

# Poincaré à la Makdisi

Nicolas Mascot

Trinity College Dublin

2026 PARI/GP workshop  
13 January 2026

# The Poincaré torsor

# Line bundles and torsors

Let  $X$  be a variety over a field  $K$ ,  
and let  $\mathcal{L} \rightarrow X$  be a line bundle.

# Line bundles and torsors

Let  $X$  be a variety over a field  $K$ ,  
and let  $\mathcal{L} \rightarrow X$  be a line bundle.

We write  $\mathcal{L}^\times$  for  $\mathcal{L}$  with the 0 section removed.

# Line bundles and torsors

Let  $X$  be a variety over a field  $K$ ,  
and let  $\mathcal{L} \rightarrow X$  be a line bundle.

We write  $\mathcal{L}^\times$  for  $\mathcal{L}$  with the 0 section removed.

The fibres of  $\mathcal{L}^\times$  are torsors under  $\mathbb{G}_m$  (free and transitive action of  $K^\times$ ).

# Enters Poincaré

Now let  $A$  be an Abelian variety over  $K$ .  
Its dual is

$$A^\vee = \text{Pic}^0(A) = \{\text{line bundles } \mathcal{L} \rightarrow A \mid \deg \mathcal{L} = 0\} / \simeq .$$

The Poincaré bundle on  $A$  is the unique line bundle

$$\mathcal{P} \longrightarrow A \times A^\vee$$

such that

- for all  $y = [\mathcal{L}] \in A^\vee$ ,  $\mathcal{P}|_{A \times \{y\}} \simeq \mathcal{L}$ ,
- and  $\mathcal{P}|_{0 \times A^\vee} \simeq \mathcal{O}_{A^\vee}$  is trivial.

The Poincaré torsor on  $A$  is  $\mathcal{P}^\times$ .

# What this means for Jacobians

Let  $C$  be a “nice” curve over  $K$ .

Its Jacobian is

$$\begin{aligned} J &\stackrel{\text{def}}{=} \text{Pic}^0(C) \\ &\stackrel{\text{def}}{=} \{\text{line bundles } \mathcal{L} \rightarrow C \mid \deg \mathcal{L} = 0\} / \simeq \\ &\stackrel{\mathcal{O}_C(D) \leftrightarrow D}{=} \{\text{divisors } D/C \mid \deg D = 0\} / \sim. \end{aligned}$$

# What this means for Jacobians

Let  $C$  be a “nice” curve over  $K$ .

Its Jacobian is

$$\begin{aligned} J &\stackrel{\text{def}}{=} \text{Pic}^0(C) \\ &\stackrel{\text{def}}{=} \{\text{line bundles } \mathcal{L} \rightarrow C \mid \deg \mathcal{L} = 0\} / \simeq \\ &\stackrel{\mathcal{O}_C(D) \leftrightarrow D}{=} \{\text{divisors } D/C \mid \deg D = 0\} / \sim . \end{aligned}$$

It is an Abelian variety, with group law induced by tensor product of line bundles / addition of divisors.

# What this means for Jacobians

Let  $C$  be a “nice” curve over  $K$ .

Its Jacobian is

$$\begin{aligned} J &\stackrel{\text{def}}{=} \text{Pic}^0(C) \\ &\stackrel{\text{def}}{=} \{\text{line bundles } \mathcal{L} \rightarrow C \mid \deg \mathcal{L} = 0\} / \simeq \\ &\stackrel{\mathcal{O}_C(D) \leftrightarrow D}{=} \{\text{divisors } D/C \mid \deg D = 0\} / \sim. \end{aligned}$$

It is an Abelian variety, with group law induced by tensor product of line bundles / addition of divisors.

Furthermore, it is self-dual:  $J^\vee \simeq J$ .

# What this means for Jacobians

Let  $C$  be a “nice” curve over  $K$ .

Its Jacobian is

$$\begin{aligned} J &\stackrel{\text{def}}{=} \text{Pic}^0(C) \\ &\stackrel{\text{def}}{=} \{\text{line bundles } \mathcal{L} \rightarrow C \mid \deg \mathcal{L} = 0\} / \simeq \\ &\stackrel{\mathcal{O}_C(D) \leftarrow D}{=} \{\text{divisors } D/C \mid \deg D = 0\} / \sim. \end{aligned}$$

It is an Abelian variety, with group law induced by tensor product of line bundles / addition of divisors.

