Ex The Gaussian Integers $= \mathbb{Z}[i] = \{a_0 + a_1 i + a_2 i^2 + \cdots a_k i^k : a_j \in \mathbb{Z}\ \forall \mathbb{Z}\}$

$= \{A + Bi : A, B \in \mathbb{Z}\}$.

This is an integral domain:

If $(a+bi)(c+di) = 0$, then

$$\left.\begin{aligned} ac - bd &= 0 \\ ad + bc &= 0 \end{aligned}\right\}$$ is there a nonzero solution $a+bi \neq 0$? $c+di \neq 0$?

For complex analysis

$\Rightarrow \quad |(a+bi)(c+di)| = |a+bi|\,|c+di|$

$= \sqrt{a^2+b^2} \cdot \sqrt{c^2+d^2} = 0$

$\Rightarrow$ either $a+bi = 0$ or $c+di = 0$.

$\therefore$ $\mathbb{Z}[i]$ is an integral domain.

Note: It's useful to have a "norm" that is multiplicative.

Also $\mathbb{Z}[i]$ is a UFD:

Units of $\mathbb{Z}[i]$: From complex analysis, in $\mathbb{Q}[i]$,

$$(a+bi)^{-1} = \frac{a-bi}{a^2+b^2}$$

$$= \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2} i$$

This in $\mathbb{Z}[i] \Leftrightarrow a^2+b^2 = 1$

$\Rightarrow a = \pm 1, b = 0$

or $a = 0, b = \pm 1$.

Units in $\mathbb{Z}[i]$ are $1, -1, i, -i$.

Let's check if $\mathbb{Z}[i]$ is a UFD:

Suppose $(a+bi)(c+di) = z$ for $a,b,c,d,$
and: $(a_2+b_2i)(c_2+d_2i) = z$ $a_2,b_2,c_2,d_2 \in \mathbb{Z}$.

$\Leftrightarrow$ $ac-bd = a_2c_2 - b_2d_2$
$ad+bc = a_2d_2 + b_2c_2$.

Elements a of a comm ring R with 1 are irreducible $\Leftrightarrow$ [a is not a unit and is nonzero] and $a=bu$ with $b,u \in R \Rightarrow b$ or u is a unit.

An element p of a comm. ring with 1 is <u>prime</u> if whenever $p \mid ab$ for $a,b \in R$, then $p \mid a$ or $p \mid b$.

($a = pm$ for some $m \in R$.)

A <u>principal ideal domain</u> (PID) is an integral domain R s.t. every ideal in R is principal.

<u>Fact</u>: In a PID an ideal $\langle p \rangle$ is maximal $\Leftrightarrow$ p is irreducible.

<u>Proof</u>: If p is reducible, $p = ab$, with a & b not units, and $\langle p \rangle \subseteq \langle a \rangle$.

But a is not $a = pr$ for some $r \in R$,
(because if so $p = (pr)b \Rightarrow rb = 1$
$\Rightarrow b$ is a unit. $\times$).

$\therefore \quad \langle p \rangle \subsetneq \langle a \rangle.$

Note – this argument tells us that $\langle f \rangle = R \Leftrightarrow f$ is a unit.

Also, $\langle a \rangle \neq R$ because if $\langle a \rangle = R$, $1 = ar$ for some $r \in R$, but a is not a unit. $\times$.

$\therefore \langle p \rangle \subsetneq \langle a \rangle \subsetneq R \quad \therefore \langle p \rangle$ is not maximal. ✓

Next, suppose $\langle p \rangle$ is not maximal $\Rightarrow \exists$ $a \in R$ s.t. $\langle p \rangle \subsetneq \langle a \rangle \subsetneq R$.

$\Rightarrow$ a is not a unit and $p = ab$ for some $b \in R$. Also, b is not unit, because otherwise $pb^{-1} = a \in \langle p \rangle$ (not true that $\langle a \rangle = \langle p \rangle$.)

$\Rightarrow p$ is reducible. ✓

$\boxtimes$

Euclidean Domain: An integral domain R is called a Euclidean domain if there exists a Euclidean function $d: R \longrightarrow \cancel{\mathbb{R}_{\geq 0}}$ $\mathbb{N} \cup \{0\}$, $d(0) = 0$, such that the division algorithm works:

For any $a \in R$, $b \in R \setminus \{0\}$, there exists $q \in R$, $r \in R$ s.t.

$$a = bq + r, \text{ where}$$
$$0 \leq d(r) < d(b)$$

Also required: $d(a) \leq d(ab)$ $\forall a, b \in R$.

q & r need not be unique. Example: in $\mathbb{Z}$, $d(z) = |z|$, $q = 2 \cdot 4 + 1 = 3 \cdot 4 + -3$

$d(1) < d(4)$ ✓ $\quad d(-3) < d(4)$ ✓

~~Note: q & r are unique!~~

Examples: • $R = \mathbb{Z}$, $d : \mathbb{Z} \to \mathbb{R}_{\geq 0}$ is

$$d(r) = |r|.$$

In fact, given $a \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus \{0\}$,

$\exists!\, q, r$ s.t. $0 \leq r < |b|$ s.t.

$$a = qb + r$$

• $R = \mathbb{R}[x] = \{\text{polynomials with real coeff.}\}$.

$d(f(x)) = \deg(f(x))$.

Given $f(x) \in \mathbb{R}[x]$, $g(x) \in \mathbb{R}[x] \setminus \{0\}$,

$\exists!\, q(x), r(x)$ s.t.

$$f(x) = g(x) q(x) + r(x) \text{ with}$$
$$0 \leq \deg(r(x)) < \deg(g(x))$$

Similar with $\mathbb{R}$ replaced by any field.

A GCD (greatest common divisor) of a, b in an integral domain R is a number $d \in R$ s.t. $d | a$ and $d | b$ and if another element d' satisfies the same property then

$$d' | d.$$

In a Euclidean domain, the Euclidean algorithm works to find the gcd of two elements a, b.

Let $d(a) \geq d(b)$.

Divide:

$$\text{①} \quad a = b q_1 + r_1$$

$$\text{②} \quad q_1 = r_1 q_2 + r_2$$

$$\text{③} \quad q_2 = r_2 q_3 + r_3$$

$$\vdots$$

$$q_k = r_k q_{k+1} + 0 \quad \text{stop}$$

$$\Rightarrow \underline{r_k = GCD}$$

$\Rightarrow$ <u>Bezout Identity</u>

$$\exists\, m, n \in R \text{ s.t.}$$

$$(a,b) = GCD = ma + nb.$$

Cor - Every ED is a PID

Domain

$$ID \supsetneq UFD \supsetneq PID \supsetneq ED \supsetneq \text{Fields} \supsetneq \text{Alg. Closed Fields}$$