Prof. Dr. U. Görtz **WS 2018/19**
F. Gora

Seminar über die Weil-Vermutungen für Kurven

Die Weil-Vermutungen sind berühmte Vermutungen, die 1949 von André Weil aufgestellt wurden und die Entwicklung der algebraischen Geometrie in den folgenden Jahrzehnten maßgeblich bestimmt haben, bis sie in den 1970er Jahren von Pierre Deligne bewiesen wurden. Der Beweis benutzt ganz entscheidend die von Grothendieck und seiner Schule entwickelte Sprache der Schemata und der étalen Kohomologie.

Die Vermutungen (nun eigentlich der Satz von Deligne, aber die alte Bezeichnung ist nach wie vor üblich) beschreiben in eleganter Weise eine verblüffende Regelmäßigkeit über die Anzahl von Lösungen eines polynomialen Gleichungssystems über endlichen Körpern $\mathbb{F}_q$, wobei q die Potenzen einer Primzahl p durchläuft. Einen Teil der Faszination macht die Tatsache aus, dass in der Beschreibung sogenannte Zeta-Funktionen auftreten, die analog zur Riemannschen Zeta-Funktion gebildet werden; der schwierigste Teil der Weil-Vermutungen besagt, dass für diese Funktionen das Analogon der Riemannschen Vermutung richtig ist.

Für algebraische Kurven liegt die Sache wesentlich einfacher als im allgemeinen Fall. In dieser Situation wurde die Vermutung bereits 1924 von Emil Artin aufgestellt und von Weil bewiesen. Diesen Satz und seinen Beweis nach Bombieri zu verstehen, ist das Thema des Seminars.

Das Seminar bietet Ihnen damit die Möglichkeit, Grundbegriffe der algebraischen Geometrie kennenzulernen, ohne zuerst einen großen technischen Apparat aufbauen zu müssen. Einige Ergebnisse (insbesondere den Satz von Riemann-Roch) werden wir als *black box* ohne Beweis benutzen — aus Zeitgründen und weil sich diese Ergebnisse in einfacher Weise aus der allgmeineren Theorie ergeben, wie sie üblicherweise in den Vorlesungen Algebraische Geometrie 1+2 entwickelt wird.

ECTS-Punkte: Das Seminar ist ein Bachelor-Seminar im Bachelorstudiengang Mathematik (oder Techno-/Wirtschaftsmathematik), das 6 ECTS-Punkte erbringt. Die Vorträge 9 – 13 können bei Bedarf so ausgebaut werden, dass sie als Master-Seminar-Vorträge angerechnet werden können.

Erforderliche Vorkenntnisse: Gute Kenntnisse in Linearer Algebra 1 und 2, Analysis 1 und in Algebra (Ringe, Ideale, Körpererweiterungen, endliche Körper, Galoistheorie). Nützlich sind Kenntnisse in Kommutativer Algebra. Der parallele Besuch der Vorlesung *Algebraische Geometrie* wird empfohlen.

Anforderungen an einen erfolgreichen Seminarvortrag.

- Ihr erstes und wichtigstes Ziel sollte sein, die im Vortrag zu behandelnde Mathematik gründlich zu verstehen. Das wird in der Regel eine ganz Menge Zeit in Anspruch nehmen; beginnen Sie daher frühzeitig mit Vorbereitung! Stellen Sie viele Fragen (sich und den anderen Seminarteilnehmern). Seien Sie diszipliniert darin, sich zu fragen, warum (ob) die im zugrundeliegenden Text aufgestellten Behauptungen richtig sind. Was lässt sich vereinfachen? Wenn Sie auf Dinge stoßen, die Sie nicht verstehen, fragen Sie die anderen

Seminarteilnehmer (diejenigen, die die Vorträge direkt vor oder nach Ihnen halten, haben sich vielleicht schon genau dieselbe Frage gestellt). Wenn Sie damit noch nicht weiterkommen, vereinbaren Sie einen Termin mit dem Assistenten, der das Seminar betreut.

