Algebraische Kurven

Dr. Stefan Kühnlein

Institut für Algebra und Geometrie, Karlsruher Institut für Technologie, Frühjahr 2012

Dies ist ein Mitwachsskript zur gleichnamigen Vorlesung aus dem Sommersemester 2012.
Der Plan ist der, dass wir zunächst kurz über ebene algebraische Kurven sprechen, und zwar über einem algebraisch abgeschlossenen Körper, dann die dort gelernten Dinge benutzen, um allgemeiner die Kurve zu einem Körper vom Transzendenzgrad 1 über einem Grundkörper einzuführen, und schließlich für diese Kurven wichtige Sätze beweisen, wie etwa den Satz von Riemann-Roch. Ich hoffe, auch auf arithmetische Dinge eingehen zu können, insbesondere die Rationalität der L-Reihe einer Kurve über einem endlichen Körper. Noch bin ich zuversichtlich.
Vieles habe ich aus dem Buch *Algebraic Curves over Finite Fields* von Carlos Moreno übernommen.

Inhaltsverzeichnis

Kapitel 1

Allgemeine Grundlagen

Wir werden hier zunächst ein bisschen Algebra machen und dann einige Begriffe der algebraischen Geometrie einführen, gerade so viel, wie es für das Verständnis der algebraischen Kurven nötig sein wird. Dann nähern wir uns der Definition der algebraischen Kurve nähern, wie sie in dieser Vorlesung verstanden sein soll.

1.1 Algebraische Ergänzungen

Hilfssatz 1.1.1 Eine Algebraizitätsaussage
Es seien k ein Körper und A eine endlich erzeugte k-Algebra, die selbst ein Körper ist.
Dann ist A algebraisch über k.

Beweis: Wir schreiben A als Quotient des Polynomrings $k[X_1, \ldots, X_n]$ und machen vollständige Induktion nach n.
Für $n = 1$ bedeutet die Voraussetzung, dass $A = k[X]/m$ für ein maximales Ideal im Polynomring gilt. Da wir die maximalen Ideale in $k[X]$ gut kennen, folgt die Behauptung.
Für den Induktionsschritt bezeichnen wir die Klasse von X_i in A mit x_i und machen einen Beweis durch Widerspruch. Wir nehmen an, dass eines der x_i nicht algebraisch über k sei. Ohne Einschränkung sei x_1 über k transzendent. Nach Induktionsvoraussetzung wissen wir jedoch, dass $x_2, \ldots, x_n$ über $k(x_1)$ algebraisch sind. Es gibt also Polynome $0 \neq f_i \in k[x_1][T],\ 2 \leq i \leq n$, sodass

$$f_i(x_i) = 0.$$

Es sei $l \in k[x_1]$ das Produkt der Leitkoeffizienten dieser Polynome. Dann sind alle x_i ganz über $k[x_1, l^{-1}]$, und da A ein Körper ist, ist auch $k[x_1, l^{-1}]$ ein Körper (Algebra, Aufgabe 2 auf Blatt 12). Aber das ist natürlich Unsinn. ◯

Satz 1.1.2 Hilberts[1] Nullstellensatz
Es seien k ein algebraisch abgeschlossener Körper und $m \subset k[X_1, \ldots, X_n]$ ein maximales Ideal.
Dann gibt es Zahlen $c_1, \ldots, c_n \in k$ sodass

$$m = (X_1 - c_1, \ldots, X_n - c_n).$$

Beweis: Da $k[X_1, \ldots, X_n]/m$ ein Körper ist, ist es eine algebraische Erweiterung von k, also k. Der zugehörige Homomorphismus Φ von $k[X_1, \ldots, X_n]$ nach k bildet X_i auf Zahlen $c_i := \Phi(X_i) \in k$ ab, und für diese gilt die behauptete Gleichheit. ◯

1.2 Die Zariskitopologie

Definition 1.2.1 Zariskitopologie[2]
Es seien k ein Körper und L ein Erweiterungskörper von k.
Für eine Teilmenge $A \subseteq L^n$ heißt

$$I(A) := \{f \in k[X_1, \ldots, X_n] \mid f|_A = 0\}$$

das *Verschwindungsideal* von A (über k).
Für ein Ideal $I \in k[X_1, \ldots, X_n]$ heißt

$$V(I) := \{P \in L^n \mid \forall f \in I : f(P) = 0\}$$

die *Verschwindungsmenge von I*.
Der *k-Zariskiabschluss* von A ist

$$\overline{A} := \{P \in L^n \mid \forall f \in V(A) : f(P) = 0\} = V(I(A)).$$

Eine Teilmenge $A \subseteq L^n$ heißt *abgeschlossen bezüglich der Zariskitopologie über k* oder auch kürzer *k-abgeschlossen*, falls

$$A = \overline{A}.$$

Wir werden noch sehen, weshalb man hier verschiedene Körper betrachtet. Im Allgemeinen wird man an k interessiert sein, aber in L mehr Freiheiten haben.

Bemerkung 1.2.2 Topologie
Es ist tatsächlich leicht einzusehen, dass die Zariskiabgeschlossenen Teilmengen die abgeschlossenen Teilmengen einer Topologie auf L^n sind.

[1] David Hilbert, 1862-1943
[2] Oscar Zariski, 1899-1986

Da $k[X_1, \ldots, X_n]$ noethersch[3] ist, ist eine Menge A genau dann abgeschlossen, wenn es endlich viele Polynome $f_1, \ldots, f_r$ gibt, sodass

$$A = \{P \in L^n \mid \forall i = 1, \ldots r : f_i(P) = 0\}.$$

Es mag anfangs etwas erstaunen, dass hier Polynome über k benutzt werden, um über Teilmengen in L^n zu reden, aber für arithmetische Anwendungen ist das oft unerlässlich.
In der klassischen algebraischen Geometrie würde man hier im Allgemeinen nur die Situation $k = L$ betrachten, und dieser Körper soll dann auch algebraisch abgeschlossen sein.

Bemerkung 1.2.3 Hilberts Nullstellensatz
Eine Folgerung aus dem Hilbertschen Nullstellensatz ist auch die folgende Aussage:
Ist k algebraisch abgeschlossen und $I \subseteq k[X_1, \ldots, X_n]$ ein Ideal, so gilt

$$I(V(I)) = \{f \in k[X_1, \ldots, X_n] \mid \exists e \in \mathbb{N} : f^e \in I\} =: \sqrt{I}.$$

Dieses Ideal nennt man auch das *Radikal von* I. Es ist klar, dass hier $\sqrt{I} \subseteq I(V(I))$ gilt, Die andere Richtung benötigt Hilberts Resultat.

Beispiel 1.2.4 Generischer Punkt

a) Die abgeschlossenen Teilmengen von k sind genau die endlichen Teilmengen von k und k selbst.

b) In der Situation $k = \mathbb{Q}$ und $L = \mathbb{C}$ treten einige interessante Fälle auf, schon was $\mathbb{Q}$-abgeschlossene Teilmengen von $\mathbb{C}$ angeht.

   Zum Beispiel ist $\{0\}$ abgeschlossen. Für algebraisches $a \in \mathbb{C}$ ist $V(a) := V(\{a\}$ das vom Minimalpolynom m von a erzeugte Ideal, also ist der Abschluss von $\{a\}$ die Nullstellenmenge dieses Minimalpolynoms, oder – anders gesagt – der Orbit von x unter der Wirkung von $\mathrm{Aut}(\mathbb{C})$.

   Der Abschluss von $\{\pi\}$ hingegen ist ganz $\mathbb{C}$, denn π ist transzendent und damit $V(\pi) = \{0\}$.

c) Im allgemeinen nennen wir einen Punkt a der abgeschlossenen Menge A *generisch*, wenn $A = \overline{\{a\}}$.

   Für viele abgeschlossenen Mengen gibt es so einen generischen Punkt, wenn nur L groß genug ist.

   Im Sinne von Weil[4] sollte man sich hier immer etwas Freiraum lassen und eventuell sogar nicht einmal fixieren, was L ist. Das ist eine Vorstufe zur Sichtweise der Schemata in der modernen algebraischen Geometrie.

[3] Emmy Noether, 1882-1935
[4] André Weil, 1906-1998

d) Wenn $k = L$ ist, dann ist jeder Punkt in k^n abgeschlossen (über k), also gibt es hier keine generischen Punkte für große abgeschlossene Mengen.

Wenn auch noch $k = L$ algebraisch abgeschlossen ist, dann sind die einelementigen Teilmengen von L^n genau die, für die das Verschwindungsideal maximal ist.

Das ist genau die Aussage von Hilberts Nullstellensatz.

Definition/Bemerkung 1.2.5 Irreduzibilität

a) Eine abgeschlossene Teilmenge $A \subseteq L^n$ heißt *k-irreduzibel*, wenn sie sich nicht als Vereinigung von zwei kleineren abgeschlossenen Teilmengen schreiben lässt.

b) Da das Verschwindungsideal einer kleineren abgeschlossenen Menge größer ist als das einer größeren, und da der Polynomring noethersch ist, kann man mit noetherscher Induktion zeigen, dass jede abgeschlossene Teilmenge eine Vereinigung von endlich vielen irreduziblen Teilmengen ist.

Ansonsten gäbe es nämlich eine minimale abgeschlossene Teilmenge A_0, die sich nicht als Vereinigung von irreduziblen schreiben lässt. A_0 wäre selbst nicht irreduzibel, also Vereinigung zweier abgeschlossener echter Teilmengen A und B. Wegen der Minimalität von A_0 sind dann aber A und B selbst Vereinigungen von irreduziblen:

$$A = C_1 \cup \cdots \cup C_c,\ B = D_1 \cup \cdots \cup D_d,$$

also auch

$$A_0 = C_1 \cup \cdots \cup C_c \cup D_1 \cup \cdots \cup D_d,$$

im Widerspruch zur Annahme.

c) Wenn $k = L$ unendlich ist, dann ist k auch irreduzibel, denn echte abgeschlossene Teilmengen sind endlich und damit k nicht Vereinigung von echten abgeschlossenen Teilmengen. Wenn k endlich ist, dann ist k nicht irreduzibel, sondern Vereinigung von endlich vielen einelementigen Mengen, die natürlich alle irreduzibel sind.

d) Eine abgeschlossene Menge A ist genau dann irreduzibel, wenn das Verschwindungsideal ein Primideal ist.

Ist nämlich A nicht irreduzibel, so ist $A = B \cup C$ für echte abgeschlossene Teilmengen, und da B und C sich nicht gegenseitig enthalten, gibt es ein $f \in I(B) \backslash I(C)$ und ein $g \in I(C) \backslash I(B)$. Daher sind $f, g \notin I(B \cup C) = I(A)$, aber $f \cdot g$ sehr wohl, also $I(A)$ kein Primideal.

Ist umgekehrt $I(A)$ kein Primideal, so gibt es $f, g \in k[X_1, \ldots, X_n],\ f, g \notin I(A),\ fg \in I(A)$. Dann sind $V(I(A)+(f)), V(I(A)+(g))$ echte abgeschlossene Teilmengen von A und A ist ihre Vereinigung, also nicht irreduzibel.

e) Die (nicht redundanten) irreduziblen Mengen, deren Vereinigung A ist, heißen die *irreduziblen Komponenten von* A. Sie sind durch A festgelegt.

f) Wenn A einen generischen Punkt hat, also $A = \overline{\{a\}}$ gilt, dann ist A irreduzibel, denn $V(A) = V(\{a\})$ ist der Kern eines Homomorphismus von $k[X_1, \ldots, X_n]$ nach L, also ein Primideal.

Umgekehrt kann man sich für ein gegebenes Primideal $P \subseteq k[X_1, \ldots, X_n]$ den Körper L so großwählen, dass ein generischer Punkt in $V(P)$ existiert. Wie werden dies nie benutzen, die Wahl von L wird in der modernen algebraischen Geometrie ohnehin vermieden durch die Sprache der Schemata.

Kapitel 2

Ebene Kurven

Hier nähern wir uns den Objekten der Vorlesung, indem wir ein paar Beispiele diskutieren von etwas, was man sicher eine Kurve zu nennen bereit ist.

2.1 Funktionen auf Kurven

Beispiel 2.1.1 Was schon Euklid kannte

a) Eine Gerade in der Ebene wird man sicher als Kurve akzeptieren. Diese ist gegeben als Nullstellenmenge eines Polynoms

$$aX + bY + c \in k[X, Y],$$

wobei a und b nicht beide 0 sind.

Hier sieht man bereits, weshalb wir uns bei der Zariskitopologie ein wenig verbogen haben, denn wenn k endlich ist, dann zerbröselt diese Gerade als endlicher Punkthaufen, und ist nicht irreduzibel.

b) Der „Kreis mit Radius r“ wird als Nullstellenmenge des Polynoms

$$X^2 + Y^2 - r^2$$

beschrieben.

Da hier r^2 steht, gibt es auch immer einen Punkt auf diesem Kreis, etwa $(r, 0)$.

Würde man jedoch das Polynom $X^2 + Y^2 - R$ für ein beliebiges R ansehen, so wäre nicht klar, dass es immer einen Punkt in der Ebene gibt, der diese Gleichung erfüllt.

Das wird erst klar, wenn man k als algebraisch abgeschlossen voraussetzt, da uns Zorns[1] Lemma und der Hilbertsche Nullstellensatz Zahlen $x, y \in k$

[1] Max August Zorn, 1906-1993

schenken, sodass $(X^2 + Y^2 - R) \subset (X - x, Y - y)$, und das heißt wieder, dass (x, y) in der Verschwindungsmenge des Polynoms liegen.

Ähnlich sieht es wieder mit der Irreduzibilität aus. Wenn k endlich ist und $0 \neq R \in k$ beliebig, dann gibt es immer mindestens einen Punkt auf der „Kurve“

$$\{(x, y) \in k^2 \mid x^2 + y^2 = R\}.$$

Aber diese Menge ist eine endliche Vereinigung von einelementigen, und daher nicht irreduzibel (da selbst nicht einelementig).

Diesem Mangel schaffen wir Abhilfe, indem wir als Kurve – zumindest vorübergehend – die Menge

$$\{(x, y) \in \overline{k}^2 \mid x^2 + y^2 = R\}$$

betrachten, wobei $\overline{k}$ der algebraische Abschluss ist.

Das kann auch im Fall von unendlichen Körpern hilfreich sein, denn zum Beispiel ist

$$\{(x, y) \in \mathbb{Q}^2 \mid x^2 + y^2 = 3\}$$

leer. Aber es gibt natürlich algebraische Punkte auf dem Kreis mit Radius $\sqrt{3}$.

In Charakteristik 2 ist die Gleichung des Kreises übrigens nicht irreduzibel, denn $X^2 + Y^2 - r^2 = (X + Y + r)^2$.

Definition 2.1.2 Ebene algebraische Kurve
Eine ebene algebraische Kurve über k ist die Verschwindungsmenge C_p eines irreduziblen Polynoms $p(X, Y) \in k[X, Y]$.
Die Irreduzibilität des Polynoms stellt auch die der Kurve sicher. Der Absolutgrad von p heißt auch der Grad von C_p.
Natürlich stellt sich hier sofort die Frage, inwieweit das irreduzible Polynom durch seine Verschwindungsmenge charakterisiert wird. Dies kann man auffassen als Spezialfall des Hilbertschen Nullstellensatzes 1.1.2 bzw. der dort nachfolgenden Bemerkung. Wir stellen das aber etwas anders sicher.
Bevor wir dies tun, halten wir fest, dass in der Literatur eine Kurve nicht unbedingt irreduzibel sein muss. Diese Zusatzbedingung entspricht jedoch unserer Hauptstoßrichtung, und auch in der allgemeineren Situation werden die meisten Sätze bewiesen, nachdem man zunächst die Kurven als irreduzibel voraussetzt und dann die Einzelinformationen zusammensetzt.

Hilfssatz 2.1.3 Lemma von Study[2]
Es sei k algebraisch abgeschlossen und $p, q \in k[X, Y]$.

[2]Christian Hugo Eduard Study, 1862-1930

a) Ist p irreduzibel und $V(p) \subseteq V(q)$, dann ist p ein Teiler von q.

b) Sind p und q beide irreduzibel und $V(p) = V(q)$, so sind p und q assoziiert, stimmen also bis auf Multiplikation mit einer Konstanten überein.

