§ Ideal classes

- Notation : R an order inside an étale $\mathbb{Q}$-algebra K.

  - $\mathcal{I}(R) = \{ \text{fractional } R\text{-ideals} \}$

- We want to turn $\mathcal{I}(R)$ into a category, so we need to define what are the morphisms.

- Fractional R-ideals are R-modules. So we take R-linear maps.

- Given $I, J \in \mathcal{I}(R)$, can we compute

$$\mathrm{Hom}_R(I, J) \;?$$

Prop Let $\varphi \in \mathrm{Hom}_R(I, J)$.
Then φ is a multiplication by some $\alpha \in K$.
That is,

$$\mathrm{Hom}_R(I, J) \overset{\text{canonical}}{\simeq} (J : I) = \{ \alpha \in K : \alpha I \subseteq J \}$$

Pf $\varphi : I \to J$ induces a unique map $\tilde{\varphi} : \underset{\substack{\| \\ K}}{I \otimes \mathbb{Q}} \to \underset{\substack{\| \\ K}}{J \otimes \mathbb{Q}}$

Since $\tilde{\varphi}$ is R-linear and K is the total quotient ring of R we have that $\tilde{\varphi}$ is uniquely determined by $\tilde{\varphi}(1_K) = \alpha$.

Hence we have, $\forall\, i \in I \quad \varphi(i) = \tilde{\varphi}(i \cdot 1_K) = i \cdot \alpha$.

Cor

- $\forall\, p$ prime of R: $\mathrm{Hom}_{R_p}(I_p, J_p) = (J_p : I_p)$

- $I \simeq J \iff \exists\, \alpha \in K^\times$ s.t. $\alpha I = J$

Def The <u>ideal class monoid</u> of R is

$$\mathrm{ICM}(R) = \mathcal{J}(R) / \simeq$$

The <u>Picard group</u> of R is

$$\mathrm{Pic}(R) = \frac{\{ I \in \mathcal{J}(R) : I \text{ is invertible in } R \}}{\simeq}$$

- The operation is ideal multiplication.

Rmk

- $\mathrm{Pic}(R) \subseteq \mathrm{ICM}(R)$
- $\mathrm{Pic}(R) = \mathrm{ICM}(M) \iff R = \mathcal{O}_K$.

Lemma The multiplicator ring is an invariant of the ideal class.

Pf Pick $I, J \in \mathcal{I}(R)$ st $I \simeq J$,

say $I = \alpha J$.

Then $(I : I) = (\alpha J : \alpha J) = (J : J)$.

Cor

$$ICM(R) \supseteq \bigsqcup_{\substack{S \text{ is an} \\ \text{overorder} \\ \text{of } R}} Pic(S)$$

Pf Use the previous lemma together with the lemma from yesterday

"I invertible in $S \Rightarrow (I : I) = S$"

Prove that TFAE:

Exercise: ① R is Bass (i.e every over-order is Gorenstein)

② $ICM(R) = \bigsqcup Pic(S)$

③ $ICM(R)$ is a Clifford monoid (i.e a $\bigsqcup$ of abelian groups)

Example: Every quadratic order is Bass

Example

- $R = \mathbb{Z}[\alpha] \subsetneq \mathbb{Q}(\alpha) = \dfrac{\mathbb{Q}[x]}{\underset{\overset{\shortparallel}{f}}{(x^3+10x^2-8)}}$ $\qquad \alpha = x \bmod (f)$.

- $I = (3, \alpha+2)$

  $J = 3\mathbb{Z} \oplus (\alpha+2)\mathbb{Z} \oplus \dfrac{\alpha^2+2\alpha}{8}\mathbb{Z}$

We have $(\alpha+\alpha^2)J = I$. So $I \simeq J$.

- $S = \mathbb{Z} \oplus \alpha\mathbb{Z} \oplus \dfrac{\alpha^2}{2}\mathbb{Z} \supset R$

Exercise: Prove that S is not Gorenstein and hence R is not Bass

§ Computing Pic (R)

- **Recall**: $\mathcal{O}_K = \mathcal{O}_{K_1} \times \dots \times \mathcal{O}_{K_R}$

  Dedeking domains

Then $$\mathrm{Pic}(\mathcal{O}_K) = \underset{\underset{Cl_{K_1}}{\parallel}}{\mathrm{Pic}(\mathcal{O}_{K_1})} \times \dots \times \underset{\underset{Cl_{K_R}}{\parallel}}{\mathrm{Pic}(\mathcal{O}_{K_R})}$$

class groups of number fields.

- There are well known algorithms to compute class groups of num. fields.

