## SECTION 51 – SEPARABLE FIELD EXTENSIONS

Let $F \leq E$ be a finite field extension, and recall that we have two numbers attached to it. The degree $[E : F]$ is the dimension of $E$ as a vector space over $F$, and the index $\{E : F\}$ is the number of homomorphisms $\tau\colon E \to \overline{F}$ fixing $F$.

**Main lessons of today.**

(1) A finite field extension $F \leq E$ is **separable** if $\{E : F\} = [E : F]$.
(2) If $F$ is of characteristic 0 or if $F$ is finite, then $F \leq E$ is always separable.
(3) If $F \leq E$ is a finite and separable field extension, then there exists an $\alpha \in E$ such that $E = F(\alpha)$.

### Multiplicities of zeros

**Example.** Consider the polynomial

$$f(x) = x^3 - 10x^2 + 33x - 36 = (x-3)(x-3)(x-4) = (x-3)^2(x-4) \in \mathbb{Q}[x]$$

The zeros of $f(x)$ are 3 and 4. Since $x - 3$ appears twice in the factorisation, we say 3 has multiplicity 2 as a zero of $f(x)$, and since $x - 4$ appears once, we say 4 has multiplicity 1 as a zero of $f(x)$.

We make this intuitive concept into a formal definition.

**Definition.** Let $f(x) = a_n x^n + \cdots + a_0 \in F[x]$. Then we can write

$$f(x) = a_n(x-\alpha_1)^{\nu_1}(x-\alpha_2)^{\nu_2}\cdots(x-\alpha_m)^{\nu_m},$$

with the $\alpha_i$ distinct elements of $\overline{F}$, and with $\nu_1 + \cdots + \nu_m = n$. The number $\nu_i$ is the **multiplicity** of $\alpha_i$ as a zero of $f(x)$.

**Theorem.** *Let $f(x) \in F[x]$ be irreducible. Then every zero of $f(x)$ in $\overline{F}$ has the same multiplicity.*

*Proof.* Let's assume $f(x)$ is monic, and write

$$f(x) = (x-\alpha_1)^{\nu_1}(x-\alpha_2)^{\nu_2}\cdots(x-\alpha_k)^{\nu_k}.$$

with $\alpha_i \in \overline{F}$ distinct, and the $\alpha_i$ are all conjugates over $F$. Let $\psi\colon \overline{F} \to \overline{F}$ be some automorphism fixing $F$. This $\psi$ must send each $\alpha_i$ to some conjugate, i.e. to some $\alpha_j$, and so gives a permutation of the set $\{\alpha_1, \ldots, \alpha_n\}$.

$$f(x) = (x-\alpha_1)^{\nu_1}(x-\alpha_2)^{\nu_2}\cdots(x-\alpha_k)^{\nu_k} = (x-\psi(\alpha_1))^{\nu_1}(x-\psi(\alpha_2))^{\nu_2}\cdots(x-\psi(\alpha_k))^{\nu_k}$$

It follows that that if $\psi(\alpha_i) = \alpha_j$, then $\nu_i = \nu_j$.

For any given $1 \leq i, j \leq k$, consider the isomorphism $\psi_{\alpha_i,\alpha_j}\colon F(\alpha_i) \to F(\alpha_j)$, which by the isomorphism extension theorem we may extend to an automorphism $\overline{\psi}_{\alpha_i,\alpha_j}\colon \overline{F} \to \overline{F}$. Since $\overline{\psi}_{\alpha_i,\alpha_j}(\alpha_i) = \alpha_j$, we must have $\nu_i = \nu_j$. □

**Corollary.** *Let $f(x) \in F[x]$ be an irreducible polynomial of degree $n$. If $f(x)$ has exactly $k$ zeros in $\overline{F}$, then each zero has multiplicity $n/k$.*

*Proof.* If $\alpha_1, \ldots, \alpha_k \in \overline{F}$ are the zeros of $f(x)$, then we get

$$f(x) = c(x-\alpha_1)^\nu \cdots (x-\alpha_k)^\nu.$$

We see

$$n = \deg f(x) = k\nu,$$

so the multiplicity of each zero is $\nu = n/k$. □

**Example.** The following irreducible polynomials in $\mathbb{Q}[x]$ are such that all their zeros are of multiplicity 1:

