M250
Burger

Todays' Theme:

Given $p(x)$ irreducible in $F[x]$, hence $p(x)$ has no root in F (a field), then $F[x]/\langle p(x)\rangle$ forms an 'extension field' of F in which $p(x)$ has a root.

Read Book's example p. 155.

- I constructed my own 'simpler' example to better understand what is going on.

$\alpha^2+2\alpha+1 = \alpha^2+1$
$= \alpha+1+1 = \alpha$

<u>ex.</u> $\mathbb{F} = \mathbb{Z}_2$ $\quad p(x) = x^2+x+1$
[illegible] in $\mathbb{Z}_2[x]$.

$\mathbb{Z}_2[x] / \langle x^2+x+1\rangle$

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

$\alpha^2+\alpha = \alpha+1+\alpha = 1$

$ax+b$

$2 \cdot 2 = 4$

$*$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

Now lets look at $p(x) = x^2+x+1$

in $\mathbb{Z}_2[x]/\langle x^2+x+1\rangle$.

$$\begin{aligned} p(\alpha) &= \alpha^2+\alpha+1 \\ &= \alpha+1+\alpha+1 \\ &= 2\alpha+2 = 0. \end{aligned}$$

$\therefore$ α is a root in the extension field.

$$\begin{aligned} p(\alpha+1) &= (\alpha+1)^2+(\alpha+1)+1 \\ &= \alpha+\alpha+1+1 = 0 \text{ also.} \end{aligned}$$

$$p(1) = 1+1+1 \neq 0$$

$p(x)$ must factor:

$x-\alpha \rightarrow$ divides $p(x)$

$$\begin{array}{r|lll} & 1 & (1+\alpha) & \\ \hline 1\ (-\alpha) & 1 & 1 & 1 \\ {\scriptstyle +2\alpha} & & & \\ 1\ \alpha & 1 & \alpha & \\ \hline & & (1+\alpha) & 1 \\ & & (1+\alpha) & 1 \\ \hline & & & 0 \end{array}$$

$\therefore$ $x^2+x+1 = (x+\alpha)(x+\alpha+1)$ $\mathcal{Q.E.D.}$

$= x^2+\alpha x + x\alpha + x + \alpha^2+\alpha = x^2+2\alpha x+\alpha+1+\alpha+x$

$= x^2+2\alpha x+2\alpha+1+x = p(x)$

Ex-11 $\quad p(x) = x^3 - 2$ is irr. in $\mathbb{Q}[x]$, but $p(x)$ will have a root in $F = \mathbb{Q}[x]/\langle x^3-2\rangle$.

Let's call the root β.

$$\therefore \quad x-\beta \mid p(x) \quad \text{in } F.$$

$$1 \;\; \beta \;\; \beta^2$$

$$1(-\beta) \;\big)\; 1 \;\; 0 \;\; 0 \;\; (-2)$$

$$1(-\beta)$$

$$\beta \;\; 0$$

$$\beta(-\beta^2)$$

$$(\beta^2)(-2)$$

$$(\beta^2)(-\beta^3)$$

$$3$$

$$-2 \quad \text{since } x^3 = 2 \text{ in the Extension field}$$

Important here!

So

$$p(x) = (x-\beta)(x^2+\beta x+\beta^2)$$

The text says $x^2+\beta x+\beta^2$ is irr. in F. why? Ex-16

Ex. 16.

$$x^2+\beta x+\beta^2$$

Q-Formula $\longrightarrow$ $$\frac{-\beta \pm \sqrt{\beta^2-4(1)(\beta^2)}}{2}$$

$$= \frac{-\beta \pm \sqrt{-3\beta^2}}{2} \qquad \Delta = -3\beta^2$$

*

Can't do for $\mathbb{Q}[x]/\langle x^3-2\rangle$ since infinite.

$$ax^2+bx+c$$

$\infty \quad \infty \quad \infty$

$-3\beta^2$ in $\mathbb{Q}[x]/\langle x^3-2\rangle$

(i) None of $\mathbb{Q}$ will make $\cancel{\mathbb{R}}$ $-3\beta^2>0$.

(ii) No 1st or 2nd degree polynomials will square to make a 3 positive

$$\pm\sqrt{-3\beta^2} \rightsquigarrow \pm\sqrt{3}\sqrt{\beta^2} = \pm 3i\beta \notin \mathbb{Q} \text{ or } \mathbb{Q}[x]/\langle p(x)\rangle$$

So; $p(x) = (x-\beta)(x^2+\beta x+\beta^2)$ is as far as one can factor in $\mathbb{Q}[x]/\langle x^3-2\rangle$.

Now repeat construction:

let $$E = F/\langle x^2+\beta x+\beta^2\rangle$$
$$= \left[\mathbb{Q}[x]/\langle x^3-2\rangle\right]/\langle x^2+\beta x+\beta^2\rangle$$

And let α be a root of $x^2+\beta x+\beta^2$ in $\overline{E}$.

so $x-\alpha \mid x^2+\beta x+\beta^2$

$$\mid (\alpha+\beta)$$

i.e.

$$\begin{array}{r|rrr} 1-\alpha & 1 & \beta & \beta^2 \\ & 1 & -\alpha & \\ \hline & & \beta+\alpha & \beta^2 \\ & & (\alpha+\beta) & -\alpha^2-\beta\alpha \\ \hline \end{array}$$

Σ.

