Title

# Ideal classes and abelian varieties over finite fields

Intro

- Goal of this mini-course is to describe an effective method to compute ab. var. over a finite field in terms of fractional ideals of orders in étale $\mathbb{Q}$-algebras.

We will need some restrictions on the ab. var.
On the other hand, we will have to consider non-maximal orders and non-invertible ideals.

- Program
  L1 : } fr. ideals. (w/ a lot of proofs)
  L2 : }
  L3 : } ab. var and categorical eq.
  L4 : } (not so many proofs)

  ⊛ Research talk on Friday 16 Nov.: • similar results in a more general setting
  \+ polarizations & period matrices
  (+ base field ext)

- Material on my webpage : - lecture notes (handwritten)
  - references
  - Magma code.

- email : stefano.marseglia89@gmail.com

Rennes, Nov 2019. Stefano Marseglia

## § Étale algebras over $\mathbb{Q}$

**Def** An étale algebra over $\mathbb{Q}$ is a finite product of finite field extension of $\mathbb{Q}$.
A number field is an étale algebra over $\mathbb{Q}$ which is a field.

**Eg** • Let $f \in \mathbb{Z}[x]$, monic.
Write $f = f_1^{e_1} \cdots f_r^{e_r}$ with $f_i$ irreducible and distinct.
Put
$$K = \frac{\mathbb{Q}[x]}{(f)}.$$
Then: $K$ is an étale alg. over $\mathbb{Q}$ $\Leftrightarrow$ $e_1 = e_2 = \dots = e_r = 1$
i.e. $f$ is square-free

$K$ is a number field $\Leftrightarrow$ $f$ is irreducible
$(r = 1,\ e_1 = 1)$

• Given a number field $k$, $K = k \times k$ is an étale algebra.

**Rmk**: étale algebras are $\begin{cases} - \text{ commutative} \\ - \text{ reduced } (= \text{no non-zero nilpotents}) \end{cases}$

**Notation**: given an étale alg. $K$
$$K^\times = \{x \in K \text{ s.t. } \exists y \in K \text{ with } xy = 1\}$$
$$= \{\text{non-zero-divisors of } K\}$$

## § Orders

Let $K$ be an étale algebra.

**Def** An *order* $R$ in $K$ is a subring $R \subseteq K$ which is also a lattice in $K$.
(i.e. free-fin. gen. $\mathbb{Z}$-module of maximal rank).

**Rmk**
- $R \otimes_{\mathbb{Z}} \mathbb{Q} = K$
  In part., $\mathrm{rk}_{\mathbb{Z}}(R) = \dim_{\mathbb{Q}}(K)$.
- $K$ is the total quotient ring of $R$:
  (put $S = R \cap K^\times$, then $K = S^{-1}R$)

**Eg** $f \in \mathbb{Z}[x]$ monic, squarefree

$$K := \frac{\mathbb{Q}[x]}{(f)}$$

$$R := \frac{\mathbb{Z}[x]}{(f)}$$ is an order in $K$
(*monogenic* or *equation* order)

**Notat.**: $K = \mathbb{Q}[\alpha]$ $\quad \alpha = x \bmod f$

$R = \mathbb{Z}[\alpha]$

Question / Exercise : $f \in \mathbb{Z}[x]$ monic sqfree
$f = f_1 \cdot f_2 \cdots f_r$, $f_i$ irred.

Then $$\frac{\mathbb{Q}[x]}{(f)} \xrightarrow{\sim} \frac{\mathbb{Q}[x]}{(f_1)} \times \frac{\mathbb{Q}[x]}{(f_2)} \times \dots \times \frac{\mathbb{Q}[x]}{(f_r)}$$

Is always true that ?
$$\frac{\mathbb{Z}[x]}{(f)} \xrightarrow{\sim} \frac{\mathbb{Z}[x]}{(f_1)} \times \dots \times \frac{\mathbb{Z}[x]}{(f_r)} \quad ?$$

**Prop** Let $K$ be an étale algebra.

1. the set of orders in $K$ admits a unique maximal element (w.r.t $\subseteq$), which we denote $\mathcal{O}_K$.
2. Write $K = K_1 \times K_2 \times \dots \times K_r$, with $K_i$ number fields.
   Then $$\mathcal{O}_K = \mathcal{O}_{K_1} \times \dots \times \mathcal{O}_{K_r}$$
   where $\mathcal{O}_{K_i}$ is the ring of integers of $K_i$.