Beweis. Wir werden in diesem Beweis ad hoc mit Resultanten arbeiten, die ansonsten in dieser Vorlesung keine Rolle spielen.
Wir schreiben

$$p(X,Y) = \sum_{i=0}^{d} a_i X^i, \quad q(X,Y) = \sum_{j=0}^{e} b_j X^j, \ a_i, b_j \in k[Y], \ a_d, b_e \neq 0.$$

Für jedes $y \in k$ mit $a_d(y), b_e(y) \neq 0$ ist

$$\{x \in k \mid p(x,y) = 0\} \subseteq \{x \in k \mid q(x,y) = 0\}$$

jeweils nicht leer, denn k ist algebraisch abgeschlossen. Also haben die Polynome $p(X,y)$ und $q(X,y)$ einen nicht konstanten gemeinsamen Teiler, und es gibt Polynome $f, g \in k[X]$, sodass

$$f(X)p(X,y) = g(X)q(X,y), \ \deg(f) < \deg(q(\cdot,y)), \ \deg(g) < \deg(p(\cdot,y)).$$

Es sind also die Polynome

$$p(X,y), \ Xp(X,y), \ldots, X^{e-1}p(X,y), \ q(X,y), Xq(X,y) \ldots, X^{d-1}q(X,y)$$

über k linear abhängig, oder – äquivalent – die Determinante der Matrix

$$R(Y) := \begin{pmatrix} a_0(Y) & a_1(Y) & \ldots & \ldots & a_d(Y) & 0 & \ldots & 0 \\ 0 & a_0(Y) & a_1(Y) & \ldots & \ldots & a_d(Y) & 0 & \vdots \\ 0 & \vdots & \ddots & \ddots & & \vdots & \ddots & \vdots \\ 0 & \ldots & 0 & a_0(Y) & a_1(Y) & \ldots & \ldots & a_d(Y) \\ b_0(Y) & b_1(Y) & \ldots & \ldots & b_e(Y) & 0 & \ldots & 0 \\ 0 & b_0(Y) & b_1(Y) & \ldots & \ldots & b_e(Y) & 0 & \vdots \\ 0 & \vdots & \ddots & \ddots & & \vdots & \ddots & \vdots \\ 0 & \ldots & 0 & b_0(Y) & b_1(Y) & \ldots & \ldots & b_e(Y) \end{pmatrix}$$

an der Stelle $Y = y$ ist 0[3]. Die Matrix ist eine $(d+e) \times (d+e)$-Matrix, und die ersten e Zeilen sind mit den a's bestückt, die letzten d mit den b's.
Diese Determinante ist ein Polynom in Y, und wir haben eben gesehen, dass es unendlich viele $y \in k$ gibt, sodass $R(y) = 0$ gilt. Es folgt $R(Y) = 0$, und damit sind die Polynome

$$p(X,Y), Xp(X,Y), \ldots X^{e-1}p(X,Y), q(X,Y), \ldots, X^{d-1}q(X,Y)$$

[3]da ist sie, die Resultante

über $k(Y)$ linear abhängig, also gibt es Polynome

$$F(X,Y),\ G(X,Y) \neq 0,\ \deg_X(F) < e,\ \deg_X(G) < D,$$

sodass

$$Gp = Fq.$$

Da p irreduzibel ist und sein Grad größer ist als der von G, muss p ein Teiler von q sein – der Polynomring ist ja faktoriell.
In Aussage b) teilen sich p und q gegenseitig, sind also assoziiert. ◯

Hilfssatz 2.1.4 Endlich!
Wenn $p, q \in k[X,Y]$ zwei nicht assoziierte, irreduzible Polynome sind, dann schneiden sich die zugehörigen Kurven C_p und C_q nur in endlich vielen Punkten.

Beweisskizze. Wie im letzten Beweis liegt ein Schnittpunkt (x,y) der beiden Kurven mit gegebenem y genau dann vor, wenn die dort betrachtete Resultante $R(y)$ 0 wird. Da diese als Polynom in Y nicht konstant verschwindet (sonst wäre p ein Teiler von q), gibt es nur endlich viele Kandidaten für y-Werte von Schnittpunkten. Aus Symmetriegründen gibt es auch nur endlich viele Kandidaten für x-Werte von Schnittpunkten, und damit insgesamt nur endlich viele Schnittpunkte. ◯

Bemerkung 2.1.5 Abgeschlossene Teilmengen

a) Hilfssatz 2.1.4 sagt uns insbesondere, dass so etwas wie der Graph der Sinusfunktion keine algebraische Kurve ist, denn er schneidet die algebraische Kurve $Y = 0$ in unendlich vielen Punkten.

b) Der letzte Hilfssatz gilt allgemeiner auch dann, wenn q nicht irreduzibel ist, solange p eben q nicht teilt. Er sagt uns, dass die (Zariski-)abgeschlossenen Teilmengen einer ebenen Kurve allesamt endlich sind oder die ganze Kurve.

c) Mit relativ einfachen Mitteln erhält man die Abschätzung, dass zwei Kurven von Grad n bzw. m sich in höchstens nm Punkten treffen.

Bemerkung 2.1.6 Die Galoisgruppe
Wir haben in der Definition gar nicht gesagt, über welchem Körper wir den affinen Raum betrachten. Der Körper k wird oft zu klein sein, und es bietet sich tatsächlich der algebraische Abschluss von k an. Dann operiert die Galoisgruppe $G = \mathrm{Aut}(\overline{k} \mid k)$ auf der Kurve C durch Anwendung auf beide Koordinaten der Punkte, und eigentlich sind die Punkte in einem Galoisorbit aus Sicht des kleinen Körpers k nicht zu unterscheiden.
Diesem Problem werden wir uns später noch einmal zu stellen haben und für den Rest dieses Kapitels festlegen, **dass k selbst schon algebraisch abgeschlossen sein soll.**

Folgerung 2.1.7 Rechtfertigung
Es sei k algebraisch abgeschlossen und $\{0\} \neq I \subset k[X,Y]$ ein Primideal, sodass $V(I)$ unendlich ist.
Dann wird I von einem irreduziblen Element erzeugt.

Beweis. Es sei $f \in I$ ein von Null verschiedenes Polynom. Wegen der Faktorialität von $k[X,Y]$ lässt sich f als Produkt von irreduziblen schreiben, von denen dann ein Faktor – nennen wir ihn p – selbst in I liegt, das ja ein Primideal ist.
Wenn $g \in I$ ein weiteres Element ist, von dem dann ein irreduzibler Faktor q in I liegt, dann sind p und q assoziiert, da

$$V(I) \subseteq C_p \cap C_q$$

unendlich ist, also wegen 2.1.4 die beiden Kurven C_p und C_q gleich sein müssen. Demnach ist jedes Element in I durch p teilbar. ◯

Bemerkung 2.1.8 Krulldimension

a) In 2.1.7 haben wir gesehen, dass unsere Definition einer algebraischen Kurve nicht vorschnell nur die Verschwindungsmenge eines einzelnen irreduziblen Polynoms herangezogen hat. Jedes größere Primideal hat nur eine endliche Verschwindungsmenge, jedes kleinere ist trivial.

b) Noch präziser können wir sagen: In $k[X,Y]$ gibt es drei Typen von Primidealen, nämlich das minimale Primideal $\{0\}$, die maximalen Primideale $(X-a, Y-b)$ für $a, b \in k$ und dazwischen noch Primideale, die von einzelnen irreduziblen Polynomen erzeugt werden.

   Eine aufsteigende Primidealkette hat also höchstens zwei echte Schritte, und diese Schranke wird erreicht. (Dies stimmt auch, wenn k nicht algebraisch abgeschlossen ist; allerdings sind dann die maximalen Ideale nicht mehr unbedingt von der angegebenen Form.)

   Man sagt dann auch, dass $k[X,Y]$ die *Krulldimension*[4] 2 hat.

Definition 2.1.9 Funktionen
Es sei C eine ebene algebraische Kurve und $V \subset k[X,Y]$ ihr Verschwindungsideal. Dabei sei $V = (p)$ vom irreduziblen Polynom p erzeugt.
Dann heißt

$$k[C] := k[X,Y]/V$$

der *Koordinatenring* von C. Jedes Element in $k[C]$ lässt sich als Funktion auf C ansehen, denn verschiedene Repräsentanten derselben Klasse unterscheiden sich ja nur um ein Polynom, das überall auf C Null ist.

[4] Wolfgang Adolf Ludwig Helmuth Krull, 1899 - 1971

Wegen 2.1.8 ist jedes von 0 verschiedene Primideal im Koordinatenring maximal. Denn: Sein Urbild in $k[X,Y]$ ist ein Primideal, das p enthält, aber nicht von p erzeugt wird.
Der Koordinatenring wird als k-Algebra erzeugt von den Koordinatenfunktionen X und Y.
Ein von Null verschiedenes Element aus $k[C]$ hat wegen 2.1.5 nur endlich viele Nullstellen in C. Auch daran sieht man:
Da C nach Definition irreduzibel ist und V damit ein Primideal, ist $k[C]$ nullteilerfrei und hat demnach einen Quotientenkörper $k(C)$, den *Funktionenkörper* von C. Ein Element von $k(C)$ nennen wir eine *rationale Funktion* auf C.
$k(C)$ hat über k Transzendenzgrad 1, denn dieser Körper wird von den Klassen von X und Y erzeugt, von denen eine transzendent ist, zwischen denen aber die algebraische Abhängigkeit $p(X,Y) = 0$ besteht.
Für einen Punkt $P \in C$ heißt

$$\mathcal{O}_P(C) := \{f \in k(C) \mid f(P) \in k\}$$

der *lokale Ring von C in P*. Er ist ein lokaler Ring mit dem einzigen maximalen Ideal

$$\mathbf{m}_P(C) := \{f \in \mathcal{O}_P(C) \mid f(P) = 0\}.$$

Jedes $f \in \mathcal{O}_P(C)$ mit $f(P) \neq 0$ ist ja in $\mathcal{O}_P(C)$ invertierbar.

Bemerkung 2.1.10 Ein noetherscher lokaler Ring
Der Ring $\mathcal{O}_P(C)$ ist noethersch.
Denn: Es ist

$$\mathcal{O}_P(C) = k[C][S^{-1}] := \{f/s \mid f \in k[C], s \in S\}, \text{ wobei } S = \{s \in k[C] \mid s(P) \neq 0\}.$$

Für ein Ideal $I \subset \mathcal{O}_P(C)$ ist $I \cap k[C]$ ein Ideal im Koordinatenring, und dieses erzeugt I in $\mathcal{O}_P(C)$, da

$$\forall i \in I : \exists s \in S : si \in I \cap k[C].$$

Da $k[C]$ als endlich erzeugte kommutative k-Algebra noethersch ist, ist $I \cap k[C]$ endlich erzeugt als $k[C]$-Ideal, und damit auch I als Ideal in $\mathcal{O}_P(C)$.

2.2 Glattheit

Definition 2.2.1 Glattheit
Es sei $p(X,Y) \in k[X,Y]$ irreduzibel und $C = C_p$ seine Verschwindungsmenge. Weiter sei $P = (x,y) \in C$ ein Punkt. Dann heißt C *glatt in P*, wenn der Gradient $(\frac{\partial p}{\partial X}, \frac{\partial p}{\partial Y})$ im Punkt P nicht verschwindet.
Wegen des Lemmas von Study 2.1.3 ist dies wohldefiniert.

Glattheit in P bedeutet, dass in diesem Punkt eine wohldefinierte Tangente existiert.
Denn: Es sei $P = (0,0)$ Die Gerade $aX + bY = 0$ ist *tangential* an C in P, wenn das Polynom $g(-bT, aT)$ durch T^2 geteilt werden kann.
Wir schreiben f als

$$g(X,Y) = \sum c_{ij} X^i Y^j,\ c_{00} = 0.$$

Dann ist der Gradient an der Stelle $(0,0)$ gerade (c_{10}, c_{01}), während $g(-bT, aT) = (-c_{10}b + c01a)T + T^2 \cdot$ Polynom in T. Also ist die Gerade genau dann tangential, wenn (a,b) ein Vielfaches von (c_{10}, c_{01}) ist – außer der Gradient ist 0, in welchem Fall jede Gerade „tangential“ ist.

Ein Punkt, in dem die Kurve nicht glatt ist, heißt ein *singulärer Punkt.* Wegen Bemerkung 2.1.5 gibt es auf einer irreduziblen Kurve nur endlich viele singuläre Punkte, wenn k algebraisch abgeschlossen ist. In der Differentialtopologie heißt so eine Aussage auch „Lemma von Sard“.
Wenn die Kurve in all ihren Punkten glatt ist, heißt sie eine *glatte Kurve.*

Bemerkung 2.2.2 Satz von der impliziten Funktion
Man kann die Definition 2.2.1 der Glattheit in einem Punkt auch auffassen als algebraische Ausnutzung des Satzes von der impliziten Funktion, der unter genau dieser Voraussetzung im Fall von $k = \mathbb{R}$ sagt, dass es eine glatte, d.h. differenzierbare, Parametrisierung von C in einer Umgebung von P gibt.

Beispiel 2.2.3 glatt oder nicht glatt

a) Der Kreis mit Radius r ist in jedem Punkt glatt, außer die Charakteristik ist 2. Aber in diesem Fall war ja ohnehin die Kreisgleichung kein Erzeuger der Verschwindungsmenge.

b) Es sei $f \in k[X]$ kein Quadrat. Die Nullstellenmenge C des Polynoms

$$Y^2 - f(X),$$

ist dann wegen Eisenstein eine irreduzible Kurve. Der Gradient des Polynoms ist $(-f'(X), 2Y)$, und dieser wird höchstens 0, wenn $Y = 0$ gilt. Damit ein solcher Punkt dann auch auf der Kurve liegt, muss $f(X) = f'(X) = 0$ gelten. Das heißt:

Ist die Charakteristik von k nicht gerade 2, dann liegen auf C genau dann singuläre Punkte, wenn f eine mehrfache Nullstelle hat.

Die durch $Y^2 = X^3$ beschriebene Menge (Neilsche[5] Parabel) hat einen singulären Punkt in $(0,0)$, genauso wie die durch $Y^2 = -X^3 + X^2$ beschriebene (Newtonknoten[6]).

[5] William Neile, 1637-1670
[6] Isaac Newton, 1643-1727

Bemerkung 2.2.4 Rekonstruktion
Wir werden im Weiteren erklären, wie man die (glatte, ebene) Kurve aus ihrem Funktionenkörper rekonstruieren kann, zumindest wenn der Grundkörper algebraisch abgeschlossen ist. Diese Einsicht werden wir dann benutzen, um den Begriff der Kurve neu und allgemeiner (nicht mehr eben) zu fassen. Insbesondere werden wir dann die Kluft zwischen dem Definitionskörper und seinem algebraischen Abschluss überwinden und Punkte auf der Kurve abstrakter sehen.

Satz 2.2.5 Eine Bewertung
Es sei $C \in k^2$ eine algebraische Kurve und $P \in C$. Dann ist C genau dann glatt in P, wenn $\mathcal{O}_P(C)$ ein diskreter Bewertungsring von $k(C)$ ist.

Beweis. Wir nehmen zunächst an, dass C glatt in P ist. Ohne Einschränkung seien $P = (0,0)$ und $\frac{\partial p}{\partial Y}(0,0) = 1$ sowie $\frac{\partial p}{\partial X}(0,0) = 0$.
Wir zeigen zunächst, dass die Klasse von X das maximale Ideal des lokalen Rings erzeugt:
Die Klassen von X und Y langen sicher zum Erzeugen. Gemäß unseren Voraussetzungen an den Gradienten gilt

$$p(X,Y) = Y(1 + Y \cdot r(X,Y)) + X^2 s(X),$$

wobei r und s Polynome in zwei bzw. einer Variablen sind.
Es folgt modulo f die Gleichheit

$$Y = -X^2 s(X)/(1 + Y \cdot r(X,Y)),$$

die zunächst formal und dann aber auch in $\mathcal{O}_P(C)$ gilt.
Damit ist $\mathcal{O}_P(C)$ ein noetherscher lokaler Ring (2.1.10), dessen maximales Ideal ein Hauptideal ist. Mit noetherscher Induktion sieht man, dass jedes Element $\neq 0$ in $\mathcal{O}_P(C)$ sich auf eindeutige Art als Einheit mal Potenz von X schreiben lässt, und der Exponent in dieser Darstellung gibt Anlass zu einer Bewertung, deren Bewertungsring gerade $\mathcal{O}_P(C)$ ist.
Also: Wenn C glatt in P ist, dann ist der lokale Ring bei P ein Bewertungsring.