- Wenn Sie die Mathematik verstanden haben, sollten Sie bewusst darüber nachdenken, wie Sie die Inhalte in Ihrem Vortrag darstellen möchten. Oft bietet es sich an, den Aufbau zu ändern, Sachen umzustrukturieren, zusätzliche Beispiele einzubauen, die Notation anzupassen, usw. — schließlich ist ein Vortrag etwas ganz anderes als ein geschriebener Text. Überlegen Sie im Vorfeld, was die Hauptpunkte Ihres Vortrags sind, die jeder Teilnehmer lernen sollte, und berücksichtigen Sie das entsprechend. Sie können nötigenfalls Sachen im Vortrag auslassen (zum Beispiel eine technische Rechnung, die zum Verständnis nicht notwendig ist (schauen Sie sie sich trotzdem genau an, um gegebenenfalls Fragen beantworten zu können!)). Denken Sie bei der Vortragsplanung darüber nach, was sich zum Weglassen eignet, damit Sie nicht am Ende wegen Zeitmangels gezwungen sind, die interessantesten Teile zu überspringen. Die Sachen, die Sie in der Vorbereitung besonders viel Zeit gekostet haben, sollten Sie nicht auslassen, denn die anderen Teilnehmer haben vermutlich ähnliche Schwierigkeiten beim Verständnis und können gerade an diesen Stellen viel lernen.

Anmerkungen zur Literatur.

Wir richten uns großenteils nach dem Skript [Ha] von Hansen, das die wesentlichen Punkte gut und prägnant präsentiert (allerdings leider eine ganze Menge kleinerer Fehler enthält, man muss also beim Lesen gut aufpassen!). Mehr Details finden sich in dem Buch [Lo] von Lorenzini, das auch empfehlenswert ist, allerdings auch viel anderen Stoff enthält, den wir nicht benötigen, und das es auch von der Art der Darstellung nicht ganz leicht macht zu finden, was man sucht.

Im Buch [St] (das wir für einige algebraische Grundlagen benutzen) wird auch die Theorie der Zetafunktion dargestellt (und vieles mehr, zum Beispiel die Verbindung zur Kodierungstheorie), allerdings abgesehen von einem kurzen Anhang nicht vom Standpunkt der algebraischen Geometrie, sondern aus der algebraischen Sichtweise der algebraischen Funktionenkörper. Für den Kurvenfall ist das zwar ausreichend (und teilweise einfacher), aber die geometrische Perspektive, die wir einnehmen wollen, ermöglicht uns erste Einblicke in die allgemeine Theorie der Varietäten und Schemata, die das größere Potential für Verallgemeinerungen hat.

Zum Teil sind die Quellen auf der Webseite verlinkt. Wenn Sie Schwierigkeiten haben, die anderen Quellen zu finden, melden Sie sich bitte bei mir.

Notation/Allgemeine Annahmen: Wir arbeiten stets über einem perfekten Körper k (d.h. alle endlichen Erweiterungen k'/k sind separabel; dies ist zum Beispiel der Fall, wenn k Charakteristik 0 hat, oder wenn k ein endlicher Körper ist). Mit $\overline{k}$ bezeichnen wir einen algebraischen Abschluss von $\overline{k}$. In den Vorträgen 8 und 11–13 ist k dann ein endlicher Körper.

0. Einführung

Übersicht über das Seminar.

1. Diskrete Bewertungsringe 1

[St] 1.1.1 – 1.1.13

Wir beginnen mit einigen Grundlagen über Funktionenkörper und (vor allem) den Begriff des diskreten Bewertungsrings. Um spätere Notationskonflikte zu vermeiden, bezeichnen Sie den Grundkörper, den Stichtenoth K nennt, bitte mit k.

2. Diskrete Bewertungsringe 2

[St] 1.1.14 – 1.1.20; 1.2

In diesem Vortrag werden die "algebraischen Vorbereitungen" beendet, bevor wir auf den geometrischen Standpunkt wechseln. Außerdem soll das Beispiel des Körpers der rationalen Funktionen über k beleuchtet werden.

3. Affine Varietäten

[Ha] 1.1.

Definieren Sie wie in [Ha] den affinen Raum $\mathbb{A}^n(\overline{k})$ und die Galois-Operation, und die Nullstellenmenge eines Ideals (ersetzen Sie die Notation V_I durch das gebräuchlichere $V(I)$). Die Bemerkung über die Topologie können Sie auslassen.

