Dedekind domains, contd. (Isaacs Ch. 29)

Def A Ded. domain is a comm. int. closed Noeth domain of dimension ≤ 1. (inconsistent compared to last lecture)

Let R Domain $F = \mathrm{frac}(R)$

Def A fractional ideal is an R-submodule $I \subseteq F$ s.t. $aI \subseteq R$ some $a \in F \setminus \{0\}$ ($\Leftrightarrow \exists\, a \in R \setminus \{0\}$ s.t. $aI \subseteq R$)

Note: Fractional ideals form a monoid via multiplication

$$IJ = \left\{ \sum_{i=1}^{n} x_i y_i \;\middle|\; x_i \in I, y_i \in J \right\}$$

R = identity element

Def $I^{-1} = \{ a \in F \mid aI \subseteq R \}$

We say I is invertible if $\exists J$ s.t. $IJ = R$

(note: in this case $II^{-1} = R$)

Last time: we showed

Lem: If R is a Ded. domain then any fractional ideal is invertible (form a group).

aside: R PID ($R = \mathbb{Z}$)

$a \in R \quad a = p_1^{n_1} \cdots p_r^{n_r}$ factorization.

from $aR = (p_1^{n_1}R)(p_2^{n_2}R)\cdots(p_r^{n_r}R)$

$= p_1^{n_1}R \cap p_2^{n_2}R \cap \cdots \cap p_r^{n_r}R$

$= (p_1R)^{n_1}\cdots(p_rR)^{n_r}$

ideals in PID $\longleftrightarrow$ generalized elements of R

frac ideals "in" PID $\longleftrightarrow$ generalized elements of F.

R PID, $I \subseteq F$ frac ideal $\Rightarrow I = aR, a \in F$

$bI \subseteq R$ some $b \in F$

$\shortparallel$

cR some $c \in R$.

$I = \frac{c}{b}R \quad a = \frac{c}{b}$.

$a \in F$ for R PID

$\underline{aR} = (p_1R)^{n_1}\cdots(p_rR)^{n_r} \quad n_i \in \mathbb{Z}$

General ded domain, I frac ideal, will have:

unique $\quad I = P_1^{n_1}\cdots P_r^{n_r} \quad I, P_i$ not nesc. principal.

$I = \mathfrak{a}R$

Prop let R be a comm. domain. Then.

R a Ded. domain $\Leftrightarrow$ every fractional ideal is invertible.

$\Leftarrow$

Sublemma: If I is an invertible frac. ideal in a comm domain R then I is finitely generated.

Pf: write $II^{-1} = R \Rightarrow 1 = \sum a_i b_i \quad a_i \in I, b_i \in I^{-1}$

claim: a_i's generate I.

if $a \in I$ then $a = a \cdot 1 = a \sum a_i b_i$

$= \sum a_i (b_i a)$

$= \langle a_1, \dots, a_n \rangle_R$ $\square$.

$b_i a \in I^{-1} I = R$

(back to proof)

if $I \triangleleft R$ ideal $\Rightarrow$ frac ideal is invertible.

$\Rightarrow I$ f.g. $\Rightarrow R$ Noeth.

Sublemma: let I be an R-submodule of F = frac R R comm. domain. If I is f.g. then I is a frac ideal.

Pf: $I = \langle a_1, \dots, a_n \rangle_R \quad a_i = \frac{b_i}{c_i}$ then $\prod c_i = c$

get $cI \subseteq R$ $\square$.

(back to proof)

Show R int. closed.

Let $\alpha \in F$ integral over R.

$R[\alpha]$ is f.g. R-module. $\Rightarrow$ it's a fractional ideal

$R[\alpha]R[\alpha] = R[\alpha]$ (subring)

$\cdot R[\alpha]^{-1}$

$\Rightarrow R[\alpha] = R. \quad \Rightarrow \alpha \in R.$

Dimension ≤ 1.

Let $P \subseteq Q$ nonzero prime ideals. WTS $P = Q$.

$\Rightarrow PQ^{-1} \subseteq QQ^{-1} = R \quad \Rightarrow PQ^{-1} \triangleleft R.$

and $(PQ^{-1})Q \subseteq P$ $\quad$ P prime either

$PQ^{-1} \subseteq P$ or $Q \subseteq P$.

if $PQ^{-1} \subseteq P$ then $\xrightarrow{\cdot P^{-1}}$ $\Rightarrow Q^{-1} \subseteq R$

$\Rightarrow R = QQ^{-1} \subseteq Q$

impossible as Q proper ideal.

$\Rightarrow Q \subseteq P \Rightarrow Q = P$ $\square$.

Prop: If R a Ded. domain and $0 \neq I \triangleleft R$ then
I can be written uniquely as $I = P_1^{n_1} \cdots P_r^{n_r}$ prime ideals P_i

Pf: Claim 1: can write as product

Claim 2: uniqueness.

