Translating Ideals to Isogenies

A tutorial on the general approach

Jonathan Komada Eriksen

Setting:

"Effective primitive embedding"

- E elliptic curve
- $\mathrm{End}(E) \supseteq O$ quadratic order OR maximal quaternion order
- $I = O\langle N, \alpha \rangle$ a (primitive, invertible) ideal of with $\mathrm{nrd}(I) = N$

Goal:

- Compute ϕ_I

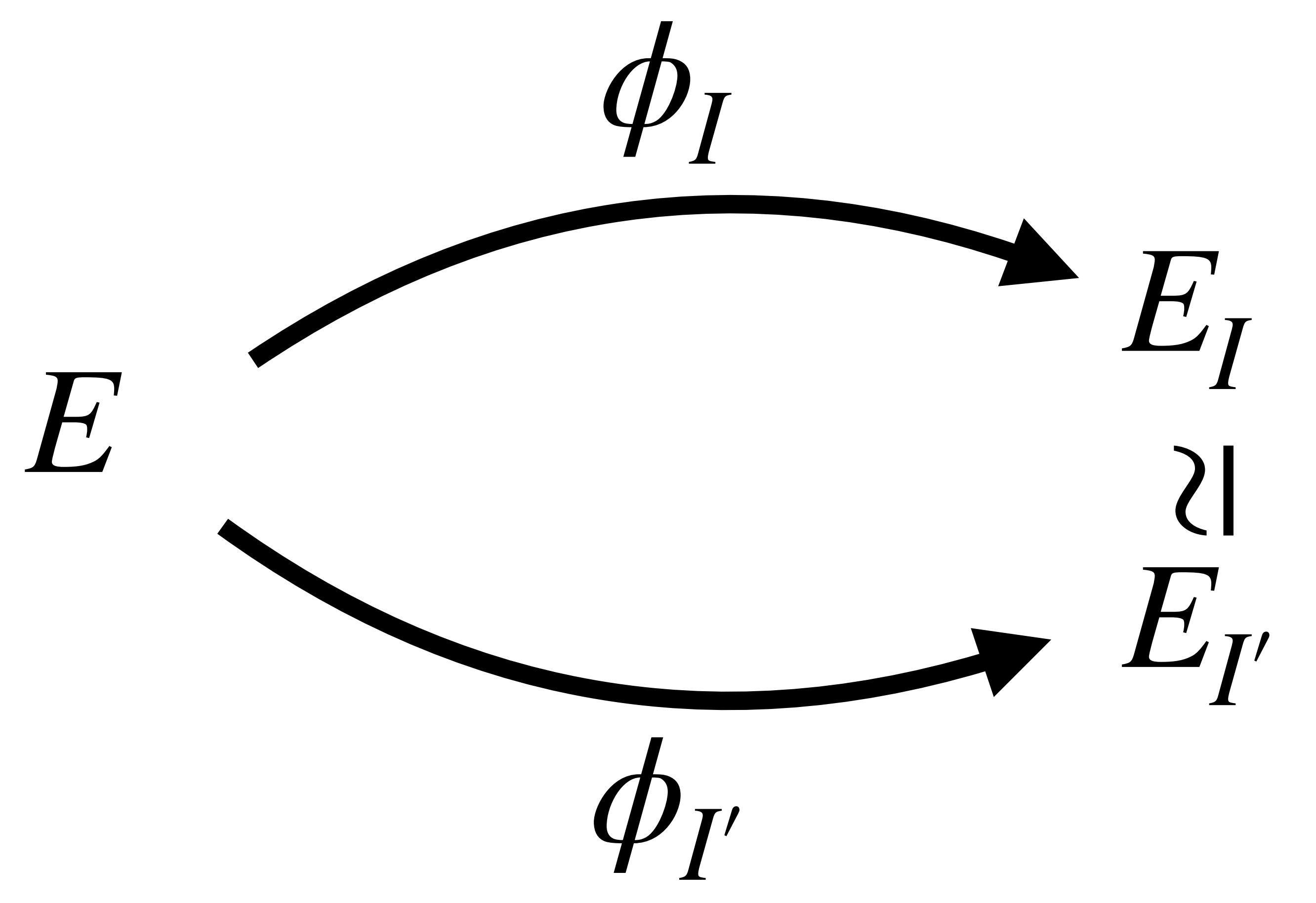
$I = \langle N, \alpha \rangle$

Some preliminaries

ϕ_I is **defined by** $\ker \phi_I = \{P \in E \mid \beta(P) = 0, \forall \beta \in I\}$

$$= E[N] \cap \ker \alpha$$

We are free to replace ϕ_I by $\phi_{I'}$ where $I' = I\beta$



$I = \langle N, \alpha \rangle$

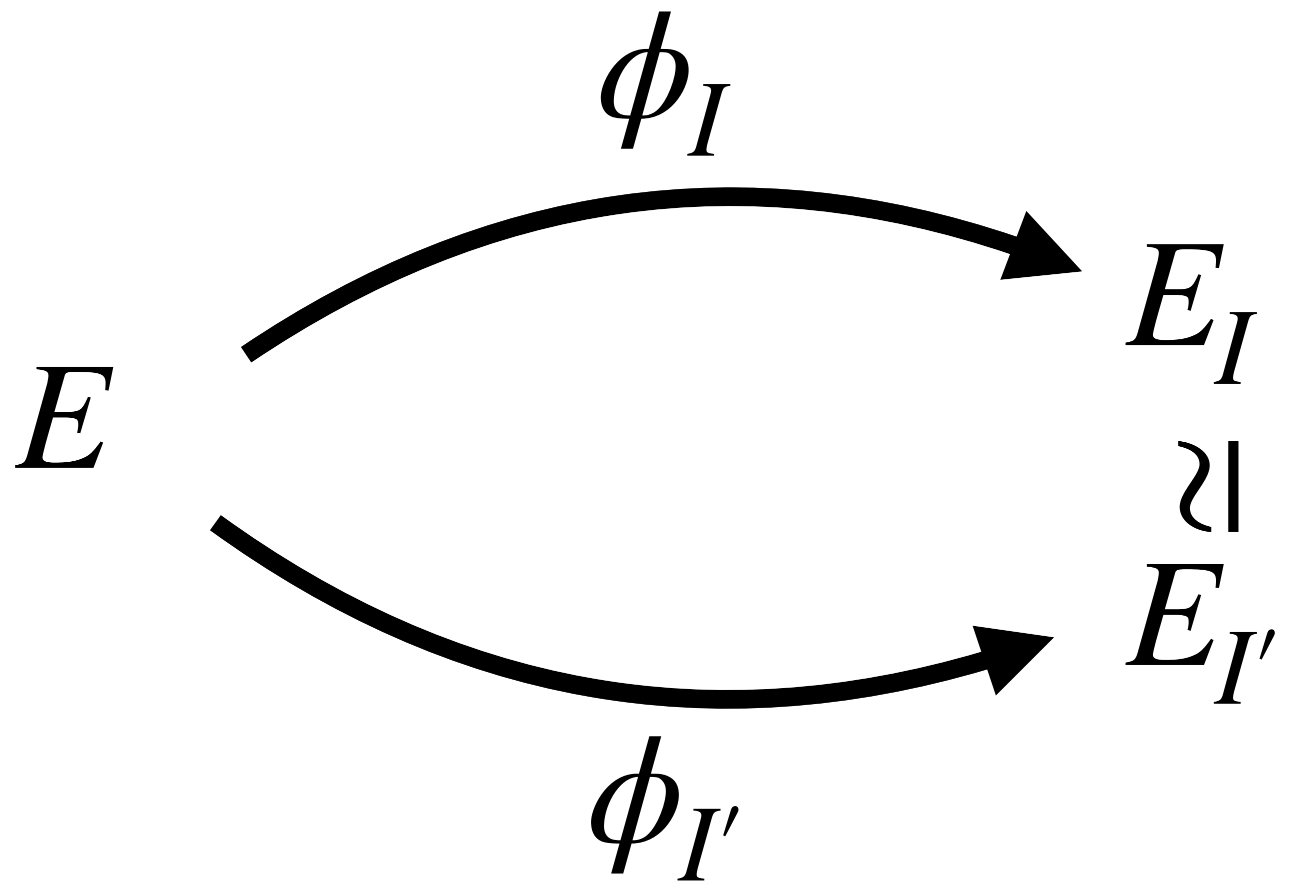
Some preliminaries

ϕ_I is **defined by** $\ker \phi_I = \{P \in E \mid \beta(P) = 0, \forall \beta \in I\}$
$= E[N] \cap \ker \alpha$

We are free to replace ϕ_I by $\phi_{I'}$ where $I' = I\beta$

First idea:

