# Die Divisorenklassengruppe

## und die Wahrheit über elliptische Kurven

Johannes Schmitt
TU Kaiserslautern
23. Juni 2020

## Divisoren

Klassengruppen

Beispiel: Elliptische Kurven

Und jetzt?

# Konvention

Varietät := normale, irreduzible, quasi-projektive Varietät über $\mathbb{C}$

# Konvention

Varietät := normale, irreduzible, quasi-projektive Varietät über $\mathbb{C}$
Kurve := 1-dimensionale Varietät
Fläche := 2-dimensionale Varietät

# Divisoren

## Definition

Sei $X$ eine Varietät. Ein **Primdivisor** auf $X$ ist eine Untervarietät $D$ mit Kodimension 1.

# Divisoren

## Definition

Sei $X$ eine Varietät. Ein **Primdivisor** auf $X$ ist eine Untervarietät $D$ mit Kodimension 1.

Die Primdivisoren erzeugen die freie abelsche Gruppe $\operatorname{Div} X$.

# Divisoren

## Definition

Sei $X$ eine Varietät. Ein **Primdivisor** auf $X$ ist eine Untervarietät $D$ mit Kodimension 1.

Die Primdivisoren erzeugen die freie abelsche Gruppe $\operatorname{Div} X$.

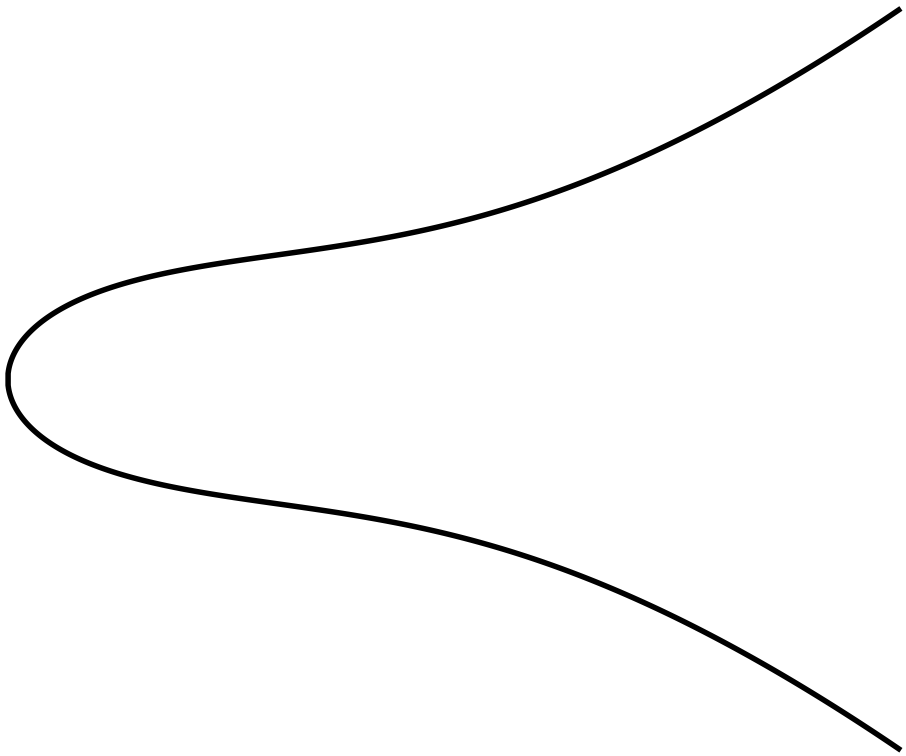
Ein **Weil Divisor** ist ein Element von $\operatorname{Div} X$.

[vɛj]

# Divisoren

## Beispiel

Sei $X$ eine Kurve.

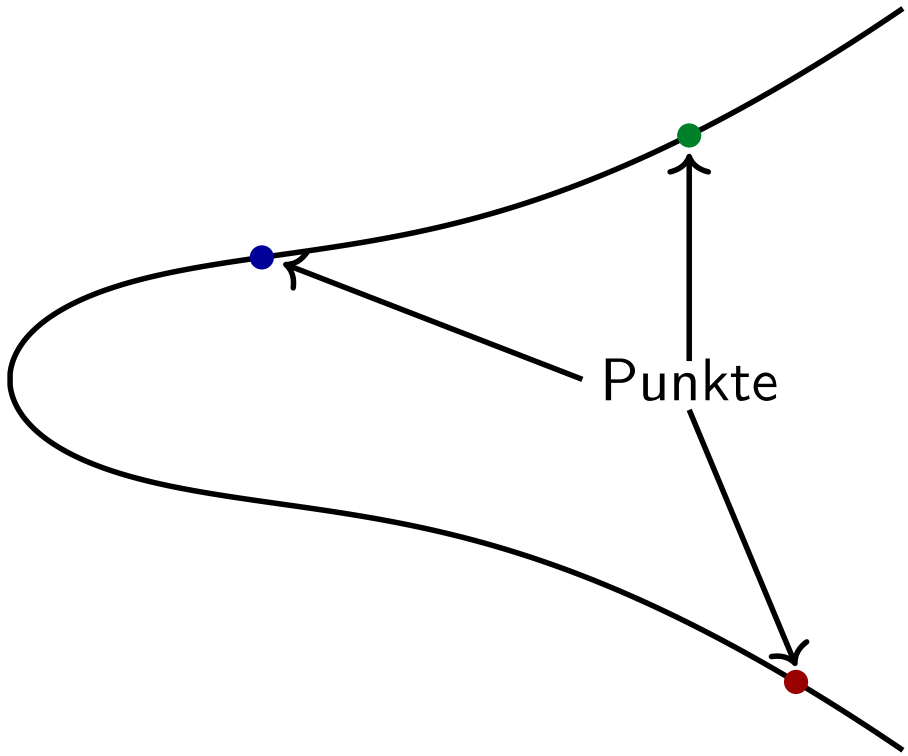


# Divisoren

## Beispiel

Sei $X$ eine Kurve.

Primdivisoren: Punkte $P$ auf $X$

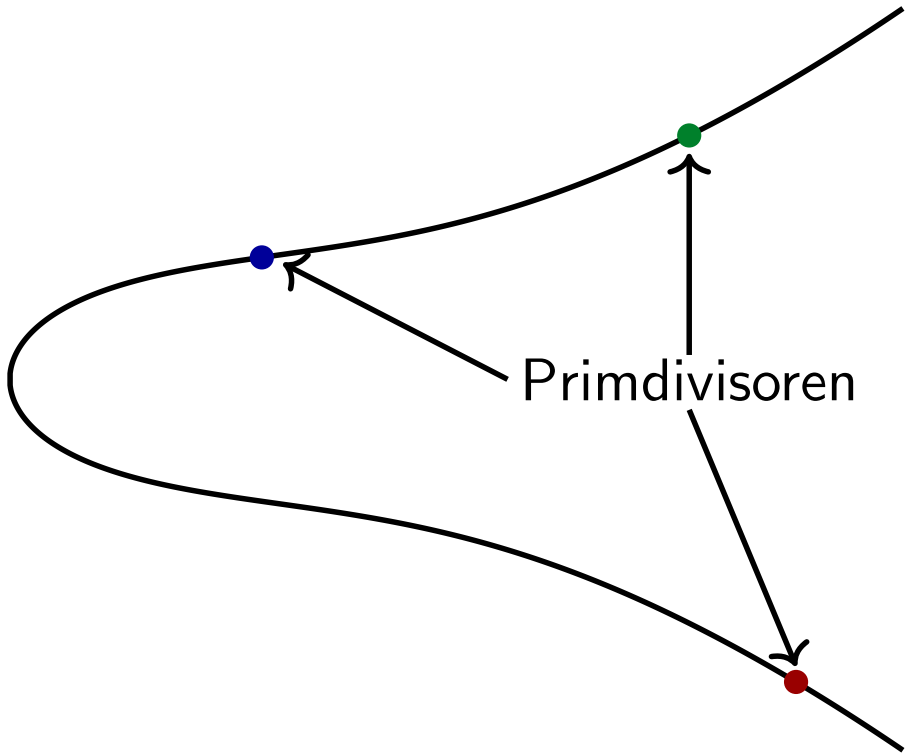


# Divisoren

## Beispiel

Sei $X$ eine Kurve.

