$\boxed{\text{ED. PID. UFD.}}$ How to check a ID is not ED?

1. A property of ED (universal side divisor)

Def: Let R be ID. An element $0 \neq a \in R \setminus U(R)$ is called a universal side divisor if for every $b \in R$, either $a \mid b$ or $a \mid b+u$ for some $u \in U(R)$

Equivalently, $a \in R \setminus U(R)$ is a universal side divisor if $R = Ra + U(R) \cup \{0\}$

Rmk If a is a universal side divisor of R then Ra is a maximal ideal of R. also $m_i \not\Rightarrow$ a usd.

proof: 1° $Ra \neq R$ since a not unit

2° sps $Ra \subsetneq I$, $\forall\, i \in I \setminus Ra$, $\exists\, r \in R$

$i = ra + u$ for some $u \in U(R)$

u is nonzero since $i \notin Ra$

$\Rightarrow$ $R = (u) = (i - ra) \subseteq I$ $\Rightarrow$ $I = R$

$\Rightarrow$ Ra is maximal.

Rmk. The converse is not true.

take $R = \mathbb{Z}$, $a = 5$, (5) is maximal.

But $3 \equiv 3$ or $-2 \mod 5$

$3, -2$ not unit.

Prop. If R is a Euclidean domain, then R has a universal side divisor.

Let norm: $\phi: R \to \mathbb{N}$ with $\phi(0) = 0$

1. If R is a field. we can set constant norm s.t.

$\phi(0) = 0$, $\phi(r) = 1 \quad \forall r \in U(R)$

then $a = 0$ is a universal side divisor as our def.

Now sps R is not a field.

Let $S := \{ \phi(r) : 0 \neq r \in R \setminus U(R) \}$

since $S \neq \phi$, S has and minimal element

Say $\phi(a)$

let $b \in R$. so $\exists\, c, d \in R$ s.t $b = ca + d$

either $d = 0$ or $\phi(d) < \phi(a)$ if $d = 0$, $a \mid b$

if $\phi(d) < \phi(a)$, since $\phi(d) \notin S \Rightarrow d \in U(R)$

Set $u := -d$, then $a \mid b + u$.

E.g. $\mathbb{Z}$, $\pm 2, \pm 3$ universal side divisor (norm. $|\,|$)

observe: $r \equiv \underbrace{0, \pm 1}_{\in\, U(R) \cup \{0\}} \mod 3$

E.g. $\mathbb{Z}[i]$ norm $r = a+bi \Rightarrow \phi(r) = a^2+b^2$

Sps. $a = x_1+y_1 i$ $b = x_2+y_2 i$ $\phi(a) = x_1^2+y_1^2$ $\phi(b) = x_2^2+y_2^2$

$$ab = x_1x_2 - y_1y_2 + (x_1y_2 + x_2y_1)i$$

$$\phi(ab) = (x_1x_2 - y_1y_2)^2 + (x_1y_2 + x_2y_1)^2$$

$$= x_1^2x_2^2 + y_1^2y_2^2 + x_1^2y_2^2 + x_2^2y_1^2$$

$$= (x_1^2+x_2^2)(y_1^2+y_2^2) = \phi(a)\phi(b)$$

it shows if $a \in U(\mathbb{Z}[i])$, $\exists\, b \in U(\mathbb{Z}[i])$

$ab = 1 \Rightarrow$ $\phi(ab) = \phi(a)\phi(b) = \phi(1) = 1$

$\Rightarrow \phi(a)$ or $\phi(b) = \pm 1$

$\Rightarrow U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$

Set $S := \{a^2+b^2 \mid a, b \in \mathbb{Z},\ a^2+b^2 > 1\}$

so the universal side divisor is $\pm 1 \pm i$

E.g. ED $\Rightarrow \exists$ usd

in other words, $\nexists$ usd $\Rightarrow$ not a ED.

Let $R = \mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$

Step 1. Specify $U(R)$

use the same approach as $\mathbb{Z}[i]$

Consider the field of fraction of R, which is $\mathbb{Q}(\sqrt{-19})$

and take the field norm which is $N(a) = a\bar{a}$

complex conj.

