Prof. Dr. H. Brenner **Osnabrück WS 2021/2023**

Elliptische Kurven

Vorlesung 7

Die zuletzt besprochene Gruppenstruktur ist eine Abbildung

$$+\colon E(K) \times E(K) \longrightarrow E(K),$$

die durch rationale Ausdrücke, also Quotienten aus Polynomen gegeben sind. Dabei haben wir auch gesehen, dass diese Darstellung als Quotient, anders als nach Kürzung bei einem Polynomring, nicht eindeutig ist. Entsprechend sind die Negationsabbildung

$$E(K) \longrightarrow E(K),\ P \longmapsto -P$$

und die Vervielfachungen

$$[m]\colon E(K) \longrightarrow E(K),\ P \longmapsto mP$$

durch rationale Ausdrücke geben. Eine elliptische Kurve in Weierstraßform kann man auf die projektive Gerade projizieren, indem man nur die x-Koordinate betrachtet (bzw. projektiv $(x,y,z) \mapsto (x,z)$ betrachtet). All diese Abbildungen werden in der Welt der Varietäten durch eine geeignete Klasse von Abbildungen beschrieben, den Morphismen. Da wir in diesem Kurs weder die Garben- noch die Schematheorie systematisch entwickeln, werden wir im Folgenden den Grundkörper als algebraisch abgeschlossen voraussetzen und die meisten Resultate nicht beweisen. Dagegen betonen wir, wie in der Welt der Kurven Morphismen mit Körpererweiterungen der Funktionenkörper zusammenhängen. Im Fall eines nicht algebraisch abgeschlossenen Körpers sind die Begriffe so zu verstehen, dass sie nach Übergang zu einem algebraischen Abschluss gelten.

Reguläre Funktionen

Definition 7.1. Es sei K ein algebraisch abgeschlossener Körper und sei $V = V(\mathfrak{a}) \subseteq \mathbb{A}^n_K$ eine affine Varietät. Es sei $P \in V$ ein Punkt, $U \subseteq V$ eine Zariski-offene Menge mit $P \in U$ und es sei $f\colon U \to \mathbb{A}^1_K = K$ eine Funktion. Dann heißt f *algebraisch* (oder *regulär* oder *polynomial*) im Punkt P, wenn es Elemente $G, H \in R = K[X_1, \ldots, X_n]/\mathfrak{a}$ gibt mit $P \in D(H) \subseteq U$ und mit

$$f(Q) = \frac{G(Q)}{H(Q)} \text{ für alle } Q \in D(H)\,.$$

Die Funktion f heißt *algebraisch* (oder *algebraisch auf* U), wenn f in jedem Punkt von U algebraisch ist.

Sämtliche Polynome aus $K[X_1, \ldots, X_n]$ kann man direkt als reguläre Funktionen auf einer affinen Teilmenge

$$V(\mathfrak{a}) \subseteq \mathbb{A}_K^n$$

und ebenso auf einer jeden offenen Teilmenge $U \subseteq V(\mathfrak{a})$ auffassen. Hier braucht man keine Nenner und auch keine von den Punkten abhängige Darstellung. Man kann sogar zeigen, dass auf einer affinen Varietät die Menge der regulären Funktionen mit dem Restklassenring $R = K[X_1, \ldots, X_n]/\mathfrak{a}$ übereinstimmt, falls $\mathfrak{a}$ ein Radikalideal ist, siehe Satz 14.9 (Algebraische Kurven (Osnabrück 2017-2018)).

Die Beschreibung der regulären Funkionen auf einer offenen Teilmenge

$$U \subseteq V(\mathfrak{a}) \subseteq \mathbb{A}_K^n$$

ist besonders einfach, wenn der affine Koordinatenring $K[X_1, \ldots, X_n]/\mathfrak{a}$ faktoriell ist, da dann die Bruchdarstellung G/H nach Kürzung eindeutig ist. Der maximale Definitionsbereich von G/H ist gleich $D(H)$.

