Algebraische Zahlentheorie
Algebra B4

Salma Kuhlmann

SS 2017

Inhaltsverzeichnis zur Vorlesung: Algebraische Zahlentheorie

Prof. Dr. Salma Kuhlmann, Simon Müller, Michele Serra

Sommersemester 2017

Algebraische Zahlentheorie
Algebra B 4 - Sommersemester 2017
Prof'in Dr. Salma Kuhlmann

1.Vorlesung

24. April 2017

Kapitel 1: Quadratische Zahlkörper

1. Der Ring der ganzen algebraischen Zahlen $\mathbb{Z}[\omega]$
2. Die Einheitsgruppe $\mathbb{Z}[\omega]^\times$

Definition 1.1 i) Ein Zahlkörper ist eine endliche Erweiterung K von $\mathbb{Q}$.

ii) $[K : \mathbb{Q}]$ heißt der Grad des Zahlkörpers.

iii) eine algebraische Zahl ist ein Element $\alpha \in K$.

iv) $\alpha \in K$ ist eine ganze (algebraische) Zahl, wenn es ein Polynom $m(x) \in \mathbb{Z}[x]$ gibt mit $m(x)$ normiert und $m(\alpha) = 0$.

Algebraische Zahlentheorie studiert die Arithmetik von Zahlkörpern, den Ring $\mathcal{O}_K := \{\alpha \in K \mid \alpha \text{ ganz }\}$, seine Ideale, Einheiten und Faktorisierung.

Sei K ein Zahlkörper.

Proposition 1.1
$\alpha \in K$ ist ganz $\iff$ $\mathrm{MinPol}_{\mathbb{Q}}(\alpha) \in \mathbb{Z}[x]$.
Insbesondere: $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$

Beweis. „$\Leftarrow$“: klar
Sei $\alpha \in \mathcal{O}_K$ und $f(x)$ normiert von minimalem Grad in $\mathbb{Z}[x]$, so dass α eine Nullstelle von $f(x)$ ist. Wenn $f(x)$ reduzibel in $\mathbb{Q}[x]$ ist, liefert dann das Lemma von Gauss, dass $f(x)$ reduzibel in $\mathbb{Z}[x]$ ist, also $f(x) = g(x)h(x)$ mit $g, h \in \mathbb{Z}[x]$ normiert, $\deg(g), \deg(h) < \deg(f)$ und $g(\alpha) = 0$ oder $h(\alpha) = 0$: Widerspruch. Also ist $f(x)$ irreduzibel in $\mathbb{Q}[x]$. Die Eindeutigkeit von $\mathrm{MinPol}_{\mathbb{Q}}(\alpha)$ ergibt nun $f(x) = \mathrm{MinPol}_{\mathbb{Q}}(\alpha) \in \mathbb{Z}[x]$.
Sei $\alpha = \frac{r}{s} \in \mathbb{Q}$, dann ist $\mathrm{MinPol}_{\mathbb{Q}}(\alpha) = x - \frac{r}{s}$, $r, s \in \mathbb{Z}$, $ggT(r, s) = 1$. Nun ist
$x - \frac{r}{s} \in \mathbb{Z}[x] \Leftrightarrow s = 1 \Leftrightarrow \alpha \in \mathbb{Z}$. □

Wir sehen also: $K = \mathbb{Q} \Rightarrow \mathcal{O}_K = \mathbb{Z}$. Wie berechnet man $\mathcal{O}_K$ im Allgemeinen?

Beispiel 1.1 (Quadratische Zahlkörper)
Zahlkörper vom Grad 2: Betrachte i.A.: Sei F ein Körper, $\mathrm{Char}(F) \neq 2$, K/F eine Körpererweiterung mit $[K:F] = 2$. Sei $\alpha \in K \backslash F$. Dann ist $\mathrm{MinPol}_F(\alpha) = x^2 + bx + c$, $b, c \in F$, also $K = F(\alpha)$ weil $[K:F] = 2$. Die Nullstellen sind $\frac{1}{2}(-b \pm \sqrt{b^2 - 4c})$ ($\mathrm{Char}(F) \neq 2$). Setze $D := b^2 - 4c \in F$. Dann gilt $K = F(\sqrt{D})$ und $D \in F$ ist kein Quadrat.

Definition 1.2
$D \in \mathbb{Z}$ ist quadratfrei, falls D ein Produkt von verschiedenen Primzahlen ist.

Zusatz: wenn $F = \mathbb{Q}$ gilt, kann man o.E. $D \in \mathbb{Z}$ mit D quadratfrei wählen

Beweis. Sei $D = \frac{\prod p_i^{\nu_i}}{\prod p_i^{\mu_i}} = \prod p_i^{\epsilon_i} \in \mathbb{Q}$, $\epsilon_i \in \mathbb{Z}$, $p_i \in \mathbb{Z}$ Primzahlen, $p_i \neq p_j$ wenn $i \neq j$.

Behauptung: O.E. gilt $\epsilon_i = 1$:

Weil $\epsilon_i = 2\rho_i$ oder $\epsilon_i = 2\rho_i + 1$, $p_i \in \mathbb{Z}$, also

$$D = \prod_{i \in I} p_i^{2\rho_i} \prod_{j \in J} p_j^{2\rho_j + 1} \Rightarrow D = \prod_{i \in I} p_i^{2\rho_i} \prod_{j \in J} p_j^{2\rho_j} \underbrace{\prod_{j \in J} p_j}_{:= D' \text{ ist quadratfrei}}$$

Damit ist aber $\sqrt{D} = \underbrace{\prod p_i^{\rho_i} \prod p_j^{\rho_j}}_{\in \mathbb{Q}} \sqrt{D'}$ und $K = \mathbb{Q}(\sqrt{D'})$. □

Setze also $K := \mathbb{Q}(\sqrt{D})$ mit D quadratfrei.

Proposition 1.2
Die Menge $\mathcal{O}_K$ der ganzen (algebraischen) Zahlen ist ein Ring und zwar

$$\mathcal{O}_K = \mathbb{Z}[\omega] := \{r + s\omega \mid, r, s \in \mathbb{Z}\}$$
$$\text{wobei } \omega := \begin{cases} \sqrt{D} \text{ wenn } D \equiv 2, 3 \bmod 4 \\ \frac{1+\sqrt{D}}{2} \text{ wenn } D \equiv 1 \bmod 4 \end{cases}$$

Beweis. NB: $D \equiv 0 \bmod 4$ ist nicht möglich.
Beobachte: $\mathbb{Z}[\omega]$ ist ein Ring; abgeschlossen unter Addition ist klar, und unter Multiplikation wenn $\omega = \sqrt{D}$ ist auch klar! Für $\omega = \frac{1+\sqrt{D}}{2}$ berechne
$(r + s\frac{1+\sqrt{D}}{2})(t + u\frac{1+\sqrt{D}}{2}) = \underbrace{(rt + su\frac{D-1}{4})}_{\in \mathbb{Z} \text{ weil } D \equiv 1 \bmod 4} + \underbrace{(ru + st + su)}_{\in \mathbb{Z}} \frac{1+\sqrt{D}}{2} \in \mathbb{Z}[\omega]$.
Nun zeigen wir $\mathbb{Z}[\omega] \subseteq \mathcal{O}_K$. Beobachte, dass:
Für $\alpha \in K, \alpha \notin \mathbb{Q}$, $\alpha = a + b\sqrt{D}$, $a, b \in \mathbb{Q}$, ist $\mathrm{MinPol}_{\mathbb{Q}}(\alpha) = x^2 - 2ax + (a^2 - b^2 D)$.
Nun sei $\alpha = r + s\omega \in \mathbb{Z}[\omega]$, $r, s \in \mathbb{Z}$, o.E. $s \neq 0$. Proposition 1.1 impliziert: Es genügt zu zeigen, dass $\mathrm{MinPol}_{\mathbb{Q}}(\alpha) \in \mathbb{Z}[x]$.

Fall 1: $D \equiv 2, 3 \bmod 4$
$\alpha = r + s\sqrt{D}$, $r, s \in \mathbb{Z}$, also $\mathrm{MinPol}_{\mathbb{Q}}(\alpha) = \underbrace{x^2 - 2rx + (r^2 - s^2 D)}_{\in \mathbb{Z}[x]}$.

Fall 2: $D \equiv 1 \bmod 4$
$\alpha = r + s\frac{1+\sqrt{D}}{2} = \underbrace{(r + \frac{s}{2})}_{:=a} + \underbrace{(\frac{s}{2})}_{:=b} \sqrt{D}$, $a, b \in \mathbb{Q}$.

Also ist $\mathrm{MinPol}_{\mathbb{Q}}(\alpha) = x^2 - 2(r+\frac{s}{2})x + ((r+\frac{s}{2})^2 - (\frac{s}{2})^2 D) = x^2 - 2\underbrace{(r+\frac{s}{2})}_{\in\mathbb{Z}}x + \underbrace{(r^2+rs+s^2\frac{1-D}{4})}_{\in\mathbb{Z}}$.

Nun zeigen wir $\mathcal{O}_K \subseteq \mathbb{Z}[\omega]$. Sei $\alpha = a + b\sqrt{D} \in \mathcal{O}_K$, $a, b \in \mathbb{Q}$. Falls $b = 0$, dann ist $\alpha \in \mathbb{Q}$ und Proposition 1.1 impliziert $\alpha \in \mathbb{Z}$, also $\alpha \in \mathbb{Z}[\omega]$. Also gilt o.E. $b \neq 0$ ($\alpha \notin \mathbb{Q}$). Betrachte $\mathrm{MinPol}_{\mathbb{Q}}(\alpha) = x^2 - 2ax + (a^2 - b^2 D)$.
Proposition 1.1 impliziert $2a \in \mathbb{Z}$ und $a^2 - b^2 D \in \mathbb{Z}$. Dann ist $4b^2 D \in \mathbb{Z}$, weil
$\underbrace{4(a^2 - b^2 D)}_{\in\mathbb{Z}} = \underbrace{(2a)^2}_{\in\mathbb{Z}} - (2b)^2 D$. Nun ist aber D quadratfrei, also $2b \in \mathbb{Z}$. Setze also $a := \frac{x}{2}$ und $b = \frac{y}{2}$, $x, y \in \mathbb{Z}$, also $x^2 - y^2 D = 4(a^2 - b^2)D$ und damit erhalten wir $x^2 - y^2 D \equiv 0 \bmod 4$, also

$$(*) \qquad y^2 D \equiv x^2 \bmod 4$$

D.h.: $y^2 D$ ist ein Quadrat mod 4.
Fortsetzung des Beweises in der 2.Vorlesung. □

Algebraische Zahlentheorie
Algebra B 4 - Sommersemester 2017
Prof'in Dr. Salma Kuhlmann

2.Vorlesung

27. April 2017

Beweis Fortsetzung. Die Quadrate mod 4 sind 0 und 1, also gilt entweder

$$(1) \quad y^2 D \equiv 0 \bmod 4$$
$$\text{oder } (2) \quad y^2 D \equiv 1 \bmod 4$$

Fall (1): $y^2 D \equiv 0 \bmod 4$ impliziert:

- entweder $y^2 \equiv 0 \bmod 4$; dann ist $x^2 \equiv 0 \bmod 4$ wegen $(*)$, also $x, y \equiv 0 \bmod 2$
- oder $y^2 \equiv D \equiv 2 \bmod 4$: unmöglich, weil 2 kein Quadrat mod 4 ist.

Fall (2): $y^2 D \equiv 1 \bmod 4 (**)$:

y^2, D sind in $\mathbb{Z}_4^\times$, also entweder 1 oder 3, also gilt:

- entweder $y^2 \equiv D \equiv 1 \bmod 4$ also $y \equiv 1 \bmod 2$, also mit $(*) + (**)$: $x \equiv 1 \bmod 2$
- oder $y^2 \equiv D \equiv 3 \bmod 4$: unmöglich, weil 3 kein Quadrat mod 4 ist.

Wir haben also gezeigt: die folgenden Fälle sind möglich:

(i) $D \equiv 2, 3 \bmod 4$ und x, y beide gerade

oder

(ii) $D \equiv 1 \bmod 4$ und x, y beide ungerade oder beide gerade.

Im Fall (i): $a = \frac{x}{2}, b = \frac{y}{2} \in \mathbb{Z}$ und damit $\alpha \in \mathbb{Z}[\omega]$, $\omega = \sqrt{D}$.
Im Fall (ii): $\alpha = a + b\sqrt{D} = r + s\omega$ mit $r := \frac{x-y}{2} \in \mathbb{Z}$ und $s := y \in \mathbb{Z}$ und $\omega = \frac{1+\sqrt{D}}{2}$. □

§Faktorisierung in $\mathcal{O}_K$?

$\mathbb{Z} = \mathcal{O}_\mathbb{Q}$ ist faktoriell (fundamentaler Satz der Arithmetik), aber im Allgemeinen ist $\mathcal{O}_K$ nicht faktoriell, z.B. (ÜA) ist $3 \in \mathbb{Z}[\sqrt{-5}]$ irreduzibel aber nicht prim. Andererseits haben wir gezeigt (siehe BIII), dass in einem faktoriellen Ring Primelemente=Irreduzibele. Wir werden zeigen, dass $\mathcal{O}_K$ noethersch ist (siehe ÜB) und damit gilt die Existenz der Faktorisierung in irreduzibele Elemente. Was fehlt also i.A ist die Eindeutigkeit (siehe ÜB). Betrachte wieder:

Beispiel 2.1
In $\mathbb{Z}[\sqrt{-5}]$ gilt

$$(\dagger) \qquad 6 = 2.3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

$2, 3, 1 + \sqrt{-5}$ und $1 - \sqrt{-5}$ sind alle irreduzibel und nicht assoziiert (siehe ÜB).
Die Idee von Kummer und Dedekind ist stattdessen eine Faktorisierung von Idealen zu verlangen: Faktorisierung vom Hauptideal $< 6 >$ ist:

$$(\ddagger) \qquad < 6 >=< 2, 1 + \sqrt{-5} >< 2, 1 - \sqrt{-5} >< 3, 1 + \sqrt{-5} >< 3, 1 - \sqrt{-5} >$$

Erinnerung: I, J Ideale, $IJ := \{ \underbrace{\sum_i a_i b_i}_{\text{endliche Summe}} \mid a_i \in I, b_i \in J\}$, z.B.:
$I =< a >$ und $J =< b > \Rightarrow IJ =< ab >$

Wir beweisen (‡). Wir behaupten:

Behauptung 1: $< 2, 1 + \sqrt{-5} >< 2, 1 - \sqrt{-5} >=< 2 >$
und $< 3, 1 + \sqrt{-5} >< 3, 1 - \sqrt{-5} >=< 3 >$

(und damit erhalten wir durch (†):
$< 2, 1 + \sqrt{-5} >< 2, 1 - \sqrt{-5} >< 3, 1 + \sqrt{-5} >< 3, 1 - \sqrt{-5} >=< 2 >< 3 >=< 6 >$.)

Bemerkung 2.1
Man könnte zeigen:

Behauptung 2: $< 2, 1 + \sqrt{-5} >< 3, 1 + \sqrt{-5} >=< 1 + \sqrt{-5} >$
und $< 2, 1 - \sqrt{-5} >< 3, 1 - \sqrt{-5} >=< 1 - \sqrt{-5} >$

und die andere Faktorisierung von 6 ausnutzen (siehe ÜB).

Beweis von Behauptung 1: Wir berechnen
$< 2, 1 + \sqrt{-5} >< 2, 1 - \sqrt{-5} >=< 4, 2 + 2\sqrt{-5}, 2 - 2\sqrt{-5}, 6 >$, wir sehen, dass alle Erzeuger hier gerade sind, also gilt $< 2, 1 + \sqrt{-5} >< 2, 1 - \sqrt{-5} >\subseteq< 2 >$. Umgekehrt:
$2 = 6 - 4 \in< 4, 2 + 2\sqrt{-5}, 2 - 2\sqrt{-5}, 6 >$ und damit ist $< 2 >\subseteq< 2, 1 + \sqrt{-5} >< 2, 1 - \sqrt{-5} >$.
□

Behauptung 3: Alle vier Ideale sind Primideale (siehe ÜB). Z.B ist die Abbildung

$$\begin{array}{rccc} \phi: & \mathbb{Z} & \to & \mathbb{Z}[\sqrt{-5}]/ < 3, 1 - \sqrt{-5} > \\ & z & \mapsto & z + < 3, 1 - \sqrt{-5} > \end{array}$$

ein surjektiver Homomorphismus mit $ker(\phi) =< 3 >$, also ist
$\mathbb{Z}[\sqrt{-5}]/ < 3, 1 - \sqrt{-5} > \cong \mathbb{Z}/ < 3 >$ ein Körper.

Algebraische Zahlentheorie
Algebra B 4 - Sommersemester 2017
Prof'in Dr. Salma Kuhlmann

3.Vorlesung

4. Mai 2017

§Einheiten

Wir berechnen nun explizit die Einheiten in $\mathbb{Z}[\omega]$.

(1) Norm auf $\mathbb{Q}(\sqrt{D})$:
$N : \mathbb{Q}(\sqrt{D}) \to \mathbb{Q}$

$$\begin{aligned} N(a+b\sqrt{D}) &= (a+b\sqrt{D})\overline{(a+b\sqrt{D})} \\ &= (a+b\sqrt{D})(a-b\sqrt{D}) \\ &= a^2 - b^2 D \end{aligned}$$

(2) (i) $D \equiv 2,3 \bmod 4, \omega = \sqrt{D}$
$N(r+s\sqrt{D}) = r^2 - s^2 D \in \mathbb{Z}$, $r, s \in \mathbb{Z}$.

(ii) $D \equiv 1 \bmod 4$, $\omega = \frac{1+\sqrt{D}}{2}$, $\alpha \in \mathbb{Z}[\omega]$, $\alpha = r + s\frac{1+\sqrt{2}}{2}$, $r, s \in \mathbb{Z}$.
Berechne:$N(\alpha) = (r+\frac{s}{2})^2 - D(\frac{s}{2})^2$, also $N(\alpha) = r^2 + rs + \frac{1-D}{4}s^2 \in \mathbb{Z}$.
Damit ist bewiesen: $N(\alpha) \in \mathbb{Z}$ für $\alpha \in \mathbb{Z}[\omega]$

(3) $N : \mathbb{Z}[\omega] \to \mathbb{Z}$ ist durch $N(\alpha) = N(r+s\omega) = (r+s\omega)\overline{(r+s\omega)} = (r+s\omega)(r+s\overline{\omega})$ gegeben, wobei $r, s \in \mathbb{Z}$ und

$$\overline{\omega} = \begin{cases} -\sqrt{D} \text{ falls } D \equiv 2,3 \bmod 4 \\ \frac{1-\sqrt{D}}{2} \text{ falls } D \equiv 1 \bmod 4 \end{cases}$$

Behauptung: $r + s\overline{\omega} \in \mathbb{Z}[\omega]$ (prüfe es!)

(4) Die Norm ist mulktiplikativ (prüfe es)

(5) **Behauptung:** $\alpha \in \mathbb{Z}[\omega]^\times \Leftrightarrow N(\alpha) = \pm 1$

Beweis. „⇒“$\alpha \in \mathbb{Z}[\omega]^\times \Rightarrow \exists \beta \in \mathbb{Z}[\omega]$ mit $\alpha\beta = 1$, also ist $N(\alpha\beta) = N(\alpha)N(\beta) = 1$ also $N(\alpha) \in \mathbb{Z}^\times \Rightarrow N(\alpha) = \pm 1$.

„⇐“ Sei $N(r+s\omega) = \pm 1$, $r, s \in \mathbb{Z}$, also ist $(r+s\omega)\underbrace{\overline{(r+s\omega)}}_{\in \mathbb{Z}[\omega]} = \pm 1$ also ist $r+s\omega$ invertierbar in $\mathbb{Z}[\omega]$ mit Inverse $\pm\overline{(r+s\omega)}$. □

Bemerkung 3.1
Betrachte die Diophantine'sche Gleichung $x^2 - Dy^2 = \pm 1$ (die Pell'sche Gleichung). Wir haben gezeigt: $x, y \in \mathbb{Z}$ ist eine Lösung$\Leftrightarrow x + y\omega \in \mathbb{Z}[\omega]^\times$

Kapitel 2: Moduln

1. Moduln
2. Moduln über HIR
3. Noether'sche Moduln

§Moduln

R ist stets ein kommutativer Ring mit Eins.

Definition 3.1 (i) Ein R-Modul ist eine abelsche Gruppe $(M,+)$ versehen mit einer Verknüpfung (Skalarmultiplikation):

$$\begin{array}{ccc} R \times M & \to & M \\ (r,x) & \mapsto & rx \end{array},$$

so dass für alle $x, y \in M$ und $r, s \in R$ Folgendes gilt:

(1) $1.x = x$

(2) $r(sx) = (rs)x$

(3) $(r+s)x = rx + sx$

(4) $r(x+y) = rx + ry$

(ii) Eine Untergruppe $N \leq M$ ist ein Untermodul, wenn $RN \subseteq N$.

