)$. Moreover, all roots are distinct.
Definition	Separable
Example	$x^2 - 2 \in \mathbb{Q}[x]$ is separable.
Theorem	Let F be a field. (1) If $\text{char}(F) = 0$, then every polynomial over $F[x]$ is separable. (2) If F is finite, then every polynomial over $F[x]$ is separable.
Example	$F = \mathbb{Z}_2(t) = \text{Frac}(\mathbb{Z}_2[t])$. $f(x) = x^2 + t$. f is irreducible over F, but f is not separable.

Definition Let E/F be an extension of fields. We say that E is a *normal extension* of F if $[E:F]$ is finite and the fixed field of $\text{Gal}(E/F) = F$. We write F ◁ E.

Example If α is a primitive 5^{th} root of unity, then $\mathbb{Q} \triangleleft \mathbb{Q}(\alpha)$.

Proof:

$4 = [\mathbb{Q}(\alpha):\mathbb{Q}] = \deg(x^4 + x^3 + x^2 + x + 1)$.

Let $G = \text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$.

$4 = [\mathbb{Q}(\alpha):\mathbb{Q}] = [\mathbb{Q}(\alpha):\mathbb{Q}(\alpha)^G][\mathbb{Q}(\alpha)^G:\mathbb{Q}]$.

Since $|G| = 4$, then $[\mathbb{Q}(\alpha):\mathbb{Q}(\alpha)^G] = 4$

(by LN 4/12/10 ($[E:E^{\text{Gal}(E/F)}] = |\text{Gal}(E/F)|$.).

Thus $[\mathbb{Q}(\alpha)^G:\mathbb{Q}] = 1$.

So $\mathbb{Q}(\alpha)^G = \mathbb{Q}$. So $\mathbb{Q} \triangleleft \mathbb{Q}(\alpha)$.

Theorem Let $F \lhd E$, $p(x)$ be an irreducible polynomial in $F[x]$, and suppose E contains at least one root of p. Then E contains all roots of $p(x)$. Moreover, all roots are distinct.

Proof:
Let $\alpha \in E$, p an irreducible polynomial in $F[x]$ such that $p(\alpha) = 0$.
Assume $F \lhd E$.
Then $[E:F] < \infty$.
$|\text{Gal}(E/F)| = [E:E^G] \leq [E:F] < \infty$.
So $\text{Gal}(E/F)$ is finite. Let $\text{Gal}(E/F) = \{\varphi_1, \ldots, \varphi_n\}$.
Let $\alpha_i = \varphi_i(\alpha) \in E$. So α_i must be a root of p as well.
Let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_k$ be distinct images of α under $\text{Gal}(E/F)$. So $k \leq n$.
Note that $\forall\ i = 1, 2, \ldots, k$ and $j = 1, 2, \ldots, k$,
$\varphi_i(\alpha_j) = \varphi_i(\varphi_j(\alpha)) \in \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ as $\varphi_j \circ \varphi_i \in \text{Gal}(E/F)$.
So φ_i permutes α_j's.
$p(x) = (x - a_1)(x - a_2)\cdots(x - a_n)r(x)$ where $r(x) \in E[x]$.
If we can show $r(x)$ is a unit, then $\alpha_1, \alpha_2, \ldots, \alpha_k$ are all the roots of p(x) and all are distinct.
Let $s(x) = (x - a_1)(x - a_2)\cdots(x - a_n)$.
We want to show $r(x), s(x) \in F[x]$.
$\varphi_i : E \to E$, which induces $\overline{\varphi}_i : E[x] \to E[x]$.
Since φ_i fixes F and permutes α_j's, then $\overline{\varphi}_i(s(x)) = s(x)$.
So φ_i fixes all the coefficients of $s(x)\ \forall\ i$.
Thus, all coefficients of $s(x)$ are in the fixed field of $\text{Gal}(E/F)$.
But $F \lhd E$, so the fixed field is F.
That is, the coefficients of $s(x)$ are in F. (i.e. $s(x) \in F[x]$)
So $p(x) = \overline{\varphi}_i(p(x)) = \overline{\varphi}_i(r(x)s(x)) = \overline{\varphi}_i(s(x))\ \overline{\varphi}_i(r(s)) = s(x)\ \overline{\varphi}_i(r(x))$.
Since $p(x) = s(x)r(x) = s(x)\ \overline{\varphi}_i(r(x))$, then
$0 = s(x)r(x) - s(x)\ \overline{\varphi}_i(r(x)) = s(x)(r(x) - \overline{\varphi}_i(r(x)))$.
Since $s(x) \neq 0$, and $F[x]$ has no zero divisors, then $r(x) = \overline{\varphi}_i(r(x))$.
Similarly, $r(x) \in F[x]$.
Thus $p(x) = s(x)r(x)$ is a factorization of $p(x)$ in $F[x]$. As $p(x)$ is irreducible over F, then $r(x)$ is a unit, since $s(x)$ is not.