Nun sei umgekehrt $\mathcal{O}_P(C)$ der Bewertungsring einer diskreten Bewertung. Wieder sei $P = (0,0)$.
Weiter sei $T := \mathrm{Kern}(\mathrm{grad}(p)|_P)$ der Tangentialraum von C im Punkt P. Dieser Tangentialraum ist eine Gerade, wenn P ein glatter Punkt ist, und k^2 sonst.
Wir betrachten zunächst

$$M := \{g \in k[C] \mid g(0) = 0\}.$$

Dies ist ein maximales Ideal in $k[C]$.

Für $f \in M$ ist der lineare Term nur modulo dem linearen Term von p wohldefiniert, aber genau das liefert uns einen wohldefinierten surjektiven Vektorraumhomomorphismus

$$\ell : M \ni f \mapsto \frac{\partial f}{\partial X}(0) \cdot X + \frac{\partial f}{\partial Y}(0) \cdot Y \in T^*.$$

Der Kern dieser Abbildung ist M^2, und damit T^* isomorph zu M/M^2.
Wir zeigen nun noch $M/M^2 = \mathbf{m}_P(C)/\mathbf{m}_P(C)^2$.
Dann folgt, da $\mathcal{O}_P(C)$ der Bewertungsring einer diskreten Bewertung ist, dass M/M^2 eindimensional ist, also T auch, und damit P ein glatter Punkt auf C.
Die behauptete Gleichheit sehen wir daran, dass wir $g \in \mathbf{m}_P(C)$ schreiben können als $g = z/n,\ z, n \in k[C], n(0) \neq 0$, und dass dann

$$g - z/n(0) = z(n(0) - n)/(n(0) \cdot n) \in \mathbf{m}_P(C)^2,$$

also die Restklasse von g modulo $\mathbf{m}_P(C)^2$ auch von $z/n(0) \in M$ vertreten wird. ◯

Definition 2.2.6 Die Ordnung
Wenn $C \subset k^2$ eine Kurve ist und P ein nichtsingulärer Punkt auf C, dann gibt es also eine Bewertung auf $k(C)$ vermöge

$$\forall f \in k(C)^\times : v_P(f) := \max\{n \in \mathbb{Z} \mid f \in \mathbf{m}_P(C)^n\}.$$

Diese Zahl heißt die *Ordnung von f in P.*
Für jedes $f \neq 0$ gibt es nur endlich viele $P \in C$, sodass $v_P(f) \neq 0$. Das liegt wieder an 2.1.4.

Bemerkung 2.2.7 Nicht alle Bewertungen
Es sei v eine nicht-triviale diskrete Bewertung von $k(C)$, deren Bewertungsring den affinen Koordinatenring $k[C]$ enthält. Der Schnitt von $k[C]$ mit dem maximalen Ideal im Bewertungsring ist dann ein maximales Ideal in $k[C]$ und daher nach Hilberts Nullstellensatz von den Klassen $X - a, Y - b$ erzeugt, wobei $(a, b) \in C$ ein geeigneter Punkt ist.
Das liefert ein Bijektion zwischen der Menge der glatten Punkte auf C und den Bewertungen, deren Bewertungsring $k[C]$ umfasst.
Allerdings wird nicht für jede diskrete Bewertung diese Bedingung erfüllt sein.
Um diesen Mangel zu heilen führen wir jetzt die projektive Geometrie ein.

2.3 Die projektive Ebene

Definition 2.3.1 Spielfeld

Die projektive Ebene über dem Körper k ist

$$\mathbb{P}^2(k) := (k^3 \setminus \{0\})/k^\times,$$

wobei wir die skalare Multiplikation herausfaktorisieren. Zwei Punkte (x, y, z) und (x', y', z') liefern also genau dann denselben Punkt in der projektiven Ebene, wenn

$$\exists \lambda \in k^\times : (x, y, z) = \lambda(x', y', z').$$

Wir schreiben für die Äquivalenzklasse $(x : y : z)$, und nennen die Einträge ein *homogenes Koordinatentupel*. Die einzelnen Koordinaten sind nicht wohldefiniert, aber sehr wohl die Verhältnisse $(x : y)$ usw. in $k \cup \{\infty\}$.
Wenn $p = \sum_{i,j} c_{i,j} X^i Y^j \in k[X, Y]$ ein irreduzibles Polynom von Absolutgrad d ist, so machen wir es homogen durch

$$\tilde{p} := \sum c_{i,j} X^i Y^j Z^{d-i-j},$$

und definieren

$$\tilde{C} := \{P \in \mathbb{P}^2 \mid \tilde{p}(P) = 0.$$

Dann ist

$$C = C_p(k) = \tilde{C} \cap \{(x : y : 1) \mid x, y \in k\}$$

unsere alte ebene algebraische Kurve zum Polynom p.
Zu $\tilde{C}$ gehören aber noch weitere Punkte, nämlich solche, bei denen z verschwindet. Diese heißen die *unendlich fernen Punkte* auf $\tilde{C}$, wobei diese Terminologie sehr subjektiv ist und von einer fest ausgezeichneten affinen Ebene ausgeht.

Bemerkung 2.3.2 Glattheit
In der Situation der eben gemachten Definition wissen wir genau, was ein glatter Punkt auf C ist. Um diese Sprechweise auf $\tilde{C}$ ausdehnen zu können, nehmen wir einen Punkt $P \in \tilde{C} \setminus C$. Dieser hat eine der beiden Koordinaten X, Y nicht Null. Sei oE $P = (1 : y : 0)$.
Dann denken wir uns P als Punkt der affinen Ebene $\{(y, z) \mid y, z \in k\}$ und betrachten die Nullstellenmenge C' des (irreduziblen!) Polynoms $\tilde{p}(1, Y, Z)$ in dieser Ebene. Dazu gehört P, und wir nennen P glatt auf $\tilde{C}$, wenn P ein glatter Punkt auf C' ist.
Die projektive Kurve $\tilde{C}$ heißt nichtsingulär, wenn nur glatte Punkte auf ihr liegen.

Beispiel 2.3.3 Elliptische Kurven
Es sei $f = \sum_{i=0}^{d} a_i X^i$, wobei $d > 0$ und $a_d \neq 0$ gelte.
Weiter sei $p(X, Y) = Y^e - f(X)$ und e kein Vielfaches der Charakteristik von k.
Dann kennen wir die singulären Punkte von C im Affinen:

$$\{(x, 0) \mid f(x) = f'(x) = 0\}.$$

Es sei $d > e$. Dann bekommen wir

$$\tilde{p}(X,Y,Z) = Z^{e-d}Y^e - \sum_{i=0}^{d} a_i X^i Z^{d-i}.$$

Was sind die unendlich fernen Punkte? Da müssen wir einfach $Z = 0$ setzen und sehen, dass die zugehörigen X und Y-Koordinaten die Gleichung

$$0 = a_d X^d$$

erfüllen.
Es gibt also nur einen unendlich fernen Punkt, nämlich $(0:1:0)$.
Wann ist dieser singulär???
Genau dann, wenn $(0,0)$ ein singulärer Punkt auf der Kurve zum Polynom

$$Z^{e-d} - \sum_{i=0}^{d} a_i X^i Z^{d-i}$$

ist.
Der Gradient im Nullpunkt ist hier

$$(a_1 Z^{d-1}, (e-d)Z^{e-d-1} - a_{d-1}X^{d-1})|_{(X,Z)=(0,0)}.$$

Das ist genau dann Null, wenn $d > 1$ gilt und $e > d+1$.
Zum Beispiel ist für ein kubisches Polynom $f(X) = X^3 - aX - b$ und $p = Y^2 - f(X)$ die projektive Kurve

$$\tilde{C} := \{(x:y:z) \in \mathbb{P}^2 \mid zy^2 = x^3 - axz^2 - bz^3\}$$

nichtsingulär, sobald $27b^2 - 4a^3 \neq 0$. Dies sieht man, wenn man den größten gemeinsamen Teiler von f und f' ausrechnet.
Solche Kurven spielen eine große Rolle in Zahlentheorie und Kryptographie, sie heißen elliptische Kurven, und wir werden später noch einmal darauf eingehen.

Bemerkung 2.3.4 Verallgemeinerung
In Verallgemeinerung von Satz 2.2.5 können wir jetzt sagen, dass zu jedem glatten Punkt auf einer Kurve $\tilde{C}$ über einem algebraisch abgeschlossenen Körper k eine diskrete Bewertung auf $k(C)$ gehört.
Umgekehrt sei eine solche diskrete Bewertung gegeben, die noch dazu nicht trivial sei. Wenn X und Y im Bewertungsring liegen, dann ist das Bewertungsideal ein maximales Ideal in $\mathcal{O}_P(C)$ in unserem alten Sinn, und damit ist sein Schnitt mit $k[C]$ im Koordinatenring maximal, und das heißt wegen 1.1.2, dass zu der Bewertung ein Punkt auf C gehört.
Wenn X und Y nicht beide zum Bewertungsring gehören, dann aber X^{-1} und/oder Y^{-1}, und man kann nach etwas Rechnung die Bewertung mit einem der unendlich fernen Punkte von $\tilde{C}$ assoziieren.

Wir können also die Punkte auf einer nichtsingulären projektiven Kurve über einem algebraisch abgeschlossenen Körper identifizieren mit Äquivalenzklassen von nichttrivialen diskreten Bewertungen des Funktionenkörpers.
Wenn der Körper k nicht algebraisch abgeschlossen ist, dann gibt es immer noch zu jedem glatten Punkt eine Bewertung, aber die Bewertungen kommen im allgemeinen her von Punkten in $\tilde{C}(\overline{k})$, wobei $\overline{k}$ der algebraische Abschluss von k ist. Jedoch liefern zwei Punkte dann die selbe Bewertung, wenn sie in einer Bahn unter der Aktion der Automorphismengruppen $\mathrm{Aut}(\overline{k} \mid k)$ liegen.

Diese Einsicht nehmen wir jetzt zum Anlass, um das Konzept der Kurve neu zu fassen.

Kapitel 3

Glatte Kurven

3.1 Ein Schema

Definition 3.1.1 Unebene Kurven

a) Es sei k ein Körper. Ein *Funktionenkörper über k* ist eine endlich erzeugte Körpererweiterung F vom Transzendenzgrad 1 über k.

Wir setzen zudem voraus, dass k in F algebraisch abgeschlossen ist, dass also alle $\alpha \in F$, die über k algebraisch sind, bereits in k liegen.

Mit anderen Worten: Für jedes $f \in F \backslash k$ ist $k[f]$ isomorph zum Polynomring in einer Variablen über k und $k(f) \subseteq F$ ist eine endliche Körpererweiterung.

Der Körper k heißt in diesem Fall der *Konstantenkörper.*

b) Es sei F ein Funktionenkörper über k. Die zu F assoziierte *Kurve* C ist dann definiert als die Menge aller (Äquivalenzklassen von) nichttrivialen diskreten Bewertungen auf F, die auf k trivial sind. Anders gesagt: Die Menge aller Bewertungsringe von F, die k enthalten und nicht F sind.

Wir werden gleich C mit einer Topologie versehen und die Funktionen in F als Funktionen auf C verstehen – wenn auch mit Anführungsstrichen.

Bemerkung 3.1.2 Krull-Akizuki

a) Wir halten ohne Beweis den folgenden Spezialfall des Satzes von Krull-Akizuki[1] fest:

Es sei $k \subset F$ ein Funktionenkörper und $f \in F \setminus k$. Dann ist der ganze Abschluss von $k[f]$ in F ein Dedekindring D_f, dessen Quotientenkörper F ist.

[1] Yasuo Akizuki, 1902 - 1984

b) Wir werden oft mit einer weniger weitreichenden Tatsache auskommen.

Der Ring $k[f]$ ist ein Hauptidealring, und wenn wir uns F als Teilring des Matrizenrings $k(f)^{d\times d}$ denken, ist $A := F \cap k[f]^{d\times d}$ ein endlich erzeugter $k[f]$-Modul (denn $k[f]$ ist ja noethersch) und eine ganze $k[f]-$Teilalgebra von F. Es sei $a_1, \ldots, a_d$ ein Erzeugendensystem von A als $k[f]-$Modul und $P_i := \sum_{j=0}^{???} c_j(f)X^j$ jeweils ein Ganzheitspolynom von a_i über $k[f]$. Offensichtlich enthält A eine $k(f)$-Basis von F, also ist F der Quotientenkörper von A.

Behauptung: Wenn $m \subset k[f]$ ein maximales Ideal in $k[f]$ ist, dann gibt es nur endlich viele maximale Ideale von A, die M enthalten.

Denn: Wenn $M \subset A$ ein maximales Ideal mit $m \subset M$ ist, dann ist A/M als $k[f]/m-$Vektorraum von den Klassen a_i mod M erzeugt, die alle über $k[f]/m$ algebraisch sind, also ist A/M isomorph zu einem endlichen algebraischen Erweiterungskörper von $k[f]/m$, der zu einem Teilkörper eines algebraischen Abschlusses $\overline{k}$ von k isomorph ist. Die a_i werden von der zugehörigen Restklassenabbildung auf Nullstellen der Polynome

$$\tilde{P}_i := \sum_{j=0}^{???} c_j(f \bmod m)X^j$$

abgebildet, und hierfür gibt es nur endliche viele Wahlen in $\overline{k}$.

Nebenbei bemerkt ist A/M eine endliche Erweiterung von k.

Natürlich gibt es immer mindestens ein solches maximales Ideal, wie uns das Lemma von Zorn verrät. Denn m enthält ja keine Einheit in $k[f]$ und daher auch keine Einheit in der ganzen Ringerweiterung A.

Hilfssatz 3.1.3 Fortsetzung folgt
Es sei $k \subset F$ ein Funktionskörper und $f \in F \setminus k$. Dann gibt es eine Fortsetzung der f-adischen Bewertung von $k(f)$ nach F.

