Field Extensions

A <u>field extension</u> is the containment of one field in another $F \subset E$. We write this as E/F.
(This is <u>not</u> to be confused with coset notation)

Examples : $\mathbb{C}/\mathbb{R}$, $\mathbb{R}/\mathbb{Q}$, $\mathbb{F}_p(x)/\mathbb{F}_p$

E/F a field extension $\Rightarrow$ $F(\alpha_1, \ldots, \alpha_n)/F$ a field extension $\forall$ $\alpha_1, \ldots, \alpha_n \in E$

Let E/F be a field extension $\Rightarrow$

1/ $(E, +)$ is an Abelian group

2/ There is a natural F-scalar multiplication on E :

$$F \times E \to E$$
$$(\lambda, v) \mapsto \lambda v$$

just multiplication in E

Nice Exercise : Field axioms $\Rightarrow$ E is an F-vector space

<u>Definition</u> A field extension E/F is <u>finite</u> $\Leftrightarrow$ E is a <u>finite dimensional</u> F-vector space

Otherwise we say E/F is an infinite extension.

If E/F is finite we write $[E : F] = \dim_F(E)$

square brackets (not the same as index)

dimension in the sense of linear algebra.

<u>Examples</u> : $\mathbb{C}/\mathbb{R}$ finite, $[\mathbb{C} : \mathbb{R}] = 2$

$\mathbb{R}/\mathbb{Q}$ infinite. ← not obvious

<u>Theorem</u> Let F be a field and $f(x) \in F[x]$ be irreducible. Then $E = F[x]/(f(x))$ is a finite extension of F and $[E : F] = \deg(f(x))$

Proof F a field $\Rightarrow F[x]$ a P.I.D.

$\Rightarrow (f(x)) \subset F[x]$ maximal $\Rightarrow F[x]/(f(x))$ a field.

The containment $F \subset F[x]$ induces a containment $F \subset F[x]/(f(x))$. Explicitely we identify $a \in F$ with $a + (f(x))$.

Let $g(x) + (f(x)) \in F[x]/(f(x))$

Euclidean property $\Rightarrow g(x) = q(x) f(x) + r(x)$

where $r(x) = 0_{F(x)}$ or $\deg(r(x)) < \deg(f(x))$

$\Rightarrow g(x) + (f(x)) = r(x) + (f(x))$

Assume $r_1(x) + (f(x)) = r(x) + (f(x))$ when $\deg(r_1(x)) < \deg(f(x))$.

$\Rightarrow r_1(x) - r(x) \in (f(x)) \Rightarrow f(x) \mid r_1(x) - r(x)$

If $r_1(x) - r(x) \neq 0_{F(x)} \Rightarrow \deg(r_1(x) - r(x)) \geq \deg(f(x))$

$\Rightarrow \deg(r(x)) \geq \deg(f(x))$ <u>or</u> $\deg(r_1(x)) \geq \deg(f(x))$

Contradiction. Hence $r_1(x) = r(x)$

Assume $\deg(f(x)) = n$. Hence for any $g(x) + (f(x)) \in F[x]/(f(x))$ $\exists!\ a_0, \dots, a_{n-1} \in F$ s.t. $g(x) + (f(x)) = a_0 + a_1 x + \dots + a_{n-1} x^{n-1} + (f(x))$

$\Rightarrow \{1 + (f(x)), x + f(x), x^2 + (f(x)), \dots, x^{n-1} + (f(x))\} \subset F[x]/(f(x))$

forms a basis for $F[x]/(f(x))$ as an F-vector space.

$\Rightarrow [F[x]/(f(x)) : F] = \dim_F(F[x]/(f(x))) = \deg(f(x))$

$\square$

__Definition__ Let E/F be a field extension. Let $\alpha \in E$

α __algebraic__ over $F \iff \exists f(x) \in F[x] \setminus \{0_{F[x]}\}$ s.t. $f(\alpha) = 0_F$

If __not__ we say α is __transcendental__ over F

E/F __algebraic extension__ $\iff \forall \alpha \in E$, α algebraic

E/F __transcendental extension__ $\iff \exists \alpha \in E$, α transcendental

__Remarks__ 1) $\alpha \in F \implies \alpha$ algebraic over F

e.g. $f(x) = x - \alpha$

The converse is __not__ true. E.g. $\mathbb{C}/\mathbb{R}$, $\alpha = i$

$i \notin \mathbb{R}$ but $f(i) = 0$ where $f(x) = x^2+1$.

2) $\mathbb{R}/\mathbb{Q}$ is a transcendental extension. E.g.

π is transcendental over $\mathbb{Q}$. This is hugely non-trivial and very hard to prove.