- $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$
- $x^2 + 1 = (x + i)(x - i)$

**Example.** Let us give one example of an irreducible polynomial whose zeros have higher multiplicity. Let $p$ be a prime, and let $F = \mathbb{Z}_p(y)$, the field of fractions of $\mathbb{Z}_p[y]$. The elements of $F$ are expressions of the form $g(y)/h(y)$ with $h(y), h(y) \in \mathbb{Z}_p[y]$. Let

$$f(x) = x^p - y \in F[x].$$

One can check that $f(x)$ is irreducible. Let $\alpha \in \overline{F}$ be a zero of $f(x)$. Then $\alpha^p = y$, and we find that

$$(x-\alpha)^p = x^p - \binom{p}{1}x^{p-1}\alpha + \binom{p}{2}x^{p-2}\alpha^2 + \cdots - \alpha^p.$$

Since $p$ divides $\binom{p}{i}$ for all $1 \le i \le p-1$, and $p \cdot a = 0$ for all $a \in F$, we have $\binom{p}{i}a = 0$ for all $a \in F, 1 \le i \le p-1$. Hence

$$(x-\alpha)^p = x^p - \alpha^p = x^p - y,$$

so the only zero of $x^p - y$ is $\alpha$, which has multiplicity $p$.

**Theorem.** *Let $F \le E$ be a finite field extension. Then $\{E : F\}$ divides $[E : F]$.*

*Proof.* We assume for simplicity $E = F(\alpha)$ with $\alpha \in E$. Then $[E : F] = \deg(\alpha, F) = \deg(\mathrm{irr}(\alpha, F))$. On the other hand $\{E : F\}$ is the number of homomorphisms $\psi\colon E \to \overline{F}$ fixing $F$. Since each such is of the form $\psi_{\alpha,\beta}$ for some conjugate $\beta \in \overline{F}$ of $\alpha$, it equals the number of conjugates of $\alpha$ over $F$. The conjugates of $\alpha$ are precisely the zeros of $\mathrm{irr}(\alpha, F)$. Writing

$$\mathrm{irr}(\alpha, F) = (x-\alpha)^\nu (x-\alpha_2)^\nu \cdots (x-\alpha_k)^\nu,$$

with the $\alpha, \alpha_i \in \overline{F}$ distinct, we have that

$$[E : F] = \deg(\mathrm{irr}(\alpha, F)) = \nu k$$

and

$$\{E : F\} = k,$$

so $\{E : F\}$ divides $[E : F]$. □

## Separable field extensions

**Definition.** A finite field extension $F \leq E$ is **separable** if $[E : F] = \{E : F\}$.

**Example.** We have $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = \{\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\} = 2$, so $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2})$ is a separable field extension.

**Example.** The extension $F \leq F(\alpha)$ is separable if and only if $\alpha$ has multiplicity 1 as a zero of $\text{irr}(\alpha, F)$, as one can see by the proof of the theorem just above.

**Theorem.** *Let $F \leq K \leq E$ be finite field extensions. The following are equivalent*

(1) *$F \leq K$ and $K \leq E$ are separable.*
(2) *$F \leq E$ is separable.*

*Proof.* We have $[E : F] = [E : K][K : F]$ and $\{E : F\} = \{E : K\}\{K : F\}$. We can write

$$[E : F] = \nu_{E/F}\{E : F\}, [E : K] = \nu_{E/K}\{E : K\}, [K : F] = \nu_{K/F}\{K : F\}$$

with all the $\nu$ positive integers, and we get

$$\nu_{E/F} = \nu_{E/K}\nu_{K/F}.$$

Then clearly

$$(1) \Leftrightarrow \nu_{E/F} = 1 \Leftrightarrow \nu_{E/K} = \nu_{K/F} = 1 \Leftrightarrow (2).$$

□

**Definition.** A field $F$ is **perfect** if every finite field extension $F \leq E$ is separable.

**Theorem.** *Let $F$ be a field. If $F$ has characteristic 0 or if $F$ is a finite field, then $F$ is perfect.*

**Example.** Every subfield of $\mathbb{C}$, such as $\mathbb{Q}$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{R}$, has characteristic 0, and so is perfect.

