Asymptotically Fast Arithmetic in the Picard Group of Algebraic Curves

Matthias Junge
University of Oldenburg

15. Mai 2017

Computeralgebra -Tagung Kassel

Goals and Achievements

- Reduce arithmetic in $\mathrm{Pic}^0(C)$ to linear algebra over $k[x]$ in
  - dimension n and
  - degree $O(g/n)$.

Goals and Achievements

- Reduce arithmetic in $\mathrm{Pic}^0(C)$ to linear algebra over $k[x]$ in
  - dimension n and
  - degree $O(g/n)$.
- Overall complexity:

$$O^{\sim}(n^{\omega-1}\, g)$$

Goals and Achievements

- Reduce arithmetic in $\mathrm{Pic}^0(C)$ to linear algebra over $k[x]$ in
  - dimension n and
  - degree $O(g/n)$.
- Overall complexity:

$$O^{\sim}(n^{\omega-1}\, g)$$

- Two main achievements:

Goals and Achievements

- Reduce arithmetic in $\mathrm{Pic}^0(C)$ to linear algebra over $k[x]$ in
  - dimension n and
  - degree $O(g/n)$.
- Overall complexity:

$$O^{\sim}(n^{\omega-1}\, g)$$

- Two main achievements:
  (1) Interpolate between best known running times (**regular** case)

Goals and Achievements

- Reduce arithmetic in $\mathrm{Pic}^0(C)$ to linear algebra over $k[x]$ in
  - dimension n and
  - degree $O(g/n)$.
- Overall complexity:

$$O^{\sim}(n^{\omega-1}\, g)$$

- Two main achievements:

  (1) Interpolate between best known running times (**regular** case)

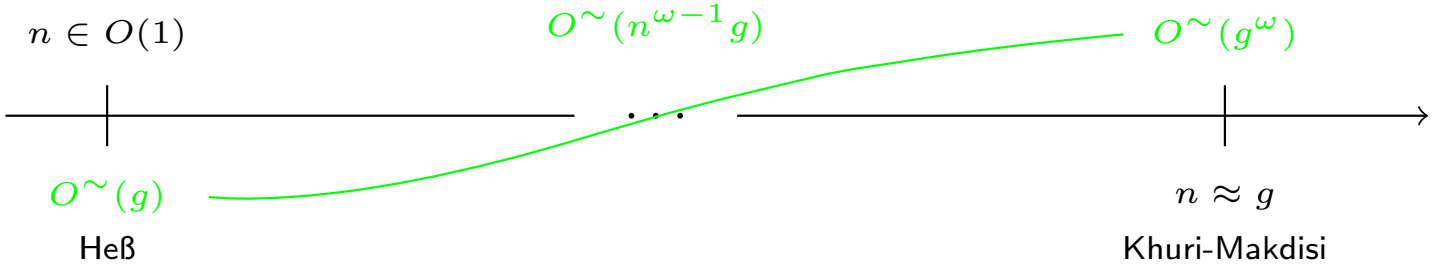
Goals and Achievements

- Reduce arithmetic in $\mathrm{Pic}^0(C)$ to linear algebra over $k[x]$ in
  - dimension n and
  - degree $O(g/n)$.
- Overall complexity:

$$O^{\sim}(n^{\omega-1}\, g)$$

- Two main achievements:

  (1) Interpolate between best known running times (**regular** case)



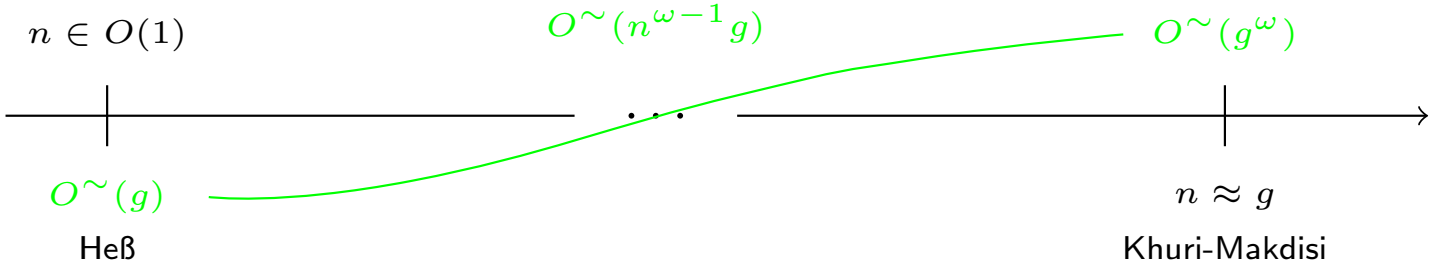
Goals and Achievements

- Reduce arithmetic in $\mathrm{Pic}^0(C)$ to linear algebra over $k[x]$ in
  - dimension n and
  - degree $O(g/n)$.
- Overall complexity:

$$O^{\sim}(n^{\omega-1}\, g)$$

- Two main achievements:

(1) Interpolate between best known running times (**regular** case)



(2) Generalize to the **singular** case where

there are **no results** until today!

$\mathrm{Pic}^0(C)$

- Object of interest:

$$\mathrm{Pic}^0(C) = \{\text{Degree zero invertible sheaves } \mathcal{F}\} \,/\, \cong$$

$\mathrm{Pic}^0(C)$

- Object of interest:

$$\mathrm{Pic}^0(C) = \{\text{Degree zero invertible sheaves } \mathcal{F}\} \,/\, \cong$$

  - is a group under tensor product of sheaves

$\mathrm{Pic}^0(C)$

- Object of interest:

$$\mathrm{Pic}^0(C) = \{\text{Degree zero invertible sheaves } \mathcal{F}\} \,/\, \cong$$

  - is a group under tensor product of sheaves
  - neutral element $\mathcal{O}_C$

$\mathrm{Pic}^0(C)$

- Object of interest:

$$\mathrm{Pic}^0(C) = \{\text{Degree zero invertible sheaves } \mathcal{F}\} \,/\, \cong$$

  - is a group under tensor product of sheaves
  - neutral element $\mathcal{O}_C$
- For concrete calculations (neither $\mathrm{DivCl}^0(C)$ nor) $\mathrm{Pic}^0(C)$ are very handy

$$\Rightarrow \text{Find new representation of } \mathrm{Pic}^0(C)!$$

$\mathrm{Pic}^0(C)$

- Object of interest:

$$\mathrm{Pic}^0(C) = \{\text{Degree zero invertible sheaves } \mathcal{F}\} \,/\, \cong$$

  - is a group under tensor product of sheaves
  - neutral element $\mathcal{O}_C$
- For concrete calculations (neither $\mathrm{DivCl}^0(C)$ nor) $\mathrm{Pic}^0(C)$ are very handy

$$\Rightarrow \text{Find new representation of } \mathrm{Pic}^0(C)!$$

- For this purpose: $\mathcal{F}$ is represented by its sections on open affines

$\mathrm{Pic}^0(C)$

- Object of interest:

$$\mathrm{Pic}^0(C) = \{\text{Degree zero invertible sheaves } \mathcal{F}\} \,/\, \cong$$

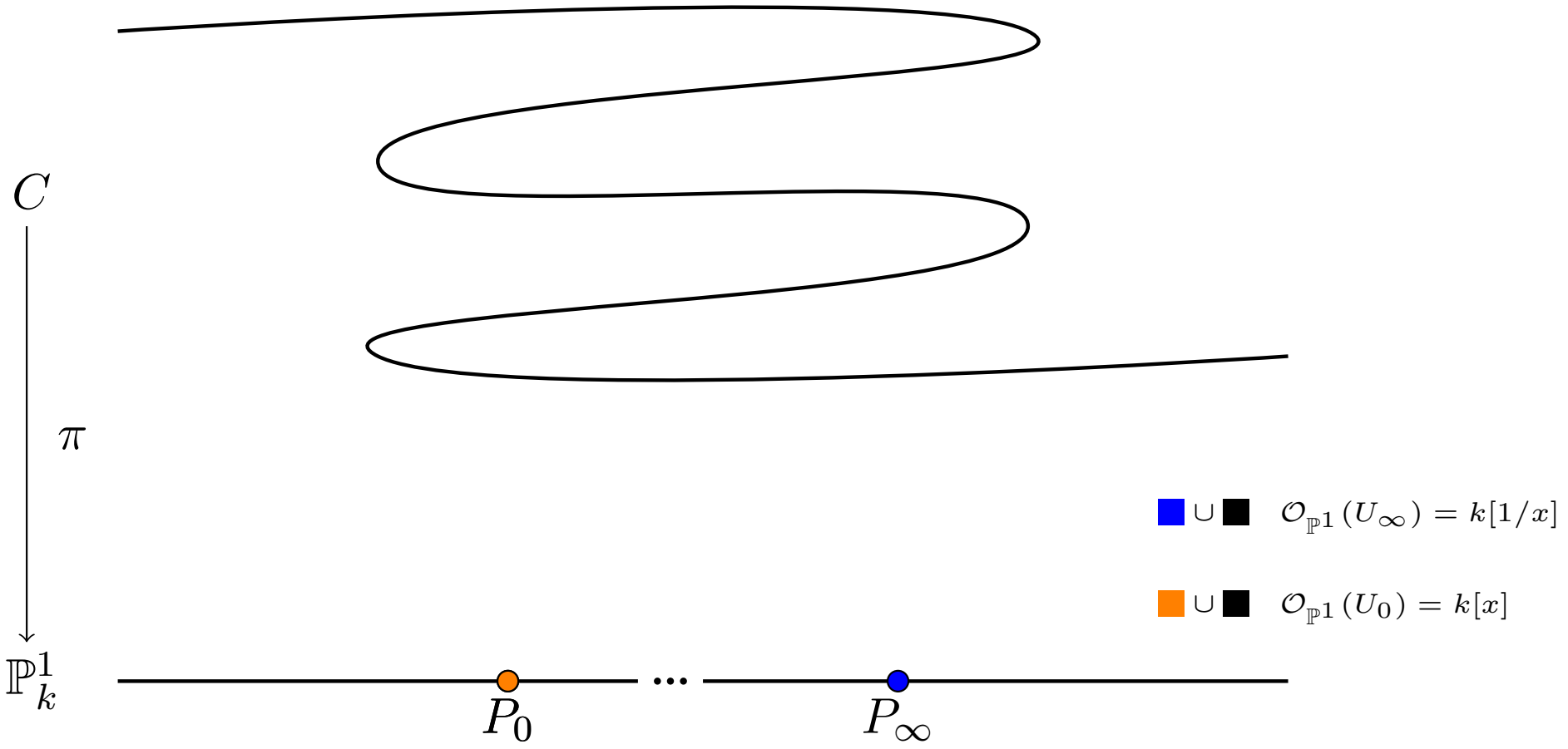
  - is a group under tensor product of sheaves
  - neutral element $\mathcal{O}_C$
- For concrete calculations (neither $\mathrm{DivCl}^0(C)$ nor) $\mathrm{Pic}^0(C)$ are very handy

$$\Rightarrow \text{Find new representation of } \mathrm{Pic}^0(C)!$$

- For this purpose: $\mathcal{F}$ is represented by its sections on open affines
- Those sections form invertible ideals of the coordinate rings

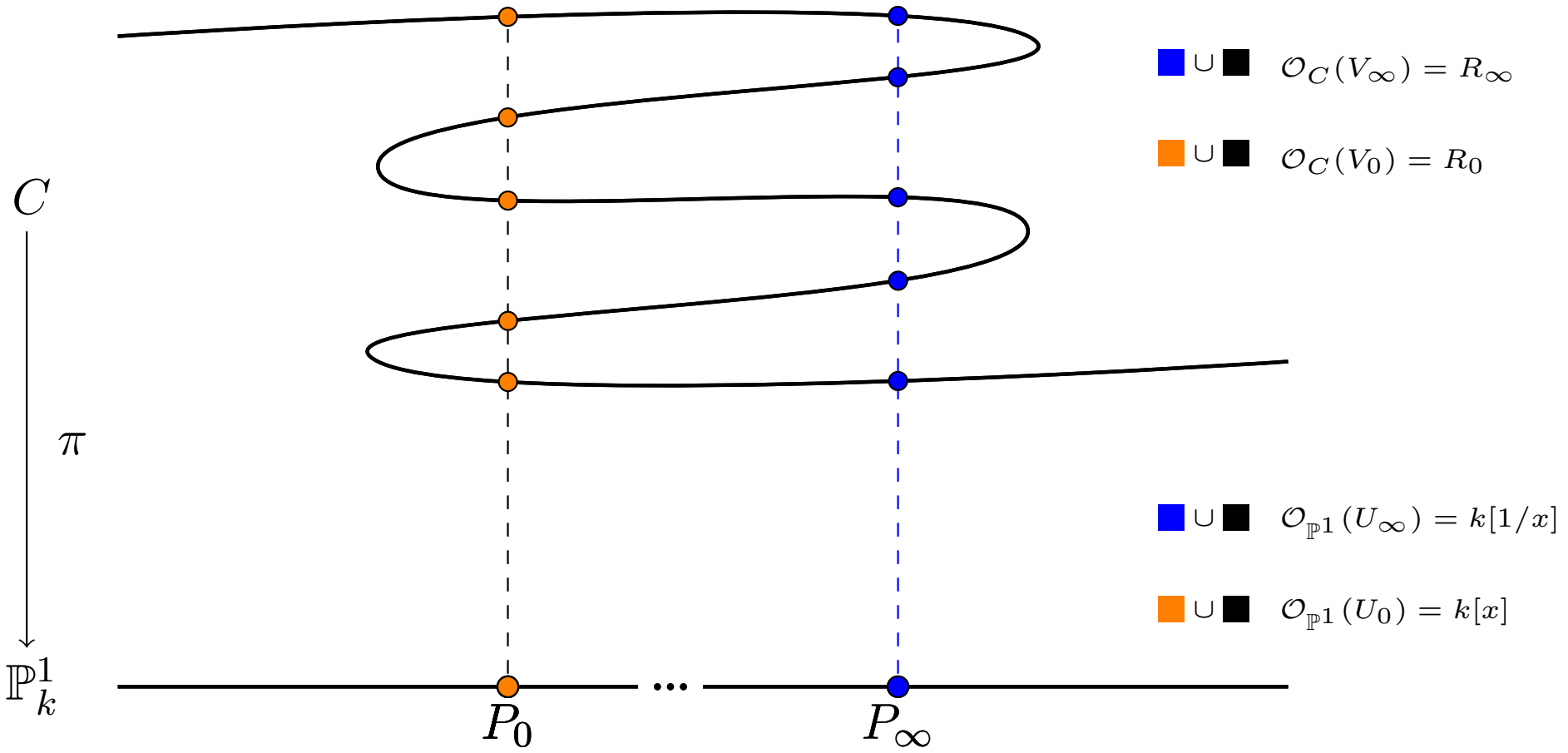
Setup

- C integral projective curve over the field k
- $\pi : C \to \mathbb{P}^1_k$ finite morphism of degree n which is separable