Furthermore, it is self-dual:  $J^\vee \simeq J$ .

## Theorem

Let  $x = [D]$  and  $y = [E] \in J$ .

The stalk of  $\mathcal{P}$  at  $(x, y) \in J \times J$  is

$$\mathcal{P}_{x,y} \simeq \mathcal{N}_D(\mathcal{O}_C(E)).$$

# What this means for Jacobians

## Theorem

Let  $x = [D]$  and  $y = [E] \in J$ .

The stalk of  $\mathcal{P}$  at  $(x, y) \in J \times J$  is

$$\mathcal{P}_{x,y} \simeq \mathcal{N}_D(\mathcal{O}_C(E)).$$

Here  $\mathcal{N}_D(f) \stackrel{\text{def}}{=} f(D) \stackrel{\text{def}}{=} \prod_i f(P_i)^{n_i}$  where  $D = \sum_i n_i P_i$ .

# What this means for Jacobians

## Theorem

Let  $x = [D]$  and  $y = [E] \in J$ .

The stalk of  $\mathcal{P}$  at  $(x, y) \in J \times J$  is

$$\mathcal{P}_{x,y} \simeq \mathcal{N}_D(\mathcal{O}_C(E)).$$

Here  $\mathcal{N}_D(f) \stackrel{\text{def}}{=} f(D) \stackrel{\text{def}}{=} \prod_i f(P_i)^{n_i}$  where  $D = \sum_i n_i P_i$ .

Thus if  $D \not\sim E$ , then the meromorphic section 1 of  $\mathcal{O}_C(E)$  is regular and nonvanishing along  $D$ , so

$$\mathcal{N}_D(1 \in \mathcal{O}_C(E)) \in \mathcal{P}_{x,y}^\times,$$

and

$$\mathcal{P}_{x,y}^\times = \left\{ \lambda \cdot \mathcal{N}_D(1 \in \mathcal{O}_C(E)) \mid \lambda \in K^\times \right\}.$$

# Partial group laws

We have partial group laws

$$\mathcal{P}_{x_1,y}^{\times} \otimes \mathcal{P}_{x_2,y}^{\times} \longrightarrow \mathcal{P}_{x_1+x_2,y}^{\times} \quad \text{and} \quad \mathcal{P}_{x,y_1}^{\times} \otimes \mathcal{P}_{x,y_2}^{\times} \longrightarrow \mathcal{P}_{x,y_1+y_2}^{\times}$$

coming from

$$\mathcal{N}_{D_1}(\mathcal{O}_C(E)) \otimes \mathcal{N}_{D_2}(\mathcal{O}_C(E)) \simeq \mathcal{N}_{D_1+D_2}(\mathcal{O}_C(E)),$$

$$\mathcal{N}_D(\mathcal{O}_C(E_1)) \otimes \mathcal{N}_D(\mathcal{O}_C(E_2)) \simeq \mathcal{N}_D(\mathcal{O}_C(E_1 + E_2)).$$

# Application: Quadratic Chabauty

# Classical Chabauty

Let  $C$  be a “nice” curve of genus  $g$  over  $\mathbb{Q}$ .

Theorem (Faltings)

*If  $g \geq 2$ , then  $C(\mathbb{Q})$  is finite.*

# Classical Chabauty

Let  $C$  be a “nice” curve of genus  $g$  over  $\mathbb{Q}$ .

Theorem (Faltings)

*If  $g \geq 2$ , then  $C(\mathbb{Q})$  is finite.*

Theorem (Mordell-Weil)

$J(\mathbb{Q}) \simeq \mathbb{Z}^r \times \text{finite group.}$

# Classical Chabauty

Let  $C$  be a “nice” curve of genus  $g$  over  $\mathbb{Q}$ .  
Suppose we know  $P_0 \in C(\mathbb{Q})$ . Then

$$j : \begin{array}{ccc} C & \longrightarrow & J \\ P & \longmapsto & [P - P_0] \end{array},$$

is an embedding (assuming  $g \neq 0$ ).

