Splitting Fields and Normal Extensions

Here we are usually dealing with a “ground field” $F$ and an extension field $K$. Throughout we will only consider finite extensions $K : F$. In most examples $F$ is the field of rational numbers $\mathbb{Q}$. While other examples will be considered, one may well think about $F$ as $\mathbb{Q}$ in the first reading.

**Definition 1** We say $f(x)$ completely splits into linear factors in $K[x]$ if we may write

$$f(x) = \prod_{i=1}^{r} (x - \alpha_i)^{m_i} \tag{1}$$

**Definition 2** We say $K$ is the splitting field of a polynomial $f(x) \in F[x]$ over $F$ if

1. $f(x)$ completely splits into linear factors in $K[x]$.
2. $K = F(\alpha_1, \ldots, \alpha_r)$, where the $\alpha_i$ are the roots of $f(x)$ in $K$. That is, $K$ may be generated from $F$ using the roots of $f(x)$ and has nothing more.

Our goal is the following result, but we shall first require preliminaries interesting in their own right.

**Theorem 0.1** Suppose $K \subset C$ is the splitting field of $f(x) \in F[x]$ over $F$. Suppose $g(x) \in F[x]$ is irreducible (over $F$) and suppose further that there is an $\beta \in K$ with $g(\beta) = 0$. Then $g(x)$ completely splits into linear factors in $K[x]$.

**Remark:** The condition that $K$ is a subfield of the complex numbers isn’t totally necessary but it somewhat simplifies the presentation and this is the main case we shall use.

**Definition 3** Let $\sigma : K_1 \rightarrow K_2$ be an isomorphism over $F$. Let $h(x) = h_0 + h_1 x + \ldots + h_w x^w \in K_1[x]$. Then $\sigma h$ is that polynomial achieved by applying $\sigma$ to all of the coefficients. That is,

$$(\sigma h)(x) = \sigma(h_0) + \sigma(h_1)x + \ldots + (\sigma h_w)x^w$$

We note $(\sigma h)(x) \in K_2[x]$.

**Theorem 0.2** If $c(x) = a(x)b(x)$ in $K_1[x]$ then $(\sigma c)(x) = (\sigma a)(x)(\sigma b)(x)$ in $K_2[x]$.
Proof: Immediate.

**Theorem 0.3** \( p(x) \in K_1[x] \) is irreducible in \( K_1 \) if and only if \((\sigma p(x)) \in K_2[x] \) is irreducible in \( K_2 \).

**Proof:** If \( p(x) = a(x)b(x) \) in \( K_1[x] \) then \((\sigma p) = (\sigma a)(\sigma b) \) in \( K_2[x] \). Conversely we may apply the isomorphism \( \sigma^{-1} \) so if \((\sigma p)(x) = a(x)b(x) \) in \( K_2[x] \), \( p(x) = (\sigma^{-1}a)(\sigma^{-1}b(x)) \) in \( K_1[x] \).

**Theorem 0.4** Let \( f(x) \in F[x] \) be irreducible over \( F \). Let \( \sigma : K_1 \to K_2 \) be an isomorphism over \( F \). Let \( f(x) = p_1(x) \cdots p_l(x) \) be the factorization of \( f(x) \) into irreducible factors in \( K_1[x] \). Then \( f(x) = (\sigma p_1)(x) \cdots (\sigma p_l)(x) \) is the factorization of \( f(x) \) into irreducible factors in \( K_2[x] \).

**Proof:** As \( f(x) \in F[x] \), \((\sigma f)(x) \) is \( f(x) \). From Theorem 0.2, \( f(x) = (\sigma p_1)(x) \cdots (\sigma p_l)(x) \) is a factorization and from Theorem 0.3 the factors are irreducible in \( K_2[x] \).

Now we shall extend an isomorphism to a larger structure.

**Theorem 0.5** Isomorphism Extension Theorem. Let \( \sigma : K_1 \to K_2 \) be an isomorphism over \( F \). Let \( p(x) \in K_1[x] \) be irreducible and let \( \alpha \) be a root of \( p \). Let \( \beta \) be a root of \((\sigma p)(x) \). Then we may extend \( \sigma \) to an isomorphism \( \sigma^+ : K_1(\alpha) \to K_2(\beta) \) by setting \( \sigma^+(\alpha) = \beta \).