Definieren Sie den affinen Koordinatenring und den (rationalen) Funktionenkörper einer affinen Varietät V.

Definieren Sie den lokalen Ring in einem Punkt $x = (x_1, \ldots, x_n) \in V \subseteq \mathbb{A}^n(\overline{k})$ wie folgt: Es ist $(X_1 - x_1, \ldots, X_n - x_n)$ ein maximales Ideal in $\overline{k}[X_1, \ldots, X_n]$, das das Ideal $I(V)$ enthält; es entspricht daher einem maximalen Ideal $\mathfrak{m}_x$ in $\overline{k}[V]$. Der lokale Ring von x ist dann der Ring

$$\mathcal{O}_{V_{\overline{k}},x} := \left\{ \frac{f}{g};\ f, g \in k[V],\ g \notin \mathfrak{m}_x \right\}.$$

(Ist V über k definiert und $x \in V(k)$, so hat man analog $k[V] \subset \mathcal{O}_{V,x} \subset k(V)$.)

(Die Ringe $\overline{k}(V)$ und $\mathcal{O}_{V_{\overline{k}},x}$ sind noethersch (ebenso wie die Varianten über k). Dies sollten Sie erwähnen, können aber auf den Beweis verzichten. Der Kernpunkt dabei ist der Hilbertsche Basissatz, der besagt, dass für jeden noetherschen Ring R auch der Polynomring $R[X]$ noethersch ist. Siehe [Fu] 1.4 und 2.4 Prop. 3.)

Erklären Sie, dass man zu $f \in \overline{k}[V]$ eine Abbildung $f\colon C(\overline{k}) \to \overline{k}$, "$x \mapsto f(x)$", erhält mit $\mathfrak{m}_x = \{f \in \overline{k}[V];\ f(x) = 0\}$.

Sei V eine über k definierte Varietät. Beweisen Sie, dass k in $k(V)$ algebraisch abgeschlossen ist. (Angenommen, es gäbe einen endlichen Erweiterungskörper $k \subsetneq k' \subset k(V)$. Wähle ein primitives Element $\alpha \in k'$ und schreibe $k' = k[\alpha] \cong k[X]/(f)$, wobei f das Minimalpolynom von α über k bezeichnet. Wir erhalten dann eine Inklusion $k[X]/(f) \subset k[V] \subset k(V)$. Zeigen Sie, dass daraus durch "Erweiterung der Skalare von k zu $\overline{k}$" eine Injektion $\overline{k}[X]/(f) \to \overline{k}[V]$ entsteht (zum Beispiel, indem Sie alle auftretenden Räume als Vektorräume über k bzw. $\overline{k}$ auffassen und geeignete Basen wählen; alternativ können Sie, sofern bekannt, das Tensorprodukt $\otimes_k \overline{k}$ verwenden). Dies ist ein Widerspruch, denn $\overline{k}[V]$ ist ein Integritätsbereich, $\overline{k}[X]/(f)$ jedoch nicht (warum?).)

4. Projektive Varietäten

[Ha] 1.2.

Definieren Sie den "projektiven Raum" $\mathbb{P}^n(\overline{k})$ über $\overline{k}$ (und analog über k) und die Galois-Operation, und begründen Sie, dass die Punkte in $\mathbb{P}^n(k)$ genau die Fixpunkte unter der Galois-Operation sind.

Definieren Sie die Begriffe eines homogenen Polynoms, eines homogenen Ideal, und der Nullstellenmenge eines solchen Ideals. Die Notation V_I (für ein homogenes (Prim-)Ideal I) in [Ha] sollten Sie ersetzen durch $V_+(I)$.

Erklären Sie die Bijektionen

$$U_i := \{(x_0 : \cdots : x_n) \in \mathbb{P}^n(\overline{k});\ x_i \neq 0\} \to \mathbb{A}^n(\overline{k}), \qquad (x_0 : \cdots : x_n) \mapsto \left(\frac{x_0}{x_i}, \ldots, \frac{x_n}{x_i}\right),$$

(wobei $\frac{x_i}{x_i}$ ausgelassen wird). Erklären Sie, dass mit dieser Identifikation die Menge $V_+(I) \cap U_i$ entweder leer (Beispiel?), oder eine affine algebraische Varietät ist, und beschreiben Sie das zugehörige Ideal in Termen von I. (Siehe zum Beispiel [Fu] 4.3 oder [GW] (1.19)–(1.21).) Die affinen Varietäten $V_+(I) \cap U_i$ bezeichnen wir als *affine Karten* von $V_+(I)$.