Beispiel 3.1 (i) $R = K$ Körper.

K-Modul=K-Vektorraum.

Untermodul=Unterraum.

(ii) $R = \mathbb{Z}$.

$\mathbb{Z}$-Modul=abelsche Gruppe.

Untermodul=Untergruppe.

(iii) $M = \{0\}$ trivialer Modul.

(iv) $M = R$ ist ein R-Modul.

Untermodul=Ideal von R.

Definition 3.2
Seien M, N zwei R-Moduln.

(i) Ein R-Moduln Homomorphismus ist ein Gruppenhomomorphismus $\phi : M \to N$, so dass $\phi(rx) = r\phi(x)$ für alle $x \in M$ und $r \in R$.

(ii) Sei $N \leq M$ ein Untermodul. Die Faktorgruppe M/N ist ein R-Modul, wenn sie mit der folgenden Skalarmultiplikation versehen ist:

$$\begin{array}{rcl} R \times M/N & \to & M/N \\ (r, x+N) & \mapsto & rx+N \end{array}$$

(iii) Bezeichnung: $\mathrm{Hom}_R(M,N) := \{\phi : M \to N \mid \phi \text{ ist ein } R-\text{Modul Homomorphismus}\}$

Lemma 3.1
Seien M, N, V drei R-Moduln.

(i) $\phi \in \mathrm{Hom}_R(M,N) \wedge \psi \in \mathrm{Hom}_R(N,V) \Rightarrow \psi \circ \phi \in \mathrm{Hom}_R(M,V)$.

(ii) $\phi \in \mathrm{Hom}_R(M,N) \Rightarrow \ker(\phi) \leq M \wedge$ Im $(\phi) \leq N$.

(iii) $\phi \in \mathrm{Hom}_R(M,N)$ bijektiv $\Rightarrow \phi^{-1} \in \mathrm{Hom}_R(N,M)$, ϕ ist dann ein R-Modul Isomorphismus.

(iv) (Projektion) Sei $N \leq M$ ein Untermodul.

$$\begin{array}{rccl} \pi : & M & \to & M/N \\ & x & \mapsto & x+N \end{array}$$

ist ein R-Modul Homomorphismus.

(v) Wenn $N \leq M$, induziert π eine Bijektion zwischen den Untermoduln von M, die N enthalten, und den Untermoduln von M/N.

Beweis. Übungsaufgabe. □

Proposition 3.2 (Homomorphiesatz für Moduln)
Sei $\phi \in \mathrm{Hom}_R(M,N)$; es gilt $M/\ker(\phi) \cong$ Im (ϕ)

Beweis. Übungsaufgabe. □

Definition 3.3 (i) Die Summe einer Familie $(M_i)_{i \in I}$ von Untermoduln eines R-Moduls M ist

$$\sum_{i \in I} M_i = \{\sum_{i \in I} x_i \mid x_i \in M_i \text{ und } x_i = 0 \text{ für fast alle } i\}$$

Es ist $\sum_{i \in I} M_i \leq M$. (ÜA)

(ii) Für $a \in M$ sei $Ra := \{ra \mid r \in R\} \leq M$. (ÜA)

(iii) Sei $A \subseteq M$. Der von A erzeugte Untermodul von M ist

$$\sum_{a \in A} Ra$$

(iv) M ist endlich erzeugt, wenn es $A \subseteq M$ existiert mit A endlich und $M = \sum_{a \in A} Ra$.

Lemma 3.3
Für $A \subseteq M$ ist $\sum_{a \in A} Ra$ der kleinste Untermodul von M, der A enthält.

Beweis. ÜA. □

Definition 3.4 (i) Die direkte Summe einer Familie $(M_i)_{i\in I}$ von R-Moduln ist der R-Modul

$$\bigoplus_{i\in I} M_i := \{(x_i)_{i\in I} \in \prod_{i\in I} M_i \mid x_i = 0 \text{ für fast alle } i\}$$

mit $r(x_i)_{i\in I} = (rx_i)_{i\in I}$ für $r \in R$.

(ii) Ein R-Modul M ist direkte Summe einer Familie $(M_i)_{i\in I}$ von Untermoduln (in Zeichen $M = \bigoplus_{i\in I} M_i$) wenn der R-Modul Homomorphismus

$$\begin{array}{ccc} \bigoplus_{i\in I} M_i & \to & M \\ (x_i)_{i\in I} & \mapsto & \sum_{i\in I} x_i \end{array}$$

ein R-Moduln-Isomorphismus ist.

(iii) Sei M ein R-Modul und $N \leq M$ ein Untermodul. Existiert ein Untermodul $V \leq M$ mit $M = N \bigoplus V$, so heißt N direkter Summand von M und V ein Komplement zu N.

Algebraische Zahlentheorie
Algebra B 4 - Sommersemester 2017
Prof'in Dr. Salma Kuhlmann

4.Vorlesung

8. Mai 2017

Lemma 4.1
Sei M ein R-Modul, $N, V \leq M$ Untermoduln. Die folgenden Bedingungen sind äquivalent:

(1) $M = N \bigoplus V$

(2) $M = N + V$ und $N \cap V = \{0\}$

(3) Jedes $x \in M$ lässt sich eindeutig schreiben als $x = y + z$ mit $y \in N, z \in V$.

Beweis. ÜA. □

Beispiel 4.1
$G = \mathbb{Z}_4$, $H =< 2 >$ hat kein Komplement im $\mathbb{Z}$-Modul G, weil die einzigen Untermoduln von G $\{0\}, H$ und G sind.

Definition 4.1 (i) Sei $S \subseteq M$. Eine lineare Kombination aus S ist ein $x \in M$, so dass $x = \sum_i r_i x_i$ (endliche Summe) mit $r_i \in R, x_i \in S$.

(ii) $\text{Span}_R(S) := \{x \mid x \text{ lineare Kombination aus } S\} = \sum_{s \in S} Rs$

Lemma 4.2
Sei $N \leq M$. Es gilt:

(1) M endlich erzeugt$\Rightarrow$ M/N endlich erzeugt.

(2) N und M/N endlich erzeugt$\Rightarrow$ M endlich erzeugt.

Beweis. ÜA □

Definition 4.2
$S \subseteq M$ ist linear unabhängig, wenn

$$\underbrace{\sum_{i \ I} r_i x_i}_{\text{endliche Summe}} = 0 \Rightarrow \forall i, r_i = 0$$

für alle $r_i \in R$ uns $x_i \in S$.

Definition 4.3 (i) $x \in M$ ist Torsionselement$\Leftrightarrow \exists r \in R$ kein Nullteiler mit $rx = 0$.

(ii) $M_{\text{tor}} := \{x \in M \mid x \text{ Torsionselement}\}$ ist ein Untermodul (vgl ÜB) von M:
Der Torsionsmodul von M.

(iii) M ist torsionsfrei, wenn $M_{\text{tor}} = \{0\}$.

Bemerkung 4.1
$x \in M_{\text{tor}} \Rightarrow \{x\}$ ist nicht linear unbhängig.

Definition 4.4 (i) $S \subseteq M$ ist eine Basis$\Leftrightarrow$ S ist linear unabhängig und erzeugt M.

Konvention: $S = \varnothing$ ist linear unabhängig und $\text{Span}(\varnothing) = \{0\}$.

(ii) M ist frei, wenn er eine Basis hat.

Bemerkung 4.2 (i) S ist genau dann eine Basis von M, wenn jedes $x \in M$ eine eindeutige Darstellung als lineare Kombination aus S hat.

(ii) Jeder K-Vektorraum hat eine Basis und ist also frei als K-Modul. Betrachte aber:

Beispiel 4.2
$G := \mathbb{Z}_2 =< 1 >$ ist nicht frei als $\mathbb{Z}$-Modul, weil $1 \in G_{\text{tor}}$

Lemma 4.3
Sei R ein Integritätsbereich und $S \subseteq M$ torsionsfrei. Folgende Bedingungen sind äquivalent:

(1) M ist frei mit Basis S

(2) $M = \bigoplus_{x \in S} Rx$

Beweis. ÜA. □

Lemma 4.4
Sei $I \lhd R$, M ein R-Modul. Dann ist

(1) $IM := \{ \underset{\text{endliche Summe}}{\sum_j r_j y_j} \mid r_j \in I, y_j \in M\}$ ein Untermodul von M

(2) M/IM ein R/I-Modul.

Beweis.
$$\begin{array}{ccc} R/I \times M/IM & \to & M/IM \\ (\bar{r}, \bar{x}) & \mapsto & \overline{rx} \end{array}$$

□

Lemma 4.5
Sei M frei mit Basis $\{x_j\}_{j \in J}$ und $I \lhd R$. Dann ist M/IM frei als R/I-Modul mit Basis $\{\overline{x}_j\}_{j \in J}$

Beweis. $\{\overline{x}_j\}$ erzeugt M/IM (ÜA). Wir zeigen die lineare Unabhängigkeit über R/I.

$$\begin{aligned} \sum_j \bar{r}_j \bar{x}_j = 0 \Leftrightarrow \sum_j r_j x_j \in IM \\ \Leftrightarrow \sum_j r_j x_j = \sum_l t_l y_l \end{aligned}$$

für geeignete $t_l \in I, y_l \in M$. Nun $y_l = \sum_k r_{l,k} x_k$, also schreiben wir $\sum_l t_l y_l$ um und bekommen $\sum_j r_j x_j = \sum_k s_k x_k$ mit $s_k \in I$. Die Eindeutigkeit der Darstellung bezüglich einer Basis impliziert nun $r_j \in I$ für alle j, also $\overline{r}_j = 0$. □

Korollar 4.6
Sei M ein R-Modul und S eine Basis mit $|S| = n \in \mathbb{N}$. Dann haben alle anderen Basen Kardinalität n.

Beweis. OE ist R kein Körper (sonst ist $R = K$ und M ein K-Vektorraum und $\dim_K M = n$ ist eindeutig).
Sei $I \lhd R$ maximal. Sei $S = \{x_j\}$. Dann ist $\{\overline{x}_j\}$ eine R/I-Basis für den K-Vektorraum M/IM, wobei $K = R/I$.
Wenn $\{y_k\}$ eine beliebige Basis von M ist, dann ist ebenso $\{\overline{y}_k\}$ eine R/I-Basis für M/IM. □

Korollar 4.7
M endlich erzeugt und frei⇒ jede Basis ist endlich.

Beweis. Sei $\{x_j\}_j$ endlich und erzeugend. Dann ist $\{\overline{x}_j\}_j$ erzeugend für M/IM als R/I-Vektorraum (I maximales Ideal), also ist M/IM endlich dimensional und damit sind notwendigerweise alle Basen von M endlich. □

Bemerkung 4.3
Wir haben gezeigt: M frei mit $\{x_j\}_{j\in J}$ Basis, dann ist $|J|$ eindeutig definiert.

Definition 4.5
Sei M frei mit Basis $\{x_j\}_{j\in J}$. Wir definieren $\dim_R M := |J|$.

Bemerkung 4.4
Wir haben in Korollar 4.6 gezeigt:
$\dim_R M = \dim_K V$, wobei $K = R/I$ und $V = M/IM$, I ein maximales Ideal von R.

Algebraische Zahlentheorie
Algebra B 4 - Sommersemester 2017
Prof'in Dr. Salma Kuhlmann

5.Vorlesung

11. Mai 2017

Notation
$R^n := \{(r_1, \ldots, r_n) \mid r_i \in R\}$ freier R-Modul (mit Komponentenweise Addition und Skalarmultiplikation), Standard Basis: $\{e_i \mid i = 1, \ldots, n\}$.

Lemma 5.1
Sei M ein R-Modul. Es gilt:
M ist endlich erzeugt $\Leftrightarrow \exists n \in \mathbb{N}$ und $K \leq R^n$ mit $M \cong R^n/K$.

Beweis. „$\Leftarrow$“ Lemma 4.2.
„$\Rightarrow$“ Sei $\{x_1, \ldots, x_n\} \subseteq M$ erzeugend. Betrachte

$$\begin{array}{cccc} \phi & R^n & \to & M \\ & (r_1, \ldots, r_n) & \mapsto & \sum r_i x_i \end{array}$$

ϕ ist ein surjektiver Homomorphismus, $K := \ker(\phi)$. □

Bemerkung 5.1
Sei M wie im Lemma 5.1: $M \neq \{0\}$ endlich erzeugt, $\{x_1, \ldots, x_n\}$ erzeugend. Dann gilt:
M ist genau dann frei mit Basis $\{x_1, \ldots, x_n\}$, wenn $\ker(\phi) = \{0\}$.
(Inbesondere für $x \in M, x \neq 0$ ist der Hauptmodul Rx genau dann frei mit Basis $\{x\}$, wenn $\{r \in R \mid rx = 0\} = \{0\}$.)

Erinnerung: $M_{\text{tor}} = \{x \in M \mid \exists r$ kein Nullteiler $, rx = 0\}$.
M ist torsionsfrei, wenn $M_{\text{tor}} = \{0\}$.
M ist ein Torsionsmodul, wenn $M_{\text{tor}} = M$.

Lemma 5.2 (a) M_{tor} ist ein Torsionsmodul und

(b) M/M_{tor} ist torsionsfrei.

Beweis. (a) ÜA

(b) Sei $\bar{x} \in M/M_{\text{tor}}$, $\bar{x}$ Torsionselement. Es existiert $b \in R$ kein Nullteiler mit $b\bar{x} = 0$, d.h. $bx \in M_{\text{tor}}$, also gibt es $c \in R$ kein Nullteiler mit $cbx = 0 =$, also $x \in M_{\text{tor}}$ und $\bar{x} = 0$.
□

Bemerkung 5.2 (i) M frei $\Rightarrow M$ torsionsfrei.

Beweis. Sei $x \in M_{\text{tor}}$ und $\{x_i\}$ eine Basis von M. Schreibe $x = \sum r_i x_i$ und sei $r \in R$ nicht Nullteiler, so dass $rx = 0$. Es ist $\sum (rr_i)x_i = 0$. $\{x_i\}$ linear unabhängig$\Rightarrow rr_i = 0 \forall i \Rightarrow r_i = 0 \forall i \Rightarrow x = 0$ □

(ii) M torsionsfrei und $N \leq M \Rightarrow N$ torsionsfrei.

(iii) R Integritätsbereich$\Rightarrow M_{\text{tor}} = \{x \in M \mid \exists r \in R, r \neq 0, rx = 0\}$

(iv) R Integritätsbereich, $x \notin M_{\text{tor}} \Rightarrow Rx$ ist frei.

§Moduln über Hauptidealbereiche

Sei nun R stets ein Hauptidealbereich.

Satz 5.1
Sei F endlich erzeugt und frei, und $M \leq F$. Dann ist M frei und $\dim_R M \leq \dim_R F$. Insbesondere ist M endlich erzeugt.

Beweis. Sei $\{x_1, \ldots, x_n\}$ eine Basis für F. Setze $M_m = M \cap \text{ Span}_R\{x_1, \ldots x_m\}$ für $m \leq n$. Wir zeigen per Induktion, daß M_m frei ist mit $\dim_R M_m \leq m$ (und damit gilt es auch für $M = M_n$).
$M_1 = M \cap Rx_1$. $x_1 \notin M_{\text{tor}}$, also ist Rx_1 frei.

$$\begin{array}{rccc} \phi: & R & \xrightarrow{\sim} & Rx_1 \\ & r & \longmapsto & rx_1 \end{array}$$

$M_1 \leq Rx_1 \Rightarrow \phi^{-1}(M_1) \lhd R \Rightarrow \phi^{-1}(M_1) =< a_1 >$ für $a_1 \in R$ und $M_1 = \phi(< a_1 >) = R(a_1 x_1)$.
Also ist M_1 frei mit $\dim_R M_1 \leq 1$.
Per Induktion nehmen wir nun an: M_m ist frei, $\dim M_m \leq m$. Betrachte $\{a \in R \mid \exists x \in M, \text{ so dass } x = b_1 x_1 + \cdots + b_m x_m + a x_{m+1}\}$ ein Ideal in R (ÜA).
Sei $a_{m+1} \in R$ ein Erzeuger davon. Ist $a_{m+1} = 0$, so ist $M_{m+1} = M_m$ und unser Beweis ist fertig. Sonst gilt $a_{m+1} \neq 0$: Setze $w = a_{m+1} x_{m+1} + v \in M_{m+1}$ mit $v \in \text{ Span}\{x_1, \ldots, x_m\}$. Sei $x \in M_{m+1}$; es existieren $b_1, \ldots, b_m, a \in R$ mit $x = b_1 x_1 + \cdots + b_m x_m + a x_{m+1}$, also

$$\begin{aligned} x &= b_1 x_1 + \cdots + b_m x_m + (c a_{m+1}) x_{m+1} \\ &= (b_1 x_1 + \cdots + b_m x_m) + (cw - cv), \end{aligned}$$

also $x - cw = \sum b_i x_i - cv \in M_{m+1} \cap \text{ Span}\{x_1, \ldots, x_m\} = M_m$. Wir haben gezeigt:
$M_{m+1} = M_m + Rw$ mit $w \neq 0$, $w \notin M_{\text{tor}}$, Rw frei mit Basis $\{w\}$. Außerdem ist $M_m \cap Rw = \{0\}$, also $M_{m+1} = M_m \oplus Rw$ und damit direkte Summe von freien Moduln, also ist M_{m+1} frei und $\dim_R M_{m+1} = \dim_R M_m + \dim_R Rw \leq m + 1$.

□

Korollar 5.2
Sei M endlich erzeugt und $N \leq M$. Dann ist N endlich erzeugt.

Beweis. OE gilt $M = R^n/K$ (per Lemma 5.1). Betrachte

$$\begin{array}{rccc} \Pi: & R^n & \to & R^n/K \\ & y & \mapsto & \bar{y} \end{array}$$

Projektionshomomorphismus.
$N \leq R^n/K \Rightarrow \Pi^{-1}(N) \leq R^n$. Satz 5.1$\Rightarrow \Pi^{-1}(N)$ ist endlich erzeugt.
Lemma 4.2$\Rightarrow N = \Pi^{-1}(N)/K$ ist auch endlich erzeugt.

□

Satz 5.3
Sei M endlich erzeugt und torsionsfrei. Dann ist M frei.

Beweis. Sei $\{y_1 \ldots, y_m\} \subseteq M$ erzeugend und $\{v_1, \ldots, v_n\}$ darunter maximal linear unabhängig. Sei $y \in \{y_1, \ldots, y_m\}$. Nach Maximalität existieren $a, b_1, \ldots, b_n \in R$ nicht alle 0, so dass
$ay + b_1 v_1 + \cdots + b_n v_n = 0$ und $a \neq 0$ (weil $\{v_1, \ldots, v_n\}$ linear unabhängig). Wir sehen also:

$\forall j = 1, \ldots, m, \exists a_j \in R, a_j \neq 0 \wedge a_j y_j \in \text{ Span}\{v_1, \ldots, v_n\}$, also $(a_1 \ldots a_m)M \leq \underbrace{\text{Span}\{v_1, \ldots, v_n\}}_{\text{frei}}$,

also (Satz 5.1) ist $(a_1 \ldots a_m)M$ frei. Nun ist

$$\begin{array}{ccc} M & \xrightarrow{\sim} & (a_1 \ldots a_m)M \\ x & \longmapsto & (a_1 \ldots a_m)x \end{array}$$

eine Isomorphie, weil $a_1 \ldots a_m \neq 0$ und M torsionsfrei ist. Also ist M auch frei.

□

Satz 5.4
Ist M endlich erzeugt, so ist $M = M_{\text{tor}} \bigoplus F$, wobei $F \leq M$ ein freier Untermodul ist. Die Dimension $\dim_R F$ ist von der Wahl von F unabhängig.

Definition 5.1
$\dim_R F$ im Satz 5.4 ist der (freier) Rang von M.

Für den Beweis vom Satz 5.4 brauchen wir:

Lemma 5.5
Sei R kommutativ mit Eins, E und E' R-Moduln, E' frei. Sei $f : E \to E'$ ein surjektiver Homomorphismus. Dann existiert ein freier Untermodul $F \leq E$, so daß $f \restriction F : F \to E'$ eine Isomorphie ist und $E = F \bigoplus \ker(f)$.