**Proof:** Set \( n \) equal the degree of \( p(x) \) so we may write

\[
K_1(\alpha) = \{c_0 + c_1\alpha + \ldots + c_{n-1}\alpha^{n-1} : c_0, \ldots, c_{n-1} \in K_1\}
\]

and

\[
K_2(\beta) = \{d_0 + d_1\beta + \ldots + d_{n-1}\beta^{n-1} : d_0, \ldots, d_{n-1} \in K_2\}
\]

Then \( \sigma^+ \) is defined by

\[
\sigma(c_0 + c_1\alpha + \ldots + c_{n-1}\alpha^{n-1}) = d_0 + d_1\beta + \ldots + d_{n-1}\beta^{n-1}
\]

where \( d_j = \sigma(c_j) \). Write \( p(x) = x^n - a_{n-1}x^{n-1} - \ldots - a_0 \). To check that \( \sigma^+ \) preserves products we basically (formally, we’d need to write more here) have to look at \( \alpha^n = a_{n-1}\alpha^{n-1} + \ldots + a_0 \). We have \((\sigma p)(x) = x^n - b_{n-1}x^{n-1} - \ldots - b_0 \), where \( b_j = \sigma(a_j) \). So \( \beta^n = b_{n-1}\beta^{n-1} + \ldots + b_0 \) and indeed \( \sigma(\alpha^n) = \beta^n \).

**Example:** Let \( F = Q \), \( \theta = 2^{1/3} \), \( \omega = e^{2\pi i/3} \), \( \eta = \theta\omega \). Define \( \sigma : Q(\theta) \to Q(\eta) \) by \( \sigma(\theta) = \eta \). Take \( p(x) = x^2 + x + 1 \) so that in this case \( \sigma p \) is \( p \). Take the root \( \omega \) for both sides. Now we extend \( \sigma \) to \( \sigma^+ : Q(\theta, \omega) \to Q(\eta, \omega) \) by setting \( \sigma^+(\omega) = \omega \).

Applying Theorem 0.5 repeatedly we get:

**Theorem 0.6** Full Isomorphism Extension Theorem. Let \( \sigma : K_1 \to K_2 \) be an isomorphism over \( F \). Let \( f(x) \in K_1[x] \) have complex roots \( \alpha_1, \ldots, \alpha_s \). Let \( \beta_1, \ldots, \beta_s \) denote the complex roots of \((\sigma f)(x) \in K_2[x] \). Then \( \sigma \) may be extended to an isomorphism \( \sigma^{++} : K_1(\alpha_1, \ldots, \alpha_s) \to K_2(\beta_1, \ldots, \beta_s) \).
Proof: Let \( p_1(x) \in K_1[x] \) be the irreducible polynomial of \( \alpha_1 \) over \( K_1 \). Let \( \beta_1 \) be a root of \( (\sigma p_1)(x) \). From Theorem 0.5 we extend \( \sigma \) to \( \sigma^+ : K_1(\alpha_1) \rightarrow K_2(\beta_1) \). Continue in this fashion extending each of the \( a_i \). (When \( a_i \) is already in the field you don’t do anything.) At the end you have a \( \sigma^{++} \) with domain \( K_1(\alpha_1, \ldots, \alpha_s) \) But the \( \sigma^{++}(a_i) \) must be the roots of \( (\sigma f)(x) \) so they must be the \( \beta_1, \ldots, \beta_s \) giving the desired extension.

Now we prove Theorem 0.1. Let \( \alpha_1, \ldots, \alpha_r \) denote the complex roots of \( f(x) \) and let \( \beta_1 = \beta, \beta_2, \ldots, \beta_s \) denote the complex roots of \( g(x) \). If the theorem fails we can assume, without loss of generality, that \( \beta_1 \in K \) and \( \beta_2 \not\in K \). Set \( K_1 = F(\beta_1) \), \( K_2 = F(\beta_2) \). As \( \beta_1, \beta_2 \) have the same minimal polynomial \( g(x) \) over \( F \) we find an isomorphism \( \sigma : K_1 \rightarrow K_2 \) which preserves \( F \) and has \( \sigma(\beta_1) = \beta_2 \).

Now from Theorem 0.6 we extend \( \sigma \) to the roots of \( f(x) \). As \( f(x) \in F[x] \), \( (\sigma f)(x) = f(x) \) so both \( f(x) \) and \( (\sigma f)(x) \) have the roots \( \alpha_1, \ldots, \alpha_r \). So the extended \( \sigma^{++} \) permutes these roots. That is, \( \sigma^{++} \) is an isomorphism from \( K_1(\alpha_1, \ldots, \alpha_r) \) to \( K_2(\alpha_1, \ldots, \alpha_r) \).