Claim 1: Assume $\exists$ ideals can't be written as product as above.
let I maximal s.t. can't be written as product.
$\exists$ P maximal $I \subsetneq P$.

$$IP^{-1} \subseteq PP^{-1} = R \quad \text{so } IP^{-1} \triangleleft R$$

and $P^{-1} \supsetneq R$

because if $P^{-1} \subseteq R$ then
$R = PP^{-1} \subseteq P$ ✗.

$\Rightarrow IP^{-1} \supsetneq I$ (uses I invertible)

$\Rightarrow IP^{-1} = P_1 P_2 \cdots P_\ell$ (allowing reps.)

$\Rightarrow I = P P_1 P_2 \cdots P_\ell$ contradicts assumption.

so claim 1 ✓.

Claim 2: If $P_1 \cdots P_\ell = Q_1 \cdots Q_r$ then
$P_1 \cdots P_\ell \subseteq Q_1$ Q_1 prime $\Rightarrow P_i \subseteq Q_1$ some i.

$\dim \le 1 \Rightarrow P_i = Q_i$

$\Rightarrow$ mult. by $P_i^{-1} = Q_i^{-1}$ get smaller chains, repeat induct etc... $\triangleright$.

Cor: Group of fractional ideals

$\simeq \bigoplus_{P \text{ prime} \neq 0 \text{ in } R} \mathbb{Z}$

$I = P_1^{n_1} \cdots P_r^{n_r}$

n_i in ith slot, 0 else.

Def $Cl(R) = \dfrac{\text{gp of fractional ideals}}{\text{subgp of principal fractional ideals}}$ aR, $a \in F \setminus \{0\}$

ex: $Cl(\mathbb{Z}) = 1$

$Cl(\mathcal{O}_K) < \infty$

K | finite ext. $\mathbb{Q}$ $\quad \mathcal{O}_K$ = int. closure of $\mathbb{Z}$ in K

$Cl(\mathbb{C}[x]) = 1$ $\qquad Cl\left(\dfrac{\mathbb{C}[x,y]}{y^2 - x^3 - 1}\right)$ is infinite.

$\simeq S^1 \times S^1$

Cl(coord. ring of curve of genus g)

$(S^1)^{2g} / \mathbb{Z}^m$

Distance & Approximation

Suppose R a comm. ring. I ideal.

Define $v_I : R \longrightarrow \mathbb{N} \cup \{\infty\}$

$a \longmapsto \sup\{ i \mid a \in I^i \}$

Define metric (assume R Noeth domain)

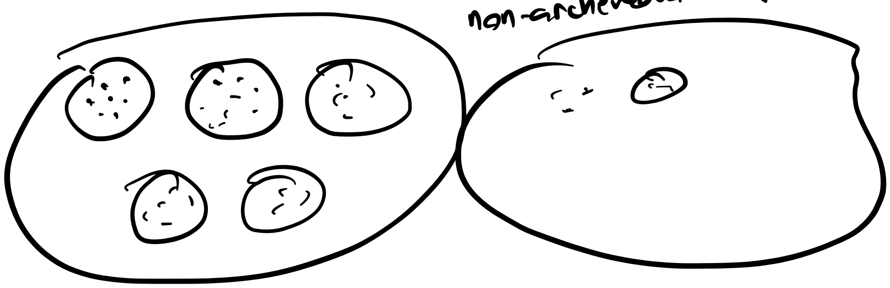
$$d_I(a,b) = e^{-v_I(a-b)}$$ e is a real numr > 1.

exercise: d_I is a metric.

Def R a ring, a norm on R is a function $|\cdot| : R \to \mathbb{R}$

s.t.
- $|a| \geq 0$ all a and $|a| = 0$ if and only if $a = 0$
- $|a+b| \leq |a| + |b|$ (non-archimedean norm if $|a+b| \leq \max\{|a|, |b|\}$)
- $|ab| \leq |a||b|$ (multiplicative if $|ab| = |a||b|$)

non-archemedean distances.



<u>**Def**</u> A valuation on a ring R (comm. ~~domain~~)

is a function $R \longrightarrow \mathbb{R} \cup \{\infty\}$

- $v(a) = \infty$ if and only if $a = 0$
- $v(a+b) \geq \min\{v(a), v(b)\}$
- $v(ab) = v(a)v(b)$

Classic notion: divisibility by a prime p in $\mathbb{Z} = R$

$$v_p(n) = \max\{m \mid p^m \mid n\}$$

<u>Observation:</u> given a valuation

$|a| = e^{-v(a)}$ is a multiplicative, non-Archimedean norm.

<u>Next time:</u> R Ded domain. each P prime $\rightsquigarrow$ valuation v_p norm $|\ |_p$

$R \longrightarrow R \times \dots \times R$

P_1-norm ... P_r-norm P_i distinct.

$r \longmapsto (r, \dots, r)$ is dense in product.