Beweis. Sei $\{x'_i\}_{i \in I}$ eine Basis für E'. Für alle $i \in I$ wähle $x_i \in E$ mit $f(x_i) = x'_i$ und setze $F := \text{ Span}_R\{x_i \mid i \in I\}$. Es ist leicht zu sehen, daß $\{x_i\}_{i \in I}$ linear unabhängig ist (ÜA), also ist F frei. Sei nun $x \in E$ und nimm $a_i \in R$, so daß $f(x) = \sum a_i x'_i$. Es gilt $f(x - \sum a_i x_i) = 0$ und damit $x - \sum a_i x_i \in \ker(f)$. Wir haben gezeigt: $E = F + \ker(f)$. Nun ist es leicht zu sehen, daß $F \cap \ker(f) = \{0\}$ (ÜA). □

Algebraische Zahlentheorie
Algebra B 4 - Sommersemester 2017
Prof'in Dr. Salma Kuhlmann

6.Vorlesung

15. Mai 2017

Beweis vom Satz 5.4. Betrachte den Homomorphismus:

$$\begin{array}{rccc} \phi: & M & \to & M/M_{\text{tor}} \\ & x & \mapsto & \bar{x} \end{array}$$

Nun ist M/M_{tor} endlich erzeugt, also (Satz 5.3) ist er frei.
Lemma 5.5 liefert $F \leq M$, F frei mit $M = \ker(\phi) \bigoplus F$ und $\phi \restriction F : F \cong M/M_{\text{tor}}$, damit ist $\dim_R F = \dim_R M/M_{\text{tor}}$ eindeutig bestimmt. □

Wir werden nun M_{tor} weiter untersuchen; wir untersuchen also endlich erzeugte Torsionsmoduln.

Definition und Notation (a) Für $r \in R$ ist $M[r] := \{x \in M \mid rx = 0\}$ der r-Torsionsmodul.

(b) $M[r^\infty] := \bigcup_{k\in\mathbb{N}} M[r^k]$.

Bemerkung 6.1
$\{0\} \neq M = M_{\text{tor}}$ endlich erzeugter Torsionsmodul $\Rightarrow \exists a \in R, a \neq 0$ mit $aM = 0$ (Seien $v_1, \ldots, v_n$ Erzeuger, $a_1, \ldots, a_n \in R$ mit $a_i \neq 0$ und $a_i v_i = 0$; setze $a := a_1 \ldots a_n$).

Lemma 6.1
Sei M endliche erzeugter Torsionsmodul und wähle $0 \neq a \in R$ mit $aM = 0$ und $a = bc$ mit $ggT(b, c) = 1$. Es ist $M = M[b] \bigoplus M[c]$.

Beweis. Es existieren $x, y \in R$ mit $1 = xb + yc$. Sei $v \in M$; es ist $v = xbv + ycv$. Dann ist $xbv \in M[c]$ und $ycv \in M[b]$, also $M = M[b] + M[c]$. Sei $v \in M[b] \cap M[c]$; wir rechnen $v = (xb + yc)v = xbv + ycv = 0$. □

Satz 6.2
Sei $0 \neq M$ endlich erzeugter Torsionsmodul. Dann ist

$$M = \bigoplus_{p \text{ prim mit } M[p^\infty]\neq 0} M[p^\infty]$$

Bemerkung 6.2
M endlich erzeugt $\Rightarrow |\{p \in R \mid p \text{ prim und } M[p^\infty] \neq 0\}| < \infty$.

Beweis. Wähle $a \neq 0$ mit $aM = 0$, $a \in R$. Lemma 6.1 und Induktion anwenden ergibt

$$M = M[a] = \bigoplus_{p|a, p \text{ prim}, M[p^\infty]\neq 0} M[p^\infty]$$

□

Bemerkung 6.3
Die Darstellung hängt nicht von a ab; ist nämlich $M = M[b]$, q prim, $q \mid b$ aber $q \nmid a$, dann ist $ggT(a, q) = 1$ und damit $M = M[aq] = M[a] \bigoplus M[q] = M$, also $M[q] = 0$

Satz 6.3
Sei $0 \neq M$ endlich erzeugt; $p \in R$ prim mit $M[p^\infty] \neq 0$. Dann existiert eine eindeutige Folge $1 \leq \nu_1 \leq \cdots \leq \nu_s \in \mathbb{N}$, so daß $M[p^\infty] \cong R/ < p^{\nu_1} > \oplus \cdots \oplus R/ < p^{\nu_s} >$.

Korollar 6.4 (Struktursatz für endlich erzeugte Moduln über HIR)
Sei R ein HIR und M ein R-Modul. Ist M endlich erzeugt über R, so ist

$$M \cong R^d \bigoplus_{i=1}^{s} \bigoplus_{j=1}^{t_i} R/ < p_i^{\nu_{ij}} >$$

mit eindeutigen $d, s \in \mathbb{N}_0$, $p_1, \ldots, p_s$ paarweise verschiedene Primelemente, $t_s \in \mathbb{N}$ und $1 \leq \nu_{ij} \leq \cdots \leq \nu_{it_s} \in \mathbb{N}$.

□

Für den Beweis vom Satz 6.3 brauchen wir einiges (Terminologie, Bemerkung, Lemma).

Terminologie:

1. $y_1, \ldots, y_m \in M$ sind unabhängig wenn $\text{Span}\{y_1, \ldots, y_m\} \cong \bigoplus_{i=1}^m Ry_i$, oder die folgende äquivalente Bedingung gilt: $a_1y_1 + \cdots + a_my_m = 0 \Rightarrow a_iy_i = 0$ für $a_1, \ldots, a_m \in R$ $\forall i = 1, \ldots, m$.

   Bemerkung 6.4
   lineare Unabhängigkeit⇒ Unabhängigkeit immer; die Umkehrung gilt für Torsionsfreie Moduln.

2. Sei $x \in M$, $\begin{array}{rccc} \phi_x : & R & \to & Rx \\ & r & \mapsto & rx \end{array}$; es gelten $I_x := \ker(\phi_x)$ ist Hauptideal und $R/I_x \cong Rx$. Ein erzeuger für I_x heißt eine <u>Periode</u> für x.

Bemerkung 6.5 (i) Sei $0 \neq M = M[p^\nu]$ ein p^ν-Torsionsmodul. Sei $x \neq 0$, $x \in M$, dann ist eine Periode für x (bis auf Einheit) der Gestalt p^l mit $l \leq \nu$; in der Tat sei $l :=$ die kleinste natürliche Zahl, wofür es gilt $p^l x = 0$.

(ii) ist ν minimal dafür, daß $M = M[p^\nu]$, so gibt es $x \in M$ mit Periode genau p^ν.

(iii) Sei $x_1 \in M$ mit Periode p^ν; setze $\overline{M} := M/Rx_1$. Es ist $\overline{M} = \overline{M}[p^\nu]$ und für jeden Vertreter y von $\bar{y} \in \bar{M}$ mit Perioden p^l beziehungsweise $p^{\bar{l}}$ gilt $l \geq \bar{l}$.

(iv) Ist p^ν minimal dafür, daß $M = M[p^\nu]$ und p^μ minimal dafür, daß $\bar{M} = \bar{M}[p^\mu]$, dann gilt $\mu \leq \nu$.

Lemma 6.5
Sei $p \in R$ prim, $M = M[p^\nu]$, $\nu \geq 1$ und minimal dafür. Wähle $x_1 \in M$ mit Periode p^ν. Setze $\overline{M} := M/Rx_1$. Seien $\bar{y}_1, \ldots, \bar{y}_m \in \overline{M}$ unabhängig. Dann gibt es Vertreter $y_i \in \bar{y}_i$ mit Periode(y_i)=Periode($\bar{y}_i$) und so daß $x_1, y_1, \ldots, y_m$ unabhängig.

Beweis. Sei $\bar{y} \in \bar{M}$ mit Periode p^n, $1 \leq n$. Sei $y \in \bar{y}$ ein Verterter. Dann ist $p^n\bar{y} = 0$ oder $p^n y \in Rx_1$, also

$$(\dagger) \qquad p^n y = p^s c x_1$$

für $c \in R, p \nmid c, s \leq \nu$ (weil Primfaktorisierung in R vorhanden ist). Ist $s = \nu$, dann gilt $p^n y = p^\nu x_1 c = 0$, also y hat Periode $\leq p^n$ und damit genau $= p^n$, und so ist der Fall erledigt.
Is aber $s < \nu$, dann hat $p^s c x_1$ Periode $p^{\nu-s}$ und damit hat y Periode $p^{n+\nu-s}$, also muss
$n + \nu - s \leq \nu$ gelten (weil $p^\nu M = 0$), also $n \leq s$, wir sehen also, daß $y - p^{s-n}cx_1 \in \bar{y}$ (vgl (†)) und hat Periode p^n.
Fortsetzung vom Beweis folgt in der 7. Vorlesung. □

Algebraische Zahlentheorie
Algebra B 4 - Sommersemester 2017
Prof'in Dr. Salma Kuhlmann

7.Vorlesung

18. Mai 2017

Fortsetzung vom Beweis von Lemma 6.5. Sei nun y_i Vertreter von $\bar{y}_i$ mit gleicher Periode. Wir zeigen: $x_1, y_1, \ldots, y_m$ sind unabhängig. Seien $a, a_1, \ldots, a_m \in R$ mit

$$(\ddagger) \qquad ax_1 + a_1y_1 + \cdots + a_my_m = 0$$

Dann ist $a_1\bar{y}_1 + \cdots + a_m\bar{y}_m = 0$, also muss $a_i\bar{y}_i = 0 \quad \forall i$ sein.
Ist p^{r_i} die Periode von $\bar{y}_i$, dann gilt $p^{r_i} \mid a_i$; p^{r_i} ist aber Periode für y_i, also gilt $a_iy_i = 0$ für alle i und damit ist (zurück in $(\ddagger)$) auch $ax_1 = 0$.

□

Beweis vom Satz 6.3. $M[p^\infty]$ endlich erzeugt⇒ O.E. $M = M[p^\infty]$ und $\exists x_1 \in M$ mit Periode p^{ν_1}, $\nu_1 \in \mathbb{N}$ minimal so daß $M = M[p^{\nu_1}]$. Betrachte $M[p]$; da $M[p]$ p-torsion ist, ist eine Skalarmultiplikation

$$\begin{array}{ccc} R/ < p > \times M[p] & \to & M[p] \\ (a+ < p >, x) & \mapsto & ax \end{array}$$

wohldefiniert ($\bar{a}_1 = \bar{a} \Rightarrow (a - a_1) = pa_2 \Rightarrow (a_1 - a)x = a_2px = 0$). Also ist $M[p]$ ein $R/ < p >$-Vektorraum.
Analog ist $\overline{M}[p]$ ein $R/ < p >$-Vektorraum, wobei $\overline{M} := M/Rx_1$.

Behauptung: $\dim \overline{M}[p] < \dim M[p]$ als $R/ < p >$-Vektorräume.

Beweis. Seien $\bar{y}_1, \ldots \bar{y}_m$ linear unabhängig in $\overline{M}[p]$. Lemma 6.5 liefert $y_i \in \bar{y}_i$ mit Periode p, so daß $x_1, y_1, \ldots, y_m$ unabhängig. Setze $z_1 := p^{\nu_1 - 1}x_1$. Dann hat z_1 Periode p, $z_1 \in M[p]$ und $z_1, y_1, \ldots, y_m \in M[p]$ sind immernoch unabhängig. □

Wir zeigen nun die Existenzaussage im Satz. Wir argumentieren per Induktion nach $\dim_{R/<p>}$.
O.E. ist $\overline{M} \neq 0$ (sonst ist $M \cong Rx_1 \cong R/ < p^{\nu_1} >$). IA⇒ $\overline{M} = \overline{M}[p^\infty] \cong R\bar{x}_2 \oplus \cdots \oplus R\bar{x}_s$ und die Periode von $\bar{x}_i$ ist p^{ν_i} (d.h $R\bar{x}_i \cong R/ < p^{\nu_i} >$ für $i = 2, \ldots, 5$) mit $1 \leq \nu_1 \leq \nu_2 \leq \cdots \leq \nu_s$.
Lemma 6.5⇒ $\exists x_2, \ldots, x_s \in M$ so daß x_i Periode p^{ν_i} hat und $x_1, \ldots, x_s$ unabhängig, d.h
$M = M[p^\infty] \cong Rx_1 \oplus \cdots \oplus Rx_s \cong R/ < p^{\nu_1} > \oplus \cdots \oplus R/ < p^{\nu_s} >$ mit $1 \leq \nu_1 \leq \nu_2 \leq \cdots \leq \nu_s$, wie behauptet.
Wir zeigen nun die Eindeutigkeit.
Sei

$$(*) \qquad 0 \neq M = M[p^\infty] \cong R/ < p^{\mu_1} > \oplus \cdots \oplus R/ < p^{\mu_s} >$$

mit $\mu := \mu_s$ maximal und $\mu_1 \leq \cdots \leq \mu_s$, d.h $M = M[p^\mu] \supsetneq M[p^{\mu-1}]$. Beachte, daß
$M[p], M[p^2]/M[p], \ldots, M[p^\mu]/M[p^{\mu-1}]$ alle $R/ < p >$-Vektorräume sind. Aus $(*)$ folgt ausserdem, daß: $M[p] \cong < p^{\mu_1 - 1} > / < p^{\mu_1} > \oplus \cdots \oplus < p^{\mu_s - 1} > / < p^{\mu_s} >$
(weil $(R/ < p^m >)[p] = < p^{m-1} > / < p^m >$ und $(N \oplus K)[p] \cong N[p] \oplus K[p]$ (ÜA) und
$\dim_{R/<p>} < p^{\mu_i - 1} > / < p^{\mu_i} > = 1$. (weil $\begin{array}{ccc} R & \to & < p^{m-1} > / < p^m > \\ x & \mapsto & p^{m-1}x + < p^m > \end{array}$ ein surjektiver Homomorphismus mit Kernel $< p >$ ist.)

Also ist $\dim_{R/<p>} M[p] = s = \sharp\{i \mid \mu_i \geq 1\}$. Schreibe nun

$$(**) \qquad M[p^2] \cong \bigoplus_{\mu_i=1} R/ < p > \oplus \bigoplus_{\mu_i>1} < p^{\mu_i-2} > / < p^{\mu_i} >$$

Aus $(**)$ folgt:

$$M[p^2]/M[p] \cong \bigoplus_{\mu_i \geq 2} (< p^{\mu_i-2} > / < p^{\mu_i} >)/(< p^{\mu_i-1} > / < p^{\mu_i} >)$$

d.h

$$M[p^2]/M[p] \cong \bigoplus_{\mu_i \geq 2} < p^{\mu_i-2} > / < p^{\mu_i-1} >$$

(und $< p^{m-2} > / < p^{m-1} > \cong R/ < p >$), also ist $\dim_{R/<p>} M[p^2]/M[p] = \sharp\{i \mid \mu_i \geq 2\}$. Allgemeiner berechnen wir $\dim_{R/<p>} M[p^m]/M[p^{m-1}] = \sharp\{i \mid \mu_i \geq m\}$ für $m = 1, 2, \ldots, \mu$. Insbesondere:
$\dim_{R/<p>} M[p^\mu]/M[p^{\mu-1}] = \sharp\{i \mid \mu_i \geq \mu\} = \sharp\{i \mid \mu_i = \mu\}$ □

§Noethersche Moduln

Sei R ein Ring, M ein R-Modul.

Lemma 7.1
Folgende Aussagen sind äquivalent für M:

1. jeder $N \leq M$ ist endlich erzeugt
2. jede aufsteigende Kette $N_1 \leq N_2 \leq \ldots$ von Untermoduln wird stationär, d.h $\exists i$ mit $N_i = N_{i+1} = \ldots$
3. jede $\varnothing \neq \mathcal{U}$ Menge von Untermoduln von M besitzt ein inklusionsmaximales Element.

Beweis. siehe nächste Vorlesung. □

Definition 7.1
M ist noethersch, wenn eine der Bedingungen (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (3) erfüllt ist.

Algebraische Zahlentheorie
Algebra B 4 - Sommersemester 2017
Prof'in Dr. Salma Kuhlmann

8.Vorlesung

22. Mai 2017

Beweis von Lemma. (1) $\Rightarrow$ (2): Setze $N := \bigcup_i N_i$, $N \leq M$.
Seien $x_1, \ldots, x_r \in N$ mit $N := \text{Span}_R\{x_1, \ldots, x_r\}$ und $i \in \mathbb{N}$, so daß $\{x_1, \ldots, x_r\} \subseteq N_i$. Dann ist $N \subseteq N_i$ und damit $N_i = N = N_{i+1} = \ldots$.
(2) $\Rightarrow$ (3): Sei $N_1 \in \mathcal{U}$ nicht maximal. Dann gibt es $N_2 \in \mathcal{U}$ mit $N_1 \subsetneq N_2$. Wiederhole mit N_2: $N_1 \subsetneq N_2 \subsetneq N_3 \subsetneq \ldots$ usw. Diese Prozedur muß nach endlich vielen Schritten anhalten und damit ein maximales Element produzieren.
(3) $\Rightarrow$ (1): Sei $N \leq M$ und $\mathcal{U}$ die Menge aller seinen endlich erzeugten Untermoduln. Es gilt $\mathcal{U} \neq \varnothing$ weil $\{0\} \in \mathcal{U}$. Sei $N' = \text{Span}_R\{x_1, \ldots, x_r\}$ ein maximales Element von $\mathcal{U}$. Ist $N \supsetneq N'$, existiert dann $x \in N \backslash N'$ und $\text{Span}_R\{x_1, \ldots, x_r, x\} \supsetneq N'$: Widerpsruch. □

Definition 8.1
M ist noethersch, wenn eine der äquivalenten Bedingungen erfüllt ist. Ein Ring R ist noethersch heißt also: Jedes Ideal von R ist endlich erzeugt.

Lemma 8.1
Sei $N \leq M$.
M ist noethersch $\Leftrightarrow$ N ist noethersch und M/N ist noethersch.

Beweis. „$\Rightarrow$“ $N' \leq N \Rightarrow N' \leq M \Rightarrow N'$ endlich erzeugt. Also ist N noethersch.
Sei nun $A/N \leq M/N$, wobei $A \leq M$ und $N \leq A$. Also ist A endlich erzeugt und damit auch A/N.
„$\Leftarrow$“ Sei $A \leq M$.
Übungsaufgabe$\Rightarrow$ $A + N/N \cong A/A \cap N$.
Nun $A + N/N \leq M/N \Rightarrow A + N/N$ endlich erzeugt, d.h $A/A \cap N$ endlich erzeugt
und $A \cap N \leq N \Rightarrow A \cap N$ endlich erzeugt.
Lemma 4.2 impliziert nun, dass A endlich erzeugt ist.

□

Korollar 8.2
M_1, M_2 noethersch$\Rightarrow$ $M_1 \oplus M_2$ noethersch.

Beweis. $M_1 \oplus M_2/M_1 \cong M_2$ ist noethersch und M_1 ist noethersch. □

Korollar 8.3
Sei R noethersch und sei M ein endlich erzeugter R-Modul. Dann ist M noethersch.

Beweis. Lemma 5.1$\Rightarrow$ $M \cong R^n/K$.
Korollar 8.2$\Rightarrow$ $R^n = R \oplus \cdots \oplus R$ ist noethersch (Induktion).
Lemma 8.1$\Rightarrow$ M ist noethersch. □

Satz (Hilbert Basissatz)
Sei R noethersch, dann ist $R[x]$ noethersch.

Beweis. Sei $I \lhd R[x]$. Betrachte $J := \{a \in R \mid a \text{ ist Leitkoeffizient von } f \in I\}$.
Es ist ein Ideal von R (ÜA), also gibt es $f_1, \ldots, f_n \in I$, so daß die Leitkoeffizienten $a_1, \ldots, a_n$ von $f_1, \ldots, f_n$ das Ideal J erzeugen. Setze $d := \max_i \deg f_i$ und betrachte den endlich erzeugten R-Modul $M_d := \sum_{i=0}^{d-1} Rx^i$, d.h den R-Modul der Polynome vom Grad $< d$.
Korollar 8.3$\Rightarrow$ M_d ist noethersch, also ist $M_d \cap I \leq M_d$ endlich erzeugt.
Seien $g_1, \ldots, g_m \in I$ Erzeuger davon.

Behauptung: $I =< f_1, \ldots, f_n, g_1, \ldots, g_m >$

Beweis. $\supseteq$ ist klar.
Sei nun $f \in I$. Wenn $\deg f < d$, dann ist $f \in< g_1, \ldots, g_m >$. O.E. gilt also
$\deg(f) =: k + 1 \geq d$. Wir argumentieren per Induktion über k. Wir multiplizieren f_i mit einer geeigneten Potenz x^{l_i} und bekommen $f_i' \in I$ mit $\deg(f_i') = k + 1$. Sei $f' = \sum_{i=1}^{n} r_i f_i'$, so dass f' und f den gleichen Leitkoeffizient haben. Also ist $\deg(f - f') \leq k$ und per Induktionsannahme gilt $f - f' \in< f_1, \ldots, f_n, g_1, \ldots, g_m >$. Da aber $f' \in< f_1, \ldots, f_n, g_1, \ldots, g_m >$ ist, bekommen wir nun $f \in< f_1, \ldots, f_n, g_1, \ldots, g_m >$ □

□

Korollar 8.4
R noethersch$\Rightarrow$ $R[x_1, \ldots, x_n]$ noethersch.

