Important facts

If u is a unit. $a \in R$.

$(a) = (ua)$

$\forall\ a, b, c \in R$, u, v units

$(a, b) = (a, b + ac)$.

or $(a, b) = (ua, v(b+ac))$

This is based on the following.

If $A_1, A_2 \ldots A_n$ are represented by $a_1 \cdots a_m$

$A_i = \sum c_{ij}\, a_j$

then $(A_1 \ldots A_n) \subset (a_1 \cdots a_m)$.

Example $\mathbb{Z}[x] / (x^2-3,\ 2x+4)$

$$\mathbb{Z}[x] / (x^2-3,\ 2(x+2))$$

Change of variable

$$\mathbb{Z}[t] \longrightarrow \mathbb{Z}[x]$$
$$t \longmapsto x+2.$$

$$\mathbb{Z}[t] / ((t-2)^2-3,\ 2t)$$
$$= \mathbb{Z}[t] / (t^2-4t+1,\ 2t)$$
$$= \mathbb{Z}[t] / (t^2+1,\ 2t)$$
$$= \mathbb{Z}[t]/(t^2+1) \Big/ (2t) \cong \mathbb{Z}[t]/(t^2+1) \Big/ (2).$$
$$\cong \mathbb{Z}[t]/(2) \Big/ (t^2+1) = (\mathbb{Z}/2\mathbb{Z})[t] \Big/ (t+1)^2$$
$$\cong \mathbb{Z}/2\mathbb{Z}[t] \Big/ (t^2)$$

Characteristic of a ring:
Adjoining elements

Goal: solve equation $f(x)=0$. in R.

Ex: $\mathbb{R}$. no solution for $f(x)=x^2+1=0$

New ring $\mathbb{R}[x]/(x^2+1) =: \bar{R}$

Now $\bar{x} \in \bar{R}$ satisfies

$$\bar{x}^2+1=0.$$

Ex:
solve the inverse equation

$$a \in R, \quad ax-1=0.$$

so $R[x]/(ax-1)$.

$R=\mathbb{Z}$
$a=3$. $\mathbb{Z}[x]/(3x-1) \cong \mathbb{Z}[\frac{1}{3}] \subset \mathbb{Q}$.

Bad ex: $R=\mathbb{Z}/6\mathbb{Z}$

$a=3$. $R[x]/(3x-1) =$ zero ring.

$R \to R[x]/(3x-1)$ is a zero morphism.

Good case: $f(x)$ is monic.

$R[x]/f(x)$. or $\left(\begin{array}{l} R[\alpha] \\ f(\alpha)=0 \end{array} \right)$

① $R[\alpha]$ has basis

$(1, \alpha, \alpha^2 \cdots \alpha^{n-1})$.

i.e. $\forall \beta \in R[\alpha]$

$\beta = g(\alpha) = \sum_{i=0}^{n-1} a_i \alpha^i$ a_i are uniquely determined by β.

If $\sum_{i=0}^{n-1} a_i \alpha^i = \sum_{i=0}^{n-1} b_i \alpha^i$, then

$a_i = b_i$.

② Can view $R[\alpha]$ the same as the set of n-tuples in R

$(a_0, a_1 \cdots a_{n-1})$

Addition is component wise addition.

3 Multiplication is defined as follows.

$\beta_1 = g_1(\alpha)$. $\beta_2 = g_2(\alpha)$

$\beta_1 \cdot \beta_2 = g_1(\alpha) \cdot g_2(\alpha)$

$= f \cdot q + r$.

Pf: 1 reduce to. uniqueness of 0

$0 = \sum_{i=0}^{n} a_i \alpha^i = g(\alpha)$

$g(\alpha) = f(\alpha) \cdot h(\alpha) \Rightarrow g(\alpha) = 0$.

Example: $\mathbb{R}$ $\quad \mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$

$$\mathbb{F}_2[x]/(x^2+x+1)$$

$0, 1, x, 1+x$

$$x(x+1) = 1 \Rightarrow x^{-1} = 1+x$$

field of order 4

Product ring

Def: $\quad R \times R'$ has a ring structure.

$$(x, x') \cdot (y, y') = (xx, y \cdot y')$$

$$(x, x') + (y, y') = (x+y, x'+y').$$

$$(0, 0')$$

$$(1, 1')$$

(Idempotent element) $e \in R$, $e^2 = e$.

Prop: a). $e' = 1-e$ is also idempotent.

b). eR is also a ring with identity e.

(Notice that eR is not a subring)

c). $R \cong eR \times e'R$

Pf: a) $(1-e)^2 = 1-2e+e^2 = 1-e$.

b). $\forall\ ea \in eR$.

$e \cdot (ea) = e^2 a = ea$

c). $R \longrightarrow eR \times e'R$.

$a \mapsto (ea, e'a)$

idea $e+e' = 1$.

$(e+e')a = ea + e'a$

bijection.

ring homomorphism.