Beweis. Auch hier wäre uns mit dem Satz von Krull-Akizuki schnell gedient, wir argumentieren aber etwas anders.
Es sei $\mathcal{S}$ die Menge aller Ringe $R \subset F$, die $k[f]$ umfassen und in denen f keine Einheit ist.
Diese Menge ist durch Inklusion geordnet, und für jede total geordnete Familie in $\mathcal{S}$ liegt auch die Vereinigung in $\mathcal{S}$. Demnach enthält $\mathcal{S}$ ein maximales Element B.
In B liegt ein maximales Ideal M, das f enthält, denn f ist auch in B keine Einheit. Dann ist aber f auch in

$$M^{-1}B := \{r/s \mid, r, s \in B, s \notin M\} \subseteq F$$

keine Einheit und damit $M^{-1} \subset B$. Es ist also B ein lokaler Ring.
Für jedes $x \in F \setminus B$ gilt: $f \in B[x]^\times$. Es gibt also $r_0, \ldots, r_n \in B$ sodass

$$1 = f \cdot \sum_{i=0}^{n} r_i x^i,$$

und damit

$$(1 - fr_0) = \sum_{i=1}^{n} f r_i x^i.$$

Da aber $1 - fr_0 \in B^\times$ eine Einheit ist, können wir dadurch teilen und erhalten eine Möglichkeit, x^{-n} als Polynom in x^{-1} vom Grad kleiner als m zu schreiben. Wäre nun auch x^{-1} nicht in B, so könnten wir dasselbe mit x^{-1} anstelle von x machen:

$$1 = \sum_{j=1}^{m} f s_j x^{-j}.$$

hier wählen wir n und m minimal. Dann folgt aus $n \geq m$

$$x^n = \sum_{j=1}^{m} f s_j x^{n-j},$$

und wir könnten weiter oben den Summanden mit x^n durch kleiner Potenzen von x ersetzen – n wäre also nicht minimal. Analog folgt aus $n \leq m$, dass m nicht minimal ist. Insgesamt kann keiner der beiden Fälle eintreten, und damit folgt:

$$\forall x \in F : x \notin B \Rightarrow x^{-1} \in B.$$

Es ist damit B ein Bewertungsring von F, in dessen maximalem Ideal M das alte f liegt, und damit das gesamte Bewertungsideal der vorgegebenen Bewertung auf $k(f)$.
Nun seien $t_0 = f, t_1, \ldots, t_e = 1$ Elemente in B, sodass $t_i/t_{i+1} \in M$. Wenn $t_1, \ldots, t_e$ über $k(f)$ linear abhängig wären, dann gäbe es eine nichttriviale Linearkombination

$$\sum_{i=1}^{e} a_i(f) t_i = 0, \quad a_i(f) \in k[f], \ f \text{ teilt nicht alle } a_i(f).$$

Wir nehmen das größte $h \leq e$ mit $a_h(0) \neq 0$ und sehen ein:

$$\sum_{i=1}^{h} a_i(0) t_i \in fB,$$

und damit

$$k \ni a_h(0) \in -\sum_{i=1}^{h-1} a_i(0) t_i/t_h + fB \subset M,$$

demnach $a_h(0) = 0$ im Widerspruch zur Wahl von h.
Eine Kette von Elementen t_i wie angegeben hat also höchstens Länge $[F : k(f)]$.
Wenn nun eine solche Kette maximaler Länge e gewählt ist, dann setze $t := t_{e-1}$.
Dann ist $M = tB$ (da B ein Bewertungsring ist...) und man kann nachrechnen, dass $\bigcap_i t^i B = \{0\}$.
Damit ist B ein diskreter Bewertungsring, die Bewertung auf B ist

$$v(b) := \max\{i \in \mathbb{N}_0 \mid b \in t^i B\}.$$

○

Definition 3.1.4 Funktionswerte von Funktionen
Es sei F ein Funktionenkörper über k und C die zugehörige Kurve.
Dann betrachten wir auf C die koendliche Topologie, d.h. die offenen Mengen sind genau $\emptyset$ und die Komplemente von endlichen Mengen.
Für $v \in C$ sei $\mathcal{O}_v$ der zugehörige Bewertungsring und $\mathbf{m}_v$ sein maximales Ideal.
Der Restklassenkörper $k_v := \mathcal{O}_v/\mathbf{m}_v$ ist dann eine endliche algebraische Erweiterung von k.
Denn: Es sei f ein Erzeuger des Bewertungsideals. Seien $u_1, \ldots, u_d \in \mathcal{O}_v$ Elemente, deren Restklassen modulo $\mathbf{m}_v$ über k linear unabhängig sind. Wären dann die Elemente selbst über $k(f)$ linear abhängig, so gäbe es eine Relation

$$0 = \sum_{i=1}^{d} a_i(f) u_i$$

mit Polynomen a_i, die nicht alle 0 und auch nicht alle Vielfache von f sind. Reduktion modulo $\mathbf{m}_v$ liefert einen Widerspruch.
Also ist $\dim_k(k_v) \leq \dim_{k(f)}(F)$.
Die Zahl $\deg(v) := [k_v : k]$ nennen wir auch den *Grad von* v.
Wir normieren v durch

$$v(f) := \sup\{k \in \mathbb{Z} \mid f \in \mathbf{m}_v^k\}.$$

Für $f \in F$ und $v \in C$ heißt f *regulär* in v, falls $v(f) \geq 0$, also falls $f \in \mathcal{O}_v$. Wenn f nicht regulär ist bei v, dann hat es dort einen *Pol* der Ordnung $|v(f)|$.
Die Restklasse von f modulo $\mathbf{m}_v$ heißt der *Wert von* f *bei* v.
Für eine offene Menge $\emptyset \neq U \subseteq C$ heißt eine Funktion $f \in F$ *regulär* auf U, falls $\forall v \in U : v(f) \geq 0$.
Anschaulich gesagt hat also f keine Polstelle auf U. Die Menge aller auf $U \neq \emptyset$ regulären Funktionen heißt $\mathcal{O}(U)$.
Künstlich setzen wir $\mathcal{O}(\emptyset) := \{0\}$.

Hilfssatz 3.1.5 Der Wert von Funktionswerten
Es seien k, F, C wie gehabt und $f \in F^\times$.

a) *Es gibt nur endlich viele $v \in C$ mit $v(f) \neq 0$.*

b) *Wenn f und g zwei Elemente von F sind, die bei unendlich vielen Stellen denselben Funktionswert haben, dann gilt $f = g$.*

c) *Wenn f überall regulär ist, ist $f \in k$.*

Beweis.
a)
Der Beweis der ersten Aussage ist klar für $f \in k$, da wir nur Bewertungen anschauen, die auf k trivial sind.
Sei also $f \in F \setminus k$. Dann ist $k[f]$ isomorph zum Polynomring, und F ist eine endliche algebraische Erweiterung von $k(f)$.
Wir nehmen einen Ring A wie in 3.1.2 b) und sehen, dass zu jeder Bewertung v mit $f \in \mathbf{m}_v$ auch ein maximales Ideal von A gehört, das f enthält. Aber hier gibt es nur endlich viele, also gibt es auch nur endliche viele solcher Bewertungen.
Analog gibt es nur endlich viele Bewertungen, für die f^{-1} im Bewertungsideal liegt.
Damit ist die erste Aussage gezeigt.
b) folgt aus a), da $f - g$ bei unendlich vielen Stellen $v \in C$ verschwindet, also dort im Bewertungsideal liegt.
Für c) schließlich benutzen wir für f^{-1} die Aussage von 3.1.3 und finden damit ein $v \in C$ mit $v(f^{-1}) > 0$, demnach also $v(f) < 0$. ◯

Bemerkung 3.1.6 Liouville
Die letzte Aussage im vorangegangenen Hilfssatz nennt man auch den Satz von Liouville. Nimmt man die klassische Variante dieses Satzes aus der Funktionentheorie, so sagt er unter Verwendung des Riemannschen Hebbarkeitssatzes, dass eine auf ganz $\mathbb{C} \cup \infty$ holomorphe Funktion konstant ist.
Bei uns sagt der Satz: Eine Funktion aus F, die auf ganz C definiert ist, ist konstant (gehört zum Konstantenkörper).
Für den Fall, dass k algebraisch abgeschlossen ist, sehen wir auch, dass eine nichtkonstante Funktion jeden Wert aus k annehmen muss, also als surjektive Abbildung von C nach $\mathbb{P}^1(k)$ gedeutet werden kann.

Bemerkung 3.1.7 Garbeneigenschaft

a) Für offenes $U \subseteq C$ können wir jetzt $f \in \mathcal{O}(U)$ identifizieren mit der „Abbildungsvorschrift“

$$U \ni v \mapsto f(v) \in k_v.$$

Der Schönheitsfehler besteht nur darin, dass k_v von v abhängt, wir also im allgemeinen keine sinvvolle Abbildung von U irgendwohin bekommen.

Wenn k algebraische abgeschlossen ist, ist stets $k_v = k$, und alles ist gut.

b) Für offene Mengen $U \subseteq V \subseteq C$ haben wir eine Inklusion

$$\rho_U^V : \mathcal{O}(V) \subseteq \mathcal{O}(U).$$

Diese Inklusion nennen wir die *Restriktion* von V nach U.

Sie erfüllt die Eigenschaften:

$$\forall U \subseteq V \subseteq W : \rho_U^V \circ \rho_V^W = \rho_U^W$$

und – falls $U = \cup_i U_i$ eine Vereinigung von offenen Teilmengen ist –

$$\forall f_i \in \mathcal{O}(U_i) : \quad \begin{array}{l} \text{falls } \forall i,j : \rho_{U_i \cup U_j}^{U_i}(f_i) = \rho_{U_i \cup U_j}^{U_j}(f_j), \\ \text{dann } \exists! f \in \mathcal{O}(U) : \forall i : f|_{U_i} = f_i. \end{array}$$

Damit wird diese Vorgabe zu einer *Garbe* auf C.

Diesen Begriff aus der Topologie werden wir nicht weiter vertiefen.

c) Insgesamt wird unser topologischer Raum C mit dieser Funktionsgarbe ein *lokal geringter Raum*, von dem man nachrechnen kann, dass er ein *Schema* ist. Auch dies soll hier nicht vertieft werden, wir benutzen diese Terminologie auch nie mehr.

Hilfssatz 3.1.8 Die Unabhängigkeit der Bewertungen
Es seien F ein Körper, $v_1, \ldots, v_h$ paarweise verschiedene nicht-triviale, normierte, diskrete Bewertungen auf F sowie $m_1, \ldots, m_h \in \mathbb{Z}$.

a) Für alle $u_1, \ldots, u_h \in F$ existiert ein ein $u \in F$, sodass

$$\forall i : v_i(u - u_i) \geq m_i.$$

b) Es existiert ein $u \in F$ sodass

$$\forall i : v_i(u) = m_i.$$

Beweis. Zunächt können wir aus a) tatsächlich b) folgern. Dazu wählen wir uns $u_i \in F$ mit $v_i(u_i) = m_i$ und anschließend gemäß a) ein $u \in F$ mit $\forall i : v_i(u_i - u) \geq m_i + 1$.
Dann gilt

$$v_i(u) = v_i(u_i + (u - u_i)) = \min\{v(u_i), v_i(u - u_i)\} = m_i$$

wegen der ultrametrischen Ungleichung.

Der Beweis von a) läuft nun induktiv über h. Der Fall $h = 1$ ist offensichtlich. Sei $h > 1$ und die Behauptung für $h - 1$ Bewertungen gezeigt.

Dies nutzen wir jetzt aus, um zu zeigen, dass die v_i über $\mathbb{Q}$ linear unabhängig sind.
Wir nehmen rationale Zahlen $r_i, 1 \leq i \leq h-1$, sodass

$$\forall z \in F : v_h(z) = \sum_i r_i v_i(z).$$

Wenn alle r_i nicht-negativ wären, so gäbe es zwei positive, und wir könnten notfalls v_h mit einem anderen v_i vertauschen, um in folgende Situation zu gelangen: Ohne Einschränkung ist mindestens ein r_i negativ. Wegen b) gibt es Funktionen $f, f' \in F^\times$ mit (hier läuft i von 1 bis $h-1$)

$$\begin{array}{lll} v_i(f) = 0, & v_i(f') = 1, & \text{falls } r_i \geq 0, \\ v_i(f) = 1, & v_i(f') = 0, & \text{falls } r_i < 0 \end{array}$$

Wir benutzen die ultrametrische Ungleichung, um einzusehen, dass

$$\forall i : \ v_i(f+f') = 0, \quad \text{also} \quad v_h(f+f') = 0.$$

Andererseits ist $v_h(f) < 0$, da in der Summe ein negativer Summand, aber kein positiver auftaucht. Daher gilt

$$v_h(f+f') = \min\{v_h(f), v_h(f')\} < 0 - \text{ein Widerspruch!}$$

Aus dieser linearen Unabhängigkeit folgt, dass die Vektoren

$$\{(v_i(z))_{i=1,\ldots,h} \mid z \in F^\times\} \in \mathbb{Z}^h$$

den ganzen Vektorraum aufspannen, es also existieren $z_1, \ldots, z_h$, sodass die Matrix $(v_i(z_j)) \in \mathbb{Z}^{h \times h}$ Rang h hat. Insbesondere gibt es auch rationale Zahlen $c_{j,k}$, sodass

$$\sum_{j=1}^{h} v_i(z_j) c_{j,k} = \begin{cases} -1 & \text{falls } i = k, \\ 1 & \text{falls } i \neq k. \end{cases}$$

Wir multiplizieren das mit einem gemeinsamen Nenner d der $c_{j,k}$ durch und erhalten

$$v_i(\prod_j z_j^{dc_{j,k}}) = \begin{cases} -d & \text{falls } i = k, \\ d & \text{falls } i \neq k. \end{cases}$$

Wir setzen $y_k := \prod_j z_j^{dc_{j,k}}$ und $x_k := \frac{1}{1-y_k^{-1}}$.
Dann folgt

$$v_i(x_k) = d, \text{ falls } i \neq k, \ v_i(1-x_i) = d.$$

Nun kann man nachrechnen, dass für $u := \sum x_i u_i$ und hinreichend großes d die Behauptung gilt. ◯

Bemerkung 3.1.9 Zariskitopologie
Nun sei wieder C die Kurve zu einem gegebenen Funktionenkörper F und $v \in C$ ein beliebiger Punkt. Dann gibt es zwei Funktionen $f, g \in F^\times$, sodass v die einzige Stelle ist, wo sowohl f als auch g eine Nullstelle besitzen.
Denn: Wähle ein $f \in F^\times$ mit $f(v) = 0$, d.h. $v(f) > 0$. Dann gibt es endlich viele Stellen $v_1 := v,\ v_2, \ldots, v_h \in C$, bei denen f verschwindet.
Nach Teil b) des eben gesehenen Satzes gibt es dann auch eine Funktion $g \in F^\times$, für die $v_1(g) = 1,\ v_2(g) = v_3(g) = \cdots = v_h(g) = 0$ gilt. Daher haben f und g nur die Nullstelle v gemeinsam.
Aus diesem Grund dürfen wir die koendliche Topologie wieder als eine Zariskitopologie auffassen: Abgeschlossene Mengen sind (Durchschnitte von) Nullstellenmengen von Funktionen.

3.2 Divisoren

Um eine suggestivere Notation zu bekommen werden wir die Elemente unserer Kurve C in Zukunft mit P notieren, und die zugehörige normierte Bewertung mit v_P. Im ganzen Abschnitt ist C die Kurve zu einem fest vorgegebenen Funktionenkörper F mit Konstantenkörper k.

Definition 3.2.1 Divisor

a) Ein *Divisor* auf C ist eine formale endliche Linearkombination

$$D = \sum_{P \in C} a_P \cdot P,\ a_P \in \mathbb{Z},\ \text{ fast alle } a_P = 0.$$

Wir schreiben notfalls auch $a_P = a_P(D)$, wenn mehrere Divisoren gleichzeitig behandelt werden.

Die Menge $Div(C)$ ist die Menge der Divisoren auf C, also die freie abelsche Gruppe über C.

Zwei Divisoren werden durch koeffizientenweise Addition addiert.

Ein Divisor heißt *positiv*, wenn $\forall P \in C : a_P \geq 0$.

Der *Grad eines Divisors* $D = \sum a_P \cdot P$ ist definiert als

$$\deg(D) := \sum_{v \in C} \deg(P) \cdot a_P.$$

Wir werden noch sehen, dass es sinnvoll ist, hier die Bewertungen durch den Grad ihres Restklassenkörpers $k_P = k_{v_P}$ über k zu gewichten.

Ein Divisor heißt *effektiv*, wenn seine Koeffizienten allesamt nicht negativ sind.

Wenn D, D' zwei Divisoren sind, dann sagen wir

$$D \geq D' :\Leftrightarrow D - D' \text{ effektiv.}$$

Der *Träger eines Divisors* D ist

$$\text{supp}(D) := \{P \in C \mid a_P(D) \neq 0\}.$$

b) Für $f \in F^\times$ setzen wir

$$(f) := \sum_{P \in C} v_P(f) \cdot P.$$

Dies ist der zu f gehörende *Hauptdivisor*. Dieser zerfällt als Differenz des *Nullstellendivisors*

$$(f)_0 := \sum_{P : v_P > 0} v_P(f) \cdot P$$

und des *Polstellendivisors*

$$(f)_\infty := -\sum_{P : v_P < 0} v_P(f) \cdot P.$$

Bemerkung 3.2.2 „Weierstraß[2] – Problem“
Wenn D ein Divisor auf C ist, dann stellt sich die Frage, ob es ein Hauptdivisor ist.
Also: Kann man ein $f \in F$ finden (oder konstruieren), das eine vorgegeben Verteilung an Null- und Polstellen hat? In der Funktionentheorie wird so etwas typischer Weise mit einem Weierstraß-Produkt versucht, wobei man natürlich den Bereich der Polynome verlässt.
Im Allgemeinen wird die Antwort also negativ sein, aber man sollte sich trotzdem die Frage für den Funktionenkörper $\mathbb{C}(X)$ durch den Kopf gehen lassen. Hier gibt es die Bewertungen $v_z,\ z \in \mathbb{C}$ und v_∞, die negative Gradbewertung.
Wenn $\frac{f}{g} \in \mathbb{C}(X)$ gegeben ist, dann ist

$$(f/g) = (f) - (g).$$

Für jedes Polynom gilt, dass

$$(f) = \sum_{z \in \mathbb{C}} \text{ord}_z(f) v_z - \deg(f) v_\infty.$$

An dieser Formel sieht man, dass der Grad jedes Hauptdivisors 0 ist.