Beweisen Sie, dass alle diejenigen $V_+(I) \cap U_i$, die nicht leer sind, verstanden als affine Varietäten, *denselben* rationalen Funktionenkörper im Sinne des vorhergehenden Vortrags haben. Diesen Körper nennen wir den (rationalen) Funktionenkörper von $V_+(I)$.

Def. 1.12 und Remark 1.13 in [Ha] können ausgelassen werden.

5. Algebraische Kurven

Wir definieren eine *(glatte projektive) Kurve über k* als eine über k definierte projektive Varietät $C(\neq \emptyset)$, so dass für alle $P \in C(\overline{k})$ der lokale Ring $\mathcal{O}_{C_{\overline{k}},P}$ ein diskreter Bewertungsring ist, und ein Element $x \in k(C)$ existiert, so dass die Erweiterung $k(C)/k(x)$ endlich ist.

(Vergleiche auch [Ha] 1.3.)

Als Teil der Definition ist die Zuordnung $P \mapsto \mathcal{O}_{C_{\overline{k}},P}$ eine Abbildung

$$C(\overline{k}) \to \{\overline{k} \subsetneq R \subset \overline{k}(C);\ R \text{ diskr. Bewertungsring}\}.$$

Zeigen Sie, dass diese Abbildung bijektiv und verträglich mit den Operationen der Galois-Gruppe $\mathrm{Gal}(\overline{k}/k)$ auf beiden Seiten ist.

(Die entscheidende Überlegung ist dabei die folgende: Wir nehmen ohne Einschränkung an, dass (mit den obigen Bezeichnungen) $C \cap U_0 \neq \emptyset$ (also $\overline{k}[C \cap U_0] \subset \overline{k}(C)$), und haben so eine Surjektion $\overline{k}[T_1, \ldots, T_n] \to \overline{k}[C \cap U_0]$. Die Bilder der Variablen T_i auf der rechten Seite bezeichnen wir wieder mit T_i. Zur Vereinfachung der Notation setzen wir $T_0 := 1$. Ist nun $i \in \{0, \ldots, n\}$ mit $C \cap U_i \neq \emptyset$, so wird das Bild von $\overline{k}[U_i] \to \overline{k}[C \cap U_i]$ erzeugt von $\frac{T_0}{T_i}, \ldots, \frac{T_n}{T_i}$.

Ist $\overline{k} \subset R \subset \overline{k}(C)$ ein diskreter Bewertungsring mit Bewertungsfunktion v_R, und ist i so dass $v_R(T_i)$ minimal ist, so liegen $\frac{T_0}{T_i}, \ldots, \frac{T_n}{T_i}$ sämtlich in R, und mindestens eines dieser Elemente ist eine Einheit. Durch Projektion auf den Restklassenkörper erhalten wir ein Element $P \in \mathbb{P}^n(\overline{k})$, und es muss dann $R = \mathcal{O}_{C_{\overline{k}},P}$ gelten.)

Erklären Sie, dass jedes Element $f \in k(C) \setminus k$ eine surjektive Abbildung nach $\mathbb{P}^1$ liefert, vgl. [St] Remark 1.1.17.

6. Ebene Kurven

In diesem Vortrag betrachten wir Kurven (im Sinne des vorhergehenden Vortrags) $C \subset \mathbb{P}^2(\overline{k})$, die durch eine einzige Gleichung definiert werden (d.h. deren zugehöriges Ideal von einem einzigen homogenen Polynom erzeugt wird).

Beweisen Sie den folgenden

Satz. Sei $f \in k[X, Y, Z]$ ein irreduzibles homogenes Polynom, so dass es kein Tripel $(x, y, z) \in \overline{k}^3 \setminus \{(0, 0, 0)\}$ gibt mit $(x : y : z) \in V_+((f))$ für das der Vektor der partiellen Ableitungen

$$\left(\frac{\partial f}{\partial X}(x, y, z), \frac{\partial f}{\partial Y}(x, y, z), \frac{\partial f}{\partial Z}(x, y, z)\right) \in \overline{k}^3$$

der Nullvektor ist. Dann ist $C := V_+(f)$ eine glatte projektive Kurve.