Beispiel 7.2. Zu einer elliptischen Kurve in affiner kurzer Weierstraßform

$$y^2 = x^3 + ax + b = (x - \lambda_1)(x - \lambda_2)(x - \lambda_3)$$

besitzen die regulären Funktionen auf einer offenen Menge im Allgemeinen keine eindeutige Darstellung als Bruch. Die Kurvengleichung kann man beispielsweise direkt als

$$\frac{y}{x - \lambda_1} = \frac{(x - \lambda_2)(x - \lambda_3)}{y}$$

interpretieren, und dies ergibt eine reguläre Funktion auf $D(x - \lambda_1, y)$. Diese Funktion ist allein im Punkt $(\lambda_1, 0)$ nicht definiert.

Definition 7.3. Es sei K ein algebraisch abgeschlossener Körper, $Y \subseteq \mathbb{P}_K^n$ eine projektive Varietät, $U \subseteq Y$ eine offene Teilmenge und $P \in U$ ein Punkt. Dann heißt eine Funktion

$$f\colon U \longrightarrow \mathbb{A}_K^1 = K$$

algebraisch (oder *regulär* oder *polynomial*) im Punkt P, wenn es eine offene affine Umgebung

$$P \in V \subseteq U$$

derart gibt, dass die auf V die eingeschränkte Funktion $f|_V$ algebraisch im Punkt P ist. f heißt *algebraisch* auf U, wenn f in jedem Punkt aus U algebraisch ist.

Zu einer offenen Menge U bildet die Menge der auf U definierten regulären Funktionen wieder eine kommutative K-Algebra, die mit $\Gamma(U, \mathcal{O}_X)$ bezeichnet wird. Zu offenen Teilmengen $V \subseteq U$ gibt es die natürliche Restriktionsabbildung

$$\Gamma(U, \mathcal{O}_X) \longrightarrow \Gamma(V, \mathcal{O}_X),$$

die ein Ringhomomorphismus ist. Von nun an verstehen wir unter einer projektiven Varietät ein projektives Nullstellengebilde zusammen mit der induzierten Zariski-Topologie und versehen mit der *Strukturgarbe* $\mathcal{O}_X$ der regulären Funktionen. Diese Konzepte übertragen sich sofort auf offene Teilmengen, was zum Begriff der quasiprojektiven Varietät führt.

Definition 7.4. Eine offene Teilmenge einer projektiven Varietät zusammen mit der induzierten Zariski-Topologie und versehen mit der Strukturgarbe der algebraischen Funktionen nennt man eine *quasiprojektive Varietät*.

Insbesondere ist eine projektive Varietät aber auch eine affine Varietät quasiprojektiv. Letzteres folgt daraus, dass man eine affine Varietät $Y \subseteq \mathbb{A}_K^n$ zu einer projektiven Varietät $\tilde{Y} \subseteq \mathbb{P}_K^n$ fortsetzen kann, in der Y eine offene Teilmenge ist.

Funktionenkörper

Zu einer irreduziblen quaiprojektiven Varietät X über einem algebraisch abgeschlossenen Körper kann man reguläre Funktionen $f \in \Gamma(U, \mathcal{O}_X)$ und $g \in \Gamma(V, \mathcal{O}_X)$ auf nichtleeren offenen Mengen $U, V \subseteq X$ miteinander addieren und multiplizieren, indem man beide Funktion über die Restriktionen in $\Gamma(U \cap V, \mathcal{O}_X)$ auffasst, wobei $U \cap V$ ebenfalls nicht leer ist, und dort die Operationen durchführt. Dabei muss man reguläre Funktionen mit ihren Einschränkungen auf nichtleeren Teilmengen identifizieren (diese natürliche Identifzierung ist im Folgenden mit Kolimes gemeint). Diese Überlegung ist die Grundlage für die folgende Definition.