Since $-19 \equiv 1 \mod 4$ you can check

$$N: R \longrightarrow \mathbb{N}$$

i.e. $\forall r \in R$, $N(r) \in \mathbb{N}$ and N is multiplicative

i.e $N(ab) = N(a)N(b)$

it shows if $a, b \in \mathbb{Z}[\frac{1+\sqrt{-19}}{2}] = R$ and

forces

$ab = 1 \Rightarrow N(a)N(b) = N(1) = 1 \Rightarrow N(a) = 1$

So $U(R) = \{\pm 1, 0\}$

Step 2. Sps. $u \in R$ is a universal side divisor

note that if $a, b \in \mathbb{Z}$, $b \neq 0$ then

$N(a + b(\frac{1+\sqrt{-19}}{2})) = a^2 + ab + 5b^2 \geq 5$

So the smallest nonzero values of N on R is

1 for ± 1

4 for ± 2

Now if u is usd $u | 2$ or $u | 2 \pm 1$

If $2 = \alpha\beta$, $4 = N(\alpha)N(\beta) \Rightarrow \alpha$ or β has norm 1.

hence the only divisor of 2 in R are $\{\pm 1, \pm 2\}$

Similarly ________ 3 in R are $\{\pm 1, \pm 3\}$

$\Rightarrow$ u only can be ± 2 or ± 3

take $x = \frac{1+\sqrt{-19}}{2}$,

check that none of $x, x\pm 1$ are divisible by ± 2 or ± 3

$\Rightarrow$ R has no usd $\Rightarrow$ R is not a ED.

above things is a explanation of Dummit.

Now we use another viewpoint. it's introduced by

KEITH CONRAD.

A more useful definition is:

A ID called ED if $\exists$ function $d: R - \{0\} \to \mathbb{N}$ s.t

(1). $d(a) \leq d(ab)$, $\forall a, b \in R$, $a, b \neq 0$

(2). $\forall a, b \in R$, $b \neq 0$ $\exists q, r$ s.t $a = bq + r$, $r = 0$ or

$d(r) < d(b)$.

The additional condition is d-inequality $d(a) \leq d(ab)$

But the two defs are equiv.

def2 $\Rightarrow$ def1 is obvious. What about def1 $\Rightarrow$ def2?

Let (R, d) ED, define: $\tilde{d}(a) = \min_{b \neq 0} d(ab)$

- $\tilde{d}(a) \leq d(a)$ since $\tilde{d}(a) \leq d(a \cdot 1)$

- $\tilde{d}(1) = \min_{b \neq 0} d(b)$

- $\forall u \in U(R)$

Thm. $\hat{d}$ satisfy d-inequality. i.e def 1 $\Rightarrow$ def 2.

$\forall a, b \neq 0$, $a, b \in R$. $\hat{d}(a) \le \hat{d}(ab)$

Now need to show R admits Euclidean Algorithm.

$\forall a, b \in R$, $b \neq 0$. set

Set $\hat{d}(b) = d(bc)$ for some $0 \neq c \in R$

then $a = (bc) q_0 + r_0$, $r_0 = 0$ or $d(r_0) < d(bc)$

Set $q = cq_0$ and $r = r_0$ so $a = bq + r$, if $r_0 = 0$, done.

assume $r_0 \neq 0$

$d(bc) = \hat{d}(b)$ and $\hat{d}(r) \le d(r)$

$\Rightarrow d(r) = d(r_0) < d(bc) \Rightarrow \hat{d}(r) < \hat{d}(b)$

i.e. $a = bq + r$, $r = 0$ or $\hat{d}(r) < \hat{d}(b)$. done.

By Abstract-Algebra-Dummit we know that q and r may not unique.

E.g. in $\mathbb{Z}[i]$

$$1+8i = \underbrace{(2-4i)}\,\underbrace{(-1+i)}_{q_1}\underbrace{-1+2i}_{r_1}$$

$$1+8i = (2-4i)\underbrace{(-2+i)}_{q_2} + \underbrace{1-2i}_{r_2}.$$

$N(r_1) = N(r_2) = 5 < N(2-4i) = 20$.

Thm: If R is ED where quotient and remainder are unique then R is a field or $R = F[T]$ for a field F

pf: Uniqueness in the division algorithm. Amer. Math Monthly 1967.

