# Die Endlichkeit der Klassenzahl für Zahlkörper

Karina Tulchinskaja

14.06.2017

Wie im letzten Vortrag sei $\mathbb{Q} \subset F$ eine separable Körpererweiterung mit $F \subset \mathbb{C}$. Im Folgenden werden wir uns mit dem Ring $D = F \cap \Omega$ befassen, wobei $\Omega$ der Ring der ganzalgebraischen Zahlen ist. Wir werden zeigen, dass es in $D$ eine Art Primfaktorzerlegung für Ideale gibt. Mit Ideal wird im Folgenden allerdings nie das Nullideal gemeint sein.

**Definition.** Man nennt zwei Ideale $\mathfrak{a}, \mathfrak{b} \subset D$ **äquivalent**, falls $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$ für $\alpha, \beta \in D \setminus \{0\}$ gilt. Dann schreiben wir $\mathfrak{a} \sim \mathfrak{b}$.
$\sim$ ist eine Äquivalenzrelation.
Die Äquivalenzklassen heißen **Idealklassen**. Ihre Anzahl bezeichnen wir als $h_F$, die **Klassenzahl** von $F$.

**Lemma. 5.** Es gibt ein $M \in \mathbb{Z}_+$, welches nur von $F$ abhängt, mit folgender Eigenschaft:
Für alle $\alpha, \beta \in D$, $\beta \neq 0$, gibt es ein $\omega \in D$ und ein $t \in \mathbb{Z}$ mit $1 \leq t \leq M$, sodass:

$$| N(t\alpha - \omega\beta) |<| N(\beta) |$$

**Beweis.** Die Elemente $t, \omega$ und $M$ werden wir im Laufe des Beweises geeignet konstruieren.
Wir definieren $\gamma = \frac{\alpha}{\beta} \in F$. Damit gilt:

$$| N(t\alpha - \omega\beta) |=| N(\beta)N(t\gamma - \omega) |$$

Also ist zu zeigen:

$$| N(t\gamma - \omega) |< 1$$

Zuerst wählen wir eine Integritätsbasis $\omega_1, ..., \omega_n$ von $D$. Damit können wir ein beliebiges Element $\lambda \in F$ schreiben als $\lambda = \sum_{i=1}^{n} \lambda_i\omega_i$ mit $\lambda_i \in \mathbb{Q}$.
Nun definieren wir $[\lambda]$ und $\{\lambda\}$ wie folgt: Zu jedem i=1,...,n sei $\lambda_i = [\lambda_i] + \{\lambda_i\}$ mit $[\lambda_i] \in \mathbb{Z}$ und $\{\lambda_i\} \in \mathbb{Q}$, wobei $0 \leq \{\lambda_i\} < 1$.
$[\lambda] = \sum_{i=1}^{n}[\lambda_i]\omega_i$ und $\{\lambda\} = \sum_{i=1}^{n}\{\lambda_i\}\omega_i$ erfüllen dann $\lambda = [\lambda] + \{\lambda\}$.
Nun führen wir eine allgemeine Abschätzung der Norm durch, welche wir im

letzten Beweisschritt benutzen werden. Dabei nutzen wir Eigenschaften der $\mathbb{Q}$-Isomorphismen $\sigma_1$,...,$\sigma_n$ aus:

$$| N(\lambda) |=| \prod_{j=1}^{n} \sigma_j(\sum_{i=1}^{n} \lambda_i\omega_i) |=| \prod_{j=1}^{n}(\sum_{i=1}^{n} \lambda_i\sigma_j(\omega_i)) |\leq (\max_{i=1,\dots,n} | \lambda_i |)^n C,$$

wobei $C =| \prod_{j=1}^{n}(\sum_{i=1}^{n} \sigma_j(\omega_i)) |$.
Wir wählen nun ein $m \in \mathbb{Z}$ mit $m > \sqrt[n]{C}$ und definieren $M = m^n$.
Betrachten wir folgende Abbildung:

$$\varphi : F \to \mathbb{R}^n, \sum_{i=1}^{n} \lambda_i\omega_i \mapsto (\lambda_1, ..., \lambda_n)$$

