Recall

$\mathbb{Z}[i] \cong \dfrac{\mathbb{Z}[x]}{(x^2+1)}$ → adjoining single elt with prop $x^2+1=0$

For any ring R, can consider $\dfrac{R[x]}{x^2+1}$

E.g 1) $R = \mathbb{F}_7$ $\quad 7 \equiv 3 \pmod 4$
$\Rightarrow -1$ not a square in $\mathbb{F}_7$ (fact)

Put $E = \dfrac{\mathbb{F}_7[x]}{(x^2+1)}$ Let j be img of x in E, ($j^2=-1$)

Claim. E is a field, $\#E = 49$ ($E = \mathbb{F}_{49}$)

every elt of E is uniquely of the form
$a+bj$, $a,b \in \mathbb{F}_7$

$\Rightarrow E$ is a 2-D vec sp / $\mathbb{F}_7$

To show field, must show mult inv!

$(a,b) \neq (0,0)$ $\quad \dfrac{1}{a+bj} = \dfrac{a-bj}{a^2+b^2}$ by above

Key pt $\quad a^2+b^2 \neq 0$ (if $a^2+b^2=0 \Rightarrow \left(\frac{a}{b}\right)^2 = -1$ ✗)

$\Rightarrow \dfrac{a-bj}{a^2+b^2}$ is a well def elt of E & the inv we seek

2) $R = \mathbb{C}$ $\quad$ let $E = \dfrac{\mathbb{C}[x]}{x^2+1}$ $\quad j =$ img of x in E
s.t. $j^2 = -1$

every elt of E can be written as
$a+bj$, $a,b \in \mathbb{C}$

(i.e. $1, j \in \mathbb{C}$ form a basis of E as a $\mathbb{C}$ v.s)

Cos $\Rightarrow i \neq j \quad -i \neq j$

$x^2+1 = (x+i)(x-i)$ holds in $\mathbb{C}[x]$

$(j+i)(j-i) = 0 \Rightarrow E$ not a domain

in fact $E \cong \mathbb{C} \times \mathbb{C}$

[in general, if A,B rings then $A \times B$ is by coordinatewise ops]

Show iso'

1st guess $(1,0) \to i$, $(0,1) \to j$ } doesn't work.

$(1,1) \longmapsto 1$

$(1,-1) \longmapsto ij$

Think abt $A \times B$

have elts $e = (1,0)$
$f = (0,1)$

following props:

- $e^2 = e$, $f^2 = f$ (iden potent)
- $ef = 0$
- $e + f = 1$

In gen, if R is a ring & e, f iden potent w/ $ef = 0$ $e+f = 1$

$\Rightarrow R \cong A \times B$
$x \longmapsto (ex, fx)$

where $A = eR$ $B = fR$

$\hookrightarrow$ a ring w/ iden elt e (but, not subring of R $\hookrightarrow 1 \notin A$)

$(1+ij)^2 = 1 + 2ij + (ij)^2$
$= 2(1+ij) \to e$

$\left(\frac{1+ij}{2}\right)^2 = \left(\frac{1+ij}{2}\right)$ ⟶ idenpotent

& $\frac{1-ij}{2} \to f$ are iden potents s.t. above holds

$ef = 0$, $e+f = 1$

$j \longmapsto -i$

$e \to (1,0)$
$f \to (0,1)$

$\hookrightarrow$ These give decomp of $E = eE \times fE \cong \mathbb{C} \times \mathbb{C}$

More generally,

let R = any (comm) ring

let $h(u)$ be a polynomial that is monic (leading coeff 1)

$h(u) = u^n + a_{n-1}u^{n-1} + \cdots + a_0 \qquad a_0, \ldots, a_{n-1} \in R$

$E = \dfrac{R[u]}{(h(u))}$ $\quad E$ is obt by adj "a root of h" to R

Prop Every elt of E can be written uniquely as

$b_0 + b_1 u + \cdots + b_{n-1}u^{n-1}$ $\longrightarrow$ can always cut down monic also help

$b_0, \ldots, b_{n-1} \in R$

(In other words $E \cong R^n$ with interesting multiplication) $\longrightarrow$ not as a ring but as R-modules

When h is not monic

Things become more complicated

Consider: $h(u) = au - 1 \qquad a \in R$

Is like adj mult inv of a

$E = \dfrac{R[u]}{(h(u))}$ is often denoted $R[1/a]$

E.g. 1) $R = \mathbb{Z} \qquad a = 2$

$\mathbb{Z}[1/2]$ is isom to subring of $\mathbb{Q}$ consisting of elts $\dfrac{a}{b}$ where b is a power of 2.

2) Generally if R is a domain $\quad (a \neq 0)$

$\Rightarrow R[1/a]$ is the subring of $\mathrm{Frac}(R)$ s.t elts look like $\dfrac{c}{d}$ where $d = a^k$

3) $R = \mathbb{Z} \qquad a = 1 \qquad$ (any ring R)

$\mathbb{Z} \xrightarrow{\text{surj}} \dfrac{\mathbb{Z}[u]}{(u-1)} \longrightarrow \mathbb{Z}$

$\boxed{\text{redue}}$

$u \longmapsto 1$

lesson: if a is a unit $R[1/a] \cong R$

4) $R[1/0] = 0$

as $h(u) = -1$ is a unit $\Rightarrow$ ideal $(h(u)) = \underline{R}$.

5) $R = \mathbb{Z}/6\mathbb{Z}$ $\quad a = 3$

$$R[1/3] = \frac{R[u]}{3u-1}$$

$$\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

$$3 \longmapsto (1,0)$$

$\Rightarrow \mathbb{Z}/3\mathbb{Z}[1/0] = 0$

$\mathbb{Z}/2\mathbb{Z}[1/1] = \mathbb{Z}/2\mathbb{Z}$

$\Rightarrow \mathbb{Z}/6\mathbb{Z}[1/3] \cong \mathbb{Z}/6\mathbb{Z}$