- Assume N_I smooth

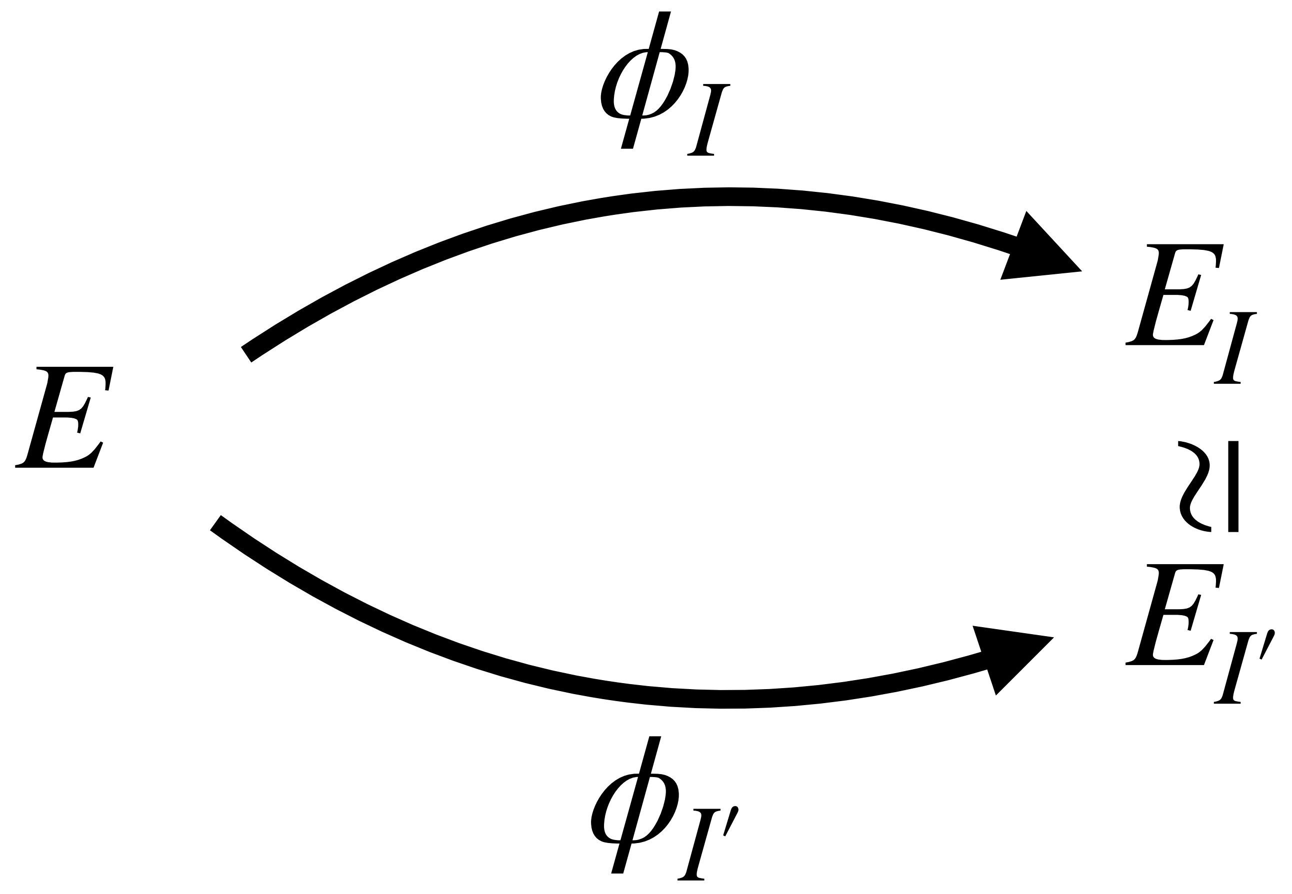


$I = \langle N, \alpha \rangle$

Some preliminaries

ϕ_I is **defined by** $\ker \phi_I = \{P \in E \mid \beta(P) = 0, \forall \beta \in I\}$
$= E[N] \cap \ker \alpha$

We are free to replace ϕ_I by $\phi_{I'}$ where $I' = I\beta$



First idea:

- Assume N_I smooth
- Recover $\ker \phi_I$

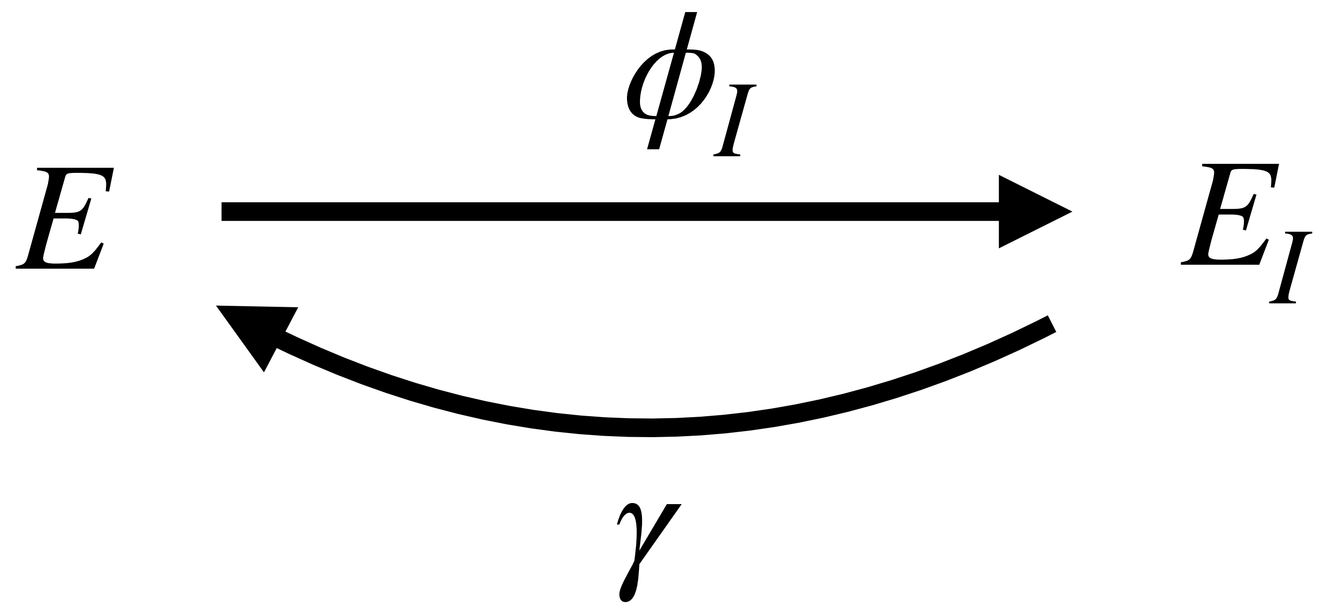
$I = \langle N, \alpha \rangle$

"Recover $\ker \phi_I$"

$$E \xrightarrow{\ \phi_I\ } E_I$$

$I = \langle N, \alpha \rangle$

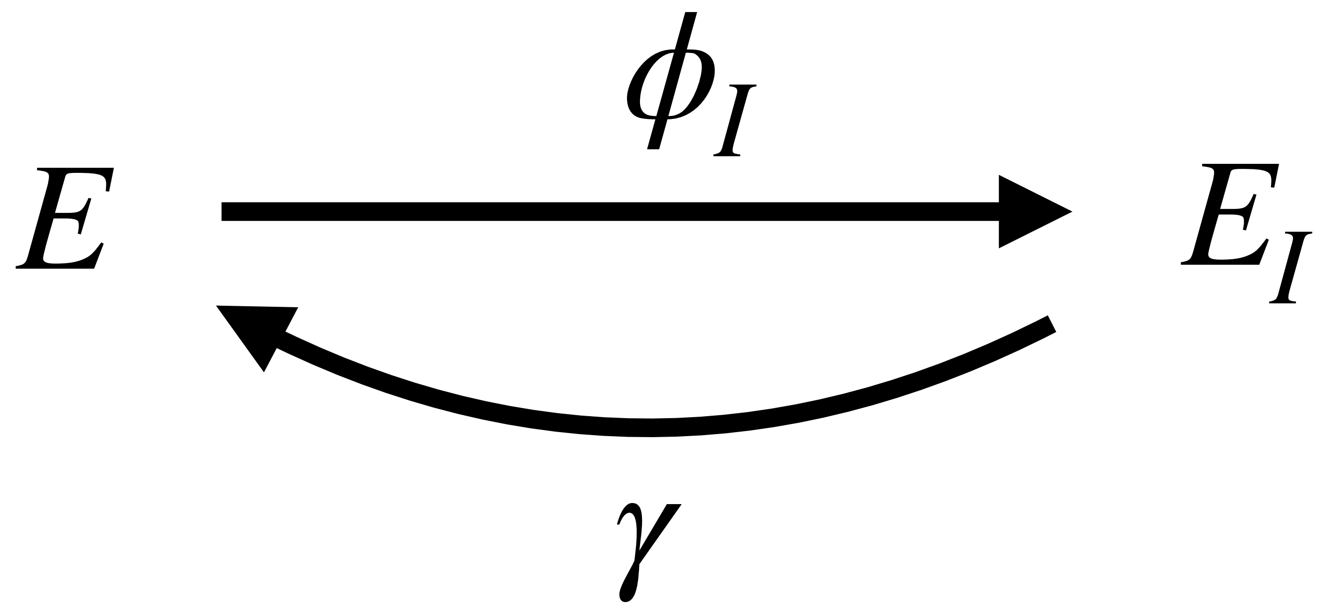
"Recover $\ker \phi_I$"



$\alpha = \gamma \circ \phi_I$

$I = \langle N, \alpha \rangle$

"Recover $\ker \phi_I$"



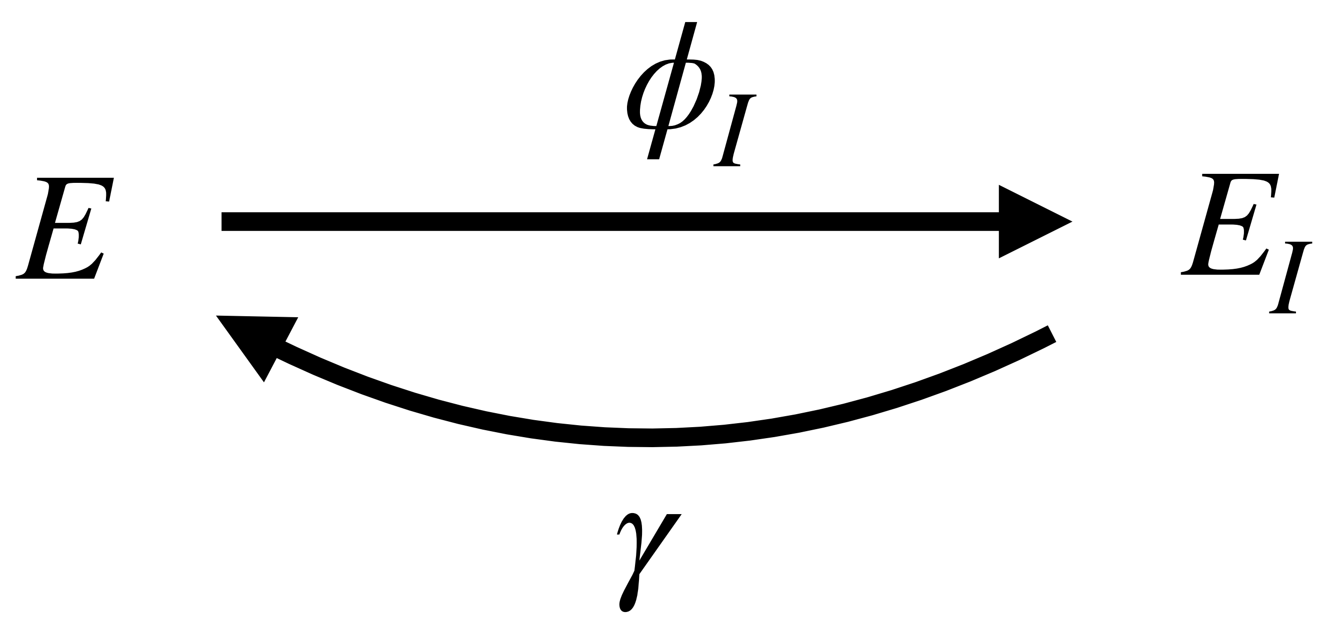
$\alpha = \gamma \circ \phi_I$

Idea: Project $E_I[N]$ onto $\ker \phi_I$

$$\ker \phi_I = \{ \widehat{\phi_I}(P) \mid P \in E_I[N] \}$$

$I = \langle N, \alpha \rangle$

"Recover $\ker \phi_I$"