# Classical Chabauty

Let  $C$  be a “nice” curve of genus  $g$  over  $\mathbb{Q}$ .  
Suppose we know  $P_0 \in C(\mathbb{Q})$ . Then

$$j : \begin{array}{ccc} C & \longrightarrow & J \\ P & \longmapsto & [P - P_0] \end{array},$$

is an embedding (assuming  $g \neq 0$ ).

## Idea (Chabauty)

Fix a Chabauty prime  $p \in \mathbb{N}$ ; catch  $C(\mathbb{Q})$  inside

$$\underbrace{C(\mathbb{Q}_p)}_{\dim 1} \cap \underbrace{\overline{J(\mathbb{Q})}}_{\dim \leq r}^{p\text{-adic}} \subset \underbrace{J(\mathbb{Q}_p)}_{\dim g}.$$

# Classical Chabauty

Let  $C$  be a “nice” curve of genus  $g$  over  $\mathbb{Q}$ .  
Suppose we know  $P_0 \in C(\mathbb{Q})$ . Then

$$j : \begin{array}{ccc} C & \longrightarrow & J \\ P & \longmapsto & [P - P_0] \end{array},$$

is an embedding (assuming  $g \neq 0$ ).

## Idea (Chabauty)

Fix a Chabauty prime  $p \in \mathbb{N}$ ; catch  $C(\mathbb{Q})$  inside

$$\underbrace{C(\mathbb{Q}_p)}_{\dim 1} \cap \underbrace{\overline{J(\mathbb{Q})}}_{\dim \leq r}^{p\text{-adic}} \subset \underbrace{J(\mathbb{Q}_p)}_{\dim g}.$$

But what if  $r \geq g$ ? Then  $J(\mathbb{Q})$  could be dense in  $J(\mathbb{Q}_p)$  . . .

# Quadratic Chabauty

Try to gain a dimension by lifting  $j$  :  $\begin{array}{ccc} C & \hookrightarrow & J \\ P & \mapsto & [P - P_0] \end{array}$  to  $\mathcal{P}^\times$ :

$$\begin{array}{ccccc} & & \mathcal{P}^\times & & \\ & \nearrow \widetilde{j} & \downarrow & & \\ C & \xrightarrow{j} & J & \xrightarrow{(\text{Id}, h)} & J \times J \\ & & & & (h \in \text{End}(J)) \end{array}$$

# Quadratic Chabauty

Try to gain a dimension by lifting  $j$  :  $\begin{array}{ccc} C & \hookrightarrow & J \\ P & \mapsto & [P - P_0] \end{array}$  to  $\mathcal{P}^\times$ :

$$\begin{array}{ccccc} & & \mathcal{P}^\times & & \\ & \nearrow \widetilde{j} & \downarrow & & \\ C & \xrightarrow{j} & J & \xrightarrow{(\text{Id}, h)} & J \times J \\ & & & & (h \in \text{End}(J)) \end{array}$$

We now try to catch  $C(\mathbb{Q})$  inside

$$C(\mathbb{Q}_p) \cap \underbrace{\mathcal{P}^\times(\mathbb{Q})}_{p\text{-adic}} \subset \mathcal{P}^\times(\mathbb{Q}_p).$$

Unfortunately,  $\mathbb{Q}^\times$  dense in  $\mathbb{Q}_p^\times$ , so  $\mathcal{P}^\times(\mathbb{Q})$  dense in  $\mathcal{P}^\times(\mathbb{Q}_p)$  whenever  $J(\mathbb{Q})$  dense in  $J(\mathbb{Q}_p)$  ...

