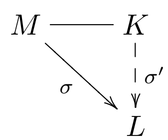
17. Normal and separable extensions

In this lecture we shall use a slightly generalized version of the Main Extension Lemma. The proof remains the same.

Lemma 17.0 (Generalized Main Extension Lemma). *Suppose we are given an algebraic extenstion K/M, an algebraically closed field L and an embedding $\sigma : M \to L$. Then there exists an embedding $\sigma' : K \to L$ s.t. $\sigma'_{|M} = \sigma$.*



17.1. **Normal extensions.**

Definition. *Let F be a field and $\{f_i\}$ a family of polynomials in $F[x]$. An extension field K of F is called a splitting field for the family $\{f_i\}$ (over F) if each f_i splits over K and K is generated by F and the roots of $\{f_i\}$.*

Extensions arising in this form are called normal and admit several equivalent characterizations.

Definition. An algebraic extension K/F is called normal if it satisfies the following equivalent conditions:

(i) Any irreducible polynomial $f(x) \in F[x]$ which has a root in K must split completely over K.
(ii) K is a splitting field for some family of polynomials in $F[x]$.
(iii) Fix [1] an algebraic closure $\overline{F}$ of F with $F \subseteq K \subseteq \overline{F}$. Then for any F-embedding $\sigma : K \to \overline{F}$ we have $\sigma(K) = K$.

The equivalence of conditions (i)-(iii) will be proved below. But first we give basic examples of a normal and non-normal extensions.

Example 17.1: Let $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ where $\omega = e^{2\pi i/3}$. The extension $K/\mathbb{Q}$ is normal as it is a splitting field over $\mathbb{Q}$ for $x^3 - 2$, as shown in Example 16.1.

Example 17.2: Let $L = \mathbb{Q}(\sqrt[3]{2})$. Then $L/\mathbb{Q}$ is not normal as it clearly violates condition (i): $f(x) = x^3 - 2$ is irreducible over $\mathbb{Q}$ and has a root $\sqrt[3]{2} \in L$, but does not split completely over L (if it did we would have $\omega\sqrt[3]{2} \in L$, which is impossible since $L \subseteq \mathbb{R}$).

[1]Note that such $\overline{F}$ exists by Observation 16.4

It is also easy to see directly that $L/\mathbb{Q}$ also violates (iii). Indeed, by Lemma 16.1 there exists a $\mathbb{Q}$-embedding $\sigma : L \to \mathbb{C}$ such that $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}\omega$, and thus $\sigma(L) \neq L$.

The following simple lemma is a partial converse of Lemma 16.1.

Lemma 17.1. *Let K/F and L/F be field extensions and $\sigma : K \to L$ an F-embedding. Then for any $\alpha \in K$ and $p(x) \in F[x]$ we have*

$$p(\alpha) = 0 \iff p(\sigma(\alpha)) = 0.$$

In particular, α and $\sigma(\alpha)$ have the same minimal polynomial over F.

Proof. Exercise. □

Theorem 17.2. *Conditions (i)-(iii) in the definition of a normal extension are indeed equivalent.*

Proof. "(i)$\Rightarrow$ (ii)" Let $\Omega = \{\mu_{\alpha,F}(x) : \alpha \in K\}$ and let A be the set of all K-roots of polynomials from Ω. Then clearly $K \subseteq F(A)$ since each $\alpha \in K$ is a root of its minimal polynomial $\mu_{\alpha,F}(x)$. For the same reason, each $p \in \Omega$ has a root in K and thus must split completely over K, whence $F(A) \subseteq K$. Therefore, $K = F(A)$ is a splitting field for Ω.

"(ii)$\Rightarrow$ (iii)" By definition there exists a family of polynomials $\Omega \subseteq F[x]$ such that $K = F(A)$ where A is the set of all $\overline{F}$-roots of elements of Ω. By Lemma 17.1 any embedding $\sigma : K \to \overline{F}$ must permute elements of A. Thus, $\sigma(A) = A$, whence

$$\sigma(K) = \sigma(F(A)) = F(\sigma(A)) = F(A) = K.$$

"(iii)$\Rightarrow$ (i)" Suppose (i) does not hold, that is, there exists an irreducible $p(x) \in F[x]$ and $\overline{F}$-roots α, β of $p(x)$ s.t. $\alpha \in K$ but $\beta \notin K$.

Then $p = \mu_{\alpha,F} = \mu_{\beta,F}$, so by Lemma 16.1 there exists an F-embedding $\sigma : F(\alpha) \to \overline{F}$ s.t. $\sigma(\alpha) = \beta$. Since $K/F(\alpha)$ is algebraic, by the Generalized Main Extension Lemma σ extends to an F-embedding $\sigma' : K \to \overline{F}$ s.t. $\sigma'_{|K} = \sigma$. Since $\sigma'(\alpha) = \beta$, we have $\sigma'(K) \neq K$, which contradicts (iii). □

17.2. **Separable extensions.**

Definition. Let F be a field. A polynomial $p(x) \in F[x]$ is called <u>separable</u> if $p(x)$ has no repeated roots in $\overline{F}$.

Lemma 17.3. $p(x) \in F[x]$ *is separable* $\iff$ $\gcd(p(x), p'(x)) = 1$.

Proof. "$\Rightarrow$" Suppose that $\gcd(p(x), p'(x)) \neq 1$. Hence $p(x)$ and $p'(x)$ have a common root $\alpha \in \overline{F}$, so $p(x) = (x-\alpha)u(x)$ and $p'(x) = (x-\alpha)v(x)$ for some

$u, v \in \overline{F}[x]$. But then $p'(x) = u(x) + (x-\alpha)u'(x)$, whence $(x-\alpha) \mid u(x)$, and so $(x-\alpha)^2 \mid p(x)$. Thus $p(x)$ has a repeated root.

"$\Leftarrow$" Similar (exercise). □

Definition. Let K/F be an algebraic extension.

(a) An element $\alpha \in K$ is called separable over F if $\mu_{\alpha,F}(x)$ is separable.
(b) The extension K/F is separable if any $\alpha \in K$ is separable over F.

Note: The polynomial $\mu_{\alpha,F}(x)$ is always irreducible. Thus, there are two possibilities:

(1) $\mu'_{\alpha,F}(x) \neq 0$. Then $\gcd(\mu_{\alpha,F}, \mu'_{\alpha,F}) = 1$ (since $\deg(\mu'_{\alpha,F}) < \deg(\mu_{\alpha,F})$), and so $\mu_{\alpha,F}$ is separable.
(2) $\mu'_{\alpha,F}(x) = 0$ in which case $\mu_{\alpha,F}$ is not separable

How can it happen that $\mu'_{\alpha,F}(x) = 0$?

Observation 17.4. *Let $f(x) \in F[x]$.*

(a) *If* $\mathrm{char} F = 0$, *then* $f'(x) = 0 \iff f$ *is constant*
(b) *If* $\mathrm{char} F = p > 0$, *then* $f'(x) = 0 \iff f = g(x^p)$ *for some* $g \in F[x]$.

Proposition 17.5. If either $\mathrm{char} F = 0$ or F is a finite field, then every algebraic extension K/F is separable.

Proof. The case $\mathrm{char} F = 0$ is clear from the above discussion. The assertion in the case of finite fields will be proved later. □