Last time: $\varphi: R \to S$ is a homomorphism if

$$\varphi(1) = 1$$
$$\varphi(a+b) = \varphi(a) + \varphi(b) \quad \forall\, a, b \in R$$
$$\varphi(ab) = \varphi(a)\,\varphi(b)$$

Prop: if $\varphi: R \to S$ is a homomorphism then
$\varphi(0) = 0$
and $\varphi(a-b) = \varphi(a) - \varphi(b)$

Pf $\varphi(0) + \varphi(0) = \varphi(0+0) = \varphi(0)$
add $-\varphi(0)$ to both sides, get
$\varphi(0) = 0$

$\varphi(a-b) + \varphi(b) = \varphi(a-b+b) = \varphi(a)$
add $-\varphi(b)$ to both sides, get
$\varphi(a-b) = \varphi(a) - \varphi(b)$ ∎

If $\varphi: R \to S$ is a hom. then
the image or range of φ

$$\text{im}(\varphi) = \{ s \in S \mid s = \varphi(r) \text{ for some } r \in R \}$$

Prop: $\text{im}(\varphi)$ is a subring of S.
(closed under $+, -, \cdot$; contains 1)

Pf Let $s_1, s_2 \in \text{im}(\varphi)$
write $s_1 = \varphi(r_1)$ and $s_2 = \varphi(r_2)$ for some $r_1, r_2 \in R$
Then $s_1 + s_2 = \varphi(r_1) + \varphi(r_2) = \varphi(r_1 + r_2) \in \text{im}\,\varphi$
$s_1 - s_2 = \varphi(r_1) - \varphi(r_2) = \varphi(r_1 - r_2)$
$s_1 \cdot s_2 = \varphi(r_1) \cdot \varphi(r_2) = \varphi(r_1 \cdot r_2)$
and
$1_S = \varphi(1_R)$.

Example: $\varphi: \mathbb{Z}[x] \longrightarrow \mathbb{Q}$

given by $\varphi(f) = f(\frac{1}{2})$

image is $\mathbb{Z}[\frac{1}{2}] = \left\{ \frac{a}{b} \in \mathbb{Q} \;\middle|\; b \text{ is a power of } 2 \right\}$

if $f = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$

then $\varphi(f) = f(\frac{1}{2}) = a_0 + \frac{a_1}{2} + \frac{a_2}{4} + \cdots + \frac{a_n}{2^n} \in \mathbb{Z}[\frac{1}{2}]$

OTOH, any $\frac{a}{2^k} \in \mathbb{Z}[\frac{1}{2}]$ is $\varphi(a \cdot x^k)$

e.g. $\frac{3}{128} \in \mathbb{Z}[\frac{1}{2}]$ is $\varphi(3x^7)$.

---

notice: $\varphi: R \to S$ is surjective iff $\text{im}(\varphi) =$ all of S.

Def. the kernel of φ (think of a peach pit.)

$$\ker \varphi = \{ r \in R \mid \varphi(r) = 0 \}$$

in prev. example, $f(\frac{1}{2}) = 0$ iff $2x-1 \mid f$ (think about it...)

$\ker \varphi = \{$ all multiples of $2x-1 \}$

$= \{ (2x-1) \cdot g \mid g \in \mathbb{Z}[x] \} \subset \mathbb{Z}[x]$

not a subring of R:

$\varphi(1_R) = 1_S$ and $1_S \neq 0_S$

so $1_R \notin \ker \varphi$

instead, $\ker \varphi$ is an ideal in R.

notice: if $a, b \in \ker \varphi$ then $a+b \in \ker \varphi$

[why? if $\varphi(a) = 0$ and $\varphi(b) = 0$ then $\varphi(a+b) = 0+0 = 0$]

if $r \in R$ and $a \in \ker \varphi$ then $r \cdot a \in \ker \varphi$

[why? if $\varphi(a) = 0$ then $\varphi(r \cdot a) = \varphi(r)\varphi(a)$
$= \varphi(r) \cdot 0 = 0$]

Def A subset $I \subset R$ is an ideal if
$\forall a, b \in I$, $a+b \in I$
and $\forall r \in R$ $\forall a \in I$, $ra \in I$ ||

so $\forall$ homomorphism $\varphi: R \to S$, $\ker \varphi \subset R$ is an ideal.

later: any ideal $I \subsetneq R$ is the ker of some hom.
$\varphi: R \to$ some other ring.

Ideals generated by elements of R.

Given some $a \in R$, the (principal) ideal generated by a is

$$\langle a \rangle = \text{all multiples of } a = \{ ra \mid r \in R \}$$

Some authors call this Ra or aR.

example: in $\mathbb{Z}$, $\langle 2 \rangle$ = even #s

$\langle -2 \rangle$ = same.

$\langle 1 \rangle$ = all of $\mathbb{Z}$

$\langle 0 \rangle = \{0\}$

in $\mathbb{Q}[x]$, $\langle x \rangle = \{ f \mid f(0) = 0 \}$

$$\langle x-1 \rangle = \{ (x-1) \cdot g \mid g \in \mathbb{Q}[x] \} = \{ f \mid f(1) = 0 \}$$

$$\langle x^2+1 \rangle = \{ f \in \mathbb{Q}[x] \mid f(i) = 0 \}$$

because if $f(i) = 0$ then $f(-i) = 0$

Why is $\langle a \rangle$ an ideal?

$$r_1 a + r_2 a = (r_1 + r_2) a$$

$$r \cdot (r_1 a) = (r \cdot r_1) a$$

Notice: $\langle a \rangle$ is the smallest ideal containing a.

if $a \in I$ then $\langle a \rangle \subset I$.