Erinnerung: Sei $R \subseteq S$ eine Ringenerweiterung und $Y \subseteq S$ eine Untermenge. Dann ist $R[Y]$ unsere Notation für den kleinsten Unterring von S, der $R \bigcup Y$ enthält.
Wenn $Y = \{y_1, \ldots, y_n\}$ endlich ist, dann schreiben wir dafür $R[y_1, \ldots, y_n]$.
Der Evaluation-Homomorphismus

$$\begin{array}{cccc} ev_y & R[x_1, \ldots, x_n] & \to & R[y_1, \ldots, y_n] \\ & f(x_1, \ldots, x_n) & \mapsto & f(y_1, \ldots, y_n) \end{array}$$

ist surjektiv, also gilt $R[y_1, \ldots, y_n] \cong R[x_1, \ldots, x_n]/ker(ev_y)$ (ein Faktorring von Polynomring), d.h $R[y_1, \ldots, y_n]$ besteht aus Polynomen in $\{y_1, \ldots, y_n\}$.

Beispiel 8.1
Sei $R = K$ ein Körper, $S = L$ eine Körpererweiterung von K. Sei $\alpha \in L$ algebraisch über K. Dann hat $ev_\alpha : K[x] \to K[\alpha]$ einen nicht-tivialen Kern, $\ker(ev_\alpha) =< \text{MinPol}_K(\alpha) >$, also ist $K[\alpha] \cong K[x]/\ker(ev_\alpha)$ mit $\ker(ev_\alpha)$ maximales Ideal. Wir sehen also: $K[\alpha]$ ist bereits ein Körper, und damit gilt $K[\alpha] = K(\alpha)$.

Korollar 8.5
Sei R noethersch, $S = R[a_1, \ldots, a_n]$ eine Ringererweiterung. Dann ist S noethersch.

Beweis. $R[a_1, \ldots, a_n] \cong R[x_1, \ldots, x_n]/\ker(ev_{\bar{a}})$. Nun Korollar 8.4 und Lemma 8.1 anwenden. □

Kapitel 3: Ganzheit

Erinnerungen

Definition 8.1
Sei $R \subseteq S$ Ringererweiterung

a) $\alpha \in S$ ist ganz über $R \Leftrightarrow \exists f \in R[x]$ normiert mit $f(\alpha) = 0$.

b) $R \subseteq S$ ist eine ganze Ringererweiterung $\Leftrightarrow$ jedes $\alpha \in S$ ist ganz über R.

Algebraische Zahlentheorie
Algebra B 4 - Sommersemester 2017
Prof'in Dr. Salma Kuhlmann

9.Vorlesung

29. Mai 2017

Proposition 9.1
Seien R, S integritätsbereiche, $R \subseteq S$ und $\alpha \in S$. Es gilt: α ist genau dann ganz über R, wenn es einen endlich erzeugten R-Untermodul $M \neq 0$ von S gibt, so daß $\alpha M \subseteq M$.
(In der Tat können wir $M = R[\alpha]$ nehmen).

Beweis. „⇒" Sei $\alpha^n + r_1\alpha^{n-1} + \cdots + r_n = 0$, $r_i \in R$.

Behauptung: $\mathrm{Span}_R\{1, \alpha, \ldots, \alpha^{n-1}\} := M$ hat die gewünschte Eigenschaft.

Beweis. $\alpha^n \in \sum_{i=0}^{n-1} R\alpha^i$, also ist
$\alpha(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}) = \alpha a_0 + a_1\alpha^2 + \cdots + a_{n-2}\alpha^{n-1} + a_{n-1} \underbrace{\alpha^n}_{\in \sum R\alpha^i}$

□

„⇐"

Erinnerung (Cramer's Formel)**:** Seien $d_1, \ldots, d_n \in R$, C eine $n \times n$ Matrix mit Einträgen in R, $C = (c_{ij})$, und sei C_j die Matrix, die man bekommt, nachdem wir die j-te Spalte von C durch $\begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix}$ ersetzen. Sei $X := \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ eine Lösung für
$CX = \begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix}$
Es gilt: $\det(C)x_j = \det(C_j) \forall j$

Sei nun $M \neq 0$ endlich erzeugt mit $\alpha M \subseteq M$ und $v_1, \ldots, v_n \in S$ Erzeuger für M. Für alle i gilt $\alpha v_i = \sum a_{ij}v_j$ für $a_{ij} \in R$. Umschreiben ergibt ein Gleichungssytem:

$$\begin{aligned} (\alpha - a_{11})v_1 - a_{12}v_2 - \cdots &= 0 \\ -a_{21}v_1 + (\alpha - a_{22})v_2 - \cdots &= 0 \\ &\vdots \\ \cdots &= 0 \end{aligned}$$

Sei C die Koeffizienten-Matrix. Cramers Formel ergibt für $C\underline{v} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$:

$\det(C)v_j = \det(C_j) = 0$
Da es mindestens ein j gibt mit $v_j \neq 0$ (weil $0 \neq M$), $v_j \in S$ und $\det(C) \in S$ und S integritätsbereich⇒ $\det(C) = 0$.

Das Berechnen dieser Determinante ergibt schliesslich eine Gleichung
$\alpha^n + c\alpha^{n-1} + \cdots + c_n = 0$ (ÜA).

□

Notation
$\overline{R}^S := \{\alpha \in S \mid \alpha \text{ ist ganz über } R\}$.

Proposition 9.2
Seien $R \subseteq S$ Erweiterung von Integritätsbereichen. Der ganze Abschluß $\overline{R}^S$ von R in S ist ein Unterring von S.

Beweis. Seien $\alpha, \beta \in S$ ganz über R, $0 \neq M$, $0 \neq N$ endlich erzeugte R-Untermoduln von S, so daß $\alpha M \subseteq M$ und $\beta N \subseteq N$. Definiere $MN := \{\sum m_i n_i \mid m_i \in M, n_i \in N\}$.
Es ist:

(a) $MN \neq 0$ ist R-Untermodul von S

(b) MN ist endlich erzeugt (wenn $\{e_1, \ldots, e_m\}$ M erzeugt und $\{f_1, \ldots, f_n\}$ N erzeugt, dann erzeugt $\{e_i f_j \mid i = 1, \ldots, m, j = 1, \ldots, n\}$ MN).

(c) MN ist abgeschlossen unter multiplikation durch $\alpha\beta$ und $\alpha \pm \beta$ (d.h $\alpha\beta MN \subseteq MN$ und $(\alpha \pm \beta)MN \subseteq MN$, (ÜA)).

Anwendung von Proposition 9.1 ergibt: $\alpha\beta$ und $\alpha \pm \beta$ sind ganz über R. □

Korollar 9.3
Seien $R \subseteq S$ Integritätsbereiche. Es gilt: S endlich erzeugt als R-Modul$\Rightarrow$ S ist ganz über R.

Satz 9.4
Sei R ein Integritätsbereich, $K := \text{Quot}(R)$, L/K eine algebraische Körpererweiterung und $\overline{R}^L$ der ganze Abschluß von R in L. Es gilt: $L = \text{Quot}(\overline{R}^L)$.

Für den Beweis brauchen wir eine:

Proposition 9.5
Sei R ein Integritätsbereich, $K := \text{Quot}(R)$,L/K eine Körpererweiterung und $\alpha \in L$ algebraisch über K. Dann gibt es $d \in R$ mit $d\alpha$ ganz über R.

Beweis. α erfüllt

$$(*) \qquad \alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0$$

mit $a_i \in K = \text{Quot}(R)$. Sei $d \in R$, so daß $\forall i, da_i \in R$. Multiplizieren von $(*)$ mit d^m ergibt $d^m\alpha^m + a_1 d^m \alpha^{m-1} + \cdots + a_m d^m = 0$, d.h $(d\alpha)^m + (a_1 d)(d\alpha)^{m-1} + \cdots + a_m d^m = 0$ □

Beweis vom Satz 9.4. $\alpha \in L$ lässt sich schreiben als $\alpha = \frac{d\alpha}{d}$, $d \in R, d\alpha \in \overline{R}^L$, d.h $\alpha \in \text{Quot}(\bar{R}^L)$, also $\text{Quot}(\bar{R}^L) \supseteq L$. Da die Inklusion $\text{Quot}(\bar{R}^L) \subseteq L$ offensichtlich ist, ist der Satz bewiesen. □

§Ganz abgeschlossene Integritätsbereiche

Definition 9.1
Ein Integritätsbereich R ist ganz abgeschlossen $\Leftrightarrow \overline{R}^K = R$, wobei $K := \text{Quot}(R)$

Beispiel 9.1
Faktorielle Integritätsbereiche sind ganz abgeschlossen (ÜB)

Wir hatten gezeigt: R faktoriell, L/K Körpererweiterung, $\alpha \in L$ algebraisch über K, dann ist α ganz über $R \Leftrightarrow \ \mathrm{MinPol}_K(\alpha) \in R[x]$.
Wir verallgemeinern nun dieses:

Proposition 9.6
Sei R ein Integritätsbereich, $K = \mathrm{Quot}(R)$ und L/K eine algebraische Körpererweiterung. Wir nehmen an, daß R ganz abgeschlossen ist. Es gilt : $\alpha \in L$ ist ganz über $R \Leftrightarrow \ \mathrm{MinPol}_K(\alpha) \in R[x]$

Beweis. „$\Leftarrow$“:✓
„$\Rightarrow$“: Sei $\alpha \in L$ und $a_i \in R$, so daß

$$(*) \qquad \alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0$$

Setze $f(x) = \ \mathrm{MinPol}_K(\alpha) \in K[x]$. Wir arbeiten in einem Zerfällungskörper für f und behaupten: alle Nullstellen von $f(x)$ sind ganz über R

Beweis. Sei α' eine Nullstelle, dann gilt
$K(\alpha) \xrightarrow[\sim]{\sigma} K(\alpha')$ mit $\sigma_{|K} = \ \mathrm{Id}$ und $\alpha \mapsto \alpha'$
anwenden von σ auf $(*)$ ergibt
$(\alpha')^m + a_1(\alpha')^{m-1} + \cdots + a_m = 0$

□

Es folgt, daß alle Koeffizienten von $f(x)$ (diese Koeffizienten von $f(x)$ sind ja elementare symmetrische Polynome in den Nullstellen von $f(x)$) sind ganz über R (da die Menge aller ganzen Elementen ein Teilring ist). Diese Koeffiziente sind andererseits in $K = \mathrm{Quot}(R)$, also R ganz abgeschlossen $\Rightarrow$ alle Koeffiziente sind $\in R$. □

Algebraische Zahlentheorie
Algebra B 4 - Sommersemester 2017
Prof'in Dr. Salma Kuhlmann

10.Vorlesung

1. Juni 2017

Proposition 10.1 (Transitivität von Ganzheit)
Seien $A \subseteq B \subseteq C$ Integritätsbereiche. Aus B ganz über A und C ganz über B folgt C ganz über A.

Für den Beweis brauchen wir:

Lemma 10.2
Seien $A \subseteq B \subseteq C$ Ringerweiterungen. Aus B endlich erzeugt als A-Modul und
C endlich erzeugt als B-Modul folgt
C endlich erzeugt als A-Modul.

Beweis. Seien $\{\beta_1, \ldots, \beta_m\}$ erzeugend für B als A-Modul und
$\{\gamma_1, \ldots, \gamma_n\}$ erzeugend für C als B-Modul.
Dann ist $\{\beta_i \gamma_j\}$ erzeugend für C als A-Modul. □

Lemma 10.3
Sei $B = A[\beta_1, \ldots, \beta_m]$ eine Ringerweiterung, mit β_i ganz über A $\forall i = 1, \ldots, m$. Dann ist B ganz über A und B ist endlich erzeugt als A-Modul.

Beweis. Induktion nach m. Induktionsanfang $m = 1$:
Seien $\beta = \beta_1$, β ganz über A, und $a_i \in A$, so daß $\beta^n + \cdots + a_n = 0$

Behauptung: $1, \beta, \beta^2, \ldots, \beta^{n-1}$ erzeugen $B = A[\beta]$ als A-Modul.

Beweis. Weil $\beta^n \in \sum_{i=0}^{n-1} A\beta^i$, kann man ein Element b aus $A[\beta]$ als

$$(*) \qquad b = c_0 + c_1\beta + \cdots + c_N\beta^N \quad (c_i \in A)$$

umschreiben, indem man $c_N\beta^N$ als A-lineare Kombination der $\beta^0, \ldots, \beta^{n-1}$ schreibt und in $(*)$ ersetzt usw... □

Induktionsschritt: schreibe $B = A[\beta_1, \ldots, \beta_{m-1}, \beta_m] = \underbrace{A[\beta_1, \ldots, \beta_{m-1}]}_{:=D}[\beta_m]$
D ist endlich erzeugt als A-Modul per Induktionsannahme und $B = D[\beta_m]$ ist endlich erzeugt als D-Modul per Induktionsanfang, da β_m a fortiori auch ganz über D ist, also sind $A \subseteq D \subseteq B$ wie in Lemma 10.2 und damit ist B endlich erzeugt als A-Modul und (Korollar 9.3) damit ist B ganz über A. □

Beweis von Proposition 10.1. Seien $\gamma \in C$ und $b_i \in B$, so daß $\gamma^n + b_1\gamma^{n-1} + \cdots + b_n = 0$
Setze $B' := A[b_1, \ldots, b_n]$. Da die b_i ganz über A sind, ist B' endlich erzeugt als A-Modul (Lemma 10.3). Nun ist γ bereits ganz über B' (Wahl der b_i), also ist $B'[\gamma]$ endlich erzeugt als B'-Modul, also (Lemma 10.2) ist $B'[\gamma]$ endlich erzeugt als A-Modul. Damit ist γ ganz über A. □

Korollar 10.4
Sei $R \subseteq S$ Ringerweiterung. Es ist: $\overline{R}^S$ ist ganz abgeschlossen in S.

Beweis. Es ist: $R \subseteq \overline{R}^S \subseteq S$. Sei $\gamma \in S$ ganz über $\overline{R}^S$, also haben wir $R \underset{\text{ganz}}{\subseteq} \overline{R}^S \underset{\text{ganz}}{\subseteq} \overline{R}^S[\gamma]$ und damit gilt nach Proposition 10.1 $R \underset{\text{ganz}}{\subseteq} \overline{R}^S[\gamma]$. Somit ist $\gamma \in \overline{R}^S$. □

Korollar 10.5
Sei $R \subseteq K$, K Körper. Dann ist $\overline{R}^K$ ganz abgeschlossen.

Beweis. $\overline{R}^K \subseteq \text{Quot}(\overline{R}^K) \subseteq K$ und $\overline{R}^K$ ist ganz abgeschlossen in K (Korollar 10.4), also ist a fortiori $\overline{R}^K$ ganz abgeschlossen (in der Zwischenerweiterung $\text{Quot}(\overline{R}^K)$). □

§Zusammenfassung: Lokalisierung

(3. Vorlesung BIII)

1. Sei R ein Integritätsbereich. $D \subseteq R$ ist multiplikativ falls $1 \in D$ und $s, t \in D \Rightarrow st \in D$
2. Sei $D \subseteq R$ multiplikativ mit $0 \notin D$, $\sim$ wird auf $R \times D$ wie folgt definiert:
   $(r, d) \sim (r', d') \Leftrightarrow rd' = dr'$. Schreibe $\frac{r}{d} := [(r, d)]$
3. $\{\frac{r}{d} \mid (r, d) \in R \times D\} := D^{-1}R$ ist ein Ring

Beispiel 10.1
$D := R\backslash\{0\}$ ist multiplikativ und $D^{-1}R = \text{Quot}(R)$.

Beispiel 10.2
$\mathfrak{p} \lhd R$ Primideal$\Rightarrow D := R\backslash\mathfrak{p}$ ist multiplikativ. Wir bezeichnen mit $R_\mathfrak{p}$ die Lokalisierung $D^{-1}R$ von R nach $\mathfrak{p}$, also ist $R_\mathfrak{p} := \{\frac{r}{d} \mid r \in R, d \notin \mathfrak{p}\}$.

Definition und Notation

a) Für $I \lhd R$ und $D \subseteq R$ multiplikativ mit $0 \notin D$, setze $I^e := D^{-1}RI$ das von I in $D^{-1}R$ erzeugte Ideal.
   ÜA: $I^e = \{\frac{a}{d} \mid a \in I, d \in D\} \lhd D^{-1}R$

b) Sei nun $I \lhd D^{-1}R$. Setze $I^c := I \cap R \lhd R$. Es gilt
   (i) $I \lhd D^{-1}R \Rightarrow I^{ce} = I$
   (ii) $I \lhd R$ prim und $I \cap D = \varnothing \Rightarrow I^{ec} = I$
   (iii) $\mathfrak{p} \mapsto \mathfrak{p}^e$ ist eine inklusionserhaltende Bijektion zwischen $\{\mathfrak{p} \in \text{Spec}(R) : p \cap D = \varnothing\}$ und $\text{Spec}(D^{-1}R)$, wobei $\text{Spec}(R)$:=Menge aller Primideale von R.

Korollar 10.1
Sei $\mathfrak{p} \lhd R$ prim. Die Abbildung $\mathfrak{q} \mapsto \mathfrak{q}R_\mathfrak{p}$ liefert eine inklusionserhaltende Bijektion $\{\mathfrak{q} \in \text{Spec}(R) \mid \mathfrak{q} \subseteq \mathfrak{p}\} \to \text{Spec}(R_\mathfrak{p})$. Insbesondere besitzt $R_\mathfrak{p}$ nur ein maximales Ideal, nämlich $\mathfrak{p}R_\mathfrak{p}$.

Definition 10.1
R ist lokal, wenn R nur ein maximales Ideal besitzt.

Lemma 10.2
R ist lokal $\Leftrightarrow R\backslash R^\times$ ist ein Ideal.

Beweis. siehe ÜB. □

§Lokalisierung und Ganzheit

ÜB B4: R noethersch, $D \subseteq R$ multiplikativ ohne Null $\Rightarrow D^{-1}R$ noethersch.

Satz
R ganz abgeschlossen$\Rightarrow D^{-1}R$ ganz abgeschlossen.

Beweis. siehe ÜB. □

Korollar
$R \subseteq R'$ ganze Erweiterung$\Rightarrow D^{-1}R \subseteq D^{-1}R'$ ganze Erweiterung.

Beweis. Siehe ÜB. □

Algebraische Zahlentheorie
Algebra B 4 - Sommersemester 2017
Prof'in Dr. Salma Kuhlmann

11.Vorlesung

8. Juni 2017

§Norm, Spur, Diskriminante

Sei L/K eine endliche Körpererweiterung.

Definition und Notation
Sei $\alpha \in L$ und betrachte die Abbildung

$$\begin{array}{rccc} \mu_{\alpha,L}: & L & \to & L \\ & x & \mapsto & \alpha x \end{array}$$

Es ist $\mu_{\alpha,L} \in \mathcal{L}_K(L,L)$ (d.h ein linearer Operator). Setze
$\chi_{\alpha,L} :=$ CharPol von $\mu_{\alpha,L}$
$f_{\alpha,L} :=$ MinPol von $\mu_{\alpha,L}$
$N_{L/K}(\alpha) := \det(\mu_{\alpha,L}) \in K$ heißt die (L/K)-Norm von α.
$Sp_{L/K}(\alpha) := \mathrm{Spur}(\mu_{\alpha,L}) \in K$ ist die (L/K)-Spur von α

Lemma 11.1 (i) $f_{\alpha,L} = \mathrm{MinPol}_K(\alpha)$; Insbesondere ist $f_\alpha := f_{\alpha,K(\alpha)} = \chi_{\alpha,K(\alpha)} = \mathrm{MinPol}_K(\alpha)$ (weil $\deg \chi_{\alpha,K(\alpha)} = [K(\alpha) : K] = \deg \mathrm{MinPol}_K(\alpha) = \deg f_{\alpha,K(\alpha)}$, und damit sind sie gleich).

(ii) $\chi_{\alpha,L} = f_{\alpha,L}^m$, wobei $m := [L : K(\alpha)]$.

Beweis. (i) Es ist leicht zu prüfen, daß $f(\mu_{\alpha,L}) = 0 \Leftrightarrow f(\alpha) = 0 \forall f \in K[x]$. Die Aussage folgt nun unmittelbar aus der Definition.