Elemente der Form $\varphi(\{\lambda\})$ liegen im Würfel $[0, 1]^n$. Diesen zerlegen wir in $m^n$ kleine Würfel mit Seitenlängen $\frac{1}{m}$. An dieser Stelle wenden wir die obigen Erkenntnisse auf $\gamma = \frac{\alpha}{\beta}$ an:
Betrachte die Elemente $\varphi(\{k\gamma\}),\ k = 1, ..., m^n + 1$. Das sind $m^n + 1$ Stück, also müssen zwei von diesen im selben kleinen Würfel liegen. Seien dies die Bilder von $\{h\gamma\}$ und $\{l\gamma\}$, ohne Einschränkung mit $h > l$.
Das bedeutet $| \{h\gamma_i\} - \{l\gamma_i\} |\leq \frac{1}{m}$ für alle $i = 1, ..., n$. Setzte $t = h - l$. Dieses $t$ erfüllt $1 \leq t \leq M$, da $1 \leq h - l \leq m^n = M$.
Definiere noch das $\omega$ so: $t\gamma = \omega + \delta$, wobei $\omega = [h\gamma] - [l\gamma]$ und $\delta = \{h\gamma\} - \{l\gamma\}$. $\omega \in D$, da $\omega_1, ..., \omega_n$ eine Integritätsbasis von $D$ ist.
Es gilt:

$$| N(t\gamma - \omega) |=| N(\delta) |\leq (max_{i=1,\dots,n} | \{h\gamma_i\} - \{l\gamma_i\} |)^n C < (\frac{1}{m})^n m^n = 1$$

$\square$

**Theorem. 1.** Die Klassenzahl $h_F$ ist endlich.

**Beweis.** Sei $\mathfrak{a} \subset D$ ein beliebiges Ideal. Es ist $| N(\lambda) |\in \mathbb{Z}_+$ für alle $\lambda \in \mathfrak{a}\backslash\{0\}$. Daher können wir ein $\beta \in \mathfrak{a} \setminus \{0\}$ wählen mit $| N(\beta) |$ minimal. Wir wählen außerdem ein beliebiges $\alpha \in \mathfrak{a} \setminus \{0\}$.
Nach Lemma 2 gibt es Elemente $\omega \in D,\ M \in \mathbb{Z}_+ \subset D$ und $t \in \mathbb{Z}_+ \subset D$ mit $1 \leq t \leq M$, sodass gilt: $| N(t\alpha - \omega\beta) |<| N(\beta) |$
Es gilt $t\alpha - \omega\beta \in \mathfrak{a}$ und aus der Minimalität von $| N(\beta) |$ folgt $t\alpha - \omega\beta = 0$. Das heißt $t\alpha \in (\beta)$, wegen $t \mid M!$ auch $M!\alpha \in (\beta)$. Da das $\alpha \in a$ beliebig gewählt war, folgt $M!\mathfrak{a} \subset (\beta)$.
Wir definieren $\mathfrak{b} = \frac{1}{\beta}M!\mathfrak{a}$. Dieses $\mathfrak{b}$ ist ein Ideal und erfüllt $M!\mathfrak{a} = (\beta)\mathfrak{b}$, das heißt $\mathfrak{a} \sim \mathfrak{b}$. Da $\beta \in \mathfrak{a}$, gilt $M!\beta \in M!\mathfrak{a} = (\beta)\mathfrak{b}$. Das zeigt $M! \in \mathfrak{b}$.
Als nächstes wollen wir zeigen, dass es nur endlich viele Ideale gibt, die $M!$ enthalten. Da in jeder Idealklasse eins davon liegt, wird daraus die Endlichkeit von $h_F$ folgen.
Sei $\mathfrak{c}$ ein Ideal in $D$, das $M!$ enthält. Diese Aussage ist äquivalent zu:

$(M!) \subset \mathfrak{c} \subset D$. Dann gilt $\mathfrak{c}/(M!) \subset D/(M!)$. Nach Proposition 12.2.3 ist $D/(M!)$ endlich, besitzt also nur endlich viele Teilmengen. Somit gibt es nur endlich viele Ideale $\mathfrak{c} \subset D$, für die $\mathfrak{c}/(M!)$ solche Teilmengen sind.