[2]Karl Theodor Wilhelm Weierstraß, 1815-1897

Ist umgekehrt $D = \sum_z a_z v_z + a_\infty v_\infty$ ein Divisor von Grad 0, so ist er auch ein Hauptdivisor. Denn:
Es seien $f = \prod_{z,\ a_z>0}(X-z)^{a_z}$ und $g = \prod_{z,\ a_z<0}(X-z)^{-a_z}$. Dann ist $(f/g) = (f) - (g)$ ein Divisor, der für jedes $z \in \mathbb{C}$ denselben Koeffizienten bei v_z stehen hat wie D, und der auch Grad 0 hat. Also stimmt auch der Koeffizient bei a_∞ überein.
Insgesamt gilt hier, dass genau die Divisoren von Grad 0 Hauptdivisoren sind. Das stimmt übrigens für jeden Konstantenkörper k.
Ganz so einfach wird die Antwort im Allgemeinen aber nicht sein. Sie lässt auch noch ein bisschen auf sich warten.

Definition 3.2.3 Abschwächung
Es sei D ein Divisor auf C. Dann gehört dazu der k-Vektorraum

$$L(D) := \{f \in F^\times \mid (f) + D \geq 0\} \cup \{0\}.$$

Dies ist (bis auf den Vorzeichenwechsel) motiviert durch das eben vorgestellte Problem.
Aus $D \leq D'$ folgt dann $L(D) \subseteq L(D')$.
Wo D einen negativen Koeffizienten a_P hat, muss f eine Nullstelle der Ordnung $\geq |a_P|$ haben. Wo a_P positiv ist darf f eine Polstelle haben, aber bitte nicht mit Ordnung größer als a_P.
Nach 3.1.6 gilt $L(0) = k$.
Für einen Divisor $D < 0$ gilt sogar $L(D) = \{0\} \subset F$.
Mit $l(D)$ bezeichnen wir die k-Dimension von $L(D)$.

Satz 3.2.4 Endlichdimensional
Für jeden Divisor D auf C ist $l(D)$ endlich. Weiter gilt für Divisoren $D' \leq D$:

$$l(D) - l(D') \leq \deg(D) - \deg(D').$$

Beweis.
Wir beweisen erst die zweite Behauptung in Form einer Abschätzung für die Dimension von $L(D)/L(D')$.
Dazu seien der Träger von D und der von D' in der endlichen Menge $S \subset C$ enthalten. Wir betrachten die folgenden Räume, die einfacher zugänglich sind als die „global“ definierten Räume $L(D), L(D')$:

$$M(D) := \{f \in F^\times \mid \forall P \in S : a_P(D) + v_P(f) \geq 0\} \cup \{0\} = \cap_{P\in S}\mathbf{m}_P^{-a_P(D)}$$

und analog

$$M(D') := \{f \in F^\times \mid \forall P \in S : a_P(D') + v_P(f) \geq 0\} \cup \{0\} = \cap_{P\in S}\mathbf{m}_P^{-a_P(D')}.$$

Mit $a_P(D)$ ist hierbei der Koeffizient bei P im Divisor D gemeint usw.

Wir haben hier $L(D') = L(D) \cap M(D')$. Das liefert

$$L(D)/L(D') = L(D)/(L(D) \cap M(D')) \cong (L(D)+M(D'))/M(D') \subseteq M(D)/M(D').$$

Wohlgemerkt achten wir bei $M(D)$ und $M(D')$ nur mehr auf die Funktionen bei endlich vielen Stellen, und jetzt nutzen wir, dass für jede Stelle $P \in S$ und jedes $n \in \mathbb{Z}$ die Menge $\mathbf{m}_P^n/\mathbf{m}_p^{n+1}$ ein eindimensionaler k_P-Vektorraum ist, und damit allgemeiner der k-Vektorraum $\mathbf{m}_P^n/\mathbf{m}_p^{n+t}$ die Dimension $\deg(P) \cdot t$ hat.
Da wir an den endlich vielen Stellen aus S die Vorgaben durch Funktionen aus F präzise und unabhängig voneinander erfüllen können, gilt wie im chinesischen Restsatz

$$M(D)/M(D') \cong \bigoplus_{P \in S} \mathbf{m}_P^{a_P(D)}/\mathbf{m}_P^{a_P(D')},$$

und dieser Vektorraum hat k-Dimension

$$\sum_{P \in S} (a_P(D) - a_P(D'))\deg(P) = \deg(D) - \deg(D').$$

Da nun für jeden Divisor D ein kleinerer negativer Divisor D' existiert, für den wir uns schon $l(D') = 0$ überlegt haben, folgt

$$l(D) = l(D) - l(D') \leq \deg(D) - \deg(D') < \infty.$$

Dass das dann wiederum mit der Formel für die Dimension des Faktorraums die zweite Behauptung impliziert ist klar. ◯

Satz 3.2.5 Der Grad eines Hauptdivisors
Es sei $f \in F^\times$. Dann hat der Hauptdivisor (f) Grad 0.
Genauer haben sowohl $(f)_0$ als auch $(f)_\infty$ Grad $[F : k(f)]$.

Beweis.
Wir zeigen $\deg((f)_0) = [F : k(f)] =: n$. Aus Symmetriegründen folgt dann auch $\deg((f)_\infty) = \deg((f^{-1})_0) = [F : k(f)]$, und damit $\deg(f) = 0$.
Es sei $N := \{P \in C \mid f(P) = 0\}$. Dies ist eine endliche Menge. Dann ist

$$\deg((f)_0) = \sum_{P \in N} v_P(f) \cdot \deg(P).$$

Um dies in den Griff zu bekommen betrachten wir

$$R := \cap_{P \in N} \mathcal{O}_{v_P} = \{x \in F \mid \forall P \in N : v_P(x) \geq 0\}.$$

Ein Element r hierin ist genau dann invertierbar, wenn

$$\forall P \in N : v_P(r) = 0.$$

Wie in 3.1.8 b) gesehen gibt es Funktionen r_P in F, sodass $v_P(r_P) = 1$ und $v_Q(r_P) = 0$ für alle $Q \in N, Q \neq P$.
Diese Funktionen sind Primelemente in R, und jedes Element $r \in R$ lässt sich schreiben als

$$r = \prod_{P \in N} r_P^{v_P(r)} \cdot \frac{r}{\prod_{P \in N} r_P^{v_P(r)}}.$$

Daher ist R ein Hauptidealring mit nur endlich vielen Primidealen.
Wir schreiben nun f als

$$f = \prod_{P \in N} r_P^{v_P(f)} \cdot u, \ u \in R^\times,$$

und sehen wegen

$$(f)_0 = \sum_{P \in N} v_P(f) \cdot P,$$

dass

$$\begin{aligned} \deg((f)_0) &= \textstyle\sum_{P \in N} v_P(f) \cdot [k_P : k] \\ &= \textstyle\sum_P \dim_k(R/r_P^{v_P(f)}R) \\ &= \dim_k(R/\textstyle\prod r_P^{v_P(f)}R) = \dim_k(R/fR). \end{aligned}$$

Hier benutzen wir zwischendurch den Chinesischen Restsatz für die paarweise teilerfremden Funktionen r_P.
Wenn nun $u_1, \ldots, u_e \in R$ Vertreter einer k-Basis von R/fR sind, dann folgt wieder wie in 3.1.4, dass $u_1, \ldots, u_e$ linear unabhängig über $k(f)$ sind, also $\deg((f)_0) \leq n$.
Sei umgekehrt $u_1, \ldots, u_n$ eine Basis von F als $k(f)$-Vektorraum, sodass alle u_i ganz über $k[f^{-1}]$ sind. Dann ist eine Polstelle von u_i auch eine Polstelle von f^{-1}, da Bewertungsringe ganz abgeschlossen sind, also u_i überall definiert ist, wo auch f^{-1} definiert ist.
Es gibt also ein $s \in \mathbb{N}$, sodass

$$(f^s)_0 + (u_i) \geq 0, \ 1 \leq i \leq n.$$

Das fixieren wir und machen es mit einem $t \in \mathbb{N}$ noch größer: die $n(t+1)$ Elemente $f^{-j}u_i, \ 0 \leq j \leq t, 1 \leq i \leq n$, sind über k linear unabhängige Elemente in $L((f^{s+t})_0)$, und es folgt mit unserer Abschätzung für die Dimension dieses Vektorraums:

$$n(t+1) \leq l((f)_0) + (s+t-1)\deg((f)_0).$$

Lässt man hier t gegen unendlich gehen, so folgt $n \leq \deg((f)_0)$, was die behauptete Gleichheit nach sich zieht. ◯

In der Theorie der elliptischen Funktionen ist diese Aussage einer der Sätze von Liouville und wird mit dem Residuensatz bewiesen. Die Ordnung einer Funktion f an der Stelle a ist ja das Residuum von f'/f bei a, und man kann zeigen, dass die Summe aller Residuen 0 ist.

Definition 3.2.6 Die Divisorenklassengruppe
Die Menge aller Hauptdivisoren ist eine Untergruppe von $\mathrm{Div}(C)$, und die Faktorgruppe heißt *Divisorenklassengruppe* oder auch *Picardgruppe*[3] von C : $\mathrm{Pic}(C)$.
Aufgrund des letzten Satzes sind die Hautpdivisoren sogar in der Gruppe der Divisoren von Grad 0 enthalten; die zugehörige Faktorgruppe heißt $\mathrm{Pic}_0(C)$.
Sie enthält für die Kurve C typische Obstruktionen dagegen, dass ein Divisor vom Grad 0 tatsächlich ein Hauptdivisor ist.
Für den rationalen Funktionenkörper $F = k(X)$ ist C die projektive Gerade, und wir finden wie in 3.2.2, dass jeder Divisor vom Grad 0 ein Hauptdivisor ist: $\mathrm{Pic}_0(\mathbb{P}^1) = 0$.

Bemerkung 3.2.7 Ein Minimierungsproblem
In 3.2.4 haben wir gesehen, dass für Divisoren $D' \leq D$ immer gilt

$$l(D) - \deg(D) \leq l(D') - \deg(D').$$

Eigentlich wollen wir auch eine untere Schranke für $l(D)$ finden, und hierfür ist es hilfreich, sich zu überlegen, dass $l(D) - \deg(D)$ nach unten beschränkt ist.
Auf jeden Fall merken wur uns die obige Ungleichung gut, denn sie ist der Dreh- und Angelpunkt für die kommenden Überlegungen.

Hilfssatz 3.2.8 Ein Minimum
Es sei $f \in F \setminus k$. Dann gibt es eine Zahl μ, sodass

$$\forall m \in \mathbb{N} : l((f^m)_0) - \deg((f^m)_0) \geq -\mu.$$

Beweis. Wir arbeiten mit der Abschätzung vom letzten Satz 3.2.5 in der Form

$$\exists s \in \mathbb{N} : \forall t \geq 0 : \deg((f^{t+1})_0) \leq l(f^{s+t}).$$

Hier steht links das damalige $n(t+1)$. Für $m \geq s$ wird daraus

$$l((f^m)_0) - \deg((f^m)_0) \geq \deg((f^{1-s})_0) = (1-s)\deg((f)_0) := -\mu.$$

Für $0 \leq m < s$ gilt $(f^m)_0 \leq (f^s)_0$, und deshalb gilt wieder

$$l((f^s)_0) - l((f^m)_0) \leq \deg((f^s)_0) - \deg((f^m)_0),$$

was auch für diesen Wert von m die gewünschte Beziehung nach sich zieht. ◯

Satz 3.2.9 Ein Satz von Riemann[4]
Sei $f \in F \setminus k$ fest gewählt und

$$\mu := \min\{l((f^m)_0) - \deg((f^m)_0) \mid m \in \mathbb{Z}\}.$$

Dann gilt für jeden Divisor D auf C die Ungleichung

$$l(D) - \deg(D) \geq \mu.$$

[3](Charles) Emile Picard, 1856-1941
[4]Bernhard Riemann, 1826 - 1866

Beweis. Wir schreiben $D = N - P$ als Differenz zweier positiver Divisoren und sehen wegen $N \geq D$ und der letzten Bemerkung, dass es reicht, die Behauptung für Divisoren $D \geq 0$ zu beweisen.
Wir dürfen also voraussetzen, dass D positiv ist, und tun dies hiermit.
Dann ist $(f^m)_0 - D \leq (f^m)_0$, und es folgt wieder

$$l((f^m)_0 - D) - \deg((f^m)_0 - D) \geq l((f^m)_0) - \deg((f^m)_0) \geq \mu.$$

Wegen $\deg((f^m)_0 - D) = m[F : k(f)] - \deg(D)$ folgt, dass für großes m die Dimension $l((f^m)_0 - D)$ positiv ist:

$$\exists 0 \neq h \in L((f^m)_0 - D).$$

Die Divisoren D und $D - (h)$ haben denselben Grad (wegen 3.2.5) und die Abbildung

$$L(D) \ni a \mapsto ha \in L(D - (h))$$

ist eine Bijektion, also stimmen auch $l(D)$ und $l(D - (h))$ überein.
Es folgt

$$l(D) - \deg(D) = l(D - (h)) - \deg(D - (h)) \geq l((f^m)_0) - \deg((f^m)_0) \geq \mu,$$

wobei wir zwischendurch wieder 3.2.4 und dieses Mal $(f^m)_0 \geq D - (h)$ benutzen. ◯

Wir nehmen diesen Satz zum Anlass für eine Definition.

Definition 3.2.10 Das Geschlecht von C
Es sei F ein Funktionenkörper über k und C die zugehörige Kurve. Dann ist das Geschlecht $g = g(C)$ definiert durch

$$1 - g(C) := \min\{l(D) - \deg(D) \mid D \in \mathrm{Div}(C)\}.$$

Es ist der Inhalt der beiden letzten Sätze, dass dieses Minimum eine ganze Zahl ist.
Wegen $l(0) - \deg(0) = 1$ ist $g \geq 0$.
Zunächst ist das Geschlecht einfach eine Zahl, der man keine schöne Interpretation ansieht, aber wenn $k = \mathbb{C}$ gilt, dann ist C auch eine kompakte Riemannsche Fläche, also insbesondere eine kompakte orientierbare Fläche, die als solche auch ein Geschlecht hat („Anzahl der Henkel“), und die beiden Definitionen liefern dieselbe Zahl.

Beispiel 3.2.11 na was wohl
a) Für $F = k(X)$ ist C wie gelernt die projektive Gerade über k.
Im Beweis von 3.2.9 haben wir gelernt, dass das fragliche Minimum bereits für positive Divisoren angenommen wird, und wir uns sogar auf die Vielfachen des Nullstellendivisors von X beschränken können.

Hier gilt

$$\deg((X^m)_0) = m.$$

Es seien $p, q \in k[X]$ teilerfremd, sodass $z = p(X)/q(X) \in L((X^m)_0)$. Jeder normierte irreduzible Teiler von $q(X)$ entspricht einer Bewertung von $k(X)$, bei der z einen Pol hat. Da dies nur bei der X-adischen Bewertung passieren darf, folgt, dass q eine Potenz von X ist.
Außerdem ist z bei unendlich definiert, was heißt, dass der Grad von p höchstens so groß wie der Grad von q ist. Es folgt

$$L((X^m)_0) = \{p(X)/X^m \mid \deg(p) \leq m\}.$$

Dieser k-vektorraum ist isomorph zum Vektorraum der Polynome vom Grad $\geq m$ und hat daher Dimension $m + 1$. Es folgt $l((X^m)_0) - \deg((X^m)_0) = 1$ für alle $m \in \mathbb{N}$ und damit $g = 0$.
Die projektive Gerade hat Geschlecht 0. Für $k = \mathbb{C}$ entspricht dies der Tatsache, dass die Riemannsche Zahlenkugel Geschlecht 0 hat: ein Sphäre ohne Henkel.

b) Sei umgekehrt F ein Funktionenkörper, sodass C Geschlecht 0 hat und einen Punkt von Grad 1 besitzt:

$$\exists P \in C : \deg(P) = 1.$$

Wir fassen P als Divisor auf.
Dann ist $l(P) - \deg(P) \geq 1 - g = 1$, also $l(P) \geq 2$ und es gibt in $L(P)$ eine nicht konstante Funktion f, deren Polstellendivisor aber kleiner als P ist. Da der Polstellendivisor nicht 0 ist, ist er P. Da demnach ist $\deg((f)_\infty) = 1$ und damit auch $[F : k(f)] = 1$, also $F = k(f)$.
c) Nun stellt sich noch die Frage, ob es eine Kurve vom Geschlecht 0 gibt, die keinen Punkt vom Grad 1 besitzt. Dies ist tatsächlich der Fall, wie uns der Funktionenkörper $F = \mathbb{R}(X)[Y]/(X^2 + Y^2 + 1)$ lehrt.
Wo X keinen Pol hat, hat auch Y keinen Pol, und im Restklassenkörper stimmt für die klassen ξ von X unf η von Y die Gleichung

$$\xi^2 + \eta^2 = -1,$$

jedoch ist der Restklasenkörper eine endliche Erweiterung von $\mathbb{R}$, also $\mathbb{C}$. Ein ähnliches Argument stimmt dort, wo X und Y einen Pol haben.
Der Nullstellendivisor von X^{-1} hat Grad 2, denn F hat Grad 2 über $\mathbb{R}(X)$. Also hat X^{-1} nur eine Nullstelle. Zu $L((X^{-m})_0)$ gehören die Funktionen

$$1, X, \ldots, X^m, Y, YX, \ldots, YX^{(m-1)},$$

die über $\mathbb{R}$ linear unabhängig sind. Hier muss man wieder bedenken, dass X und Y denselben Polstellendivisor haben. Es ist also

$$l((X^{-m})_0) \geq 2m + 1, \quad \text{also} \quad l((X^{-m})_0) - \deg((X^{-m})_0) \geq 1$$

für alle $m \in \mathbb{N}$, und damit ist das Geschlecht höchstens 0. Kleiner kann es jedoch nicht sein.

