§2.1 Definitions and basic theorems

Theory of field extentions show none is possible

We start with some definitions.

Defn ① If $F \subseteq K$ is a subfield of a field K, then K is called an extention of F and we write $K:F$

or K/F

② let $K:F$ be a field extention and $A \subseteq K$ a subset of K
Then we write

$F[A]$ = intersection of all subrings of K which contains A and F
= smallest subring of K which contains F and A

$F(A)$ = intersection of all subfields of K containing A and F
= smallest subfield of K containing F and A

③ An extention $K:F$ is called simple if $\exists\, a \in K$ such that $K = F(a)$
a is called a primitive element

④ If we hae 2 extentions $[K:F]$ and $[L:K]$ then K is called an intermediate field of the extention $[L:F]$

<u>Ex</u> $\mathbb{R}:\mathbb{Q}$, $\mathbb{C}:\mathbb{R}$ are field extentions
$\mathbb{C}:\mathbb{Q}$

We have the following simple lemma

<u>Lemma 2.1</u> Let $K:F$ be a field extention
Then K is a F-vectorspace

<u>Pf</u> $(K,+,0)$ is an abelian group and the restriction of multiplication in K to F defines a scalar multiplication

$$F \times K \longrightarrow K$$
$$\lambda, x \longmapsto \lambda x$$

and the distributive laws

$$(\lambda+\mu)x = \lambda x + \mu x$$
$$\lambda(x+y) = \lambda x + \lambda y$$

as well as associative law $(\lambda\mu)x = \lambda(\mu x)$, $1.x = x$ hold, Hence K is a F-vector space.

<u>Defn</u> Let $K:F$ be a field extention
The <u>degree</u> of the field extention is defined as the dimension of K as a F-vector space and is denoted by $[K:F]$ $= \dim_F K$

We write $[K:F]=\infty$ if it is not a finite dim'l vector space.
We say the field extention is <u>finite</u> if $\dim_F K = [K:F] < \infty$.

The degree of field extentions behave multiplicatively

<u>Thm 2.2</u> If K is an intermediate field of a field extention $[L:F]$ then

$$[L:F] = [L:K][K:F]$$

with the convention that $n\infty = \infty$ $\forall n \in \mathbb{Z}_{>0}$

In Particular $L:F$ is finite iff $L:K$ is finite and $K:F$ is finite.

<u>Proof</u> If L/K or K/F is not finite then L/F is not finite

for example if K/F is infinite then there are ∞ly many elements of K hence of L which are lin. independent over F so $[L:F]$ is infinite.

Similarly if L/K is infinite then there are ∞ly many elts of L lin indep. over K so certainly lin. indep over F. Hence $[L:F]$ is infinite.

So we can assume L/K and K/F are both finite.

Let $\{x_1, \dots x_n\}$ be a basis of K/F and
$\{y_1, \dots y_m\}$ " " " L/K.

Then Claim: $\{x_i y_j \mid i=1,\dots,n, \ j=1,\dots,m\}$
is a basis of L/F.

Pf of claim (a) They generate L over F:
Since if $y \in L$ then

$$y = \sum_{j=1}^{m} b_j y_j \quad \text{with} \quad b_j \in K$$

For all j, $b_j \in K$ we have

$$b_j = \sum_{i=1}^{n} a_{ij} x_i \quad , a_{ij} \in F$$

Thus we get $\quad y = \sum_{j=1}^{m} \sum_{i=1}^{n} a_{ij} x_i y_j$

Hence $\{x_i y_j\}_{i,j}$ generate L over F.

(b) They are lin. indep over F
Since if $\sum_{i,j} a_{ij} x_i y_j = 0$ w/ $a_{ij} \in F$

Then since $\{y_j\}$'s are lin indep over K

$$\sum_{i=1}^{n} a_{ij} x_i = 0 \quad \forall j$$

Since $\{x_i\}$'s are lin indep $/F$

$a_{ij} = 0 \quad \forall i, j$ ⊠

Question: How can we construct extentions of fields?