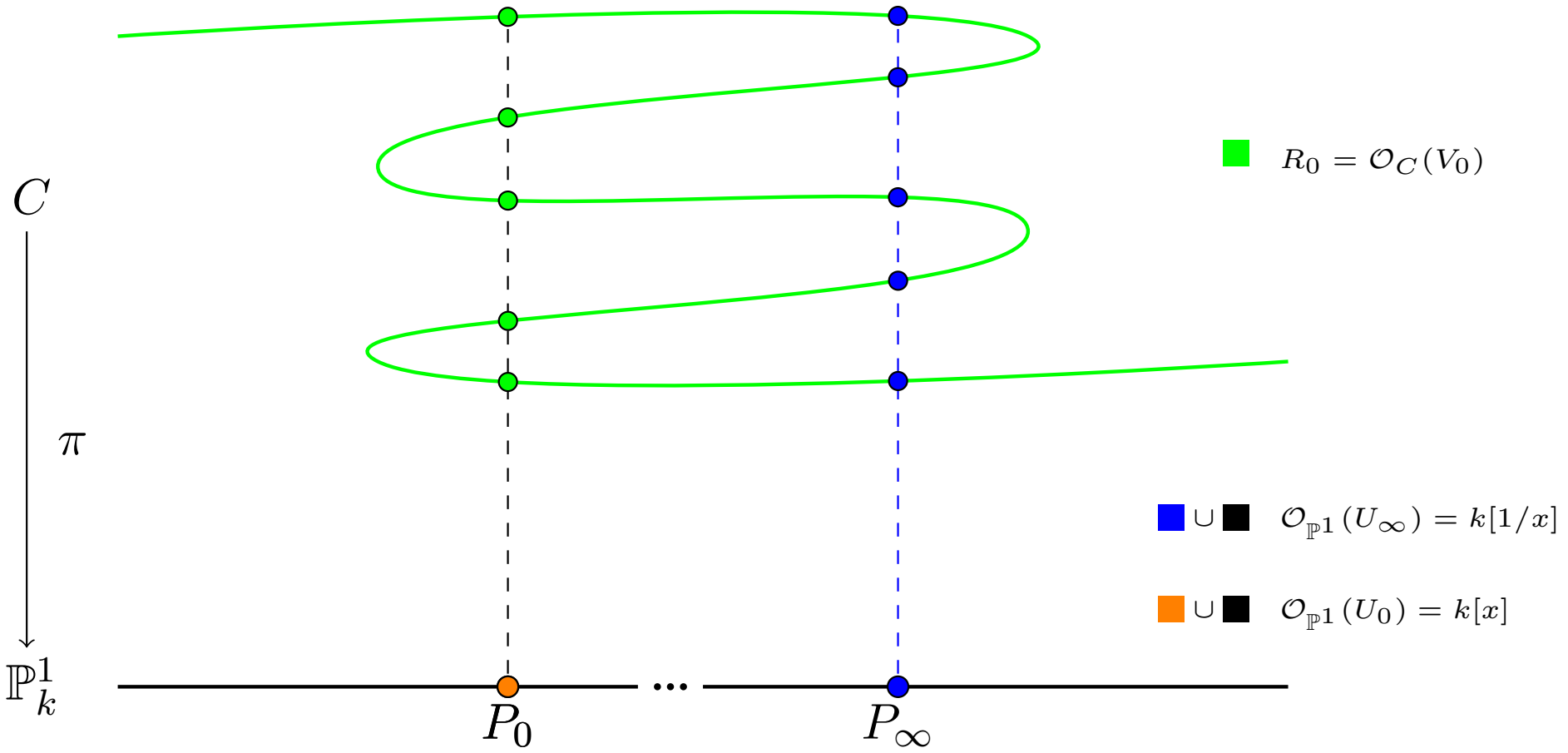
Setup

- C integral projective curve over the field k
- $\pi : C \to \mathbb{P}^1_k$ finite morphism of degree n which is separable



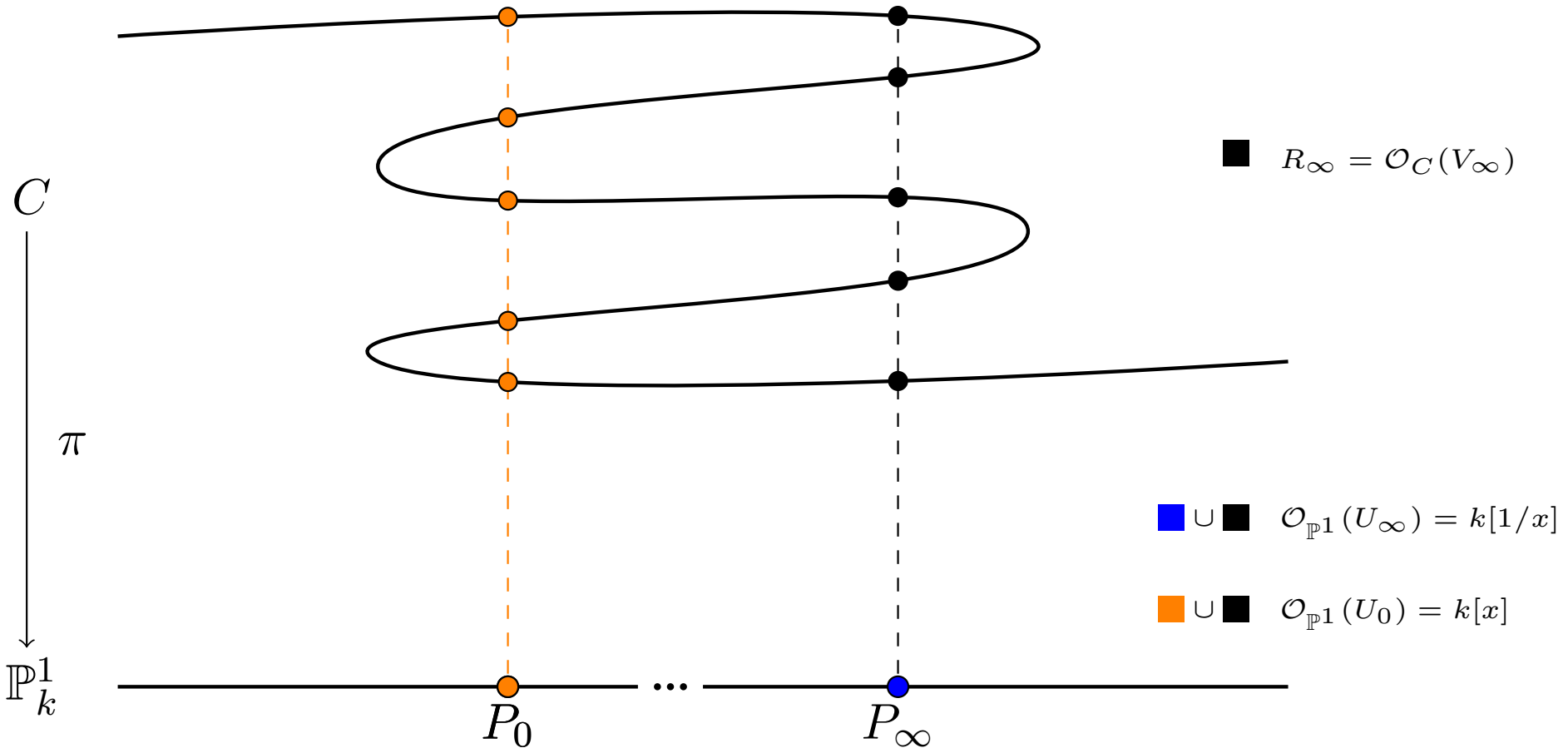
Setup

- C integral projective curve over the field k
- $\pi : C \to \mathbb{P}^1_k$ finite morphism of degree n which is separable



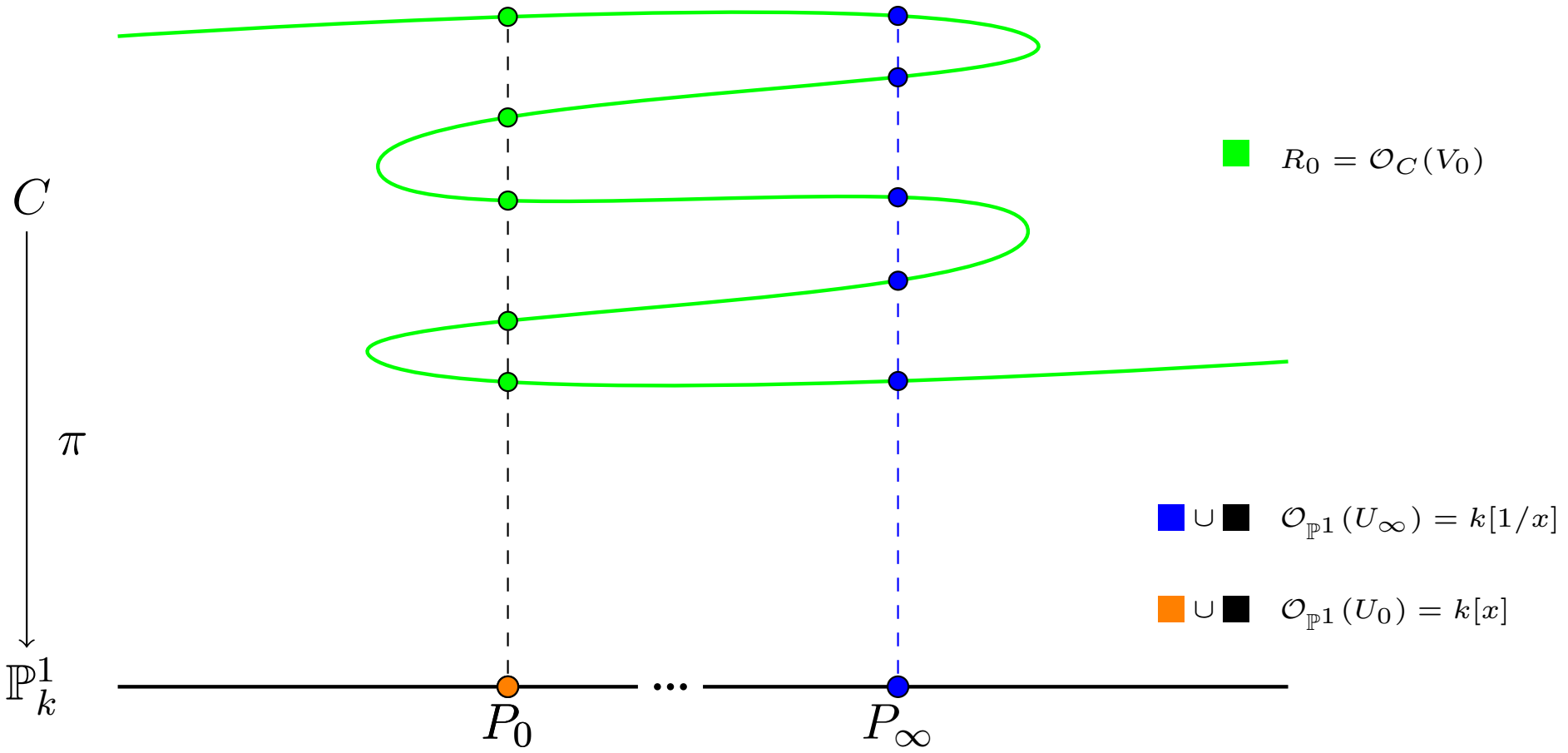
Setup

- C integral projective curve over the field k
- $\pi : C \to \mathbb{P}^1_k$ finite morphism of degree n which is separable