□

**Proposition. 12.2.5** Für jedes Ideal $\mathfrak{a} \subset D$ gibt es ein $k \in \mathbb{Z},\ 1 \leq k \leq h_F$, sodass $\mathfrak{a}^k$ ein Hauptideal ist.

**Beweis.** Sei $\mathfrak{a} \subsetneq D$ beliebiges Ideal. Betrachte die Ideale $\mathfrak{a}, \mathfrak{a}^2, ..., \mathfrak{a}^{h_F+1}$. Mindestens zwei von diesen müssen zueinander äquivalent sein: $\mathfrak{a}^i \sim \mathfrak{a}^j$, ohne Einschränkung mit $i < j$.
Für gewisse $\alpha, \beta \in D \setminus \{0\}$ gilt also: $(\alpha)\mathfrak{a}^i = (\beta)\mathfrak{a}^j = (\beta)\mathfrak{a}^{j-i}\mathfrak{a}^i$. Rausteilen von $\beta$ liefert $\frac{\alpha}{\beta}\mathfrak{a}^i = \mathfrak{a}^{j-i}\mathfrak{a}^i \subset \mathfrak{a}^i$ und nach Lemma 3 gilt $\frac{\alpha}{\beta} \in D$.
Obige Zeile wird damit zu $(\frac{\alpha}{\beta})\mathfrak{a}^i = \mathfrak{a}^{j-i}\mathfrak{a}^i$. Schließlich folgt $\mathfrak{a}^{j-i} = (\frac{\alpha}{\beta})$ mit Proposition 12.2.4.

□

**Behauptung.** Die Idealklasse von $D$ ist die Klasse der Hauptideale:
$[\mathfrak{a}] = [D] \Leftrightarrow \mathfrak{a}$ Hauptideal

**Beweis.** Die Rückrichtung ist trivial. Für die Hinrichtung zeigen wir beide Inklusionen separat.
Es gelte $[\mathfrak{a}]$ = [D], also $(\alpha)\mathfrak{a} = (\beta)D = (\beta)$ für gewisse $\alpha, \beta \in D$.
Für jedes $a \in \mathfrak{a}$ gibt es ein $r \in D$ mit $\alpha a = r\beta$. Somit $a = r\frac{\beta}{\alpha} \in (\frac{\beta}{\alpha})$.
Andererseits gibt es ein $a \in \mathfrak{a}$ mit $\beta = \alpha a$, also $\frac{\beta}{\alpha} = a \in \mathfrak{a}$.

□

An dieser Stelle bietet es sich an zu erwähnen, dass die Menge der Idealklassen eine Gruppe bildet. Die Verknüpfung ist dabei definiert als $[\mathfrak{a}] \cdot [\mathfrak{b}] = [\mathfrak{a}\mathfrak{b}]$, und man rechnet leicht nach, dass dies wohldefiniert ist.
Assoziativität in dieser Gruppe folgt aus der Assoziatiovität des Ringes $D$.
Das neutrale Element ist die Idealklasse von $D$, denn $[\mathfrak{a}] \cdot [D] = [\mathfrak{a}D] = [\mathfrak{a}]$ für alle Ideale $\mathfrak{a} \subset D$.
Inverse Elemente sind von der Form $[\mathfrak{a}]^{-1} = [\mathfrak{a}^{k-1}]$, wobei das $k$ so wie in der vorangeganenen Proposition gegeben ist.
Schließlich folgt mit obiger Behauptung und der Tatsache, dass die Menge der Idealklassen eine Gruppe der Ordnung $h_F$ bildet, dass $\mathfrak{a}^{h_F}$ ein Hauptideal ist, für jedes Ideal $\mathfrak{a} \subset D$.

**Proposition. 12.2.6.** Seien $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \subset D$ Ideale mit $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{c}$. Dann gilt $\mathfrak{b} = \mathfrak{c}$.