**Pf** (Exercise)

**Def** $\mathcal{O}_K$ is the <u>maximal order</u> of $K$

## § Fractional ideals



$K$ ét. alg $/\mathbb{Q}$;

$R$ an order in $K$.

**Def** A fractional $R$-ideal is a sub-$R$-module $I$ of $K$ which is a lattice in $K$.

i.e.: • $I \cdot R = I$

• $I \otimes_{\mathbb{Z}} \mathbb{Q} = K$

Rmk: $I$ a fr. $R$-id, $I \subseteq R \Rightarrow R/I$ is finite!

**Lemma** An ideal $I$ of $R$ is a fractional $R$-ideal if and only if $I \cap K^\times \neq \phi$

Pf Let $d \in K^\times \cap I$. Then $dR \subseteq I \subseteq R \Rightarrow I$ is a free fing gen. $\mathbb{Z}$-module of the same rank of $R$. Hence, $I$ is a lattice in $K$.

Converse: Exercise

---

Rmk - Given a fractional $R$-ideal $I$ there exists $d \in I$ s.t $dI \subseteq R$.

- Observe that $dI \underset{R}{\simeq} I$.

**Example:**

$$f = x^3 + 10x^2 - 8$$

$$K = \frac{\mathbb{Q}[x]}{f} = \mathbb{Q}(\alpha)$$

$$R = \mathbb{Z}[\alpha] = \frac{\mathbb{Z}[x]}{f} \quad \text{order in } K$$

$S = \mathbb{Z} \oplus \alpha\mathbb{Z} \oplus \frac{\alpha^2}{2}\mathbb{Z}$ is an order in $K$ and a fractional $R$-ideal.

Observe $2 \cdot S \subseteq R$.

Lemma Let $I, J$ be fractional R-ideals. Then:

- $I+J$, $I\cap J$, $I\cdot J$ are fractional ideals
- $(I:J) = \{x \in K : xJ \subseteq I\}$ is a fr. id
- $I^t = \{x \in K : Tr(xI) \subseteq \mathbb{Z}\}$ is a fr. id.

Notation : $\mathcal{J}(R) = \{$ fractional - R - ideal $\}$

- $\mathcal{J}(R)$ is a commutative monoid w.r.t ideal mult.

$$I, J \mapsto I\cdot J$$

with unit $R$, since $IR = RI = I$, for every $I \in \mathcal{J}(R)$

Def. An over-order of $R$ is an order $S$ in $K$ st $R \subseteq S$.

Eg $O_K$ is an over-order of $R$.

- For every $I \in \mathcal{J}(R)$, $(I:I)$ is an over-order of $R$, called the multiplicator ring of $I$

Rmk If $S$ is an o.o. of $R$ then $\mathcal{J}(S) \subseteq \mathcal{J}(R)$

Lemma : for $I, J \in \mathcal{J}(R)$, $x \in K^\times$

- $(I^t)^t = I$
- $I \subset J \Leftrightarrow I^t \supset J^t$
- $(I\cap J)^t = I^t + J^t$
- $(xI)^t = \frac{1}{x} I^t$
- $(I:J) = (I^t J)^t$
- $(I:J) = (J^t : I^t)$
- $II^t = S^t \Leftrightarrow (I:I) = S$

L1.7

**Def** A prime of $R$ is a maximal ideal $\mathfrak{p}$ of $R$.

**Lemma**: $\{\text{primes of } R\} = \{\text{prime ideals of } R \text{ which are fractional } R\text{-ideals}\}$

**Pf** "$\supseteq$" If $\mathfrak{p}$ is a prime ideal and a fractional $R$-id then $R/\mathfrak{p}$ is a finite integral domain

$\Rightarrow R/\mathfrak{p}$ is a field $\Leftrightarrow \mathfrak{p}$ is maximal.

