Mar 05

<u>Definition</u>: Let F be a field, an extension of F is a field E such that $E \supset F$
(F is a subfield of E);
denoted E/F ; $\begin{array}{c} E \\ | \\ F \end{array}$

* A "symmetry" of E/F
"automorphism" of E/F
is an isomorphism $\phi: E \to E$
s.t. $\phi|_F = Id_F$

<u>Ex</u>) $\mathbb{C}/\mathbb{R}$, $\begin{array}{c} \mathbb{C} \\ | \\ \mathbb{R} \end{array}$ $\phi(z) = \bar{z}$ complex conjuga
$a+ib \longmapsto a-ib$
$\overline{z+w} = \bar{z} + \bar{w}$ preserves addition
$\overline{z \cdot w} = \bar{z} \cdot \bar{w}$ " multiplica
$\bar{0} = 0$
"less symmetric" $\phi(a) = a$, $a \in \mathbb{R}$.

Two ways of obtaining extensions ($F = \mathbb{Q}, \ldots$)
later → 1. Add to F $\sqrt[2]{a}, \sqrt[3]{a}, \sqrt[7]{a}, \ldots$ $a \in F$
today → 2. Given $f \in F[x]$, form a new field containi all roots of f.
"very symmetric"

<u>Thm</u>: Let $f \in F[x]$ be non-constant. (degree higher tho
Then there exist an extension E of F in which f has a root.

<u>Proof</u>: Let p be an irreducible factor of f.
Consider $E = F[x]/\langle p \rangle$
($\langle p \rangle$ is maximal $\Leftrightarrow$ p is irreducible)
$\Rightarrow E$ is a field
$F \subset E$ by mapping $c \in F$ to $[c] = c + \langle p \rangle$

consider $[x] = x + \langle p \rangle \in E$

Claim: $p([x]) = 0$

Pf: $p = \sum a_i x_i \quad a_i \in F \subset E$

$p([x]) = \sum a_i [x]^i = \sum [a_i][x^i]$ (in $E = F/\langle p \rangle$)

$= \sum [a_i x^i] = [\sum a_i x^i] = [p] = 0$

$\Rightarrow$ p has a root in E

so f has a root in E

Ex) $f = x^2 + 1$ over $\mathbb{R}$

$E = \mathbb{R}[x]/\langle x^2+1 \rangle = \mathbb{C}$

$[x] \longleftarrow i$ root

$\{[a+xb]\} \longleftarrow \{a+ib\}$

$[a+xb] \longleftarrow a+ib$

Ex) $\underset{f''}{x^5 + 2x^2 + 2x + 2} = \underset{p_1}{(x^2+1)}\,\underset{p_2}{(x^3+2x+2)}$

$\mathbb{Z}/3[x]$

$E_1 = \mathbb{Z}/3[x]/\langle x^2+1 \rangle \quad 3^2 = 9$ elements

$[x]$ is a root of f

$E_2 = \mathbb{Z}/3[x]/\langle x^3+2x+2 \rangle \quad 3^3 = 27$ elements

$[x]$ is a root of f.

Def: $f \in F[x]$ "splits" in some E/F if f is a product of linear factors in $E[x]$

Ex) $x^2 - 2$ does not split in $\mathbb{Q}$ but splits in $\mathbb{R}$.

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

product of linear terms in $\mathbb{R}$

Mar 05

Continuation of def'n
Given $f \in F[x]$ say that an extension E/F is a splitting field for f over F if 1. f splits in E
2. f does not split in any proper subfield of E.
ie, if $F \subset K \subsetneq E$ K is a proper subfield of E then f does not split in $K[x]$.

A splitting field of x^2-2 over $\mathbb{Q}$
$\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$
— " — over $\mathbb{R}$
$E = \mathbb{R}$.

Def'n: Let E/F & let $a_1, \dots, a_n \in E$
"F adjoined with" $a_1, \dots, a_n$
$= F(a_1 \dots a_n) =$
"the smallest subfield of E that contains $F \cup \{a_1 \dots a_n\}$"
$=$ (The intersection of all subfields $K \subset E$ that contain $F \cup \{a_1 \dots a_n\}$)
$=$ (everything you can get from $F \cup \{a_1 \dots a_n\}$ using $+, -, \times, \div$ in E)

If $f \in F[x]$ splits in E/F, and $a_1 \dots a_n$ are the roots of f in E, then
$F(a_1 \dots a_n)$ is a splitting field for f over F.

Proof: In $E[x]$,
$f = b(x-a_1)\cdots(x-a_n)$ since F splits in E
where $a_1 \dots a_n$ are the roots of f in E
and b is the coefficient of x^n in f,

so $b \in F$.

* f splits in $F(a_1 \dots a_n)$
* In E, the splitting of f is unique, so if f splits in $K[x]$ where $F \subset K \subset E$, then that splitting is the one of E, ie, it is $f = b(x-a_1)\dots(x-a_n)$
$\Rightarrow a_i \in K \Rightarrow K \supset F(a_1 \dots a_n)$

$F(a_1, \dots a_n)$ is the minimum field containing F in which f splits, so $F(a_1 \dots a_n)$ is a splitting field of f. $\square$

<u>Ex)</u> $f = x^4 - x^2 - 2 = (x^2-2)(x^2+1) \in \mathbb{Q}[x]$
In $\mathbb{C}$, $f = (x-\sqrt{2})(x+\sqrt{2})(x-i)(x+i)$
so, a splitting field for f over $\mathbb{Q}$ would be $\mathbb{Q}(\sqrt{2}, i) = \{a + b\sqrt{2} + ci + d\sqrt{2}i : a, b, c, d \in \mathbb{Q}\}$

<u>Ex)</u> $\overset{=f}{x^2 + x + 2}$ over $\mathbb{Z}/3$: mod out by quadratic
Consider $E = (\mathbb{Z}/3)[x]/\langle f \rangle$ (9 elements) (3^2)
E contains $[x]$ which is a root of f.
$\Rightarrow$ If E contains α, a root of f, then $(x-\alpha) \mid f$ so $f = (x-\alpha)q$ for $q \in E[x]$
but $\deg q = 1$ ($\therefore q$ is linear)
$\Rightarrow f$ is written as linear
so f splits in E.