In our homework we do some exercise about quadratic ring.

that is.

Def A quadratic ring is a ring of the form $\mathbb{Z}[\gamma]$ where γ is a complex number that is a root of an irreducible quadratic poly. $T^2+aT+b \in \mathbb{Z}[T]$ with leading coefficient 1.

We call $\mathbb{Z}[\gamma]$ real if $\gamma \in \mathbb{R}$ and imaginary otherwise.

ie $\quad \mathbb{Z}[\gamma] \cong \mathbb{Z}[T]/T^2+aT+b$

$$\gamma = \frac{-a \pm \sqrt{a^2-4b}}{2}$$

if a even, $\quad \mathbb{Z}[\gamma] = \mathbb{Z}[\sqrt{m}]$ where $m = (\frac{a}{2})^2 - b$

if a odd $\quad \mathbb{Z}[\gamma] = \mathbb{Z}[\frac{1+\sqrt{m}}{2}] \qquad m = a^2-4b.$

and since $\gamma^2 = -a\gamma - b \in \mathbb{Z}\gamma + \mathbb{Z}$

you can prove $\mathbb{Z}[\gamma] = \mathbb{Z} + \mathbb{Z}\gamma = \{a+b\gamma \mid a, b \in \mathbb{Z}\}$.

Rmk. $\mathbb{Z}[\sqrt{m}] \neq \mathbb{Z}[\frac{1+\sqrt{m}}{2}]$

e.g. $\mathbb{Z}[\frac{1+\sqrt{5}}{2}] \neq \mathbb{Z}[\sqrt{5}]$ although $\mathbb{Q}(\frac{1+\sqrt{5}}{2}) = \mathbb{Q}(\sqrt{5})$

$\frac{1}{2}+\frac{1}{2}\sqrt{5}$

γ is one root of $T^2+aT+b=0$, the orther root is called the "conjugation" of γ, denoted by $\bar{\gamma}$

$\bar{\gamma}=-a-\gamma$.

if $\alpha = x+y\gamma \in \mathbb{Z}[\gamma]$ then $\bar{\alpha} = x-ay-y\gamma$

E.g. if $\gamma=\sqrt{2}$. $\overline{x+y\sqrt{2}} = x-y\sqrt{2}$.

if $\gamma=\frac{1+\sqrt{5}}{2}$. $\overline{x+y\gamma} = x+y-y\gamma$.

or $\overline{x+y\cdot\frac{1+\sqrt{5}}{2}} = x+y\frac{1-\sqrt{5}}{2} = x+y-y\frac{1+\sqrt{5}}{2}$

There is a special norm for quadratic ring is define to be $N(\alpha)=\alpha\bar{\alpha} = x^2-axy+by^2$

this is an integer. $N(\alpha)=0 \iff \alpha=0$.

if $c\in\mathbb{Z}$, $N(c)=c^2$

$N(\pm 1)=1$, if $\gamma=\sqrt{m}$ $N(x+y\sqrt{m})=x^2-my^2$.

E.g. $\mathbb{Z}[\sqrt{2}]$, $x+y\sqrt{2}$, $N(x+y\sqrt{2})=x^2-2y^2$ $\Big\}$ $\pm$

E.g. $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ $x+y\gamma$ $N(x+y\gamma)=x^2+xy-y^2$

E.g. $\mathbb{Z}[\sqrt{-5}]$ $N(x+y\gamma)=x^2+5y^2$ only +

Thm. $N(\alpha\beta) = N(\alpha)N(\beta)$

Some $\mathbb{Z}[\gamma]$ take $d(\alpha) = |N(\alpha)|$ become ED.

So 1. is q-ring ED? $d = |N|$

2. is q-ring norm-ED (under the special norm. ED)

In 2004. $\mathbb{Z}[\sqrt{14}]$ is shown be ED. but

$\boxed{\text{Thm}}$ $\mathbb{Z}[\sqrt{14}]$ is not norm-ED.

aim. show $1+\sqrt{14} = 2\gamma + \rho$ where $|N(\rho)| < |N(2)| = 4$ no solu.

