Seminar Einführung in die Theorie elliptischer Kurven

Lokale und globale Körper

Saskia Klaus

18.06.2015

1 Motivation

Betrachten wir den Ring $\mathbb{Z}$ und eine Primzahl $p \in \mathbb{Z}$. Wie können wir das Zerlegungsverhalten von p in einem vergrößerten Ring, beispielsweise $\mathbb{Z}[i]$ beschreiben? Genauere Betrachtung führt uns in diesem Beispiel auf das folgende Gesetz:

p bleibt prim $\Leftrightarrow p \equiv 3 \mod 4$,

p zerfällt in das Produkt zweier nichtassoziierter Elemente $\Leftrightarrow p \equiv 1 \mod 4$,

p zerfällt in das Produkt zweier assoziierter Elemente $\Leftrightarrow p = 2$.

Diese Fragestellung soll in diesem Vortrag verallgemeinert werden.

2 Dedekindringe, Erweiterung von Primidealen

Definition. Sei $A \subseteq B$ eine Ringerweiterung. Wir nennen ein $b \in B$ *ganz* über A genau dann, wenn b Nullstelle eines normierten Polynoms $f \in A[X]$ ist.

Bemerkung. Diese Definition ist äquivalent dazu, dass $A[b]$ als A-Modul endlich erzeugt ist. Daraus erhalten wir leicht, dass für zwei ganze Elemente b_1, b_2 auch ihre Summe $b_1 + b_2$ und ihr Produkt $b_1 b_2$ ganz sind: Wegen der Ganzheit von b_1 und b_2 ist $A[b_1, b_2]$ ein endlich erzeugter A-Modul, also auch $A[b_1, b_2, b_1 + b_2]$.

Definition. Sei A ein nullteilerfreier Ring, $K = Q(A)$ der Quotientenkörper und L/K eine endliche Körpererweiterung. Dann ist $A_L := \{x \in L \mid x \text{ ganz über } A\}$ der *Ganzabschluss* von A in L. A heißt *ganzabgeschlossen*, wenn $A = A_K$.

Bemerkung. Da $L = Q(A_L)$ und $(A_L)_L = A_L$, ist A_L ganzabgeschlossen.

Lemma 1. Ist A ein Hauptidealring, $K = Q(A)$ und L/K endliche Erweiterung, so ist $B = A_L$ ein freier A-Modul vom Rang $[L : K]$. Insbesondere existiert also eine Basis von B als A-Modul. Eine solche nennt man *Ganzheitsbasis*.

Definition. Sei K ein Zahlkörper (d.h. eine endliche Erweiterung von $\mathbb{Q}$), O_K der Ganzabschluss von $\mathbb{Z}$ in K und $(\alpha_1, \ldots, \alpha_n)$ eine (nach dem vorherigen Lemma existierende) Ganzheitsbasis von O_K. Sei weiter $\mathrm{sp}\colon K \times K \to \mathbb{Q}$, $(x, y) \mapsto \mathrm{sp}_{K/\mathbb{Q}}(xy)$ die Spurform.
Die Zahl $d_K := \det(\mathrm{sp}(\alpha_i, \alpha_j))_{ij}$ heißt *Diskriminante* von K.

Satz 2. d_K hängt nicht von der Wahl der Ganzheitsbasis ab.

Satz 3. Ist $K = \mathbb{Q}\left(\sqrt{d}\right)$ mit quadratfreiem d, so gilt $O_K = \begin{cases} \mathbb{Z}\left[\sqrt{d}\right] & d \not\equiv 1 \mod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & d \equiv 1 \mod 4 \end{cases}$

Im ersten Fall gilt $d_K = 4d$, im zweiten stimmt die Diskriminante mit d überein.

Definition. Ein noetherscher, ganzabgeschlossener, nullteilerfreier Ring, in dem jedes Primideal ungleich Null ein Maximalideal ist, heißt *Dedekindring*.

Beispiel.
- Hauptidealringe sind Dedekindringe, insbesondere also $\mathbb{Z}$.
- Ist A ein Dedekindring, K sein Quotientenkörper und L/K eine endliche Erweiterung, so ist der Ganzabschluss von A in L ein Dedekindring.