Definition 7.5. Es sei X eine irreduzible quasiprojektive Varietät. Dann ist der Kolimes der $\Gamma(U, \mathcal{O}_X)$ über alle nichtleeren offenen Mengen $U \subseteq X$ ein Körper, den man den *Funktionenkörper* von X nennt.

Wir bezeichnen den Funktionenkörper zumeist mit $Q(X)$. Die Körpereigenschaft beruht darauf, dass man von einer Darsellung $f = G/H$ (mit $G, H \neq 0$) auf einer affinen Teilmenge ausgehen kann und dann auf der Teilmenge davon, die entsteht, wenn man die Nullstellenmenge von G herausnimmt, die reguläre Funktion $f^{-1} = H/G$ zur Verfügung hat.

Bei einer irreduziblen Varietät liegen alle auf irgendwelchen offenen Mengen definierten regulären Funktionen in dem einen Funktionenkörper. Wenn $U \subseteq X$ eine offene affine Teilmenge mit globalem Schnittring R ist, so ist der Funktionenkörper gleich dem Quotientenkörper von R. Für eine elliptische Kurve in Weierstraßform ist der Funktionenkörper gleich $Q(K[x,y]/(y^2 - x^3 - ax - b))$. Das ist eine endliche Körpererweiterung vom Grad 2 über dem Körper der rationalen Funktionen $K(x)$.

Im Fall einer irreduziblen Varietät X der Dimension d ist der Funktionenkörper zu X ein Körper über K mit dem Transzendenzgrad d, d.h. es

gibt eine endliche Körpererweiterung $K(T_1, \ldots, T_n) \subseteq Q(V)$. Speziell haben bei irreduziblen Kurven die Funktionenkörper den Transzendenzgrad 1. Im Kurvenfall gilt sogar der folgende Satz.

Satz 7.6. *Es sei K ein algebraisch abgeschlossener Körper. Dann gibt es eine Entsprechung zwischen den glatten projektiven Kurven über K und den Körpern über K vom Transzendenzgrad 1.*

Ohne die beiden Voraussetzungen glatt und projektiv stimmt diese Aussage hochgradig nicht. Man sollte diese Aussage als einen deutlichen Hinweis darauf verstehen, dass die Eigenschaften glatt und projektiv eine optimale geometrische Realisierung des Funktionenkörpers liefern. Die Grundidee für den Beweis dieses Satzes ist, in dem Körper Q mit Transzendenzgrad 1 die Menge aller diskreten Bewertungsringe oberhalb von K zu nehmen und aus diesen die Punkte einer Kurve zu machen.

In höherer Dimension gilt die Aussage nicht, man kann zwar jede Körpererweiterung von K mit endlichem Transzendenzgrad d als Funktionenkörper einer d-dimensionalen (auch projektiven) Varietät realisieren. Man kann auch, zumindest in Charakteristik 0 (Singularitätenauflösung) Glattheit erreichen, es gibt aber verschiedene konkurrierende Modelle. Die Menge aller diskreten Bewertungsringe ist hier viel zu groß und kann nicht zu einer Varietät gemacht werden.

Morphismen

Definition 7.7. Es seien X und Y quasiprojektive Varietäten über einem algebraisch abgeschlossenen Körper und sei

$$\psi\colon\ Y \longrightarrow X$$

eine stetige Abbildung. Dann nennt man ψ einen *Morphismus* (von quasiprojektiven Varietäten), wenn für jede offene Teilmenge $U \subseteq X$ und jede algebraische Funktion $f \in \Gamma(U, \mathcal{O}_X)$ gilt, dass die zusammengesetzte Funktion

$$f \circ \psi : \psi^{-1}(U) \longrightarrow U \xrightarrow{f} \mathbb{A}^1_K$$

zu $\Gamma(\psi^{-1}(U), \mathcal{O}_Y)$ gehört.