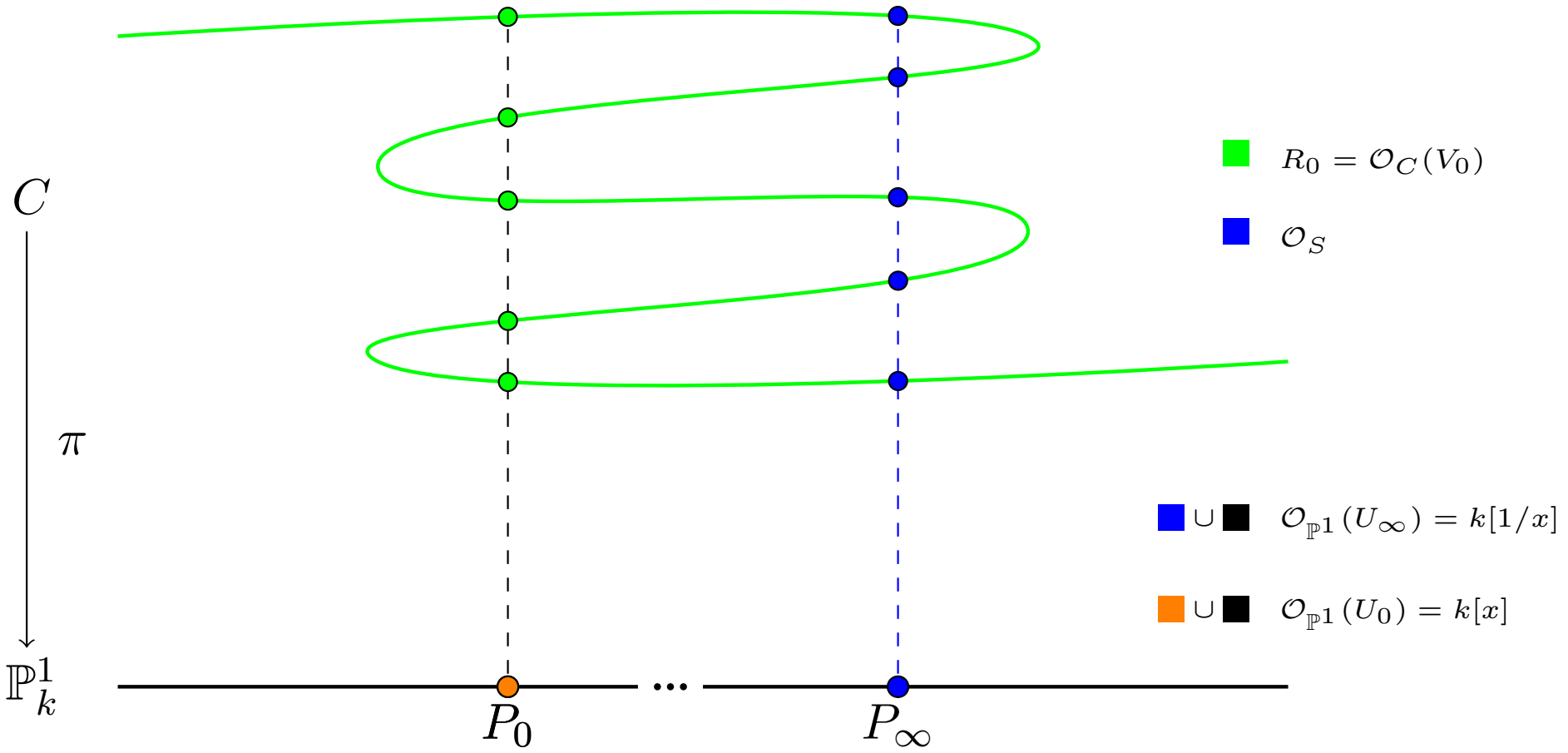
Setup

- C integral projective curve over the field k
- $\pi : C \to \mathbb{P}^1_k$ finite morphism of degree n which is separable



Setup

- C integral projective curve over the field k
- $\pi : C \to \mathbb{P}^1_k$ finite morphism of degree n which is separable



Construction of $\mathcal{F}(S)$:

- Natural morphism $g : \mathrm{Spec}(\mathcal{O}_S) \to C$

$\mathcal{F}(S)$

Construction of $\mathcal{F}(S)$:

- Natural morphism $g : \mathrm{Spec}(\mathcal{O}_S) \to C$
- $\mathcal{F}_{|S} := g^*\mathcal{F}$ is invertible sheaf on $\mathrm{Spec}(\mathcal{O}_S)$

$\mathcal{F}(S)$

Construction of $\mathcal{F}(S)$:

- Natural morphism $g : \mathrm{Spec}(\mathcal{O}_S) \to C$
- $\mathcal{F}_{|S} := g^*\mathcal{F}$ is invertible sheaf on $\mathrm{Spec}(\mathcal{O}_S)$
- $\mathcal{F}(S) := \mathcal{F}_{|S}(S)$ invertible ideal of $\mathcal{O}_S$

$\mathcal{F}(S)$

Construction of $\mathcal{F}(S)$:

- Natural morphism $g : \mathrm{Spec}(\mathcal{O}_S) \to C$
- $\mathcal{F}_{|S} := g^*\mathcal{F}$ is invertible sheaf on $\mathrm{Spec}(\mathcal{O}_S)$
- $\mathcal{F}(S) := \mathcal{F}_{|S}(S)$ invertible ideal of $\mathcal{O}_S$

„Information above P_∞“

- $S = \pi^{-1}\{P_\infty\}$

$\mathcal{F}(S)$

Construction of $\mathcal{F}(S)$:

- Natural morphism $g : \mathrm{Spec}(\mathcal{O}_S) \to C$
- $\mathcal{F}_{|S} := g^*\mathcal{F}$ is invertible sheaf on $\mathrm{Spec}(\mathcal{O}_S)$
- $\mathcal{F}(S) := \mathcal{F}_{|S}(S)$ invertible ideal of $\mathcal{O}_S$

„Information above P_∞“

- $S = \pi^{-1}\{P_\infty\}$
- $\mathcal{O}_S = \bigcap_{P \in S} \mathcal{O}_{C,P}$

$\mathcal{F}(S)$

Construction of $\mathcal{F}(S)$:

- Natural morphism $g : \mathrm{Spec}(\mathcal{O}_S) \to C$
- $\mathcal{F}_{|S} := g^*\mathcal{F}$ is invertible sheaf on $\mathrm{Spec}(\mathcal{O}_S)$
- $\mathcal{F}(S) := \mathcal{F}_{|S}(S)$ invertible ideal of $\mathcal{O}_S$

„Information above P_∞“

- $S = \pi^{-1}\{P_\infty\}$
- $\mathcal{O}_S = \bigcap_{P \in S} \mathcal{O}_{C,P}$
- $\mathcal{O}_S$ semi-local ring, i.e. I fractional ideal of $\mathcal{O}_S$, then

$$I \text{ invertible} \Leftrightarrow I \text{ principal}$$

$\mathcal{F}(S)$

Construction of $\mathcal{F}(S)$:

- Natural morphism $g : \mathrm{Spec}(\mathcal{O}_S) \to C$
- $\mathcal{F}_{|S} := g^*\mathcal{F}$ is invertible sheaf on $\mathrm{Spec}(\mathcal{O}_S)$
- $\mathcal{F}(S) = h\,\mathcal{O}_S$, $h \in k(C)$ invertible ideal of $\mathcal{O}_S$

„Information above P_∞“

- $S = \pi^{-1}\{P_\infty\}$
- $\mathcal{O}_S = \bigcap_{P \in S} \mathcal{O}_{C,P}$
- $\mathcal{O}_S$ semi-local ring, i.e. I fractional ideal of $\mathcal{O}_S$, then

$$I \text{ invertible} \Leftrightarrow I \text{ principal}$$

$\mathcal{F}(S)$

Construction of $\mathcal{F}(S)$:

- Natural morphism $g : \mathrm{Spec}(\mathcal{O}_S) \to C$
- $\mathcal{F}_{|S} := g^*\mathcal{F}$ is invertible sheaf on $\mathrm{Spec}(\mathcal{O}_S)$
- $\mathcal{F}(S) = h\,\mathcal{O}_S$, $h \in k(C)$ invertible ideal of $\mathcal{O}_S$

„Information above P_∞“

- $S = \pi^{-1}\{P_\infty\}$
- $\mathcal{O}_S = \bigcap_{P \in S} \mathcal{O}_{C,P}$
- $\mathcal{O}_S$ semi-local ring, i.e. I fractional ideal of $\mathcal{O}_S$, then

$$I \text{ invertible} \Leftrightarrow I \text{ principal}$$

$\mathcal{F}$ represented by $\mathcal{F}(V_0)$ and $\mathcal{F}(S)$

New $\mathrm{Pic}^0(C)$ Representation

- $\mathcal{I}_x = \{\text{Invertible Ideals } I \text{ of } R_0 \text{ with } \deg_k I \equiv 0 \bmod n\}$

New $\mathrm{Pic}^0(C)$ Representation

- $\mathcal{I}_x = \{\text{Invertible Ideals } I \text{ of } R_0 \text{ with } \deg_k I \equiv 0 \bmod n\}$
- $\mathcal{P}_x = \{\text{Principal Ideals } fR_0 \text{ with } f\mathcal{O}_S = x^r\mathcal{O}_S\} \trianglelefteq \mathcal{I}_x$

New $\mathrm{Pic}^0(C)$ Representation

- $\mathcal{I}_x = \{\text{Invertible Ideals } I \text{ of } R_0 \text{ with } \deg_k I \equiv 0 \bmod n\}$
- $\mathcal{P}_x = \{\text{Principal Ideals } fR_0 \text{ with } f\mathcal{O}_S = x^r\mathcal{O}_S\} \trianglelefteq \mathcal{I}_x$

Theorem

For all $[\mathcal{F}] \in \mathrm{Pic}^0(C)$ there exists $D \in \mathrm{Div}^0(C)$ s.t.

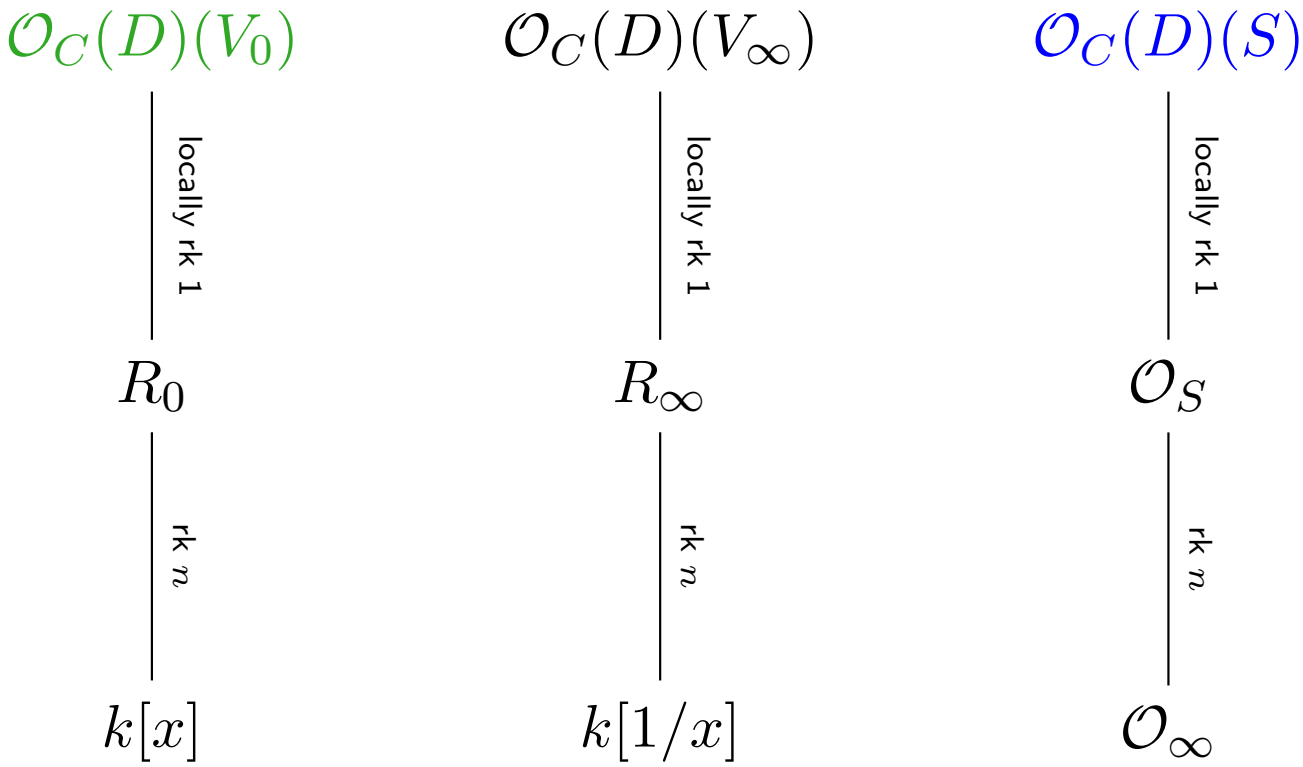
$$[\mathcal{F}] = [\mathcal{O}_C(D)], \quad I = \mathcal{O}_C(D)(V_0) \subseteq R_0, \quad \mathcal{O}_C(D)(S) = x^r\,\mathcal{O}_S$$