**Beweis.** Nach vorangegangener Proposition ist $\mathfrak{a}^k = (\alpha)$ für ein $\alpha \in D \setminus \{0\}$ und ein $k \in \mathbb{Z}_+$. Multiplizieren von $\mathfrak{ab} = \mathfrak{ac}$ mit $\mathfrak{a}^{k-1}$ liefert $(\alpha)\mathfrak{b} = (\alpha)\mathfrak{c}$. Also gilt $\mathfrak{b} = \mathfrak{c}$.

□

**Proposition. 12.2.7.** Seien $\mathfrak{a}, \mathfrak{b} \subset D$ Ideale mit $\mathfrak{a} \subset \mathfrak{b}$. Dann gibt es ein Ideal $\mathfrak{c} \subset D$ mit $\mathfrak{a} = \mathfrak{bc}$.

**Beweis.** Es gilt $\mathfrak{b}^k = (\beta)$ für ein $\beta \in D \setminus \{0\}$ und ein $k \in \mathbb{Z}_+$. Multiplizieren von $\mathfrak{a} \subset \mathfrak{b}$ mit $\mathfrak{b}^{k-1}$ liefert $\mathfrak{b}^{k-1}\mathfrak{a} \subset (\beta)$. Definiere nun $\mathfrak{c} = \frac{1}{\beta}\mathfrak{b}^{k-1}\mathfrak{a}$. $\mathfrak{c} \subset D$ ist Ideal und erfüllt: $\mathfrak{bc} = \mathfrak{a}$.

□

Man sieht, dass sich Inklusionen von Idealen in $D$ ähnlich verhalten wie die Teilbarkeit von ganzen Zahlen. Dabei haben die Oberideale in $D$ ähnliche Eigenschaften wie Teiler in $\mathbb{Z}$.
Der Ring $\mathbb{Z}$ besitzt auch obige Eigenschaft:

**Beispiel.** Für die Zahlen 2, 3 und 6 gilt: $2 \cdot 3 = 6$.
Betrachte nun die entsprechenden Ideale (2), (3) und (6) in $\mathbb{Z}$. Es gilt $(6) \subset (2)$, und das Ideal (3) erfüllt $(6) = (2)(3) = (2 \cdot 3)$.

In $\mathbb{Z}$ lässt sich die Primfaktorzerlegung von Elementen leicht auf Ideale verallgemeinern, da $\mathbb{Z}$ ein Hauptidealring ist. Auch für den Ring D ist dies möglich und wird im Folgenden gezeigt. Die Primelemente sind dabei genau die Primideale.

**Proposition. 12.2.8.** Jedes Ideal $\mathfrak{a} \subset D$ lässt sich als endliches Produkt von Primidealen schreiben.

**Beweis.** Ist $\mathfrak{a} = D$, so ist offenbar $D = \prod_{\mathfrak{p} \subset D \text{ prim}} \mathfrak{p}^0$.
Sei nun $\mathfrak{a} \subsetneq D$. Dieses Ideal ist nach dem Lemma von Zorn in einem maximalen Ideal enthalten. Nach Korollar 2 sind das genau die Primideale.
Wähle also ein Primideal $\mathfrak{p}_1$, sodass $\mathfrak{a} \subset \mathfrak{p}_1$. Nach vorangegangener Proposition gibt es ein Ideal $\mathfrak{a}_1$, sodass $\mathfrak{a} = \mathfrak{p}_1\mathfrak{a}_1$. Falls $\mathfrak{a}_1 = D$ ist, sind wir fertig.
Falls $\mathfrak{a}_1 \subsetneq D$, ist dieses Ideal in einem Primideal $\mathfrak{p}_2$ enthalten. Schreibe $\mathfrak{a}_1 \subset \mathfrak{p}_2$. Anschließend finden wir ein Ideal $\mathfrak{a}_2$, welches $\mathfrak{a}_1 = \mathfrak{p}_2\mathfrak{a}_2$ erfüllt, und damit gilt $\mathfrak{a} = \mathfrak{p}_1\mathfrak{a}_1 = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{a}_2$. Wir sind also fertig, falls $\mathfrak{a}_2 = D$ ist, und führen den obigen Prozess analog fort, falls $\mathfrak{a}_2 \subsetneq D$ ist.
Nach endlich vielen Schritten sind wir fertig, denn wir bilden die aufsteigende Idealkette $\mathfrak{a} \subset \mathfrak{a}_1 \subset \mathfrak{a}_2 \subset ...$ im noetherschen Ring $D$. Das bedeutet, ab einem Index $t$ gilt $\mathfrak{a}_i = D$ für alle $i \geq t$.
Die entsprechend gefundenen Primideale erfüllen dann $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2...\mathfrak{p}_t$.

