Quotient Rings

reminder on modular arithmetic:
we defined $m \equiv n \pmod 6$
to mean $m - n$ is a mult. of 6.
$6 \mid m-n$
now: $m-n \in \langle 6 \rangle$
saw that it's an equiv. rel.
and it respects $+$ and $\cdot$.
if $m \equiv m' \pmod 6$ and $n \equiv n' \pmod 6$
then $m+n \equiv m'+n' \pmod 6$ and $m \cdot n \equiv m' \cdot n' \pmod 6$

defined $\bar{m} = \{ m' \in \mathbb{Z} \mid m' \equiv m \pmod 6 \}$
"the equiv. class of $m \pmod 6$"

$\mathbb{Z}_6 = \{$ all equivalence class $\bar{m} \mid m \in \mathbb{Z} \}$

$= \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5} \}$

$\hookrightarrow \{ \ldots, -5, 1, 7, 13, \ldots \}$

$\bar{m}+\bar{n}$ and $\bar{m} \cdot \bar{n}$ are well-defined
so $\mathbb{Z}_6$ is a ring and

$\mathbb{Z} \longrightarrow \mathbb{Z}_6$ is a homomorphism.
$m \longmapsto \bar{m}$

in $\mathbb{Q}(x)$, could have talked about

$f \equiv g \pmod{x}$

would mean $f-g$ is a mult. of x, aka same const. term.

$x^2+2x+3 \equiv 5x^2+4x+3 \pmod{x}$

$f \equiv g \pmod{x^2}$

would mean same const. and linear term.

$x^2+2x+3 \not\equiv 5x^2+4x+3 \pmod{x^2}$

$x^2+2x+3 \equiv 5x^2+2x+3 \pmod{x^2}$

fun: $f \equiv g \mod (x-5)$

$\iff x-5 \mid (f-g)$

$\iff 5$ is a root of $f-g$

$\iff f(5) = g(5)$

Let R be a comm. ring
let $I \subset R$ be an ideal.

for $a, b \in R$, define

$$a \equiv b \pmod{I}$$

to mean $a - b \in I$

example:
$R = \mathbb{Z}$
$I = \langle 6 \rangle$

also $R = \mathbb{Z}[\sqrt{-5}]$
$I = (3, 1+\sqrt{-5})$
on next homework

Prop: it's an equiv. relation

Pf: reflexive: $a \equiv a \pmod{I}$
because $a - a = 0 \in I$

symmetric: if $a \equiv b \pmod{I}$ then
$a - b \in I$
so $b - a = (-1)(a - b) \in I$
so $b \equiv a \pmod{I}$

transitive: if $a \equiv b \pmod{I}$
and $b \equiv c \pmod{I}$

then $a - c = (a - b) + (b - c) \in I$
($a - b \in I$, $b - c \in I$)

so $a \equiv c \pmod{I}$ ☐

Prop: equiv. mod I respects $+$ and $\cdot$:

if $a \equiv a' \pmod{I}$ and $b \equiv b' \pmod{I}$
then $a+b \equiv a'+b' \pmod{I}$ ✓
and $a \cdot b \equiv a' \cdot b' \pmod{I}$ ✓

Pf: $(a'+b') - (a+b) = \underbrace{(a'-a)}_{\in I} + \underbrace{(b'-b)}_{\in I} \in I$

bec. I is closed under $+$.

$$ab - a'b' = ab - ab' + ab' - a'b'$$

$$= a\underbrace{(b-b')}_{\in I} + \underbrace{(a-a')}_{\in I} b' \in I$$

because I is an ideal. ∎

For $a \in R$, define $\bar{a} = \{a' \in R \mid a \equiv a' \pmod{I}\}$
the equiv. class of a

(Some authors call this $a + I$)

Then by prop. above, $\bar{a} + \bar{b} = \overline{a+b}$
and $\bar{a} \cdot \bar{b} = \overline{ab}$ is well-defined.

Let R/I (Say "R mod I") $= \{$all equiv. classes $\bar{a} \mid a \in R\}$

it's a ring.

the map $R \longrightarrow R/I$ is a homomorphism.
$a \longmapsto \bar{a}$

$\mathbb{Z}_6 = \mathbb{Z}/\langle 6 \rangle$ for example