# Quadratic Chabauty

Try to gain a dimension by lifting  $j : C \hookrightarrow J$  to  $\mathcal{P}^\times$ :  
 $P \mapsto [P - P_0]$

Let  $\mathcal{C}/\mathbb{Z}$  be a proper model of  $C/\mathbb{Q}$ , so that  $\mathcal{C}(\mathbb{Z}) = C(\mathbb{Q})$ ,  
and let  $\mathcal{J}$  be the Néron model of  $J$ :

$$\begin{array}{ccccc} & & \mathcal{P}^\times & & \\ & \nearrow \widetilde{j} & \downarrow & & \\ \mathcal{C} & \xrightarrow{j} & \mathcal{J} & \xrightarrow{(\text{Id}, h)} & \mathcal{J} \times \mathcal{J} \\ & & & & (h \in \text{End}(J)) \end{array}$$

# Quadratic Chabauty

Try to gain a dimension by lifting  $j : \begin{matrix} C & \hookrightarrow & J \\ P & \mapsto & [P - P_0] \end{matrix}$  to  $\mathcal{P}^\times$ :

Let  $\mathcal{C}/\mathbb{Z}$  be a proper model of  $C/\mathbb{Q}$ , so that  $\mathcal{C}(\mathbb{Z}) = C(\mathbb{Q})$ , and let  $\mathcal{J}$  be the Néron model of  $J$ :

$$\begin{array}{ccccc} & & \mathcal{P}^\times & & \\ & \nearrow \widetilde{j} & \downarrow & & \\ \mathcal{C} & \xrightarrow{j} & \mathcal{J} & \xrightarrow{(\text{Id}, h)} & \mathcal{J} \times \mathcal{J} \\ & & & & (h \in \text{End}(J)) \end{array}$$

Since  $\mathbb{G}_m(\mathbb{Z}) = \mathbb{Z}^\times = \{\pm 1\}$  is finite, we know the possible  $\mathbb{G}_m$ -components of  $\widetilde{j}(\mathcal{C}(\mathbb{Z}))$ .

# Implementing $J$ and $\mathcal{P}^\times$

# Makdisi's framework

Let  $C/K$  be a “nice” curve of genus  $g$ .

Assume  $C(K)$  large (e.g.  $K = \mathbb{C}$  or  $\mathbb{Q}_p$ , or extend  $K$ ).

Pick line bundle  $\mathcal{L} \rightarrow C$  of degree  $d_0 = \deg \mathcal{L} \gg_g 0$ ,  
and fix points  $Q_1, \dots, Q_m \in C(K)$  ( $m \gg_{d_0} 0$ ).

Write  $V_n =$  global sections of  $\mathcal{L}^{\otimes n}$  ( $n = 1, 2, \dots, 5$ ).

Each  $0 \neq s \in V_n$  has divisor  $(s)_n$ , effective of degree  $n \cdot d_0$ .

More generally, when  $D$  is an effective divisor, write

$V_n(-D) \subset V_n$  for the sections of  $\mathcal{L}^{\otimes n}(-D)$ .

Embed the  $V_n$  into  $K^m$  by  $s \mapsto (s(Q_1), \dots, s(Q_m))$ .

Each point  $x \in J$  is of the form  $x = [\mathcal{L}(-D)]$  for some  
effective divisor  $D$  of degree  $d_0$ , and is represented by

$V_2(-D) \stackrel{\text{def}}{=} \text{sections of } \mathcal{L}^{\otimes 2}(-D) \subset V_2 \subset K^m$ .

# Makdisi's framework

Pick line bundle  $\mathcal{L} \rightarrow C$  of degree  $d_0 = \deg \mathcal{L} \gg_g 0$ ,  
and fix points  $Q_1, \dots, Q_m \in C(K)$  ( $m \gg_{d_0} 0$ ).

Write  $V_n =$  global sections of  $\mathcal{L}^{\otimes n}$  ( $n = 1, 2, \dots, 5$ ).

Each  $0 \neq s \in V_n$  has divisor  $(s)_n$ , effective of degree  $n \cdot d_0$ .

More generally, when  $D$  is an effective divisor, write

$V_n(-D) \subset V_n$  for the sections of  $\mathcal{L}^{\otimes n}(-D)$ .

Embed the  $V_n$  into  $K^m$  by  $s \mapsto (s(Q_1), \dots, s(Q_m))$ .

Each point  $x \in J$  is of the form  $x = [\mathcal{L}(-D)]$  for some effective divisor  $D$  of degree  $d_0$ , and is represented by

$V_2(-D) \stackrel{\text{def}}{=} \text{sections of } \mathcal{L}^{\otimes 2}(-D) \subset V_2 \subset K^m$ .

