Subrings

Let R be a ring.
A subset $S \subset R$ is a subring if
it's closed under $+, -, \cdot$, and contains 1.
that is: $\forall a, b \in S$, have $a+b, a-b, a \cdot b \in S$
and also $1 \in S$.

Examples: $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

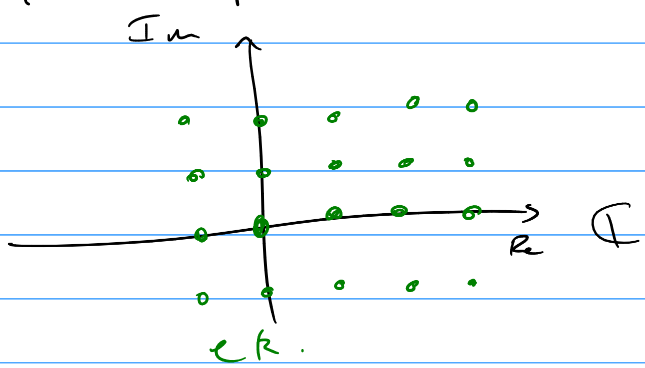
but not $\mathbb{N} = \{0, 1, 2, \dots\} \subset \mathbb{Z}$
closed under $+$ and $\cdot$ but not $-$

not $\{\text{even \#s}\} \subset \mathbb{Z}$
closed under $+, -, \cdot$, but doesn't contain 1

not $\{\text{odd \#s}\} \subset \mathbb{Z}$
closed under $\cdot$ and cont. 1
but not closed under $+$ or $-$

"Gaussian Integers"

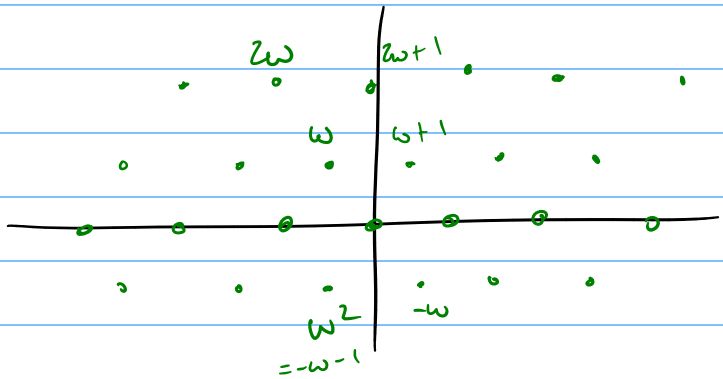
$$\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$$



"Eisenstein Integers"

$$\mathbb{Z}[\omega] = \{ a + b\omega \mid a, b \in \mathbb{Z} \} \subset \mathbb{C}$$

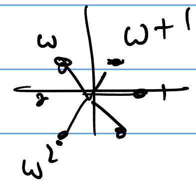
$$\omega = e^{2\pi i/3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$$



why closed under $\cdot$?

$$(a+b\omega)(c+d\omega) = ac + (ad+bc)\omega + bd\omega^2$$

notice $\omega^2 + \omega + 1 = 0$
$\omega^2 = -\omega - 1$



=

$$\mathbb{Z}[\sqrt{2}] = \{ a + b\sqrt{2} \mid a, b \in \mathbb{Z} \} \subset \mathbb{R}$$

can't draw a good picture.
application to Pell's eqn. $x^2 - 2y^2 = 1$

=

$\{ a + b\sqrt[3]{2} \mid a, b \in \mathbb{Z} \}$ is not a subring of $\mathbb{Z}$
not closed under mult.

but $\mathbb{Z}[\sqrt[3]{2}] = \{ a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Z} \} \subset \mathbb{Z}$
is a subring.

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

$$\frac{a}{2^m} + \frac{b}{2^n} = \frac{2^n a + 2^m b}{2^{m+n}}$$

maybe cancel some factors of 2, but that's ok.

Sim. closed under $-$ and $\cdot$

contains $1 = \frac{1}{2^0}$

$\mathbb{Z}_{(2)} = \left\{ \frac{a}{b} \in \mathbb{Q} \;\middle|\; b \text{ is odd} \right\} \subset \mathbb{Q}$

$$\underbrace{\frac{a}{b} + \frac{c}{d}}_{\text{odd}} \rightsquigarrow = \frac{ad+bc}{\underbrace{bd}_{\text{odd}}}$$

if we reduce the fraction, denom is still odd.

Sim. closed under $-$ and $\cdot$

Contains $1 = \frac{1}{1}$

---

upper triangular matrices

$$\left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{R} \right\} \subset M_2(\mathbb{R})$$

check: closed under $+, -, \cdot$. contains $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

could do bigger matrices $\begin{pmatrix} \cdot & \cdot & \cdot & \cdot \\ & \cdot & \cdot & \cdot \\ 0 & & \ddots & \vdots \end{pmatrix}$

or lower triangular...

matrices of the form

$$\left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \,\middle|\, a, b \in \mathbb{R} \right\} \subset M_2(\mathbb{R})$$

check: add, subtract, multiply two of these
$\rightsquigarrow$ get another of the same kind.

contains $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$$\{\text{cont. functions } [0,1] \to \mathbb{R}\}$$

$$\subset \{\text{all functions } [0,1] \to \mathbb{R}\}$$

Isomorphisms

"same shape"

Let R, S be rings.

Def a map $\varphi: R \to S$ is an <u>isomorphism</u>

if it's a bijection,
$\varphi(a+b) = \varphi(a) + \varphi(b)$ $\forall\, a, b \in R$
$\varphi(ab) = \varphi(a) \cdot \varphi(b)$
and $\varphi(1) = 1$

R and S are iso<u>morphic</u> if $\exists$ an isomorphism
$\varphi: R \to S$.

think of R and S as
"the same ring"

Examples:

(1) $\varphi : \mathbb{C} \longrightarrow \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \middle| \ a, b \in \mathbb{R} \right\} \subset M_2(\mathbb{R})$

$a+bi \longmapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$

lot to check here!

$1 \longmapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$i \longmapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \rightsquigarrow$ check that $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$

just as $i^2 = -1$.

(2) complex conjugation

$\varphi : \mathbb{C} \longrightarrow \mathbb{C}$

$a+bi \longmapsto a-bi$

or $z \longmapsto \bar{z}$

know that $\overline{zw} = \bar{z}\,\bar{w}$ and $\overline{z+w} = \bar{z} + \bar{w}$

and $\bar{1} = 1$.

(3) Chinese Remainder Theorem

$\mathbb{Z}_{12} \longrightarrow \mathbb{Z}_3 \times \mathbb{Z}_4$

$\bar{a} \longmapsto (\bar{a}, \bar{a})$

$\bar{0} \longmapsto (\bar{0}, \bar{0})$ continued on worksheet.

$\bar{1} \longmapsto (\bar{1}, \bar{1})$

$\bar{2} \longmapsto (\bar{2}, \bar{2})$

$\bar{3} \longmapsto (\bar{0}, \bar{3})$

$\bar{4} \longmapsto (\bar{1}, \bar{0})$

$\bar{5} \longmapsto (\bar{2}, \bar{1})$

$\bar{6} \longmapsto (\bar{0}, \bar{2})$

$\vdots$