What’s wrong with this? Well, remember that \( K_1 = F(\beta_1) \) with \( \beta_1 \in F(\alpha_1, \ldots, \alpha_r) \) so that \( K_1(\alpha_1, \ldots, \alpha_r) = F(\alpha_1, \ldots, \alpha_r) \). But \( K_2 = F(\beta_2) \) with \( \beta_2 \not\in F(\alpha_1, \ldots, \alpha_r) \) and so \( K_2(\alpha_1, \ldots, \alpha_r) = F(\alpha_1, \ldots, \alpha_r, \beta_2) \) is a nontrivial extension of \( K_1(\alpha_1, \ldots, \alpha_r) \). But isomorphisms over \( F \) preserve dimension over \( F \) (a nice exercise!) and the Tower Theorem would give \( [F(\beta_2, \alpha_1, \ldots, \alpha_r) : F] \) to be strictly bigger than \( [F(\beta_1, \alpha_1, \ldots, \alpha_r) : F] \), a contradiction.

Now that we have proven Theorem 0.1 we give an important definition that distinguishes certain kind of field extensions.

**Definition 1** Suppose \( F \subset K \) are subfields of \( C \) with \( K \) a finite extension of \( F \). We say that the extension \( K : F \) is normal if the following hold.

1. There is an \( f(x) \in F[x] \) with \( K \) the splitting field of \( f(x) \) over \( F \).
2. Every \( g(x) \in F[x] \) which is irreducible (over \( F \)) and has a root in \( K \) completely splits into linear factors in \( K[x] \).

When this occurs we often say that \( K \) is a normal extension of \( F \).

**Theorem 0.7** The two conditions in Definition 1 are equivalent. That is, either one implies the other.

**Proof:** We’ve already done the hard part. Theorem 0.1 gives that condition 1 implies condition 2. Now assume condition 2. As \([K : F]\) is finite write \( K = F(\alpha_1, \ldots, \alpha_s) \) for some finite number of \( \alpha_1, \ldots, \alpha_s \). For each \( \alpha_i \) let \( p_i(x) \in F[x] \) be its irreducible polynomial over \( F \).

We claim \( K \) is the splitting field of \( f(x) \) where we set \( f(x) \) to be the product \( p_1(x) \cdots p_s(x) \). By Condition 2 all of the roots of each \( p_i(x) \) are in \( F \) and so the extension of \( F \) by all of the roots of \( f(x) \) (that is, all of the roots of each \( p_i(x) \)) is still inside of \( K \). But the roots include \( \alpha_1, \ldots, \alpha_s \) so the extension must include \( F(\alpha_1, \ldots, \alpha_s) \) which is all of \( K \). That is, the extension of \( F \) by all of the roots of \( f(x) \) is precisely \( K \), giving the claim.

**Some Examples:**
1. \( K = Q(2^{1/3}) \) is not a normal extension of \( Q \) as the polynomial \( x^3 - 2 \in Q[x] \) (irreducible by Eisenstein's criterion) has one root in \( K \) but its other roots are not in \( K \).

2. \( K = Q(\sqrt[3]{2}, \sqrt[3]{3}) \) is a normal extension of \( Q \) as the polynomial \((x^2 - 2)(x^2 - 3)\) has roots \( \sqrt[3]{2}, -\sqrt[3]{2}, \sqrt[3]{3}, -\sqrt[3]{3} \) and extending \( Q \) by these four roots gives precisely \( K \).

3. \( K = Q(2^{1/3}, \omega) \) (with \( \omega = e^{2\pi i/3} \)) is a normal extension of \( Q \) as the polynomial \( x^3 - 2 \in Q[x] \) has roots \( 2^{1/3}, 2^{1/3}\omega, 2^{1/3}\omega^2 \) and extending \( Q \) by these four roots gives precisely \( K \).

4. Let \( \epsilon = e^{2\pi i/5} \). Then \( K = Q(\epsilon) \) is a normal extension of \( Q \) as the polynomial \((x^5 - 1)/(x - 1) = x^4 + x^3 + x^2 + x + 1 \) has roots \( \epsilon, \epsilon^2, \epsilon^3, \epsilon^4 \) and extending \( Q \) by these four roots gives precisely \( K \).

