Examples of Rings

$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

Let $d \in \mathbb{Z}$.

$\mathbb{Z}[\sqrt{d}] \subseteq \mathbb{Q}(\sqrt{d})$.

Then
d is square free if $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}$.

Otherwise

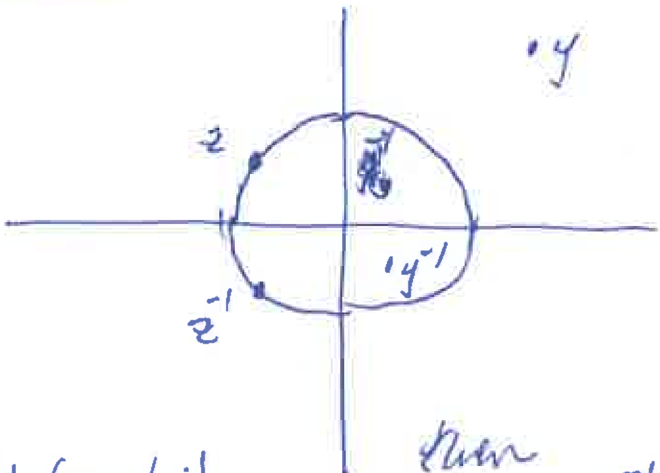
$\mathbb{Q}(\sqrt{d})$
$|$ with $\dim_{\mathbb{Q}}(\mathbb{Q}(\sqrt{d})) = 2$ and
$\mathbb{Q}$
$m_{\sqrt{d},\mathbb{Q}}(x) = x^2 - d$.

If $d \in \mathbb{Z}_{>0}$ then $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{R}$

If $d \in \mathbb{Z}_{<0}$ then $\mathbb{Q}(\sqrt{d}) \not\subseteq \mathbb{R}$.

Always $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{C}$.

Inverses in $\mathbb{C}$



Since
$(a+bi)\dfrac{(a-bi)}{a^2+b^2} = 1$
then
$y^{-1} = \dfrac{\bar{y}}{|y|^2} = \dfrac{1}{r}e^{i\theta}$

when $y = a+bi = re^{i\theta}$.

If $d \in \mathbb{Z}_{>0}$ and $y = a + \sqrt{d}\, b$ then

$$(a+b\sqrt{d})(a-b\sqrt{d}) = a^2 - b^2 d^2$$

and
$$y^{-1} = \frac{a - b\sqrt{d}}{a^2 - b^2 d^2}$$

<u>Looking at $\mathbb{Q}[\sqrt{d}]$ as 2×2 matrices</u>

If $\mathbb{Q}[\sqrt{d}] \neq \mathbb{Q}$ then

$\mathbb{Q}[\sqrt{d}]$ has $\mathbb{Q}$-basis $\{1, \sqrt{d}\}$

The matrix of multiplication by 1, with respect to the basis $\{1, \sqrt{d}\}$ is
$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
The matrix of multiplication by $\sqrt{d}$, with respect to the basis $\{1, \sqrt{d}\}$ is
$$\begin{pmatrix} 0 & d \\ 1 & 0 \end{pmatrix}.$$
So
$$\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$$
$$\cong \left\{ \begin{pmatrix} a & bd \\ b & a \end{pmatrix} \,\middle|\, a, b \in \mathbb{Q} \right\}$$
and
$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$$
$$\cong \left\{ \begin{pmatrix} a & bd \\ b & a \end{pmatrix} \,\middle|\, a, b \in \mathbb{Z} \right\}.$$

Then

$$\det\begin{pmatrix} a & bd \\ b & a \end{pmatrix} = a^2-b^2d \quad \text{and} \quad \mathrm{tr}\begin{pmatrix} a & bd \\ b & a \end{pmatrix} = 2a$$

and

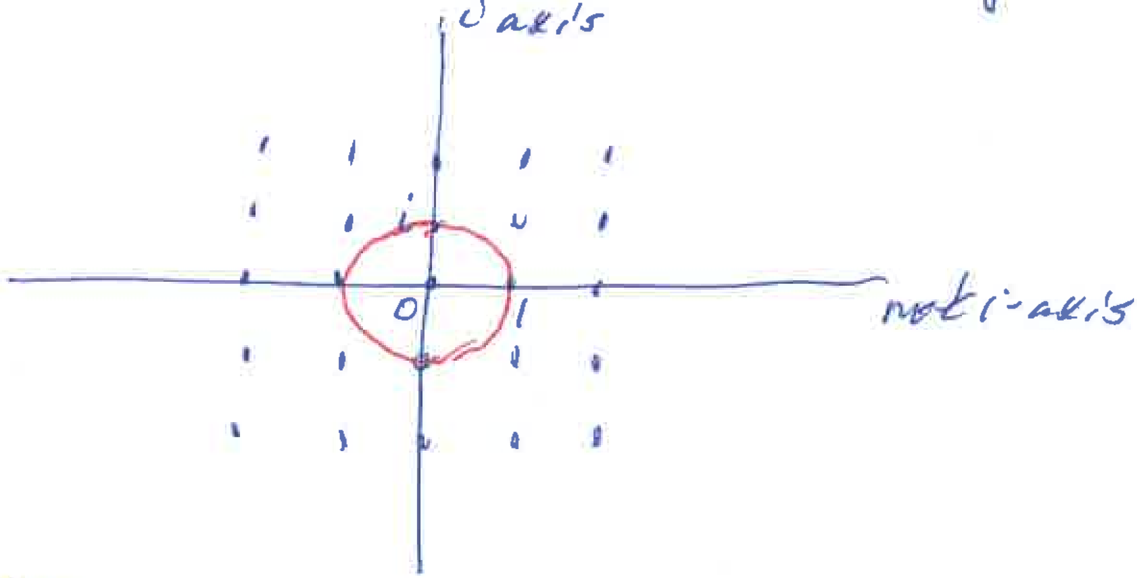
$$\begin{pmatrix} a & bd \\ b & a \end{pmatrix}^{-1} = \frac{1}{a^2-b^2d}\begin{pmatrix} a & -bd \\ -b & a \end{pmatrix}$$