Satz 4. In einem Dedekindring hat jedes Ideal $\mathfrak{a} \neq 0$ eine bis auf Reihenfolge eindeutige Zerlegung $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_n$ in das Produkt von Primidealen $\mathfrak{p}_i \neq 0$.

Sei ab jetzt in diesem Abschnitt A stets ein Dedekindring, $K = Q(A)$ sein Quotientenkörper, L/K endliche Erweiterung und $B = A_L$.
Sei $\mathfrak{p}$ ein Primideal in A. Über $\mathfrak{p} = \mathfrak{p}B$ können wir es als Ideal in B auffassen. Da B ein Dedekindring ist, hat dieses eine eindeutige Primidealzerlegung: $\mathfrak{p} = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$.

Definition. e_i in der obigen Gleichung heißt *Verzweigungsindex*, die Zahl $f_i = [B/\mathfrak{P}_i : A/\mathfrak{p}]$ *Trägheitsgrad* von $\mathfrak{P}_i$ über $\mathfrak{p}$.

Satz 5. (fundamentale Gleichung)
Ist L/K separabel und $n = [L : K]$, so gilt $\sum_{i=1}^{r} e_i f_i = n$.

Definition. In der Erweiterung $A \subseteq B = A_L$ und der Darstellung von $\mathfrak{p}$ als Produkt von Primidealen in B wie oben, nennt man $\mathfrak{p}$

- total zerlegt $\Leftrightarrow r = n \,(\Rightarrow e_i = 1 = f_i \;\forall\, i)$
- unzerlegt $\Leftrightarrow r = 1$
- unverzweigt $\Leftrightarrow e_i = 1$ und $B/\mathfrak{P}_i$ über $A/\mathfrak{p}$ separabel $\;\forall i$
- träge $\Leftrightarrow$ unverzweigt und $r = 1$

Lemma 6. Sei L/K separable Erweiterung. Dann existieren nur endlich viele Primideale in K, die in L verzweigen.

Satz 7. Sei $K = \mathbb{Q}(\sqrt{d})$ quadratischer Zahlkörper. Dann gelten:

(i) Eine Primzahl $p \neq 2$ ist in O_K $\begin{cases} \text{träge} & \Leftrightarrow \left(\frac{d_K}{p}\right) = -1 \\ \text{voll zerlegt} & \Leftrightarrow \left(\frac{d_K}{p}\right) = 1 \\ \text{verzweigt} & \Leftrightarrow \left(\frac{d_K}{p}\right) = 0 \end{cases}$

(ii) 2 ist in $\mathcal{O}_K$ $\begin{cases} \text{träge} & \Leftrightarrow d_K \equiv 5 \mod 8 \\ \text{voll zerlegt} & \Leftrightarrow d_K \equiv 1 \mod 8 \\ \text{verzweigt} & \Leftrightarrow 2 | d_K \end{cases}$

Sei ab jetzt L/K galoissch, G bezeichne die Galoisgruppe.

Lemma 8. *G wirkt transitiv auf der Menge der Primideale $\mathfrak{P}$ über $\mathfrak{p}$ (d.h. auf der Menge der Primideale, die in der eindeutigen Primzerlegung von $\mathfrak{p}$ auftauchen).*

Definition. Für $\mathfrak{P}$ über $\mathfrak{p}$ heißt $G_{\mathfrak{P}} = \{\sigma \in G \mid \sigma\mathfrak{P} = \mathfrak{P}\}$ die *Zerlegungsgruppe* von $\mathfrak{P}$ über K.

Bemerkung. Offenbar entspricht die Anzahl der verschiedenen Primideale über $\mathfrak{p}$ gerade dem Index $(G : G_{\mathfrak{P}})$.

3 Bewertungstheorie

Definition.