3.3 Der Satz von Riemann-Roch

Definition 3.3.1 Präadele
a) Es seien F und C wie gehabt. Der *Präadelring von* F ist dann

$$A := \{(f_P)_{P\in C} \mid f_P \in F, \quad \text{fast alle } f_P \in \mathcal{O}_P\}.$$

Ein Element hiervon heißt ein Präadel.
Es ist klar, dass A ein Ring ist; er enthält F als Teilring via

$$F \ni f \mapsto (f, f, f, f, f, f \dots) \in A.$$

Das „Prä“ wird man los, indem man in der Definition $f_P \in F_P$ fordert, was die Komplettierung von F an der zu P gehörenden Bewertung ist. Hierzu wird eventuell später noch etwas gesagt.
Der Adel kommt hier auf folgende Weise ins Spiel: Es wurde ursprünglich und wohl zunächst im Zahlkörperfall die sogenannte Idelegruppe gebildet, die die gebrochenen Ideale im Zahlkörper (hochgradig redundant) parametrisiert und ihren Namen daher hat. Der Adelring ist eine Art additive Variante der Idelegruppe, weshalb das I zu einem A wird.

b) Für einen Divisor $D = \sum_P a_P P$ auf C sei

$$A(D) := \{(f_P)_P \in A \mid \forall P \in C : v_P(f_P) + a_P \geq 0\}.$$

Offensichtlich gilt hier für $D' \leq D$, dass $A(D') \subseteq A(D)$.
Außerdem ist $A(D) \cap F = L(D)$, was den Ring für uns interessant macht.
Ein Vergleich zum Beweis von 3.2.4 zeigt, dass

$$\dim_k(A(D)/A(D')) = \deg(D) - \deg(D').$$

Die dortige Ungleichung wird hier zur Gleichung, denn in A haben wir viel größere Freiheiten, Elemente zu wählen.

Hilfssatz 3.3.2 Eine Dimensionsabschätzung
Für Divisoren $D \leq \tilde{D}$ auf C gilt

$$\dim[(A(\tilde{D})+F)/(A(D)+F)] = l(D)-\deg(D)-(l(\tilde{D})-\deg(\tilde{D})) \leq l(D)-\deg(D)+g-1.$$

Beweis. Wir benutzen ein paar Mal Isomorphiesätze:

$$\begin{aligned}(A(\tilde{D}) + F)/(A(D) + F) &\cong A(\tilde{D})/[A(\tilde{D}) \cap (A(D) + F)] \\ &\cong A(\tilde{D})/[A(D) + L(\tilde{D})] \\ &\cong [A(\tilde{D})/A(D)] \,/\, [(A(D) + L(\tilde{D}))/A(D)]\end{aligned}$$

und wegen

$$(A(D) + L(\tilde{D}))/A(D) \cong L(\tilde{D})/L(D)$$

und der Bemerkung eben folgt die Behauptung. ◯

Bemerkung 3.3.3 Endlichdimensional
Es seien D ein Divisor auf C und $a_1, \ldots, a_r \in A$. Diese endlich vielen Präadele liege in einem gemeinsamen $A(\tilde{D})$, wobei wir $\tilde{D} \geq D$ nehmen können. Das zeigt zusammen mit dem letzten Hilfssatz, dass die a_i in $A/(A(D)+F)$ k-linear abhängig sind.
Also hat $A/(A(D)+F)$ als k-Vektorraum höchstens Dimension $\delta(D) := l(D) - \deg(D) + g - 1$.
Wir nennen $\delta(D)$ den *Spezialitätsgrad* von D.

Hilfssatz 3.3.4 Eine Dimensionsformel
Für jeden Divisor D auf C gilt $\delta(D) = \dim_k(A/(A(D)+F))$.

Beweis. Wir müssen nur noch $\leq$ zeigen.
Hierzu wählen wir einen Divisor D_0, für den $l(D_0) - \deg(D_0) = 1 - g$ gilt. Für jeden größeren Divisor gilt dies dann auch, also können wir D_0 auch größer als D wählen. Der Untervektorraum $(A(D_0)+F)/(A(D)+F)$ von $A/(A(D)+F)$ hat dann aber nach dem Beweis von 3.3.2 genau Dimension $l(D) - \deg(D) - (l(D_0) - \deg(D_0)) \geq l(D) - \deg(D) + g - 1 = \delta(D)$. ◯

Definition 3.3.5 Pseudodifferentiale
Eine k-Linearform ω auf A heißt eine *Pseudodifferentialform* auf C, wenn ein Divisor D existiert, sodass $A(D) + F \subseteq \mathrm{Kern}(\omega)$.
Die Menge aller Pseudodifferentialformen ist ein k-Vektorraum namens Ω oder Ω_C.
Für einen Divisor D setzen wir

$$\Omega(D) := \{\omega \in \mathrm{Hom}_k(A, k) \mid A(D) + F \subseteq \mathrm{Kern}(\omega)\}.$$

Dann gilt nach Definition

$$\Omega = \bigcup_D \Omega(D).$$

Wir können $\Omega(D)$ mit dem Dualraum von $A/(A(D)+F)$ identifizieren, dessen Dimension wir eben berechnet haben, wissen also auch, dass

$$\dim_k(\Omega(D)) = \delta(D).$$

Für den Nulldivisor 0 heißt $\Omega(0)$ auch der Raum der „Pseudodifferentialformen der ersten Art“. Seine Dimension ist g.
Ω erhält eine F-Vektorraumstruktur durch

$$\forall \omega \in \Omega, f \in F, a \in A : (f\omega)(a) := \omega(fa).$$

Dies ist wieder eine Linearform auf A, und der Kern enthält $f^{-1} \cdot (A(D)+F) = A(D + (f)) + F$, wenn $A(D)+F$ im Kern von ω liegt.

Hilfssatz 3.3.6 Eindimensional
$\dim_F(\Omega) = 1$.

Beweis. Es seien $\omega_1, \omega_2 \in \Omega$ zwei von Null verschiedene Pseudodifferentiale. Für einen geeigneten Divisor D liegen beide in $\Omega(D)$. Wir dürfen D auch durch einen kleineren Divisor ersetzen und nehmen OBdA an, dass er negatievn Grad hat. Nun betrachten wir für $n \in \mathbb{N}$ in $\Omega((n+1)D)$ die beiden Untervektorräume

$$L(-nD)\omega_i, \ i = 1 \text{ oder } 2.$$

NB: $f\omega_i$ verschwindet wegen $(f) + D \geq nD + D$ tatsächlich auf $A((n+1)D)$. Die Abbildungen sind injektiv, da ω_i nicht 0 ist. Die Dimensionen der Bilder addieren sich daher zu

$$2l(-nD) \geq -2n \deg(D) + 2 - 2g,$$

und wenn $n > \frac{3g-3}{|\deg(D)|}$ ist dies größer als

$$l((n+1)D) - \deg((n+1)D) + g - 1 = \delta((n+1)D) = \dim_k \Omega((n+1)D).$$

Die beiden Untervektorräume haben in diesem Fall also einen nichttrivialen Schnitt, es gibt also $f_1, f_2 \neq 0$, sodass $f_1\omega_1 = f_2\omega_2$. Daher sind ω_1 und ω_2 linear abhängig, die Dimension von Ω mithin ≤ 1. ◯

Bemerkung 3.3.7 Ein kgV
Für zwei Divisoren $D = \sum_P a_P P$ und $D' = \sum_P a'_P P$ auf C definieren wir das kleinste gemeinsame Vielfache durch

$$kgV(D, D') := \sum_P \max(a_P, a'_P) \cdot P.$$

Jedes $\omega \in \Omega(D) \cap \Omega(D')$ verschwindet sowohl auf $A(D)$ als auch auf $A(D')$, und damit auf $A(kgV(D, D'))$. Daher gilt

$$\Omega(D) \cap \Omega(D') \subseteq \Omega(kgV(D, D')).$$

Die umgekehrte Inklusion folgt wieder, da sowohl D als auch D' kleiner ist als das kgV.

Konstruktion 3.3.8 Ein Divisor
Es sei $\omega \in \Omega$ ein von 0 verschiedenes Pseudodifferential.
Wir konstruieren nun dazu einen Divisor auf dolgende Art: Wenn $\omega \in \Omega(D)$ gilt, dann ist $L(D) \to \Omega(0), \ f \mapsto f\omega$, eine injektive Abbildung, also $l(D) \leq \delta(g) = g$. Wegen $l(D) \geq \deg(D) + 1 - g$ folgt $\deg(D) \leq 2g - 1$.

Nun wählen wir einen Divisor K mit $\omega \in \Omega(K)$ von maximalem Grad. Dann ist K eindeutig bestimmt, denn ist K' ein weiterer solcher Divisor, so wäre ω auch in $\Omega(kgV(K, K'))$, und damit $K = K'$.
Wir sehen an der Konstruktion auch die Äquivalenz

$$\omega \in L(D) \Leftrightarrow D \leq K.$$

Wir schreiben $(\omega) := K$ für diesen Divisor.
Weiter gilt offensichtlich $(f\omega) = (f) + (\omega)$, sodass die zu zwei Differentialformen assoziierten Divisoren dasselbe Element in der Divisorklassengruppe $\mathrm{Pic}(C)$ vertreten. Diese Divisorenklasse heißt die *kanonische Klasse* oder auch die Klasse der *kanonischen Divisoren*.
Ist $K = (\omega)$ ein kanonischer Divisor, so ist

$$L(K - D) \to \Omega(D),\ f \mapsto f\omega$$

ein Isomorphismus, also ist

$$l(K - D) = \dim_k(\Omega(D) = \delta(D) = l(D) - \deg(D) + g - 1.$$

Es folgt der

Satz 3.3.9 Satz von Riemann-Roch
Für jeden Divisor D auf C und jeden kanonischen Divisor K auf C gilt

$$l(D) = l(K - D) + \deg(D) - g + 1.$$

Beispiel 3.3.10 Die kanonische Klasse
Setzt man im Satz von Riemann-Roch speziell $D = 0$, so folgt für einen kanonischen Divisor K aus $l(0) = 1$ die Gleichung

$$l(K) = g.$$

Setzt man dann $D = K$, so folgt auch noch

$$\deg(K) = 2g - 2.$$

Wenn also nun $\deg(D) > 2g-2$ gilt, dann ist $K-D$ ein Divisor negativen Grads und damit $l(K - D) = 0$. In diesem Fall gilt durchwegs

$$l(D) = \deg(D) + 1 - g.$$

Kapitel 4

Anwendungen des Satzes von Riemann-Roch

4.1 Elliptische Kurven

Definition 4.1.1 Elliptische Kurve
Es sei F ein Funktionskörper und C die zugehörige Kurve. Dann heißt C eine *elliptische Kurve,* wenn sie Geschlecht 1 und mindestens einen Punkt vom Grad 1 besitzt.
Wir nennen dann die Kurve zumeist E.
Dies ist der einfachste Fall nach dem in 3.2.11 behandelten der projektiven Geraden. Wir werden hier noch nebenher eine Gruppenstruktur entdecken, die für manche echte Anwendung bedeutsam ist.

Bemerkung 4.1.2 Am Schopf gepackt
Es sei E eine elliptische Kurve zum Funktionenkörper F über dem Konstantenkörper k. Weiter wählen wir einen Punkt $P \in E$ vom Grad 1, den es voraussetzungsgemäß gibt.
Nun betrachten wir $L(nP)$, wobei $n \in \mathbb{N}$. Es gilt wegen Riemann-Roch und 3.3.10 für alle $n \in \mathbb{N}$:

$$\deg(nP) = n > 0 = 2g - 2, \quad \text{also} \quad l(nP) = n.$$

Wegen $k \subseteq L(P)$ folgt also $k = l(P)$, aber es existiert ein nichtkonstantes $X \in L(2P)$. Der Poldivisor von X ist genau $2P$. Daher ist nach 3.2.5 der Körper F eine quadratische Erweiterung von $k(X)$.
Wegen $k + kX \subset L(3P)$ gibt es auch noch ein $Y \in L(3P)$, das keine Linearkombination von 1 und X ist. Y hat einen dreifach Pol bei P.
In $L(6P)$ liegen schließlich die 7 Funktionen

$$1, X, Y, X^2, XY, X^3, Y^2,$$

die nicht mehr linear unabhängig sein können. Demnach gibt es eine Relation

$$Y^2 + (a_1X + a_3)Y - (a_0X^3 + a_2X^2 + a_4X + a_6) = 0,$$

und es stellt sich heraus, dass F die quadratische Erweiterung von $k(X)$ ist, die zu dieser Gleichung gehört.
Man kann nun noch im Körper F herumspielen, insbesondere, wenn die Charakteristik von k nicht 2 ist. Dann lässt sich Y so wählen, dass der lineare Term verschwindet, und wir erhalten

$$Y^2 = a_0X^3 + a_2X^2 + a_4X + a_6.$$

Aus Gradgründen (für den Poldivisor) muss $a_0 \neq 0$ gelten. Ersetzen wir X durch $a_0^{-1}X$ und Y durch $a_0^{-2}Y$, so können wir auch a_0 loswerden.
Schließlich dürfen wir noch im Fall Charakteristik $\neq 3$ das X durch eine additive Konstante so abändern, dass auch a_2 verschwindet.
Wir kommen dann bei der *einfachen Weierstraß-Gleichung*

$$Y^2 = X^3 + a_4X + a_6$$

an. Manchmal sind hier in der Literatur auch andere Vorzeichenwahlen bzw. sogar weitere Vorfaktoren der Gestalt 2^e3^f zu finden, die daher rühren, dass man die allgemeine Situation mit der Theorie der elliptischen Funktionen in Einklang bringen will, wo diese Faktoren natürlicher Weise auftreten.
Gäbe es hier eine mehrfache Nullstelle des kubischen Polynoms auf der rechten Seite, so könnten wir es als $Y^2 = (X - a)^2(X - b)$ schreiben, was mit $\eta := Y/(X - a)$ auf $\eta^2 = X - b$ und damit auf $F = k(\eta)$ führt. Dies widerspräche der Voraussetzung, dass E Geschlecht 1 hat.
Demnach gibt es solch eine mehrfache Nullstelle nicht, jedenfalls nicht in k. Da wir mittlerweile jedoch vorausgesetzt haben, dass die Charakteristik weder 2 noch 3 ist, gibt es dann auch im algebraischen Abschluss keine mehrfache Nullstelle.
Das Beispiel 2.3.3 zeigt uns daher, dass die Gleichung

$$Y^2 = X^3 + a_4X + a_6$$

eine glatte Kurve in der projektiven Ebene definiert.
Dies versöhnt wieder unsere abstrakte neue Theorie mit der geometrischen Anschauung. Die Galoisbahnen von Punkten auf dieser Kurve (mit Koeffizienten in algebraischen Erweiterungskörpern von k) entsprechen den Äquivalenzklassen von Bewertungen von F, die auf k konstant sind. Der anfänglich gegebene Punkt vom Grad 1 ist hier der unendlich ferne Punkt $(0 : 1 : 0)$.
Es lohnt sich hier zu vermerken, dass $k[X, Y]$ (wobei nach wie vor die obige Relation gilt) ein Dedekindring ist, nämlich der ganze Abschluss von $k[X]$ in F, denn es ist eine (eigentlich die) maximale $k[X]$-Ordnung in F. Jede nichttriviale Bewertung auf F, die auf k trivial ist und die nicht vom Punkt $(0 : 1 : 0)$ herkommt,

ist eine Bewertung, deren Bewertungsring X und damit auch Y enthält. Sie geht einher mit der Restklassenabbildung

$$k[X,Y] \mapsto k_v \subset \overline{k},$$

die zwangsläufig gegeben ist durch die Wahl zweier Zahlen $x, y \in \overline{k}$, die als Bilder von X und Y die Relation

$$y^2 = x^3 + a_4 x + a_6$$

erfüllen, also Punkte auf der durch diese Gleichung beschriebenen ebenen Kurve sind. Da $k[X,Y]$ ganz abgeschlossen ist, ist der Restklassenkörper tatsächlich $k(x,y)$, und wir erhalten eine Bijektion zwischen den nichttrivialen normierten Bewertungen auf F, die auf k trivial sind und $k[X,Y]$ im Bewertungsring enthalten, und Äquivalenzklassen von Punkten in der Ebene, die Nullstellen des definierenden Polynoms sind.