"$\subseteq$" If $\mathfrak{p}$ is a max ideal of $R$ then

$\mathfrak{p} \cap \mathbb{Z} = \{p\}$ rational prime

b/c $R$ is integral over $\mathbb{Z}$ So given a prime ideal $\mathfrak{p}$ of $R$ we have $\mathfrak{p}$ is max $\Leftrightarrow \mathfrak{p} \cap \mathbb{Z}$ is max

$\Rightarrow \mathfrak{p} \cap K^\times \neq \phi$.

$\boxplus$

**Def** Let $I \in \mathcal{J}(R)$ is called invertible in $R$ if there exists $J \in \mathcal{J}(R)$ s.t. $IJ = R$

**Rmk** If such $J$ exists then $J = (R:I)$.

**Lemma** If $I \in \mathcal{J}(R)$ is invertible in $R$ then

$$(I:I) = R$$

**Pf**
- $I \in \mathcal{J}(R) \Rightarrow IR = I \Rightarrow R \subseteq (I:I)$
- mult $(I:I)I = I$ on both sides by $(R:I)$

$$\Rightarrow (I:I)\underbrace{I(R:I)}_{=R} = \underbrace{I(R:I)}_{=R}$$

$$\Rightarrow \underset{(I:I)}{\underset{\cup}{(I:I)}}\underset{1 \in R}{R} = R$$

$\boxplus$

Example

as before

- $R = \dfrac{\mathbb{Z}[x]}{(\underbrace{x^3+10x^2-8}_{=f})}$ $\qquad \alpha = x \bmod f$

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

- $[S : R] = 2$

- $I = 3R + (\alpha+2)R.$

One can check

$(I:I) = R$

$(R:I) = \mathbb{Z} \oplus \alpha\mathbb{Z} \oplus \left(-\frac{1}{3} + \frac{1}{3}\alpha + \frac{1}{3}\alpha^2\right)\mathbb{Z}$

and $I \cdot (R:I) = R.$

- $J = \mathbb{Z} \oplus \dfrac{\alpha}{2}\mathbb{Z} \oplus \dfrac{\alpha^2}{2}\mathbb{Z}$

$(J:J) = S$

and $J \cdot (S:J) \underbrace{\subsetneq S}_{2}$

Def* Let $T$ be a ring and $I$ an ideal of $T$. We say that $I$ is invertible (inT) if there exists an ideal $J$ of $T$ and a non-zero divisor $d$ of $T$ such that

$$I \cdot J = dT$$

Rmk Def* is equiv. to Def but it allows us to talk about invertibility of ideals in any ring.

# Invertibility and localizations



__Lemma 1)__ Let $T$ be a Noetherian ring. Then $T$ is a principal ideal ring iff every maximal ideal is principal.
[Kaplanski, 12.3]

__Lemma 2)__ Let $T$ be a semilocal ring (= finitely many maximal ideals) and let $I$ be a $T$-ideal. Then $I$ is invertible iff $I$ is principal and generated by a non-zero divisor. [Gilmer, Prop 7.4]

__Lemma 3)__ Let $R$ be an order in $K$ and $I \subseteq R$ be a fractional $R$-ideal. Then $I$ is invertible in $R$ iff $I_p$ is a principal $R_p$-ideal for every prime $p$ of $R$