Beachten Sie dazu, dass die obigen Bedingungen analoge Eigenschaften für die partiellen Ableitungen der Dehomogenisierungen von f liefern. Der wesentliche Punkt ist dann, zu beweisen, dass alle lokalen Ringe von C diskrete Bewertungsringe sind. Siehe [Fu] 3.2 Thm. 1; die Implikation, für die dort auf das Theorem 2 verwiesen wird, benötigen wir nicht. (Man kann auch zeigen, dass die Irreduzibilität von f schon aus der anderen Bedingung folgt; vielleicht können Sie erklären, dass ein Produkt zweier linearer Polynome jedenfalls die Bedingung an die Ableitungen nicht erfüllen kann.)

Geben Sie ein Beispiel eines irreduziblen Polynoms f, für das die obigen Bedingungen an die partiellen Ableitungen verletzt sind.

Erklären Sie, wann ein Polynom der Form $f = Y^2Z - X^3 - aXZ^2 - bZ^3$ (mit $a, b \in k$) die obigen Bedingungen erfüllt. (Dies liefert Beispiele für sogenannte elliptische Kurven.)

Schön wäre es, wenn Sie auch einige der Beispiele in [Ha] 1.3 diskutieren könnten.

7. Divisoren

Sei C eine über k definierte algebraische Kurve. Ein *Divisor* auf der Kurve C ist eine formale Linearkombination

$$\sum_{P \in C(\overline{k})} n_P[P], \quad n_P \in \mathbb{Z}, \quad n_P = 0 \text{ für alle bis auf endlich viele } P.$$

Die additive Gruppe der Divisoren bezeichnen wir mit $\mathrm{Div}(C)$. Der *Grad* von D ist

$$\deg(D) = \sum_P n_P \in \mathbb{Z}.$$

Wir erhalten so einen Gruppenhomomorphismus $\deg\colon \mathrm{Div}(C) \to \mathbb{Z}$ und bezeichnen seinen Kern mit $\mathrm{Div}^0(C)$. (Vergleiche [Ha] Def. 1.23; den Grad definieren wir anders!) Definiere die partielle Ordnung $\leq$, die Galois-Operation und die Untergruppen $\mathrm{Div}_k(C)$ und $\mathrm{Div}_k^0(C)$ wie in [Ha]. Man nennt einen Divisor D *positiv* oder *effektiv*, wenn $D \geq 0$.

Erinnern Sie an die Null-/Polstellenordnung einer "Funktion" $f \in \overline{k}(C)$ in einem Punkt P (im Sinne der Bewertungsfunktion $v_P \colon \overline{k}(C)^\times \to \mathbb{Z}$ zum lokalen Ring in P). Definieren Sie den Null-/Polstellendivisor $\operatorname{div}(f)$ von f.

Hier ist zu zeigen, dass $v_P(f) = 0$ für alle bis auf endlich viele P. Der Kernpunkt hierfür ist Punkt (v) des folgenden Lemmas:

Lemma.

(i) Sei R ein noetherscher Ring und $\mathscr{M}$ einen nicht-leere Menge von Idealen von R. Dann besitzt die Menge $\mathscr{M}$ ein maximales Element (bezüglich der Inklusion von Idealen).

(ii) Sei R ein noetherscher Ring, $\mathfrak{a} \subseteq R$ ein Ideal. Dann lässt sich das Radikal

$$\operatorname{rad}(\mathfrak{a}) := \{h \in \overline{k}[V];\ \exists n \geq 0 : h^n \in \mathfrak{a}\}$$

als der Durchschnitt von endlich vielen Primidealen $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ schreiben.

(iii) Seien $\mathfrak{p}_1, \ldots, \mathfrak{p}_n, \mathfrak{p}$ Primideale in einem Ring mit

$$\bigcap \mathfrak{p}_i \subseteq \mathfrak{p}.$$

Dann existiert ein i mit $\mathfrak{p}_i \subseteq \mathfrak{p}$.