(ii) Sei $\{\lambda_1, \ldots, \lambda_m\}$ eine Basis für $L/K(\alpha)$, also

$$(*) \qquad L = \bigoplus_{i=1}^{m} K(\alpha)\lambda_i$$

Setze $W_i := K(\alpha)\lambda_i$; die W_i sind (prüfe!) $\mu_{\alpha,L}$-invariante K-Unterräume und

$$(**) \qquad L = \bigoplus_{i=1}^{m} W_i \text{ als } K\text{-Vektorraum,}$$

d.h $\mu_{\alpha,L} : L \to L$
$\mu_{\alpha,K(\alpha)} : K(\alpha) \to K(\alpha)$
und $\begin{array}{ccccc} K(\alpha) & \overset{\omega_i}{\tilde{\to}} & W_i \\ x & \mapsto & x\lambda_i \end{array}$ als K-Vektorräume, wobei ω_i die folgende Eingenschaft hat:
$\omega_i \circ \mu_{\alpha,K(\alpha)} = \mu_{\alpha,L} \circ \omega_i$ auf $K(\alpha)$, d.h $\mu_{\alpha,L} = \bigoplus_{i=1}^m \mu_{\alpha,K(\alpha)}$

und $\underbrace{\mu_{\alpha,L} \restriction W_i = \omega_i \circ (\mu_{\alpha,K(\alpha)}) \circ \omega_i^{-1}}_{\text{ähnliche lineare Transformationen}}$ (prüfe!)

$(**)$ liefet nun (LA I+II), daß

$$\begin{aligned}
\chi_{\alpha,L} &= \text{CharPol}(\mu_{\alpha,L}) \\
&= \prod_{i=1}^{m} \text{CharPol}(\mu_{\alpha,L} \restriction_{W_i}) \\
&= \prod_{i=1}^{m} \text{CharPol}(\omega_i \circ \mu_{\alpha,K(\alpha)} \circ \omega_i^{-1}) \\
&= \prod_{i=1}^{m} \text{CharPol}(\mu_{\alpha,K(\alpha)}) \\
&= \prod_{i=1}^{m} \chi_{\alpha,K(\alpha)} \\
&\overset{(i)}{=} \prod_{i=1}^{m} f_\alpha
\end{aligned}$$

□

Lemma 11.2
Seien $\alpha, \beta \in L$, $\lambda \in K$ und $n = [L : K]$. Es gilt:

1. $N_{L/K}(\alpha\beta) = N_{L/K}(\alpha)N_{L/K}(\beta)$
2. $Sp_{L/K}(\lambda\alpha + \beta) = \lambda Sp_{L/K}(\alpha) + Sp_{L/K}(\beta)$
3. $N_{L/K}(\lambda) = \lambda^n, Sp_{L/K}(\lambda) = n\lambda$
4. Sei $f_{\alpha,L} = x^\nu + a_{\nu-1}x^{\nu-1} + \cdots + a_0, \quad a_i \in K.$

Setze $\mu := [L : K(\alpha)] = \frac{n}{\nu}$. Es gilt:

(i) $N_{L/K}(\alpha) = (-1)^n a_0^\mu$

(ii) $Sp_{L/K}(\alpha) = -\mu a_{\nu-1}$

Beweis. 1. $\mu_{\alpha\beta,L} = \mu_{\alpha,L} \circ \mu_{\beta,L}$ und die Determinante ist multiplikativ (LA II).

2. $\mu_{\lambda\alpha+\beta,L} = \lambda\mu_{\alpha,L} + \mu_{\beta,L}$ und die Spur ist additiv (LA II).

3. $N_{L/K}(\lambda) = \det(\mu_{\lambda,L}) = \det(\lambda \text{ Id}_L) = \lambda^n$.
   Analog $Sp_{L/K}(\lambda) = \text{Spur}(\lambda \text{ Id}_L) = n\lambda$.

4. **Erinnerung**(LA I+II): $A \in M_{n\times n}(K)$, setze $\text{CharPol}(A) = \det(xI - A) = x^n + b_{n-1}x^{n-1} + \cdots + b_0$. Es ist $b_0 = (-1)^n \det A$ und $b_{n-1} = -\text{Spur}(A)$.

(i) $\nu = [K(\alpha) : K], \quad \mu = [L : K(\alpha)], \quad n = \nu\mu$. $N_{L/K}(\alpha) = \det(\mu_{\alpha,L})$ und

$$(\dagger) \qquad \chi_{\alpha,L} = x^n + b_{n-1}x^{n-1} + \cdots + b_0 = (f_\alpha)^\mu$$

also gilt $(-1)^n \det(\mu_{\alpha,L}) = b_0$ und Koeffizientenvergleich in $(\dagger)$ ergibt $b_0 = a_0^\mu$.

(ii) $b_{n-1} = -Sp_{L/K}(\alpha)$, Koeffizientenvergleich in (†) ergibt: links ist Koeffizient von x^{n-1}, gleich Koeffizient von $x^{\nu\mu-1}$ rechts, also ist gleich $\mu a_{\nu-1}$ (ÜA).

□

Proposition 11.3
Sei $n = [L : K]$, $\beta \in L$, $f(x) = \text{ MinPol}_K(\beta)$ und $\deg f := m = [K(\beta) : K]$. Seien
$\beta = \beta_1, \beta_2, \ldots, \beta_m$ alle Nullstellen von f. Es ist $N_{L/K}(\beta) = (\prod \beta_i)^r$ und $Sp_{L/K}(\beta) = r \sum \beta_i$, wobei $r := \frac{n}{m} = [L : K(\beta)]$

Beweis. (Lemma 11.2 4-(i) und 4-(ii) anwenden) Sei $f_{\beta,L} = \text{ MinPol}_K(\beta) = x^m + a_{m-1}x^{m-1} + \cdots + a_0$, $a_i \in K$. Nun ist $\prod \beta_i = (-1)^m a_0$ und $\sum \beta_i = -a_{m-1}$ (Algebra BIII), also ist
$(\prod \beta_i)^r = (-1)^{mr} a_0^r \overset{(i)}{=} N_{L/K}(\beta)$ und $r \sum \beta_i = -r a_{m-1} \overset{(ii)}{=} Sp_{L/K}(\beta)$. □

Satz 11.4
Sei L/K separabel, $[L : K] = n$ und $\{\sigma_1, \ldots, \sigma_n\}$ die Menge der verschiedenen K-Einbettungen von L (in der normalen Abschluss Ω von L/K). Sei $\beta \in L$. Es ist $N_{L/K}(\beta) = \prod_{k=1}^n \sigma_k(\beta)$ und $Sp_{L/K}(\beta) = \sum_{k=1}^n \sigma_k(\beta)$

Beweis. (Wir zeigen in der 12. Vorlesung, daß $\sigma_1, \ldots \sigma_n$ existieren) Sei $f(x) := \text{ MinPol}_K(\beta)$, $[K(\beta) : K] = m = \deg f$ und setze $r := [L : K(\beta)]$, und
$\beta = \beta_1, \beta_2, \ldots, \beta_m$ die verschiedene Nullstellen von f.

Behauptung: Für $i = 1, \ldots, m$ gibt es genau r Einbettungen von L in Ω, die β auf β_i absenden (d.h β_i erscheint genau r mal in $\{\sigma_k(\beta)\}_k$) (Diese Behauptung wird auch in der 12. Vorlesung bewiesen).

Nun folgt aus Prop 11.3, daß
$N_{L/K}(\beta) = (\prod_{i=1}^m \beta_i)^r = \prod_{i=1}^n \sigma_i(\beta)$ und $Sp_{L/K}(\beta) = r(\sum_{i=1}^m \beta_i) = \sum_{i=1}^n \sigma_i(\beta)$. □

Algebraische Zahlentheorie
Algebra B 4 - Sommersemester 2017
Prof'in Dr. Salma Kuhlmann

12.Vorlesung

12 Juni 2017

Korollar 12.1
Sei R ein ganz abgeschlossener Integritätsbereich, $K := \text{Quot}(R)$, L/K eine endliche Körpererweiterung. Sei $\beta \in \overline{R}^L$; dann sind $N_{L/K}(\beta) \in R$ und $Sp_{L/K}(\beta) \in R$.

Beweis. $\beta \in \overline{R}^L, \beta_1, \ldots, \beta_m$ die Nullstellen von $\text{MinPol}_K(\beta) \in R[x] \Rightarrow \beta_1, \ldots, \beta_m \in \overline{R}^L$. Nun ist außerdem $K \ni N_{L/K}(\beta) = (\prod \beta_i)^r$ und $Sp_{L/K} = r \sum \beta_i \in K$, also $N_{L/K}(\beta) \in \overline{R}^L$ und $Sp_{L/K} \in \overline{R}^L$. Nun ist aber R ganz abgeschlossen, also folgt die Behauptung. □

Satz 12.2
Sei L/K separabel, $[L : K] = n$, Ω die normale Hülle von L/K. Dann gelten:

1. $\exists \sigma_1, \ldots, \sigma_n$ verschiedene Einbettungen von L/K in Ω.
2. Für $\beta \in L$ mit $[K(\beta) : K] = m = \frac{n}{r}$ und $[L : K(\beta)] = r$ und $\sigma \in \{\sigma_1, \ldots, \sigma_n\}$ kommt $\sigma(\beta)$ genau r mal in der Folge $(\sigma_1(\beta), \ldots, \sigma_n(\beta))$ vor.

Beweis. (1) Sei $L = K(\gamma)$, $\text{MinPol}_K(\gamma) = g$ und $\gamma_1, \ldots, \gamma_n$ die n verschiedenen Nullstellen von g in Ω.

$$\begin{array}{ccc} L & \overset{\sigma_k}{\hookrightarrow} & \Omega \\ \gamma & \mapsto & \gamma_k \\ K & \overset{\sigma_k \restriction K}{\longrightarrow} & K \\ & = Id & \end{array}$$

(Isomorphismus $K(\gamma) \cong K[x]/ < g(x) > \cong K(\gamma_k)$ aus Algebra BIII)

(2) $L/K(\beta)$ und $K(\beta)/K$ sind separabel, also liefert (1) m Einbettungen von $K(\beta)$ über K in Ω' (Ω' :=normale Hülle von $L/K(\beta)$, $\Omega' \supseteq \Omega$), und r Einbettungen von L über $K(\beta)$ in Ω'; zusammengefasst:

$\exists m$ Einbettungen von $K(\beta)$ über K in Ω'

$\exists r$ Einbettungen von L über $K(\beta)$ in Ω',

$\exists mr = n$ Einbettungen von L über K in Ω'.

$$L \overset{\lambda_1, \ldots, \lambda_r}{\underset{K(\beta)}{\hookrightarrow}} \Omega'$$

$$K(\beta) \overset{\mu_1, \ldots, \mu_m}{\underset{K}{\hookrightarrow}} \Omega'$$

Betrachte:

$L \xrightarrow{\sim} \lambda_i(L) \subseteq \Omega'$ und schreibe $L = K(\beta)(\gamma)$, also $\lambda_i(L) = K(\beta)(\lambda_i(\gamma))$.

Definiere $K(\beta)(\lambda_i(\gamma)) \xrightarrow{\tilde{\mu}_j} \Omega'$ durch: $\tilde{\mu}_j \restriction K(\beta) = \mu_j$ und $\lambda_i(\gamma) \mapsto \lambda_i(\gamma)$.

Betrachte nun $L \xrightarrow{\lambda_i}_{\sim} \lambda_i(L) \xrightarrow{\tilde{\mu}_j} \Omega'$.

Es ist klar, daß $(\tilde{\mu}_j \circ \lambda_i)$ Einbettung von L über Kin Ω' ist für alle $j = 1, \ldots, m$ und $i = 1, \ldots, r$. Also ist $\{\tilde{\mu}_j \circ \lambda_i, j = 1, \ldots, m, i = 1, \ldots, r\} \subseteq \{\sigma_1, \ldots, \sigma_n\}$.

Außerdem ist $\tilde{\mu}_j \circ \lambda_i$ eindeutig durch ihre Bilder für γ und β bestimmt. Nun ist

$(\tilde{\mu}_j \circ \lambda_i)(\gamma) = \tilde{\mu}_j(\lambda_i(\gamma)) = \lambda_i(\gamma)$ und

$$(*) \qquad (\tilde{\mu}_j \circ \lambda_i)(\beta) = \mu_j(\beta)$$

Es folgt $\{\tilde{\mu}_j \circ \lambda_i \mid j = 1, \ldots, m, i = 1, \ldots, r\} = \{\sigma_1, \ldots, \sigma_n\}$ und $\forall \sigma \in \{\sigma_1, \ldots \sigma_n\}$ ist $\sigma(\beta)$ r mal wiederholt wie in $(*)$.

□

Korollar 12.3
Sei $K \subseteq E \subseteq L$ mit L/K endlich separabel, $[L : K] = n$, und $\alpha \in L$. Dann gelten:

(i) $N_{L/K}(\alpha) = N_{E/K}(N_{L/E}(\alpha))$ und

(ii) $Sp_{L/K}(\alpha) = Sp_{E/K}(Sp_{L/E}(\alpha))$

Beweis. (i) $N_{L/K}(\alpha) = \prod_{k=1}^{n} \sigma_k(\alpha)$ wobei $\{\sigma_1, \ldots, \sigma_n\}$ die Einbettungen von L/K in Ω sind. Nun $\forall k, \exists i, \exists j$, so daß $\sigma_k = \tilde{\mu}_j \circ \lambda_i$ (Bezeichnung wie im letzten Beweis). Also

$N_{L/K}(\alpha) \overset{\text{Hom}}{=} \prod_{j=1}^{m} \tilde{\mu}_j(\prod_{i=1}^{r} \lambda_i(\alpha))$. Nun folgt aus dem letzten Beweis, daß
$\prod_{i=1}^{r} \lambda_i(\alpha) = N_{L/E}(\alpha) \in E$ (insbesondere ist
$\tilde{\mu}_j(\prod_{i=1}^{r} \lambda_i(\alpha)) = \mu_j(\prod_{i=1}^{r} \lambda_i(\alpha)))$,
also $N_{L/K}(\alpha) = \prod_{j=1}^{m} \mu_j(N_{L/E}(\alpha)) = N_{E/K}(N_{L/E}(\alpha))$.

□

§Erinnerung: Bilineare Formen

Definition 1. Sei V ein endlichdimensionaler Vektorraum über K, $\dim_K V = n$ und $B : V \times V \to K$ eine bilineare Form.

2. B ist symmetrisch$\Leftrightarrow B(x, y) = B(y, x) \forall x, y \in V$.

3. Die Matrix-Darstellung von B bezüglich der Basis $\{v_i \mid i = 1, \ldots, n\} = \mathcal{B}$ ist definiert durch:

   $\mathbb{B}_{ij} = B(v_i, v_j)$

   Es gilt $\forall x, y \in V, [y]_{\mathcal{B}}^t \mathbb{B} [x]_{\mathcal{B}} = B(x, y)$

4. $\mathbb{B}' = P^t \mathbb{B} P$, wobei $\mathbb{B}'$ die Darstellung von B bezüglich einer Basis $\{v_i' \mid i = 1, \ldots, n\}$ und P die Basiswechselmatrix ist.

Algebraische Zahlentheorie
Algebra B 4 - Sommersemester 2017
Prof'in Dr. Salma Kuhlmann

13.Vorlesung

19 Juni 2017

Erinnerung: Bilineare Formen (Fortsetzung)
Definitionen und Bemerkungen: Sei V ein endlichdimensionaler Vektorraum über K. Sei $B : V \times V \to K$ bilinear symmetrisch. Für alle $x \in V$ definiere:
$B_x : V \to K$ durch $B_x(y) = B(x, y)$
(oder $B_y : V \to K$ durch $B_y(x) = B(x, y)$)
B heißt nicht ausgeartet, wenn: $\forall x \in V, x \neq 0 \Rightarrow Bx \neq 0$.
Bemerke, daß

(i) $B_x \in V^*$

(ii) B nicht ausgeartet$\Leftrightarrow \det \mathbb{B} \neq 0$ für eine (alle) Matrixdarstellungen $\mathbb{B}$ von B (ÜA).

(iii) B ist nicht ausgeartet$\Leftrightarrow$ die lineare Abbildung

$$\begin{array}{rccc} \phi_B : & V & \to & V^* \\ & x & \mapsto & B_x \end{array}$$

hat Kern $\{0\}$ (ÜA).

(iv) Da $\dim V = \dim V^*$ gilt also:

B nicht ausgeartet$\Leftrightarrow \phi_B$ ist eine Isomorphie

(v) Sei $\mathcal{B} := \{v_1, \ldots, v_n\}$ eine K-Basis für V, B nicht ausgeartet; setze $w_i := \phi_B^{-1}(v_i^*)$. Dann gilt $B(v_i, w_j) = \delta_{ij} \forall i, j$. Die Basis $\{w_i \mid i = 1, \ldots, n\}$ heißt die zu $\{v_1, \ldots, v_n\}$ B-duale Basis für V. Die B-duale Basis hat die folgende nützliche Eigenschaft:

$\forall v \in V$ mit $v = \sum c_i v_i$ ist $c_i = B(v, w_i)$ (ÜA).

§Die Spur bilineare Form

Fact 1: Sei L/K eine endliche separable Körpererweiterung; dann definiert die Abbildung

$$\begin{array}{rccc} B_{L/K} : & L \times L & \to & K \\ & (x, y) & \mapsto & Sp_{L/K}(xy) \end{array}$$

eine symmetrische bilineare Form (ÜA).

Fact 2: $B_{L/K}$ ist nicht ausgeartet.

Beweis. (Satz vom Primitivelement) Sei $\gamma \in L$, so daß $L := K(\gamma)$; dann ist $\{\gamma^0, \ldots, \gamma^{n-1}\}$ eine K-Basis für L. Wir berechnen die Matrixdarstellung $\mathbb{B}$ der bilinearen Form bezüglich dieser Basis:

$\mathbb{B}_{ij} = Sp(\gamma^{i+j}) \overset{\text{Satz 11 Vor.}}{=} \sum_{k=1}^{n} \sigma_k(\gamma^{i+j}) \overset{\text{Hom}}{=} \sum_{k=1}^{n} \sigma_k(\gamma)^{i+j}$, wobei $\sigma_1, \ldots, \sigma_n$ die n verschiedenen Einbettungen von L in Ω sind.
Bezeichne $\gamma_1, \ldots, \gamma_n$ die n verschiedenen Nullstellen von $\operatorname{MinPol}_K(\gamma)$, also ist $\{\gamma_1, \ldots, \gamma_n\} = \{\sigma_1(\gamma), \ldots, \sigma_n(\gamma)\}$. Wir schreiben um $\mathbb{B}_{ij} = \sum_{k=1}^{n} \gamma_k^{i+j}$
Daraus sehen wir, daß $\mathbb{B}$ ein Produkt von zwei Matrizen mit $\det \neq 0$ ist, nämlich $\mathbb{B} = \mathcal{V}^t\mathcal{V}$ und $\det \mathbb{B} = (\det \mathcal{V})^2$, wobei $\mathcal{V}$ die Vandermonde Matrix :

$$\begin{pmatrix} \gamma_1^0 & \cdots & \gamma_1^{n-1} \\ \gamma_2^0 & \cdots & \gamma_2^{n-1} \\ \vdots & & \vdots \\ \gamma_n^0 & \cdots & \gamma_n^{n-1} \end{pmatrix}$$

ist (In LA II haben wir gezeigt, daß $\det \mathcal{V} \neq 0$). Also ist $\det \mathbb{B} \neq 0$ und somit ist gezeigt, daß $B_{L/K}$ nicht ausgeartet ist.

□

Bemerkung (siehe ÜB)
Sei L/K endlich separabel, $[L : K] = n$. Wir können andere Basen betrachten (anstatt $\{\gamma^0, \ldots, \gamma^{n-1}\}$): Sei $\{v_1, \ldots, v_n\}$ eine beliebige Basis für L/K und wie zuvor $\{\sigma_1, \ldots, \sigma_n\}$ die n verschiedenen Einbettungen von L/K in Ω. Dann ist die Matrix $\mathbb{B}$ von $B_{L/K}$ bezüglich $\{v_1, \ldots, v_n\}$ $\mathcal{V}^t\mathcal{V}$, wobei $\mathcal{V}_{ij} := \sigma_i(v_j)$ für alle i, j, also ist $\det \mathbb{B} = (\det \mathcal{V})^2$.

Satz
Sei R ein ganz abgeschlossener Integritätsbereich, $K = \operatorname{Quot}(R)$, L/K eine endliche separable Erweiterung, $n = [L : K]$ und $S = \overline{R}^L$. Dann gibt es $M \subseteq L, M' \subseteq L$ R-Untermoduln von L, beide frei von Dimension n, so daß $M \subseteq S \subseteq M'$.

Beweis. später □

Korollar 13.1
Sei R ein ganz abgeschlossener Integritätsbereich, R noethersch, $K = \operatorname{Quot}(R)$. Dann ist $S := \overline{R}^L$ ein endlich erzeugter R-Modul.

Beweis. M' ist ein endlich erzeugter Modul über einem noetherschen Ring, also ist M' ein noetherscher R-Modul, und damit ist jeder Untermodul endlich erzeugt.

□

Korollar 13.2
Sei R ein HIR, L/K eine endliche separable Körpererweiterung und $n = [L : K]$. Dann ist $S := \overline{R}^L$ ein freier R-Modul der Dimension n.