Pf

- Assume $I$ is invertible in $R$. Then
$$I\,(R:I) = R$$
which localized at $p$ becomes
$$I_p \underbrace{(R:I)_p}_{\substack{\| \\ (R_p : I_p)}} = R_p$$
$\Rightarrow I_p$ is invertible in $R_p$ (local) $\overset{\text{Lemma 2}}{\Rightarrow}$ $I_p$ is princ and gen by a non z.d

- Assume $I_p = x R_p$ (dep. on $p$) $\forall p$
and consider the inclusion $\quad i : I(R:I) \subseteq R$.
Now $i$ is surjective (i.e. =) at every $p$:
$$I_p\,(R_p : I_p) = xR_p\,(R_p : xR_p) = \cancel{x}R_p \cdot \tfrac{1}{\cancel{x}}(R_p : R_p) = R_p$$
hence also globally

**Cor** Let $\mathfrak{p}$ be a prime of $R$.
Then $\mathfrak{p}$ is invertible in $R$ iff $R_\mathfrak{p}$ is a princ. ideal ring.

**Pf**
- $\mathfrak{p}$ invertible $\overset{L.2}{\Rightarrow}$ $\mathfrak{p}R_\mathfrak{p}$ is a princ. $R_\mathfrak{p}$ ideal
  unique max ideal of $R_\mathfrak{p}$
  $\Rightarrow$ $R_\mathfrak{p}$ is a P.I.R.
- $R_\mathfrak{p}$ a P.I.R. $\Rightarrow$ $\mathfrak{p}R_\mathfrak{p} = xR_\mathfrak{p}$.
  If $\mathfrak{q}$ is a prime $\neq \mathfrak{p}$, then
  $$\mathfrak{p}R_\mathfrak{q} = R_\mathfrak{q}$$
  $\Rightarrow$ $\mathfrak{p}$ is locally princ. at every prime
  $\overset{L.3}{\Rightarrow}$ $\mathfrak{p}$ invertible in $R$

---

**Cor** Every fractional $R$-ideal is invertible in $R$.

$$\Updownarrow$$

$$R = \mathcal{O}_K$$

**Pf** "$\Downarrow$" Recall: $I$ inv. in $R \Rightarrow (I:I) = R$.

Apply it to $\mathfrak{f} = (R : \mathcal{O}_K)$ conductor of $R$

- $(\mathfrak{f} : \mathfrak{f}) = \mathcal{O}_K$ $\qquad \mathfrak{f}\mathcal{O}_K \subseteq R$

$$\mathfrak{f}\mathcal{O}_K = (\mathfrak{f}\mathcal{O}_K) \cdot \mathcal{O}_K$$

$\Rightarrow \mathfrak{f}\mathcal{O}_K \subseteq \mathfrak{f}$ Hence "=".

then $\underbrace{(\mathfrak{f} : \mathfrak{f})}_{= R} = \mathcal{O}_K$

by hypothesis

"$\Uparrow$" We will prove that every prime $\mathfrak{p}$ of $\mathcal{O}_K$ is invertible.

- Write $K = K_1 \times \dots \times K_r$, $K_i$ number fields

then $\mathcal{O}_K = \mathcal{O}_{K_1} \times \dots \times \mathcal{O}_{K_r}$

Hence $\exists i$ st $\mathfrak{p} = \mathcal{O}_{K_1} \times \dots \times \mathfrak{p}_i \times \dots \mathcal{O}_{K_r}$ for $\mathfrak{p}_i$ prime of $\mathcal{O}_{K_i}$

Now $\mathcal{O}_{K_i}$ is a Dedekind domain

by "classical" number theory we have that

$\mathfrak{p}_i$ is invertible in $\mathcal{O}_{K_i}$

$\Rightarrow \mathfrak{p}$ is invertible in $\mathcal{O}_K$.

$\Rightarrow \mathcal{O}_{K,\mathfrak{p}}$ is a P.I.R.

$\Rightarrow \forall I \in \mathcal{I}(\mathcal{O}_K)$ $\quad I_\mathfrak{p}$ is princ ($\Leftrightarrow$ invertible)

$\Rightarrow I$ inv.