Jede reguläre Funktion auf U definiert einen Morphismus

$$U \longrightarrow \mathbb{A}^1_K.$$

Ein Morphismus

$$U \longrightarrow \mathbb{A}^n_K$$

ist nichts anderes als ein Tupel von n regulären Funktionen. Ein Morphismus

$$U \longrightarrow V(\mathfrak{a}) \subseteq \mathbb{A}^n_K$$

ist einfach ein Morphismus nach $\mathbb{A}_K^n$, dessen Bild in der abgeschlossenen Teilmenge $V(\mathfrak{a})$ landet. Für affine Varietäten

$$X = V(\mathfrak{a}) \subseteq \mathbb{A}_K^n$$

und

$$Y = V(\mathfrak{b}) \subseteq \mathbb{A}_K^m$$

ist ein Morphismus

$$V(\mathfrak{b}) \longrightarrow V(\mathfrak{a})$$

äquivalent zu einem K-Algebrahomomorphismus

$$K[X_1, \ldots, X_n]/\mathfrak{a} \longrightarrow K[Y_1, \ldots, Y_m]/\mathfrak{b},$$

also gegeben durch n Polynome P_i in m Variablen Y_j, die $F(P_1, \ldots, P_n) \in \mathfrak{b}$ für $F \in \mathfrak{a}$ erfüllen müssen. Da ein Morphismus ein lokales Konzept ist, kann man einen Morphismus

$$Y \longrightarrow X$$

auf diese affine Situation zurückführen. Zu einer offenen affinen Überdeckung

$$X = \bigcup_{i \in I} U_i$$

und einer affinen Überdeckung

$$\psi^{-1}(U_i) = \bigcup_{j \in J_i} V_j$$

muss

$$V_j \longrightarrow U_i$$

ein Morphismus zwischen affinen Varietäten sein, also durch einen Ringhomomorphismus zwischen K-Algebren und damit durch Polynome festgelegt sein.

Zu irreduziblen Varietäten X, Y und einem Morphismus

$$\psi\colon\ Y \longrightarrow X$$

mit der Eigenschaft, dass das Bild von Y in X dicht ist, ist zu jeder offenen Teilmenge $U \subseteq X$ der Ringhomomorphismus

$$\Gamma(U, \mathcal{O}_X) \longrightarrow \Gamma(\psi^{-1}(U), \mathcal{O}_Y)$$

injektiv ist. In dieser Situation erhält man einen Ringhomomorphismus

$$Q(X) \longrightarrow Q(Y)$$

der zugehörigen Funktionenkörper.

Bemerkung 7.8. Eine glatte Varietät X über $\mathbb{C}$ kann man als eine komplexe Mannigfaltigkeit X^h auffassen, wobei sich die komplexe (feine) Topologie und die holomorphe Struktur lokal aus der Situation

$$V(\mathfrak{a}) \subseteq \mathbb{A}_{\mathbb{C}}^n = \mathbb{C}^n$$

ergibt. Zu einem Morphismus

$$\psi\colon\ Y \longrightarrow X$$

zwischen glatten Varietäten über $\mathbb{C}$ gehört auch eine holomorphe Abbildung

$$\psi^h\colon\ Y^h \longrightarrow X^h.$$

Dies beruht darauf, dass rationale Funktionen, also Quotienten aus Polynomen in mehreren Variablen, holomorph sind.

Endliche Morphismen

Definition 7.9. Es seien X und Y quasiprojektive Varietäten über einem algebraisch abgeschlossenen Körper und sei

$$\psi\colon\ X \longrightarrow Y$$

ein Morphismus. Man nennt ψ *endlich*, wenn es eine offene affine Überdeckung $Y = \bigcup_{i\in I} V_i$ derart gibt, dass auch die Urbilder $\psi^{-1}(V_i)$ affin sind und die zugehörigen Ringhomomorphismen

$$\Gamma(V_i, \mathcal{O}_Y) \longrightarrow \Gamma(\psi^{-1}(V_i), \mathcal{O}_X)$$

endlich sind.

Zu einem endlichen Morphismus ist für jeden Punkt die Faser endlich. Bei einem endlichen surjektiven Morphismus zwischen irreduziblen Varietäten ist die zugehörige Erweiterung der Funktionenkörper eine endliche Körpererweiterung.