Definition Let $f \in F[x]$. We say f is separable if each of its irreducible factors has no repeated roots in a splitting field of f.

Example $x^2 - 2 \in \mathbb{Q}[x]$ is separable. $x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$. These roots are distinct.

Theorem Let F be a field.
(1) If char(F) = 0, then every polynomial over $F[x]$ is separable.
(2) If F is finite, then every polynomial over $F[x]$ is separable.

Proof:
(1) Assume f is irreducible and char(F) = 0.
We want to show f has no repeated roots.
We can show f, f' are relatively prime.
Let $f(x) = c_n x^n + \cdots + c_1 x + c_0$, for some $c_i \in F$.
Then $f'(x) = nc_n x^{n-1} + \cdots + 2c_2 x + c_1$.
Note: Since char(F) = 0, we know $c_n \neq 0 \Rightarrow nc_n \neq 0$, thus deg f' = n – 1.
Let $d(x)$ be a gcd of f, f'.
$d \mid f' \Rightarrow \deg d \leq n - 1$.
$d \mid f \Rightarrow d$ is a unit or d, f are associates since f is irreducible.
Since deg $d <$ deg f then d, f are not associates. So d is a unit.
Thus f, f' are relatively prime.
So f has no repeated roots by Field Extension Part II, #1(d)(Let K be a splitting field for $f(x)$, then $f(x)$ has no repeated roots in K if and only if $f(x)$ and $f'(x)$ are relatively prime.)
$\therefore$ Every polynomial over $F[x]$ is separable.

Proof:
(2) If F is finite, then char(F) = p for some prime p.
Let $f(x) \in F[x]$ such that f is irreducible over F.
Suppose f is not separable. Then f, f' cannot be relatively prime.
Hence $f'(x) = 0$. Thus each coefficient of $f'(x)$ is a multiple of p.
So then $f(x) = a_m x^{pm} + a_{m-1} x^{p(m-1)} + \cdots + a_1 x^p + a_0$.
Let $g(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0 \in F[x]$.
Then $f(x) = g(x^p)$.
Define σ_p: $F \to F$ by $\sigma_p(u) = u^p$.
This is an automorphism by Galois Theory I, HW #4.
So for each $a_i \in F$ $\exists$ $b_i \in F$ such that $a_i = b_i^p$.
Thus we have the following:

$$\begin{aligned} f(x) &= g(x^p) \\ &= a_m x^{pm} + a^{m-1} x^{p(m-1)} + \cdots + a_1 x^p + a_0 \\ &= b_m{}^p x^{pm} + b_{m-1}{}^p x^{p(m-1)} + \cdots + b_1{}^p x^p + b_0{}^p \\ &= (b_m x^m)^p + (b_{m-1} x^{m-1})^p + \cdots + (b_1 x)^p + b_0{}^p \\ &= (b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0)^p \text{ since char}(F) = p. \end{aligned}$$

Since $b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0 \in F[x]$, we have factored f in $F[x]$ into non-unit factors, a contradiction since f is irreducible.

Example $F = \mathbb{Z}_2(t) = \text{Frac}(\mathbb{Z}_2[t])$. $f(x) = x^2 + t$.
f is irreducible over F, but f is not separable.
It's a great exercise to show f is irreducible over F.
Suppose $\sqrt{t} \in F$.
Then $\sqrt{t} = \dfrac{a_0 + a_1 t + \cdots + a_n t^n}{b_0 + b_1 t + \cdots + b_m t^m}$ for some $a_i, b_j \in F$.
Note that since each $a_i, b_j \in \{0, 1\}$, then $a_n = b_m = 1$.
Thus, after squaring both sides, we have
$t = \left(\dfrac{a_0 + a_1 t + \cdots + t^n}{b_0 + b_1 t + \cdots + t^m}\right)^2$. Hence, for some $c_i, d_j \in F$,
$td_0 + d_1 t^2 + \cdots + t^{2m+1} = t(d_0 + d_1 t + \cdots + t^{2m}) = c_0 + c_1 t + \cdots + t^{2n}$.
And so we have a polynomial in t over $\mathbb{Z}_2$ of degree $2m + 1$ equal to a polynomial in t over $\mathbb{Z}_2$ of degree $2n$.
However, by Lecture Notes 3/10/10 (If E/F is an extension, $a \in E$ where a is algebraic over F, $p(x)$ is an irreducible polynomial in $F[x]$ such that a is a root, deg $p(x) = n$, then (1) every element in $F(a)$ can be expressed uniquely as $c_0 + c_1 a + \cdots + c_n a^n$ where $c_i \in F$.) elements in $\mathbb{Z}_2(t)$ have unique representation, and we have a contradiction.
$\therefore \sqrt{t} \notin F$, hence f is irreducible over F.