Given $a, b \in R$, the ideal that they generate:

$\langle a, b \rangle = \{$ all R-linear combinations of a and $b\}$

$= \{ ra + sb \mid r, s \in R \}$ Sometimes: $Ra + Rb$

Smallest ideal cont. a and b:

if $a \in I$ and $b \in I$ then $ra \in I$ $\forall r \in R$

$sb \in I$ $\forall s \in R$

$ra + sb \in I$

so $\langle a, b \rangle \subset I$.

Have a lot of experience:

in $\mathbb{Z}$, $\langle 6, 10 \rangle = \{ 6m + 10n \mid m, n \in \mathbb{Z} \}$

$= \langle 2 \rangle$ (Worksheet 2).

in $\mathbb{Q}[x]$, $\langle x^4 + x^3 - x^2 - 2x - 2, \; x^3 - 1 \rangle$

$= \langle x^2 + x + 1 \rangle = \langle -x^2 - x - 1 \rangle$

(Worksheet 17).

By Euclidean algorithm, any ideal in $\mathbb{Z}$ or $F[x]$ can be generated by one element

Later (Friday?)

in $\mathbb{Z}[\sqrt{-5}] = \{ a + b\sqrt{-5} \mid a, b \in \mathbb{Z} \}$,

the ideal $(2, 1 + \sqrt{-5})$ is not principal.

in $\mathbb{Q}[x,y]$ = { things like $3 + 2x + 4xy - 7y^2$ }

the ideal $\langle x, y \rangle = \{ f \mid f(0,0) = 0 \}$
is not principal.

Worksheet last time:

$\varphi : \mathbb{Z}[i] \longrightarrow \mathbb{Z}_2$

$a+bi \longmapsto \bar{a} + \bar{b}$.

Similar: $\varphi : \mathbb{Z}[i] \longrightarrow \mathbb{Z}_5$

$a+bi \longmapsto \bar{a} + \bar{2}\bar{b}$

Homomorphism? $\varphi(1) = \varphi(1+0i) = \bar{1} + \bar{2}\bar{0} = \bar{1}$ ✓

$$\varphi(a+bi + c+di) = \varphi((a+c) + (b+d)i)$$
$$= \overline{a+c} + \bar{2}(\overline{b+d})$$
$$= \bar{a} + \bar{c} + \bar{2}\bar{b} + \bar{2}\bar{d}$$

$$\varphi(a+bi) + \varphi(c+di) = \bar{a} + \bar{2}\bar{b} + \bar{c} + \bar{2}\bar{d}$$ ✓

$$\varphi((a+bi)(c+di)) = \varphi((ac - bd) + (ad+bc)i)$$
$$= \overline{ac} - \overline{bd} + \bar{2}(\overline{ad} + \overline{bc})$$

$$\varphi(a+bi)\,\varphi(c+di) = (\bar{a} + \bar{2}\bar{b})(\bar{c} + \bar{2}\bar{d})$$
$$= \bar{a}\bar{c} + \bar{2}\bar{b}\bar{c} + \bar{2}\bar{a}\bar{d} + \bar{4}\bar{b}\bar{d}$$ ✓

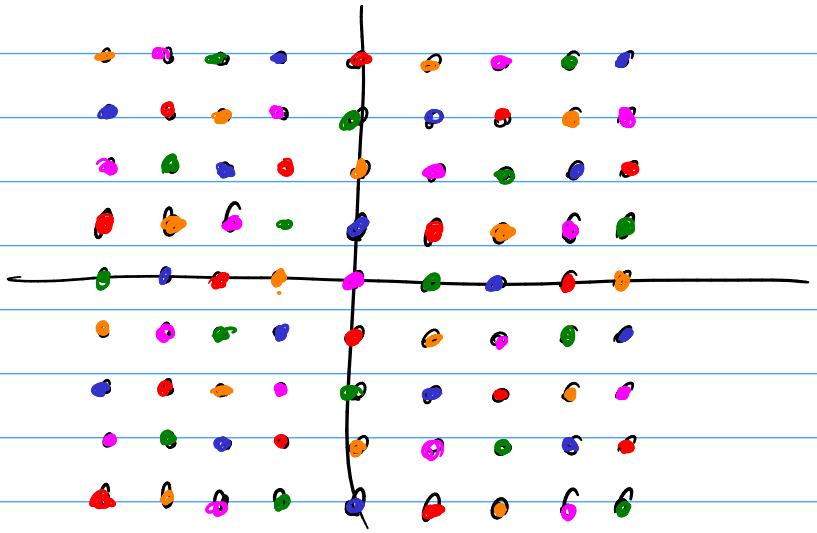
$$-\bar{1} = \bar{4} \text{ in } \mathbb{Z}_5$$

Point: $i^2 = -1$, and in $\mathbb{Z}_5$ we have $\bar{2}^2 = -\bar{1}$

Picture:

$a+bi \longmapsto \bar{a} + 2\bar{b}$

$\mathbb{Z}[i] \longrightarrow \mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$



$i \mapsto \bar{2}$

$\{1\} \mapsto \bar{0}$

$2i \mapsto \bar{4}$

$\hookrightarrow \ker = \{z \in \mathbb{Z}[i] \mid \varphi(z) = \bar{0}\}$

$\varphi(1+2i) = 0$

$\varphi(\text{an mult. of } (1+2i)) = 0$

fun: $\ker \varphi = \langle 1+2i \rangle$.