- Let $R \subsetneq \mathcal{O}_K$. We have an exact sequence:

(*) $$0 \longrightarrow R^\times \xrightarrow{\iota} \mathcal{O}_K^\times \xrightarrow{\alpha} \frac{(\mathcal{O}_K/\mathfrak{f})^\times}{(R/\mathfrak{f})^\times} \xrightarrow{\beta} \mathrm{Pic}(R) \xrightarrow{\pi} \mathrm{Pic}(\mathcal{O}_K) \longrightarrow 0$$

- $R^\times = \{ x \in R \mid \exists\, y \in R \text{ with } xy = 1 \}$
- $\mathcal{O}^\times =$ analogous
- $\mathfrak{f} = (R : \mathcal{O}_K) = \{ x \in K \mid x\mathcal{O}_K \subseteq R \}$

  $=$ the biggest fr. $\mathcal{O}_K$-ideal contained in R.

+ ι = inclusion
+ α = projection
+ β = induced by $\tilde{\beta} : (\mathcal{O}/\mathfrak{f})^\times \longrightarrow \mathrm{Pic}(R)$

  $u + \mathfrak{f} \longmapsto [u\mathcal{O}_K \cap R]_{\simeq}$
+ π = induced by $(I \mapsto I\mathcal{O}_K)$

Exercise : ⊛ Prove that ⊛ is exact.
See Keith Conrad notes on the conductor.

Important : - Kliiners - Pauli gave an efficient method to compute $\left(\mathcal{O}_K/_f\right)^\times \Big/ \left(R/_f\right)^\times$, $\underset{p}{\bigoplus} \dfrac{\mathcal{O}_{K,p}^\times}{R_p^\times}$

- there are methods to compute $\operatorname{Pic} \mathcal{O}_K$ and $\mathcal{O}_K^\times$

$\Longrightarrow$ We can compute efficiently also $R^\times$ and $\operatorname{Pic}(R)$.

---

§ Compute ICM(R) for R Bass

1) Compute $\mathcal{O}_K$
2) Compute all over-orders S : $R \subseteq S \subseteq \mathcal{O}_K$ by looking at the finite quotient $\mathcal{O}_K/_R$
3) For every such S compute S^t and test if S^t is invertible i.e $S = S^t(S:S^t)$
4) If this is the case (i.e. R is Bass).
output $ICM(R) = \bigsqcup \operatorname{Pic}(S)$.

- If R is not Bass, then we need a different method.

§ Weak equivalence

Prop Let I, J be fractional R-ideals.
TFAE:
1. $I_p \simeq J_p$ as R_p-modules, for every prime p of R
2. $1 \in (I:J)(J:I)$
3. $\underbrace{(I:I) = (J:J)}_{=S}$ "same mult. ring"
   and there exists a fract. S-id. invertible L in S such that
   $$I = L\,J.$$

Def If ①, ②, ③ hold, then I and J are called weakly equivalent.

Pf "① ⇒ ②"
There exists, for each p, a non-zero div. x of the total quotient ring of R_p s.t.
$$I_p = x\,J_p.$$
Hence
$$((I:J)(J:I))_p = (I_p:J_p)(J_p:I_p) =$$
$$= (xJ_p:J_p)(J_p:xJ_p) = x(J_p:J_p)\tfrac{1}{x}(J_p:J_p) = (J_p:J_p).$$
So the natural inclusion
$$(I:J)(J:I) \subseteq (J:J)$$
is locally surjective at every p ⇒ it is an equality
$$(I:J)(J:I) = (J:J) \ni 1$$

"② ⇒ ③"

$$(I:J)(J:I) \begin{array}{l} \subseteq (J:J) \\ \subseteq (I:I) \end{array}$$

$1 \in$ ⇒ all equalities ⇒ $(I:I) = (J:J)$.

Put $S = (I:I)$.

We have $(I:J)(J:I) = S$

i.e both $(I:J)$ and $(J:I)$ are inv. in S

Now: $$I = I \cdot S = I(I:J)(J:I) \subseteq J \cdot (I:J) \subseteq I$$

⇒ all equalities

$$\Rightarrow I = \underset{\overset{\Vert}{L}}{(I:J)}\, J$$

"③ ⇒ ①"

$\forall\, p$ in R, S_p is semilocal, so $L_p = x S_p$.

Hence $$I_p = L_p J_p = x \underbrace{S_p J_p}_{= J_p} = x J_p$$

i.e $I_p \simeq J_p$

∎

Def • $\mathcal{W}(R) = \mathcal{J}(R) / \underset{wk}{\sim}$ — weak eq.

weak eq. class monoid

• for any order S in K

$$\overline{\mathcal{W}}(S) = \frac{\{ I \in \mathcal{J}(S) \mid (I:I) = S\}}{\underset{wk}{\sim}}$$

(Well def b/c of ③)

and
$$\overline{ICM}(S) = \frac{\{ I \in \mathcal{J}(S) \mid (I:I) = S\}}{\simeq}$$

Rmk With this notation:
S is Gorenstein $\Leftrightarrow$ $\overline{\mathcal{W}}(S) = \{[S]_{wk}\}$ $\Leftrightarrow$ $\overline{ICM}(S) = \mathrm{Pic}(S)$

Rmk:
① : wk. eq. has a local nature
② : wk. eq. is easy to test
③ : "we mod out by inv. S-ideals"

Cor: Assume that $I \underset{wk}{\simeq} J$.
1) Then $I = (I:J)J$ and $(I:J)$ is invertible in $S := (I:I)$.
2) Also, $I \simeq J \Leftrightarrow (I:J)$ is principal in S

Pf 1) already done before.
2) "$\Rightarrow$" Say $I = xJ = xS \cdot J$
Then $(I:J) = (xJ:J) = x(J:J) = xS$
"$\Leftarrow$" Use 1).

