$m\mathbb{Z}$ is $\langle m \rangle$ = ideal generated by $m \in \mathbb{Z}$ in the ring $\mathbb{Z}$.

It's a principal ideal. It's prime if m is prime.

$\langle 3, x \rangle$ is an ideal in $\mathbb{Z}[x]$ = {polynomials with coefficients in $\mathbb{Z}$}

$\rightarrow$ Not principal.

FYI we write $\mathbb{Z}(x)$ to mean $\left\{ \frac{p(x)}{q(x)} : q(x) \neq 0, \ p(x), q(x) \text{ are polys with coeff in } \mathbb{Z}. \right\}$.

Proof: Suppose $\langle 3, x \rangle = \langle p(x) \rangle$ for some $p(x) = a_0 + a_1 x + \dots + a_k x^k$ with $a_j \in \mathbb{Z}$ $\forall j$.

Then $3 = p(x)\, q(x)$ for some $q(x) \in \mathbb{Z}[x]$.

$\Rightarrow a_0 = 1$ or 3, $a_j = 0$ for $j > 0$.

$a_0 \neq 1$, because $1 \notin \langle 3, x \rangle$, so $p(x) = 3$.

But then we must also have

$x = p(x)\, h(x)$ for some $h(x) \in \mathbb{Z}[x]$.

$\Rightarrow x = 3h(x)$, impossible since that would imply the coeff. of x is a multiple of 3.

$\Rightarrow \langle 3, x \rangle$ is not principal. $\blacksquare$

In fact: $\langle 3, x \rangle = \{ a_0 + a_1 x + \dots + a_k x^k \in \mathbb{Z}[x] : a_0 \equiv 0 \bmod 3 \}$.

Why?: If $\overbrace{3h(x) + x k(x)}^{p(x)} \in \langle 3, x \rangle$ for some $h(x), k(x)$ in $\mathbb{Z}[x]$, then

$$p(x) = 3h_0 + \underset{\text{no const.}}{(\text{polynomial})} = \underbrace{3h_0}_{a_0} + x \left(\text{another polynomial} \right)$$

h_0 = constant term of $h(x)$

$\therefore a_0 \equiv 0 \bmod 3.$

If this is true for any $a_1, a_2, \dots, a_k \in \mathbb{Z}$,

$$a_0 + a_1 x + \dots + a_k x^k = \overset{3k_0}{\overset{\shortparallel}{a_0}} + x(a_1 + a_2 x + \dots + a_k x^{k-1})$$

$$\in \langle 3, x \rangle.$$

$$\therefore \mathbb{Z}[x] / \langle 3, x \rangle \cong \mathbb{Z}_3 \quad \left[\mathbb{Z}[x] = (0 + \langle 3,x \rangle) \cup (1 + \langle 3,x \rangle) \cup (2 + \langle 3,x \rangle) \right]$$

eg $\quad 2x + 3 = 3(1) + x(2) \in \langle 3, x \rangle$

$$x^2 + 7x + 3 = 3(1) + x(x+7) \in \langle 3, x \rangle$$

in $\mathbb{Z}[x]$.

Other good examples of ideals.

$R = C([0,1]) = \{$continuous $\mathbb{R}$-valued fcns on $[0,1]\}$.

let $I = \{ f \in R : f(\frac{1}{2}) = 0 \}$.

This is an ideal.

Interesting Facts:

- Let R be a commutative ring with 1, let A be an ideal in R. Then

  A is Prime $\iff$ R/A is an integral domain.

Proof: R/A is an integral domain $\iff \forall a, b \in R$, if $(a+A)(b+A) = A$, then a or b is in A.

$\iff \forall a, b \in R$, if $ab + A = A$ then a or b is in A

$\Leftrightarrow \forall a,b \in R$ if $ab \in A$ then a or b is in A.

$\Leftrightarrow$ A is a prime ideal. $\boxtimes$

- If R is a com. ring with 1, and if A is an ideal in R, then R/A is a field $\Leftrightarrow$ A is a maximal ideal.

Proof: Suppose R/A is a field. Suppose $b \in R \setminus A$.

Then let I be the ideal generated by A & b.

Since $b + A \in R/A$, $b \notin A$, $\exists c \in R$ s.t.

inverse of $b+A$ in R/A.

$$(b+A)(c+A) = 1 + A$$

$$\Rightarrow bc + A = 1 + A$$

$$\left.\begin{array}{l} \Rightarrow 1 - \underset{\underset{I}{\cap}}{bc} = \underset{\underset{I}{\cap}}{a} \in A \end{array}\right\} \Rightarrow 1 \in I \Rightarrow I = R.$$

$\therefore$ Since b was arbitrary, the only ideal that contains A is $R \Rightarrow A$ is maximal. ✓

Now suppose A is maximal. We need to show that $\forall b \in R \setminus A$, b has an inverse in R/A, ie

$\exists c \in R$ s.t. $bc - 1 \in A$

Let $J = \{br + a : r \in R, a \in A\}$ — This is an ideal that contains A, $\neq A$, so $J = R$. In particular, $1 \in J$. $\Rightarrow$ $\exists r \in R$ and $a \in A$ s.t. $br + a = 1$

$\Rightarrow br - 1 = a \in A$. $\Leftrightarrow$ $r + A$ is the inverse of $b + A$. $\Rightarrow$ R/A is a field. $\boxtimes$

- Note that every field F is automatically an integral domain. Sp $a, b \in F$, suppose $ab = 0$. If $a \neq 0$, a^{-1} exists, so $a^{-1}(ab) = a^{-1} \cdot 0 \Rightarrow b = 0$. $\boxtimes$

  $\therefore F$ is an integral domain.

- If R is a comm. ring with 1, then every maximal ideal is prime.

  Pf: Let A be a maximal ideal in R. Then R/A is a field $\Rightarrow R/A$ is an integral domain $\Rightarrow A$ is prime. $\boxtimes$

Question: We looked at $R = \mathbb{Z}[x]$, with $A = \langle 3, x \rangle$, not principal. Is this ideal prime? maximal?

$R/A \cong \mathbb{Z}_3$, a field $\Rightarrow A$ is maximal and A is prime.

(but A is not principal!)

could be generalized: $\langle p, x \rangle$

prime.