Beweis. Ein Untermodul (von freiem Modul der Dimension $= n$ und über einem HIR) ist frei der Dimension $\leq n$, also:
$S \subseteq M' \Rightarrow S$ frei der Dimension $\leq n$
$M \subseteq S \Rightarrow \dim M = n \leq \dim S \leq n \Rightarrow \dim S = n$ □

Korollar 13.3
$R = \mathbb{Z}$. L ist ein Zahlkörper$\Rightarrow \mathcal{O}_L$ ist ein freier $\mathbb{Z}$-Modul der Dimension $[L : K]$

Algebraische Zahlentheorie
Algebra B 4 - Sommersemester 2017
Prof'in Dr. Salma Kuhlmann

14.Vorlesung

22 Juni 2017

Beweis vom Satz. L/K endlich und separabel, $K = \text{Quot}(R)$, R ein ganz abgeschlossener Integritätsbereich, $S = \overline{R}^L$. $B_{L/K} : L \times L \to K$ $B_{L/K}(x, y) = Sp_{L/K}(xy)$. Die Einschränkung von $B_{L/K}$ auf $S \times S$ hat Werte in R. Sei $\{\nu_1, \ldots, \nu_n\}$ eine Basis für L/K (a fortiori linear unabhängig über R). Erinnerung: $\forall \alpha \in L \exists r \in R$ mit $r\alpha \in S$, also gilt o.E. $\{\nu_1, \ldots, \nu_n\} \subseteq S$. Sei $\{\mu_1, \ldots, \mu_n\}$ die $B_{L/K}$-duale Basis und setze $M := \bigoplus R\nu_i$ und $M' = \bigoplus R\mu_i$. Es ist klar, dass $M \subseteq S$. Wir zeigen $S \subseteq M'$. Sei $\alpha \in S$, $\alpha = \sum c_i\mu_i$ aber $c_i = B_{L/K}(\alpha, \nu_i) \in R$ □

Definition 14.1
Sei R ein HIR, $n = [L : K]$, L/K separable Erweiterung, $S = \overline{R}^L$ ist ein freier R-Modul der Dimension n. Eine Basis $\{\mu_1, \ldots, \mu_n\}$ von S über R heißt Ganzheitsbasis.

Wir wollen nun Ganzheitsbasen finden.

Bemerkung 14.1
Sei V ein endlichdimensionaler K-Vektorraum, B eine nicht ausgeartete bilineare Form,
$\mathcal{B} = \{v_1, \ldots, v_n\} \subseteq V$. Dann ist $\mathcal{B}$ genau dann eine Basis für V über K, wenn $\det(B(v_i, v_j)) \neq 0$.

Beweis. „⇒“ 13. Vorlesung.
„⇐“Sei $\{w_1, \ldots, w_n\}$ eine Basis und $v_i = \sum_j c_{ij}w_j$, $P := [c_{ij}]$, $P \in M_{n\times n}(K)$. Es ist
$B(v_i, v_j) = P^t[B(w_i, w_j)]P$ und $\det P \neq 0 \Leftrightarrow \{v_1 \ldots, v_n\}$ linear unabhängig. Außerdem ist

$$\det[B(v_i, v_j)] = (\det P)^2 \underbrace{\det[B(w_i, w_j)]}_{\neq 0}$$

also $\det[B(v_i, v_j)] \neq 0 \Leftrightarrow \{v_1, \ldots, v_n\}$ linear unabhängig. □

Wir werden eine analogue Prozedur für R-Basen von S betrachten:

Diskriminante (einer Ringerweiterung)
Wir haben $B_{L/K} : S \times S \to R$. Für $\nu_1, \ldots, \nu_n \in S$ definiere
$D(\nu_1, \ldots, \nu_n) := \det(B_{L/K}(\nu_i, \nu_j)) \in R$.

Lemma 14.1
Seien $\{v_1, \ldots, v_n\}$ und $\{\mu_1, \ldots, \mu_n\}$ Basen für S als R-Modul. Dann ist $D(\nu_1, \ldots, \nu_n) = \pi^2 D(\mu_1, \ldots, \mu_n)$ mit $\pi \in R^\times$.

Beweis. Wir haben $D(\nu_1, \ldots, \nu_n) = [\det P]^2 D(\mu_1, \ldots, \mu_n)$, wobei $P \in M_{n\times n}(R)$ und P invertierbar (weil P Basiswechselmatrix ist), also folgt aus Cramer's Formel, daß $\det P \in R^\times$. □

Wir definieren für $x, y \in R$:
$x \sim y \Leftrightarrow x = \pi^2 y$ für ein $\pi \in R^\times$.
Lemma 14.1 besagt: für alle Basen $\{\nu_1, \ldots, \nu_n\}$ von S als R-Modul liegen $D(\nu_1, \ldots, \nu_n)$ in der gleichen Äquivalenzklasse.

Definition 14.2
$D(S/R) := [D(\nu_1, \ldots, \nu_n)]_\sim$ für eine (alle) Basis $\{\nu_1, \ldots, \nu_n\} \subseteq S$ von S als R-Modul.

Bemerkung 14.2
$R = \mathbb{Z} \Rightarrow \mathbb{Z}^\times = \{\pm 1\}$, also hier haben wir $D(\nu_1, \ldots, \nu_n) \sim D(\mu_1, \ldots, \mu_n) \Leftrightarrow D(\nu_1, \ldots, \nu_n) = D(\mu_1, \ldots, \mu_n)$

Satz 14.2
Sei $\{\gamma_1, \ldots, \gamma_n\} \subseteq S$. Dann ist $\{\gamma_1, \ldots, \gamma_n\}$ genau dann eine Basis von S über R, wenn $[D(\gamma_1, \ldots, \gamma_n)]_\sim = D(S/R)$.

Beweis. „$\Rightarrow$“ folgt aus Lemma 14.1.
„$\Leftarrow$“ Sei $\mathcal{B} := \{\nu_1, \ldots, \nu_n\}$ eine Basis von S als R-Modul, so daß
$\det[B_{L/K}(\gamma_i, \gamma_j)] = D(\gamma_1, \ldots, \gamma_n) = \pi^2 D(\gamma_1, \ldots, \gamma_n) = \pi^2 \det[B_{L/K}(\nu_i, \nu_j)]$ mit $\pi \in R^\times$. Betrachte

$$C: \begin{array}{ccc} S & \to & S \\ \nu_i & \mapsto & \gamma_i \end{array} \quad R\text{-Modul Homomorphismus.}$$

$$(*) \qquad P = [C]_{\mathcal{B}} \in M_{n\times n}(R)$$

$$(**) \qquad \text{also } [B_{L/K}(\gamma_i, \gamma_j)] = P^t [B_{L/K}(\nu_i, \nu_j)] P$$

also

$$(***) \qquad (\det P)^2 = \pi^2$$

und somit ist $\det P \in R^\times$ (weil $\det P = \pm\pi$), also ist P invertierbar (über R), also ist C invertierbarer R-Homomorphismus, d.h $\{\gamma_1, \ldots, \gamma_n\}$ ist eine Basis. □

Ab jetzt: $R = \mathbb{Z}, L = \mathbb{Q}(\alpha)$ Zahlkörper, α primitives Element. O.E.: $\alpha \in \mathcal{O}_L := \overline{\mathbb{Z}}^L$. $\mathcal{O}_L$ ist frei vom Rang $[L : \mathbb{Q}]$, $D(\mathcal{O}_L/\mathbb{Z})$ ist die Diskriminante des Zahlkörpers L.
Fragestellung: Sei $\mathcal{B}$ eine Basis für L/K, so daß $\mathcal{B} \subseteq \mathcal{O}_L$. Ist $\mathcal{B}$ für $\mathcal{O}_L$ eine Basis als $\mathbb{Z}$-Modul?
Insbesondere: $\{1, \alpha, \ldots, \alpha^{n-1}\} \subseteq \mathcal{O}_L$ ist eine Basis für L über $\mathbb{Q}$ (also sicher $\mathbb{Z}$-linear unabhängig), aber wann ist $\{1, \alpha, \ldots, \alpha^{n-1}\}$ eine Basis für $\mathcal{O}_L$ über $\mathbb{Z}$?
Wir berechnen:

$$\begin{aligned} D(1, \alpha, \ldots, \alpha^{n-1}) &= \det[B_{L/\mathbb{Q}}(\alpha^i, \alpha^j)] \\ &\overset{\text{13. Vor}}{=} (\text{Vandermonde Determinante})^2 \\ &\overset{\text{LAII}}{=} [\prod_{i<j} (\alpha_i - \alpha_j)]^2 \end{aligned}$$

wobei $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ die verschiedene Nullstellen von $f := \text{MinPol}_{\mathbb{Q}}(\alpha)$ sind.

Definition 14.3
$D(f) := \prod_{i<j}(\alpha_i - \alpha_j)^2$ für ein irreduzibles $f \in \mathbb{Q}[x]$ und $\alpha_1, \ldots, \alpha_n$ alle Nullstellen von f. $D(f)$ ist die Diskriminante von f.

Bemerkung 14.3
Sei $\{\beta_1, \ldots, \beta_n\}$ eine Ganzheitsbasis (für $\mathcal{O}_L$ als $\mathbb{Z}$-Modul) und P wie in $(*)$, dann ist

$$\begin{aligned} \mathbb{Z} \ni D(f) &= D(1, \alpha, \ldots, \alpha^{n-1}) \\ &\overset{(**)}{=} (\det P)^2 D(\beta_1, \ldots, \beta_n) \\ &= (\det P)^2 D(\mathcal{O}_L/\mathbb{Z}) \qquad (\dagger) \end{aligned}$$

Aus $(\dagger)$ folgt:

(i) (aus (†) und Satz 14.2) wenn wir $D(\mathcal{O}_L/\mathbb{Z})$ berechnen können, dann können wir auch entscheiden, ob $\{1, \alpha, \ldots, \alpha^{n-1}\}$ eine Ganzheitsbasis ist

(ii) Ist $D(f)$ quadratfrei, dann ist $\det P = \pm 1$, also ist P invertierbar über R und $\{1, \alpha, \ldots, \alpha^{n-1}\}$ ist eine Ganzheitsbasis.

(iii) Wenn $D(f)$ nicht quadratfrei ist, benutzen wir Stickelberger's Satz

Satz (Satz von Stickelberger)
$D(\mathcal{O}_L/\mathbb{Z}) \equiv 0, 1 \bmod 4$ (also ist Quadrat mod 4).

Beweis. Später (15. Vorlesung). □

Anwendung: Sei L quadratischer Zahlkörper, $[L : \mathbb{Q}] = 2$, $L = \mathbb{Q}(\sqrt{d}), d \in \mathbb{Z}$ quadratfrei.

Fall 1: $d \equiv 2, 3 \bmod 4$.

Behauptung: $\{1, \sqrt{d}\}$ ist eine Ganzheitsbasis un somit ist $\mathcal{O}_L = \mathbb{Z}[\sqrt{d}]$

Beweis. Setze $\alpha := \sqrt{d}$ primitives Element, $d \in \mathcal{O}_L$ und $\mathrm{MinPol}_{\mathbb{Q}}(\alpha) := f(x) = x^2 - d$. Seine Nullstellen sind
$x_{1,2} := \frac{-b \pm \sqrt{b^2-4ac}}{2a}$, also ist $D(f) = (x_1 - x_2)^2 = 4d$. Nun ist $4d = \underbrace{(\det P)^2}_{\in \mathbb{Z}} \underbrace{D(\mathcal{O}_L/\mathbb{Z})}_{\equiv 0,1 \bmod 4}$
$P \in M_{n\times n}(\mathbb{Z})$.

Behauptung: $D(\mathcal{O}_L/\mathbb{Z}) \equiv 0 \bmod 4$

Beweis. wenn $D(\mathcal{O}_L/\mathbb{Z}) \equiv 1$ wäre, wäre dann $(\det P)^2 \equiv 0$, aber dann $\underbrace{d}_{\equiv 2,3} = \underbrace{l^2}_{\equiv 0,1} \underbrace{D(\mathcal{O}_L/\mathbb{Z})}_{\equiv 1}$:
Widerspruch. □

Es gilt also $4d = (\det P)^2 \underbrace{D(\mathcal{O}_L/\mathbb{Z})}_{\equiv 0 \bmod 4}$. 4 auf beiden Seiten kürzen ergibt: $d = (\det P)^2 w$ und
d quadratfrei$\Rightarrow (\det P)^2 = 1$, also ist $\det P = \pm 1$, also ist $\{1, d\}$ eine Ganzheitsbasis. □

Fall 2: $d \equiv 1 \bmod 4$

Behauptung: $\{1, \frac{1+\sqrt{d}}{2}\}$ ist eine Ganzheitsbasis, also ist $\mathcal{O}_L = \mathbb{Z}[\omega]$, wobei $\omega = \frac{1}{2}(1+\sqrt{d})$

Beweis. $f = \mathrm{MinPol}_{\mathbb{Q}}(\omega) = x^2 - x + [\frac{1-d}{4}] \in \mathbb{Z}[x]$ und $D(f) = 1 - [4(\frac{1-d}{4})] = d$, d quadratfrei, also folgt nun unsere Behauptung aus Bemerkung 14.3(ii). □

Algebraische Zahlentheorie
Algebra B 4 - Sommersemester 2017
Prof'in Dr. Salma Kuhlmann

15.Vorlesung

26 Juni 2017

Beweis von Stickelberger.

Erinnerung (ÜB)**:** Sei L/K eine endliche separable Erweiterung, $\{\mu_1, \dots, \mu_n\}$ eine Basis, $n = [L : K]$, $\sigma_1, \dots, \sigma_n$ die verschiedene Einbettungen von L über K in Ω; dann gilt $\det(B_{L/K}(\mu_i, \mu_j)) = \underbrace{(\det(\sigma_i(\mu_j))^2}_{\neq 0} \in \mathbb{Z}$.
Sei nun $\{\mu_1, \dots, \mu_n\}$ eine Ganzheitsbasis von $\mathcal{O}_L$ über $\mathbb{Z}$; es ist

$$\begin{aligned} D(\mathcal{O}_L/\mathbb{Z}) &= [\sum_{\pi \in S_n} (\operatorname{sign}(\pi)\sigma_{\pi(1)}(\mu_1) \dots \sigma_{\pi(n)}(\mu_n)]^2 \\ &= [(\sum_{\pi \in A_n} \operatorname{sign}(\pi) \dots) + (\sum_{\pi \in S_n \setminus A_n} \operatorname{sign}(\pi))]^2 \\ &= (G - U)^2 \in \mathbb{Z} \end{aligned}$$

wobei $G := (\sum_{\pi \in A_n} \dots) \in \mathcal{O}_L \subseteq \Omega$ und $U := -(\sum_{\pi \in S_n \setminus A_n} \dots) \in \mathcal{O}_L \subseteq \Omega$.
Nun ist $L \subseteq \Omega$ galoissch. Für $\tau \in \operatorname{Gal}(\Omega/\mathbb{Q})$:

Bemerkung
$\sigma_1, \dots, \sigma_n : L \hookrightarrow \Omega$, sei $i \in \{1, \dots, n\}$, $L \xrightarrow{\sigma_i} \Omega \xrightarrow{\tau} \Omega$, also $\exists j \in \{1, \dots, n\}$, so daß $\tau \circ \sigma_i = \sigma_j$, also ist die Abbildung $\rho : i \mapsto j \quad (\rho(i) = j \Leftrightarrow \tau \circ \sigma_i = \sigma_j)$ eine Permutation, d.h $\rho \in S_n$.

Wir berechnen:

$$\begin{aligned} &\tau(\sigma_{\pi(1)}(\mu_1) \dots \sigma_{\pi(n)}(\mu_n)) = \\ &\tau \circ \sigma_{\pi(1)}(\mu_1) \dots \tau \circ \sigma_{\pi(n)}(\mu_n) = \\ &\sigma_{\rho\circ\pi(1)}(\mu_1) \dots \sigma_{\rho\circ\pi(n)}(\mu_n) \end{aligned}$$

Daraus folgt: $\rho \in A_n \Rightarrow \tau(G) = G, \tau(U) = U$ und $\rho \in S_n \setminus A_n \Rightarrow \tau(G) = U, \tau(U) = G$ und somit ist $\tau(G + U) = G + U$ und $\tau(GU) = GU \quad \forall \tau \in \operatorname{Gal}(\Omega/\mathbb{Q})$.
Nun $\Omega/\mathbb{Q}$ galoissch $\Rightarrow G + U, GU \in \operatorname{Inv}(\Omega/\mathbb{Q}) \underset{FSGT}{=} \mathbb{Q}$
$G + U, GU \in \mathbb{Q}$ und $\mathbb{Z}$ ganz abgeschlossen$\Rightarrow G + U, GU \in \mathbb{Z}$. Also ist
$D(\mathcal{O}_L/\mathbb{Z}) = (G - U)^2 = \underbrace{(G + U)^2}_{\in \mathbb{Z}} - \underbrace{4GU}_{\in 4\mathbb{Z}} \Rightarrow (G - U)^2 \equiv (G + U)^2 \bmod 4$ in $\mathbb{Z}$. □

Definition 15.1
Sei $L/\mathbb{Q}$ ein Zahlkörper. Eine Einbettung von L in $\mathbb{C}$ ist reell, wenn ihr Bild in $\mathbb{R}$ liegt; sonst ist sie komplex.

Bemerkung
Setze $L = \mathbb{Q}(\alpha)$, $[L : \mathbb{Q}] = n$, $f := \operatorname{MinPol}_{\mathbb{Q}}(\alpha)$, $f = \prod(x - \alpha_i) \in \mathbb{C}[X]$ mit r reellen Nullstellen und $2s$ komplexen Nullstellen, so daß $n = 2s + r$; dann hat L genau r relle Einbettungen in $\mathbb{C}$ und $2s$ komplexe Einbettungen in $\mathbb{C}$.

Satz (Satz von Brill)
(Ansatz wie oben) Es gilt $\text{sign}D(\mathcal{O}_L/\mathbb{Z}) = (-1)^s$

Beweis. Sei $\{\alpha_1, \ldots, \alpha_n\} \subseteq \mathcal{O}_L$ Basis für $L/\mathbb{Q}$ (es ist immer möglich, solch eine Basis zu finden, z.B. α primitives Element in $\mathcal{O}_L$ und $\alpha_i := \alpha^i$). Es ist
$D(\alpha_1, \ldots, \alpha_n) = (\det P)^2 D(\mathcal{O}_L/\mathbb{Z})$ ($P \in M_{n\times n}(\mathbb{Z})$ nicht unbedingt invertierbar). Insbesondere $\text{sign}D(\alpha_1, \ldots, \alpha_n) = \text{sign}D(\mathcal{O}_L/\mathbb{Z})$. Wir berechnen nun $\text{sign}D(1, \alpha, \ldots, \alpha^{n-1})$, d.h wir berechnen $\text{sign}D(f)$, wobei $f := \text{MinPol}_{\mathbb{Q}}(\alpha)$. Seien $\beta_1, \ldots, \beta_r, z_1, \ldots, z_s, \bar{z}_1, \ldots, \bar{z}_s$ alle Nullstellen von f in $\mathbb{C}$.

$$f = \prod(x - \alpha_i) = \prod_r (x - \beta_j) \prod_s (x - z_k) \prod_s (x - \bar{z}_k)$$

$$\underset{\text{Def 14. Vor.}}{\Rightarrow} D(f) = \prod_{i<j} (\beta_i - \beta_j)^2 \prod_{i,k} (\beta_i - z_k)^2 \prod_{i,k} (\beta_i - \bar{z}_k)^2 \prod_{k<l} (z_k - z_l)^2 \prod_{k,l} (z_k - \bar{z}_l)^2 \prod_{k<l} (\bar{z}_k - \bar{z}_l)^2$$

.
Bezeichnung: $\mathbb{R}_+ = \mathbb{R}^{>0}, \mathbb{R}_- := \mathbb{R}^{<0}$.
Nun ist $\prod_{i<j}(\beta_i - \beta_j)^2 \in \mathbb{R}^2 > 0$ ($\beta_i \neq \beta_j$),
$\underbrace{\prod_{i,k}(\beta_i - z_k)^2}_{:=w} \underbrace{\prod_{i,k}(\beta_i - \bar{z}_k)^2}_{\bar{w}} = w\bar{w} \in \mathbb{R}_+$.
Analog für $\prod_{k<l}(z_k - z_l)^2 \prod_{k<l}(\bar{z}_k - \bar{z}_l)^2 \in \mathbb{R}_+$, also bleibt $\prod_{k,l}(z_k - \bar{z}_l)^2$ übrig zu behandeln: ist $k \neq l$, dann erscheinen die Faktoren $z_k - \bar{z}_l$ sowie $z_l - \bar{z}_k$ im Produkt, also
$(z_k - \bar{z}_l)(z_l - \bar{z}_k)^2 = [-\underbrace{(z_k - \bar{z}_l)(\bar{z}_k - z_l)}_{\in \mathbb{R}^+}]^2 \in \mathbb{R}_+$. Letztendlich ist also
$\text{sign}(D(1, \alpha, \ldots, \alpha^{n-1})) = \text{sign}(\prod_{k=1}^s (z_k - \bar{z}_k)^2)$,
aber $z_k - \bar{z}_k \in i\mathbb{R}$, also ist $(z_k - \bar{z}_k)^2 \in \mathbb{R}_-$, also ist $\prod_{k=1}^s (z_k - \bar{z}_k)^2$ Produkt von s negativen reellen Zahlen, und damit ist sein Zeichen $(-1)^s$. □

