Elliptische Kurven Kryptographie

Kevin Kappelmann, Lukas Stevens

Technische Universität München

26. Mai 2016

Überblick

Definition affiner Ebenen

Definition

Es sei $\mathcal{A}$ eine Menge von Punkten und $\mathcal{G}$ eine Menge von Geraden mit $\mathcal{G} \subseteq Pot(A)$. Bei $(\mathcal{A}, \mathcal{G})$ handelt es sich um eine affine Ebene, wenn folgende Bedingungen erfüllt sind:

1. Zu je zwei Elementen $a, b \in \mathcal{A}$ mit $a \neq b$ existiert genau ein $G \in \mathcal{G}$ mit $a, b \in G$.
2. Zu $G \in \mathcal{G}$ und $a \in \mathcal{A} \setminus G$ existiert genau ein $G' \in \mathcal{G}$ mit $a \in G'$ und $G \cap G' = \emptyset$.
3. Es existieren drei Elemente $a, b, c \in \mathcal{A}$ mit $c \notin \overline{a, b}$.

Definition projektiver Ebenen

Definition

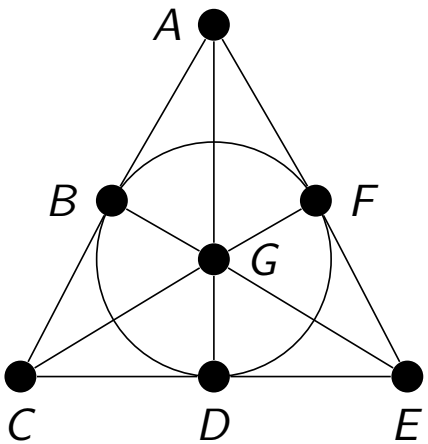
Es sei $\mathcal{A}$ eine Menge von Punkten und $\mathcal{G}$ eine Menge von Geraden mit $\mathcal{G} \subseteq Pot(A)$. Bei $(\mathcal{A}, \mathcal{G})$ handelt es sich um eine projektive Ebene, wenn folgende Bedingungen erfüllt sind:

1. Zu je zwei Elementen $P, Q \in \mathcal{P}$ mit $P \neq Q$ existiert genau ein $G \in \mathcal{G}$ mit $P, Q \in G$.
2. Für je zwei $G, H \in \mathcal{G}$ mit $G \neq H$ gilt $|G \cap H| = 1$.
3. Es existieren vier verschiedene Elemente in $\mathcal{P}$, sodass immer höchstens zwei davon in jedem beliebigen $G \in \mathcal{G}$ liegen.

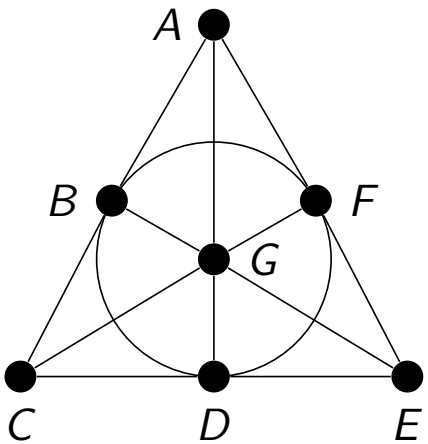
PG(2, $\mathbb{F}$)

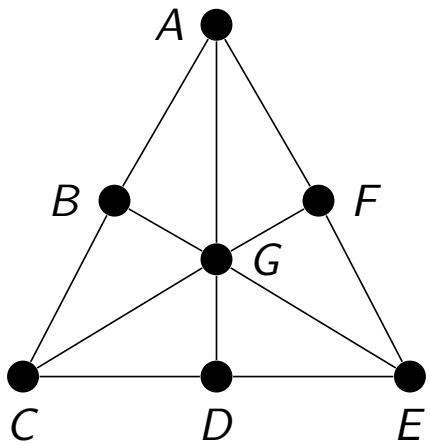
Konstruktion affiner Ebenen aus projektiven Ebenen

Konstruktion affiner Ebenen aus projektiven Ebenen

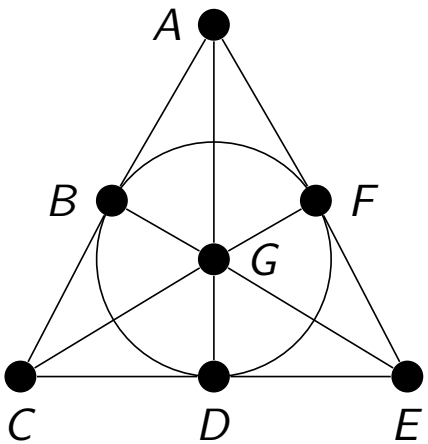


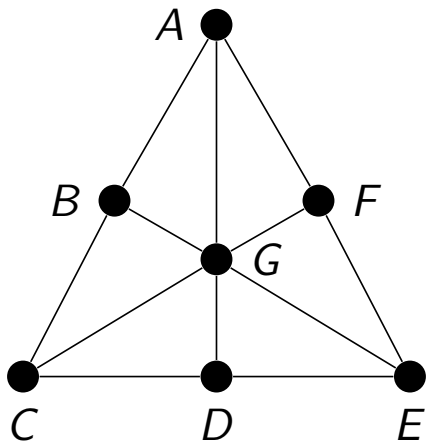
Konstruktion affiner Ebenen aus projektiven Ebenen

