Dedekind domains. (Sect. 2.2)

Definition: An integral domain A is called Dedekind if A is noetherian, integrally closed, and every non-zero prime ideal is maximal

Ex: 1) $K/\mathbb{Q}$ finite,
$\Rightarrow \mathcal{O}_K$ Dedekind

2) $\mathbb{Z}[T]$ not Dedekind

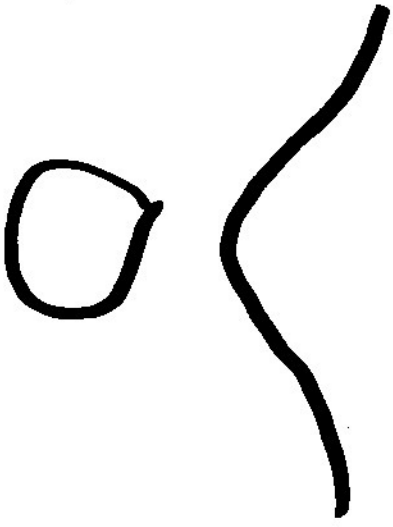
Why?

* Geometry: "affine smooth curves"

are the spectra of Dedekind rings

e.g.

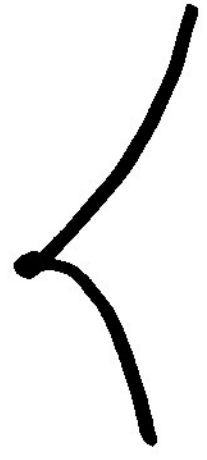
$k[x,y]/y^2 - x(x-1)(x+1)$ char $k \neq 2$



"affine elliptic curve"

but not

$k[x,y]/y^2 - x^3$



* Arithmetic: $\mathcal{O}_K$ $\neq$, $K/\mathbb{Q}$ finite, is a Dedekind, but not nec. UFD

E.g.: $K = \mathbb{Q}(\sqrt{-5})$

$\Rightarrow 3^2 = (2-\sqrt{-5})(2+\sqrt{-5})$,

$3 \in \mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ is irreducible and prime

Namely, $\mathcal{O}_K^\times = \{x \in \mathcal{O}_K \mid N(x) \in \{\pm 1\}\}$

$\{\pm 1\}$ $\quad$ $a^2+b^2 \cdot 5$ if $x = a + b\cdot\sqrt{-5}$

Calculate

$N_{K/\mathbb{Q}}(3) = 9 = N_{K/\mathbb{Q}}(2-\sqrt{-5})$

$= N_{K/\mathbb{Q}}(2+\sqrt{-5})$

but $3 \neq \pm(2 \pm \sqrt{-5})$.

Note: $N_{K/\mathbb{Q}}(x) \neq \pm 3$ for all $x \in \mathcal{O}_K$

⚠ Thm: A Dedekind domain, $I \subseteq A$ ideal. Then:

1) $\exists$ prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r \subseteq A$ s.t. and $a_1, \dots, a_r \in \mathbb{Z}_{\geq 0}$, s.t. $I = \mathfrak{p}_1^{a_1} \cdot \dots \cdot \mathfrak{p}_r^{a_r}$

(Recall: R any ring, $I, J \subseteq R$ ideals $\Rightarrow I \cdot J := \langle x \cdot y \mid x \in I, y \in J \rangle_A$

2) If $\mathfrak{p}_1, \dots, \mathfrak{p}_r, \mathfrak{q}_1, \dots, \mathfrak{q}_s \subseteq A$ prime, and $a_1, \dots, a_r, b_1, \dots, b_s \in \mathbb{Z}_{\geq 0}$ s.t. $\mathfrak{p}_1^{a_1} \cdot \dots \cdot \mathfrak{p}_r^{a_r} = \mathfrak{q}_1^{b_1} \cdot \dots \cdot \mathfrak{q}_s^{b_s} \neq 0$

$\Rightarrow r = s$, up to permutation, $\mathfrak{p}_i = \mathfrak{q}_j$ and $a_i = b_j$