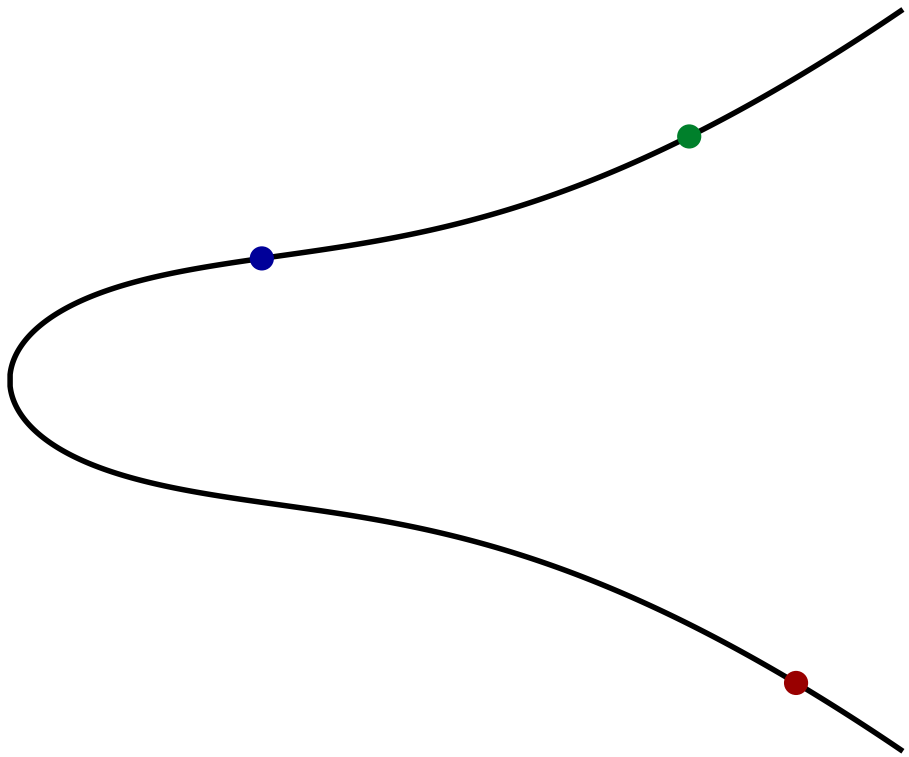
Primdivisoren: Punkte $P$ auf $X$



# Divisoren

## Beispiel

Sei $X$ eine Kurve.
Primdivisoren: Punkte $P$ auf $X$
Divisoren: Formale Summen von Punkten $\sum_{P \in X} n_P P$ ($n_P \in \mathbb{Z}$, nur endlich viele nicht 0)

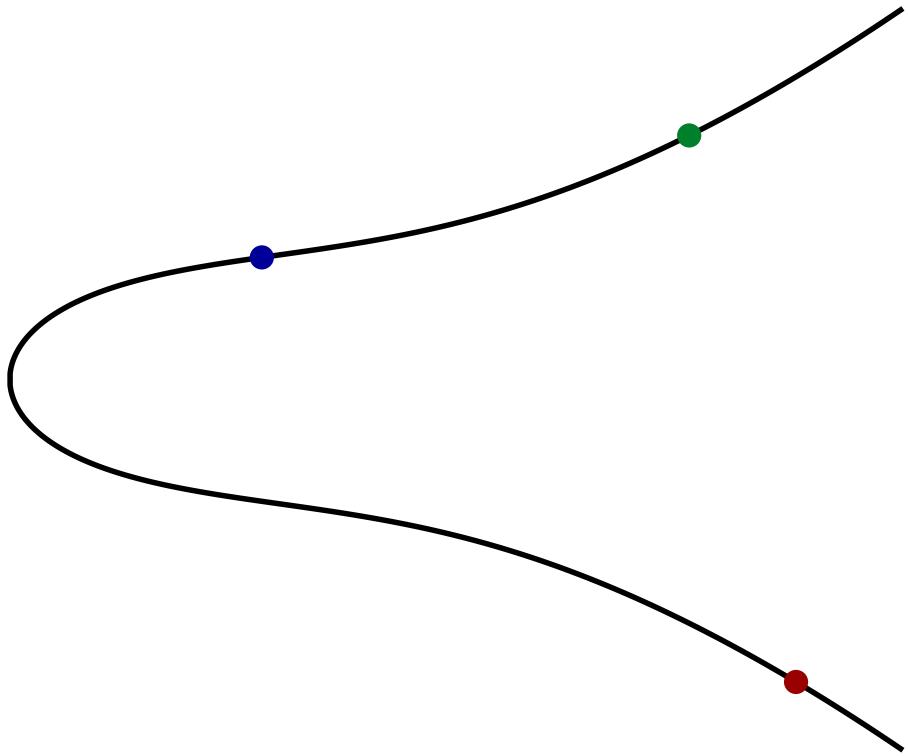


# Divisoren

## Beispiel

Sei $X$ eine Kurve.
Primdivisoren: Punkte $P$ auf $X$
Divisoren: Formale Summen von Punkten $\sum_{P \in X} n_P P$ ($n_P \in \mathbb{Z}$, nur endlich viele nicht 0)

- $\bullet + \bullet$,

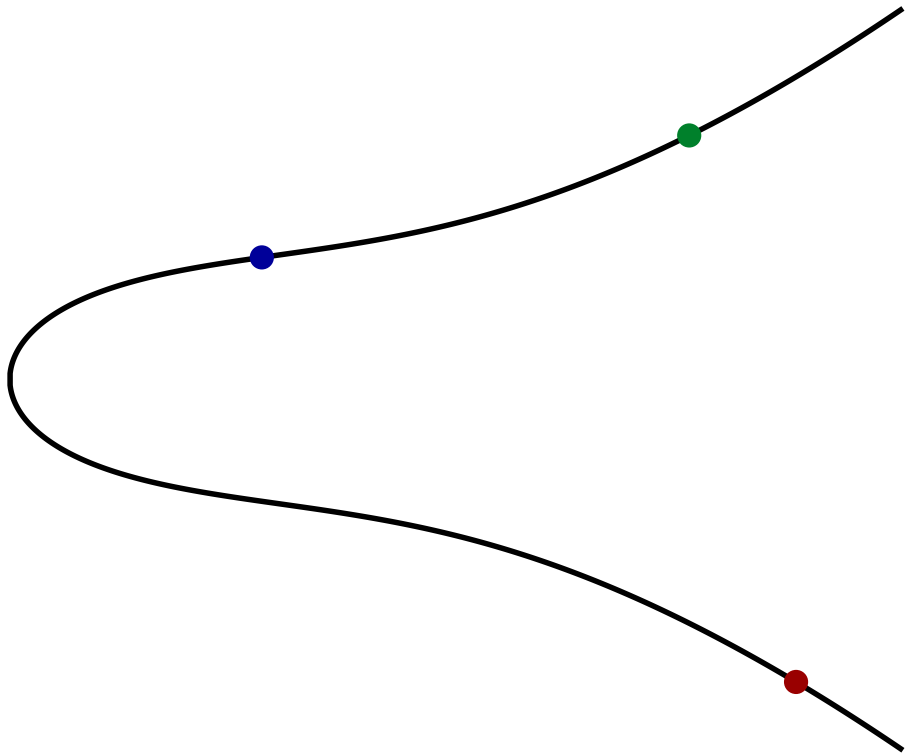


# Divisoren

## Beispiel

Sei $X$ eine Kurve.
Primdivisoren: Punkte $P$ auf $X$
Divisoren: Formale Summen von Punkten $\sum_{P \in X} n_P P$ ($n_P \in \mathbb{Z}$, nur endlich viele nicht 0)