Konstruktion 4.1.3 Eine Gruppenstruktur
Es sei E eine elliptische Kurve über dem Konstantenkörper k und $N \in E$ ein fest gewählter Punkt vom Grad 1.
Wir bezeichnen mit $E(k)$ die Menge aller Punkte vom Grad 1. Dann betrachten wir die folgende Abbildung

$$\delta : E(k) \to \mathrm{Pic}_0(E), \quad \delta(P) := [P - N].$$

a) Diese Abbildung ist injektiv.

b) Das Bild von δ ist eine Untergruppe von $\mathrm{Pic}_0(E)$.

Denn:
a) Wenn $[P-N] = [Q-N]$ gilt, wobei $P, Q \in E(k)$ sind, dann gibt es definitionsgemäß eine Funktion $f \in F^\times$ derart, dass

$$P - Q = (P - N) - (Q - N) = (f)$$

der zu f gehörige Hauptdivisor ist. Wäre nun $P \neq Q$, so hieße das, dass f einen einfachen Pol bei Q hat und sonst regulär ist, aber das wiederum hieße $\deg((f)_\infty) = 1$ und daher ist nach 3.2.5 $F = k(f)$ ein rationaler Funktionenkörper, was unsere Situation aber ausschließt.
b) Wir müssen nun zeigen, dass für alle $P, Q \in E(k)$ gilt, dass

$$[P - Q] = \delta(P) - \delta(Q) \in \delta(E(k)),$$

also

$$\exists R \in E(k) : [P - Q] = [R - N].$$

Im Fall $P = Q$ dürfen wir $R = N$ wählen, im Fall $Q = N$ dafür $R = P$.

In allen anderen Fällen studieren wir den Divisor $P-Q+N$, der Grad 1 hat und damit $l(P-Q+N)=1$ erfüllt.
Wir nehmen in $L(P-Q+N)$ eine Funktion $f \neq 0$ und betrachten deren Divisor. f hat eine Nullstelle bei Q und ist damit nicht konstant, aber dann kann der Poldivisor nicht Grad 1 haben, sonst wäre wieder $F = k(f)$, also ist der Poldivisor von F tatsächlich $P+N$, und damit hat der Nullstellendivisor auch Grad 2, es gibt also ein $R \in E(k)$ mit

$$(f) = P + N - Q - R.$$

Das wollten wir wissen.
Das Zurückziehen der Gruppenstruktur auf $\delta(E(k))$ nach $E(k)$ macht aus dieser Menge eine Gruppe. Es ist $P * Q$ derjenige Punkt, für den $P+Q-(P*Q)-N$ ein Hauptdivisor ist.
Das neutrale Element ist unser alter Punkt N. Es ist diese Gruppenstruktur, die elliptische Kurven für Anwendungen innerhalb (z.B. Zahlentheorie) und außerhalb (z.B. Kryptographie) der Mathematik interessant macht.
Konkret wird dies in unserem Modell $Y^2 = X^3 + a_4X + a_6$ realisiert, indem man zu zwei Punkten P, Q auf der Kurve die Verbindungsgerade als Nullstellenmenge einer linearen Funktion hinschreibt. Diese ist ein Polynom und liefert damit ein Element im Koordinatenring von E, dessen Nullstellendivisor meistens aus den beiden Punkten P, Q und dem dritten Schnittpunkt der Geraden und der Kurve besteht (wenn die Gerade nicht gerade tangential oder „senkrecht“ ist).
Dann ist $P*Q$ der Spiegelpunkt des dritten Schnittpunkts bezüglich der x-Achse.

Es folgt nun ein kurzer Abriss der komplex-analytischen Theorie der elliptischen Kurven und hoffentlich die Erkenntnis, dass hier Algebra und komplexe Analysis eng Hand in Hand gehen..

Definition/Bemerkung 4.1.4 Elliptische Funktionen
Es sei $\Lambda \subseteq \mathbb{C}$ ein (volles) Gitter, also eine diskrete und kokompakte Untergruppe, oder auch eine Untergruppe, die von zwei Elementen erzeugt wird, welche reell linear unabhängig sind.
Eine Λ-*elliptische Funktion* ist eine $\Lambda-$periodische meromorphe Funktion auf $\mathbb{C}$, also eine Funktion

$$f \in \mathcal{M}(\mathbb{C}): \quad \forall \lambda \in \Lambda,\ \forall z \in \mathbb{C} : f(z+\lambda) = f(z).$$

Hierbei ist auch der Funktionswert ∞ zugelassen, der bei Polen angenommen wird.
Die Menge F aller Λ-elliptischen Funktionen ist ein Körper, der $\mathbb{C}$ umfasst und $\mathbb{C}$ ist die Menge aller holomorphen Elemente in F, denn eine holomorphe Funktion in F ist ganz und beschränkt, da sie auf jedem Kompaktum beschränkt ist, und alle Funktionswerte auf einem kompakten Fundamentalbereich für die Aktion

von Λ auf $\mathbb{C}$ angenommen werden. Das ist Liouvilles erster Satz über elliptische Funktionen.
Mit f ist auch die Ableitung elliptisch. Außerdem können wir eine Funktion $f \in F$ auch als Funktion auf $\mathbb{C}/\Lambda$ auffassen.

Hilfssatz 4.1.5 Liouvilles zweiter Satz
Es sei $\Lambda \leq \mathbb{C}$ ein volles Gitter und $f \neq 0$ eine Λ-elliptische Funktion.
Dann gilt

$$\sum_{z \in \mathbb{C}/\Lambda} \operatorname{Res}(f, z) = 0.$$

Beweis. Wir wählen zwei Erzeuger $u, v \in \Lambda$ und ein $a \in \mathbb{C}$, sodass f auf dem Rand von

$$\mathcal{F} := \{a + xu + yv \mid 0 \leq x, y \leq 1\}$$

keinen Pol hat. Nach dem Residuensatz ist dann

$$\sum_{z \in \mathbb{C}/\Lambda} \operatorname{Res}(f, z) = \frac{1}{2\pi \mathrm{i}} \int_{\partial \mathcal{F}} f(z) \mathrm{d}z,$$

und dieses Integral wird 0, da sich aufgrund der Periodizität die Wegintegrale auf gegenüberliegenden Seiten des durchlaufenen Parallelogramms gegenseitig wegheben.
Dass es so ein a gibt liegt daran, dass weit und breit nur endlich viele Pole von f existieren. ◯

Folgerung 4.1.6 Nicht ganz einfach
Es kann nicht sein, dass f genau einen Pol modulo Λ hat und dieser einfach ist. Denn sonst wäre die Summe der Residuen gerade das Residuum an dieser einen Polstelle.

Hilfssatz 4.1.7 Liouvilles dritter Satz
Es sei $\Lambda \leq \mathbb{C}$ ein volles Gitter und $f \neq 0$ eine Λ-elliptische Funktion.
Dann ist die Summe aller Ordnungen von f ebenfalls 0.

Beweis. Auch f/f' ist eine elliptische Funktion, und Liouvilles zweiter Satz zusammen mit dem Argumentprinzip liefert was wir brauchen. ◯

Folgerung 4.1.8 Surjektiv
Ist f elliptisch und nicht konstant, so wird jede komplexe Zahl b von f genauso oft als Wert angenommen wie die 0 (und wie ∞).
Denn auch $f - b$ ist elliptisch und hat dieselben Polordnungen wie f.

Konstruktion 4.1.9 Die Weierstras-$\wp$-Funktion
Sei weiterhin Λ ein volles Gitter in $\mathbb{C}$. Wir wollen nun eine nichtkonstante elliptische Funktion konstruieren. Unser Ziel ist, dass diese Funktion modulo Λ nur eine Polstelle hat. Diese muss dann mindestens doppelt sein, und das Residuum an dieser Stelle ist 0. Wir versuchen unser Glück mit einem doppelten Pol. Dann ist der Hauptteil von f bei einer Polstelle p gerade $c \cdot \frac{1}{(z-p)^2}$ für eine konstante c. Wir wollen den Pol bei den Gitterpunkten.
Idee: Fange an mit $1/z^2$ und mache das per Zwang Λ-invariant.
Der naive Ansatz ist

$$f(z) := \sum_{\lambda \in \Lambda} \frac{1}{(z-\lambda)^2},$$

allerdings scheitert dieser, da diese Reihe nicht konvergiert. Der nächste Versuch

$$\wp(z) := \sum_{0 \neq \lambda \in \Lambda} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}\right) + \frac{1}{z^2},$$

erzwingt zwar die (lokal gleichmäßige) Konvergenz, aber nun ist die Periodizität nicht mehr offensichtlich.
Immerhin ist sie gerade, d.h. $\wp(-z) = \wp(z)$, und an diesem Strohhalm werden wir uns aus dem Sumpf ziehen:

Hilfssatz 4.1.10 Glück gehabt
Die so definierte Funktion $\wp$ ist Λ-elliptisch.

Beweis. Wir betrachten zunächst die Ableitung

$$\wp'(z) = -2 \sum_{\lambda} \frac{1}{(z-\lambda)^3},$$

in der die Null keine Sonderrolle mehr spielt. Diese ist offensichtlich elliptisch. Sie ist aber auch ungerade, und daher ist für jeden Gitterpunkt λ

$$\wp'(\lambda/2) = -\wp'(\lambda/2),$$

also ist das 0, wenn nicht $\lambda/2$ selbst im Gitter liegt (wo man dann einen Pol hat). Für jedes $\lambda \in \Lambda$ gibt es nun eine konstante c_λ mit

$$\wp(z+\lambda) = c_\lambda + \wp(z),$$

denn die Funktionen links und rechts haben dieselbe Ableitung. Offensichtlich ist c ein Homomorphismus von λ nach $\mathbb{C}$. Wenn nun λ ein primitiver Gittervektor ist, dann folgt für $z = -\lambda/2$

$$\wp(-\lambda/2) = \wp(\lambda/2) = \wp(-\lambda/2 + \lambda) = c_\lambda + \wp(-\lambda/2),$$

also $c_\lambda = 0$. Daher ist c_λ für alle λ, denn wir wissen das für Erzeuger von Λ. ◯

Hilfssatz 4.1.11 Ein Funktionenkörper
Es sei $\Lambda \leq \mathbb{C}$ ein volles Gitter und $f \in F$ eine Λ-elliptische Funktion.
Wenn f gerade ist, dann ist f eine rationale Funktion in $\wp$.
Es gilt $F = \mathbb{C}(\wp, \wp')$, und dies ist eine quadratische Erweiterung von $\mathbb{C}(\wp)$.

Beweisskizze. Es sei f gegeben. Durch Multiplikation mit Funktionen der Gestalt $\wp(z-a)$ kann man – da f gerade ist und mithin auch der Poldivisor symmetrisch ist – dafür sorgen, dass f nur in Gitterpunkten Polstellen hat. Die Polordnung hier ist gerade, da f gerade ist, und jetzt können wir ein geeignetes Polynom in $\wp$ abziehen, sodass die Differenz keinen Pol mehr bei 0 hat. Also ist sie holomorph, und wir sind fertig.
Die Abbildung $F \ni f(z) \mapsto f(-z) \in F$ ist ein Automorphismus der Ordnung 2. Der Fixkörper besteht aus allen geraden elliptischen Funktionen, ist also $\mathbb{C}(\wp)$, und F ist eine quadratische Erweiterung davon (Satz von Artin). Da $\wp'$ ungerade ist, wird diese quadratische Erweiterung von $\wp'$ erzeugt. ◯

Bemerkung 4.1.12 Das Weierstraß-Polynom
In der gerade behandelten Situation gilt noch mehr: $\wp'^2$ ist in $\mathbb{C}(\wp)$.
Da $(\wp')^2$ eine gerade Funktion ist, die nur in Gitterpunkten Pole hat ist nach dem Beweis $\wp'^2$ ein Polynom in $\wp$. Die Polordnung ist 6 und nun muss man sich genau die beteiligten Hauptteil hinschreiben, um einzusehen, dass

$$\wp'^2 = 4\wp^3 - 60G_4\wp - 140G_6,$$

wobei wir für $k \geq 3$

$$G_k := \sum_{\lambda \neq 0} \lambda^{-k}$$

setzen. Diese *Eisensteinreihen* spielen eine wichtige Rolle in der Theorie der Modulformen. Da $\wp'$ drei verschiedene einfache Nullstellen hat, folgt

$$\wp'^2 = 4(\wp - \wp(\lambda_1/2))(\wp - \wp(\lambda_2/2))(\wp - \wp((\lambda_1 * \lambda_2)/2)),$$

wobei $\lambda_{1/2}$ gewählte Basisvektoren von Λ sind.
Die Werte der $\wp$-Funktion sind hier paarweise verschieden, und daher hat das kubische Polynom keine doppelte Nullstelle. Wir finden auf diese Art genau die Situation aus 4.1.2 wieder.
Die Theorie der Modulformen lehrt, dass es für jedes zulässige kubische Polynom rechter Hand ein geeignetes Gitter gibt.
Für

$$E := \{(x : y : z) \in \mathbb{P}^2(\mathbb{C}) \mid y^2z = 4x^3 - 60G_4xz^2 - 140G_6z^3\}$$

ist die Abbildung

$$\mathbb{C}/\Lambda \ni [z] \mapsto \begin{cases} (\wp(z) : \wp'(z) : 1), & z \notin \Lambda, \\ (0 : 1 : 0) & , \ z \in \Lambda, \end{cases}$$

eine Bijektion, wenn wir die Klasse der Gitterpunkte nach $(0:1:0)$ schicken. Damit wird $\mathbb{C}/\Lambda$ zu einer algebraischen Kurve vom Geschlecht 1, was auch dem topologische Geschlecht entspricht. Wir sehen aber auch eine Gruppenstruktur. Diese passt mit der algebraisch konstruierten zusammen, das ist der Inhalt der Additionstheoreme für die $\wp$-Funktion.
Insbesondere kennt man hier die Gruppenstruktur sehr gut, das ist einfach $(\mathbb{R}/\mathbb{Z})^2$, und man sieht, dass die Torsionsgruppe $(\mathbb{Q}/\mathbb{Z})^2$ ist.