$$\deg_k I = rn \leq 2\,g + n$$

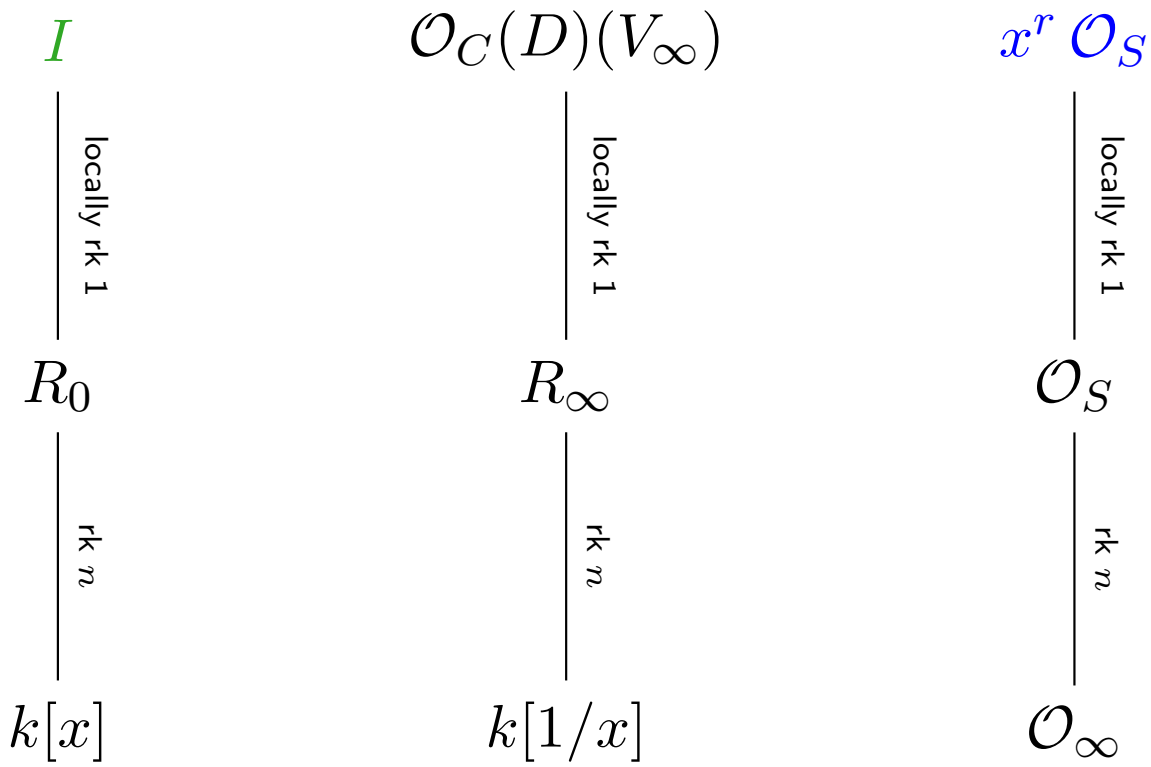
This induces an isomorphism

$$\Phi : \mathrm{Pic}^0(C) \to \mathcal{I}_x/\mathcal{P}_x, \quad [\mathcal{O}_C(D)] \mapsto [\mathcal{O}_C(D)(V_0)]$$