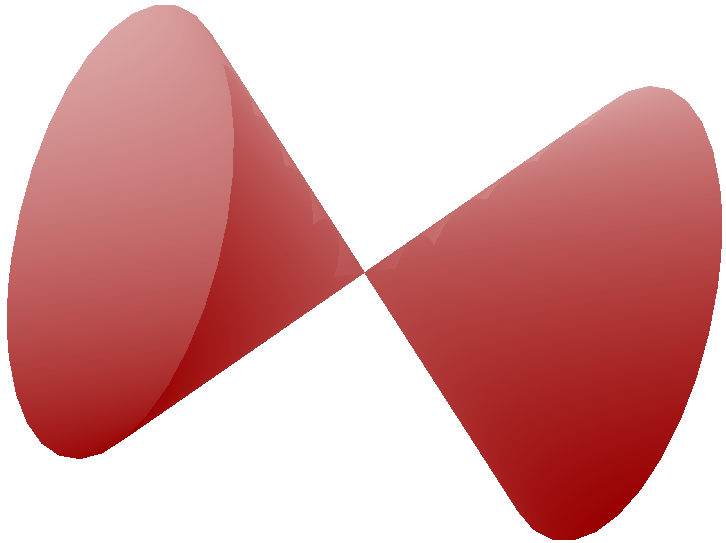
$\bullet + \bullet$, $2\bullet - \bullet$, ...



# Divisoren

## Beispiel

Sei $X$ eine Fläche.

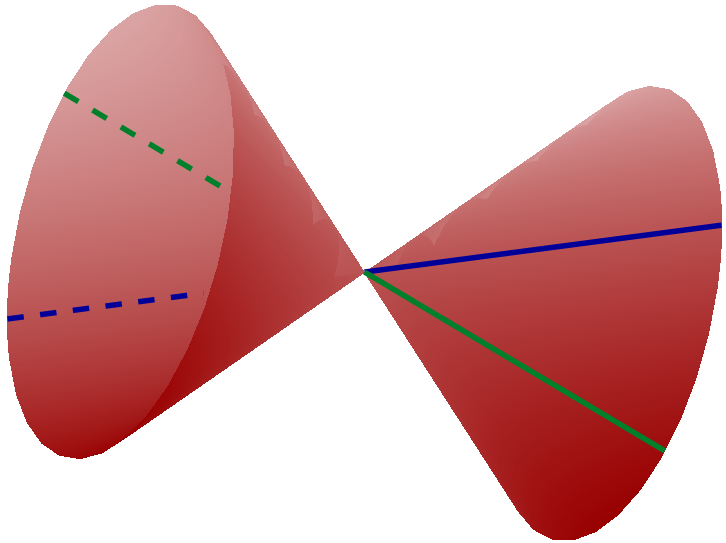


# Divisoren

## Beispiel

Sei $X$ eine Fläche.

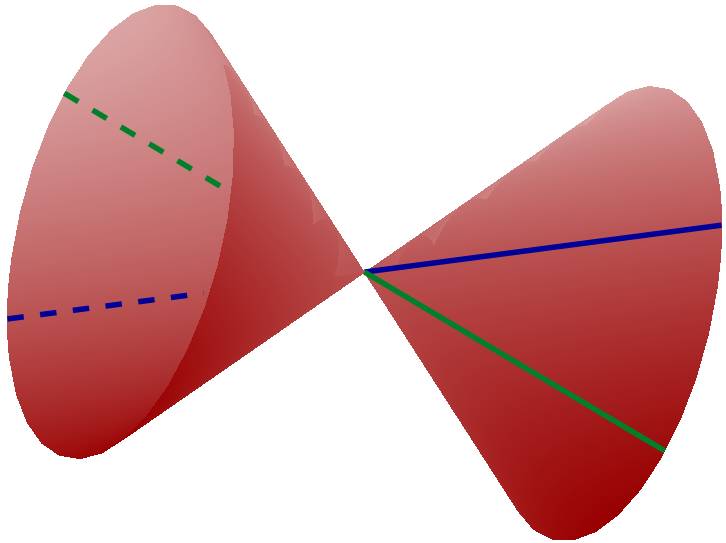
Primdivisoren: Kurven $C$ auf $X$



# Divisoren

## Beispiel

Sei $X$ eine Fläche.
Primdivisoren: Kurven $C$ auf $X$
Divisoren: Formale Summen von Kurven $\sum_{C \subseteq X} n_C C$



# Hauptdivisoren

## Fakt

Sei $X$ eine Varietät und $Y \subseteq X$ ein Primdivisor.

# Hauptdivisoren

## Fakt

Sei $X$ eine Varietät und $Y \subseteq X$ ein Primdivisor. Dann korrespondiert ein diskreter Bewertungsring $\mathcal{O}_Y$ und eine diskrete Bewertung $v_Y$ zu $Y$.

# Hauptdivisoren

## Fakt

Sei $X$ eine Varietät und $Y \subseteq X$ ein Primdivisor. Dann korrespondiert ein diskreter Bewertungsring $\mathcal{O}_Y$ und eine diskrete Bewertung $v_Y$ zu $Y$. Der Divisor $Y$ ist eindeutig durch $v_Y$ bestimmt.

# Hauptdivisoren

## Fakt

Sei $X$ eine Varietät und $Y \subseteq X$ ein Primdivisor. Dann korrespondiert ein diskreter Bewertungsring $\mathcal{O}_Y$ und eine diskrete Bewertung $v_Y$ zu $Y$. Der Divisor $Y$ ist eindeutig durch $v_Y$ bestimmt.

## Lemma

Sei $0 \neq f$ eine reguläre Funktion auf $X$. Dann ist $v_Y(f) \in \mathbb{Z}$ für alle Primdivisoren $Y$ und $v_Y(f) \neq 0$ für nur endlich viele Primdivisoren.

# Hauptdivisoren

## Fakt

Sei $X$ eine Varietät und $Y \subseteq X$ ein Primdivisor. Dann korrespondiert ein diskreter Bewertungsring $\mathcal{O}_Y$ und eine diskrete Bewertung $v_Y$ zu $Y$. Der Divisor $Y$ ist eindeutig durch $v_Y$ bestimmt.

## Lemma

Sei $0 \neq f$ eine reguläre Funktion auf $X$. Dann ist $v_Y(f) \in \mathbb{Z}$ für alle Primdivisoren $Y$ und $v_Y(f) \neq 0$ für nur endlich viele Primdivisoren.

## Definition

Sei $0 \neq f$ eine reguläre Funktion auf $X$. Der **Divisor** $(f)$ von $f$ ist definiert als

$$(f) := \sum_{Y \subseteq X} v_Y(f) \cdot Y,$$

wobei die Summe über alle Primdivisoren läuft.

# Hauptdivisoren

## Fakt

Sei $X$ eine Varietät und $Y \subseteq X$ ein Primdivisor. Dann korrespondiert ein diskreter Bewertungsring $\mathcal{O}_Y$ und eine diskrete Bewertung $v_Y$ zu $Y$. Der Divisor $Y$ ist eindeutig durch $v_Y$ bestimmt.

## Lemma

Sei $0 \neq f$ eine reguläre Funktion auf $X$. Dann ist $v_Y(f) \in \mathbb{Z}$ für alle Primdivisoren $Y$ und $v_Y(f) \neq 0$ für nur endlich viele Primdivisoren.

## Definition

Sei $0 \neq f$ eine reguläre Funktion auf $X$. Der **Divisor** $(f)$ von $f$ ist definiert als

$$(f) := \sum_{Y \subseteq X} v_Y(f) \cdot Y,$$

wobei die Summe über alle Primdivisoren läuft. Divisoren dieser Form heißen **Hauptdivisoren**.

# Hauptdivisoren

## Beispiel

Sei $X$ eine (glatte) Kurve.

# Hauptdivisoren

## Beispiel

Sei $X$ eine (glatte) Kurve.
Dann ist $v_P$ gerade die Vielfachheit im Punkt $P$.

