1 4/8

Extension Fields

A field E is an extension field of field F if F is a subfield of E.

$E \supset F$

Examples: $\mathbb{R} \subset \mathbb{C}$ $\quad \mathbb{Q} \subset \mathbb{R}$

Fundamental Thm of Field Theory
(Kronecker 1887)

Let F be a field & $f(x) \neq c$ be in $F[x]$

Then $\exists\, E \supset F$ such that $f(x)$ has a root in E.

Ex: x^2-2 does not factor in $\mathbb{Q}$ but in $\mathbb{Q}(\sqrt{2})$ it does as $(x-\sqrt{2})(x+\sqrt{2})$

notice ( ) and not [ ]. $\quad a+b\sqrt{2}$

Proof: Since $F[x]$ is an integral domain, moreover a UFD, $f(x)$ has at least one irreducible factor, call it $p(x)$. Then we conclude that $F[x]/\langle p(x)\rangle$ is a field

(by maximality of $\langle p(x)\rangle$.

Candidate for extension field of F over which $f(x)$ has a root is:

$$E = F[x]/\langle p(x)\rangle$$

Elements of E look like $a + \langle p(x)\rangle$

$$a \rightsquigarrow a + \langle p(x)\rangle$$

Now show $\exists$ root of $p(x)$ in E.

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots a_1 x + a_0$$

Try $x+\langle p(x)\rangle$ as root of $p(x)$.

$a_n\left(x+\langle p(x)\rangle\right)^n + a_{n-1}\left(x+\langle p(x)\rangle\right)^{n-1} + \cdots$

$\cdots a_1\left(x+\langle p(x)\rangle\right) + a_0$

$\langle p(x)\rangle$

Consider $\left(x+\langle p(x)\rangle\right)^n = x^n + nx^{n-1}\langle p(x)\rangle + \cdots \left(\langle p(x)\rangle\right)^n = \langle p(x)\rangle$

$= x^n + \langle p(x)\rangle$

$a_n\left(x^n+\langle p(x)\rangle\right) + a_{n-1}\left(x^{n-1}+\langle p(x)\rangle\right) + \cdots$

$a_1(x+\langle p(x)\rangle + a_0 = ?$

$= a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \quad + \langle p(x)\rangle$

$p(x)+\langle p(x)\rangle = \langle p(x)\rangle = 0$

? $\blacksquare$

$\dfrac{\mathbb{R}}{\langle x^2+1\rangle} \cong \mathbb{C}$

$x^2+1=0$ or $x^2=-1$

Let $f(x) = 2x+1 \in \mathbb{Z}_4[x]$. If $f(x)$ had a zero in any (extension) ring containing $\mathbb{Z}_4$. Say β is such a zero. $2\beta+1 = 0$,

$2(2\beta+1) = 2 \cdot 0 = 0$. $2(2\beta+1) = 4\beta+2$

So $\underbrace{4}_{0}\beta+2 = 0 \Rightarrow 2 = 0 \Rightarrow\Leftarrow$

Let E be an extension field of F, further, let $f(x) \in F[x]$. If $f(x)$ factors into linear factors: $f(x) = (x-r_1)(x-r_2)\cdots(x-r_n)$ we say E is a splitting field for $f(x)$ over F. E is smallest extension in this regard. $F(r_1, r_2, \dots r_n)$

$F(\alpha) = \left\{ \frac{f + n\alpha}{g + m\alpha} \right\}$ $\qquad$ $\underline{F[\alpha]}$

Given x^2+1 in $\mathbb{Q}[x]$, note

$(x+i)(x-i) = x^2+1$ in $\mathbb{C}$. (factors but not splitting field)

The splitting field is $\mathbb{Q}(i) = \{a+bi ; a, b \in \mathbb{Q}\}$

A splitting field of x^2+1 over $\mathbb{R}$ is $\underline{\underline{\mathbb{C}}}$

$\mathbb{R}(i) = \mathbb{C}$