$\blacksquare$

§ Compute $\mathcal{W}(R)$.

- Observe
$$\mathcal{W}(R) = \bigsqcup_{\substack{S \text{ overorder} \\ \text{of } R}} \overline{\mathcal{W}}(S)$$

- It is enough to compute each $\overline{\mathcal{W}}(S)$.

- **Prop** - Let I be a fract. R-ideal with $(I:I) = S$.
  - Let T be an over-order of S s.t. $S^t T$ is invertible in T.
  - Let f be a fract. ideal s.t. $f \subseteq S$ and $T \subseteq (f:f)$.

Then there exists J s.t.
 ⊕ $J \underset{wk}{\simeq} I$
 ⊕ $f \subseteq J \subseteq T$.

- Rmks: - one can take $f = (S:T)$
  - one can take $T = \mathcal{O}_K$.
  - Prop says that every weak eq. class has a representative between f and T i.e in the finite quotient T/f.

- We deduce that $\overline{\mathcal{W}}(S)$ is finite $\Rightarrow$ $\mathcal{W}(R)$ is finite

- One wants to keep T/f as small as possible to gain in efficiency.

Pf

$$[I]_{\simeq} \longmapsto [I\cdot T]_{\simeq}$$

- $\mathrm{Pic}(S) \xrightarrow{\pi} \mathrm{Pic}(T)$ is onto.

$$\text{b/c.}\quad \begin{tikzcd} \mathrm{Pic}(S) \arrow[rr, "\pi"] \arrow[dr] & & \mathrm{Pic}(T) \arrow[dl] \\ & \mathrm{Pic}(\mathcal{O}_K) & \end{tikzcd}$$

- $(I:I) = S \Leftrightarrow I\cdot I^t = S^t$

So $I\cdot T$ is invertible in T.

- Put $J' =$ representative in $\mathcal{J}(S)$ of $\pi^{-1}((T : IT))$

- Set $J = I\cdot J'$.

Note $J \underset{wk}{\simeq} I$ b/c J' is invertible in S.

and $JT = T$.

- Hence $J \subseteq (T:T) = T$.

- Also $\mathfrak{f} J = \mathfrak{f} T\cdot J = \mathfrak{f} T = \mathfrak{f}$

Since $\mathfrak{f} \subseteq S = (I:I) = (J:J)$

we get $\underset{\mathfrak{f}}{\underset{\|}{\mathfrak{f}J}} \subseteq J$

∎

§ Compute $ICM(R)$

We can compute $\overline{W}(S)$ for every over-order S of R.

Thm The action of $Pic(S)$ on $\overline{ICM}(S)$ is free and

$$\circledast \qquad \overline{W}(S) = \overline{ICM}(S) / Pic(S).$$

Hence if $\{I_1, \dots, I_s\}$ is a set of rep's of $\overline{W}(S)$

and if $\{J_1, \dots, J_k\}$ ——— // ——— $Pic(S)$

then $\{I_i J_j\}$ is a set of reps of $\overline{ICM}(S)$.

Pf

$\circledast$ follows from the fact that weak eq. means modding out by invertible ideals.

We need to prove the freeness part.

i.e. if there exists

I with $(I:I) = S$

s.t. $IJ_1 \underset{wk}{\simeq} I \cdot J_2$ for J_1, J_2 invertible in S

then $J_1 \simeq J_2$.

By mult. on both sides for $(S : J_1)$ we are reduced to prove that

$$I = IJ \qquad (J \text{ inv.})$$

then $S \simeq J$.

We do it locally at every p. of S.

$I \underset{wk}{\simeq} IJ \Rightarrow \exists\ x \in \mathrm{Tot}(S_p)^\times$ st

$$I_p = I_p x J_p$$

Also, (xJ_p) is invertible in S_p

$$\Rightarrow xJ_p = yS_p \text{ for some } y \in \mathrm{Tot}(S_p)^\times$$

Then $\quad I_p = yI_p \Rightarrow y \in S_p$

and $\quad \frac{1}{y} I_p = I_p \Rightarrow 1/y \in S_p$

So $\quad y \in S_p^\times$ and hence $xJ_p = S_p$.

i.e $\quad J_p \simeq S_p$

Conclusion

Using Thm we have an algorithm to compute $\overline{ICM}(S)$ $\forall$ overord S of R

Hence we can compute

$$ICM(R) = \bigsqcup_{\substack{S \text{ overord} \\ \text{of } R}} \overline{ICM}(S)$$