__Theorem__ E/F finite $\implies E/F$ algebraic

__Proof__ Let $[E:F] = \dim_F(E) = n$

Let $\alpha \in E$. $\implies \{1, \alpha, \alpha^2, \dots, \alpha^n\}$ is a subset of size $n+1 \implies$ it is linear dependent over $F \implies \exists\, a_0, \dots, a_n \in F$, not all zero such that

$a_0 \cdot 1 + a_1\alpha + a_2\alpha^2 + \dots + a_n\alpha^n = 0_F$

$\implies f(\alpha) = 0$ where $f(x) = a_0 + a_1 x + \dots + a_n x^n \in F[x]$

$f(x) \neq 0_{F[x]} \implies \alpha$ algebraic over F. $\square$

Warning E/F algebraic $\not\Rightarrow$ E/F finite

Example : $\overline{\mathbb{Q}}/\mathbb{Q}$, $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ algebraic over } \mathbb{Q}\}$

hard to prove its a subfield of $\mathbb{C}$.

Definition Let E/F be a field extension and $\alpha \in E$ be algebraic over F. The minimal polynomial of α over F is $f(x) \in F[x] \setminus \{0_{F[x]}\}$ of minimal degree such that

1. $f(x)$ monic
2. $f(\alpha) = 0_F$

Example $\mathbb{R}/\mathbb{Q}$ $\alpha = \sqrt{2}$ has minimal polynomial $x^2 - 2$ over $\mathbb{Q}$.

Theorem Let E/F be a field extension and $\alpha \in E$ be algebraic with minimal polynomial $f(x) \in F[x]$. Then

A/ If $g(x) \in F[x]$ then $g(\alpha) = 0 \iff f(x) \mid g(x)$

B/ $f(x)$ is irreducible in $F[x]$

Proof

A/ Euclidean property $\Rightarrow g(x) = q(x) f(x) + r(x)$ where $r(x) = 0_{F[x]}$ ($\Rightarrow f(x) \mid g(x)$) or $\deg(r(x)) < \deg(f(x))$.

$g(\alpha) = 0_F \Rightarrow q(\alpha) f(\alpha) + r(\alpha) = 0_F$

$\Rightarrow r(\alpha) = 0_F$

If $r(x) \neq 0_{F[x]}$ this contradicts the minimality of the degree of $f(x)$ (Note we can always scale $r(x)$ to make it monic)

$\Rightarrow f(x) \mid g(x)$

B/ By definition $f(x) \neq 0_{F[x]}$ and $f(x) \notin (F[x])^*$.

$f(x) = a(x)b(x)$, $a(x), b(x) \in F[x]$

$\Rightarrow a(\alpha)b(\alpha) = 0_F \Rightarrow$ either $a(\alpha) = 0_F$ or $b(\alpha) = 0_F$

$a(\alpha) = 0 \Rightarrow f(x) \mid a(x) \Rightarrow b(x) \in (F[x])^*$

$b(\alpha) = 0 \Rightarrow f(x) \mid b(x) \Rightarrow a(x) \in (F[x])^*$

$\Rightarrow f(x)$ irreducible

$\square$

<u>Theorem</u> Let E/F be a field extension and $\alpha \in E$ be algebraic with minimal polynomial $f(x) \in F[x]$ then the homomorphism

$$\phi : F[x] \longrightarrow E$$
$$g(x) \longmapsto g(\alpha)$$

induces an isomorphism $F[x]/(f(x)) \cong F[\alpha]$

Hence $F[\alpha] = F(\alpha)$ and $[F(\alpha) : F] = \deg(f(x))$

<u>Proof</u> Recall $F[\alpha] = \{ g(\alpha) \mid g(x) \in F[x] \}$

Hence by 1st Isomorphism theorem

$$F[x]/\ker\phi \cong F[\alpha] \subset E$$

$\ker\phi = \{ g(x) \in F[x] \mid g(\alpha) = 0_F \}$

$g(\alpha) = 0_F \iff f(x) \underset{\text{in } F[x]}{\mid} g(x) \Rightarrow \ker\phi = (f(x))$

$$\Rightarrow F[x]/(f(x)) \cong F[\alpha] \subset E$$

$f(x)$ irreducible $\Rightarrow$ $(f(x)) \subset F[x]$ maximal

$\Rightarrow$ $F[x]/(f(x))$ a field $\Rightarrow$ $F[\alpha]$ a field

$\Rightarrow$ $F(\alpha) = \mathrm{Frac}(F[\alpha]) = F[\alpha]$

and $[F(\alpha) : F] = [F[x]/(f(x)) : F] = \deg(f(x))$

$\square$

<u>Remark</u> If E/F is a field extension and

$\alpha_1, \dots, \alpha_n \in E$ are algebraic $\Rightarrow$ $F(\alpha_1, \dots, \alpha_n) = F[\alpha_1, \dots, \alpha_n]$

However we cannot easily express $F[\alpha_1, \dots, \alpha_n]$ as a quotient ring.

ε