$\therefore x^2+\beta x+\beta^2 = (x-\alpha)(x+\alpha+\beta)$ $\beta^2+\alpha^2+\beta\alpha = 0$ since $\cancel{p(\alpha)}$ $\alpha^2+\beta\alpha+\beta^2=0$

So in E: $x^3-2 = (x-\beta)(x-\alpha)(x+\alpha+\beta)$, $\rightsquigarrow$ without going to $\mathbb{C}$ we made a field that factors to lin. terms.

<u>Thm 4.</u> F a field, $p(x) \in F[x]$ $\deg p(x) = n > 0$

There is a field K s.t. $F \subseteq K$ and $p(x)$ factors into lin. terms.

<u>pf.</u> Induction on degree of $p(x)$.

<u>$n=1$</u> If $\deg p(x) = 1$ then $p(x) = x - \alpha$, so it must have a root in the base field, since $\alpha \in F$. So $K = F$. ✓

Suppose $P(x) = P_1(x) P_2(x) \cdots P_k(x)$ where each factor is irreducible

$\deg p(x) > 1$ and the theorem holds for $0 < m < n$

let $F_1 = F[x] / \langle P_1(x) \rangle$, then $P_1(x)$ has at least 1 root α_1 in F_1, s.t. $F \subseteq F_1$

so $P(x) = (x - \alpha_1) q(x)$ in $F_1[x]$, and $\deg q(x) < n$, By induct. hyp. $\exists K$ s.t. $F \subseteq F_1 \subseteq K$ s.t.

$q(x)$ factors into linear terms $\blacksquare$

<u>Ex 12</u> $p(x) = x^3 + 2x + 1$ is irr. in $\mathbb{Z}_3[x]$. ✓

✓ $0 + 0 + 1 = 1 \neq 0$

$1 + 2 + 1 = 1 \neq 0$

$8 + 4 + 1 = 13 \neq 0$

Let β be a root in $F = \mathbb{Z}_3[x] / \langle p(x) \rangle$

$$
\begin{array}{r|l}
 & 1 \quad \beta \quad (2+\beta^2) \\ \hline
1 \; -\beta & 1 \quad 0 \quad 2 \quad 1 \\
 & 1 \; -\beta \\ \hline
 & \beta^2 \\
 & \beta - \beta^2 \\ \hline
 & 2 + \beta^2 \quad 1 \\
 & 2 + \beta^2 \; - 2\beta - \beta^3 \\ \hline
 & 1 + 2\beta + \beta^3 = 0 \text{ in } F\,!
\end{array}
$$

$\therefore$ in F; $p(x) = (x - \beta)(x^2 + \beta x + (\beta^2 + 2))$

Q-F.

$$x = \frac{-\beta \pm \sqrt{\beta^2 - 4(\beta^2 + 2)}}{2}$$

$$\Delta = \left[\beta^2 - 4\beta^2 - 8\right]_3 = \beta^2 + 2\beta^2 + 1)$$
$$= (\beta + 1)^2$$

p.166

*Ex.B $\quad p(x) = x^3 + x + 1 \quad$ in $\quad F = \mathbb{Z}_2[x] / \langle p(x) \rangle$.

Factor $p(x)$ in F.

Pfs.

1) Clearly $p(x)$ is irr. in $\mathbb{Z}_2$;

Let $\alpha = [x]$

2) and Let $p(\alpha) = 0$ in F.

$\rightarrow \quad 1(-\alpha) = (1\ \alpha) \mid p(x).$

i.e.

$$
\begin{array}{r|llll}
 & 1 & \alpha & (1+\alpha^2) & \\
\hline
1\ \alpha & 1 & 0 & 1 & 1 \\
 & 1 & \alpha & & \\
\hline
 & & \alpha & 1 & \\
 & & \alpha & \alpha^2 & \\
\hline
 & & & 1-\alpha^2 = 1+\alpha^2 & 1 \\
 & & & (1+\alpha^2) & \alpha+\alpha^3 \\
\hline
 & & & & 1-\alpha-\alpha^3
\end{array}
$$

$1 - \alpha - \alpha^3 = \alpha^3 + \alpha + 1 \equiv 0 \mod p(x)$

$\therefore p(x) = (x+\alpha)(x^2 + \alpha x + (1+\alpha^2))$

so far.

So;

$$p(x) = (x-\alpha)(x^2+\alpha x+1+\alpha^2)$$

Can't use Q-Formula.

why?

Need to check all elements of

$$\mathbb{Z}_2[x] / \langle p(x) \rangle$$

to see if there are roots.

$\deg p(x) = 3 \longrightarrow ax^2+bx+c$

$$2 \cdot 2 \cdot 2$$

8 elements.

(see p. 10 handout)

Math 250 3.7 lecture notes (page 10)
Burger

$$F = \frac{\mathbb{Z}_2[x]}{\langle x^3 + x + 1 \rangle}$$

Let $\alpha = [x]$

*	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0								
1								
α								
$\alpha+1$								
α^2								
α^2+1								
$\alpha^2+\alpha$								
$\alpha^2+\alpha+1$								

Does $x^2 + \alpha x + 1 + \alpha^2$ have roots in F?