# Hauptdivisoren

## Beispiel

Sei $X$ eine (glatte) Kurve.
Dann ist $v_P$ gerade die Vielfachheit im Punkt $P$. Ist $f$ eine reguläre Funktion auf $X$, dann gilt lokal $f = g/h$ mit $g, h \in \mathbb{C}[X]$.

# Hauptdivisoren

## Beispiel

Sei $X$ eine (glatte) Kurve.
Dann ist $v_P$ gerade die Vielfachheit im Punkt $P$. Ist $f$ eine reguläre Funktion auf $X$, dann gilt lokal $f = g/h$ mit $g, h \in \mathbb{C}[X]$.
Punkte $P \in X$ mit $v_P(f) \neq 0$ sind die Nullstellen von $g$ und $h$.

# Hauptdivisoren

## Beispiel

Sei $X$ eine (glatte) Kurve.
Dann ist $v_P$ gerade die Vielfachheit im Punkt $P$. Ist $f$ eine reguläre Funktion auf $X$, dann gilt lokal $f = g/h$ mit $g, h \in \mathbb{C}[X]$.
Punkte $P \in X$ mit $v_P(f) \neq 0$ sind die Nullstellen von $g$ und $h$.
"Nullstellen" und "Pole" von $f$.

Divisoren

## Klassengruppen

Beispiel: Elliptische Kurven

Und jetzt?

# Klassengruppen

## Definition

Zwei Divisoren $D, D' \in \operatorname{Div} X$ heißen **linear äquivalent**, wenn $D - D'$ ein Hauptdivisor ist.

# Klassengruppen

## Definition

Zwei Divisoren $D, D' \in \operatorname{Div} X$ heißen **linear äquivalent**, wenn $D - D'$ ein Hauptdivisor ist.
Notation: $D \sim D'$.

# Klassengruppen

## Definition

Zwei Divisoren $D, D' \in \operatorname{Div} X$ heißen **linear äquivalent**, wenn $D - D'$ ein Hauptdivisor ist.
Notation: $D \sim D'$.
Die Gruppe $\operatorname{Div} X$ modulo die Gruppe der Hauptdivisoren ist die **Divisorenklassengruppe** $\operatorname{Cl} X$.

# Klassengruppen

## Definition

Zwei Divisoren $D, D' \in \operatorname{Div} X$ heißen **linear äquivalent**, wenn $D - D'$ ein Hauptdivisor ist.
Notation: $D \sim D'$.
Die Gruppe $\operatorname{Div} X$ modulo die Gruppe der Hauptdivisoren ist die **Divisorenklassengruppe** $\operatorname{Cl} X$.

## (Triviales) Beispiel

Ist $X = \mathbb{A}^n$, dann ist $\operatorname{Cl} X = 0$.

# Klassengruppen

## Definition

Zwei Divisoren $D, D' \in \operatorname{Div} X$ heißen **linear äquivalent**, wenn $D - D'$ ein Hauptdivisor ist.
Notation: $D \sim D'$.
Die Gruppe $\operatorname{Div} X$ modulo die Gruppe der Hauptdivisoren ist die **Divisorenklassengruppe** $\operatorname{Cl} X$.

## (Triviales) Beispiel

Ist $X = \mathbb{A}^n$, dann ist $\operatorname{Cl} X = 0$.

Allgemeiner: Ein noetherscher Ring $R$ ist UFD genau dann, wenn $\operatorname{Spec} R$ normal und $\operatorname{Cl}(\operatorname{Spec} R) = 0$.

# Klassengruppen

## Definition

Zwei Divisoren $D, D' \in \operatorname{Div} X$ heißen **linear äquivalent**, wenn $D - D'$ ein Hauptdivisor ist.
Notation: $D \sim D'$.
Die Gruppe $\operatorname{Div} X$ modulo die Gruppe der Hauptdivisoren ist die **Divisorenklassengruppe** $\operatorname{Cl} X$.

## (Triviales) Beispiel

Ist $X = \mathbb{A}^n$, dann ist $\operatorname{Cl} X = 0$.

Allgemeiner: Ein noetherscher Ring $R$ ist UFD genau dann, wenn $\operatorname{Spec} R$ normal und $\operatorname{Cl}(\operatorname{Spec} R) = 0$.

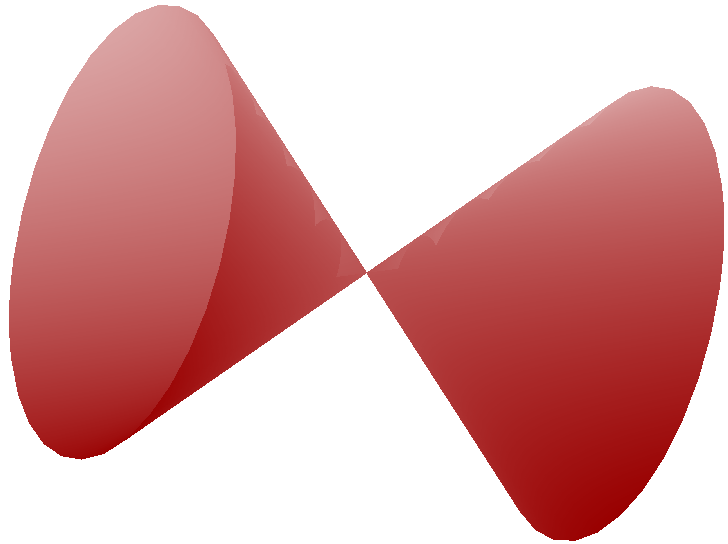
## Beispiel (für Zahlentheoretiker)

Ist $R$ ein Dedekindring, dann ist $\operatorname{Cl}(\operatorname{Spec} R)$ gerade die Idealklassengruppe von $R$.

# Klassengruppen

## Interessantes Beispiel

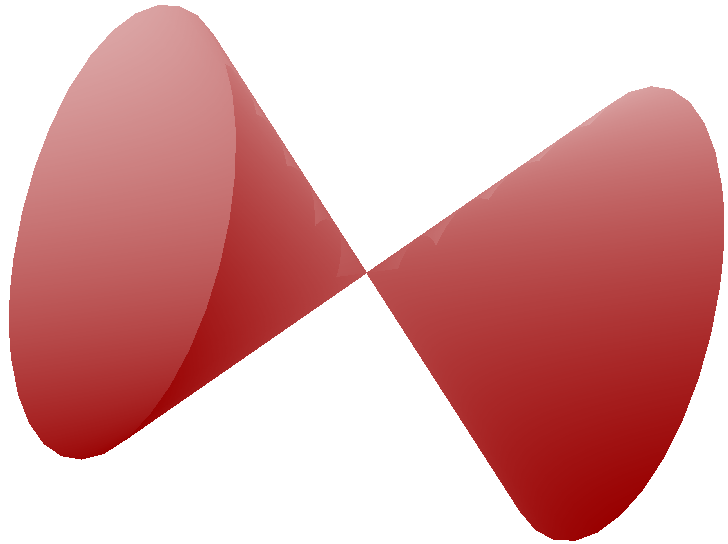
Sei $X = V(xy - z^2)$.



# Klassengruppen

## Interessantes Beispiel

Sei $X = V(xy - z^2)$. Dann gilt $\mathrm{Cl}\, X = C_2$.



