1 Normal extensions

Let $K \subseteq L$ be fields.

Recall that an element $a \in L$ is *algebraic* over K if its annihilator

$$\mathrm{Ann}(a) = \{P(x) \in K[x] : P(a) = 0\}$$

is nonzero. In this case $\mathrm{Ann}(a)$ contains a unique monic irreducible generator.

This generator is the *minimal polynomial* of a over K.

Recall that the field extension $L \mid K$ is *algebraic* if every $a \in L$ is algebraic over K.

Also recall that a polynomial $P(x) \in L[x]$ *splits* if it completely factors as

$$P(x) = c(x - a_1)(x - a_2)\cdots(x - a_n) \qquad \text{for some } c, a_1, a_2, \ldots, a_n \in L.$$

Definition. An algebraic field extension $L \mid K$ is *normal* if the minimal polynomial over K of any element of L splits in L.

Example. Consider the following field extensions.

(a) The extension $\mathbb{Q}(\sqrt[3]{2}) \mid \mathbb{Q}$ is not normal.

One can show that the minimal polynomial of $\sqrt[3]{2}$ is $x^3 - 2$.

But $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ and $x^3 - 2$ has non-real roots, so it does not split in $\mathbb{Q}(\sqrt[3]{2})$.

(b) The extension $\mathbb{Q}(\sqrt{2}) \mid \mathbb{Q}$ is normal.

To see this, let $a \in \mathbb{Q}(\sqrt{2})$ and let $m_a(x) \in \mathbb{Q}[x]$ be its minimal polynomial.

Since $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ we have $\deg(m_a(x)) \leq 2$.

But $m_a(x)$ has a root in $\mathbb{Q}(\sqrt{2})$, and any polynomial of degree ≤ 2 splits if it has a root.

Hence $m_a(x)$ splits in $\mathbb{Q}(\sqrt{2})$.

Recall that a nonzero polynomial $P(x) \in K[x]$ is *separable* if all of its irreducible factors $Q(x)$ have no multiple roots, in the formal sense that $\gcd(Q(x), Q'(x)) = 1$.

Lemma. Let $M = K(\alpha_1, \ldots, \alpha_k) \mid K$ be an algebraic field extension.

Write $m_{\alpha_i}(x)$ is the minimal polynomial of α_i over K.

Let $J \mid K$ be a field extension in which the polynomial $\prod_{i=1}^{k} m_{\alpha_i}(x) \in K[x]$ splits. Then:

(a) There is a homomorphism $M \mid K \to J \mid K$.

(b) The number of such homomorphisms is finite.

(c) This number is $[M : K]$ if the polynomials m_{α_i} are all separable.

In other words, the set of extensions of the homomorphism $K \hookrightarrow J$ to a homomorphism $M \mid K \hookrightarrow J \mid K$ is finite and nonempty, and if all the m_{α_i} are separable, then this set has cardinality $[M : K]$.

Proof. We prove the first and the second assertion together.

From results last time, there is an extension of $K \hookrightarrow J$ to a K-linear homomorphism $K(\alpha_1) \hookrightarrow J$.

Also, there are only finitely many such extensions since each corresponds to a root of m_{α_1} in J.

Now note that the minimal polynomial of α_2 over $K(\alpha_1)$ divides $m_{\alpha_2}(x)$.

Thus it has a root in J since $m_{\alpha_2}(x)$ splits in J.

We conclude again that any homomorphism $K(\alpha_1) \mid K \to J \mid K$ has an extension to a homomorphism

$$K(\alpha_1)(\alpha_2) = K(\alpha_1, \alpha_2) \mid K \to J \mid K$$

and that there are only finitely many such extensions.

Continuing this way, we see that there is an extension of the homomorphism $K \hookrightarrow J$ to a homomorphism

$$K(\alpha_1, \ldots, \alpha_k) = M \mid K \to J \mid K$$

and that there are only finitely many such homomorphisms.

We now prove the third assertion.

We repeat the reasoning just made, computing degrees along the way.

According to results last time, there are

$$[K(\alpha_1) : K] = \deg(m_{\alpha_1}(x))$$

extensions of $K \hookrightarrow J$ to homomorphisms $K(\alpha_1) \mid K \to J \mid K$ since $m_{\alpha_1}(x)$ has no multiple roots.

Similarly, for any homomorphism $K(\alpha_1) \mid K \to J \mid J$ there are

$$[K(\alpha_1, \alpha_2) : K(\alpha_1)]$$

extensions of this map to homomorphism $K(\alpha_1, \alpha_2) \mid K \to J \mid K$.