Beispiel 7.10. Es sei F die kubische Gleichung einer elliptischen Kurve in kurzer homogener Weierstraßform, also $F = Y^2Z - X^3 - aXZ^2 - bZ^3$. Wir betrachten die Abbildung

$$V_+(F) \longrightarrow \mathbb{P}^1_K,\ (x,y,z) \longmapsto (x,y).$$

Diese ist die Einschränkung des Morphismus (einer Projektion weg von einem Punkt)

$$\mathbb{P}^2_K \setminus \{(0,0,1)\} \longrightarrow \mathbb{P}^1_K,\ (x,y,z) \longmapsto (x,y),$$

und damit selbst ein Morphismus. Auf der affinen Gerade $D_+(x) \subseteq \mathbb{P}^1_K$ ist diese Abbildung mit $U = Y/X$ und $V = Z/X$ gleich

$$V(U^2V - 1 - aV^2 - bV^3) \longrightarrow \mathbb{A}^1_K,\ (u,v) \longmapsto u.$$

Dies ist eine endliche Abbildung, da

$$K[U] \subseteq K[U,V]/(U^2V - 1 - aV^2 - bV^3)$$

eine endliche Ringerweiterung mit der Basis $1, V, V^2$ ist. Auf der affinen Gerade $D_+(y) \subseteq \mathbb{P}^1_K$ ist diese Abbildung mit $S = X/Y$ und $T = Z/Y$ gleich

$$V(T - S^3 - aST^2 - bT^3) \longrightarrow \mathbb{A}^1_K,\ (s,t) \longmapsto s.$$

Dies ist ebenfalls eine endliche Erweiterung mit einer Basis aus 3 Elementen.

Wir betrachten nun die Abbildung

$$V_+(F) \longrightarrow \mathbb{P}^1_K,\ (x,y,z) \longmapsto (x,z),$$

die auf $D_+(Z)$ die Einschränkung des Morphismus

$$\mathbb{P}^2_K \setminus \{(0,1,0)\} \longrightarrow \mathbb{P}^1_K,\ (x,y,z) \longmapsto (x,z),$$

sei und die darüberhinaus $(0,1,0)$ auf $(1,0)$ abbildet. Die Stetigkeit ist klar. Auf der affinen Gerade $D_+(z) \subseteq \mathbb{P}^1_K$ ist diese Abbildung mit $W = X/Z$ und $R = Y/Z$ gleich

$$V(R^2 - W^3 - aW - b) \longrightarrow \mathbb{A}^1_K,\ (w,r) \longmapsto w,$$

was der endlichen Ringerweiterung

$$K[W] \subseteq K[W,R]/(R^2 - W^3 - aW - b)$$

mit der Basis $1, R$ entspricht. Oberhalb von $D_+(x) \subseteq \mathbb{P}^1_K$ betrachten wir nicht (die scheinbar natürlichere Definitionsmenge) $D_+(x)$, da dies $(0,1,0)$ nicht enthält, sondern $D_+(Y^2 - bZ^2)$. Der zugehörige Ring ist schwieriger zu beschreiben, aber auch endlich vom Grad 2.

Satz 7.11. *Es seien C und D irreduzible projektive Kurven über einem algebraisch abgeschlossenen Körper und sei $\psi\colon C \to D$ ein Morphismus. Dann ist entweder ψ konstant oder aber ein endlicher Morphismus.*

Ein endlicher Morphismus

$$\varphi\colon C \longrightarrow D$$

zwischen irreduziblen Kurven führt in natürlicher Weise zu einer endlichen Körpererweiterung $Q(D) \subseteq Q(C)$ der Funktionenkörper. Diese Erweiterung kann man durch die Quotientenkörper zu beliebigen offenen affinen Teilmengen erhalten. Über diese Beobachtung kann man viele Begrifflichkeiten aus der Körpertheorie in die Theorie der Kurven überführen, beispielsweise Grad und Separabilität. Es gilt sogar der folgende Zusammenhang.