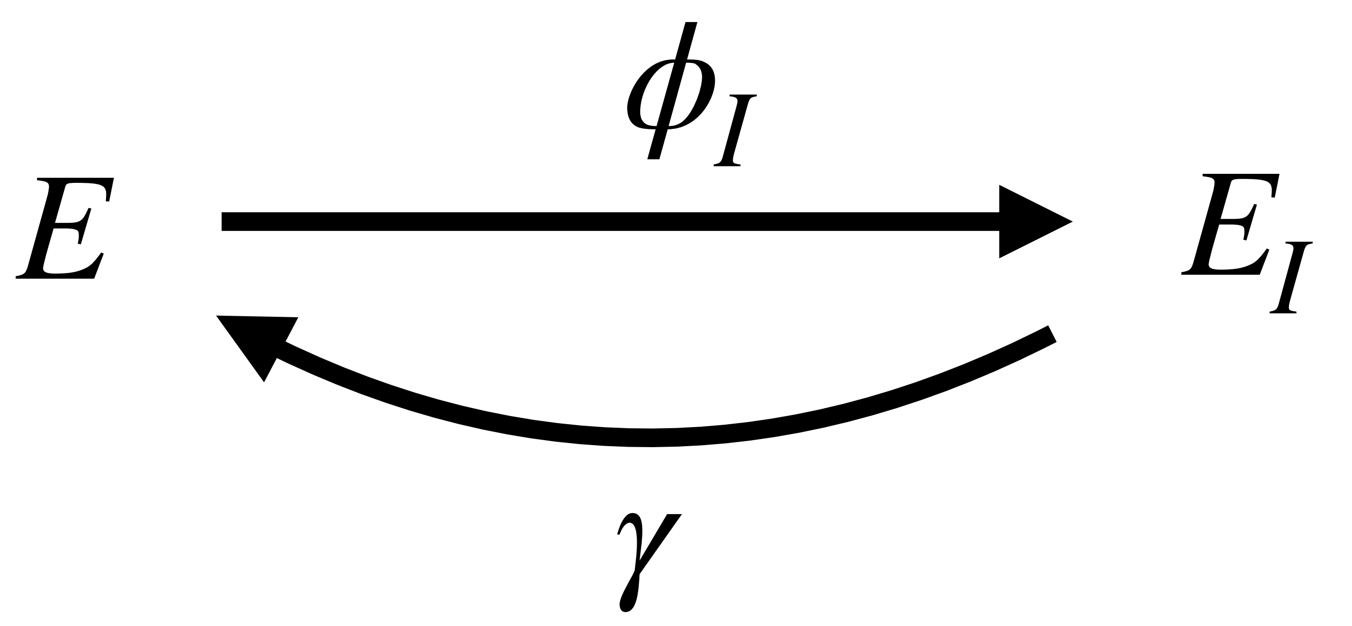
$\alpha = \gamma \circ \phi_I$

Idea: Project $E_I[N]$ onto $\ker \phi_I$

$$
\begin{aligned}
\ker \phi_I &= \{ \widehat{\phi_I}(P) \mid P \in E_I[N] \} \\
&= \{ \widehat{\phi_I}(\hat{\gamma}(P)) \mid P \in E[N] \}
\end{aligned}
$$

$I = \langle N, \alpha \rangle$

"Recover $\ker \phi_I$"



$\alpha = \gamma \circ \phi_I$

Idea: Project $E_I[N]$ onto $\ker \phi_I$

$$
\begin{aligned}
\ker \phi_I &= \{ \widehat{\phi_I}(P) \mid P \in E_I[N] \} \\
&= \{ \widehat{\phi_I}(\hat{\gamma}(P)) \mid P \in E[N] \} \\
&= \{ \hat{\alpha}(P) \mid P \in E[N] \}
\end{aligned}
$$

"Often" enough to take a single point of order N

"Assume N_I smooth", i.e. find $I' \sim I$ with smooth norm

O quadratic	O quaternionic

"Assume N_I smooth", i.e. find $I' \sim I$ with smooth norm

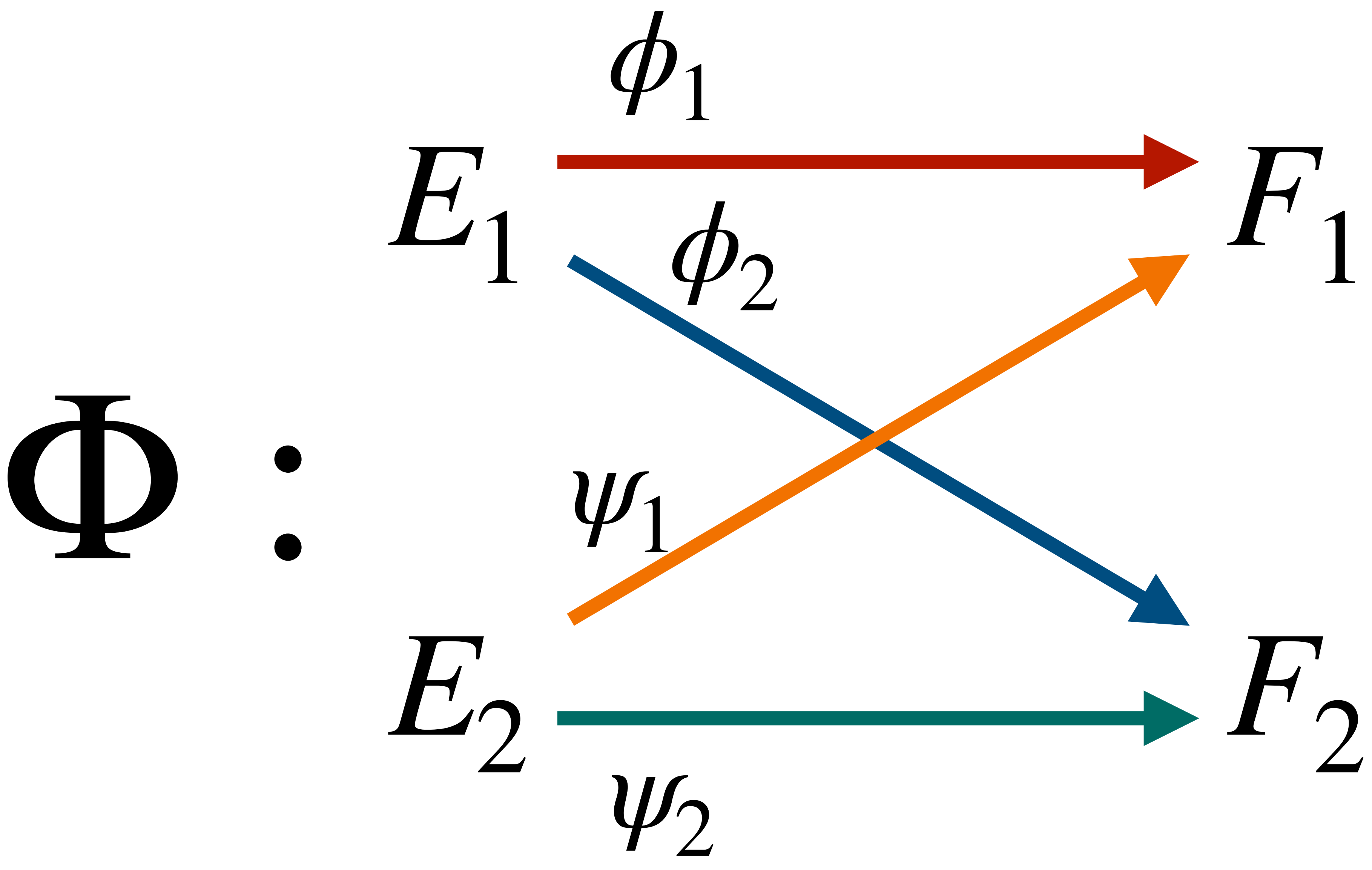
O quadratic	O quaternionic
No polynomial time algorithm in general :((	

"Assume N_I smooth", i.e. find $I' \sim I$ with smooth norm

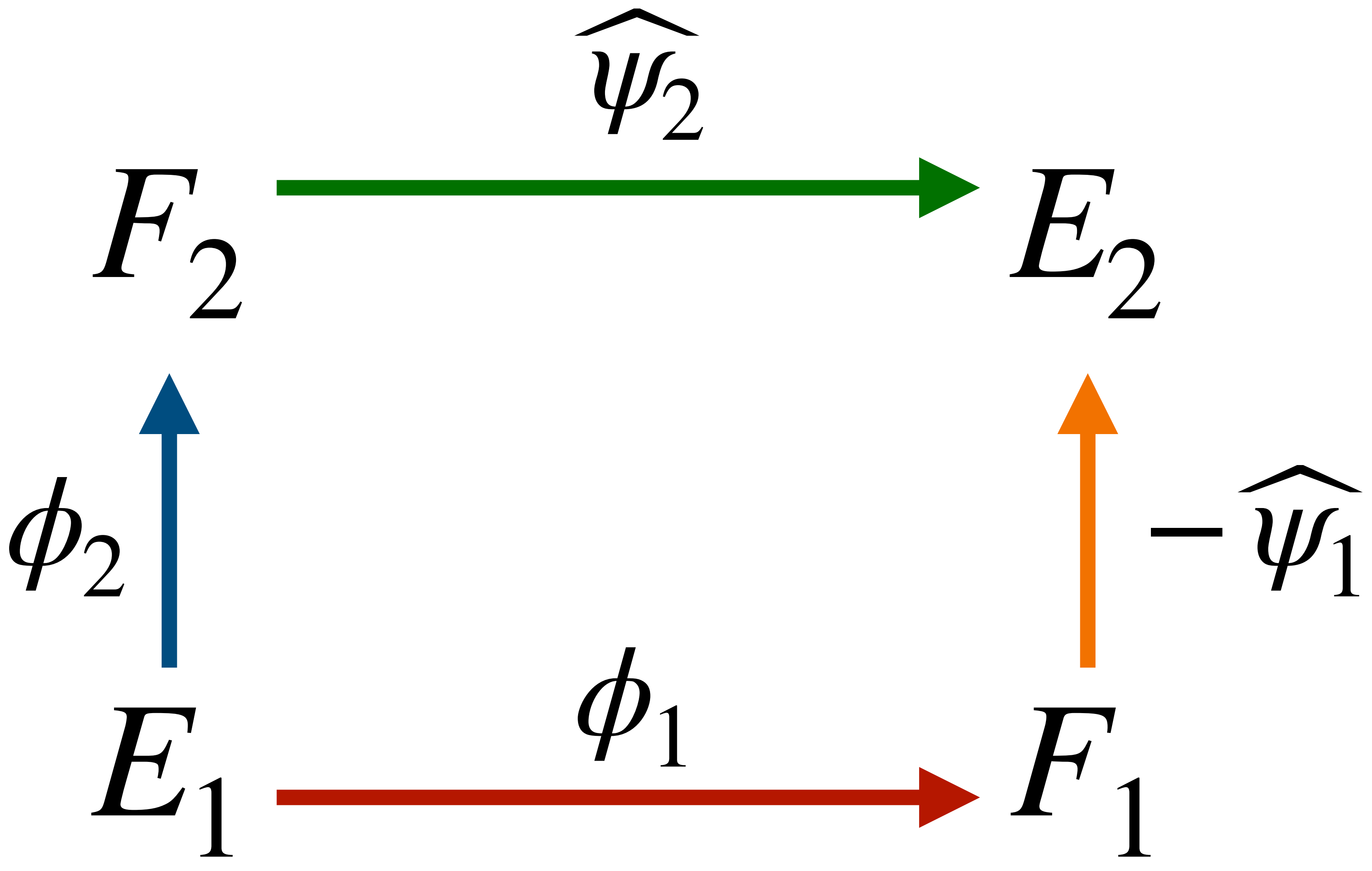
<table>
<tr><th rowspan="2">O quadratic</th><th colspan="2">O quaternionic</th></tr>
<tr><td>$O = \mathcal{O}_0$</td><td>$O \neq \mathcal{O}_0$</td></tr>
<tr><td>No polynomial time algorithm in general :((</td><td></td><td></td></tr>
</table>