To find q, long division

$$
\begin{array}{r}
x + (1+\alpha) \\
(x-\alpha) \overline{\big) x^2 + x + 2} \\
\underline{x^2 - \alpha x} \\
(1+\alpha)x + 2 \\
\underline{(1+\alpha)x - \alpha(1+\alpha)}
\end{array}
$$

(in $E = \mathbb{Z}/3(\alpha)$)

$\rightarrow 2 + \alpha(1+\alpha) =$ remainder

Mar 5

but $2+\alpha(1+\alpha) = \alpha^2+\alpha+2$ is in E
$\therefore \alpha^2+\alpha+2=0$
$\Rightarrow$ remainder $=0$
$\Rightarrow$ splitting of f in E or $\mathbb{Z}/3(\alpha)$
where $f = (x-\alpha)(x+(1+\alpha))$

Not obvious that you get all of E by adding α to $\mathbb{Z}/3$. So... here's theorem

<u>Thm</u>: Let $p \in F[x]$ be irreducible, and let a be a root of p in some extension E of F ($P(a)=0$). Then there is
$\phi: F[x]/\langle p\rangle \xrightarrow{\sim} F(a)$ (ϕ is an isomorphism)
s.t. $\phi([x]) = a$

<u>Proof</u>: for a general $[g] \in F[x]/\langle p\rangle$
set $\phi([g]) = g(a)$
ϕ is well-defined: if $g \sim g'$ then $g(a)=g'(a)$
indeed, $g\sim g' \Rightarrow g-g' = pq$ for some $q \in F[$
so $g(a)-g'(a) = p(a)\cdot q(a) = 0\cdot q(a) = 0$
so $g(a) = g'(a)$ $\square$

suppose $[g] \in \operatorname{Ker}\phi$

Ker ϕ is an ideal in $F[x]/\langle p \rangle$

$[1] \notin \ker \phi \quad [1] \xmapsto{\phi} 1(a) = 1 \neq 0$

Aside

Claim: In a field K, the only ideals are $\{0\}$ and K

Proof: $A \subset K$ is an ideal and $A \neq \{0\}$

Then $\exists c \neq 0$ s.t. $c \in A \Rightarrow c^{-1}c \in A$

$\Rightarrow 1 \in A \Rightarrow A = K$

So as the Ker $\phi \neq$ everything, Ker $\phi = \{0\}$ $\therefore \phi$ is

Claim: If $\psi : K \to R$ is a homomorphism of a field into a ring, then im ψ is a field.

im $\psi \subset R$

Proof: Suppose $r \in$ im ψ show r has inverse

for $r \neq 0$, $r = \psi(c)$ for some $c \in K$ $\therefore c \neq 0$

$\therefore c^{-1}$ exist, and then

$\psi(c^{-1})r = \psi(c^{-1})\psi(c) = \psi(c^{-1} \cdot c) = \psi(1) =$

$\therefore$ image of a field is always a field

In our case, we have a domain which is a field and range which is a field

$\therefore$ im ϕ is a subfield of $F(a)$ contain

$c \in F$ $(\phi([c]) = c(a) = c)$

and also contains a $(\phi([x]) = x(a) = a)$

but $F(a)$ is the smallest field containi

F & a, so im $(\phi) = F(a)$

So ϕ is 1-1 & onto

Mar 5

<u>Cor 1</u>: Suppose $p \in F[x]$ is irreducible,
$a \in E/F$ and $p(a) = 0$
$a' \in E'/F$ and $p(a') = 0$
then $F(a)$ (a subfield of E)
is isomorphic to $F(a')$ (a subfield of E')

<u>Pf</u>: $F(a) \underset{\phi}{\cong} F[x]/\langle p \rangle \underset{\phi'}{\cong} F[a']$

$\phi' \circ \phi^{-1}$

<u>Cor 2</u>: In this case $\left(\begin{array}{l} p \in F[x] \text{ irreducible}, \\ a \in E/F, \ p(a) = 0 \end{array} \right)$
Every element of $F(a)$ can be written in a unique way as a combination as:

$$c_0 + c_1 a + c_2 a^2 + \cdots + c_{n-1} a^{n-1}$$

where $n = \deg p$ & $c_0, \ldots, c_{n-1} \in F$.

<u>Example</u>: $\pi \in \mathbb{R}/\mathbb{Q}$ (π isn't a root of any polynom
$\mathbb{Q}(\pi) = \{\pi + \pi^2 + \frac{1}{2}\pi^{1000}, \frac{\pi^2 - \pi}{3\pi + \pi^{1000}} \ldots\}$

$\therefore$ not obvious.

<u>Proof</u>: $F[x]/\langle p \rangle$ $p = x^n + \cdots$
$F[x]/\langle p \rangle$ is generated by polynomials in x, in it, $[x^n] = [\text{lower order terms}]$
So $F[x]/\langle p \rangle = \{[c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}]\}$

But ϕ takes these to
$c_0 + c_1 a + \cdots + c_{n-1} a^{n-1}$

So $F(a)$ is a vector space over F of dimens
n.