(iv) Sei $V = C \cap U_i \neq \emptyset$ eine "affine Karte von C". Sei $\mathfrak{p} \subset \overline{k}[V]$ ein Primideal, das vom Nullideal verschieden ist. Dann ist $\mathfrak{p}$ ein maximales Ideal.

(v) Sei $V = C \cap U_i \neq \emptyset$ eine "affine Karte von C" und $g \in \overline{k}[V]$, $g \neq 0$. Dann liegt g in höchstens endlich vielen maximalen Idealen des Rings $\overline{k}[V]$.

Beweis. Für Teil (i) siehe [Fu] 1.5 Lemma. Nun zeigen wir (ii). Wir sagen, ein Ideal $\mathfrak{a}$ habe die Eigenschaft (DP), wenn sich $\operatorname{rad}(\mathfrak{a})$ als Durchschnitt von endlich vielen Primidealen schreiben lässt. Sei

$$\mathscr{M} := \{\mathfrak{a};\ \mathfrak{a} \text{ erfüllt nicht (DP)}\}.$$

Wir wollen zeigen, dass diese Menge leer ist. Andernfalls sei $\mathfrak{a} \in \mathscr{M}$ ein maximales Element. Dann ist $\mathfrak{a} = \operatorname{rad}(\mathfrak{a})$ kein Primideal, es existieren also $f, g \in R \setminus \mathfrak{a}$ mit $fg \in \mathfrak{a}$. Dann gilt $\mathfrak{a} \subsetneq (\mathfrak{a}, f)$, $\mathfrak{a} \subsetneq (\mathfrak{a}, g)$ und

$$\mathfrak{a} = (\mathfrak{a}, f) \cap (\mathfrak{a}, g).$$

Daraus erhält man einen Widerspruch zur Maximalität von $\mathfrak{a}$.

Aussage (iii) ist eine Standardeigenschaft von Primidealen (wenn die Folgerung falsch wäre, gäbe es $g_i \in \mathfrak{p}_i \setminus \mathfrak{p}$ für alle i. Betrachte dann das Produkt dieser Elemente).

Zu (iv) sei $\mathfrak{p} \neq 0$ ein Primideal. Dann existiert nach [St] Theorem 1.1.19 und Vortrag 5 ein Punkt $P \in V(\overline{k})$, so dass das maximale Ideal von $\mathcal{O}_{V,P}$ das Ideal $\mathfrak{p}$ enthält. Zeigen Sie, dass das von $\mathfrak{p}$ in $\mathcal{O}_{V,P}$ erzeugte Ideal $\mathfrak{P}$ ein Primideal mit der Eigenschaft $\mathfrak{P} \cap \overline{k}[V] = \mathfrak{p}$ ist. Die einzigen Primideale in $\mathcal{O}_{V,P}$ sind aber 0 und das maximale Ideal.

Teil (v) folgt nun aus (ii), (iii) und (iv). □

Mit dem Lemma können Sie die obige Aussage beweisen, indem Sie alle Karten $C \cap U_i$ betrachten und f jeweils als Quotient zweier Elemente aus $\overline{k}[V]$ schreiben.

Begründen Sie, dass für $f \in k(C)^\times$ der Divisor $\mathrm{div}(f)$ in $\mathrm{Div}_k(C)$ liegt.

8. Die Zeta-Funktion einer algebraischen Kurve

[Ha] 2.1 + 2.2 bis Prop. 2.2.20.

In diesem Vortrag soll nun der Begriff der Zetafunktion einer (glatten projektiven) Kurve über einem endlichen Körper eingeführt werden, und in Beziehung gesetzt werden zu Divisoren auf der Kurve. Bei den Beispielen müssen Sie vermutlich einiges kürzen, Sie sollten sie aber nicht komplett weglassen.

Erinnern Sie bei der Produktdarstellung der Zetafunktion an das ähnliche Eulerprodukt für die Riemannsche Zetafunktion, das wir im Einführungsvortrag gesehen haben.

9. Lineare Äquivalenz

[Ha], Def. 1.24, zweiter Teil.

Wir haben im vorhergehenden Vortrag gesehen, dass die Zetafunktion eng mit den Anzahlen von Divisoren mit gewissen Eigenschaften zusammenhängt. Um die Zetafunktion besser zu verstehen, studieren wir daher in diesem und dem folgenden Vortrag die Struktur der Gruppe $\mathrm{Div}_k(C)$ genauer.