Satz 7.12. *Es sei K ein algebraisch abgeschlossener Körper. Dann gibt es eine Entsprechung zwischen den glatten projektiven Kurven über K und den Körpern über K vom Transzendenzgrad 1, wobei sich endliche Morphismen und endliche Körpererweiterungen entsprechen.*

Lemma 7.13. *Es sei C eine glatte irreduzible Kurve über einem algebraisch abgeschlossenen Körper K und sei Q der Funktionenkörper von C. Dann definiert jede rationale Funktion $q \in Q$ in natürlicher Weise einen Morphismus*

$$q\colon C \longrightarrow \mathbb{P}^1_K$$

in die projektive Gerade $\mathbb{P}^1_K$.

Lemma 7.14. *Es sei K ein algebraisch abgeschlossener Körper und sei*

$$E = V_+(F) \subseteq \mathbb{P}^2_K$$

eine elliptische Kurve über K mit einem fixierten Punkt $\mathfrak{O} \in E$. Dann sind die Addition

$$+\colon E \times E \longrightarrow E,$$

die Negation

$$E \longrightarrow E,\ P \longmapsto -P,$$

und die Vervielfachung

$$[m]\colon E \longrightarrow E,\ P \longmapsto mP,$$

Morphismen.

Beweis. Dies folgt aus den expliziten Beschreibungen in Satz 6.5. □

Eine Varietät, die diese Eigenschaften erfüllt, heißt *Gruppenvarietät*. Man verlangt also, dass es eine Verknüpfungsabbildung und eine Inversenbildung gibt, die einerseits Morphismen sind und andererseits die Gruppeneigenschaften erfüllen.

Definition 7.15. Es sei E eine elliptische Kurve über einem Körper K und sei $Q \in E$. Man nennt die zusammengesetzte Abbildung

$$E \stackrel{P \mapsto (P,Q)}{\longrightarrow} E \times E \stackrel{+}{\longrightarrow} E$$

die *Translation* mit Q. Sie wird mit τ_Q bezeichnet.

Aufgrund von Lemma 7.14 handelt es sich bei einer Translation um einen Morphismus. Translationen sind Automorphismen, die Umkehrabbildung zu τ_P ist τ_{-P}. Da mittels der Translation τ_{P-Q} der Punkt Q in den Punkt P ismorph überführt wird, sieht eine elliptische Kurve in jedem Punkt gleich aus. Man spricht von einem homogenen Objekt. Die affinen Räume und die projektiven Räume sind ebenfalls in diesem Sinne homogen, die meisten Varietäten sind es aber nicht, häufig ist die Automorphismusgruppe endlich.

Definition 7.16. Eine *abelsche Varietät* über einem algebraisch abgeschlossenen Körper K ist eine irreduzible projektive Varietät A, die zugleich eine Gruppenvarietät ist.

Man kann zeigen, dass auf einer abelschen Varietät die Gruppenstruktur stets kommutativ ist und dass es sich um eine glatte Varietät handelt. Elliptische Kurven sind einfach die eindimensionalen abelschen Varietäten. Statt irreduzibel genügt es, zusammenhängend zu fordern. Nichtprojektive Gruppenvarietäten müssen nicht kommutativ sein, beispielsweise ist die allgemeine lineare Gruppe eine irreduzible nichtkommutative Gruppenvarietät. Ein großer Unterschied zwischen elliptischen Kurven und abelschen Varietäten höherer Dimension ist, dass letztere nicht durch einfache Gleichungen beschrieben werden können. Insbesondere können sie nicht durch eine einzige Gleichung beschrieben werden.

Aufgrund von Bemerkung 7.8 kann eine abelsche Varietät und insbesondere eine elliptische Kurve über $\mathbb{C}$ auch als eine komplexe Lie-Gruppe aufgefasst werden, siehe die folgenden Vorlesungen.

Abbildungsverzeichnis