Answer: We obtain field extentions $K \supseteq F$ as try to solve polynomial equations over F

eg $p(x) = x^2 - 2x - 1 \in \mathbb{Q}[x]$
can we solve $p(x) = 0$ in $\mathbb{Q}$

Completing squares gives
$0 = x^2 - 2x - 1 = (x-1)^2 - 2$
$\Rightarrow (x-1)^2 = 2$. Since 2 is not a square in $\mathbb{Q}$, $p(x) = 0$ has no soln in $\mathbb{Q}$
It can be solved in $\mathbb{R}$ but can we do this more economically?
Indeed $\mathbb{Q}(\sqrt{2}) = \{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \}$
is a field which is much smaller than $\mathbb{R}$
and $p(x) = (x - 1 + \sqrt{2})(x - 1 - \sqrt{2})$ factors in $\mathbb{Q}(\sqrt{2})[x]$
$x^2 - 2x - 1$ is irred in $\mathbb{Q}[x]$ but in $\mathbb{Q}(\sqrt{2})[x]$ or $\mathbb{R}[x]$ factors into linear factors.

This suggests the next question
Question: Given a poly $p(x) \in F[x]$ is there a larger field K such that p has a zero in K
or going further is there a large field L s.t $p(x)$ can be written as a product of linear factors. If yes can we

do this economically, ie L is the smallest such field. (Such a field L will be called the splitting field of $p(x)$.
The first theorem ~~field~~ in this direction is

Theorem 2.3. (Kronecker). Let F be a field, let $p(x) \in F[x]$ be an irreducible polynomial. Then $\exists$ a field K containing an isomorphic copy of F in which $p(x)$ has a root

Proof: Since $p(x)$ is irreducible the ideal $I = (p(x))$ is maximal in the PID $F[x]$.
Let $K := F[x]/I = F[x]/(p(x))$. Then K is a field

Consider the canonical map

$$\pi : F[x] \longrightarrow F[x]/I = K$$

$\pi|_F$ gives a hom $\pi|_F : F \longrightarrow K$

Since $\pi|_F$ is a hom of fields, it is injective

Recall Lemma: $\varphi : F \to K$ a hom of fields
Then φ is injective
Proof: $\ker\varphi$ is an ideal of F, a field
Only ideals of a field is $0, F$
Since $\varphi(1) = 1_K \neq 0$, $\ker\varphi \neq F$
and $\ker\varphi = 0$, φ injective

Hence $F \simeq \pi(F)' \subset K$ and K contains
an isomorphic copy of F.
It remains to show that K has
a root of $p(x)$.

Let $\alpha := \pi(x) = \bar{x} \in K = F[x]/I$
ie $\alpha = x + (p(x)) = x + I$
If $p(x) = a_0 + a_1 x + \dots + a_n x^n$
then
$$p(\alpha) = p(\bar{x}) = a_0 + I + a_1(x+I) + \dots + a_n(x+I)^n$$
$$= (a_0 + a_1 x + \dots + a_n x^n) + I$$
$$= p(x) + I = p(x) + (p(x)) = 0_K.$$
$\boxtimes$

Eg $p(x) = x^2+1 \in \mathbb{R}[x]$. Has no zeroes in $\mathbb{R}$
let $K = \mathbb{R}[x]/(x^2+1)$ hence irred.

Identify $r \in \mathbb{R}$ w/ $r + (x^2+1) \in \mathbb{R}[x]/(x^2+1)$
to view $\mathbb{R}$ as a subfield of K

Let $\alpha = x + (x^2+1) \in K$. Then

$$\alpha^2 + 1_K = (x^2 + (x^2+1)) + (1 + (x^2+1))$$
$$= x^2+1 + (x^2+1) = 0_K$$
ie α is a zero of x^2+1