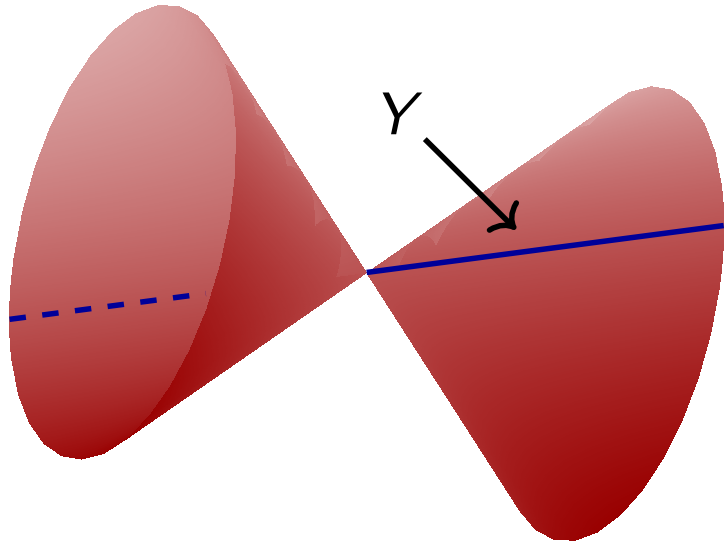
# Klassengruppen

## Interessantes Beispiel

Sei $X = V(xy - z^2)$. Dann gilt $\mathrm{Cl}\, X = C_2$.

## Beweisfragmente

Sei $Y = V(y, z) \subseteq X$.



# Klassengruppen

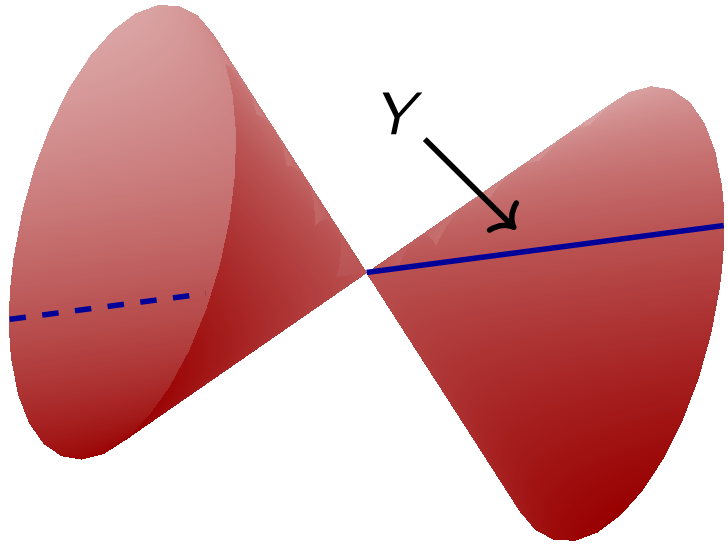
## Interessantes Beispiel

Sei $X = V(xy - z^2)$. Dann gilt $\mathrm{Cl}\, X = C_2$.

## Beweisfragmente

Sei $Y = V(y, z) \subseteq X$.

Exakte Sequenz: $\mathbb{Z} \xrightarrow{1 \mapsto 1 \cdot Y} \mathrm{Cl}\, X \longrightarrow \mathrm{Cl}(X - Y) \longrightarrow 0$.



# Klassengruppen

## Interessantes Beispiel

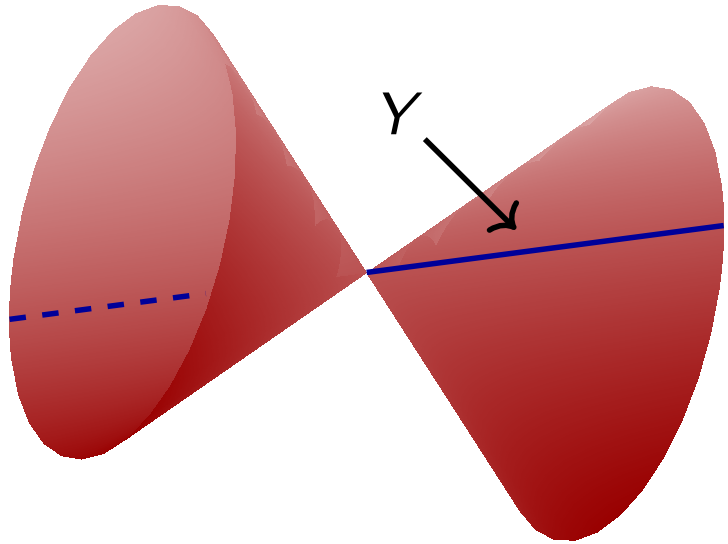
Sei $X = V(xy - z^2)$. Dann gilt $\mathrm{Cl}\, X = C_2$.

## Beweisfragmente

Sei $Y = V(y, z) \subseteq X$.

Exakte Sequenz: $\mathbb{Z} \xrightarrow{1 \mapsto 1 \cdot Y} \mathrm{Cl}\, X \longrightarrow \mathrm{Cl}(X - Y) \longrightarrow 0$.

Man kann zeigen: $Y$ ist kein Hauptdivisor, aber $2Y = (y)$.



# Klassengruppen

## Interessantes Beispiel

Sei $X = V(xy - z^2)$. Dann gilt $\mathrm{Cl}\, X = C_2$.

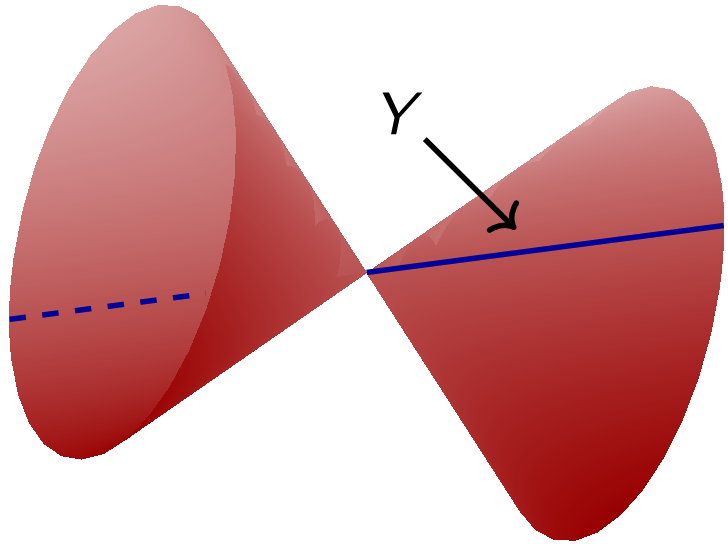
## Beweisfragmente

Sei $Y = V(y, z) \subseteq X$.

Exakte Sequenz: $\mathbb{Z} \xrightarrow{1 \mapsto 1 \cdot Y} \mathrm{Cl}\, X \longrightarrow \mathrm{Cl}(X - Y) \longrightarrow 0$.

Man kann zeigen: $Y$ ist kein Hauptdivisor, aber $2Y = (y)$.

Mit UFD-Fakt: $\mathrm{Cl}(X - Y) = 0$.



Divisoren

Klassengruppen

## Beispiel: Elliptische Kurven

Und jetzt?

# Elliptische Kurven

## Definition

Eine **elliptische Kurve** $C$ ist eine glatte Kurve von Geschlecht 1.

# Elliptische Kurven

## Definition

Eine **elliptische Kurve** $C$ ist eine glatte Kurve von Geschlecht 1.
Äquivalent: $C$ ist eine glatte Kurve mit Gleichung

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

$a_i \in \mathbb{C}$.

# Elliptische Kurven

## Definition

Eine **elliptische Kurve** $C$ ist eine glatte Kurve von Geschlecht 1.
Äquivalent: $C$ ist eine glatte Kurve mit Gleichung

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

$a_i \in \mathbb{C}$.

Affine Gleichung: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ oder kurz $y^2 = x^3 + ax + b$.

# Elliptische Kurven

## Definition

Eine **elliptische Kurve** $C$ ist eine glatte Kurve von Geschlecht 1.
Äquivalent: $C$ ist eine glatte Kurve mit Gleichung

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

$a_i \in \mathbb{C}$.

Affine Gleichung: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ oder kurz $y^2 = x^3 + ax + b$. Glatt genau dann, wenn $-4a^3 - 27b^2 \neq 0$.