Restores unique factorization
by passage to ideals

In above ex. ($K = \mathbb{Q}(\sqrt{-5})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$)

$(3) = \mathfrak{p}_1 \cdot \mathfrak{p}_2$ with $\mathfrak{p}_1 = (3, \sqrt{-5}-1)$

$\mathfrak{p}_2 = \bar{\mathfrak{p}}_1 = (3, 1+\sqrt{-5})$

(Use that $\mathcal{O}_K/(3) \cong \mathbb{F}_3[T]/T^2+5$

with $T^2+5 \equiv (T-1)(T+1) \bmod (3)$)

Indeed,

$\mathfrak{p}_1 \cdot \mathfrak{p}_2 = (9, 3(\sqrt{-5}-1), 3(1+\sqrt{-5}),$

$+1+5=6)$

$= (3, 3(\sqrt{-5}-1), 3(1+\sqrt{-5}), 6)$

$= (3)$

So,

$$(3)^2 = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_1 \cdot \mathfrak{p}_2 = \mathfrak{p}_1^2 \cdot \mathfrak{p}_2^2$$

with

$$\mathfrak{p}_1^2 = (9, 3(\sqrt{-5}-1), -5-2\sqrt{-5}+1)$$

$$= (9, 3(\sqrt{-5}-1), \sqrt{-5}-7$$

$$= (9, 3\sqrt{-5}-3, \sqrt{-5}+2)$$

$$= (9, -9, \sqrt{-5}+2)$$

$$= (2, +\sqrt{-5})$$

$(\sqrt{-5}+2)$ has norm 9

Thus, the factorization

$$3^2 = (2+\sqrt{-5})(2-\sqrt{-5})$$

appears by regrouping

the fact

$$(3)^2 = \underbrace{\mathfrak{p}_1 \cdot \mathfrak{p}_2}_{(3)} \cdot \underbrace{\mathfrak{p}_1 \cdot \mathfrak{p}_2}_{(3)} = \underbrace{\mathfrak{p}_1^2}_{(2+\sqrt{-5})} \cdot \underbrace{\mathfrak{p}_2^2}_{(2-\sqrt{-5})}$$

$\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$

Note: $K/\mathbb{Q}$ number field, $p \in \mathbb{Z}$

$(p) \cdot \mathcal{O}_K = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$ with

$\mathfrak{p}_1, \ldots, \mathfrak{p}_r \subseteq \mathcal{O}_K$ prime

If $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are principal, i.e.

$\mathfrak{p}_i = (\pi_i)$, then

$p = \varepsilon \cdot \pi_1 \cdot \ldots \cdot \pi_r$ with $\varepsilon \in \mathcal{O}_K^\times$

In fact (Corollary 2.2.7.)

$\mathcal{O}_K$ is a UFD $\Leftrightarrow$ $\mathcal{O}_K$ is a PID

In example

$(3, \sqrt{-5}-1) \subseteq \mathcal{O}_K$ not principal

Indeed, assume $(3, \sqrt{-5}-1) = (x)$

for some x

$\Rightarrow N_{K/\mathbb{Q}}(x) \mid N_{K/\mathbb{Q}}(\sqrt{-5}-1) = 6$

$\&\ N_{K/\mathbb{Q}}(x) \mid N_{K/\mathbb{Q}}(3) = 9$

$\Rightarrow N_{K/\mathbb{Q}}(x) = \pm 3$ ↯

$N_{K/\mathbb{Q}}$

$\|$

$a^2 + 5b^2$ if $x = a + b\sqrt{-5}$,

$a, b \in \mathbb{Z}$.

Definition: A domain, $K = \mathrm{Frac}(A)$

A fractional ideal of A is a sub-A-module $I \subseteq K$, s.t. $d \cdot I \subseteq A$ for some non-zero $d \in A$

missing in Tian

Heuristic: "ideals" $\hookrightarrow$ "integers"

"fract. ideals" $\hookrightarrow$ "rationals"

Ind part, we have

1) $I \subseteq A$ ideal $\Rightarrow I$ fractional ideal

2) addition: I, J fract.