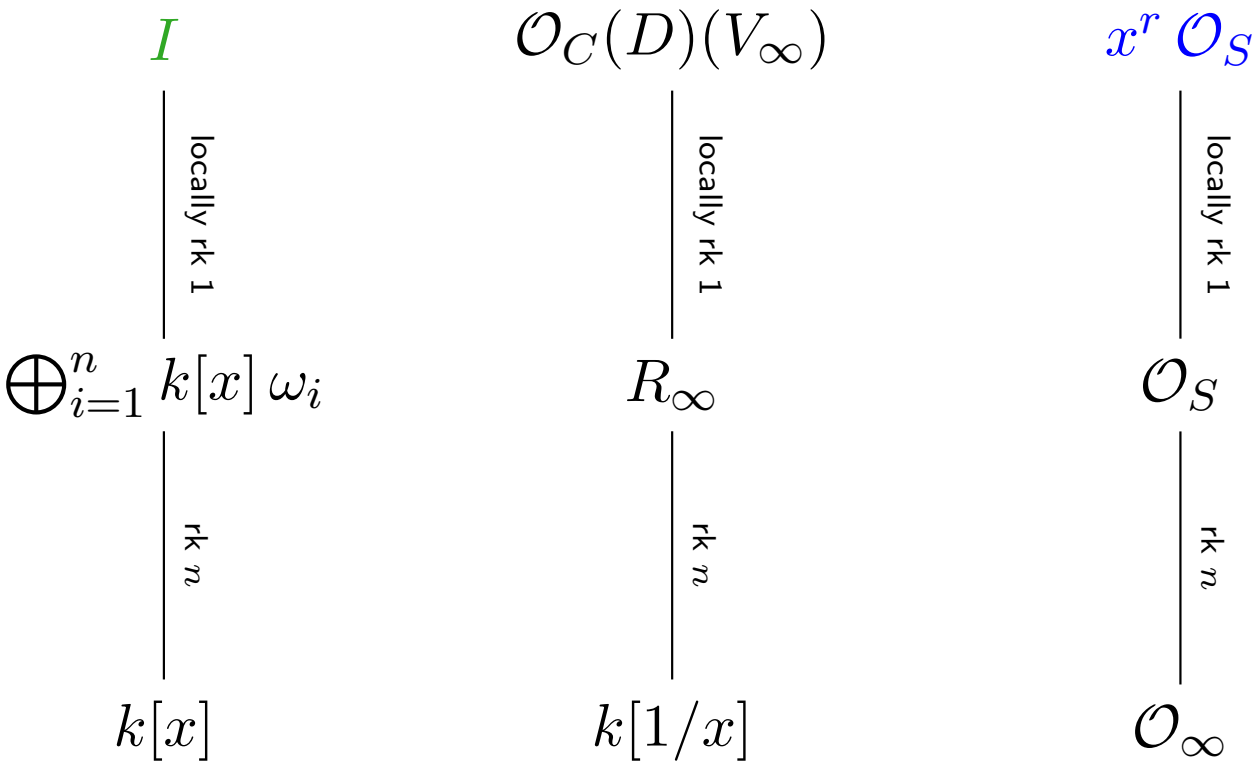
From Sheaves to Matrices



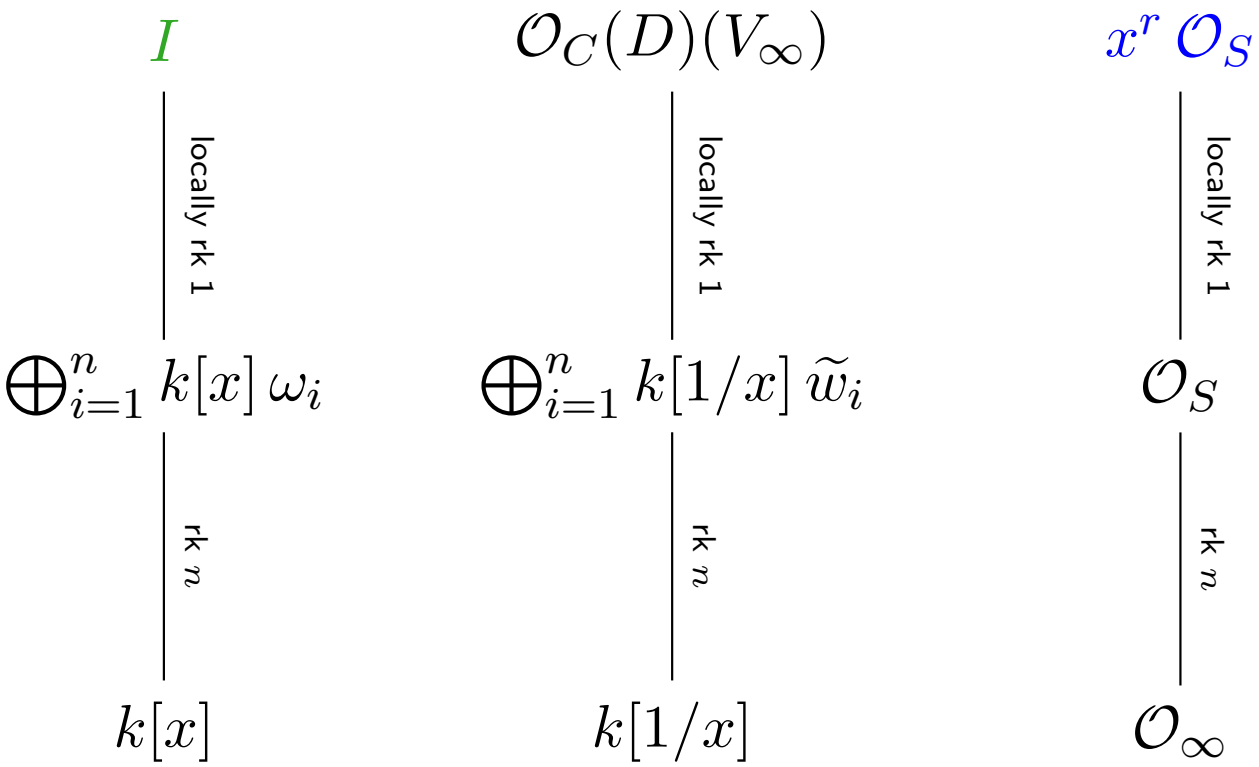
From Sheaves to Matrices



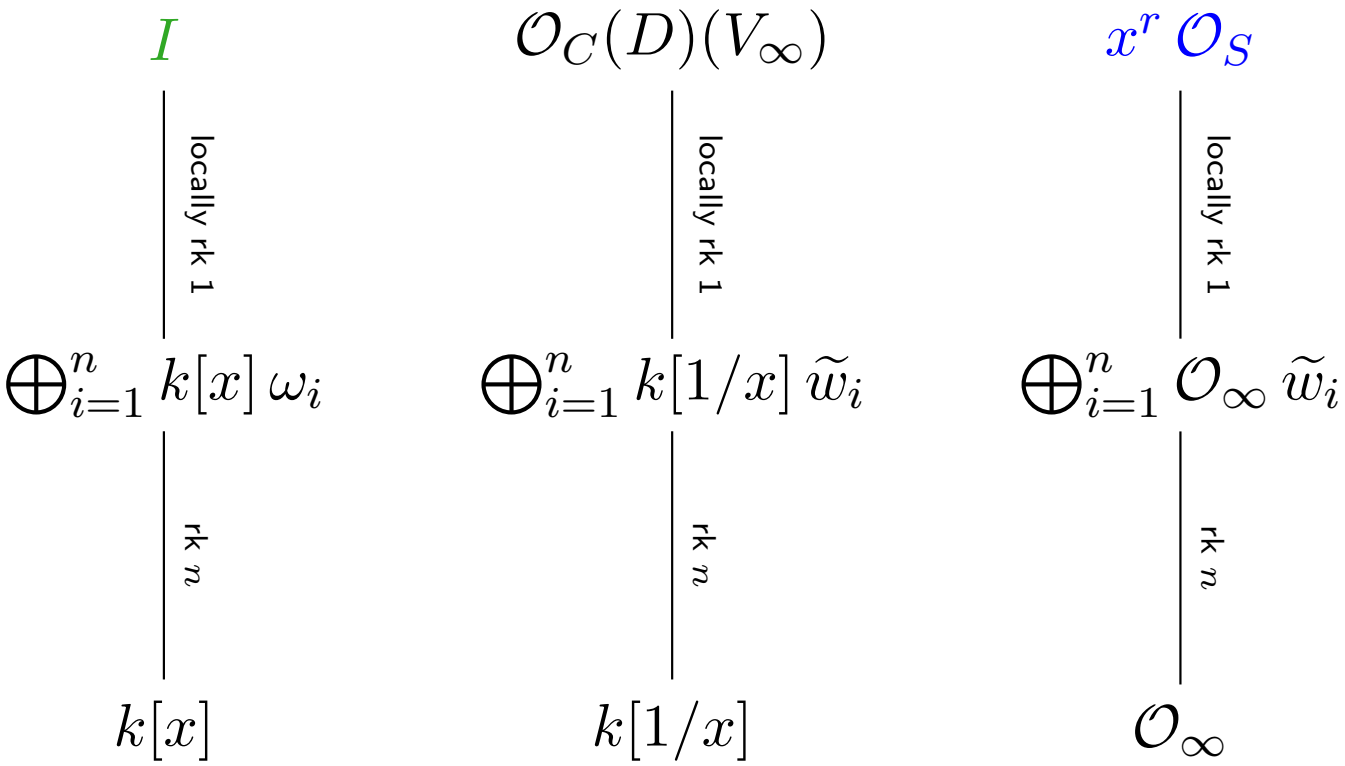
From Sheaves to Matrices



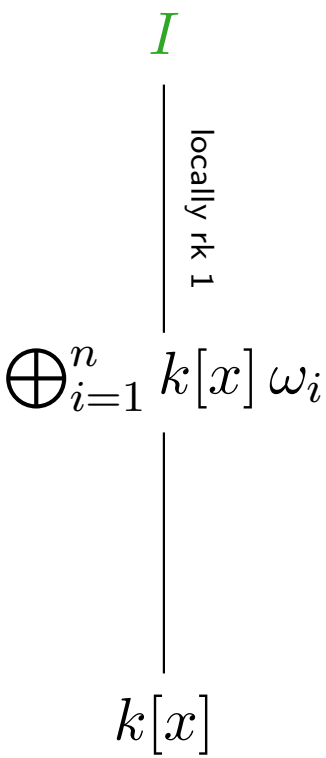
From Sheaves to Matrices

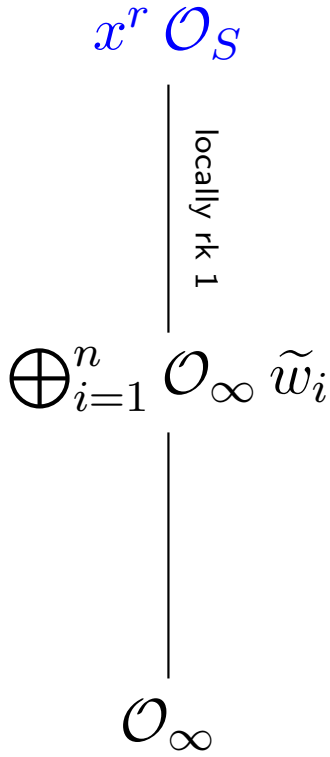


From Sheaves to Matrices

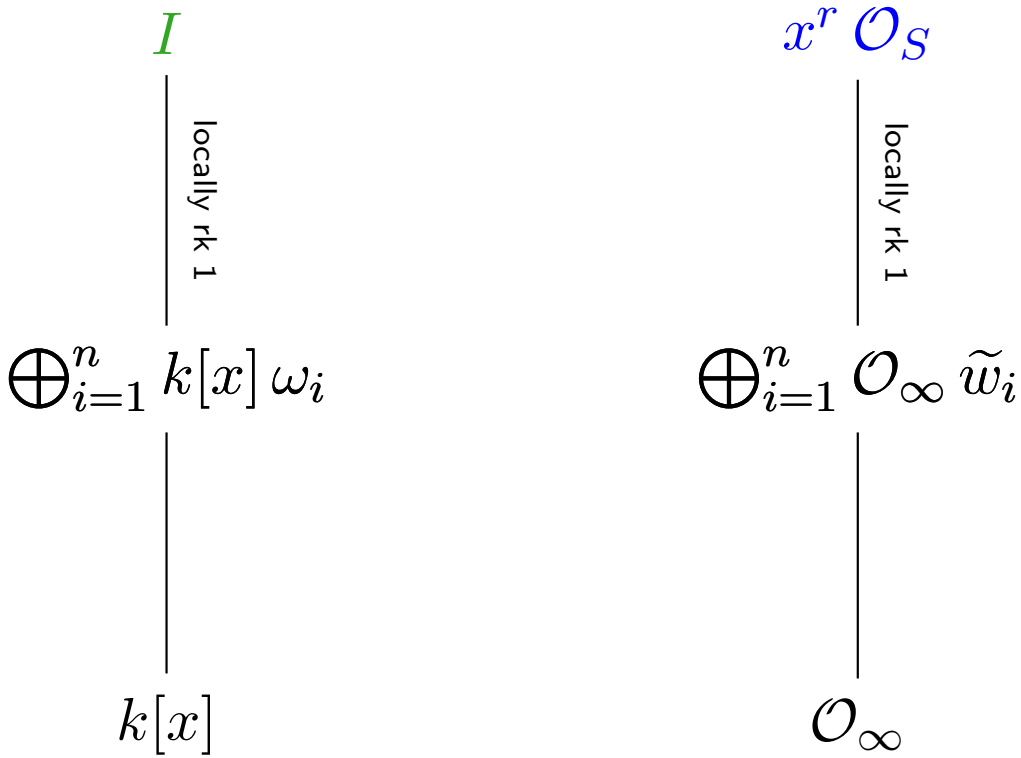


From Sheaves to Matrices

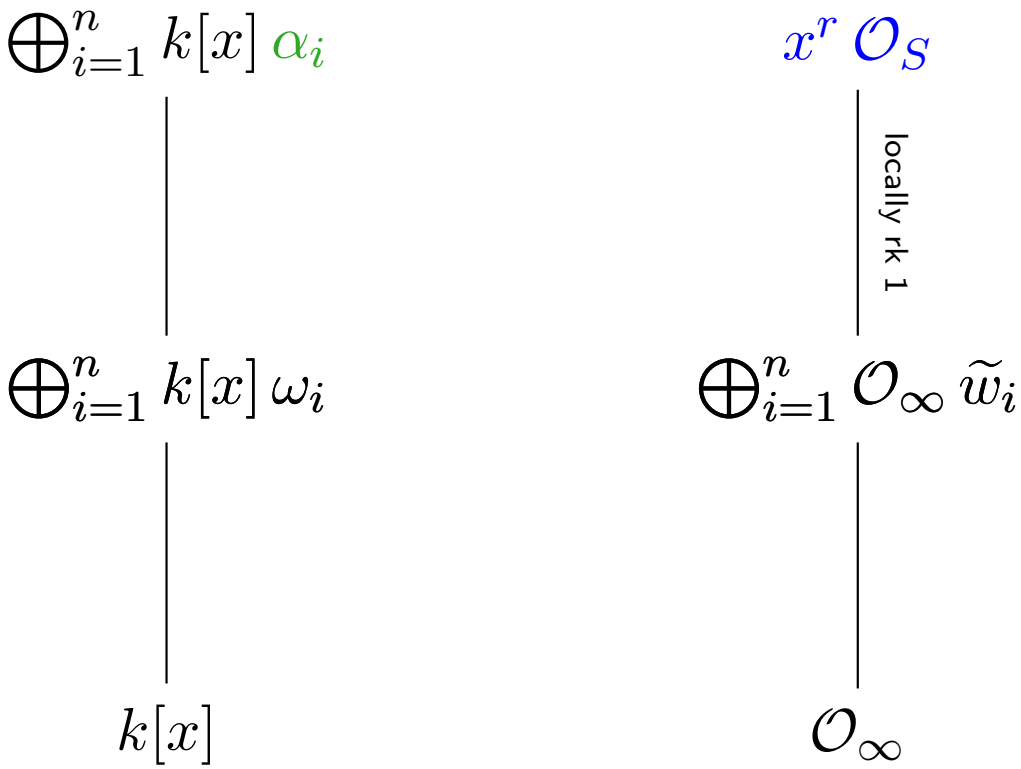




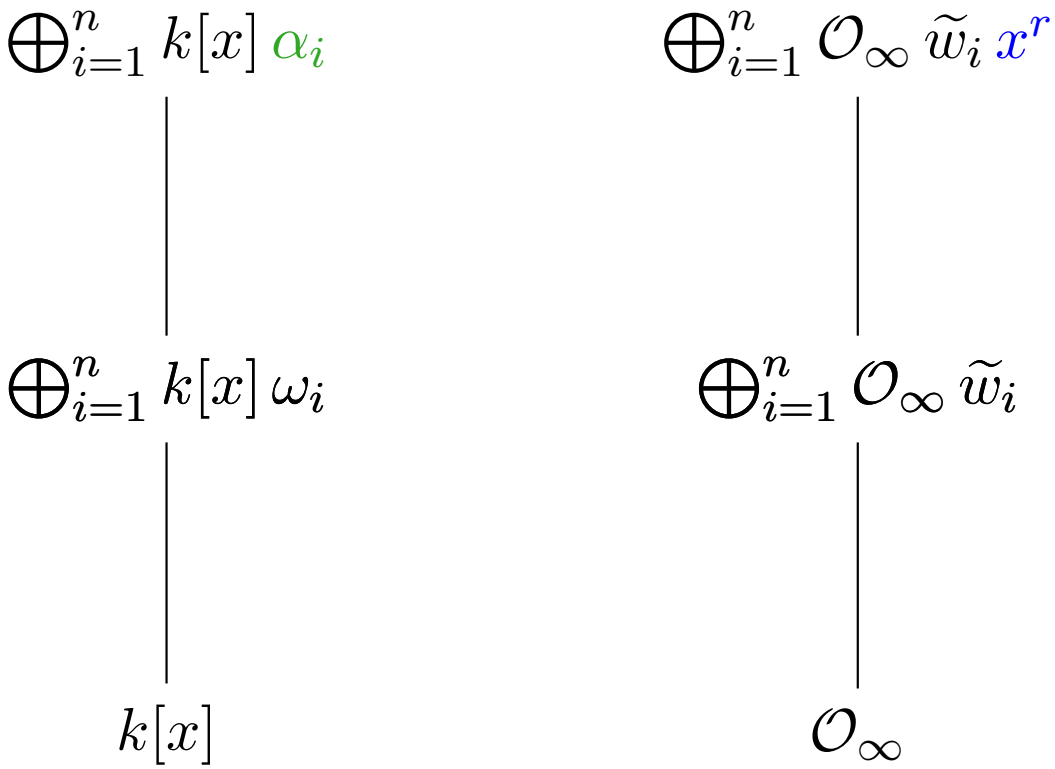
From Sheaves to Matrices



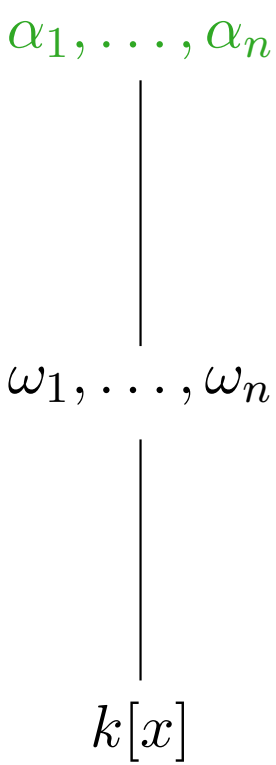
From Sheaves to Matrices

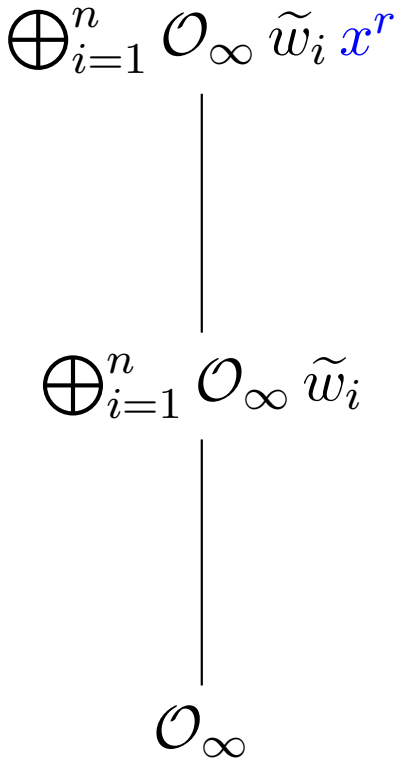


From Sheaves to Matrices

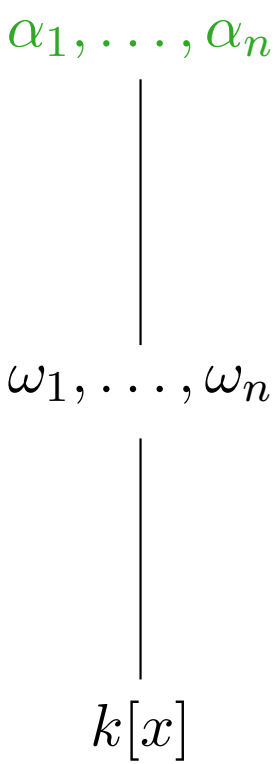


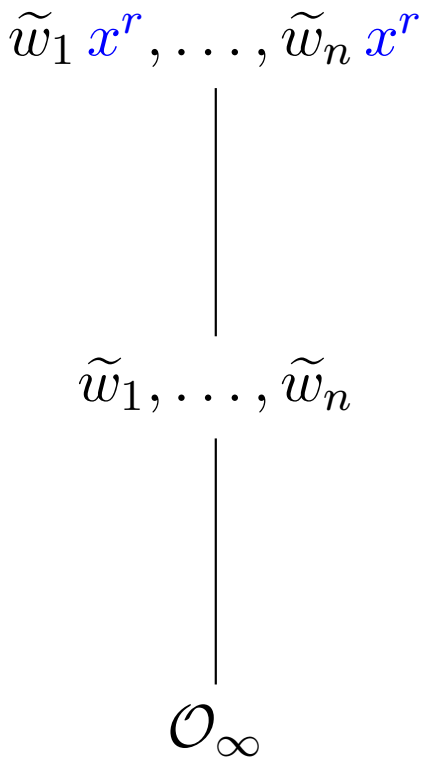
From Sheaves to Matrices



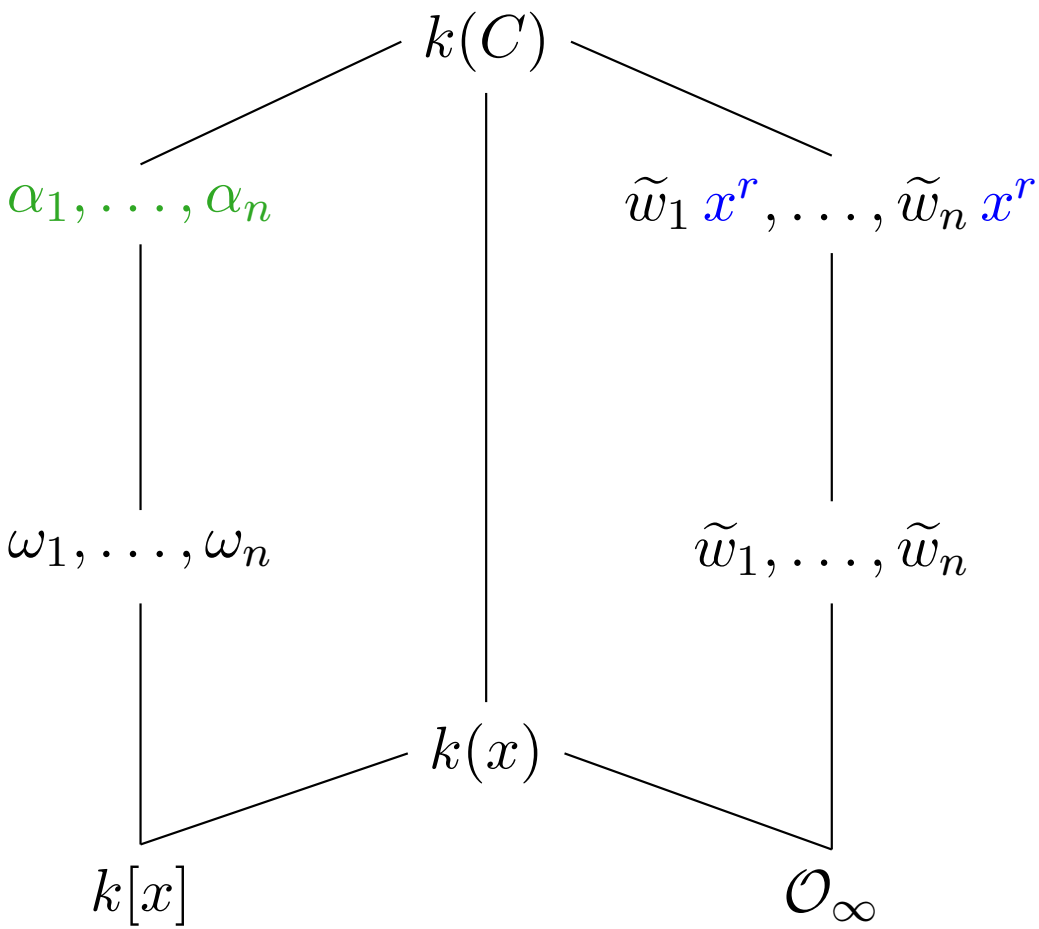


From Sheaves to Matrices

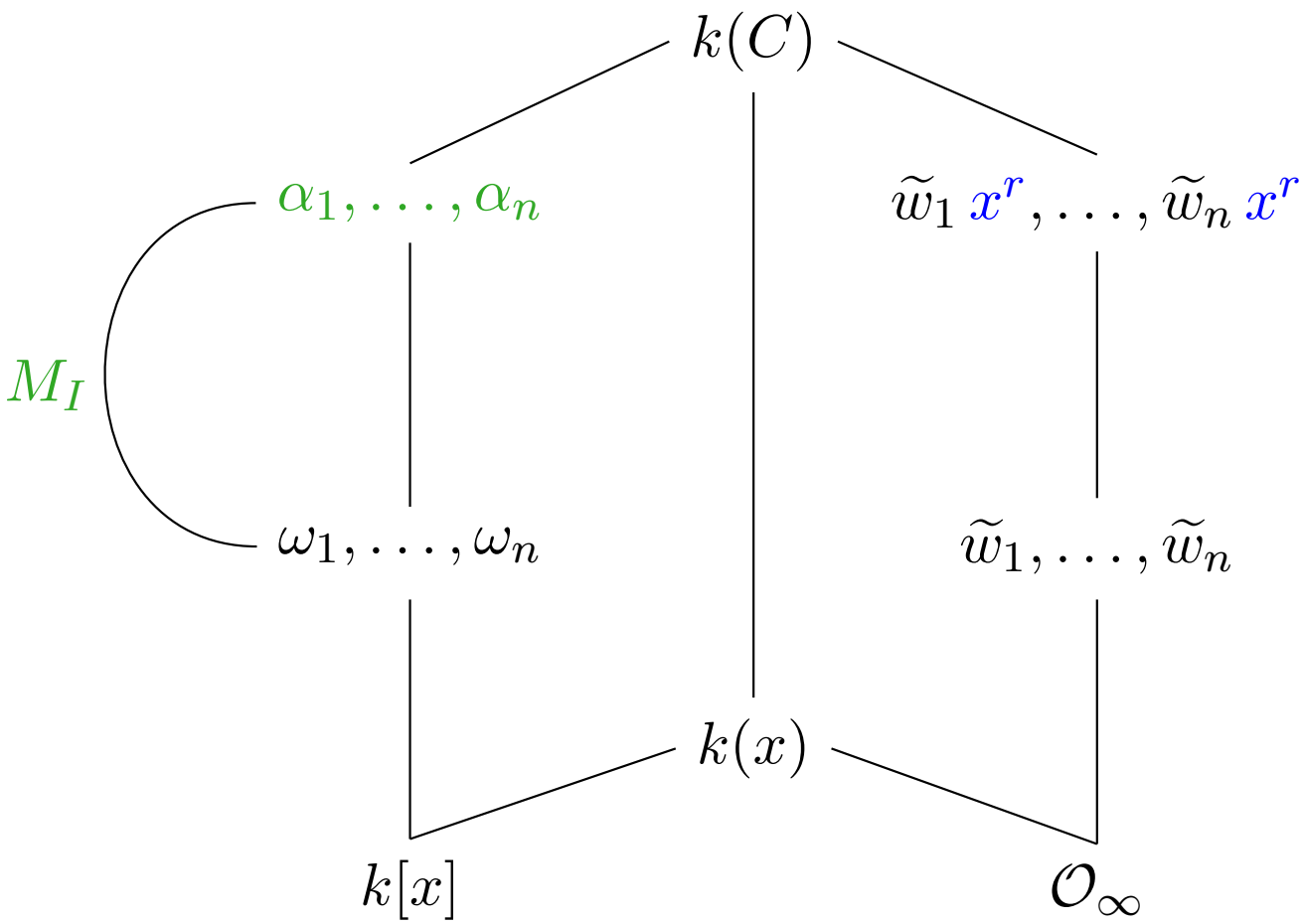