In particular,  $0 \in J$  is represented by  $s \cdot V_1 \subset V_2$   
for any  $0 \neq s \in V_1$ , corresponding to  $D = (s)_1$ .

# Equality test

## Algorithm (Makdisi's equality test)

Given  $V_2(-D)$  and  $V_2(-D')$  representing  $x = [\mathcal{L}(-D)]$  and  $y = [\mathcal{L}(-D')] \in J$ ,

- ① Pick  $0 \neq u \in V_2(-D) \rightsquigarrow (u)_2 = D + E$ .
- ② Compute  $u \cdot V_2(-D') = V_4(-D - D' - E)$ .
- ③ Compute

$$W = V_2(-D' - E) = \{v \in V_2 \mid v \cdot V_2(-D) \subset u \cdot V_2(-D')\}.$$

- If  $x = y$ , then  $W = K \cdot u'$  where  $D + (u')_2 = D' + (u)_2$ .
- If  $x \neq y$ , then  $W = \{0\}$ .

Note: the “linear equivalence certificate”  $u/u' \in K(C)$  is randomised.

# Representing $\mathcal{P}_{x,y}^\times$

Let  $x = [\mathcal{L}(-D)]$  and  $y = [\mathcal{L}(-E)] \in J$ . What is  $\mathcal{P}_{x,y}^\times$ ?

# Representing $\mathcal{P}_{x,y}^\times$

Let  $x = [\mathcal{L}(-D)]$  and  $y = [\mathcal{L}(-E)] \in J$ . What is  $\mathcal{P}_{x,y}^\times$ ?

Fix  $s_0 \in V_1$ , and let  $D_0 \stackrel{\text{def}}{=} (s_0)_1$ .

Then  $\mathcal{L} \simeq \mathcal{O}_C(D_0) \rightsquigarrow x = [D - D_0]$ ,  $y = [E - D_0]$ .

Unfortunately,  $D - D_0$  and  $E - D_0$  intersect,  
so  $\mathcal{N}_{D-D_0}(1 \in \mathcal{O}_C(E - D_0))$  is not a valid element of  $\mathcal{P}_{x,y}^\times$ .

# Representing $\mathcal{P}_{x,y}^\times$

Let  $x = [\mathcal{L}(-D)]$  and  $y = [\mathcal{L}(-E)] \in J$ . What is  $\mathcal{P}_{x,y}^\times$ ?

Fix  $s_0 \in V_1$ , and let  $D_0 \stackrel{\text{def}}{=} (s_0)_1$ .

Then  $\mathcal{L} \simeq \mathcal{O}_C(D_0) \rightsquigarrow x = [D - D_0]$ ,  $y = [E - D_0]$ .

Unfortunately,  $D - D_0$  and  $E - D_0$  intersect,  
so  $\mathcal{N}_{D-D_0}(1 \in \mathcal{O}_C(E - D_0))$  is not a valid element of  $\mathcal{P}_{x,y}^\times$ .

Solution: fix another  $t_0 \in V_1$ , such that  $E_0 \stackrel{\text{def}}{=} (t_0)_1 \not\sim D_0$ .

If  $D \not\sim E_0$ ,  $E \not\sim D_0$ , and  $D \not\sim E$ , then

$$[D, E] \stackrel{\text{def}}{=} \mathcal{N}_{D-D_0}(1 \in \mathcal{O}_C(E - E_0)) \in \mathcal{P}_{x,y}^\times,$$

and  $\mathcal{P}_{x,y}^\times = \{\lambda \cdot [D, E] \mid \lambda \in K^\times\}$ .

$\rightsquigarrow$  We can use  $[D, E]$  as a reference point for  $\mathcal{P}_{x,y}^\times$ .

# Representing $\mathcal{P}_{x,y}^\times$

Fix  $s_0 \in V_1$ , and let  $D_0 \stackrel{\text{def}}{=} (s_0)_1$ .

Then  $\mathcal{L} \simeq \mathcal{O}_C(D_0) \rightsquigarrow x = [D - D_0]$ ,  $y = [E - D_0]$ .