Proposition 15.1
Sei L/K endlich separabel, $\sigma_1, \ldots, \sigma_n$ die Einbettungen von L über K in Ω, α primitives Element, $f := \text{MinPol}_K(\alpha)$, $\alpha_1, \ldots, \alpha_n$ die verschiedenen Nullstellen von f.
Es ist $D(f) = (-1)^{\frac{n(n-1)}{2}} N_{L/K}(f'(\alpha))$

Beweis. $f = \prod(x - \alpha_i) \Rightarrow$

$$(\ddagger) \qquad f' = \sum_{i=1}^n (\prod_{j\neq i} (x - \alpha_j)$$

Andererseits (per Definition der $N_{L/K}$) haben wir
$N_{L/K}(f'(\alpha)) = \prod_{k=1}^n \sigma_k(f'(\alpha)) = \prod_{k=1}^n (f'(\sigma_k(\alpha))) = \prod_{k=1}^n f'(\alpha_k)$.
Einsetzen von α_k in ($\ddagger$) ergibt
$f'(\alpha_k) = \prod_{j\neq k}(\alpha_k - \alpha_j)$, also ist
$N_{L/K}(f'(\alpha)) = \prod_{k=1}^n \prod_{j\neq k}(\alpha_k - \alpha_j)$. Wir vergleichen nun dieses Produkt mit
$D(f) = \prod_{j<k}(\alpha_k - \alpha_j)^2$. In $N_{L/K}(f'(\alpha))$ erscheint jede Differenz $(\alpha_k - \alpha_j)$ zweimal und zwar für (j, k) und (k, j). Wir berechnen nun: für jedes $k = 1, \ldots, n$, $j < k \Rightarrow (\alpha_j - \alpha_k)^2$ erscheint in $D(f)$. Dagegen erscheint
$(\alpha_j - \alpha_k)(\alpha_k - \alpha_j) = -(\alpha_j - \alpha_k)^2$ im Produk, d.h $\forall k = 1, \ldots, n$ und $j < k$ wird ein Faktor (-1) beigetragen, insgesamt also $(n-1) + (n-2) + \cdots + 0$ Beiträge. □

Proposition/Beispiel
Sei $f(x) = x^n + ax + b$ irreduzibel, α eine Nullstelle,
$L := \mathbb{Q}(\alpha)$, $n = [L : \mathbb{Q}]$. Setze $\gamma := f'(\alpha) = n\alpha^{n-1} + a$. Wir berechnen $N_{L/\mathbb{Q}}(\gamma)$ (damit wir eine Formel für $D(f)$ bekommen). Nun erfüllt α: $\alpha^n + a\alpha + b = 0$. Multiplizieren mit α^{-1} ergibt $\alpha^{n-1} + a + b\alpha^{-1} = 0$, also ist $\gamma = -n(a + b\alpha^{-1}) + a = -(n-1)a - (nb\alpha^{-1})$, d.h $\alpha = \frac{-nb}{\gamma+(n-1)a}$ und somit ist $L = \mathbb{Q}(\alpha) = \mathbb{Q}(\gamma)$ und $n = [\mathbb{Q}(\gamma) : \mathbb{Q}]$.
Andererseits ist $f(\frac{-nb}{x+(n-1)a}) = \frac{p(x)}{q(x)} \in \mathbb{Q}(x)$,
also $f(\alpha) = \frac{p(\gamma)}{q(\gamma)} = 0$ und somit ist $p(\gamma) = 0$. Nun ist aber
$p(x) = (x + (n-1)a)^n - na(x + (n-1)a)^{n-1} + (-1)^n n^n b^{n-1}$. Also ist $p(x)$ normiert, $\deg p = n$ und $p(\gamma) = 0$, d.h $p(x)$ ist das $\mathrm{MinPol}_{\mathbb{Q}}(\gamma)$. Wir berechnen nun (Lemma 11.2)
$N_{L/\mathbb{Q}}(\gamma) = (-1)^n(n-1)^n a^n - na(n-1)^{n-1}a^{n-1} + (-1)^n n^n b^{n-1}$
Also $N_{L/\mathbb{Q}}(\gamma) = n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n$
und $D(f) = (-1)^{\frac{n(n-1)}{2}}(n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n)$

Beispiel
$f(x) = x^3 - x - 1$ ist irreduzibel in $\mathbb{Q}[x]$. Sei $\alpha \in \mathbb{C}$ eine Nullstelle, berechne $D(1, \alpha, \alpha^2) = D(f) \overset{\text{Prop}}{=} -23$ ist quadratfrei, und $\alpha \in \mathcal{O}_L$ (weil $\mathrm{MinPol}_{\mathbb{Q}}(\alpha) = f(x) \in \mathbb{Z}[x]$), also ist $\{1, \alpha, \alpha^2\}$ eine Ganzheitsbasis von $\mathcal{O}_L$ über $\mathbb{Z}$ und $\mathcal{O}_L = \mathbb{Z}[\alpha]$.

Algebraische Zahlentheorie
Algebra B 4 - Sommersemester 2017
Prof'in Dr. Salma Kuhlmann

16.Vorlesung

29 Juni 2017

Kapitel 4: Dedekindringe

Definition 16.1
Ein Ring R ist ein Dedekindring, wenn R ein Integritätsbereich ist und jedes Ideal ein Produkt von Primidealen ist.

Notation (Erinnerung)
$I, J \lhd R$, dann ist
$IJ := \{\sum_{i=1}^{n} x_i y_j \mid x_i \in I, y_j \in J, n \in \mathbb{N}\} \lhd R$.

Beispiel 1. HIR

2. R Dedekindring und $0 \neq S \subseteq R$ multiplikativ $\Rightarrow S^{-1}R$ Dedekindring.

3. Wir werden zeigen: sei R ein Dedekindring und $K = \text{Quot}(R)$, L/K endlich separabel, dann ist $\overline{R}^L$ ein Dedekindring

Definition 16.2 (i) Sei R integer und $K = \text{Quot}(R)$. Ein R-Untermodul $B \subseteq K$ heißt gebrochenes Ideal, wenn es $d \in R$ mit $d \neq 0$ gibt, so daß $B \subseteq \frac{1}{d}R$.

(ii) Ideale in R sind auch gebrochene Ideale ($d = 1$), wir nennen sie ganze Ideale.

(iii) Sei $x = \frac{a}{b} \in K$, $a, b \in R, b \neq 0$. Dann ist $B := Rx$ ein gebrochenes Hauptideal.

Bemerkung (i) B ist ein gebrochenes Ideal $\Leftrightarrow \exists d \neq 0$ in R und $A \lhd R$ so daß $B = (\frac{1}{d})A$.

(ii) Die Idealoperationen $+, ., \cap$ sind auf gebrochenen Idealen wohldefiniert:

$$B \subseteq (\tfrac{1}{d})R, B' \subseteq (\tfrac{1}{d'})R \Rightarrow \begin{cases} B + B' \subseteq (\frac{1}{dd'})R \\ BB' \subseteq (\frac{1}{dd'})R \\ B \cap B' \subseteq (\frac{1}{d})R \end{cases}$$

genauer: $BB' = (\frac{1}{dd'})IJ$ $I, J \lhd R$, wobei $B = (\frac{1}{d})I$ und $B' = (\frac{1}{d'})J$.

Definition 16.3
Das gebrochene Ideal B ist invertierbar, wenn es ein gebrochenes Ideal B' gibt mit
$BB' = R \quad (*)$.

Bemerkung (i) B invertierbar$\Rightarrow \exists! B'$, das $(*)$ erfüllt ($BB' = BB'' = R \Rightarrow B' = B''$). Wir bezeichnen $B' := B^{-1}$.

(ii) Ein gebrochenes Hauptideal $B = xR$ mit $x \in K$ und $x \neq 0$ ist invertierbar mit $B^{-1} = x^{-1}R$.

Notation
Seien B, B' gebrochene Ideale. Setze $(B : B') := \{x \in K \mid xB' \subseteq B\}$

Bemerkung
$(B : B')$ ist ein R-Modul. Wenn $B' \neq \{0\}$, $B \subseteq \frac{1}{d}R$ und $a \in B'(d \neq 0, a \neq 0)$, dann ist $(B : B') \subseteq \frac{1}{da}R$.

Lemma 16.1
Ist A ein invertierbares gebrochenes Ideal, gilt dann $A^{-1} = (R : A)$
(Also: A invertierbar$\Leftrightarrow A.(R : A) = R$)

Beweis. Sei $AA' = R$. Dann ist $A' \subseteq (R : A)$. Andererseits ist $A.(R : A) \subseteq R$. Es folgt $(R : A) = A'A(R : A) \subseteq A'R = A'$ □

Lemma 16.2
Ist jedes ganzes Ideal$\neq 0$ invertierbar, ist dann jedes $\neq 0$ gebrochenes Ideal invertierbar.

Beweis. Sei $B = \frac{1}{d}A$ ein gebrochenes Ideal (mit $A \lhd R, d \in R, d \neq 0$), dann ist $B^{-1} = dA^{-1}$. □

Lemma 16.3
Ein invertierbares gebrochenes Ideal ist ein endlich erzeugter R-Modul.

Beweis. $AA^{-1} = R \Rightarrow \exists\{x_i\} \subseteq A$ und $\{x_i'\} \subseteq A^{-1}$, so daß $\sum x_i x_i' = 1$. Es folgt:
$x \in A \Rightarrow x = 1x = \sum \underbrace{xx_i'}_{\in R} x_i$. □

Definition 16.4
Die (multiplikative) Gruppe $\mathcal{J}$ der invertierbaren ($\neq 0$) gebrochenen Ideale, geteilt durch die Untergruppe der gebrochenen Hauptideale $\mathcal{H}$, heißt die Klassengruppe von R.
Ihre Ordnung heißt die Klassenzahl von R.
$(\mathcal{K}l(R) = \mathcal{J}/\mathcal{H}, |\mathcal{K}l(R)| = h_R)$.

Beispiel 16.1
Sei R ein HIR. Dann ist die Klassengruppe trivial und die Klassenzahl 1.

Algebraische Zahlentheorie
Algebra B 4 - Sommersemester 2017
Prof'in Dr. Salma Kuhlmann

17.Vorlesung

3 Juli 2017

Sei R ein Integritätsbereich.

Lemma 17.1
Sei $\{A_i\}$ eine endliche Menge von $\neq 0$ ganzen Idealen, so daß $B := \prod_i A_i$ invertierbar ist . Dann ist A_i invertierbar für jedes i. Insbesondere gilt: Ist das Produkt B ein Hauptideal, so ist jedes A_i invertierbar.

Beweis. $B^{-1}(\prod_i A_i) = R \Rightarrow A_i \underbrace{(B^{-1} \prod_{j \neq i} A_j)}_{:=A_i^{-1}} = R$ □

Lemma 17.2
Für Produkte von invertierbaren (ganzen) Primidealen ist die Faktorisierung als Produkt von Primidealen eindeutig.

Bemerkung 17.1
Sei $\mathfrak{p} \lhd R$ ein Primideal und $I, J \lhd R$. Es ist: $\mathfrak{p} \supseteq IJ \Rightarrow \mathfrak{p} \supseteq I$ oder $\mathfrak{p} \supseteq J$.

Beweis von Lemma 17.2. Sei $A = \prod_i \mathfrak{p}_i$, $\mathfrak{p}_i$ invertierbar (ganze) Primideale Sei $A = \prod_i \mathfrak{q}_i$, wobei $\mathfrak{q}_i$ Primideale sind.
Sei $\mathfrak{p}_1$ ein minimales (für Inklusion) Mitglied von $\{\mathfrak{p}_i\}$. Aus $\prod_j \mathfrak{q}_j \subseteq \mathfrak{p}_1$ folgt o.E. $\mathfrak{q}_1 \subseteq \mathfrak{p}_1$. Analog folgt aus $\prod_i \mathfrak{p}_i \subseteq \mathfrak{q}_1$, daß $\mathfrak{p}_r \subseteq \mathfrak{q}_1$ für ein geeignetes r, also ist $\mathfrak{p}_r \subseteq \mathfrak{q}_1 \subseteq \mathfrak{p}_1$. Aus der Minimalität folgt nun $\mathfrak{p}_r = \mathfrak{p}_1 = \mathfrak{q}_1$, also $\mathfrak{p}_1^{-1}(\prod_i \mathfrak{p}_i) = \mathfrak{q}_1^{-1}(\prod_j \mathfrak{q}_j)$ und damit bekommen wir : $\prod_{i \neq 1} \mathfrak{p}_i = \prod_{j \neq 1} \mathfrak{q}_j$. Per Induktion fortsetzen. □

Satz 17.3
Sei R ein Dedekindring und $\mathfrak{p}$ ein echtes Primideal ($\mathfrak{p} \neq \{0\}, \mathfrak{p} \neq R$). Dann ist $\mathfrak{p}$ invertierbar und maximal.

Beweis.

Behauptung 1: Sei $\mathfrak{p}$ ein echtes invertierbares Primideal. Dann ist $\mathfrak{p}$ maximal.

Beweis. Sei $a \in R$, $a \notin \mathfrak{p}$ und betrachte die Ideale $\mathfrak{p} + Ra$ und $\mathfrak{p} + Ra^2$. Da R ein Dedekindring ist, haben wir eine Faktorisierung $\mathfrak{p} + Ra = \prod_{i=1}^n \mathfrak{p}_i$ und $\mathfrak{p} + Ra^2 = \prod_{j=1}^m \mathfrak{q}_j$ mit $\mathfrak{p}_i, \mathfrak{q}_j$ Primideale. Setze $\overline{R} := R/\mathfrak{p}$ und $\bar{a} := a \bmod \mathfrak{p}$. Wir haben:

$(*)$ $\overline{R}.\bar{a} = \prod(\mathfrak{p}_i/\mathfrak{p})$

$(**)$ $\overline{R}.\bar{a}^2 = \prod(\mathfrak{q}_j/\mathfrak{p})$

und $\mathfrak{p}_i/\mathfrak{p}, \mathfrak{q}_j/\mathfrak{p}$ sind Primideale. Nun sind $\overline{R}.\bar{a}$ und $\overline{R}.\bar{a}^2$ Hauptideale, also sind sie invertierbar und es folgt (Lemma 17.1): $\mathfrak{p}_i/\mathfrak{p}$ und $\mathfrak{q}_j/\mathfrak{p}$ sind alle invertierbar. Aber

$$(***) \qquad \overline{R}\bar{a}^2 = (\overline{R}\bar{a})^2 = \prod_{i=1}^{n} (\mathfrak{p}_i/\mathfrak{p})^2$$

Vegleiche $(*), (**)$ und $(***)$. Es folgt nun (Lemma 17.2): Die Ideale $\{\mathfrak{q}_j/\mathfrak{p}\}$ sind die Ideale $\{\mathfrak{p}_i/\mathfrak{p}\}$ wiederholt zweimal, d.h. $m = 2n$ und wir können umnummerieren, so daß o.E: $\mathfrak{q}_{2i}/\mathfrak{p} = \mathfrak{q}_{2i-1}/\mathfrak{p} = \mathfrak{p}_i/\mathfrak{p}$. Es folgt: $\mathfrak{q}_{2i} = \mathfrak{q}_{2i-1} = \mathfrak{p}_i$. Wir bekommen:

$$(0) \qquad \mathfrak{p} + Ra^2 = \prod_{j=1}^{m} \mathfrak{q}_j = \prod_{i=1}^{n} \mathfrak{p}_i^2 = (\mathfrak{p} + Ra)^2$$

Daraus folgt

$$(\dagger) \qquad \mathfrak{p} \underset{(1)}{\subseteq} (\mathfrak{p} + Ra)^2 \underset{(2)}{\subseteq} \mathfrak{p}^2 + Ra$$

Begründung für (1): $\mathfrak{p} \subseteq \mathfrak{p} + Ra^2$ gilt immer, nun folgt (1) aus (0).
Begründung für (2): I.A. gilt Distributivitätsgesetz für Ideale I, J_1, J_2: $I(J_1 + J_2) = IJ_1 + IJ_2$. Insbesondere gilt hier:

$$\begin{aligned}(\mathfrak{p} + Ra)(\mathfrak{p} + Ra) &= (\mathfrak{p} + Ra)\mathfrak{p} + (\mathfrak{p} + Ra)Ra \\ &= \mathfrak{p}^2 + (\mathfrak{p}Ra + \mathfrak{p}Ra) + RaRa\end{aligned}$$

Nun ist $RaRa = a^2R$ und (da $I + I = I$ immer gilt)
$\mathfrak{p}Ra + \mathfrak{p}Ra = \mathfrak{p}Ra$, also $(\mathfrak{p} + Ra)^2 = \mathfrak{p}^2 + \mathfrak{p}Ra + Ra^2$. Da offensichtlich $\mathfrak{p}Ra \subseteq Ra$ und $Ra^2 \subseteq Ra$, bekommen wir:
$(\mathfrak{p} + Ra)^2 \subseteq \mathfrak{p}^2 + Ra + Ra = \mathfrak{p}^2 + Ra$.
Aus $(\dagger)$ folgt: $\forall x \in \mathfrak{p} \exists y \in \mathfrak{p}^2, z \in R$ mit $x = y + za$, also $za = \underbrace{x - y}_{\in \mathfrak{p}}$, aber $a \notin \mathfrak{p}$, also $z \in \mathfrak{p}$. D.h.:
$\mathfrak{p} \subseteq \mathfrak{p}^2 + \mathfrak{p}a$. Die andere Inklusion $\mathfrak{p} \supseteq \mathfrak{p}^2 + \mathfrak{p}a$ ist offensichtlich, also $\mathfrak{p} = \mathfrak{p}^2 + \mathfrak{p}a = \mathfrak{p}(\mathfrak{p} + Ra)$.
Da $\mathfrak{p}$ per Annahme invertierbar ist, folgt: $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}^{-1}\mathfrak{p}(\mathfrak{p} + Ra)$, d.h. $R = \mathfrak{p} + Ra$.
Da $a \in R \backslash \mathfrak{p}$ beliebig ist, folgt nun: $\mathfrak{p}$ ist maximal.

□

Behauptung 2: Jedes echtes Primideal ist invertierbar

Beweis. Sei $0 \neq b \in \mathfrak{p}$ und schreibe $Rb = \prod_i \mathfrak{p}_i$ mit $\mathfrak{p}_i$ Primideal (da R Dedekindring ist). Aus Lemma 17.1 folgt: jedes $\mathfrak{p}_i$ ist invertierbar. Aus Behauptung 1 folgt: jedes $\mathfrak{p}_i$ ist maximal. Da aber $\mathfrak{p} \supseteq \prod_i \mathfrak{p}_i$ ist, folgt o.E., daß $\mathfrak{p} \supseteq \mathfrak{p}_1$ und damit $\mathfrak{p} = \mathfrak{p}_1$ und $\mathfrak{p}$ ist invertierbar. □

□

Korollar 17.4
Sei R ein Dedekindring, dann ist die Faktorisierung von Idealen (als Produkt von Primidealen) eindeutig.

Beweis. Folgt unmittelbar aus Lemma 17.2 und Satz 17.3. □

Korollar 17.5
Sei R ein Dedekindring. Jedes $\neq 0$ gebrochenes Ideal ist invertierbar.

Beweis. Jedes (ganzes) Ideal $\neq 0$ ist Produkt von (invertierbaren) Primidealen, also ist jedes $\neq 0$ (ganzes) Ideal invertierbar und damit (Lemma 16.2) ist auch jedes gebrochenes Ideal $\neq 0$ invertierbar. □

Satz 17.6
Sei R ein Integritätsbereich. Es ist:
R ist ein Dedekindring$\Leftrightarrow$ jedes Ideal $\neq 0$ in R ist invertierbar.

Beweis. "$\Rightarrow$" folgt aus Satz 17.3 (beziehungsweise Korollar 17.5).
"$\Leftarrow$" Lemma 16.3 impliziert, daß R noethersch ist (jedes Ideal ist endlich erzeugt). Wir zeigen nun: jedes echtes Ideal ist Produkt von maximalen Idealen (insbesondere ist R ein Dedekindring). Sonst ist die Menge der echten Idealen, die kein solches Produkt sind, nicht leer. Sei $\mathfrak{a} \neq 0$ ein maximales Element davon ($\mathfrak{a}$ existiert, weil R noethersch ist). Da $\mathfrak{a}$ kein maximales Ideal ist, ist $\mathfrak{a}$ in einem maximalen Ideal $\mathfrak{m}$ strikt enthalten. Betrachte nun das (gebrochene) Ideal $\mathfrak{m}^{-1}\mathfrak{a}$.