# § Gorenstein Orders

**Prop** Let $R$ be an order in $K$.
TFAE:

(A) $\forall I \in \mathcal{J}(R)$ with $(I:I) = R$ is invertible in $R$

$\circledast$ (B) $\forall I \in \mathcal{J}(R)$ we have $(R:(R:I)) = I$.

(C) $R^t$ is invertible (in $R$)

**Def** An order $R$ satisfying $\circledast$ is called Gorenstein.
If every over-order of $R$ is Gorenstein then $R$ is called a Bass order

**Pf** Recall $(I:I) = R \Leftrightarrow I \cdot I^t = R^t$

and $(R^t : R^t) = (R:R) = R$

So "(A) $\Leftrightarrow$ (C)."

"(C) $\Rightarrow$ (B)"

Exercise. See Buchmann, Lenstra
Approx Ring of Integers

"(B) $\Rightarrow$ (C)":

$(R:(R:R^t)) = R^t$

$(R^t(R:R^t))^t = R^t$

$\wedge t$

$R^t(R:R^t) = R$ done.

Exercise Consider:

$$K = \frac{\mathbb{Q}[x]}{(x^2+1)} = \mathbb{Q}(i)$$

$$\mathcal{O}_K = \mathbb{Z}[i]$$

$$R = \mathbb{Z}[2i] = \mathbb{Z} \oplus 2i\mathbb{Z}$$

Compute: $\mathcal{O}_K^t$, $R^t$, $\mathfrak{f} := (R : \mathcal{O}_K)$

Solution

$$K = \mathbb{Q} \oplus i\mathbb{Q}$$

$$\mathcal{O}_K = \mathbb{Z} \oplus i\mathbb{Z} \rightsquigarrow$$

$$\mathcal{O}_K^t = \{x \in K : \mathrm{Tr}(x\mathcal{O}_K) \subseteq \mathbb{Z}\}$$

$$\mathcal{O}_K^t = a\mathbb{Z} \oplus b\mathbb{Z} \qquad a, b \in K$$

$$\mathrm{Tr}(1 \cdot a) = 1$$

$$\mathrm{Tr}(1 \cdot b) = 0$$

$$\mathrm{Tr}(i \cdot a) = 0$$

$$\mathrm{Tr}(i \cdot b) = 1$$

Write $a = a_1 + i a_2$
$b = b_1 + i b_2$

$$1 \cdot a = a = \begin{array}{c} \begin{pmatrix} a_1 & -a_2 \\ a_2 & a_1 \end{pmatrix} \\ 1a \qquad ia \end{array}$$

$$\mathrm{Tr}\left( \quad \right) = 2a_1 = 1$$

$$ia = \begin{pmatrix} -a_2 & -a_1 \\ a_1 & -a_2 \end{pmatrix}$$

$$\| \qquad 1 \cdot ia \qquad i \cdot ia = -a$$

$$-a_2 + ia_1$$

$$\mathrm{Tr}\left( \quad \right) = -2a_2 = 1$$

$$\Rightarrow a_2 = -\frac{1}{2}$$

$(*)$

$(*)$: $\mathcal{O}_K^t = \frac{1}{2}\mathbb{Z} \oplus \left(-\frac{1}{2}\right) i\mathbb{Z}$

$$= \frac{1}{2i}\mathcal{O}_K$$

$$R^t = \frac{1}{4i} R = -\frac{1}{4} i R$$

$$\mathfrak{f} = (R : \mathcal{O}_K) = \left(R^t \cdot \mathcal{O}_K\right)^t = \cancel{\mathcal{O}_K}$$

$$\| $$

$$= \left(+\frac{1}{4i}\mathcal{O}_K\right)^t =$$

$$= 4i\, \mathcal{O}_K^t$$

$$= 4i \cdot \frac{1}{2i}\mathcal{O}_K = 2\mathcal{O}_K$$