Solution: fix another  $t_0 \in V_1$ , such that  $E_0 \stackrel{\text{def}}{=} (t_0)_1 \not\sim D_0$ .

If  $D \not\sim E_0$ ,  $E \not\sim D_0$ , and  $D \not\sim E$ , then

$$[D, E] \stackrel{\text{def}}{=} \mathcal{N}_{D-D_0}(1 \in \mathcal{O}_C(E - E_0)) \in \mathcal{P}_{x,y}^\times,$$

and  $\mathcal{P}_{x,y}^\times = \{\lambda \cdot [D, E] \mid \lambda \in K^\times\}$ .

$\rightsquigarrow$  We can use  $[D, E]$  as a reference point for  $\mathcal{P}_{x,y}^\times$ .

However, it depends on the choice of effective divisors  $D$ ,  $E$  such that  $x = [\mathcal{L}(-D)]$  and  $y = [\mathcal{L}(-E)] \dots$

# Comparison formula

## Algorithm (Comparison in $\mathcal{P}^\times$ )

Given 4 points  $x_1 = [\mathcal{L}(-D_1)]$ ,  $y_1 = [\mathcal{L}(-E_1)]$ ,  
 $x_2 = [\mathcal{L}(-D_2)]$ ,  $y_2 = [\mathcal{L}(-E_2)]$  of  $J$ ,  
we want to compare  $[D_1, E_1]$  with  $[D_2, E_2]$ .

- ① Use Makdisi's equality test to check  $x_1 = x_2$  and  $y_1 = y_2$ .  
If not, complain / terminate.  
Otherwise, we get  $d_1, d_2, e_1, e_2 \in V_2$  such that  
 $D_1 + (d_1)_2 = D_2 + (d_2)_2$  and  $E_1 + (e_1)_2 = E_2 + (e_2)_2$ .
- ② Output that  $[D_2, E_2] = \lambda \cdot [D_1, E_1]$ , where

$$\lambda = \frac{\mathcal{N}_{E_2}(d_1/d_2) \mathcal{N}_{D_0}(e_1/e_2)}{\mathcal{N}_{E_0}(d_1/d_2) \mathcal{N}_{D_1}(e_1/e_2)} = \frac{\mathcal{N}_{E_1}(d_1/d_2) \mathcal{N}_{D_0}(e_1/e_2)}{\mathcal{N}_{E_0}(d_1/d_2) \mathcal{N}_{D_2}(e_1/e_2)}.$$

Notes:  $V_2(-D_0) = s_0 \cdot V_1$ , and  $V_2(-E_0) = t_0 \cdot V_1$ .

May need to run several times until the norms work.

# Evaluating norms

Given  $V_2(-D)$  encoding effective  $D = \sum_i n_i P_i$ , and columns in  $K^m$  representing  $u, v \in V_2$  not vanishing at the  $P_i$ , want to evaluate

$$\mathcal{N}_D(u/v) = \prod_i \frac{u}{v} (P_i)^{n_i} \in K^\times.$$

## Algorithm (Norm)

- ① Compute  $V_4(-D) = V_2 \cdot V_2(-D)$ .
- ② Find supplements  $V_2 = S \oplus V_2(-D)$  and  $V_4 = T \oplus V_4(-D)$ .
- ③ Compute  $\Delta_u = \det( S \hookrightarrow V_2 \xrightarrow{u} V_4 \twoheadrightarrow T )$  and  $\Delta_v$ .
- ④ Output  $\mathcal{N}_D(u/v) = \Delta_u / \Delta_v$ .

Explanation:  $V(-D) = \text{Ker} (s \mapsto s(D))$ .