$\square$

Wir haben bisher gesehen, dass man Ideale in $D$ als endliche Produkte von Primidealen schreiben kann. Das nächste Ziel wird es sein, zu beweisen, dass diese Zerlegung eindeutig ist. Zuvor brauchen wir aber noch einige Hilfsmittel.

Die absteigende Kette $\mathfrak{p} \supset \mathfrak{p}^2 \supset \mathfrak{p}^3 \supset ...$ von Primidealpotenzen ist eine Kette echter Teilmengen: $\mathfrak{p} \supsetneq \mathfrak{p}^2 \supsetneq \mathfrak{p}^3 \supsetneq ...$ . Das sieht man mit einer Widerspruchsannahme. Nehmen wir an, es gälte $\mathfrak{p}^i = \mathfrak{p}^{i+1}$ für ein gewisses $i \in \mathbb{N}$. Dann ist $D\mathfrak{p}^i = \mathfrak{p}\mathfrak{p}^i$, nach Proposition 12.2.6 also $D = \mathfrak{p}$, was ein Widerspruch zu $\mathfrak{p}$ prim ist.

**Definition.** Seien $\mathfrak{a}, \mathfrak{p} \subset D$ Ideale, $\mathfrak{p}$ prim. Wir definieren $ord_{\mathfrak{p}}(\mathfrak{a})$ als $t \geq 0$, sodass gilt: $\mathfrak{a} \subset \mathfrak{p}^t, \mathfrak{a} \not\subset \mathfrak{p}^{t+1}$.
Nach obiger Vorüberlegung ist dieses $t$ eindeutig.

**Proposition. 12.2.9** Seien $\mathfrak{a}, \mathfrak{b} \subset D$ Ideale, $\mathfrak{p}, \mathfrak{p}_0 \subset D$ Primideale. Es gelten:
(a) $ord_{\mathfrak{p}}(\mathfrak{p}) = 1$.
(b) $ord_{\mathfrak{p}}(\mathfrak{p}_0) = 0$, falls $\mathfrak{p} \neq \mathfrak{p}_0$.
(c) $ord_{\mathfrak{p}}(\mathfrak{a}\mathfrak{b}) = ord_{\mathfrak{p}}(\mathfrak{a}) + ord_{\mathfrak{p}}(\mathfrak{b})$.