# Elliptische Kurven

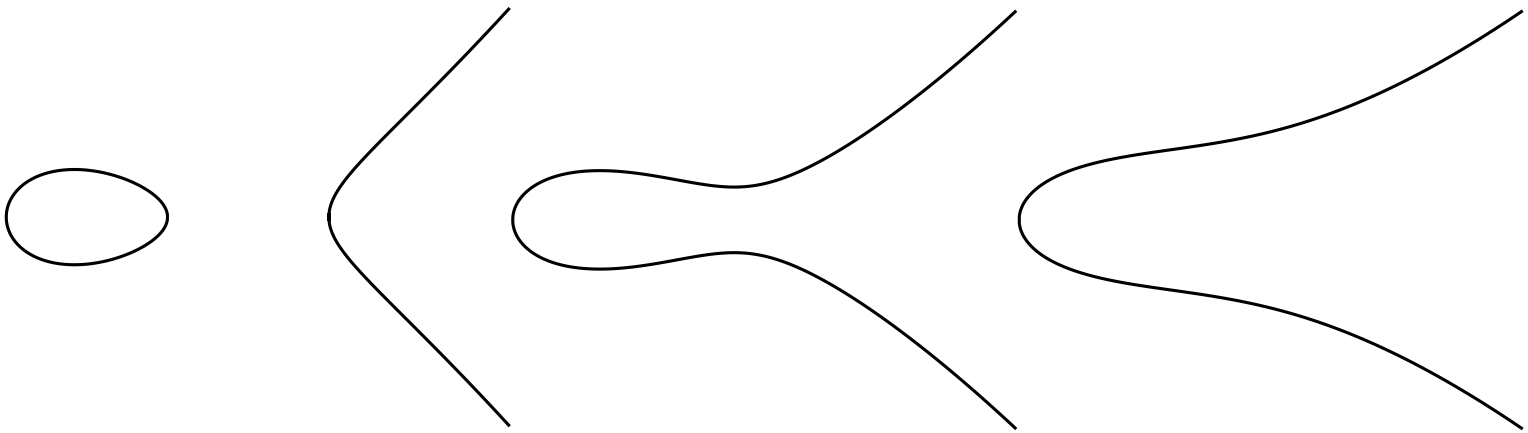
## Definition

Eine **elliptische Kurve** $C$ ist eine glatte Kurve von Geschlecht 1.
Äquivalent: $C$ ist eine glatte Kurve mit Gleichung

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

$a_i \in \mathbb{C}$.

Affine Gleichung: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ oder kurz $y^2 = x^3 + ax + b$. Glatt genau dann, wenn $-4a^3 - 27b^2 \neq 0$.



(a) $y^2 = x^3 - 2x$ (b) $y^2 = x^3 - x + 1$ (c) $y^2 = x^3 + 2x + 4$

# Elliptische Kurven

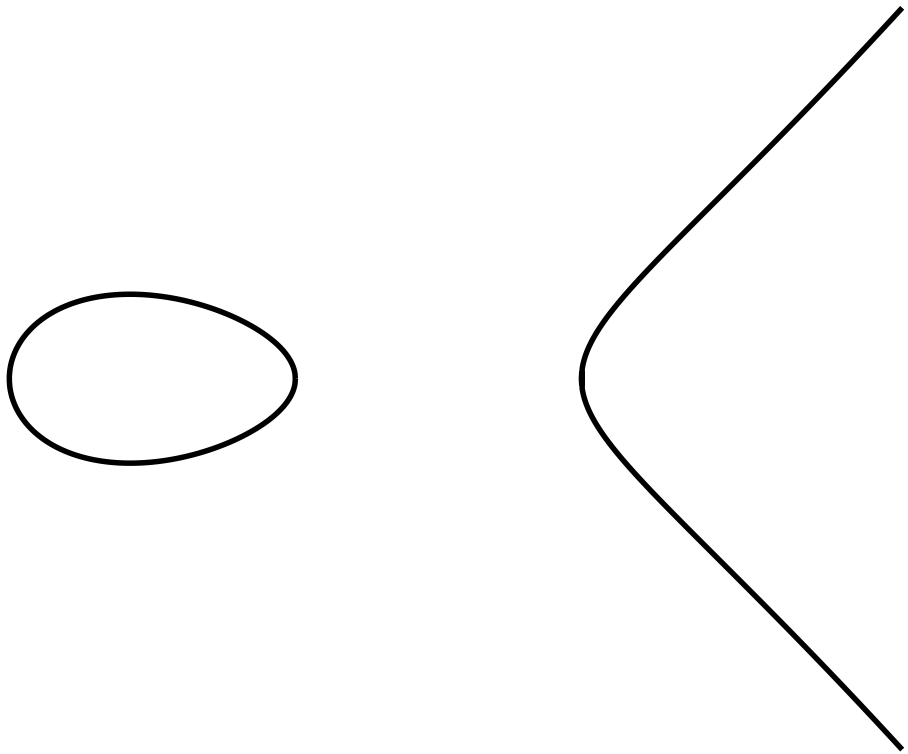
Punkte einer Elliptischen Kurve bilden eine abelsche Gruppe.

# Elliptische Kurven

Punkte einer Elliptischen Kurve bilden eine abelsche Gruppe.
Neutrales Element: $\infty$, (aka $[0:0:1]$).

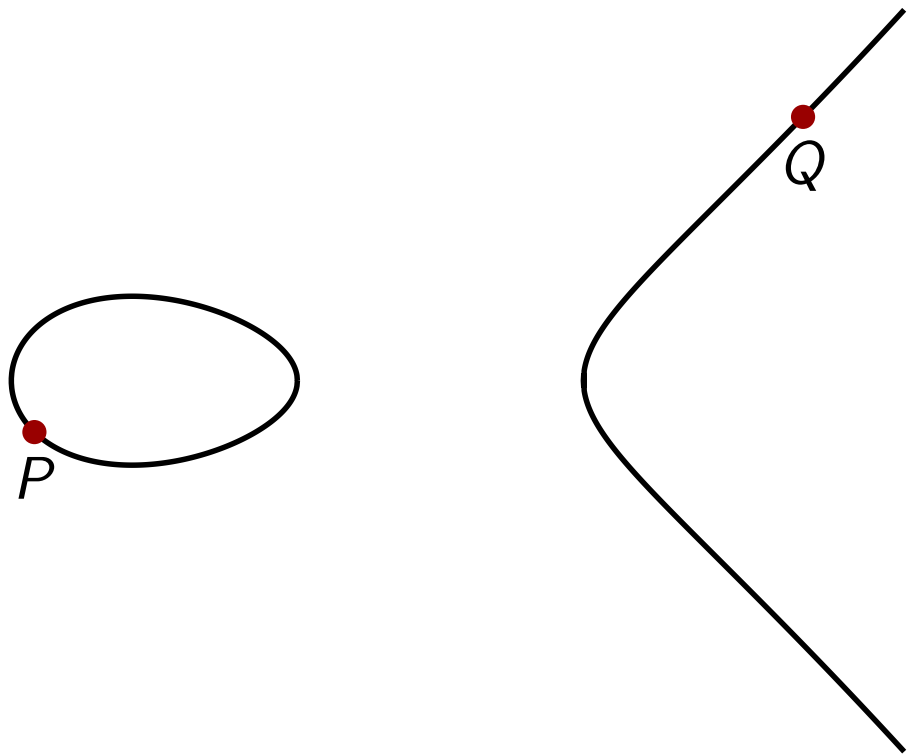
# Elliptische Kurven

Punkte einer Elliptischen Kurve bilden eine abelsche Gruppe.
Neutrales Element: $\infty$, (aka $[0 : 0 : 1]$).