# Summary

- We fix once and for all  $\mathcal{L} \gg 0 \rightarrow C$ ,  
and then two sections  $s_0, t_0$  of  $\mathcal{L}$  such that

$$D_0 \stackrel{\text{def}}{=} (s_0)_1 \quad \not\sim \quad E_0 \stackrel{\text{def}}{=} (t_0)_1.$$

- Given  $x, y \in J$ , choose effective divisors  $D, E$  such that

$$x = [\mathcal{L}(-D)], \quad y = [\mathcal{L}(-E)] \quad \text{and} \quad D \not\sim E_0, \quad E \not\sim D_0, \quad D \not\sim E,$$

and represent them by

$$V_2(-D), \quad V_2(-E) \quad \subset V_2 = \text{sections of } \mathcal{L}^{\otimes 2}.$$

- Then  $[D, E] \stackrel{\text{def}}{=} \mathcal{N}_{D-D_0}(1 \in \mathcal{O}_C(E - E_0)) \in \mathcal{P}_{x,y}^{\times}$ ,  
so we represent  $\lambda \cdot [D, E] \in \mathcal{P}_{x,y}^{\times}$  by the triple

$$( \quad V_2(-D) \quad , \quad V_2(-E) \quad , \quad \lambda \quad )$$

(where  $\lambda \in K^{\times}$ ).

# Group law in $J$

## Algorithm (Makdisi's addflip)

Given  $V_2(-D_1)$  and  $V_2(-D_2)$

representing  $x_1 = [\mathcal{L}(-D_1)]$  and  $x_2 = [\mathcal{L}(-D_2)] \in J$ ,

compute  $V_2(-D_3)$  representing  $x_3 = [\mathcal{L}(-D_3)]$   
such that  $x_1 + x_2 + x_3 = 0 \in J$ .

- ① Compute  $V_4(-D_1 - D_2) = V_2(-D_1) \cdot V_2(-D_2)$ .
- ② Compute  $V_3(-D_1 - D_2) = \{v \in V_3 \mid v \cdot V_1 \subset V_4(-D_1 - D_2)\}$ .
- ③ Pick  $0 \neq u \in V_3(-D_1 - D_2)$ , so  $(u)_3 = D_1 + D_2 + D_3$ .
- ④ Compute  $u \cdot V_2 = V_5(-D_1 - D_2 - D_3)$ .
- ⑤ Compute  $V_2(-D_3) = \{v \in V_2 \mid v \cdot V_3(-D_1 - D_2) \subset u \cdot V_2\}$ .

## Algorithm (Makdisi's negation)

Given  $V_2(-D)$  representing  $x = [\mathcal{L}(-D)] \in J$ ,  
compute  $V_2(-D')$  representing  $x' = [\mathcal{L}(-D')] \in J$   
such that  $x + x' = 0 \in J$ .

- ① Pick  $0 \neq u \in V_2(-D)$ , so that  $(u)_2 = D + D'$ .
- ② Compute  $u \cdot V_2 = V_4(-D - D')$ .
- ③ Compute  $V_2(-D') = \{v \in V_2 \mid v \cdot V_2(-D) \subset u \cdot V_2\}$ .

# Partial group laws in $\mathcal{P}^\times$

## Algorithm (Left partial group law in $\mathcal{P}^\times$ )

Given 4 points of  $J$

$x_1 = [\mathcal{L}(-D_1)]$ ,  $y_1 = [\mathcal{L}(-E_1)]$ ,  $x_2 = [\mathcal{L}(-D_2)]$ ,  $y_2 = [\mathcal{L}(-E_2)]$   
such that  $y_1 = y_2 \stackrel{\text{def}}{=} y$ ,

want to apply  $\mathcal{P}_{x_1, y}^\times \otimes \mathcal{P}_{x_2, y}^\times \rightarrow \mathcal{P}_{x_1 + x_2, y}^\times$  to  $[D_1, E_1]$  and  $[D_2, E_2]$ .

- ① Find  $\lambda \in K^\times$  such that  $[D_2, E_2] = \lambda[D_2, E_1]$ .
- ② Find  $(V_2(-D_3), u)$  such that  $(u)_3 = D_1 + D_2 + D_3$ , and then  $(V_2(-D_4), v)$  such that  $(v)_2 = D_3 + D_4$ .
- ③ Output  $\lambda \cdot \mu \cdot [D_4, E_1]$ , where  $\mu = \mathcal{N}_{E_1} \left( \frac{u}{vs_0} \right) \Big/ \mathcal{N}_{E_0} \left( \frac{u}{vs_0} \right)$ .

The right partial group law is similar.