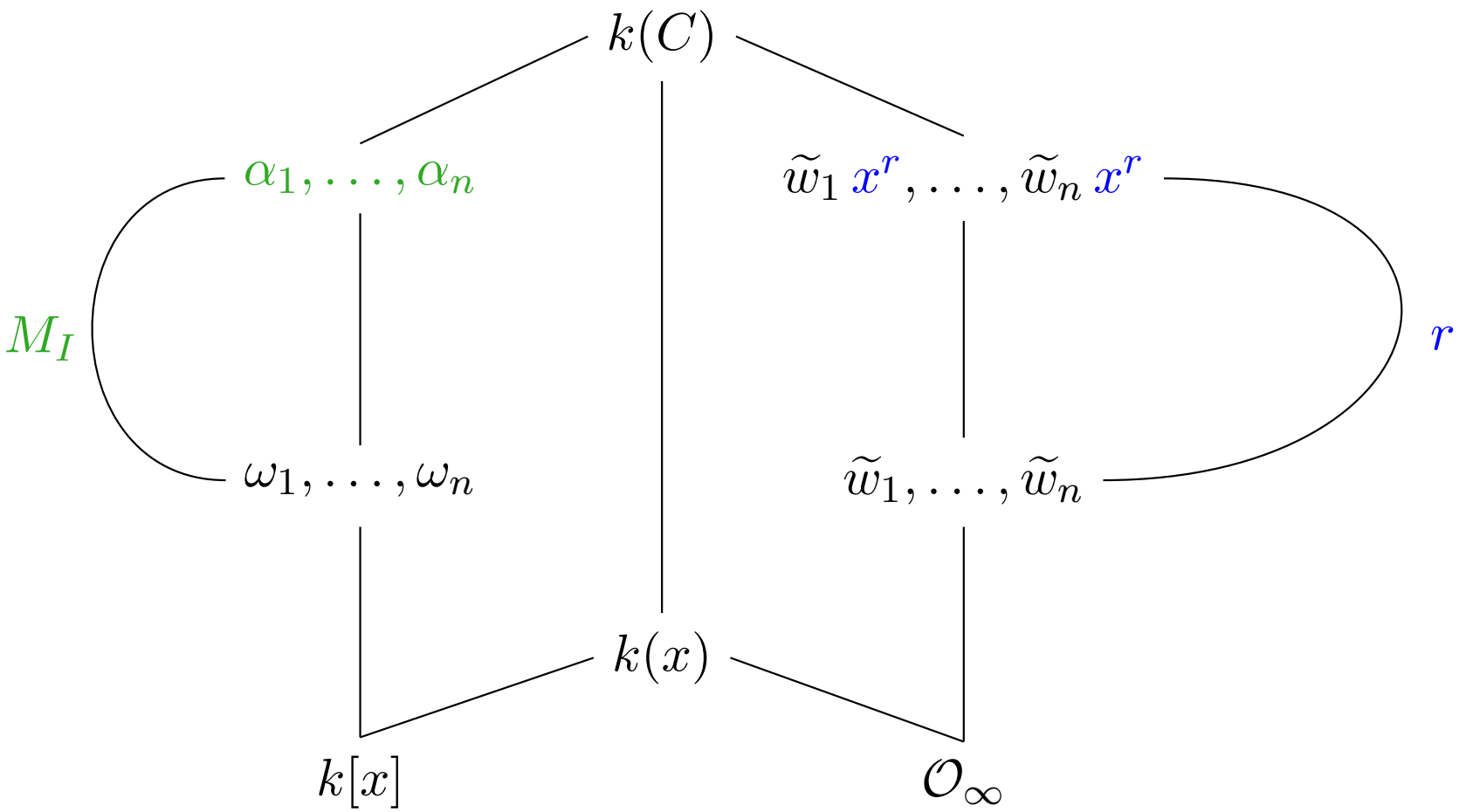
From Sheaves to Matrices



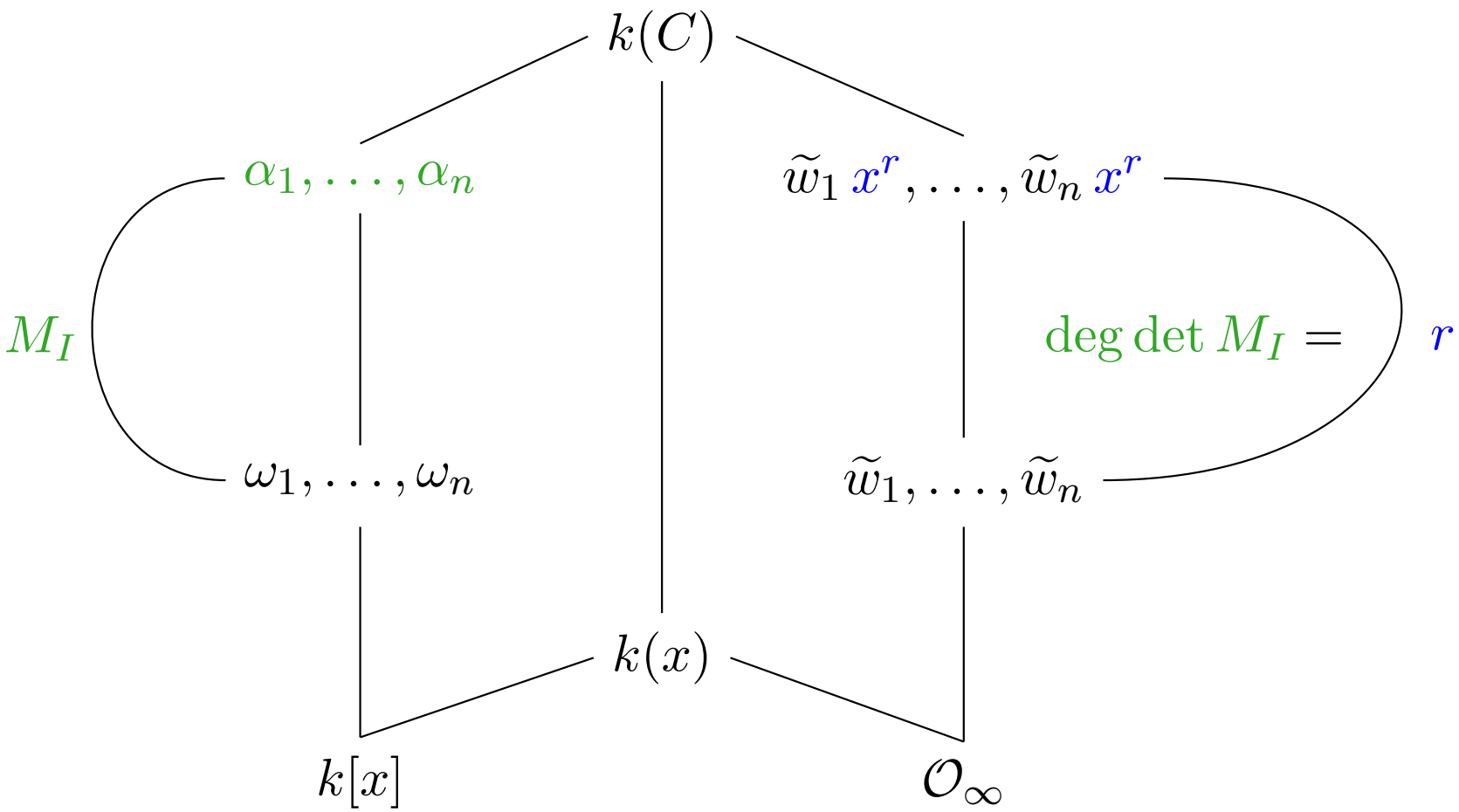
From Sheaves to Matrices



From Sheaves to Matrices



From Sheaves to Matrices



Arithmetic

- Solely work with matrices $M_I \in k[x]^{n \times n}$ of integral ideals I of R_0

Arithmetic

- Solely work with matrices $M_I \in k[x]^{n \times n}$ of integral ideals I of R_0
  - with bounded degrees (in $O(g/n)$)

Arithmetic

- Solely work with matrices $M_I \in k[x]^{n \times n}$ of integral ideals I of R_0
  - with bounded degrees (in $O(g/n)$)
- Tensor product of sheaves boils down to ideal multiplication:

Arithmetic

- Solely work with matrices $M_I \in k[x]^{n \times n}$ of integral ideals I of R_0
  - with bounded degrees (in $O(g/n)$)
- Tensor product of sheaves boils down to ideal multiplication:
  - How to multiply using matrices?