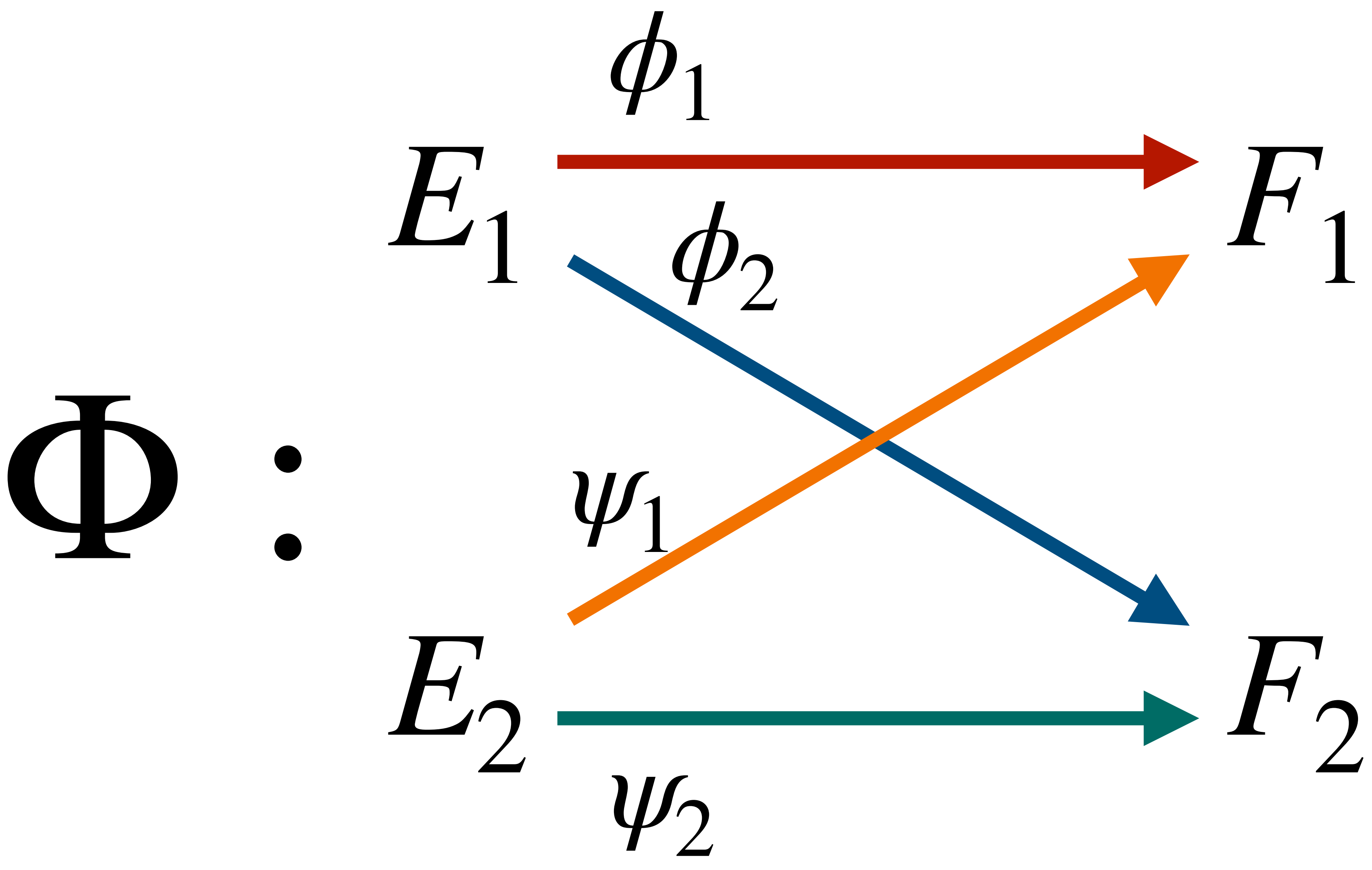
"Assume N_I smooth", i.e. find $I' \sim I$ with smooth norm

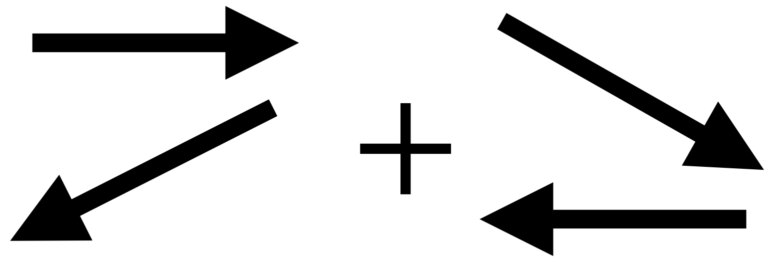
<table>
<tr><th colspan="1">O quadratic</th><th colspan="2">O quaternionic</th></tr>
<tr><td rowspan="2">No polynomial time algorithm in general :((</td><td>$O = \mathcal{O}_0$</td><td>$O \neq \mathcal{O}_0$</td></tr>
<tr><td>KLPT
- Issue: Output size $N_I > p^3$</td><td></td></tr>
</table>


Φ :
E1
E2
F1
F2
ϕ1
ϕ2
ψ1
ψ2

F_2
$\widehat{\psi_2}$
E_2
ϕ_2
$-\widehat{\psi_1}$
E_1
ϕ_1
F_1
$\Phi :$
E_1
ϕ_1
F_1
ϕ_2
ψ_1
E_2
F_2
ψ_2