- Ein Betrag auf einem Körper K ist eine Funktion $|\cdot| \colon K \to \mathbb{R}_{\geq 0}$ mit den folgenden Eigenschaften:
  (i) $|x| = 0 \Leftrightarrow x = 0$
  (ii) $|xy| = |x| \cdot |y|$
  (iii) $|x + y| \leq |x| + |y|$
- Ein Betrag $|\cdot|$ heißt *nichtarchimedisch* genau dann, wenn $|x + y| \leq \max\{|x|, |y|\}$.
- Zwei Beträge $|\cdot|_1, |\cdot|_2$ heißen äquivalent $\Leftrightarrow$ es gibt ein $s \in \mathbb{R}_{>0}$, sodass $|x|_1 = |x|_2^s \ \forall x \in K$.

Definition. Eine nichtarchimedische *Bewertung* auf K ist eine Funktion $v \colon K \to \mathbb{R} \cup \{\infty\}$, sodass
(i) $v(x) = \infty \Leftrightarrow x = 0$
(ii) $v(xy) = v(x) + v(y)$
(iii) $v(x + y) \geq \min\{v(x), v(y)\}$

Bemerkung. Die Konzepte Betrag und Bewertung lassen sich im folgenden Sinn ineinander überführen:

- Für eine Bewertung v und ein $q \in \mathbb{R}_{>1}$ ist $|x|_v := q^{-v(x)} \ \forall x \in K$ ein Betrag,
- für einen (nichtarchimedischen) Betrag $|\cdot|$ ist $v(x) := \log |x|$ eine Bewertung.

Definition. $\mathcal{O} = \{x \in K \mid v(x) \geq 0\}$ heißt *Bewertungsring* zu v. Den Körper $k := \mathcal{O}/\mathfrak{p}$ für das eindeutige Primideal $\mathfrak{p} = \{x \in K \mid v(x) > 0\}$ nennen wir den *Restklassenkörper* der Bewertung.

Die Bewertungstheorie steht mit den Betrachtungen aus dem zweiten Abschnitt in Verbindung, indem wir für einen Dedekindring A und seinen Quotientenkörper $K = Q(A)$ und jedes Primideal $0 \neq \mathfrak{p} \subseteq A$ die $\mathfrak{p}$-adische Bewertung $v_{\mathfrak{p}}$ definieren durch $v_{\mathfrak{p}}(a) = v_{\mathfrak{p}}$, wobei $(a) = \prod_{\mathfrak{q}} \mathfrak{q}^{v_{\mathfrak{q}}}$.

Definition. Eine Bewertung v heißt *diskret* genau dann, wenn es ein $\delta > 0$ gibt, sodass für alle $x \in K : (1 - \delta < |x|_v < 1 + \delta \Rightarrow |x|_v = 1)$.

Bemerkung. Jede diskrete Bewertung ist nichtarchimedisch.

Definition. Ein *lokaler* Körper ist ein bezüglich einer diskreten Bewertung vollständiger Körper mit endlichem Restklassenkörper.
Ein *globaler* Körper ist eine endliche Erweiterung von $\mathbb{Q}$ oder $\mathbb{F}_p(T)$.

Satz 9.
- Ist K ein archimedischer lokaler Körper[1], so ist K isomorph zu $\mathbb{R}$ oder $\mathbb{C}$.
- Ist K ein nichtarchimedischer lokaler Körper der Charakteristik 0, so ist K isomorph zu einer endlichen Erweiterung von $\mathbb{Q}_p$, wobei die Primzahl p gerade die Charakteristik des Restklassenkörpers ist.
- Ist K ein nichtarchimedischer lokaler Körper mit Charakteristik $p > 0$, so ist K isomorph zu einer endlichen Erweiterung von $\mathbb{F}_p((T))$.

Lemma 10. (Hensels Lemma)
Sei $(A, \mathfrak{m})$ ein lokaler vollständiger Ring, $k = A/\mathfrak{m}$ sein Restklassenkörper. Sei weiter $f \in A[X]$, sodass die Reduktion $\overline{f} \in k[X]$ eine einfache Nullstelle $\lambda \in k$ hat. Dann existiert ein eindeutig bestimmtes $x \in A$ mit $f(x) = 0$ und $\overline{x} = \lambda$.