Hence, there are

$$[K(\alpha_1) : K] \cdot [K(\alpha_1, \alpha_2) : K(\alpha_1)] = [K(\alpha_1, \alpha_2) : K]$$

extensions of $K \hookrightarrow J$ to a homomorphism $K(\alpha_1, \alpha_2) \mid K \hookrightarrow J \mid K$.

Continuing this way, we see that there are

$$[K(\alpha_1) : K] \cdot [K(\alpha_1, \alpha_2) : K(\alpha_1)] \cdot [K(\alpha_1, \alpha_2, \alpha_3) : K(\alpha_1, \alpha_2)] \cdots [M : K(\alpha_1, \ldots, \alpha_{k-1})] = [M : K]$$

extensions of $K \hookrightarrow J$ to homomorphisms $M \mid K \hookrightarrow J \mid K$. □

Theorem. Suppose $L \mid K$ is a finite field extension. Then the following are equivalent:

(a) The extension $L \mid K$ is normal.

(b) The extension $L \mid K$ is a splitting extension for a polynomial with coefficients in K.

Proof. Suppose that $L \mid K$ is finite and normal.

Let $\alpha_1, \ldots, \alpha_k$ be generators for L over K, that is, a K-basis. Let

$$P(x) := \prod_{i=1}^{k} m_{\alpha_i}(x)$$

where $m_{\alpha_i}(x)$ is the minimal polynomial of α_i over K.

Then by assumption $P(x)$ splits in L and the roots of $P(x)$ generate L, so L is a splitting field of $P(x)$.

Suppose now that L is a splitting field of a polynomial in $K[x]$ with roots $\beta_1, \ldots, \beta_k \in L$.

Let $\alpha \in L$ so that $L = K(\alpha, \beta_1, \ldots, \beta_k)$.

Let J be a splitting field of the product of the minimal polynomials over K of the elements $\alpha, \beta_1, \ldots, \beta_k$.

Now choose a root ρ in J of the minimal polynomial $Q(x)$ of α over K.

From last time, there is an extension of the map $K \hookrightarrow J$ to a homomorphism

$$\mu : K(\alpha) \mid K \hookrightarrow J \mid K$$

such that $\mu(\alpha) = \rho$.

Notice that by the lemma that there is an extension of μ to a homomorphism $\lambda : L \mid K \hookrightarrow J \mid K$.

Again by results last time, the image by λ of L in J is independent of λ, and thus of μ.

Hence the image by λ of L in J contains all the roots of $Q(x)$, i.e., $Q(x)$ splits in the image of λ.

But $Q(x)$ has coefficients in K and λ gives an isomorphism between L and the image of λ.

So we see that $Q(x)$ splits in L, which is what we wanted to prove. □

Recall that $\mathrm{Aut}_K(L)$ is the group of K-linear field homorphisms $L \to L$.

(All of these homomorphisms are isomorphisms when $[L : K] < \infty$.)

Theorem. Let $L \mid K$ be the splitting field of a separable polynomial over K. Then

$$\#\mathrm{Aut}_K(L) = [L : K].$$

Proof. By the previous theorem, this follows after applying the lemma with $L = M = J$. □

If $L \mid K$ is a field extension and G is any subgroup of $\mathrm{Aut}_K(L)$, then let

$$L^G = \{a \in L : f(a) = a \text{ for all } f \in G\}.$$

Theorem. Let $\iota : K \hookrightarrow L$ be a finite field extension.

Then $\mathrm{Aut}_K(L)$ is finite. Furthermore, the following statements are equivalent:

(i) It holds that $\iota(K) = L^{\mathrm{Aut}_K(L)}$.

(ii) The extension $L \mid K$ is normal and separable.

(iii) The extension $L \mid K$ is a splitting extension for a separable polynomial with coefficients in K.

Proof. The fact that $\mathrm{Aut}_K(L)$ is finite is a consequence of the second assertion in the lemma.
In more detail, if $\mathrm{Aut}_K(L)$ were infinite, then one could obtain infinitely many maps of K-extensions

$$L \hookrightarrow J$$

by composing a given map $L \hookrightarrow J$ with the elements of $\mathrm{Aut}_K(L)$.

Now, we show (i) $\Rightarrow$ (ii):

Let $P(x)$ be the minimal polynomial of the element $\alpha \in L$.

We have to show that $P(x)$ splits and is separable.