**Example.** A non-perfect field must have characteristic $p > 0$ and be infinite. The simplest example of a non-perfect field is $\mathbb{Z}_p(y)$. The extension $\mathbb{Z}_p(y) < \mathbb{Z}_p(y)(\alpha)$, where $\alpha$ is a zero of $x^p - y$, is non-separable.

**Theorem** (A special case)**.** *Let $F$ be a field of characteristic 0, and let $f(x) \in F[x]$ be irreducible. Then every zero of $f(x)$ has multiplicity 1.*

*Proof.* We will assume that $F \leq \mathbb{R}$, and so we can take $\overline{F} \leq \mathbb{C}$.

Let $\alpha \in \overline{F}$ be a zero of $f(x)$, and assume for a contradiction that it has multiplicity $\geq 2$. Since $f(x)$ is irreducible, we have $f(x) = \text{irr}(\alpha, F)$, and $f(x)$ has minimal degree among all non-zero polynomials in $F[x]$ with $\alpha$ as a zero.

Then over $\overline{F}$ we can factor

$$f(x) = c(x - \alpha)^\nu (x - \alpha_2)^\nu \cdots (x - \alpha_k)^\nu = (x - \alpha)^2 g(x),$$

where $g(x)$ is some polynomial. Since $F \leq \mathbb{R}$, we can think of $f(x)$ as a real function of a real variable $x$, and we can then consider the derivative $f'(x)$. If

$$f(x) = a_n x^n + \cdots + a_0 \qquad a_i \in F,$$

we have

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

and so $f'(x) \in F[x]$. From $f(x) = (x - \alpha)^2 g(x)$ we get

$$f'(x) = 2(x - \alpha)g(x) + (x - \alpha)^2 g'(x),$$

so clearly

$$f'(\alpha) = 2(\alpha - \alpha)g(\alpha) + (\alpha - \alpha)^2 g'(\alpha) = 0.$$

Since $f(x)$ is non-constant, $f'(x) \neq 0$, and clearly $f'(x)$ has smaller degree than $f(x)$. But $f(x)$ is irreducible, and therefore it is the polynomial with smallest degree in $F[x]$ having $\alpha$ as a zero. This gives a contradiction (to our assumption that $\alpha$ has multiplicity $\geq 2$). □

**Remark.** The above proof uses $F \leq \mathbb{R}$ so that we can differentiate $f(x)$ and use the ordinary rules of differentiation. It turns out that differentiation of polynomials can be defined for any field by the usual formulas $(x^n)' = nx^{n-1}$, and the above proof can be made to work for any characteristic 0 field.

*Proof that characteristic 0 fields are perfect.* Let $F$ be a field of characteristic 0. Let $F \leq E = F(\alpha)$ be a simple field extension of degree $n$. Then $\deg(\text{irr}(\alpha, F)) = n$, and since $F$ has characteristic 0, we know that $\text{irr}(\alpha, F)$ has $n$ distinct zeros in $\overline{F}$. Therefore $\alpha$ has $n$ conjugates in $\overline{F}$, so $\{F(\alpha) : F\} = n = [F(\alpha) : F]$, and hence $F \leq F(\alpha)$ is separable.

If $F \leq E$ is a general finite extension, then $E = F(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_i$ algebraic over $F$. Since all the extensions

$$F \leq F(\alpha_1) \leq F(\alpha_1, \alpha_2) \leq \cdots \leq F(\alpha_1, \ldots, \alpha_n)$$

are simple, they are separable, and hence $F \leq F(\alpha_1, \ldots, \alpha_n)$ is separable. □

## The primitive element theorem

**Theorem** (The primitive element theorem)**.** *Let $F \leq E$ be a finite and separable field extension. Then there exists an element $\alpha \in E$ such that $E = F(\alpha)$.*

**Example.** Consider $\mathbb{Q} < \mathbb{Q}(\sqrt{2}, \sqrt{3})$. It has been shown in a previous example that also $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.