Wir können dieses Lemma verwenden, indem wir einen vollständigen Körper (K, v) betrachten sowie seinen Bewertungsring $A = \mathcal{O}$, das eindeutigen Maximalideal $\mathfrak{m} = \mathfrak{p}$ und den zugehörigen Restklassenkörper $k = \mathcal{O}/\mathfrak{p}$. Insbesondere haben lokale Körper also die praktische Eigenschaft, dass man Nullstellen im Restklassenkörper liften kann.

4 Fortsetzung von Bewertungen

Definition. Sei L/K eine Körpererweiterung, v eine Bewertung auf K. Eine Bewertung w auf L heißt Fortsetzung von v, wenn $|x|_v = |x|_w$ für alle $x \in K$. Notation: $w|v$.

Satz 11. Sei L/K endlich separabel, v diskrete Bewertung auf K und $B = (\mathcal{O}_v)_L$. Dann gibt es eine 1:1-Korrespondenz zwischen den Primidealen $0 \neq \mathfrak{P} \subseteq B$ über $\mathfrak{p}_v$ und den Bewertungen w auf L mit $w|v$.
Insbesondere existieren Fortsetzungen von v.

Bemerkung. Ist (K, v) vollständig und L/K eine algebraische Erweiterung, so ist die Fortsetzung w eindeutig.

Definition. Sei L/K eine Erweiterung, v Bewertung auf K, w eine Fortsetzung auf L. Dann heißen $e_w = (w(L^\times) : v(K^\times))$ Verzweigungsindex und $f_w = [\lambda_w : \kappa]$ Trägheitsgrad von w über K, wobei wir mit λ_w und κ die jeweiligen Restklassenkörper bezeichnen.

Man kann zeigen, dass Verzweigungsindex und Trägheitsgrad der Fortsetzung w mit dem Verzweigungsindex und Trägheitsgrad des (nach obigem Satz existierenden) zugehörigen Primideals übereinstimmen.

[1] Laut unserer Definition sind archimedische lokale Körper nicht möglich, man kann lokale Körper aber auch so definieren, dass dies ohne Widerspruch funktioniert. Der Vollständigkeit halber ist der erste Teil des Satzes trotzdem mit genannt.

Satz 12. (fundamentale Gleichung)
Sei L/K eine endliche separable Erweiterung, v eine diskrete Bewertung auf K, dann gilt

$$\sum_{w|v} e_w f_w = [L : K].$$

Sei ab jetzt L/K endlich galoissch, $G = G(L/K)$ die Galoisgruppe und v eine nichtarchimedische Bewertung auf K.

Lemma 13. G wirkt transitiv auf der Menge der Fortsetzungen von v.

Definition. Sei $w|v$ eine Fortsetzung auf L. Dann heißt $G_w = G_w(L/K) = \{\sigma \in G \mid w \circ \sigma = w\}$ die Zerlegungsgruppe von w über K.

Satz 14. $G_w(L/K) \cong G(L_w/K_v)$, wobei K_v die Vervollständigung von K bezüglich v und L_w die Vervollständigung von L bezüglich w bezeichnen.

Satz 15. Sei $Z_w = L^{G_w}$ und $w_z := w|_{Z_w}$. Dann gelten:
(i) w_z setzt sich eindeutig auf L fort
(ii) $f_w(L/Z_w) = f_w(L/K),\ e_w(L/Z_w) = e_w(L/K)$
(iii) $f_{w_z}(Z_w/K) = 1 = e_{w_z}(Z_w/K)$

Jedes $\sigma \in G_w$ induziert einen Automorphismus $\overline{\sigma}\colon \lambda \to \lambda,\ x \mod \mathfrak{P}_w \mapsto \sigma x \mod \mathfrak{P}_w$ (wobei λ der Restklassenkörper zu w, $\mathfrak{P}_w$ das Primideal).

Satz 16. Die Restklassenkörpererweiterung λ über κ ist normal und der Homomorphismus $G_w \to G(\lambda/\kappa),\ \sigma \mapsto \overline{\sigma}$ ist surjektiv.

Definition. $I_w = I_w(L/K) = \ker(G_w \to G(\lambda/\kappa))$ heißt Trägheitsgruppe von w.