Write $\mathrm{Orb}(\mathrm{Aut}_K(L), \alpha)$ the set of elements $f(\alpha) \in L$ for all $f \in \mathrm{Aut}_K(L)$. Then let

$$Q(x) := \prod_{\beta \in \mathrm{Orb}(\mathrm{Aut}_K(L),\alpha)} (x - \beta).$$

By construction, $Q(x)$ is separable.

Let $d := \#\mathrm{Orb}(\mathrm{Aut}_K(L), \alpha)$. Let $\beta_1, \ldots, \beta_d$ be the elements of $\mathrm{Orb}(\mathrm{Aut}_K(L), \alpha)$. We have

$$Q(x) = x^d - e_1(\beta_1, \ldots, \beta_d)x^{d-1} + \cdots + (-1)^d e_d(\beta_1, \ldots, \beta_d)$$

Now note that for any $\gamma \in \mathrm{Aut}_K(L)$ and any $i \in \{1, \ldots, d\}$, we have

$$\gamma(e_i(\beta_1, \ldots, \beta_d)) = e_i(\gamma(\beta_1), \ldots, \gamma(\beta_d))$$

and thus, since e_i is a symmetric polynomial and γ permutes the elements of $\mathrm{Orb}(\mathrm{Aut}_K(L), \alpha)$,

$$e_i(\gamma(\beta_1), \ldots, \gamma(\beta_d)) = e_i(\beta_1, \ldots, \beta_d).$$

Since γ was arbitrary, we see that $e_i(\beta_1, \ldots, \beta_d) \in L^G = \iota(K)$. Thus $Q(x) \in \iota(K)[x]$.

Abusing language, we identify $Q(x)$ with a polynomial in $K[x]$ via ι.

On the other hand $\alpha \in \mathrm{Orb}(\mathrm{Aut}_K(L), \alpha)$ so that $Q(\alpha) = 0$.

Thus, by the definition of $P(x)$, we see that $P(x)$ divides $Q(x)$.

Hence $P(x)$ splits in L and has no multiple roots. In particular, it is separable.

Next, we show (ii) $\Rightarrow$ (iii):

Let $\alpha_1, \ldots, \alpha_k$ be generators of L over K.

Let $P(x) := \prod_{i=1}^k m_{\alpha_i}(x)$, where $m_{\alpha_i}(x)$ is the minimal polynomial of α_i over K.

Then $P(x)$ is a separable polynomial by construction.

On the other hand, L is a splitting field for $P(x)$.

Finally, we show (iii) $\Rightarrow$ (i):

$L^{\mathrm{Aut}_K(L)}$ contains the image of K as any element of $\mathrm{Aut}_K(L)$ fixes the image of K in L.

Thus the extension $L \mid K$ is the composition of an extension $L^{\mathrm{Aut}_K(L)} \mid K$ and $L \mid L^{\mathrm{Aut}_K(L)}$.

The extension $L \mid L^{\mathrm{Aut}_K(L)}$ is also the splitting field of a separable polynomial over $L^{\mathrm{Aut}_K(L)}$.

(To see this, use the same polynomial as for $L \mid K$).

Also, tautologically, the subgroup $\mathrm{Aut}_{L^{\mathrm{Aut}_K(L)}}(L) \subseteq \mathrm{Aut}_K(L)$ coincides with $\mathrm{Aut}_K(L)$.

Now, using the previous theorem, we may compute that

$$[L : L^{\mathrm{Aut}_K(L)}] = \#\mathrm{Aut}_{L^{\mathrm{Aut}_K(L)}}(L) = \#\mathrm{Aut}_K(L) = [L : K] = [L : L^{\mathrm{Aut}_K(L)}][L^{\mathrm{Aut}_K(L)} : K].$$

Thus we must have $[L^{\mathrm{Aut}_K(L)} : K] = 1$ and $L^{\mathrm{Aut}_K(L)} = \iota(K)$.

These implications finish the proof of the theorem. □

Corollary. Let $L \mid K$ be an algebraic field extension.
Suppose L is generated by $\alpha_1, \ldots, \alpha_n \in M$ and that the minimal polynomial of each α_i is separable.
Then the extension $L \mid K$ is separable.

Proof. There is an extension $M \mid L$ such that $M \mid K$ is the splitting field of a separable polynomial.
(See results from the last lecture.)
By the previous theorem, the extension $M \mid K$ is separable.
Thus by definition the extension $L \mid K$ is also separable. □