Bemerkung 4.1.13 Nachlese
Zu einem beliebigen Körper k zurückkehrend kann man sich erneut fragen, wie die Gruppenstruktur von $E(k)$ für eine elliptische Kurve E über k mit Funktionenkörper F aussieht. Hier hat man einige Informationen parat. Insbesondere ist für eine natürliche Zahl n, die kein Vielfaches der Charakteristik von k ist, die Untergruppe $E[n](k) := \{P \in E(k) \mid n \cdot P = 0\}$ isomorph zu einer Untergruppe von $[(\frac{1}{n}\mathbb{Z})/\mathbb{Z}]^2$. Wenn k perfekt ist und $\overline{k}$ ein algebraischer Abschluss von k, dann ist $\overline{k} \otimes_k F$ ein elliptischer Funktionenkörper über $\overline{k}$, und die Galoisgruppe $G = \mathrm{Aut}(\overline{k} \mid k)$ operiert auf $E(\overline{k})$ in natürlicher Weise und sogar als Automorphismen der Gruppenstruktur. Das liefert für jedes n einen Homomorphismus

$$\rho_n : G \to \mathrm{Aut}(E[n](\overline{k}) \cong \mathrm{GL}_2(\mathbb{Z}/\mathbb{Z}),$$

wobei die letzte Identifikation wieder nur stimmt wenn die Charakteristik von k kein Teiler von n ist. Diese Darstellungen liefern Information über G, und so etwas systematisch auszuschlachten ist eines der Hauptgeschäfte der arithmetischen Geometrie.
Interessant ist natürlich vor allem der Zahlkörperfall, speziell $k = \mathbb{Q}$. Hier sagt der Satz von Mordell[1] und Weil[2], dass $E(\mathbb{Q})$ endlich ist, also in eine frei-abelsche Gruppe von endlichem Rang und einen endlichen Torsionsanteil zerfällt. Ein Satz von Mazur[3] sagt genau, welche Gruppen hier als Torsionsgruppen auftauchen können (endlich viele Typen).
Es ist nicht bekannt, ob $E(\mathbb{Q})$ beliebig groß werden kann. Der Rekord steht derzeit bei 24. Der Rang ist schwer zu bestimmen, es gibt aber die Vermutung von Birch[4] und Swinnerton-Dyer[5], die grob gesagt zunächst darin besteht, dass sich der Rang als Nullstellenordnung der L-Reihe von E bei $s = 1$ bestimmen lässt, wobei ich jetzt nicht verrate, wie diese L-Reihe gebildet wird.
Diese Vermutung entstand in den 1960er Jahren aufgrund zahlreicher numerischer Berechnungen, wobei zunächst nicht klar war, ob die L-Reihe berhaupt dort sinnvoll definiert ist, wo man das Residuum betrachtet. Dies wurde erst 1994 durch

[1] Louis Mordell, 1888 - 1972
[2] André Weil, 1906 - 1998
[3] Barry Mazur, 1937 -
[4] Bryan Birch, 1931 -
[5] Sir Peter, 1927 -

Wiles Beweis der Modularitätsvermutung sichergestellt, was jedoch den Beweis der Vermutung von Birch und Swinnerton-Dyer nicht näherrückte.

4.2 Kurven über endlichen Körpern

In diesem ganzen Abschnitt sei k der endliche Körper mit q Elementen und C eine (glatte, projektive) Kurve über k, also die Kurve zu einem Funktionenkörper, der k als Konstantenkörper hat.

Definition 4.2.1 Ein Zählproblem
Es seien k ein endlicher Körper, F ein Funktionenkörper über k und C die zugehörige Kurve.
Wie vorhin sei $C(k)$ die Menge aller Punkte auf C, deren Restklassenkörper k ist.
Dies ist eine endliche Menge. Allgemeiner ist für jedes $d \in \mathbb{N}$ die Menge aller Punkte von Grad $\leq d$ endlich, denn wenn $f \in F \setminus k$ eine nicht konstante Funktion ist, dann ist jede Bewertung w auf F die Fortsetzung einer Bewertung v auf $k(f)$, aber die Anzahl der Bewertungen von $k(f)$ mit gegebenem Bewertungskörper ist endlich, und da letztlich wegen 3.1.5 jede Bewertung von $k(f)$ nur endlich viele Fortsetzungen nach F hat, gibt es auch dort nur endlich viele Punkte mit Grad $\leq d$ für jedes $d \in \mathbb{N}$.
Es ist eine alte Aufgabe, die Anzahl der Elemente von $C(k)$ zu bestimmen. Dieser Aufgabe wenden wir uns jetzt zu.

Hilfssatz 4.2.2 Noch mehr Endlichkeit
Es seien k ein endlicher Körper, F ein Funktionenkörper über k und C die zugehörige Kurve. Dann ist $\mathrm{Pic}_0(C)$ *endlich und gleich*

$$\#\{\mathcal{D} \in \mathrm{Pic}(C) \mid \deg(\mathcal{D}) = d\}$$

für jede ganze Zahl d, die als Grad eines Divisors vorkommt.

Beweis. Da der Grad auf jeder Divisorklasse konstant ist, können wir ihn als Homomorphismus von $\mathrm{Pic}(C)$ nach $\mathbb{Z}$ auffassen. $\mathrm{Pic}_0(C)$ ist der Kern hiervon, und das zeigt die zweite Behauptung.
Nun weisen wir nach, dass für $d > g = g(C)$ nur endlich viele Divisorenklassen vom Grad d existieren können.
Sei D eine davon. Dann ist $l(D) \geq \deg(D) + 1 - g > 0$, also gibt es ein $f \in L(D), f \neq 0$. Es folgt $(f) + D \geq 0$, wir können also jede Divisorenklasse durch einen nicht-negativen Divisor repräsentieren. Da es aber nur endlich viele Punkte gibt, deren Grad nicht größer ist als d, gibt es auch nur endlich viele positive Divisoren vom Grad $\leq d$. ◯

Definition 4.2.3 Eine Klassenzahl
Es sei F ein Funktionenkörper mit endlichem Konstantenkörper k.
a) Die Zahl $h(C) := \#\mathrm{Pic}_0(C)$ heißt die *Klassenzahl* von F.
b) Wir setzen

$$Z_F(t) := \sum_{\mathrm{Div}(C) \ni D \geq 0} t^{\deg D} = \prod_{P \in C} \frac{1}{1 - t^{\deg P}}.$$

Die zweite Identität gilt zunächst formal, wir werden in Kürze sehen, dass Z_F positiven Konvergenzradius hat, und dann stimmt die zweite Identität auch innerhalb diese Konvergenzradius, da das Produkt hier absolut konvergiert.
Weiter sei $n_d := \#\{D \in \mathrm{Div}(C) \mid D \geq 0, \deg(D) = d\}$.
Dann ist

$$Z_F(t) = \sum_{d=0}^{\infty} n_d t^d.$$

c) Für einen Divisor D setzen wir $N(D) := q^{\deg(D)}$, wobei $q = \#k$.
Ist speziell $D = P \in C$ ein Punkt, so ist $N(P)$ die Kardinalität des Restklassenkörpers bei P.
d) Wir substituieren in Z_F anstelle von t die Zahl q^{-s} und erhalten eine Dirichletreihe:

$$\zeta_F(s) := \sum_{D \geq 0} N(D)^{-s} = \prod_{P \in C} \frac{1}{1 - N(P)^{-s}}.$$

Sie heißt die *Hasse*[6]*-Weil Zetafunktion* von C. Die Produktentwicklung stimmt wieder zunächst nur formal, wir kümmern uns gleich noch um Konvergenz.

Beispiel 4.2.4 Die projektive Gerade
Es sei $F = k(X)$. Die positiven Divisoren, deren Träger nicht ∞ enthält, entsprechen bijektiv (via Nullstellendivisor) den Idealen in $k[X]$, also den normierten Polynomen. Es gibt genau q^d Polynome vom Grad d, und damit ist

$$\zeta_F(s) = \sum_d q^d \cdot q^{-sd} \cdot \frac{1}{1 - q^{-s}},$$

wobei der letzte Faktor die positiven Divisoren mit Träger in $\{\infty\}$ zählt. Also ist

$$\zeta_F(s) = \frac{1}{(1 - qq^{-s})(1 - q^{-s})}$$

und diese Funktion hat Polstellen bei $1 + 2\pi\mathrm{i}\mathbb{Z}$ und $0 + 2\pi\mathrm{i}\mathbb{Z}$, alle Nullstellen haben Realteil $\frac{1}{2}$. (Da gibt es allerdings keine.)

[6]Helmut Hasse, 1898 - 1979

Satz 4.2.5 Die Kardinalfrage
Es seien $k = \mathbb{F}_q$, F ein Funktionenkörper über k und C die zugehörige Kurve. Dann ist $Z_F(t)$ eine rationale Funktion und es gilt

$$Z_F(1/(qt)) = (qt^2)^{1-g} Z_F(t).$$

Beweis. Es sei D ein Divisor. Dann ist die Anzahl der positiven, zu D äquivalenten Divisoren gleich

$$\frac{q^{l(D)} - 1}{q - 1},$$

denn solch ein Divisor ist von der Gestalt $(f) + D \geq 0$, also $f \in L(D), f \neq 0$, und je $q - 1$ solche Funktionen liefern denselben Divisor.
Für $d > 2g - 2$ ist wegen Riemann-Roch $l(D) = \deg(D) + 1 - g$, und das heißt, dass für dieses d genau

$$h(C) \cdot \frac{q^{\deg(D)+1-g} - 1}{q - 1}$$

positive Divisoren vom Grad d existieren, wenn mindestens einer existiert.
Wir sammeln jetzt Divisorenklassen $\mathcal{D}$ mit gleichem Grad zusammen und benutzen für jede davon die Notation $l(\mathcal{D}) := l(D)$, wobei D ein Vertreter der Klasse ist.
Die Summe für $Z_F(t)$ teilen wir nun in zwei Summanden auf, einmal die Klassen vom Grad $\leq 2g - 2$ und dann die Klassen von größerem Grad, fr die Riemann-Roch besonders bequem ist. Es folgt für den Erzeuger $a \in \mathbb{N}$ von $\deg(\mathrm{Div}(C))$:

$$\begin{aligned} \tfrac{q-1}{h(C)} Z_F(t) &= \textstyle\sum_{0 \leq \deg(\mathcal{D}) \leq 2g-2} q^{l(\mathcal{D}))} t^{\deg(D)} + \sum_{ad > 2g-2} q^{ad+1-g} t^{ad} - \sum_{d=0}^{\infty} t^{ad} \\ &= \textstyle\sum_{0 \leq \deg(\mathcal{D}) \leq 2g-2} q^{l(\mathcal{D}))} t^{\deg(D)} + q^{1-g} (qt)^{2g-2+a} \frac{1}{1-(qt)^a} - \frac{1}{1-t^a}. \end{aligned}$$

Dies gilt im Falle der Konvergenz der beteiligten geometrischen Reihen, also für $|qt| < 1$. Außerdem ist die Rationalität von Z_F damit sichergestellt.
Um nun die Funktionalgleichung einzusehen benutzen wir die hergestellte Zerlegung von Z_F und rechnen nach, dass beide Summanden (das Polynom und die Summe der beiden nicht ganzen Teile) jeder für sich die behauptete Gleichung erfüllen.
Das ist im zweiten Fall einfach, und nur für die endliche Summe wird ein Argument benutzt. Es sei nämlich $\mathcal{K}$ die Klasse der kanonischen Divisoren auf C. Dann gilt nach Riemann Roch

$$l(\mathcal{D}) = l(\mathcal{K} - \mathcal{D}) + 1 - g.$$

Da der Grad von $\mathcal{K}$ gerade $2g - 2$ ist, wird durch $\mathcal{D} \mapsto \mathcal{K} - \mathcal{D}$ eine Permutation der Divisorenklassen mit Grad zwischen 0 und $2g - 2$ vorgenommen, und unter Verwendung von Riemann-Roch folgt die behauptete Gleichung. ◯

Hilfssatz 4.2.6 Eine Erweiterung
Es seien k und F wie gehabt und $k_n = \mathbb{F}_{q^n}$ für eine natürliche Zahl n. Weiter sei $F_n = k_n F$ (Kompositum im algebraischen Abschluss von F). Dann ist F_n ein Funktionenkörper über k_n, und es gilt

$$Z_{F_n}(t^n) = \prod_{\zeta^n=1} Z_F(\zeta t).$$

Beweis. Es seien C bzw. C_n die zu F bzw. F_n gehörenden Kurven und $P \in C$ ein Punkt mit Grad d. Weiter sei $\mathcal{O}_P$ der Bewertungsring von P und $\mathbf{m}_P$ sein maximales Ideal. Es ist $k_P = \mathcal{O}_P/\mathbf{m}_P = \mathbb{F}_{q^d} = k_d$. Die zu P gehörige Bewertung bezeichnen wir mit v. Es sei π ein Erzeuger von $\mathbf{m}_P$.
Die Körpererweiterung $F \subseteq F_n$ ist auch eine Galoiserweiterung vom Grad d, und wir können auch F_n mit $k_n \otimes_k F$ identifizeren.
Der Ring $R := k_n\mathcal{O}_P$ ist ein Teilring von F_n, der F_n als Quotientenkörper hat. Er ist in den Bewertungsringen aller Fortsetzungen von v nach F_n enthalten, und wir können diese Fortsetzungen einfach an den maximalen Idealen von R ablesen. Die Restklassenkörpr finden wir via

$$k_n \otimes_k k_d = k_\kappa \times \ldots \times k_\kappa,$$

wobei $\kappa = \mathrm{kgV}(d, n)$ gilt. Die Anzahl der Faktoren ist $\gamma = \mathrm{ggT}(n, d)$. Die Grade der entsprechenden Punkte auf C_n sind alle κ/n, denn als Konstantenkörper dient ja jetzt k_n.
Mit dieser Information lässt sich nachrechnen, dass alle Fortsetzungen von v nach F_n in der Funktion $Z_{F_n}(t)$ zusammen einen Faktor

$$\frac{1}{(1-t^{\kappa/n})^\gamma}$$

liefern. Substituiert man hier t^n als t, so wird daraus

$$\frac{1}{(1-t^\kappa)^\gamma} = \prod_{\zeta^n=1} \frac{1}{1-(\zeta t)^d},$$

wobei man die letzte Identität durch Vergleich der Nullstellen der Nenner samt Vielfachheiten überprüfen kann.
Wenn man diese Identität für alle Punkte P von C und die Produktzerlegung von Z_F benutzt, so folgt die behauptete Gleichheit. ◯

Folgerung 4.2.7 $a = 1$
Im Beweis von 4.2.5 ist $a = 1$, es gibt also Divisoren vom Grad 1, und man hat

$$Z_F(t) = \frac{L(t)}{(1-t)(1-qt)},\ L(t) \in \mathbb{C}[t], \deg(L) = 2g.$$

Beweis.
Im Beweis des zitierten Satzes haben wir

$$Z_F(t) = \frac{L(t)}{(1-t^a)(1-(qt)^a)}$$

gesehen, wobei der Grad von L hier noch $2g-2+2a$ ist. Nun wählen wir im letzten Hilfssatz k_n so, dass auf C_n ein Punkt vom Grad 1 liegt. Dann ist

$$Z_{F_n}(t) = \frac{\tilde{L}(t)}{(1-t)(1-q^n t)}.$$

Wenn man nun $Z_{F_n}(t^n)$ mit $\prod_{\zeta^n=1} Z_F(\zeta t)$ vergleicht, so stellt man fest, dass die Polstellenordnungen nur dann zusammenpassen, wenn $a = 1$. ◯

Folgerung 4.2.8 *Die Funktion $Z_F(t)$ hat die Gestalt*

$$Z_F(t) = \frac{P(t)}{(1-qt)(1-t)},$$

wobei $P(t)$ ein Polynom vom Grad $2g$ mit konstantem Term 1 ist.
Es ist

$$P(\frac{1}{qt}) = (qt^2)^{2g} P(t),$$

und P lässt sich als

$$P(t) = \prod_{i=1}^{2g} (1 - a_i t)$$

faktorisieren, wobei $a_i \cdot a_{g+1} = q$.
Weiter ist $\#C(k) = q + 1 - \sum_{i=1}^{2g} a_i$.
In der Situation von 4.2.6 hat C das gleiche Geschlecht wie C_n.

Der Formel aus 4.2.6 entnimmt man, dass daher auch $\#C_n(k_n) = q^n + 1 - \sum_{i=1}^{2g} a_i^n$ gilt. Die von Hasse und Weil bewiesene Riemannsche Vermutung für C besagt hier, dass alle a_i in Wirklichkeit Betrag $\sqrt{q}$ haben, und daher

$$|\#C_n(k_n) - q^n - 1| \leq 2g\sqrt{q}$$

gilt. Diese Abschätzung (Hasse-Schranke) ist sogar äquivalent zur Riemannschen Vermutung, von der es auch einen neueren Beweis gibt, der mit relativ elementaren Mitteln auskommt. Eine geTEXte Version dieser Arbeit von Bombieri findet sich hier:
http://berndt-schwerdtfeger.de/v4/bbk430.pdf

Index