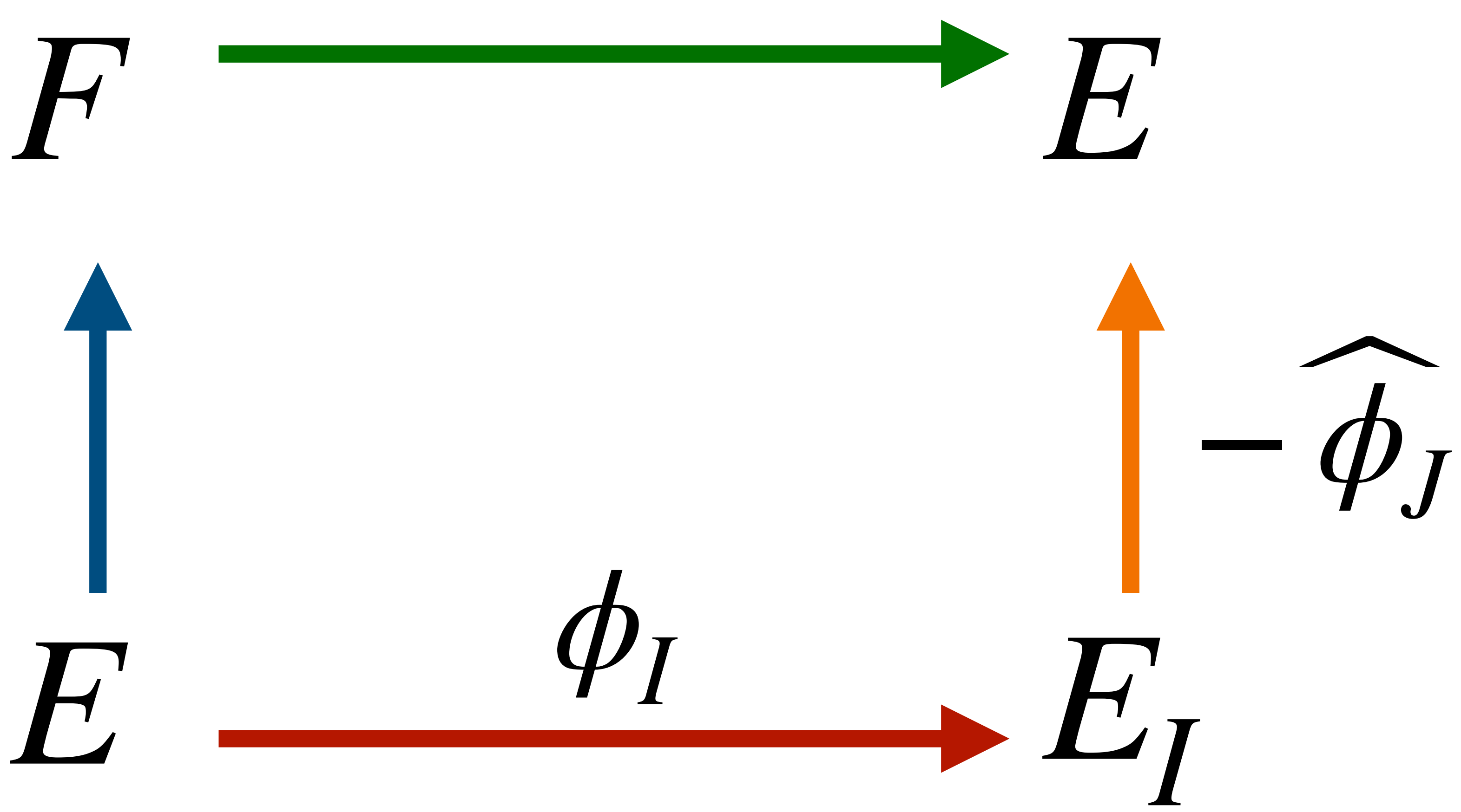


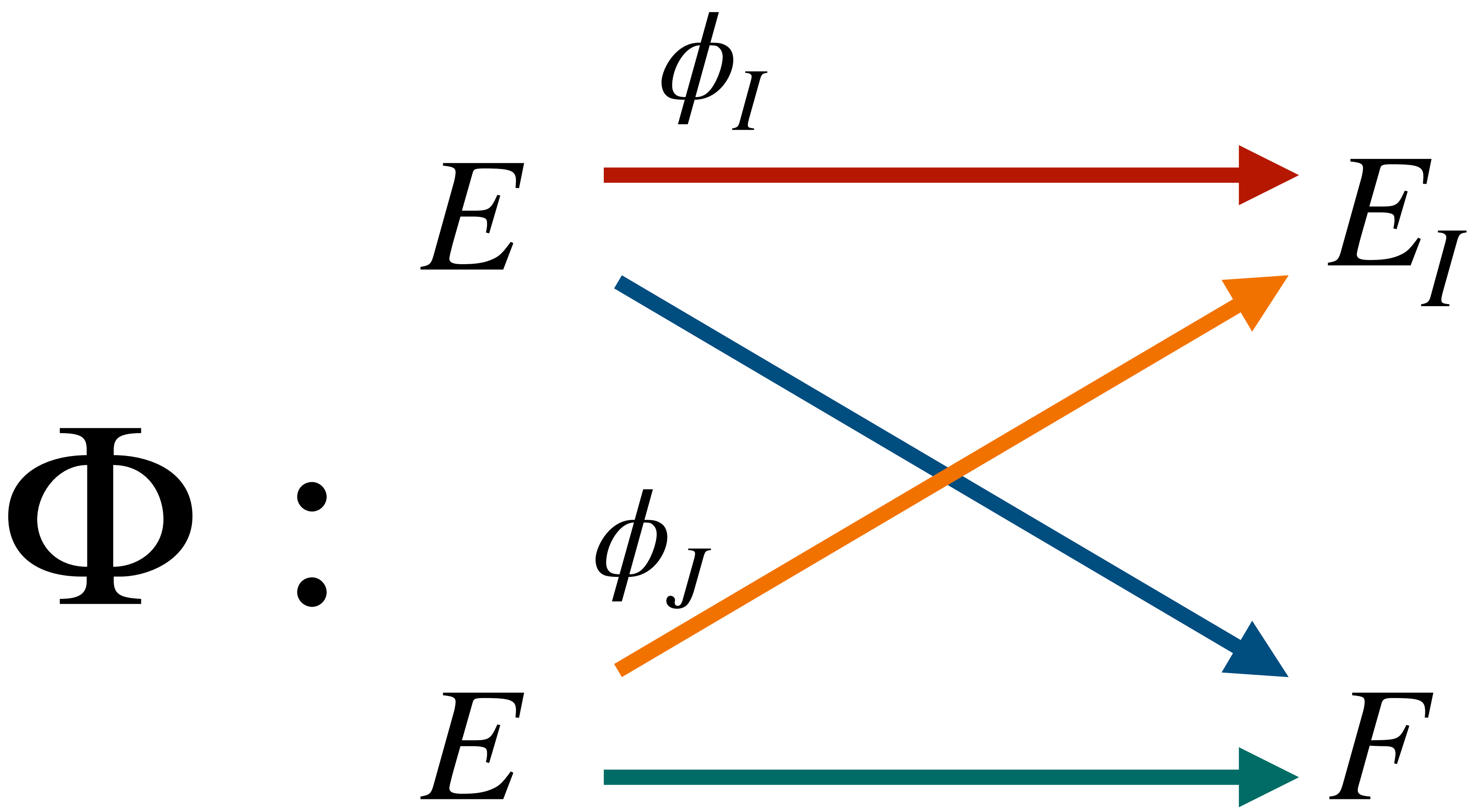


Kani's lemma implies that if  = trivial (and assumption on degrees)

then Φ is a (N, N)-isogeny (wrt. the product polarisation)

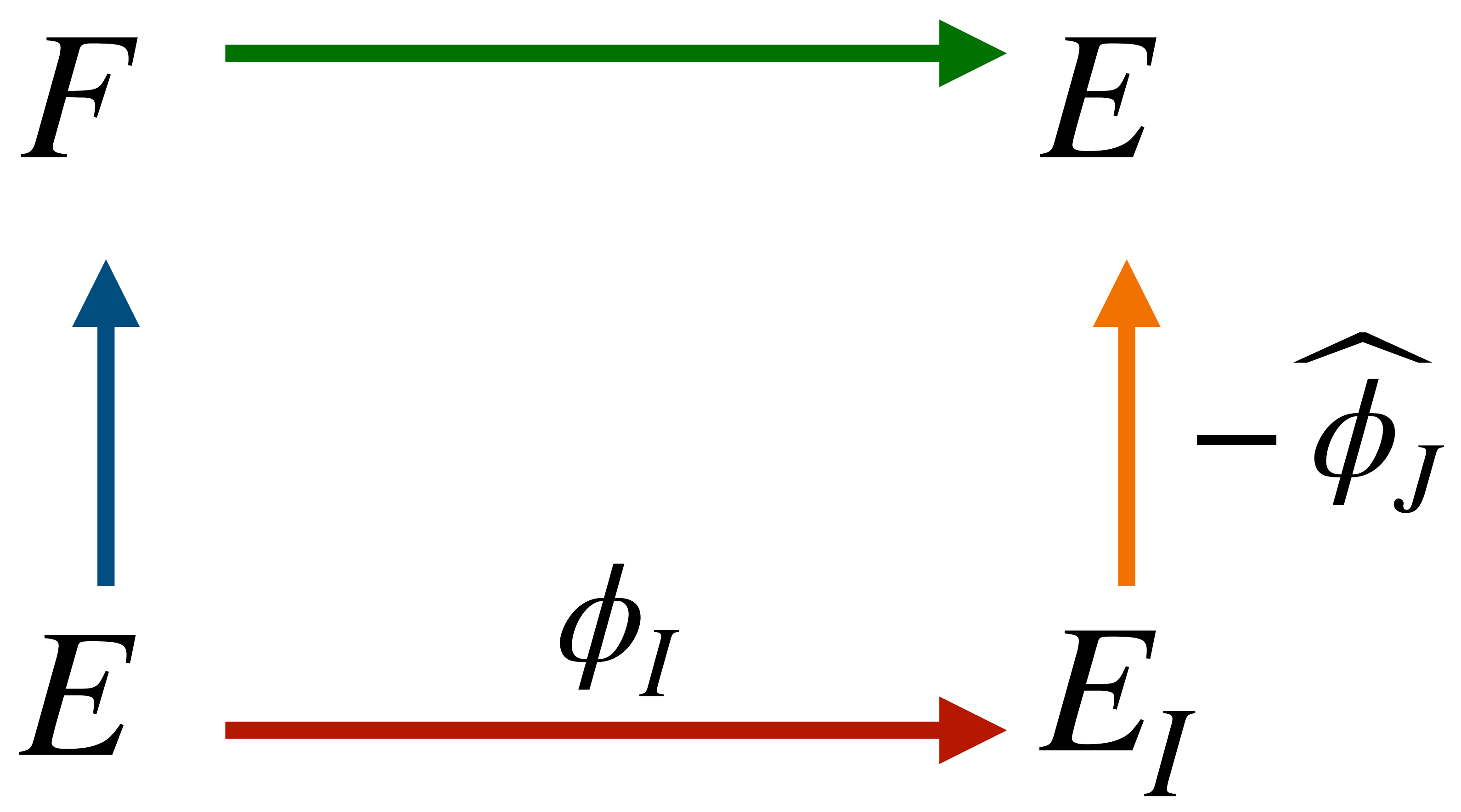
$$N = \deg \phi_1 + \deg \phi_2$$

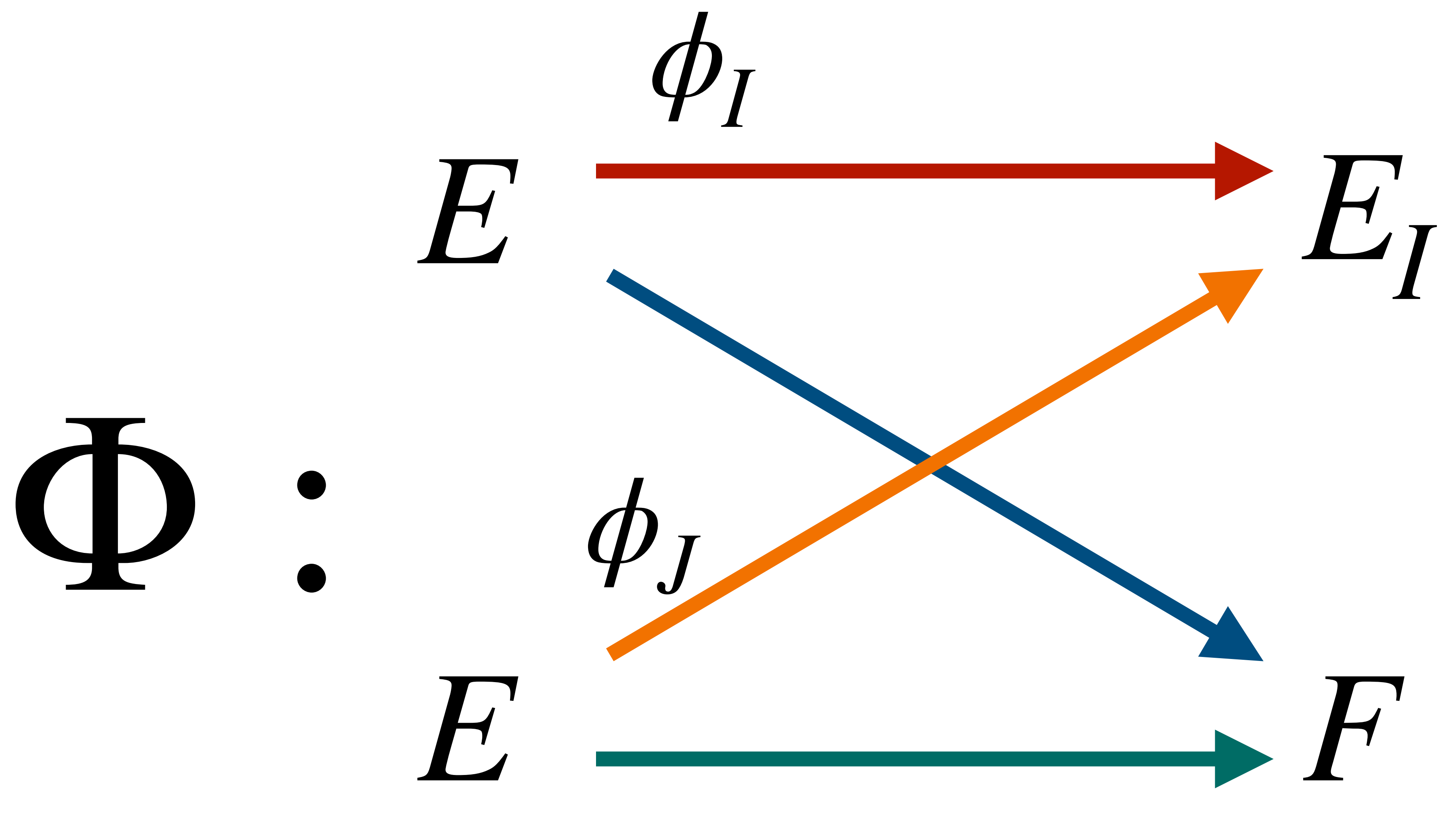




New idea:

- Assume $I \sim J$ with $\mathrm{nrd}(I) + \mathrm{nrd}(J) = 2^e$
- Recover $\ker \Phi$

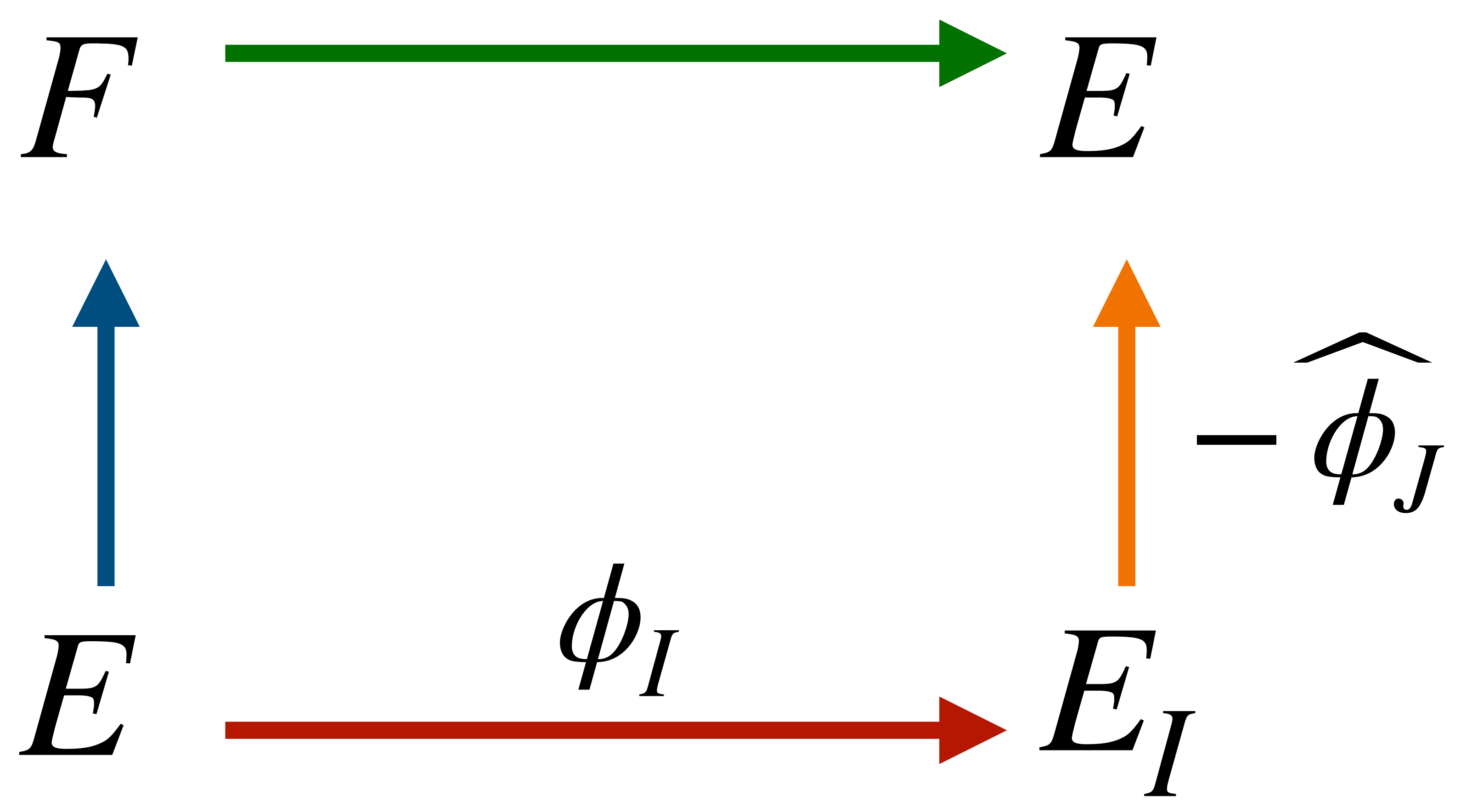


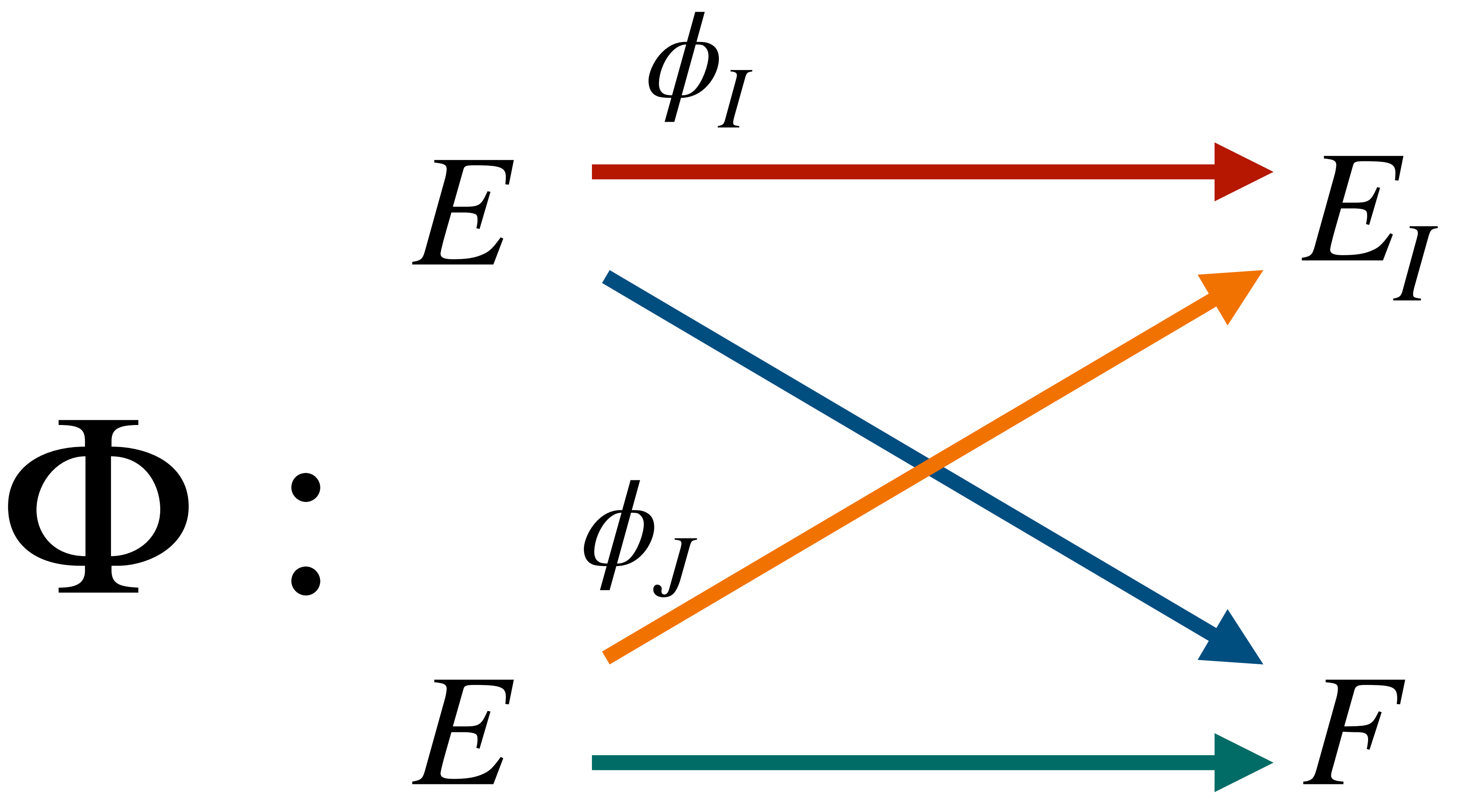


$$\ker\Phi = \{(\widehat{\phi_I}(P), \widehat{\phi_J}(Q)) \mid P, Q \in E_I[2^e]\}$$

New idea:

- Assume $I \sim J$ with $\mathrm{nrd}(I) + \mathrm{nrd}(J) = 2^e$
- Recover $\ker\Phi$