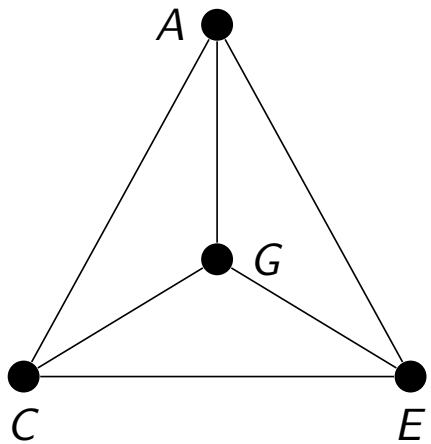




Konstruktion affiner Ebenen aus projektiven Ebenen

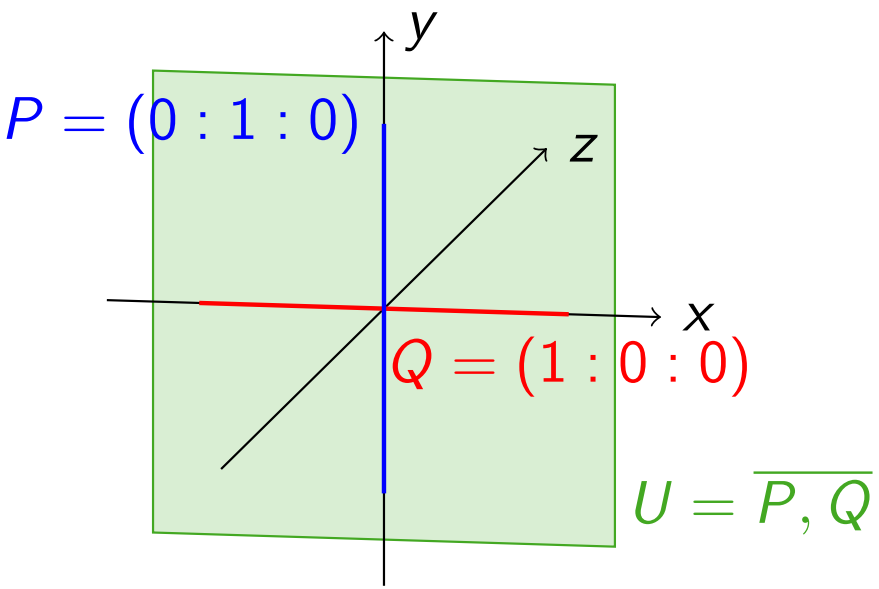






Elliptische Kurven - Die unendlich ferne Gerade

- Wähle $U := \overline{P, Q}$ mit $P = (1 : 0 : 0), Q = (0 : 1 : 0)$.
- U ist im dreidimensionalen Raum genau die x,y-Ebene mit $z = 0$.



- Wir bezeichnen U als die **unendlich ferne Gerade**.

Paragraphs of Text

Sed iaculis dapibus gravida. Morbi sed tortor erat, nec interdum arcu. Sed id lorem lectus. Quisque viverra augue id sem ornare non aliquam nibh tristique. Aenean in ligula nisl. Nulla sed tellus ipsum. Donec vestibulum ligula non lorem vulputate fermentum accumsan neque mollis.

Sed diam enim, sagittis nec condimentum sit amet, ullamcorper sit amet libero. Aliquam vel dui orci, a porta odio. Nullam id suscipit ipsum. Aenean lobortis commodo sem, ut commodo leo gravida vitae. Pellentesque vehicula ante iaculis arcu pretium rutrum eget sit amet purus. Integer ornare nulla quis neque ultrices lobortis. Vestibulum ultrices tincidunt libero, quis commodo erat ullamcorper id.

Bullet Points

- Lorem ipsum dolor sit amet, consectetur adipiscing elit
- Aliquam blandit faucibus nisi, sit amet dapibus enim tempus eu
- Nulla commodo, erat quis gravida posuere, elit lacus lobortis est, quis porttitor odio mauris at libero
- Nam cursus est eget velit posuere pellentesque
- Vestibulum faucibus velit a augue condimentum quis convallis nulla gravida

Blocks of Highlighted Text

Block 1

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Integer lectus nisl, ultricies in feugiat rutrum, porttitor sit amet augue. Aliquam ut tortor mauris. Sed volutpat ante purus, quis accumsan dolor.

Block 2

Pellentesque sed tellus purus. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Vestibulum quis magna at risus dictum tempor eu vitae velit.

Block 3

Suspendisse tincidunt sagittis gravida. Curabitur condimentum, enim sed venenatis rutrum, ipsum neque consectetur orci, sed blandit justo nisi ac lacus.

Multiple Columns

Heading

1. Statement
2. Explanation
3. Example

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Integer lectus nisl, ultricies in feugiat rutrum, porttitor sit amet augue. Aliquam ut tortor mauris. Sed volutpat ante purus, quis accumsan dolor.

Table

Treatments	**Response 1**	**Response 2**
Treatment 1	0.0003262	0.562
Treatment 2	0.0015681	0.910
Treatment 3	0.0009271	0.296

Tabelle: Table caption

Theorem

Satz (Mass–energy equivalence)

$E = mc^2$

Verbatim

Beispiel (Theorem Slide Code)

```
\begin{frame}
    \frametitle{Theorem}
    \begin{theorem}[Mass--energy equivalence]
        $E = mc^2$
    \end{theorem}
\end{frame}
```

Figure

Uncomment the code on this slide to include your own image from the same directory as the template TeX file.

References

John Smith (2012)

Title of the publication

Journal Name 12(3), 45 – 678.

The End