Arithmetic

- Solely work with matrices $M_I \in k[x]^{n \times n}$ of integral ideals I of R_0
  - with bounded degrees (in $O(g/n)$)
- Tensor product of sheaves boils down to ideal multiplication:
  - How to multiply using matrices?
  - We don't know!

Arithmetic

- Solely work with matrices $M_I \in k[x]^{n \times n}$ of integral ideals I of R_0
  - with bounded degrees (in $O(g/n)$)
- Tensor product of sheaves boils down to ideal multiplication:
  - How to multiply using matrices?
  - We don't know!
  - Instead: Division of ideals

Arithmetic

- Solely work with matrices $M_I \in k[x]^{n \times n}$ of integral ideals I of R_0
  - with bounded degrees (in $O(g/n)$)
- Tensor product of sheaves boils down to ideal multiplication:
  - How to multiply using matrices?
  - We don't know!
  - Instead: Division of ideals
- The general idea / How we will proceed:

Arithmetic

- Solely work with matrices $M_I \in k[x]^{n \times n}$ of integral ideals I of R_0
  - with bounded degrees (in $O(g/n)$)
- Tensor product of sheaves boils down to ideal multiplication:
  - How to multiply using matrices?
  - We don't know!
  - Instead: Division of ideals
- The general idea / How we will proceed:
  - Compute integral quotients

Arithmetic

- Solely work with matrices $M_I \in k[x]^{n \times n}$ of integral ideals I of R_0
  - with bounded degrees (in $O(g/n)$)
- Tensor product of sheaves boils down to ideal multiplication:
  - How to multiply using matrices?
  - We don't know!
  - Instead: Division of ideals
- The general idea / How we will proceed:
  - Compute integral quotients
  - Generalize to non-integral quotients using modifications functions

Arithmetic

- Solely work with matrices $M_I \in k[x]^{n \times n}$ of integral ideals I of R_0
  - with bounded degrees (in $O(g/n)$)
- Tensor product of sheaves boils down to ideal multiplication:
  - How to multiply using matrices?
  - We don't know!
  - Instead: Division of ideals
- The general idea / How we will proceed:
  - Compute integral quotients
  - Generalize to non-integral quotients using modifications functions
  - Test of identity

Quotients

By definition

$$J/I = \{z \in k(C) \mid z\,I \subseteq J\}$$

and thus we have the equivalence:

Quotients

By definition

$$J/I = \{z \in k(C) \mid z\,I \subseteq J\}$$

and thus we have the equivalence:

$$z \in J/I \Leftrightarrow \exists\ \mu_i \in k[x]^n : \begin{pmatrix} M_{\beta_1} & M_J & 0 & \dots & 0 \\ M_{\beta_2} & 0 & M_J & 0 & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ M_{\beta_h} & 0 & \dots & 0 & M_J \end{pmatrix} \begin{pmatrix} \vec{z} \\ \mu_1 \\ \vdots \\ \mu_h \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Quotients

By definition

$$J/I = \{z \in k(C) \mid z\,I \subseteq J\}$$

and thus we have the equivalence:

$$z \in J/I \Leftrightarrow \exists\ \mu_i \in k[x]^n : \begin{pmatrix} M_{\beta_1} & M_J & 0 & \dots & 0 \\ M_{\beta_2} & 0 & M_J & 0 & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ M_{\beta_h} & 0 & \dots & 0 & M_J \end{pmatrix} \begin{pmatrix} \vec{z} \\ \mu_1 \\ \vdots \\ \mu_h \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

- Let $\beta_1, \dots, \beta_h$ be a generating set of I with h small

Quotients

By definition

$$J/I = \{z \in k(C) \mid z\,I \subseteq J\}$$

and thus we have the equivalence:

$$z \in J/I \Leftrightarrow \exists\ \mu_i \in k[x]^n : \begin{pmatrix} M_{\beta_1} & M_J & 0 & \dots & 0 \\ M_{\beta_2} & 0 & M_J & 0 & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ M_{\beta_h} & 0 & \dots & 0 & M_J \end{pmatrix} \begin{pmatrix} \vec{z} \\ \mu_1 \\ \vdots \\ \mu_h \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

- Let $\beta_1, \dots, \beta_h$ be a generating set of I with h small
- $M =$ big matrix, $\ker M = \left\{v \in k[x]^{h(n+1)} \mid M\,v = 0\right\}$

Quotients

By definition

$$J/I = \{z \in k(C) \mid z\,I \subseteq J\}$$

and thus we have the equivalence:

$$z \in J/I \Leftrightarrow \exists\ \mu_i \in k[x]^n : \begin{pmatrix} M_{\beta_1} & M_J & 0 & \dots & 0 \\ M_{\beta_2} & 0 & M_J & 0 & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ M_{\beta_h} & 0 & \dots & 0 & M_J \end{pmatrix} \begin{pmatrix} \vec{z} \\ \mu_1 \\ \vdots \\ \mu_h \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

- Let $\beta_1, \dots, \beta_h$ be a generating set of I with h small
- $M =$ big matrix, $\ker M = \left\{v \in k[x]^{h(n+1)} \mid M\,v = 0\right\}$
- Top $(n \times n)$ matrix of $\ker M$ gives basis matrix of J/I

Integral Division

`IntegralDivision`

Input:	$J \subseteq I \subseteq R_0$	given by $M_I,\ M_J \in k[x]^{n\times n}$
Output:	$J/I \subseteq R_0$	given by $M_{J/I} \in k[x]^{n\times n}$

Integral Division

IntegralDivision

Input:	$J \subseteq I \subseteq R_0$	given by $M_I,\ M_J \in k[x]^{n\times n}$
Output:	$J/I \subseteq R_0$	given by $M_{J/I} \in k[x]^{n\times n}$

(1) $(\vec{\beta}_j)_{1\le j\le h} \leftarrow (\sum_{i=1}^{n} \mu_{ij}\ M_I(i))_{1\le j\le h},\ \mu_{ij} \in \{0,1\}$ chosen randomly

(2) $(M_{\beta_1}, \ldots, M_{\beta_h}) \leftarrow (\underline{\texttt{BasMat}}(\vec{\beta}_j))_{1\le j\le h}$

(3) $M_{\ker} \leftarrow \underline{\texttt{MatrixKernel}}(\texttt{BigMatrix}((M_{\beta_1}, \ldots, M_{\beta_h}), M_J))$

(4) $M \leftarrow$ `ReducedBasisMatrix`(Top$(n \times n)$-Matrix of $M_{\ker}$ of Rank n)

(5) If $\deg\det(M) \neq \deg\det(M_J) - \deg\det(M_I)$, then goto (1).

(6) `return` M

Non-integral case

- To reduce the non-integral division to the integral one, we use modification fuctions

Non-integral case

- To reduce the non-integral division to the integral one, we use modification fuctions
  - J, $I \subseteq R_0$ with $J \not\subseteq I$, then $J/I \not\subseteq R_0$

Non-integral case

- To reduce the non-integral division to the integral one, we use modification fuctions
  - J, $I \subseteq R_0$ with $J \not\subseteq I$, then $J/I \not\subseteq R_0$
  - Take $f \in I$, then $fR_0 \cdot J \subseteq I$ and thus $fR_0 \cdot J/I \subseteq R_0$

Non-integral case

- To reduce the non-integral division to the integral one, we use modification fuctions
  - J, $I \subseteq R_0$ with $J \not\subseteq I$, then $J/I \not\subseteq R_0$
  - Take $f \in I$, then $fR_0 \cdot J \subseteq I$ and thus $fR_0 \cdot J/I \subseteq R_0$
- Thus we need algorithms for

Non-integral case

- To reduce the non-integral division to the integral one, we use modification fuctions
  - J, $I \subseteq R_0$ with $J \not\subseteq I$, then $J/I \not\subseteq R_0$
  - Take $f \in I$, then $fR_0 \cdot J \subseteq I$ and thus $fR_0 \cdot J/I \subseteq R_0$
- Thus we need algorithms for
  (1) Computing a modification function $f \in I$ with $fR_0 \in \mathcal{P}_x$ and

Non-integral case

- To reduce the non-integral division to the integral one, we use modification fuctions
  - J, $I \subseteq R_0$ with $J \not\subseteq I$, then $J/I \not\subseteq R_0$
  - Take $f \in I$, then $fR_0 \cdot J \subseteq I$ and thus $fR_0 \cdot J/I \subseteq R_0$
- Thus we need algorithms for
  (1) Computing a modification function $f \in I$ with $fR_0 \in \mathcal{P}_x$ and
  (2) for computing the standard basis matrix M_f of f s.t.

$$(f\,\omega_1, \ldots, f\,\omega_n) = (\omega_1, \ldots, \omega_n)\,M_f.$$

Ad (1)

ModFct

Input:	I	given by M_I	s.t. $\deg_k I \in O(g)$, $\deg M_I \in O(g/n)$
Output:	f	given by $\vec{f}$	s.t. $f \in I$, $fR_0 \in \mathcal{P}_x$, $\deg M_f \leq \frac{6g+\deg_k I}{n}$
			$\deg_k fR_0 \leq 2g + \deg_k I + n$

Ad (1)

ModFct

Input:	I	given by M_I	s.t. $\deg_k I \in O(g)$, $\deg M_I \in O(g/n)$
Output:	f	given by $\vec{f}$	s.t. $f \in I$, $fR_0 \in \mathcal{P}_x$, $\deg M_f \leq \frac{6g+\deg_k I}{n}$
			$\deg_k fR_0 \leq 2g + \deg_k I + n$

(1) $s \leftarrow \deg \det(M_I)$, $r \leftarrow \lceil (s+2g)/n \rceil$

(2) $M \leftarrow \underline{\texttt{ReduceMatrix}}\left((x^{-|0|_i - s}\delta_{i,j})M_I\right)$,
$(|D_I|_i)_i \leftarrow$ neg. column degrees of M

(3) $N \leftarrow M\,(x^{|D_I|_i}\delta_{i,j})$, $N_\infty \leftarrow (N_{i,j} \bmod P_\infty)_{i,j}$

(4) $(\mu_1, \ldots, \mu_n)^T \leftarrow \texttt{SolveLES}_k\left(UN_\infty, (1, \ldots, 1)^T\right)$

(5) $\texttt{return}\ \vec{f} \leftarrow (x^{-|0|_i}\delta_{i,j})N(\mu_1 x^r, \ldots, \mu_n x^r)^T$

Ad (2)

Multiplication Shift:

- Compute $y \in R_0$ and $h \in k[x]$ s.t.

Ad (2)

Multiplication Shift:

- Compute $y \in R_0$ and $h \in k[x]$ s.t.
- $T_h : R_0/hR_0 \xrightarrow{\simeq} k[x,y]/hk[x,y]$

Ad (2)

Multiplication Shift:

- Compute $y \in R_0$ and $h \in k[x]$ s.t.
- $T_h : R_0/hR_0 \xrightarrow{\simeq} k[x,y]/hk[x,y]$

Ad (2)

Multiplication Shift:

- Compute $y \in R_0$ and $h \in k[x]$ s.t.
- $T_h : R_0/hR_0 \xrightarrow{\simeq} k[x,y]/hk[x,y]$

BasMat

Input:	$f \in R_0$	given by $\vec{f}$	s.t. $\deg_k fR_0 \leq \frac{2g+\deg_k I}{n}$
Output:	M_f		s.t. $\deg M_f \leq \frac{6g+\deg_k I}{n}1$

Ad (2)

Multiplication Shift:

- Compute $y \in R_0$ and $h \in k[x]$ s.t.
- $T_h : R_0/hR_0 \xrightarrow{\simeq} k[x,y]/hk[x,y]$

BasMat

Input:	$f \in R_0$	given by $\vec{f}$	s.t. $\deg_k f R_0 \leq \frac{2g+\deg_k I}{n}$
Output:	M_f		s.t. $\deg M_f \leq \frac{6g+\deg_k I}{n} 1$

(1) $T_f \leftarrow \texttt{Reduce}_h(T_h \vec{f})$

(2) $B \leftarrow \texttt{Reduce}_h(T_f \cdot T_h \vec{\omega}_1) \ldots \texttt{Reduce}_h(T_f \cdot T_h \vec{\omega}_n)$

(3) $\texttt{return Reduce}_h(T_h^{-1} \cdot B)$

General Division / Group Law

Division

Input:	$J,\, I \subseteq R_0$	given by $M_I,\, M_J \in k[x]^{n\times n}$	
Output:	$H \subseteq R_0$	given by $M_H \in k[x]^{n\times n}$	s.t. $[H] = [J/I]$