Definieren Sie den Begriff der linearen Äquivalenz und die Notationen $\mathscr{L}(D)$, $\ell(D)$. Beweisen Sie:

- lineare Äquivalenz ist eine Äquivalenzrelation
- [Ha] Lemma A.13 (bis auf Teil (d); der in [Ha] gegebene "Beweis" ist in dieser Form nicht tragfähig).
- $D \sim 0 \Leftrightarrow (\deg(D) = 0 \text{ und } \ell(D) = 1)$.

Wenn genügend Zeit ist, könnten Sie erklären, wie [Ha] A.13 (d) mit der *Produktformel* zusammenhängt. (Details dazu gerne auf Nachfrage.)

Erklären Sie, dass es zu jedem $d \geq 0$ nur endlich viele Divisoren $D \in \mathrm{Div}_k(C)$ mit $D \geq 0$ und $\deg(D) = d$ gibt.

Erklären Sie, dass $(\mathscr{L}(D) \setminus \{0\})/k^\times$ in Bijektion steht zur Menge aller positiven Divisoren, die zu D linear äquivalent sind. Leiten Sie eine Formel für die Anzahl der über k definierten, positiven, zu $D \in \mathrm{Div}_k(C)$ linear äquivalenten Divisoren ab, in dem Fall, dass k ein endlicher Körper ist.

10. Der Satz von Riemann-Roch

[Ha] 1.4 Prop. 1.25 – Prop. 1.29.

Hiervon sollten Sie Prop. 1.25 und Cor. 1.28 beweisen, und den Satz von Riemann-Roch (Thm. 1.26) und Prop. 1.29 ohne Beweis angeben. Als weiteres "Korollar" sollten Sie angeben, dass $\deg(\mathrm{div}(f)) = 0$ für alle $f \in \overline{k}(C)^\times$.

Beweisen Sie den Satz von Riemann-Roch für $\mathbb{P}^1$. In diesem Fall sind alle Divisoren desselben Grades linear äquivalent, es ist $g = 0$, und für K können wir $-2[P]$ für irgendeinen Punkt P wählen. (Der Beweise des allgemeinen Falls ist natürlich deutlich schwieriger, wäre aber auch nicht außer Reichweite: In zwei bis drei Seminarvorträgen ließe er sich abhandeln, siehe [St] Theorem 1.5.15. Wir widmen uns in diesem Seminar stattdessen lieber den Anwendungen auf die Zetafunktion, auch weil sich der Beweis des Satzes von Riemann-Roch in den Vorlesungen zur algebraischen Geometrie als einfache Anwendung der sogenannten Serre-Dualität ergibt.)

Erklären Sie die folgende Anwendung des Satzes von Riemann-Roch: Sei E/k eine (glatte projektive) Kurve vom Geschlecht $g = 1$, und sei $O \in E(k)$ (man nennt E eine *elliptische Kurve*). Sei $\mathrm{Div}_k^0(E) \subset \mathrm{Div}_k(E)$ die Untergruppe der Divisoren vom Grad 0, und $\mathrm{Pic}_k^0(E) = \mathrm{Div}_k^0(E)/\sim$ die Menge der linearen Äquivalenzklassen darin. Dann ist die Abbildung

$$E(k) \to \mathrm{Pic}_k^0(E), \qquad P \mapsto [P] - [O],$$

eine Bijektion, und da die rechte Seite eine abelsche Gruppe ist, erhalten wir die Struktur einer abelschen Gruppe auf der linken Seite. (Sei D ein Divisor mit $\deg(D) = 1$. Zeigen Sie zunächst, dass $\ell(D) = 1$; folgern Sie, dass D linear äquivalent zu einem eindeutig bestimmten positiven Divisor (vom selben Grad) ist.)

11. Rationalität der Zeta-Funktion und Funktionalgleichung

[Ha] 2.21 – 2.36. (Achten Sie auf Tippfehler, zum Beispiel in der Definition von Z_1.)