Bemerkung. Es gilt $I_w = \{\sigma \in G_w \mid \sigma x \equiv x \mod \mathfrak{P}_w\ \forall x \in \mathcal{O}_w\}$.

Wir haben eine exakte Folge $1 \to I_w \to G_w \to G(\lambda/\kappa) \to 1$.

Satz 17. Sei $T_w = L^{I_w}$. Die Erweiterung T_w/Z_w ist galoissch und die Galoisgruppe entspricht gerade $G(T_w/Z_w) = G(\lambda/\kappa)$. Sei $w_T = w|_{T_w}$. Dann gilt:
(i) $e_w(L/T_w) = e_w(L/K),\ f_w(L/T_w) = 1$
(ii) $e_{w_T}(T_w/Z_w) = 1,\ f_{w_T}(T_w/Z_w) = f_w(L/K)$.

Also haben wir die Verzweigungsindizes und Trägheitsgrade nun wie folgt aufgeteilt:

$$K \overset{1}{\underset{1}{\subseteq}} Z_w \overset{1}{\underset{f}{\subseteq}} T_w \overset{e}{\underset{1}{\subseteq}} L$$

Definition. Eine endliche separable Erweiterung lokaler Körper L/K heißt *unverzweigt*, wenn die Restklassenkörpererweiterung λ/κ separabel ist und $[L : K] = [\lambda : \kappa]$.

Bemerkung. Komposita unverzweigter Erweiterungen sind unverzweigt.

Definition. Sei L/K algebraisch. Das Kompositum aller unverzweigten Teilerweiterungen heißt *maximal unverzweigte* Teilerweiterung von L/K.

Lemma 18. T_w/Z_w ist die maximal unverzweigte Teilerweiterung von L/Z_w.

5 Beispiel

Sei $K = \mathbb{Q}(\sqrt{d})$ ein quadratischer Zahlkörper. Wie können wir das Ideal (3) für $d = -5, 3, 5$ zerlegen?
Nach den bisherigen Betrachtungen haben wir verschiedene Möglichkeiten:

- das Ideal zerlegen, direkt ausrechnen
- ein Primideal $\mathfrak{P}$ über (3) finden und mit Hilfe der Gruppe $G_{\mathfrak{P}}$ bestimmen, ob es weitere gibt, ggf. weitere Primideale über (3) finden
- die Galoisgruppe der Lokalisierungen bestimmen

Wir betrachten nun das erste Verfahren. Die Lösungen lassen sich meist noch weiter zusammenfassen, aber hier seien sie so dargestellt, wie man sie durch Ausrechnen erhält.
Fall 1:
Sei $d = -5 \equiv 3 \mod 4$, also $d_K = -20$. Wegen $\left(\frac{-20}{3}\right) = 1$ ist das Ideal (3) hier zerlegt. Wir betrachten nun den Ganzheitsring $O_K = \mathbb{Z}[\sqrt{-5}] \cong \mathbb{Z}[X]/(X^2 + 5)$. Es gilt:

$$O_K/(3) \cong (\mathbb{Z}/3\mathbb{Z}[X])/(X^2 + 5) = (\mathbb{Z}/3\mathbb{Z}[X])/(X^2 + 2) \cong (\mathbb{Z}/3\mathbb{Z}[X])/(X + 2) \times (\mathbb{Z}/3\mathbb{Z}[X])/(X + 1)$$

Also können wir (3) schreiben als $(3) = (3, \sqrt{-5} + 2)(3, \sqrt{-5} + 1)$.

Fall 2: Sei $d = 3$, dann ist die Diskriminante $d_K = 12$. Wegen $\left(\frac{12}{3}\right) = 0$ verzweigt (3) in diesem Fall. Für das Minimalpolynom gilt in diesem Fall $X^2 - 3 \equiv X^2 \mod 3$, also $(3) = (3, \sqrt{-3})^2$.

Fall 3: Ist $d = 5 \equiv 1 \mod 4$, so ist $d_K = 5$, und wegen $\left(\frac{5}{3}\right) = -1$ ist (3) träge, bleibt also prim.