<u>Good examples</u> $d \in \{2,1,0,-1,-2,-3\}$.

$$\mathbb{Z}[\sqrt{0}] = \mathbb{Z} \subseteq \mathbb{Q}(\sqrt{0}) = \mathbb{Q}$$

$$\mathbb{Z}[\sqrt{1}] = \mathbb{Z} \subseteq \mathbb{Q}(\sqrt{1}) = \mathbb{Q}.$$

$\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$ is the <u>Gaussian integers</u>



Then $\mathbb{Z}[i]^\times = \{1,-1,i,-i\}$

and

$$\mathbb{Z}[i] \cong \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \;\middle|\; a,b \in \mathbb{Z} \right\}.$$

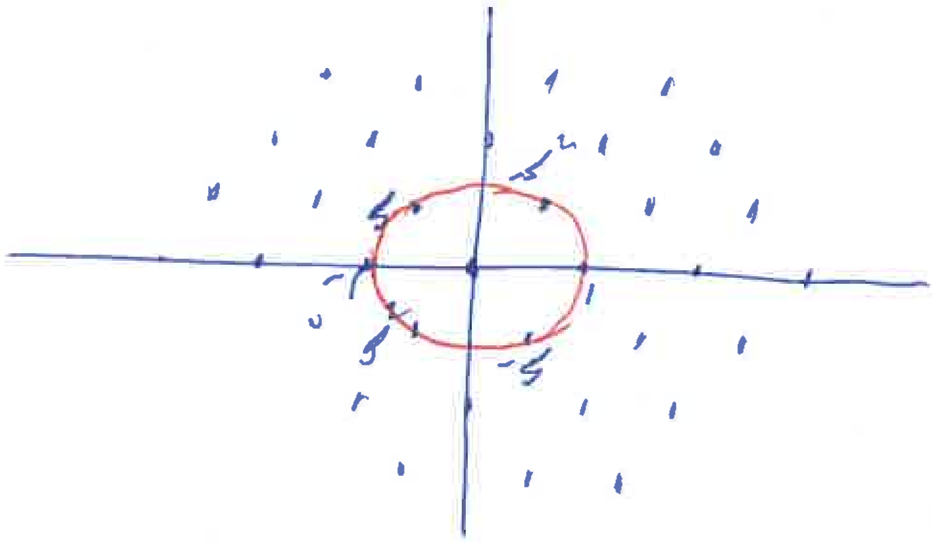
Note $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ corresponds to $i^2 = -1$.

Key point: $\boxed{-3 \equiv 1 \bmod 4.}$

The ring of integers of $\mathbb{Q}(\sqrt{-3})$ is

$$\mathbb{Z}[\zeta] = \left\{ \frac{a+b\sqrt{3}\,i}{2} \;\middle|\; \begin{array}{l}\text{both } a,b \text{ are even or}\\ \text{both } a,b \text{ are odd,}\\ a,b\in\mathbb{Z}\end{array} \right\}$$

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



$\mathbb{Z}[\zeta]^\times = \{1, -\zeta^2, \zeta, -1, \zeta^2, -\zeta\}$

Proposition

(a) $(\mathbb{Z}[\zeta], |\cdot|^2)$ is a Euclidean domain

(b) $\mathbb{Z}[\zeta]$ is a PID

(c) $\mathbb{Z}[\zeta]$ is a UFD

(d) $\mathbb{Z}[\zeta]$ is a Dedekind domain

(e) $\mathbb{Z}[\zeta]$ has field of fractions $\mathbb{Q}(\sqrt{-3})$

(f) If $d \in \mathbb{Z}[\zeta]$ then the principal ideal $d\mathbb{Z}[\zeta]$ is a 6-spoked ray emanating from 0 with distances d.

Which are the maximal ideals? 16.05.2024
Which are the prime ideals? Algebra Lect. 33 (5)
A. Ram

The ring $\mathbb{Z}[\sqrt{-5}]$ is not a UFD,
For example:

$$3\cdot 3 = 9 = (2+\sqrt{-5})(2-\sqrt{-5}) \quad \text{and}$$

$$2\cdot 3 = 6 = (1+\sqrt{-5})(1-\sqrt{-5}).$$

The ring $\mathbb{Z}[\sqrt{-5}]$ is not a PID (and not a Euclidean domain).

The ring $\mathbb{Z}[\sqrt{-5}]$ is a Dedekind domain.

Theorem (see Shult and Surowski Prop. 9.A.1)
Let $d\in\mathbb{Z}_{>0}$ and let $\mathbb{A}(\sqrt{-d})$ be the ring of integers of $\mathbb{Q}(\sqrt{-d})$.

(a) $(\mathbb{A}(\sqrt{-d}), |\cdot|^2)$ is a Euclidean domain if and only if $d\in\{1, 2, 3, 7, 11\}$

(b) $\mathbb{A}(\sqrt{-d})$ is a PID if and only if $d\in\{1, 2, 3, 7, 11, 19, 43, 67, 163\}$.

(c) $\mathbb{A}(\sqrt{-d})$ is a UFD if and only if $\mathbb{A}(\sqrt{-d})$ is a PID.

(d) $\mathbb{A}(\sqrt{-d})$ is a Dedekind domain.