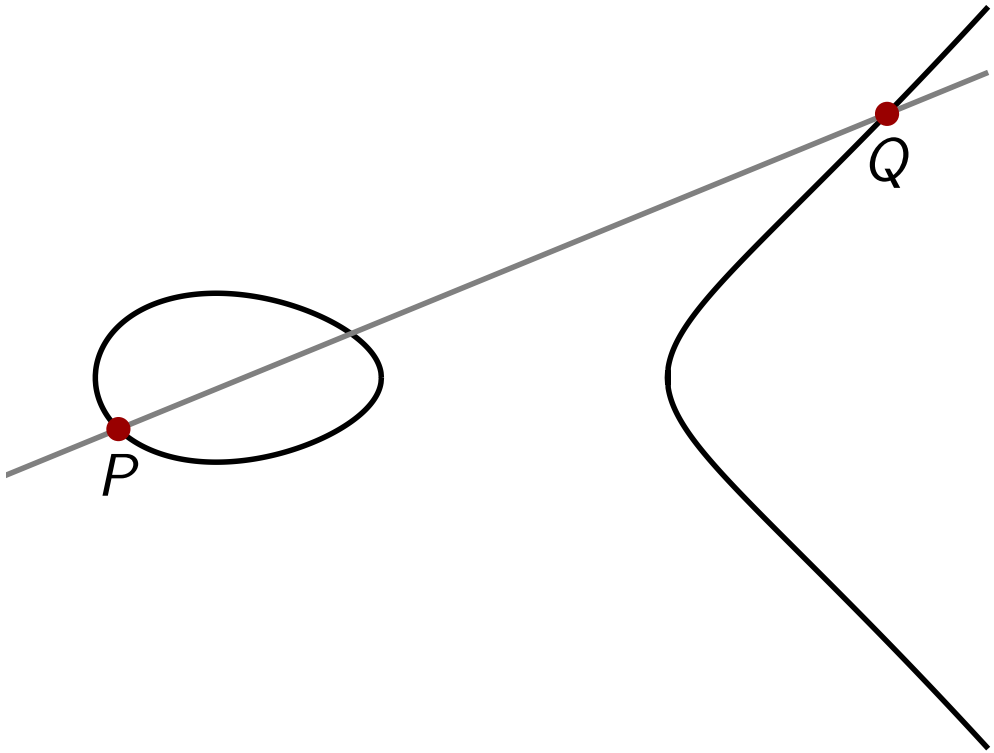
# Elliptische Kurven

Punkte einer Elliptischen Kurve bilden eine abelsche Gruppe.
Neutrales Element: $\infty$, (aka $[0:0:1]$).



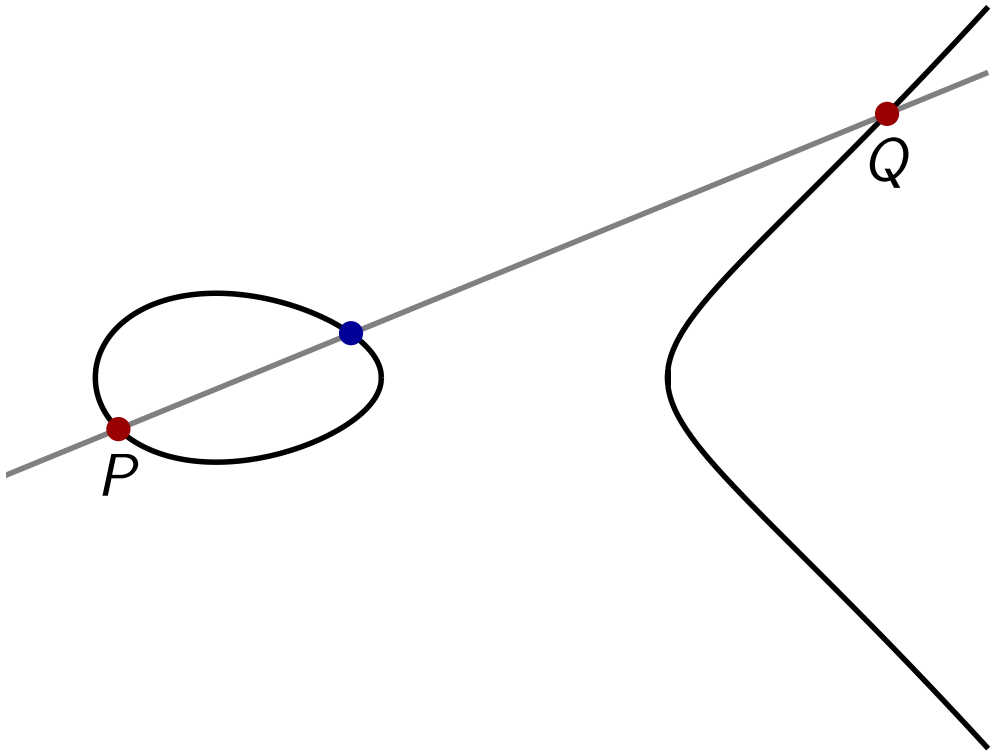
# Elliptische Kurven

Punkte einer Elliptischen Kurve bilden eine abelsche Gruppe.
Neutrales Element: $\infty$, (aka $[0:0:1]$).



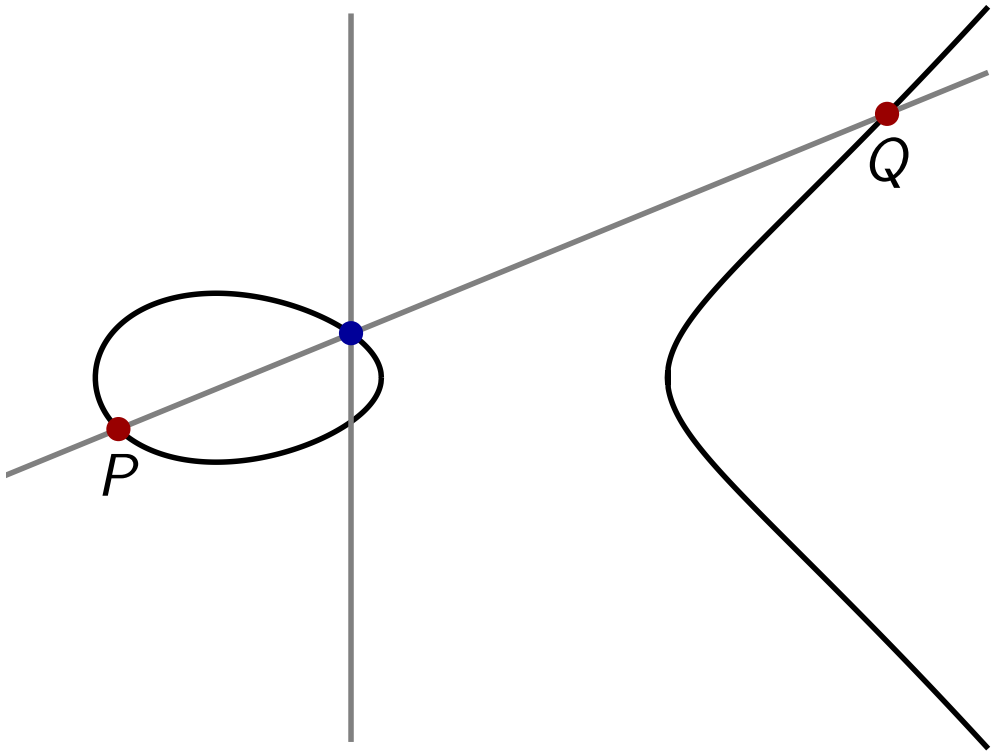
# Elliptische Kurven

Punkte einer Elliptischen Kurve bilden eine abelsche Gruppe.
Neutrales Element: $\infty$, (aka $[0:0:1]$).