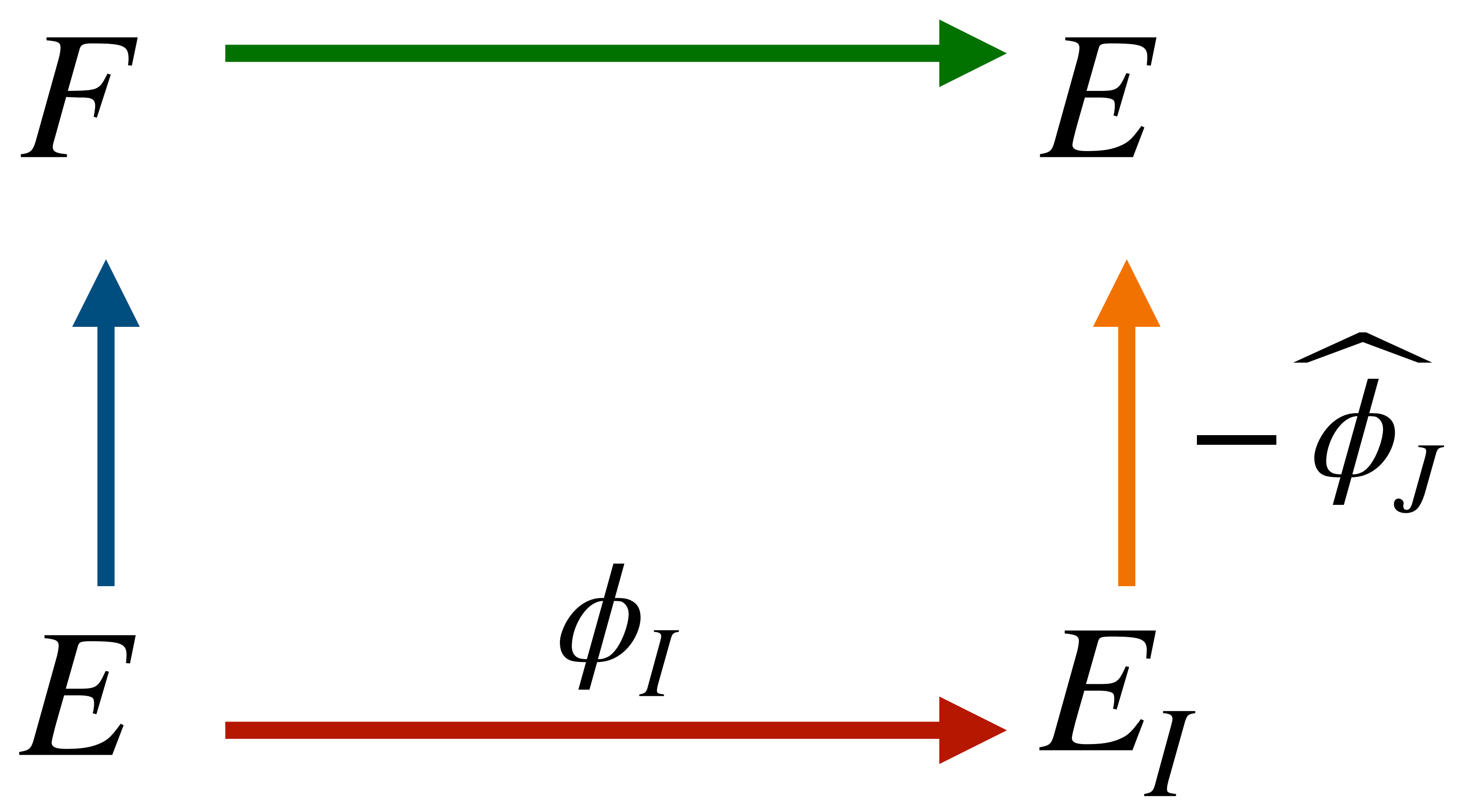


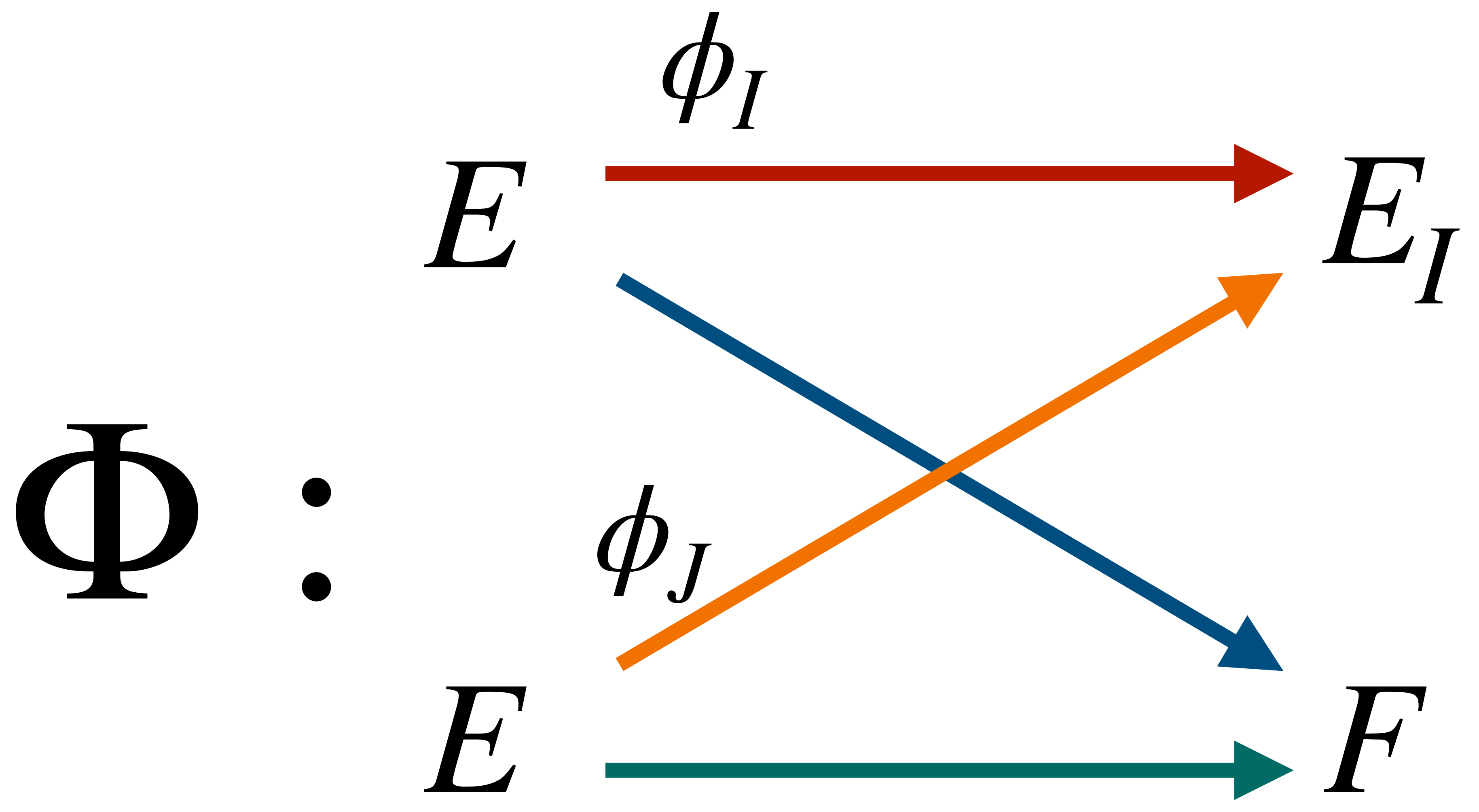


$$\ker \Phi = \{(\widehat{\phi_I}(P), \widehat{\phi_J}(Q)) \mid P, Q \in E_I[2^e]\}$$
$$= \{(\phi_I \circ \widehat{\phi_I}(P), \phi_I \circ \widehat{\phi_J}(Q)) \mid P, Q \in E[2^e]\}$$

New idea:

- Assume $I \sim J$ with $\mathrm{nrd}(I) + \mathrm{nrd}(J) = 2^e$
- Recover $\ker \Phi$





$$
\begin{aligned}
\ker \Phi &= \{(\widehat{\phi_I}(P), \widehat{\phi_J}(Q)) \mid P, Q \in E_I[2^e]\} \\
&= \{(\phi_I \circ \widehat{\phi_I}(P), \phi_I \circ \widehat{\phi_J}(Q)) \mid P, Q \in E[2^e]\} \\
&= \{([N_I]P, \gamma(Q)) \mid P, Q \in E[2^e]\}
\end{aligned}
$$

New idea:

- Assume $I \sim J$ with $\mathrm{nrd}(I) + \mathrm{nrd}(J) = 2^e$
- Recover $\ker \Phi$

"Assume $I \sim J$ with $\mathrm{nrd}(I) + \mathrm{nrd}(J) = 2^e$"

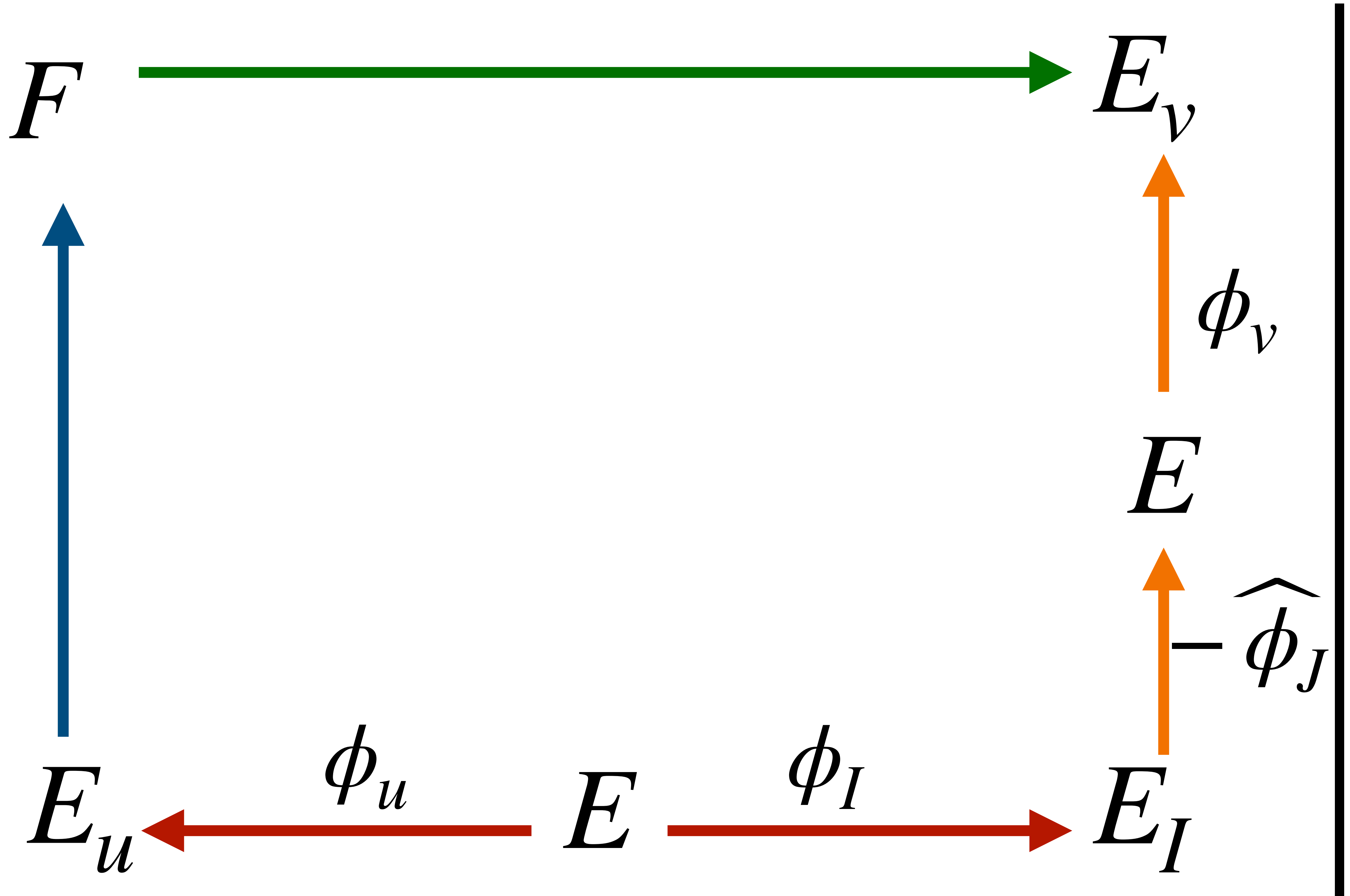
$\mathcal{O}$ quadratic	$\mathcal{O}$ quaternionic
KLaPoTi: this is an KLPT instance!	Brainstorm?

