We already know for $S \subseteq R$ then

S is a subring if for all $a, b \in S$

- I. $a + b \in S$
- II. $0 \in S$
- III. $-a \in S$ ($a + x = 0$ has a solution $x = -a \in S$)

IV. $ab \in S$

Thm 3.6

We want to show for $S \subseteq R$ then S is a subring . . .

Given: if for all $a, b \in S$

i) $a - b \in S$ $\qquad a - b = a + -b$, $-b \in R$

ii) $ab \in S$

Proof: Let $c, d \in S$

IV. we know $cd \in S$ by property ii

prove II Show $0 \in S$

$c \in S$ $\qquad a = c,\ b = c$

~~$a - b = c - c = 0 \in S$~~

$c - c \in S$ by (i) $\qquad c - c = 0$ so $0 \in S$

Legal & short

prove III show $-d \in S$

$0, d \in S$

$0 - d \in S$

$0 - d = -d$ so $-d \in S$

prove I show $c + d \in S$

$c - (-d) = c + d$

$c \in S$ by $-d \in S$

so $c - (-d) \in S$, so $c + d \in S$.

$I \subseteq R$ is an ideal if   definition

a) I is a sub ring

b) if $a \in I$, $r \in R$ then $ar \in I$ and $ra \in I$

Theorem: For $I \subseteq R$ such that

i) $a-b \in I$ for any $a, b \in I$ $\left\langle \begin{array}{l} a+b \in I \\ 0 \in I \\ -b \in I \end{array} \right.$

ii) $ar \in I$ and $ra \in I$ for any $a \in I$, $r \in R$

then I is an ideal

---

a) Let $a, b \in I$.

By (i) $a-b \in I$

By (ii) $ab \in I$ (because $b \in I \Rightarrow b \in R$)

So I is a subring of R

b) by ii) if $a \in I$, $r \in R$ then $ar \in I$.

Qn: Is $\mathbb{Z} \subseteq \mathbb{Z}[x]$ an ideal? $a, b \in \mathbb{Z}$, $p(x) \in \mathbb{Z}[x]$

$a-b \overset{?}{\in} \mathbb{Z}$ $a \cdot b \in \mathbb{Z}$ ← sub-ring

$a \cdot p$? No: $3(x+1) = 3x+3 \notin \mathbb{Z}$

Not an ideal

Is E = polynomials with even constant terms $E \subseteq \mathbb{Z}[x]$ an ideal? example $2x+2 \in E$; $x^2 + 0 \in E$ (even)

$a - b \in E$? yes $(x \cdots + e_1) - (x \cdots + e_2)$ = $x \cdots + (e_1 - e_2)$ (even) $6x^3 + 0 \in E$ (even)

$a \cdot p \in E$? yes $x^3 + x^2 + 2 \in E$

mult. polys   constants multiply → new constant   even(anything) = even

★ HW (Monday) 6.1 #3, 4, 5, 6a, 7ab

Let $R \to S$ be rings, and let $f: R \to S$ be a homomorphism.

Then, for $a, b, 0_R \in R$

i) $f(0_R) = 0_S$

ii) $f(-a) = -f(a)$

iii) $f(a-b) = f(a) - f(b)$

---

proof:

i) $a + 0_R = a$

so $f(a + 0_R) = f(a)$ because f is a function

and $f(a) + f(0_R) = f(a)$ because f is a homomorphism

$+ -f(a) \qquad + -f(a)$ ← can do because S is a ring

$0_S + f(0_R) = 0_S$ defn. of $-f(a)$

$f(0_R) = 0_S$ defn of 0_S. $\square$

ii) $a + -a = 0_R$

$f(a + -a) = f(0_R)$ f is a function

$f(a) + f(-a) = 0_S$ by (i) and f is homomorphism.

$-f(a) \qquad -f(a)$

$0_S + f(-a) = -f(a)$

$f(-a) = -f(a)$ $\square$

iii) $f(a-b) = f(a+(-b))$ defn. of $a-b$

$= f(a) + f(-b)$ f is homomorphism

$= f(a) + -f(b)$ by (ii)

$= f(a) - f(b)$ $\square$

[Center of a ring is a subring
$S \cap R$ is a subring

Let R, S be rings, and let
$f: R \to S$ be a homomorphism ☆
Then the kernel of f: $\ker(f) = \{r \mid r \in R,\ f(r) = 0_S\}$
☆ is a subring of R.

proof: Let $x, y \in \ker(f)$

then $f(x) = 0_S \quad f(y) = 0_S$
defn. of $\ker(f)$

show $x - y \in \ker(f)$

$f(x-y) = f(x) - f(y)$ because f is homomorpho

$= 0_S - 0_S = 0_S$

so ~~ff~~ $x - y \in \ker(f)$

show $xy \in \ker(f)$

$f(xy) = f(x) \cdot f(y)$ f is homomph

$= 0_S \cdot 0_S = 0_S$

so $xy \in \ker(f)$

Is $\ker(f) \leq R$ an ideal?

Let $x \in \ker(f)$ $\quad r \in R$ $\quad xr \in \ker(f)$

$f(x) = 0_S$

$f(xr) = f(x) \cdot f(r)$

$= 0_S \cdot f(r) = 0_S$

yes - $\ker(f)$ is an ideal!