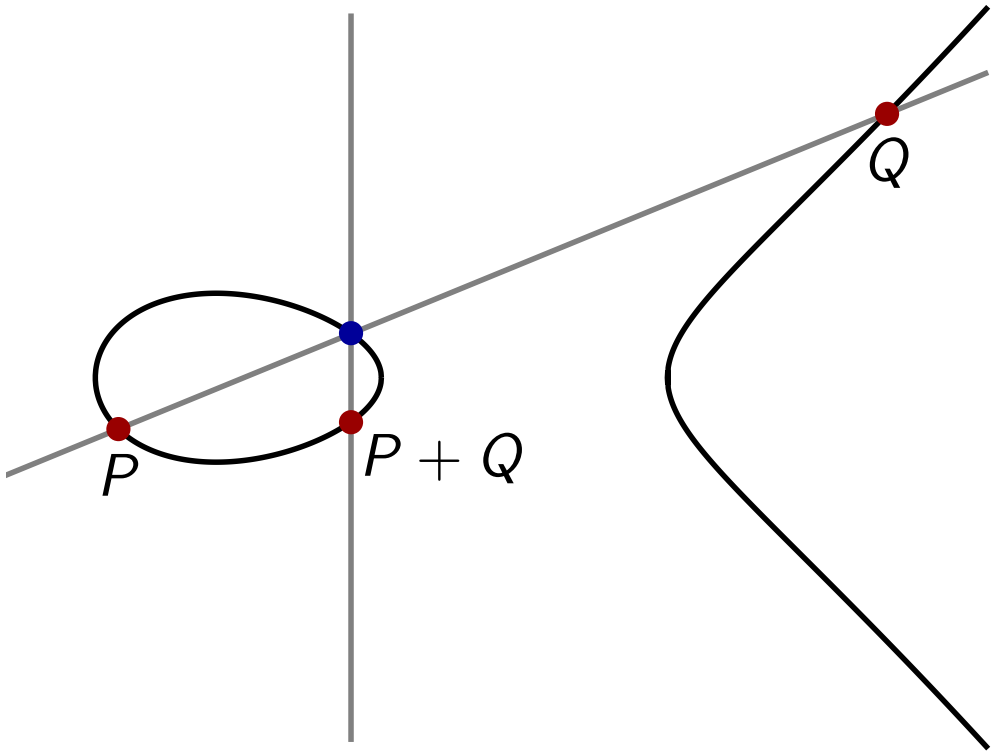
# Elliptische Kurven

Punkte einer Elliptischen Kurve bilden eine abelsche Gruppe.
Neutrales Element: $\infty$, (aka $[0:0:1]$).



# Elliptische Kurven

Punkte einer Elliptischen Kurve bilden eine abelsche Gruppe.
Neutrales Element: $\infty$, (aka $[0:0:1]$).



# Hä?

Gerade durch . . .

Spiegeln . . .

Wer kommt auf sowas?

Ist das jetzt nur Zufall,
dass das geht?

# Hä?

Gerade durch . . .

Spiegeln . . .

# Die Wahrheit

Wer kommt auf sowas?

Ist das jetzt nur Zufall,
dass das geht?

# Die Wahrheit

Sei $C$ eine elliptische Kurve.

# Die Wahrheit

Sei $C$ eine elliptische Kurve.

## Definition

Der **Grad** eines Divisors $D = \sum_{i=1}^{k} n_i P_i$ auf $C$ ist definitert als $\deg D = \sum_{i=1}^{k} n_i$.

# Die Wahrheit

Sei $C$ eine elliptische Kurve.

## Definition

Der **Grad** eines Divisors $D = \sum_{i=1}^{k} n_i P_i$ auf $C$ ist definitert als $\deg D = \sum_{i=1}^{k} n_i$.

## Fakt

Ein Hauptdivisor hat Grad 0.

# Die Wahrheit

Sei $C$ eine elliptische Kurve.

## Definition

Der **Grad** eines Divisors $D = \sum_{i=1}^{k} n_i P_i$ auf $C$ ist definitert als $\deg D = \sum_{i=1}^{k} n_i$.

## Fakt

Ein Hauptdivisor hat Grad 0.

Es gibt also eine wohldefinierte Abbildung $\deg : \mathrm{Cl}\, C \to \mathbb{Z}$.

# Die Wahrheit

Sei $C$ eine elliptische Kurve.

## Definition

Der **Grad** eines Divisors $D = \sum_{i=1}^{k} n_i P_i$ auf $C$ ist definitert als $\deg D = \sum_{i=1}^{k} n_i$.

## Fakt

Ein Hauptdivisor hat Grad 0.

Es gibt also eine wohldefinierte Abbildung $\deg : \mathrm{Cl}\, C \to \mathbb{Z}$. Sei $\mathrm{Cl}^0\, C$ der Kern dieser Abbildung.

# Die Wahrheit

## Fakt

Es gibt eine Bijektion zwischen den Punkten von $C$ und den Elementen von $\mathrm{Cl}^0\, C$.

# Die Wahrheit

**Fakt**

Es gibt eine Bijektion zwischen den Punkten von $C$ und den Elementen von $\mathrm{Cl}^0\, C$.

**Beweisidee.**

Bilde einen Punkt $P \in C$ auf $P - \infty$ ab.

# Die Wahrheit

## Fakt

Es gibt eine Bijektion zwischen den Punkten von $C$ und den Elementen von $\mathrm{Cl}^0\, C$.

## Beweisidee.

Bilde einen Punkt $P \in C$ auf $P - \infty$ ab.
Für Surjektivität: Gemäß Satz von Riemann-Roch existiert ein Punkt linear äquivalent zu $D + \infty$ für jeden Divisor $D$ mit $\deg D = 0$.

# Die Wahrheit

## Fakt

Es gibt eine Bijektion zwischen den Punkten von $C$ und den Elementen von $\mathrm{Cl}^0\, C$.

## Beweisidee.

Bilde einen Punkt $P \in C$ auf $P - \infty$ ab.
Für Surjektivität: Gemäß Satz von Riemann-Roch existiert ein Punkt linear äquivalent zu $D + \infty$ für jeden Divisor $D$ mit $\deg D = 0$.
Für Injektivität: Gilt $P \sim Q$ für $P, Q \in C$, dann wäre $C$ birational zu $\mathbb{P}^1$, aber $C$ ist von Geschlecht 1. □

Divisoren

Klassengruppen

Beispiel: Elliptische Kurven

Und jetzt?

# Und jetzt?

## Cartier-Divisoren

Verallgemeinerung von Weil-Divisoren auf beliebige Schemata.

# Und jetzt?

## Cartier-Divisoren

Verallgemeinerung von Weil-Divisoren auf beliebige Schemata.
Hier: Cartier-Divisoren bilden Untergruppe ("lokale Hauptdivisoren").

# Und jetzt?

## Cartier-Divisoren

Verallgemeinerung von Weil-Divisoren auf beliebige Schemata.
Hier: Cartier-Divisoren bilden Untergruppe ("lokale Hauptdivisoren").
Aber: nicht jeder Cartier-Divisor ist Weil-Divisor.

# Und jetzt?

## Cartier-Divisoren

Verallgemeinerung von Weil-Divisoren auf beliebige Schemata.
Hier: Cartier-Divisoren bilden Untergruppe ("lokale Hauptdivisoren").
Aber: nicht jeder Cartier-Divisor ist Weil-Divisor.

Für Zahlentheoretiker: Nicht-maximale Ordnungen haben keine Klassengruppe aber eine Picard-Gruppe.

# Und jetzt?

## Cartier-Divisoren

Verallgemeinerung von Weil-Divisoren auf beliebige Schemata.
Hier: Cartier-Divisoren bilden Untergruppe ("lokale Hauptdivisoren").
Aber: nicht jeder Cartier-Divisor ist Weil-Divisor.

Für Zahlentheoretiker: Nicht-maximale Ordnungen haben keine Klassengruppe aber eine Picard-Gruppe.

## Cox Ringe

Ring von regulären Funktionen auf $X$ der mit $\mathrm{Cl}\, X$ graduiert ist.

# Und jetzt?

## Cartier-Divisoren

Verallgemeinerung von Weil-Divisoren auf beliebige Schemata.
Hier: Cartier-Divisoren bilden Untergruppe ("lokale Hauptdivisoren").
Aber: nicht jeder Cartier-Divisor ist Weil-Divisor.

Für Zahlentheoretiker: Nicht-maximale Ordnungen haben keine Klassengruppe aber eine Picard-Gruppe.

## Cox Ringe

Ring von regulären Funktionen auf $X$ der mit $\mathrm{Cl}\, X$ graduiert ist.
Nächstes Mal!