Wir können nun mit Hilfe des Satzes von Riemann-Roch beweisen, dass die Zetafunktion eine rationale Funktion (d.h. Quotient zweier Polynome) ist und die gewünschte "Funktionalgleichung" erfüllt.

Die Aussage, dass —mit den Notationen von [Ha]— $\delta = 1$ gilt, ist es wert, als eigener Satz genannt zu werden (diese Tatsache wurde zuerst von F. K. Schmidt bewiesen; wenn genug Zeit ist, könnten Sie daraus folgern, dass für eine Kurve C über einem endlichen Körper $k = \mathbb{F}_q$ vom Geschlecht ≤ 1 stets $C(k) \neq \emptyset$ gilt).

Einfache Manipulationen von Potenzreihen (geom. Reihe) und rationalen Funktionen (z.B. Ende des Beweises von Prop. 2.26, Beweis von Prop. 2.27) sollten kurz gehalten werden.

12. Der Satz von Bombieri

[Ha] 2.34, 2.35, 3.2.

Der Satz von Bombieri ist der schwierigste Teil des Beweises der Weil-Vermutungen für Kurven. Erklären Sie die Grundidee ((i) auf Seite 235 von [Bo]), bevor Sie den eigentlichen Beweis beginnen. Den Beweis von Prop. 3.4 können Sie, wenn gewünscht, durch das Argument von [Lo], Ch. X, Lemma 5.1, ersetzen.

Wenn Sie das Gefühl haben, dass es die Darstellung vereinfacht, können Sie sich für den Beweis von Theorem 3.9 auf den Fall $\sigma = \mathrm{id}$ beschränken.

13. Der Beweis der Riemannschen Vermutung für Zeta-Funktionen von Kurven

[Ha] 3.1 + 3.3

In diesem Vortrag soll der Abschluss des Beweises skizziert werden, der auf einer trickreichen Idee beruht, die fehlende Abschätzung für die Kurve C durch die Untersuchung einer geeigneten Kurve C' zu beweisen, für deren Funktionenkörper wir Inklusionen

$$k(C') \supseteq k(C) \supseteq k(\mathbb{P}^1)$$

haben und so dass die Erweiterung $k(C')/k(\mathbb{P}^1)$ eine Galois-Erweiterung ist. Einige Ergebnisse müssen wir hierzu allerdings als *black box* benutzen, insbesondere die Tatsache, dass jeder Funktionenkörper von einer algebraischen Kurve herkommt (siehe [H] I.6), und die Beschreibung der Fasern der Abbildungen $C' \to C$ und $C' \to \mathbb{P}^1$ in der obigen Konstellation. (Siehe [St] Theorem 3.11, Theorem 3.7.1, Cor. 3.7.2.)

Die Definition von $N^\sigma(C)$ (Seite 36 unten in [Ha]) ist eventuell missverständlich. Wir setzen

$$N^\sigma(C) = \#\{P \in C(\overline{k});\ \sigma(P) = F(P)\},$$

wobei $F\colon C(\overline{k}) \to C(\overline{k})$ die Frobeniusbijektion bezeichnet, die alle Koordinaten in die q-te Potenz erhebt. Mehrere der Formulierungen (zum Beispiel die Aussage von Prop. 3.18) sollten Sie präzisieren, was die Abhängigkeit von q betrifft.

Literatur

[Bo] E. Bombieri, *Counting points on curves over finite fields*, Séminaire Bourbaki, Exposé no. 430 (1972/73).

[Fu] W. Fulton, *Algebraic Curves. An Introduction to Algebraic Geometry* (Available online at `http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf`)

[GW] U. Görtz, T. Wedhorn, *Algebraic Geometry I. Schemes*, Vieweg+Teubner, 2010.

[Ha] S. H. Hansen, *Rational Points on Curves over Finite Fields*, Lect. Notes Ser., Aarhus Univ. Mat. Institute, 1995. Available online.

[H] R. Hartshorne, *Algebraic Geometry*, Springer Graduate Texts in Mathematics **52** (1977).

[Lo] D. Lorenzini, *An invitation to Arithmetic Geometry*, Grad. Studies in Math. **9**, Amer. Math. Soc., 1996.

[St] H. Stichenoth, *Algebraic Function Fields and Codes*, Springer Graduate Texts in Math. **254**, 2nd ed., 2009.