$\Rightarrow I + J := \{a + b \in K \mid a \in I, b \in J\}$ fractional

3) multiplication:

$I \cdot J := \langle a \cdot b \mid a \in I, b \in J \rangle_A$ fract.

4) unit: $A \cdot I = A$

5) If $I \neq 0$, an "inverse"

$$I^{-1} = \{x \in K \mid x \cdot I \subseteq A\}$$

⚠: 1) (2) + (3) $\subseteq \mathbb{Z}$

$\parallel$

(1) = (2) + (9)

2) In general: $I^{-1} \cdot I \neq A$

(Exercise: Find examples if $A = \mathbb{Z}[T]$ or $A = \mathbb{Z}[-\sqrt{5}]$)

But If A Dedekind, then

$I^{-1} \cdot I = A$ (see line before Cor. 2.28)

The case $I = \mathfrak{p} \subseteq A$ is Le 2.26.

↑

main pt of proof

The proof of La 2.2.6. uses all prop. of Dedekind ring.

La: R any ring, $\mathfrak{p} \subseteq R$ prime,
$\mathfrak{a}_1, \dots, \mathfrak{a}_r \subseteq A$ ideals, s.t.

$\mathfrak{p} \supseteq \mathfrak{a}_1 \cdot \dots \cdot \mathfrak{a}_r$

$\Rightarrow \exists\, i$, s.t. $\mathfrak{p} \supseteq \mathfrak{a}_i$

Proof: If wrong $\Rightarrow \exists\, t_i \in \mathfrak{a}_i \setminus \mathfrak{p}$

$\Rightarrow t_1 \cdot \dots \cdot t_r \in \mathfrak{p} \Rightarrow \lightning$ ∎

In Corollary 2.2.10. one can add

5) $v_{\mathfrak{p}}(x \cdot y) = v_{\mathfrak{p}}(x) + v_{\mathfrak{p}}(y)$ for $x, y \in K$

If $K = \mathbb{Q}$, the $v_{\mathfrak{p}}$ are exactly the p-adic valuations of $\mathbb{Q}$

Final def: A Dedekind ring, $K = \mathrm{Frac} K$

1) $\mathcal{I} := \{ I \subseteq K$ non-zero fractional ideals$\}$, group under multiplikation

2) $I \in \mathcal{I}$ principal if $x \cdot A = I$ for some $x \in K$

$\mathcal{P} := \{ I \in \mathcal{I}$ principal$\} \subseteq \mathcal{I}$

3) $Cl_K := Cl_A := \mathcal{I}/\mathcal{P}$

⚠ the class group of A (or K)

Note: * $\mathcal{I}$ is free abelian on $\{ \mathfrak{p} \subseteq A$ max.$\}$

* Cl_A "measures" the failure of unique fact. of elt. in A.

e.g. $Cl_A = \{1\} \Leftrightarrow A$ PID

Fun fact (Claborn):
Any abelian group is the
class group of some Dedekind ring.

For number fields (later):
Thm: $K/\mathbb{Q}$ finite $\Rightarrow$ Cl_K finite

⚠ $h_K := \#Cl_K$ is the
class number of K

Open conj: # Is any finite abelian
group the class grp of a
number field?

Ex (later): $Cl_{\mathbb{Z}[\sqrt{-5}]} \simeq \mathbb{Z}/2$

gen. by $(3, \sqrt{-5}-1)$ $(\mathfrak{p}_1^2 = (2+\sqrt{-5}))$
$\mathfrak{p}_3$

$D \in \mathbb{Z}$ squarefree, $K = \mathbb{Q}(\sqrt{D})$

If $D < 0 \Rightarrow$ $Cl_K = \{1\}$ iff

$$\Delta_K = \{-3, -4, -7, -8, -11, -19, -43, -67, -163\}$$

Open conj:

$Cl_K = \{1\}$ for inf. many $D > 0$