General Division / Group Law

Division

Input:	$J,\, I \subseteq R_0$	given by $M_I,\, M_J \in k[x]^{n\times n}$	
Output:	$H \subseteq R_0$	given by $M_H \in k[x]^{n\times n}$	s.t. $[H] = [J/I]$

(1) $M_f \leftarrow \texttt{ModFctBasMat}(M_I)$

(2) $M \leftarrow \texttt{ReducedBasisMatrix}(M_f \cdot M_J)$

(3) $\texttt{return IntegralDivision}(M, M_J)$

Test of Identity

- There exists an invariant $|I| := |D_I|_1$ of each Ideal I s.t.

$$|I| \geq 0 \Leftrightarrow [I] = [R_0]$$

Test of Identity

- There exists an invariant $|I| := |D_I|_1$ of each Ideal I s.t.

$$|I| \geq 0 \Leftrightarrow [I] = [R_0]$$

- $|I|$ can be easily read off from (a reduced variant of) basis matrix M_I

Test of Identity

- There exists an invariant $|I| := |D_I|_1$ of each Ideal I s.t.

$$|I| \geq 0 \Leftrightarrow [I] = [R_0]$$

- $|I|$ can be easily read off from (a reduced variant of) basis matrix M_I

Test of Identity

- There exists an invariant $|I| := |D_I|_1$ of each Ideal I s.t.

$$|I| \geq 0 \Leftrightarrow [I] = [R_0]$$

- $|I|$ can be easily read off from (a reduced variant of) basis matrix M_I

`IdentityTest`

Input:	$I \subseteq R_0$	given by $M_I \in k[x]^{n \times n}$	s.t. $\deg_k I \in O(g)$
Output:	Yes if $[I] = [R_0]$	No if $[I] \neq [R_0]$	

Test of Identity

- There exists an invariant $|I| := |D_I|_1$ of each Ideal I s.t.

$$|I| \geq 0 \Leftrightarrow [I] = [R_0]$$

- $|I|$ can be easily read off from (a reduced variant of) basis matrix M_I

`IdentityTest`

Input:	$I \subseteq R_0$	given by $M_I \in k[x]^{n \times n}$	s.t. $\deg_k I \in O(g)$
Output:	Yes if $[I] = [R_0]$	No if $[I] \neq [R_0]$	

(1) $|I| \leftarrow$`ReadOffInvariant`(M_I)

(2) If $|I| \geq 0$, then `return` **Yes**

(3) `return` **No**

Ingredients

- Riemann-Roch for singular curves

Ingredients

- Riemann-Roch for singular curves
  - $\deg_k \mathcal{O}_C(D) \geq 2\,g - 1 \Rightarrow \dim_k \mathrm{H}^0\left(C, \mathcal{O}_C(D)\right) = \deg_k \mathcal{O}_C(D) + 1 - g$ (for non lci curves)

Ingredients

- Riemann-Roch for singular curves
  - $\deg_k \mathcal{O}_C(D) \geq 2\,g - 1 \Rightarrow \dim_k \mathrm{H}^0\left(C, \mathcal{O}_C(D)\right) = \deg_k \mathcal{O}_C(D) + 1 - g$ (for non lci curves)
- Strong Approximation (singular case **!**):
  Let $\mathcal{F} \subseteq \mathcal{G}$ be coherent sheaves on C with $\deg_k \mathcal{F} \geq 2g - 1$.
  Then the following sequence is exact:

$$0 \to \mathrm{H}^0\left(C, \mathcal{F}\right) \to \mathrm{H}^0\left(C, \mathcal{G}\right) \to \coprod_{P \in C} \mathcal{G}_P / \mathcal{F}_P \to 0$$

Ingredients

- Riemann-Roch for singular curves
  - $\deg_k \mathcal{O}_C(D) \geq 2\,g - 1 \Rightarrow \dim_k \mathrm{H}^0\left(C, \mathcal{O}_C(D)\right) = \deg_k \mathcal{O}_C(D) + 1 - g$ (for non lci curves)
- Strong Approximation (singular case **!**):
  Let $\mathcal{F} \subseteq \mathcal{G}$ be coherent sheaves on C with $\deg_k \mathcal{F} \geq 2g - 1$.
  Then the following sequence is exact:

$$0 \to \mathrm{H}^0\left(C, \mathcal{F}\right) \to \mathrm{H}^0\left(C, \mathcal{G}\right) \to \coprod_{P \in C} \mathcal{G}_P / \mathcal{F}_P \to 0$$

- Birkhoff matrix decomposition/Grothendieck:
  $\mathcal{F}$ coherent torsion free sheaf on C:

$$\pi_* \mathcal{F} = \bigoplus_{i=1}^{n} \mathcal{O}_{\mathbb{P}^1}\left(|\mathcal{F}|_i\right).$$

Achievements

- Reduced arithmetic in $\mathrm{Pic}^0(C)$ to linear algebra over $k[x]$ in
  - dimension n and
  - degree $O(g/n)$.

Achievements

- Reduced arithmetic in $\mathrm{Pic}^0(C)$ to linear algebra over $k[x]$ in
  - dimension n and
  - degree $O(g/n)$.
- Overall complexity:

$$O^{\sim}(n^{\omega-1}\, g)$$

Achievements

- Reduced arithmetic in $\mathrm{Pic}^0(C)$ to linear algebra over $k[x]$ in
  - dimension n and
  - degree $O(g/n)$.
- Overall complexity:

$$O^{\sim}(n^{\omega-1}\, g)$$

- Two main achievements:

Achievements

- Reduced arithmetic in $\mathrm{Pic}^0(C)$ to linear algebra over $k[x]$ in
  - dimension n and
  - degree $O(g/n)$.
- Overall complexity:

$$O^{\sim}(n^{\omega-1}\, g)$$

- Two main achievements:
  (1) Interpolate between best known running times (**regular** case)

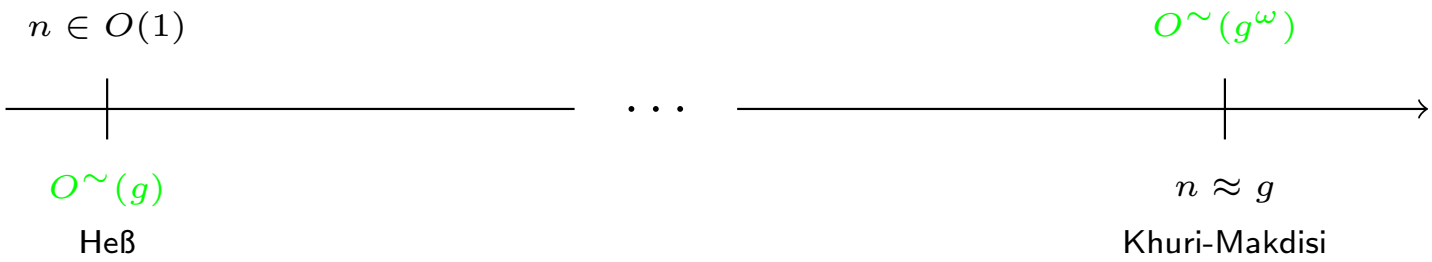
Achievements

- Reduced arithmetic in $\mathrm{Pic}^0(C)$ to linear algebra over $k[x]$ in
  - dimension n and
  - degree $O(g/n)$.
- Overall complexity:

$$O^{\sim}(n^{\omega-1}\, g)$$

- Two main achievements:

  (1) Interpolate between best known running times (**regular** case)

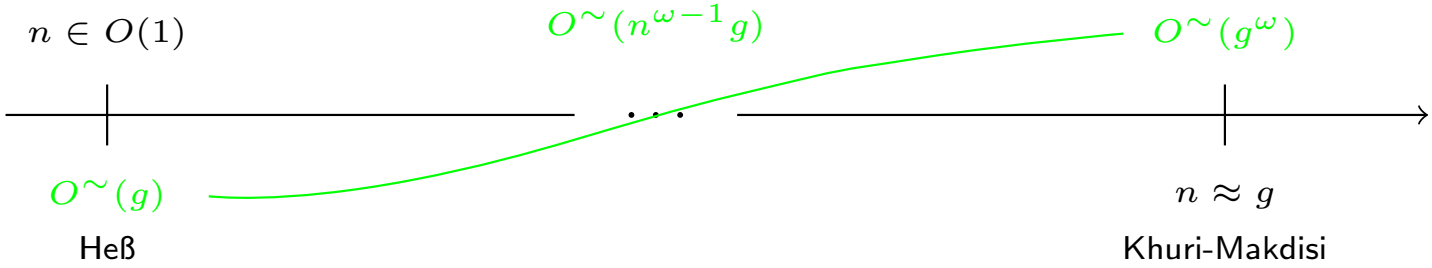


Achievements

- Reduced arithmetic in $\mathrm{Pic}^0(C)$ to linear algebra over $k[x]$ in
  - dimension n and
  - degree $O(g/n)$.
- Overall complexity:

$$O^{\sim}(n^{\omega-1}\, g)$$

- Two main achievements:
  (1) Interpolate between best known running times (**regular** case)



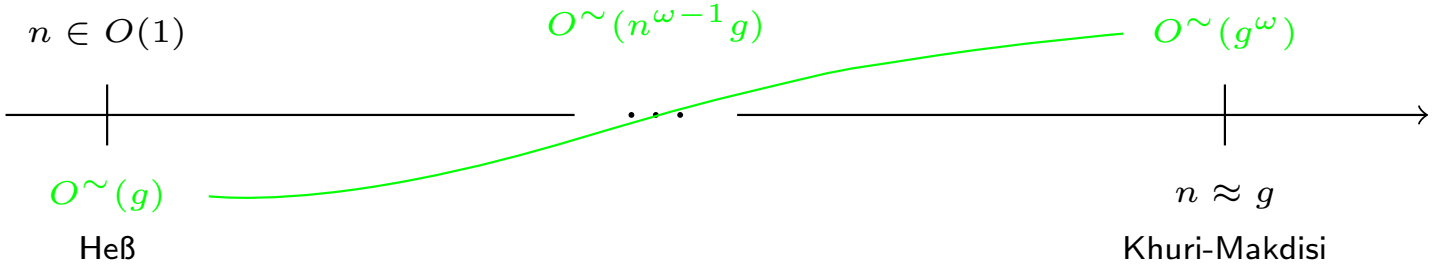
Achievements

- Reduced arithmetic in $\mathrm{Pic}^0(C)$ to linear algebra over $k[x]$ in
  - dimension n and
  - degree $O(g/n)$.
- Overall complexity:

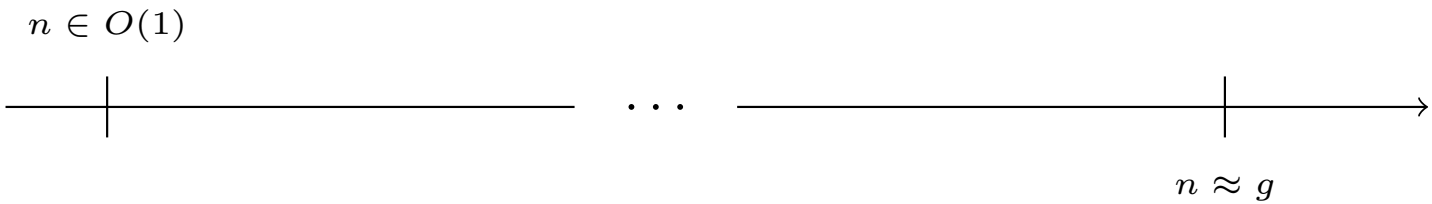
$$O^{\sim}(n^{\omega-1}\, g)$$

- Two main achievements:

(1) Interpolate between best known running times (**regular** case)



(2) First results for the **singular** case (as fast as the regular case):



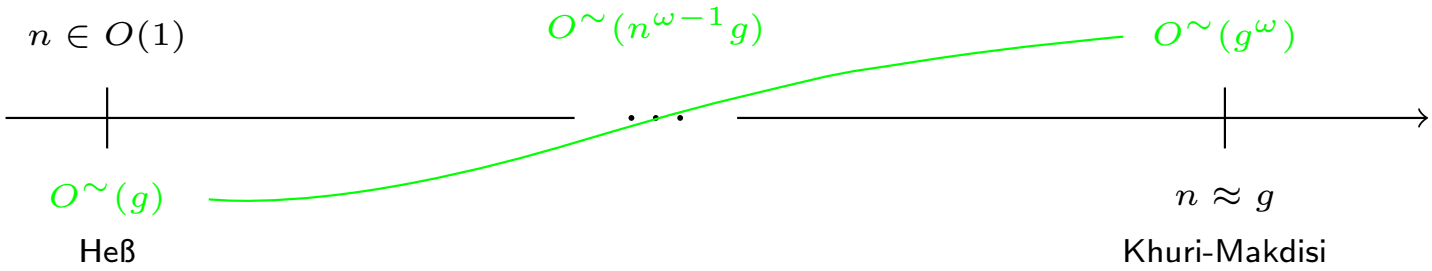
Achievements

- Reduced arithmetic in $\mathrm{Pic}^0(C)$ to linear algebra over $k[x]$ in
  - dimension n and
  - degree $O(g/n)$.
- Overall complexity:

$$O^{\sim}(n^{\omega-1}\, g)$$

- Two main achievements:

(1) Interpolate between best known running times (**regular** case)



(2) First results for the **singular** case (as fast as the regular case):