If $\phi : \mathbb{Z}_5 \to \mathbb{Z}_{10}$ is a ring homomorphism

$\Rightarrow$ (*) $\phi(a+b) = \phi(a) + \phi(b)$

(**) $\phi(ab) = \phi(a)\phi(b)$

$\Rightarrow$

$\phi(0)=0$

$\phi(1) = 2$ ✓ (*)

$\phi(1)\phi(n) = \phi(n)$

$\phi(1)$ must be identity on even elements - (**) does not work

$\phi(1\cdot 1) = \underline{\phi(1)\phi(1)}$

$\underset{2}{\phi(1)} \neq 2\cdot 2$

$a^2 = a$ in $\mathbb{Z}_m$ $\quad a = \phi(1)$

$a^2 = a \mod m$, $a \neq 0$

$a^2 - a = 0 \mod m$

$a(a-1) = 0 \mod m.$

$5\cdot 4 = 0 \mod 10$

Other kinds of rings.

Given a comm. ring with 1, R, we say an element a is irreducible if whenever $a = b\cdot c$ for $b, c \in R$, then b or c is a unit.

[Eg: 2 is irreducible in $\mathbb{Z}$ $\quad 2 = 2\cdot 1,\ 2 = (-2)(-1)$]

units

6 is not irreducible in $\mathbb{Z}$

$6 = \boxed{2\cdot 3}$ or $\boxed{(-2)(-3)}$

or $1\cdot 6$ or $(-1)(-6)$

Two elements a,b of R are called associates

if $a = bu$ for some unit $u \in R^\times$.)

$6 = -6(-1)$ 6 & -6 are associates

$2 = (-2)(-1)$ 2 & -2 are associates)

Different Kinds of Integral Domains:

UFD: Unique factorization Domain - An integral domain D such that every nonzero element $a \in D$ can be written $a = p_1 p_2 \cdots p_k$, where each p_j is an irreducible element, and this product is unique up to reordering, up to multiplication by units.

ie $a = p_{\sigma(1)} p_{\sigma(2)} \cdots p_{\sigma(k)}$ $\forall \sigma \in S_k$.

Example: $\mathbb{Z}$ is a UFD,

$12 = 2 \cdot 2 \cdot 3$

$12 = (-3)(-2)(2)$

$= (3)(-2)(-2)$

$= p_1(u)(u^{-1}p_2)$ $p_3 \cdots p_k$ where u is a unit.

$a = (u_1 p_1 u_2 p_2 \cdots u_k p_k)(u_1 u_2 \cdots u_k)^{-1}$

$\{a + b\sqrt{-3} : a, b \in \mathbb{Z}\} = \mathbb{Z}[\sqrt{-3}]$ is an ID (integral domain) but not a UFD.

$(1+\sqrt{-3})(1-\sqrt{-3}) = 4 = 2 \cdot 2$

$(a + b\sqrt{-3})(c + d\sqrt{-3}) = ((ac - 3bd) + (bc + ad)\sqrt{-3})$

Suppose $(1+\sqrt{-3})u = 2 \Rightarrow u = a + b\sqrt{-3}$

for some unit u.

$(1+\sqrt{-3})(a+b\sqrt{-3})=2$ $\quad (a-3b)=2$ $\quad 4a=2 \Rightarrow a=\frac{1}{2}$

$a+b=0 \Rightarrow$ But $\frac{1}{2}+\_\sqrt{-3} \notin \mathbb{Z}[\sqrt{-3}]$.

$\therefore$ There are two different factorizations of 4

$$(1+\sqrt{-3})(1-\sqrt{-3}) = 2\cdot 2 = 4.$$

$\therefore \mathbb{Z}[\sqrt{-3}]$ is not a UFD.

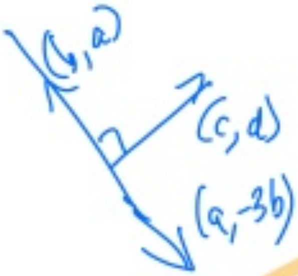
Is $\mathbb{Z}[\sqrt{-3}]$ an integral domain?

$$(a+b\sqrt{-3})(c+d\sqrt{-3}) = 0$$

$$ac-3bd=0 \rightarrow (a,-3b)\cdot(c,d)=0$$

$$bc+ad=0$$

$$\hookrightarrow (b,a)\cdot(c,d)=0$$



One of c & d at least is nonzero $\Rightarrow (c,d)$ is a nonzero vector.

$\Rightarrow (b,a)$ & $(a,-3b)$ are on the same line.

If a & b are not both zero,

eg if $a=0$ $(b,0)$ & $(0,-3b)$ are on the same line $\Rightarrow b=0$.

if $b=0$ $(0,a)$ & $(a,0)$ are on the same line $\Rightarrow a=0$.

$\Rightarrow$ both a & b are nonzero!

$$m(b,a) = (a,-3b)$$

$$mb=a$$

$$ma=-3b \Rightarrow m=\frac{-3b}{a} \Rightarrow -\frac{3b^2}{a}=a$$

$$\Rightarrow -3b^2=a^2$$

$$\Rightarrow b=a=0.$$

Contradiction

$\therefore$ No zero divisors: $\mathbb{Z}[\sqrt{-3}]$ is an ID but not a UFD.