5. Let \( K = Q(2^{1/4}) \) and \( F = Q(2^{1/2}) \). Then \( K \) is a normal extension of \( F \) as the polynomial \( x^2 - 2 \in F[x] \) has roots \( 2^{1/4}, -2^{1/4} \) and extending \( F \) by these two roots gives precisely \( K \).

6. Let \( K = Q(2^{1/4}) \). Then \( K \) is not a normal extension of \( Q \) as the polynomial \( x^4 - 2 \in Q[x] \) (irreducible by Eisenstein's criterion) has two roots \( 2^{1/4}, -2^{1/4} \) in \( K \) but the other two roots \( 2^{1/4}i, -2^{1/4}i \) are not in \( K \). (One reason why \( 2^{1/4}i \notin K \) is that all elements of \( K \) are real.)

A Cautionary Note: The last two examples emphasize that when we talk about a normal extension we are talking about two fields, that \( K \) is normal over \( F \). Further, consider the tower \( Q \subset F \subset K \), with \( F = Q(2^{1/2}) \) and \( K = Q(2^{1/4}) \). Then \( F \) is a normal extension of \( Q \) as it is an extension of \( Q \) by the two roots of \( x^2 - 2 \). We’ve seen that \( K \) is a normal extension of \( F \). But it is not true (as we just saw) that \( K \) is a normal extension of \( Q \). That is, we do not have a transitive property for normality, just because blip is normal over blop which is normal over blanket we cannot deduce that blip is normal over blanket.

While we have to be careful about towers of fields, the following is useful and easy.

**Theorem 0.8** The Middle Normal Theorem Let \( K \subset L \subset F \) be fields and assume \( F : K \) is a normal field extension. Then \( F : L \) is a normal field extension.

**Proof:** From Definition 1, condition 1, there is an \( f(x) \in K[x] \) with \( F \) the splitting field of \( f(x) \) over \( K \). That is, \( f \) splits entirely in \( K[x] \) with roots \( \alpha_1, \ldots, \alpha_r \in F \) and \( F = K(\alpha_1, \ldots, \alpha_r) \). But now we can simply consider \( f(x) \) as a polynomial in \( L[x] \). It still splits entirely in \( K[x] \) with roots \( \alpha_1, \ldots, \alpha_r \). As \( K \subset L \) we have \( K(\alpha_1, \ldots, \alpha_r) \subset L(\alpha_1, \ldots, \alpha_r) \) and since \( \alpha_1, \ldots, \alpha_r \in F \) and \( L \subset F \), \( L(\alpha_1, \ldots, \alpha_r) \subset K \) so that \( L(\alpha_1, \ldots, \alpha_r) = F \) and so the \( F \) is a normal extension over \( L \) by the same Definition 1, condition 1 and the same \( f(x) \).
Caution: Under the assumptions of Theorem 0.8 we do not necessarily have $L : K$ a normal extension.

Here is a nice property of normal field extensions that say, somehow, that they are nailed down.

**Theorem 0.9** Let $K : F$ be a normal field extension. Let $K'$ be a field and $\sigma : K \to K'$ an isomorphism over $F$. (Recall, this means $\sigma(c) = c$ for all $c \in F$.) Then $K' = K$.

**Proof:** We can write $K = F(\alpha_1, \ldots, \alpha_s)$. Then $K' = F(\sigma(\alpha_1), \ldots, \sigma(\alpha_s))$. For each $i$, $\alpha_i$ and $\sigma(\alpha_i)$ satisfy the same irreducible polynomial $p_i(x) \in F[x]$. As $K : F$ is normal this means $\sigma(\alpha_i) \in K$. Thus $K' \subseteq K$. Similarly, going backward with $\sigma^{-1}$, $K \subseteq K'$ and so $K = K'$.

A Cautionary Note: Theorem 0.9 does not say that each element of $K$ is fixed by $\sigma$. Indeed, $\sigma$ can move around the elements of $K$ but the set of elements remains the same.

**Theorem 0.10** Let $K : F$ be a finite field extension. Then there is an extension $K \subset K^+$ so that $K^+$ is a normal field extension of $F$.

**Proof:** As $[K : F]$ is finite we can write $K = F(\alpha_1, \ldots, \alpha_r)$ for some finite number of $\alpha$’s. Let $p_i(x)$ be the minimal polynomial for $\alpha_i$ in $F[x]$. Set $K^+$ to be the splitting field for the product $f(x) = p_1(x) \cdots p_r(x)$. As a splitting field it is a normal extension of $F$ and it contains $\alpha_1, \ldots, \alpha_r$ and therefore $K$.