**Beweis.** (a) Trivial, da die absteigende Kette von Primidealpotenzen eine Kette echter Inklusionen ist.
(b) Seien $\mathfrak{p} \neq \mathfrak{p}_0$. Angenommen, $ord_{\mathfrak{p}}(\mathfrak{p}_0) = t > 0$. Das bedeutet $\mathfrak{p}_0 \subset \mathfrak{p}^t \subset \mathfrak{p}$. Da $\mathfrak{p}, \mathfrak{p}_0$ maximale Ideale sind, folgt $\mathfrak{p} = \mathfrak{p}_0$, ein Widerspruch zur Annahme.
(c) Seien $t = ord_{\mathfrak{p}}(a)$ und $s = ord_{\mathfrak{p}}(b)$. Das bedeutet $\mathfrak{a} \subset \mathfrak{p}^t, \mathfrak{a} \not\subset \mathfrak{p}^{t+1}, \mathfrak{b} \subset \mathfrak{p}^s, \mathfrak{b} \not\subset \mathfrak{p}^{s+1}$.
Nach Proposition 12.2.7 gibt es Ideale $\mathfrak{a}_0, \mathfrak{b}_0 \subset D$, welche $\mathfrak{a} = \mathfrak{p}^t\mathfrak{a}_0, \mathfrak{b} = \mathfrak{p}^s\mathfrak{b}_0$ erfüllen. Dabei sind $\mathfrak{a}_0 \not\subset \mathfrak{p}$ und $\mathfrak{b}_0 \not\subset \mathfrak{p}$: Wäre $\mathfrak{a}_0 \subset \mathfrak{p}$, so würde daraus folgen $\mathfrak{a} = \mathfrak{p}^t\mathfrak{a}_0 \subset \mathfrak{p}^{t+1}$, ein Widerspruch zu $ord_{\mathfrak{p}}(\mathfrak{a}) = t$. Analog sieht man $\mathfrak{b}_0 \not\subset \mathfrak{p}$.
Man sieht leicht: $\mathfrak{a}\mathfrak{b} = \mathfrak{p}^{t+s}\mathfrak{a}_0\mathfrak{b}_0 \subset \mathfrak{p}^{t+s}$. Es ist noch zu zeigen: $\mathfrak{a}\mathfrak{b} \not\subset \mathfrak{p}^{t+s+1}$.
Nehmen wir an, es würde doch $\mathfrak{a}\mathfrak{b} \subset \mathfrak{p}^{t+s+1}$ gelten. Dann gibt es ein Ideal $\mathfrak{c} \subset D$, welches $\mathfrak{a}\mathfrak{b} = \mathfrak{p}^{t+s+1}\mathfrak{c}$ erfüllt. Dann folgt aus $\mathfrak{p}^{t+s}\mathfrak{a}_0\mathfrak{b}_0 = \mathfrak{a}\mathfrak{b} = \mathfrak{p}^{t+s+1}\mathfrak{c}$ mit Proposition 12.2.6 $\mathfrak{a}_0\mathfrak{b}_0 = \mathfrak{p}\mathfrak{c} \subset \mathfrak{p}$. Da $\mathfrak{p}$ ein Primideal ist, muss bereits $\mathfrak{a}_0 \subset \mathfrak{p}$ oder $\mathfrak{b}_0 \subset \mathfrak{p}$. Das haben wir aber oben ausgeschlossen. Damit haben wir gezeigt: $\mathfrak{a}\mathfrak{b} \not\subset \mathfrak{p}^{t+s+1}$.

$\square$

Schließlich sind wir in der Lage, die Eindeutigkeit der Zerlegung eines Ideals in Primideale zu beweisen:

**Theorem. 2.** Sei $\mathfrak{a} \subset D$ Ideal. Sei $\mathfrak{a} = \prod_{\mathfrak{p} \subset D \text{ prim}} \mathfrak{p}^{e(\mathfrak{p})}$ eine Zerlegung in Primideale. Dann sind alle bis auf endlich viele Exponenten 0 und die Exponenten sind eindeutig festgelegt durch $e(\mathfrak{p}) = ord_{\mathfrak{p}}(\mathfrak{a})$.

**Beweis.** Dass so eine Zerlegung existiert, sowie dass alle bis auf endlich viele Exponenten 0 sein müssen, sahen wir bereits im Beweis von Proposition 12.2.8.
Wir zeigen jetzt: $e(\mathfrak{p}) = ord_{\mathfrak{p}}(\mathfrak{a})$.
Sei $\mathfrak{p}_0 \subset D$ ein Primideal. Wir wenden $ord_{\mathfrak{p}_0}$ auf beide Seiten der Gleichung $\mathfrak{a} = \prod_{\mathfrak{p} \subset D \text{ prim}} \mathfrak{p}^{e(\mathfrak{p})}$ an. Dabei benutzen wir zum Vereinfachen der Ausdrücke die letzte Proposition:
$ord_{\mathfrak{p}_0}(\mathfrak{a}) = ord_{\mathfrak{p}_0}(\prod_{\mathfrak{p} \subset D \text{ prim}} \mathfrak{p}^{e(\mathfrak{p})}) = \sum_{\mathfrak{p} \subset D \text{ prim}} ord_{\mathfrak{p}_0}(\mathfrak{p}^{e(\mathfrak{p})})$
$= \sum_{\mathfrak{p} \subset D \text{ prim}} e(\mathfrak{p}) ord_{\mathfrak{p}_0}(\mathfrak{p}) = e(\mathfrak{p}_0)$

□