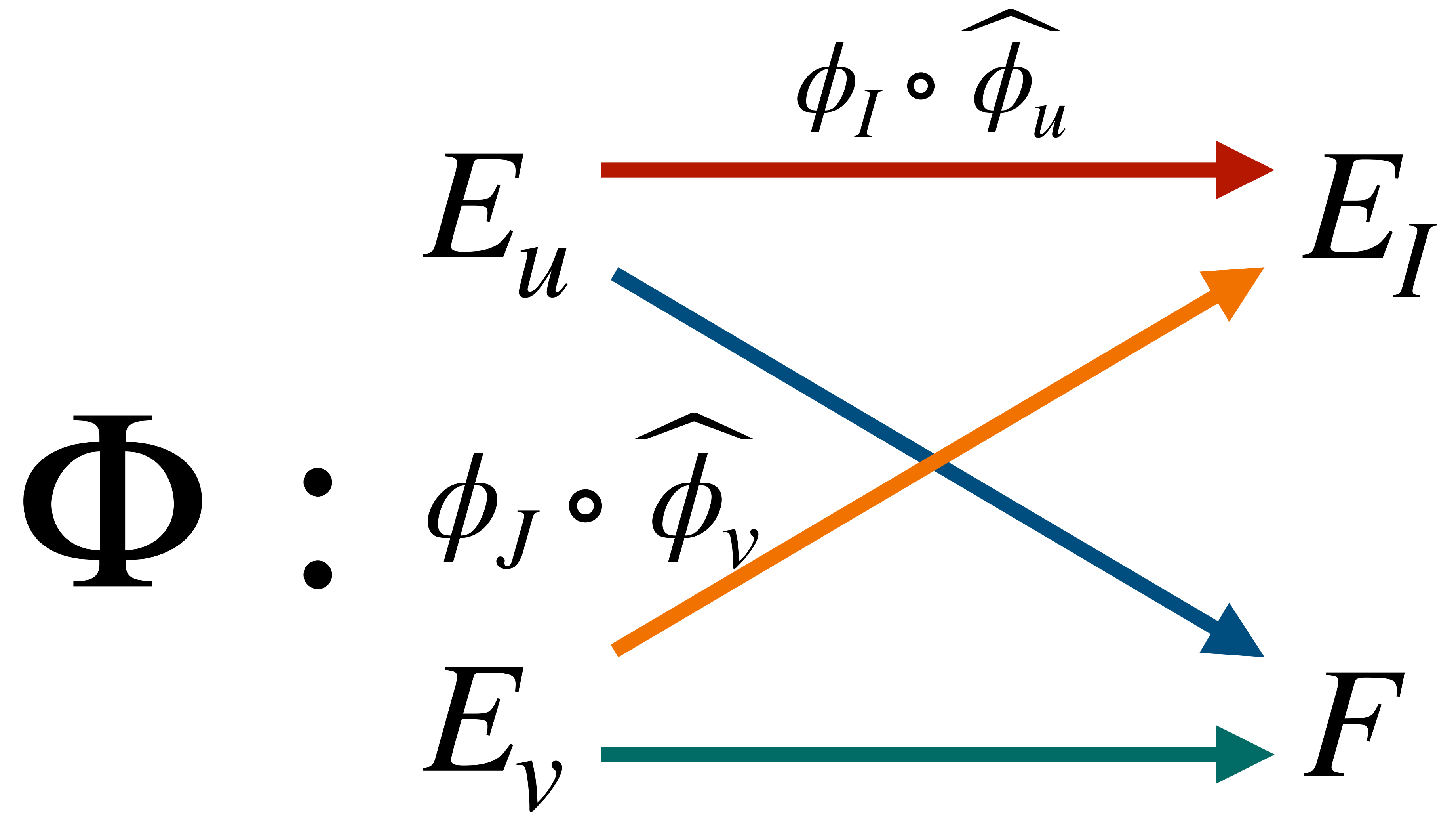
"Assume $I \sim J$ with $\mathrm{nrd}(I) + \mathrm{nrd}(J) = 2^e$"

$\mathcal{O}$ quadratic	$\mathcal{O}$ quaternionic
KLaPoTi: this is an KLPT instance!	Brainstorm?

New idea:

- Assume $I \sim J$ and $u, v \in \mathbb{N}$ with $uN_I + vN_J = 2^e$
- Recover $\ker \Phi$





$$\ker \Phi = \{(\widehat{\phi_u}([N_I]P), \widehat{\phi_v}(\gamma(Q))) \mid P, Q \in E[2^e]\}$$

New idea:

- Assume $I \sim J$ and $u, v \in \mathbb{N}$ with $uN_I + vN_J = 2^e$
- Recover $\ker \Phi$

$$\ker \Phi = \{(\widehat{\phi_u}([N_I]P), \widehat{\phi_v}(\gamma(Q))) \mid P, Q \in E[2^e]\}$$

Requires computing **random** isogenies of prescribed degree u, v

New idea:

- Assume $I \sim J$ and $u, v \in \mathbb{N}$ with $uN_I + vN_J = 2^e$
- Recover $\ker \Phi$

"Computing **random** isogenies of prescribed degree u, v"

O quadratic	O quaternionic	
	$O = \mathcal{O}_0$	

"Computing **random** isogenies of prescribed degree u, v"

O quadratic	O quaternionic	
Ref. Pierrick's talk:	$O = \mathcal{O}_0$	
Restrictions on u, v, ϕ_u, ϕ_v live in dimension 2		

"Computing **random** isogenies of prescribed degree u, v"

O quadratic	O quaternionic
Ref. Pierrick's talk:	$O = \mathcal{O}_0$
Restrictions on u, v, ϕ_u, ϕ_v live in dimension 2	- No restrictions on u, v, - find ϕ_u, ϕ_v dimension 1 - "QFESTA-trick"

"Assume $I \sim J$ and $u, v \in \mathbb{N}$ with $uN_I + vN_J = 2^e$"

Aaaaalmost enough: Take "smallest" norm $I, J \sim K$

Issue: Expect $N_I \approx N_J \approx \sqrt{p}$, while $2^e < p$

O quadratic	O quaternionic
	$O = \mathcal{O}_0$

"Assume $I \sim J$ and $u, v \in \mathbb{N}$ with $uN_I + vN_J = 2^e$"

Aaaaalmost enough: Take "smallest" norm $I, J \sim K$

Issue: Expect $N_I \approx N_J \approx \sqrt{p}$, while $2^e < p$

O quadratic	O quaternionic

Ref. Pierrick's talk:
- Rerandomization:
  - Replace K by KL for some easy to compute ϕ_L
  - **Essential:** $\mathrm{End}(E_L) = O$
	$O = \mathcal{O}_0$

"Assume $I \sim J$ and $u, v \in \mathbb{N}$ with $uN_I + vN_J = 2^e$"

Aaaaalmost enough: Take "smallest" norm $I, J \sim K$

Issue: Expect $N_I \approx N_J \approx \sqrt{p}$, while $2^e < p$

O quadratic

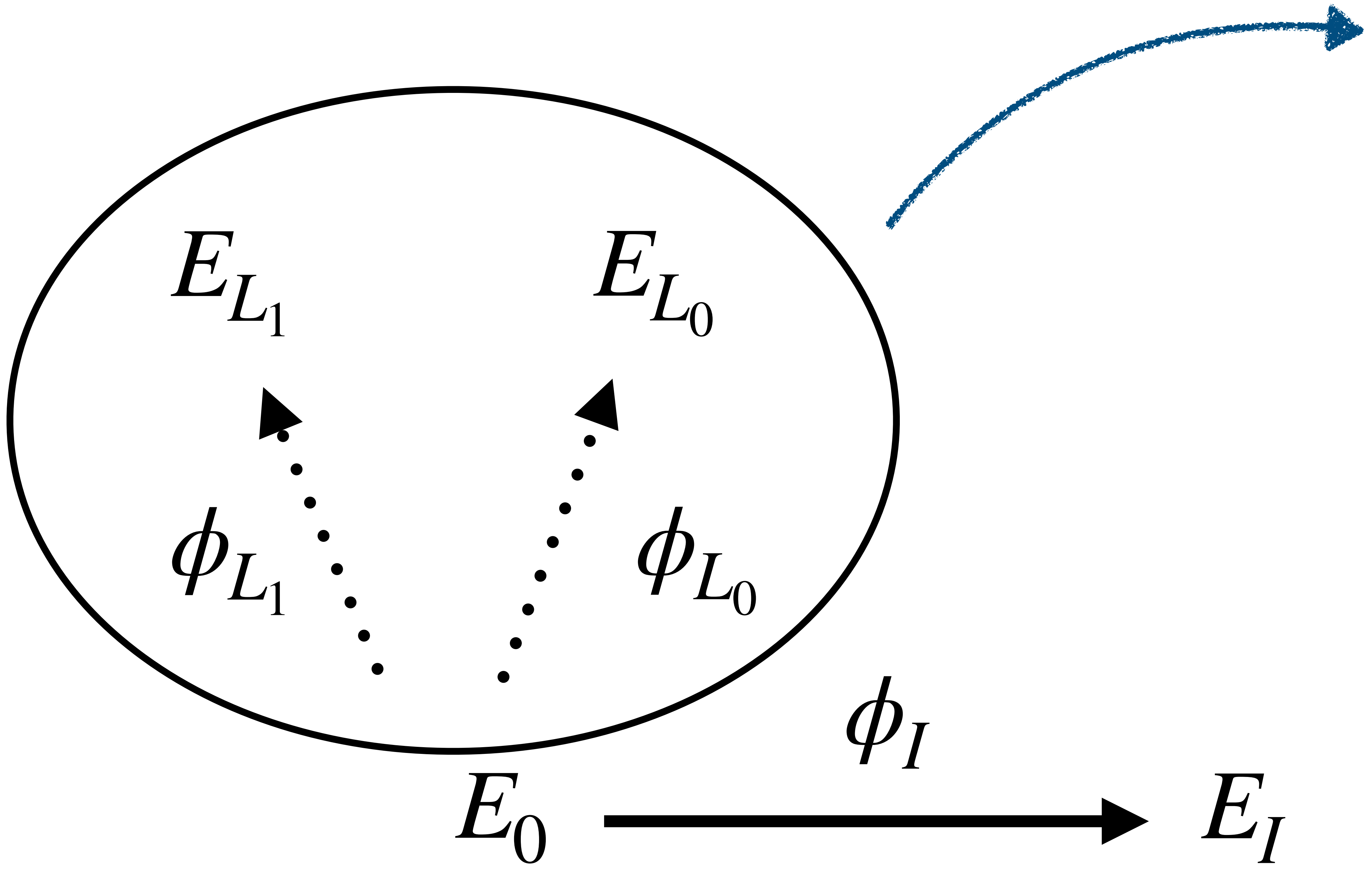
Ref. Pierrick's talk:

- Rerandomization:
  - Replace K by KL for some easy to compute ϕ_L
  - **Essential:** $\mathrm{End}(E_L) = O$

O quaternionic

$O = \mathcal{O}_0$

- Rerandomization:
  - **Issue:** $\mathrm{End}(E_L) \neq \mathcal{O}_0$



Precompute these isogenies with $\mathrm{End}(E_{L_i})$ "special p-extremal"

Rerandomization:

- Replace K with these specific KL_i

Open questions for quaternion case (relevant for SQIsign):

How to find $I \sim J$ with $\mathrm{nrd}(I) + \mathrm{nrd}(J) = 2^n$?

→ Probably difficult
Big efficiency gain if successful!

Apply tricks from PEGASIS to reduce failure probability/rerandomization

→ Will probably work
Maybe limited impact