Assume. $\exists$ $\gamma = m + n\sqrt{14}$, $\rho = a + b\sqrt{14}$

then $1+\sqrt{14} = (2m+a) + (2n+b)\sqrt{14}$

$\Rightarrow 2m+a = 1 \quad 2n+b = 1 \Rightarrow a = 1-2m \quad b = 1-2n.$

$$\left| (1-2m)^2 - 14(1-2n)^2 \right| < 4$$

$$\Rightarrow \underbrace{(2m-1)^2 - 14(2n-1)^2}_{\text{odd.}} = 0, \pm 1, \pm 2, \pm 3$$

only $\pm 1, \pm 3$ and $2m-1$ odd, $2n-1$ odd.

odd number square $\equiv 1 \mod 8$

$\Rightarrow (2m-1)^2 - 14(2n-1)^2 = 3$

mod 7 $\Rightarrow (2m-1)^2 \equiv 3 \mod 7.$

$1^2 = 1 \quad 2^2 = 4 \quad 3^2 = 2 \quad 4^2 = 2 \quad 5^2 = 4 \quad 6^2 = 1$ no 3.

↯.

$\boxed{\text{Thm}}$. Let R be PID. $F = \text{frac} R$ $f(t) \in R[t]$ monic

a root in $f(t)$ in F must in R. this is called Integral closed domain.

pf. a root of $f(t)$ in F can be write as $x = \frac{a}{b}$ where

a, b coprime in R if R PID.

(if $x = \frac{a}{b}$ take $(d) = (a, b)$. $\frac{a'd}{b'd} = \frac{a'}{b'}$ reduced form).

let $f(t) = t^n + c_{n-1}t^{n-1} + \cdots + c_1 t + c_0$, $n \geq 1$

$0 = f(a/b) = \frac{a^n}{b^n} + \cdots + c_1 \frac{a}{b} + c_0$.

$\Rightarrow 0 = a^n + c_{n-1} a^{n-1} b + \cdots + c_1 a b^{n-1} + c_0 b^n$. i.e. PID must be ICD.

i.e. $b | a^n$ i.e $b | 1$ $\Rightarrow$ $a/b = ab^{-1} \in R$

$\boxed{\text{Thm}}$. if m is an integer that is not square and has a repeated prime factor. then $\mathbb{Z}[\sqrt{m}]$ not PID.

pf: Let p prime, $p^2 | m$, $\Rightarrow$ $m = p^2 m'$

$\sqrt{m'} = \sqrt{m}/p$, $\sqrt{m'}$ is in $\text{frac}(\mathbb{Z}[\sqrt{m}])$ but $\sqrt{m'} \notin \mathbb{Z}[\sqrt{m}]$

now take. $f(t) = t^2 - m'$ monic in $\mathbb{Z}[t] \subset \mathbb{Z}[\sqrt{m}][t]$

by Thm before. $\mathbb{Z}[\sqrt{m}]$ not PID.

ED $\Rightarrow$ PID $\Rightarrow$ ICD

$\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ $\mathbb{Z}[\sqrt{5}]$

$\boxed{\text{Thm}}$. In quadratic ring, $\mathbb{Z}[\gamma]$, units are the elements with norm ± 1.

pruf: If $\alpha\beta = 1$ in $\mathbb{Z}[\gamma]$ $N(\alpha)N(\beta) = N(1) = 1$.

$N(\alpha), N(\beta) = \pm 1$

conversely if $N(\alpha) = \pm 1$ then $\alpha\bar{\alpha} = \pm 1$, α has inverse $\mp\bar{\alpha}$

$\boxed{\text{E.g}}$ $\mathbb{Z}[\sqrt{2}]$

$x^2 - 2y^2 = \pm 1$ i.e $1+\sqrt{2}$ unit

and $(1+\sqrt{2})^n$ unit. inf. many.

$\boxed{\text{E.g}}$ $\mathbb{Z}[\sqrt{3}]$

$x^2 - 3y^2 = \pm 1 \Rightarrow 2+\sqrt{3}$ unit. inf many.

$\boxed{\text{E.g}}$ $\mathbb{Z}[\sqrt{-2}]$

$x^2 + 2y^2 = 1 \Rightarrow \pm 1$ two units.

$\boxed{\text{E.g}}$ $\mathbb{Z}[i]$

$x^2 + y^2 = 1 \Rightarrow \pm 1, \pm i$ 4 units.