Behauptung 1: $\mathfrak{m}^{-1}\mathfrak{a}$ ist ein ganzes Ideal.

Beweis. $\mathfrak{a} \subseteq \mathfrak{m} \Rightarrow \mathfrak{m}^{-1}\mathfrak{a} \subseteq R$. Bemerke nun: wenn I ein gebrochenes Ideal ist und $I \subseteq R$, ist dann $I \lhd R$. □

Behauptung 2: $\mathfrak{m}^{-1}\mathfrak{a} \supsetneq \mathfrak{a}$

Beweis. Es ist klar, daß $\mathfrak{m}^{-1}\mathfrak{a} = \mathfrak{a} \Rightarrow \mathfrak{m}\mathfrak{a} = \mathfrak{a}$; das ist aber wegen Hilfslemma (siehe hier weiter unten) unmöglich. □

Es folgt: $\mathfrak{m}^{-1}\mathfrak{a}$ ist ein Produkt von maximalen Idealen (folgt aus der Wahl von $\mathfrak{a}$), und damit ist $\mathfrak{a} = \mathfrak{m}(\mathfrak{m}^{-1}\mathfrak{a})$ auch solch ein Produkt: Widerspruch zur Wahl von $\mathfrak{a}$.

□

Hilfslemma
Seien $\mathfrak{a}, \mathfrak{m}$ Ideale in einem Ring R mit $\mathfrak{a}$ endlich erzeugt und $\mathfrak{m}\mathfrak{a} = \mathfrak{a}$. Dann existiert $z \in \mathfrak{m}$, so daß $(1 - z)\mathfrak{a} = 0$ (Insbesondere ist $\mathfrak{m}\mathfrak{a} = \mathfrak{a}$ unmöglich, wenn $1 \notin \mathfrak{m}$,$\mathfrak{a} \neq 0$ und R ein Integritätsbereich ist).

Beweis. Sei $\{x_1, \ldots, x_n\}$ erzeugend für $\mathfrak{a}$ und $\mathfrak{a}_i$ das von $\{x_i, \ldots, x_n\}$ erzeugte Ideal (also $\mathfrak{a} = \mathfrak{a}_1$), und setze $\mathfrak{a}_{n+1} = \{0\}$. Wir zeigen per Induktion über i: $\exists z_i \in \mathfrak{m}$, so daß $(1 - z_i)\mathfrak{a} \subseteq \mathfrak{a}_i$ (dann ist $z := z_{n+1}$ das gesuchte Element).
Für $i = 1$ setze $z_1 = 0$.
Aus $(1 - z_i)\mathfrak{a} \subset \mathfrak{a}_i$ und $\mathfrak{a} \subset \mathfrak{m}\mathfrak{a}$ folgt $(1 - z_i)\mathfrak{a} \subseteq \mathfrak{m}\mathfrak{a}_i$. Insbesondere gilt $(1 - z_i)x_i = \sum_{j=i}^{n} z_{ij}x_j$ für geeignete $z_{ij} \in \mathfrak{m}$, also ist $(1 - z_i - z_{ii})x_i \in \mathfrak{a}_{i+1}$ und wir können nehmen:
$1 - z_{i+1} := (1 - z_i)(1 - z_i - z_{ii})$. □

Algebraische Zahlentheorie
Algebra B 4 - Sommersemester 2017
Prof'in Dr. Salma Kuhlmann

18.Vorlesung

6 Juli 2017

Satz 18.1
Sei R ein Integritätsbereich. Dann ist
R Dedekindring $\Leftrightarrow$ R erfüllt:

1. R ist noethersch
2. Jedes echte Primideal ist maximal
3. R ist ganz abgeschlossen.

Beweis. „$\Rightarrow$“

1. folgt aus Kor 17.5 und Lemma 16.3
2. folgt aus Satz 17.6
3. Setze $K := \text{Quot}(R)$, sei $a \in K$ und $f(x) \in R[x]$ normiert mit $f(a) = 0$, $\deg(f) = n$. Setze $M := R + Ra + \cdots + Ra^{n-1}$, schreibe $a = \frac{b}{c}$, $b, c \in R$. Dann ist $c^{n-1}M \subseteq R$, somit ist M ein gebrochenes Ideal. Außerdem gilt $M^2 = M$ (prüfe!) und M^{-1} existiert, also ist $M^{-1}M^2 = R$, d.h $M = R$. Da $a \in M$, gilt nun $a \in R$.

„$\Leftarrow$“ Wir zeigen 1.+2.+3.$\Rightarrow$ jedes $\neq 0$ gebrochenes Ideal ist invertierbar. Sei also I ein gebrochenes Ideal. Setze $I^* := (R : I)$

Erinnerung: $(R : I) = \{x \in K \mid xI \subseteq R\}$. Ein gebrochenes Ideal I ist invertierbar $\Leftrightarrow$ $II^* = R$. Allgemein gilt $II^* \lhd R$.

Betrachte das (ganze) Ideal I^*I. Es gelten: $II^*(II^*)^* \subseteq R$, also $I(I^*(II^*)^*) \subseteq R$ also
$I^*(II^*) \subseteq I^*$ per Definition von I^*. Setze $S := \{x \in K \mid xI^* \subseteq I^*\}$. Es ist: $S \subseteq R$ (siehe Hilfslemma 18.3 hier weiter unten). Wir bekommen also :
$(II^*)^* \subseteq S \subseteq R$
Wenn $II^* = R$ gilt, ist I invertierbar und wir sind fertig, sonst ist $II^* \lhd R$, aber dann ist (wegen Hilfslemma 18.4) $(II^*)^* \supsetneq R$: Widerspruch. □

Wir beweisen nun die Hilfslemmata.

Hilfslemma 18.1
Ein gebrochenes ideal von einem noetherschen Integritätsbereich R ist ein endlich erzeugter R-Modul.

Beweis. Setze $I = \frac{1}{d}I'$, wobei $d \in R, d \neq 0$ und $I' \lhd R$. R noethersch $\Rightarrow$ I' ist endlich erzeugt mit erzeugender Menge $\{x_1, \ldots, x_r\}$. Dann ist offensichtlich $\{\frac{x_1}{d}, \ldots, \frac{x_r}{d}\}$ erzeugend für I. □

Hilfslemma 18.2
Ein $\neq 0$ ideal in einem noetherschen Ring enthält ein Produkt von $\neq 0$ Primidealen.

Beweis. Sonst ist die Menge der $\neq 0$ Ideale, die kein solches Produkt enthalten, nicht leer. Da R noethersch ist, sei $0 \neq I$ ein maximales Mitglied davon. Da I kein Primideal ist, gibt es Ideale I_1, I_2, so daß $I_1 I_2 \subseteq I$, aber $I_1 \supsetneq I$ und $I_2 \supsetneq I$ (z.B. $\exists a, b \in R$, so daß $ab \in I$, aber $a \notin I$ und $b \notin I$, setze $I_1 := I + Ra$ und $I_2 := I + Rb$).
Aus der Wahl von I folgt: I_1 und I_2 enthalten ein Produkt von $\neq 0$ Primidealen, und somit enthält $I \supseteq I_1 I_2$ auch solch ein Produkt. Widerspruch zur Wahl von I. □

Hilfslemma 18.3
Sei R ein ganz abgeschlossener noetherscher Integritätsbereich, $K = \text{Quot}(R)$, $I \subseteq K$ ein gebrochenes Ideal von R; dann ist $S := \{x \in K \mid xI \subseteq I\} = R$

Beweis. Sei $x \in S$. Wegen Hilfslemma 18.1 ist I ein endlich erzeugter R-Modul. Aus $xI \subseteq I$ und Proposition 9.1 folgt: x ist ganz über R. Da R ganz abgeschlossen ist folgt: $x \in R$. Also $S \subseteq R$. Da offensichtlich $R \subseteq S$, haben wir $R = S$. □

Hilfslemma 18.4
Sei R ein noetherscher Integritätsbereich, so daß jedes $\neq 0$ Primideal ein Maximalideal ist. Sei $I \lhd R$. Dann ist $I^* \supsetneq R$.

Bemerkung
Da $I \lhd R$, ist es klar, daß $I^* \supseteq R$. Wir zeigen $I^* \neq R$.

Beweis. Sei $a \neq 0, a \in I$, so daß $R \supseteq I \supseteq aR$. Hilfslemma 18.2 liefert $aR \supseteq \mathfrak{p}_1 \dots \mathfrak{p}_m$, $\mathfrak{p}_i \neq 0$ Primideale; o.E. sei m minimal. Sei $\mathfrak{p} \supseteq I$ Maximalideal, also $\mathfrak{p} \supseteq I \supseteq aR \supseteq \prod_{i=1}^m \mathfrak{p}_i$. Da beide $\mathfrak{p}$ und $\mathfrak{p}_i$ Primideale sind, folgt aus unserer Annahme, daß $\mathfrak{p} = \mathfrak{p}_i$ für geeignetes i. ($\mathfrak{p}$ Primideal und $\mathfrak{p} \supseteq \prod_i \mathfrak{p}_i \Rightarrow \exists i, \mathfrak{p} \supseteq \mathfrak{p}_i$, aber $\mathfrak{p}_i$ Maximalideal $\Rightarrow \mathfrak{p} = \mathfrak{p}_i$).
Also ist o.E. $\mathfrak{p} = \mathfrak{p}_1$. Wenn $m = 1$, dann ist $aR = I$ und $I^* = I^{-1} = a^{-1}R$, und da $I \subsetneq R$, ist $a^{-1} \notin R$, also $I^{-1} \supsetneq R$. Wenn $m > 1$: dann ist $aR \not\supseteq \mathfrak{p}_2 \dots \mathfrak{p}_m$ per Minimalität von m, wähle $b \in \prod_{i=2}^m \mathfrak{p}_i$, aber $b \notin aR$ und setze $c := a^{-1}b$. Dann ist $c \notin R$ und $cI \subseteq c\mathfrak{p} = a^{-1}b\mathfrak{p} \subseteq a^{-1}\mathfrak{p} \prod_{i=2}^m \mathfrak{p}_i \subseteq a^{-1}(aR) = R$. Wir haben gezeigt: $c \in I^*$, also $I^* \supsetneq R$. □

Satz 18.2
Sei R ein Dedekindbereich, $K = \text{Quot}(R)$, L/K eine endliche separable Erweiterung. Dann ist $\overline{R}^L$ ein Dedekindbereich.

Bemerkung
Wir zeigen, daß $\overline{R}^L$ 1. + 2. + 3. von Satz 18.1 erfüllt.

Beweis. 1. $\overline{R}^L$ ist noethersch:

Satz 13.Vorlesung $\Rightarrow M \subseteq \overline{R}^L \subseteq M'$, also ist $\overline{R}^L$ in einem endlich erzeugten R-Modul M' enthalten, und da R noethersch ist, folgt (aus Korollar 8.3), daß M' ein noetherscher R-Modul ist. D.h.: $\overline{R}^L$ ist ein Untermodul eines noetherschen R-Modul. Es folgt: jedes Ideal in $\overline{R}^L$ ist endlich erzeugt als R-Modul (und a fortiori als $\overline{R}^L$-Modul), d.h.: $\overline{R}^L$ ist noethersch.

3. $\overline{R}^L$ ist ganz abgeschlossen: Korollar 10.5.

2. Jedes $\neq 0$ Primideal von $\overline{R}^L$ ist ein Maximalideal:

   Sei $0 \neq \mathfrak{q}$ ein Primideal, $\beta \neq 0$, $\beta \in \mathfrak{q}$, β ganz über R. Es existiert $a_i \in R$, so daß $\beta^n + a_1\beta^{n-1} + \dots + a_n = 0$ mit n minimal, $a_n \neq 0, a_n \in \beta\overline{R}^L \cap R$, so daß $\mathfrak{p} := \mathfrak{q} \cap R \neq \{0\}$ Primideal in R, also ist $\mathfrak{p}$ ein Maximalideal in R, also ist $R/\mathfrak{p}$ ein Körper. Nun ist $\overline{R}^L/\mathfrak{q}$ ein Integritätsbereich und die Einbettung

$$\begin{array}{rcl} R/\mathfrak{p} & \hookrightarrow & \overline{R}^L/\mathfrak{q} \\ a+\mathfrak{p} & \mapsto & a+\mathfrak{q} \end{array}$$

liefert: $R/\mathfrak{p}$ ist isomorph zu einem Unterkörper von $\overline{R}^L/\mathfrak{q}$. Außerdem ist $\overline{R}^L/\mathfrak{q}$ algebraisch über $R/\mathfrak{p}$ (weil $\overline{R}^L$ ganz über R ist). Es folgt nun aus dem nächsten Hilfslemma, daß $\overline{R}^L/\mathfrak{q}$ ein Körper ist; $\mathfrak{q}$ ist maximal.

□

Hilfslemma 18.5
Sei D ein Integritätsbereich, $k \subseteq D$ ein Unterkörper, so daß D/k algebraisch ist. Dann ist D ein Körper.

Algebraische Zahlentheorie
Algebra B 4 - Sommersemester 2017
Prof'in Dr. Salma Kuhlmann

19.Vorlesung

10 Juli 2017

Beweis vom Hilfslemma am Ende der 18.Vorlesung. Sei $0 \neq \beta \in D$. Da β algebraisch über k ist, ist $k[\beta]$ ein endlichdimensionaler K-Vektorraum. Die Abbildung $\begin{array}{ccc} k[\beta] & \to & k[\beta] \\ x & \mapsto & \beta x \end{array}$ ist linear und injektiv (weil D ein Integritätsbereich ist), also folgt aus LA: Die Abbildung ist surjektiv. Insbesondere gibt es $\beta' \in k[\beta]$, so daß $\beta\beta' = 1 \in k[\beta]$

□

Notation und Termonologie
Zusammenfassung: Gebrochene Ideale in einem Dedekindbereich.
Sei R ein Dedekindbereich, $K :=$ Quot(R). Die Menge Id(R) der $\neq 0$ gebrochenen Ideale von R ist eine abelsche Gruppe, sie enthält die Untergruppe $H(R)$ der gebrochenen Hauptideale. Die Faktorgruppe $\mathcal{K}l(R) :=$ Id$(R)/H(R)$ heißt die Ideal Klassengruppe von R. Ihre Ordnung $|\mathcal{K}l(R)|$ heißt die Klassenzahl von R.

Proposition 19.1
Ein Dedekindbereich ist genau dann faktoriell, wenn es ein Hauptidealbereich ist (d.h.: Ein Dedekindbereich hat Klassenzahl = 1 genau dann, wenn er faktoriell ist).

Beweis. Sei R ein Dedekindbereich.
„⇐“ Jedes HIR ist faktoriell.
„⇒“ Sei nun R faktoriell; es genügt zu zeigen, daß jedes $\neq 0$ Primideal $\mathfrak{p}$ ein Hauptideal ist (da jedes Ideal ein Produkt von Primidealen ist, und das Produkt von Hauptidealen ein Hauptideal ist). Sei $0 \neq a \in \mathfrak{p}$; dann ist a ein Produkt von irreduziblen Elementen. Da $\mathfrak{p}$ ein Primideal ist, enthält $\mathfrak{p}$ ein Primfaktor π von a. Nun folgt aus $\mathfrak{p} \supseteq < \pi >$, daß $\mathfrak{p} = < \pi >$, weil $< \pi >$ ein Primideal, also ein Maximalideal ist (R ist Dedekind). □

Zusatz: Sei R ein Dedekindbereich. Jedes $\neq 0$ gebrochenes Ideal hat eine eindeutige Faktorisierung als Produkt von ganzen Potenzen von Primidealen.

Beweis. Sei $\mathfrak{a}$ ein gebrochenes Ideal und $d \neq 0$, $d \in R$, so daß $d\mathfrak{a} \lhd R$. Schreibe eindeutig
$d\mathfrak{a} = p_1^{r_1} \dots p_m^{r_m}$, p_i Primideal, $r_i \in \mathbb{N}_0$,
$< d >= p_1^{s_1} \dots p_m^{s_m}$, $s_i \in \mathbb{N}_0$. Dann ist $\mathfrak{a} = \prod_{i=1}^m p_i^{r_i - s_i}$, $r_i - s_i \in \mathbb{Z}$. □

Kapitel 5: Die Klassenzahl eines Zahlkörpers

§Gitter in $\mathbb{R}^n$

Definition 19.1 (i) Sei $\{e_1, \ldots, e_m\}$ linear unabhängig in $\mathbb{R}^n$ (also $m \leq n$). Die von $\{e_1, \ldots, e_m\}$ erzeugte additive Gruppe Γ ist ein Gitter der Dimension m. D.h.: $\Gamma := \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_m$ (freie abelsche Gruppe vom Rang m).

Wenn $m = n$ heißt Γ vollständiges Gitter
Bezeichnung: $||x||$ ist die euklisdische Norm für $x \in \mathbb{R}^n$.

(ii) $X \subseteq \mathbb{R}^n$ ist beschränkt, wenn es ein $r \in \mathbb{R}_+$ gibt, so daß $X \subseteq B_r(0)$:=die Kugel mit Zentrum 0 und Radius r.

(iii) $X \subseteq \mathbb{R}^n$ ist diskret, wenn $|B_r(0) \cap X| < \infty$ für alle $r \in \mathbb{R}_+$.

Satz 19.1
Eine additive Untergruppe Γ von $(\mathbb{R}^n, +)$ ist genau dann ein Gitter, wenn Γ diskret ist.

Beweis. „$\Rightarrow$“ o.E. ist Γ vollständig. Sei $\{e_1, \ldots, e_n\}$ eine Basis für $\mathbb{R}^n$, die Γ erzeugt, und $v \in \mathbb{R}^n$. Es gibt $\lambda_i \in \mathbb{R}$, so daß $v = \sum_{i=1}^n \lambda_i e_i$.
Definiere:

$$\begin{array}{lccc} f & : \mathbb{R}^n & \to & \mathbb{R}^n \\ & f(\sum \lambda_i e_i) & \mapsto & (\lambda_1, \ldots, \lambda_n) \end{array}$$

Es ist : $f(B_r(0))$ ist beschränkt, d.h. es existiert k, so daß $||f(v)|| \leq k \quad \forall v \in B_r(0)$.
Wenn $v = \sum_{i=1}^n a_i e_i \in \Gamma \cap B_r(0)$ $(a_i \in \mathbb{Z})$, dann ist $||(a_1, \ldots, a_n)|| \leq k$. Es folgt:

$$(*) \qquad |a_i| \leq k \quad \forall i = 1, \ldots, n$$

Wir sehen, daß die Anzahl von $a \in \mathbb{Z}$, die $(*)$ erfüllen können, endlich ist, also ist $\Gamma \cap B_r(0)$ endlich.
„$\Leftarrow$“ Wir zeigen per Induktion nach n, daß Γ ein Gitter ist. Sei $\{g_1, \ldots, g_m\}$ eine maximal linear unabhängige Untermenge von Γ und setze $V := \text{Span}_{\mathbb{R}}\{g_1, \ldots, g_{m-1}\}$. Betrachte $\Gamma_0 := \Gamma \cap V$. Dann ist Γ_0 immernoch diskret und per Induktionsannahme ein Gitter. Seien $\{h_1, \ldots, h_{m'}\}$ eine linear unabhängige Menge, die Γ_0 erzeugt. Da $g_1, \ldots, g_{m-1} \in \Gamma_0$, muss $m' = m - 1$ gelten. Wir können $\{g_1, \ldots, g_{m-1}\}$ durch $\{h_1, \ldots, h_{m-1}\}$ erzetzen. (D.h.: wir können o.E. annehmen: jedes Element aus Γ_0 ist eine $\mathbb{Z}$-lineare Kombination der g_i).
Betrachte nun die Untermenge von Γ:
$T := \{x \in \Gamma \mid x = \sum_{i=1}^m a_i g_i, a_i \in \mathbb{R}, 0 \leq a_i < 1, i = 1, \ldots, m-1 \text{ und } 0 \leq a_m \leq 1\}$.
T ist beschränkt (also endlich, da Γ diskret ist). Wähle $x' \in T, x' = \sum_{i=1}^m b_i g_i$ mit b_m kleinste $\neq 0$ Koeffizient von g_m.

Behauptung: $\{g_1, \ldots, g_{m-1}, x'\}$ erzeugt Γ (über $\mathbb{Z}$)

Beweis. Es ist klar, daß diese Menge immernoch linear unabhängig ist. Außerdem: für $g \in \Gamma$ gibt es $c_i \in \mathbb{Z}$ $(\lfloor b_i \rfloor \in \mathbb{Z})$, so daß $g' = g - c_m x' - \sum_{i=1}^{m-1} c_i g_i \in T$, und der Koeffizient von g_m in g' ist ≥ 0 aber kleiner als b_m. Aus der Wahl von x' gilt nun: dieser Koeffizient ist 0, also ist $g' \in \Gamma_0$. $\square$

□

Definition 19.2
Sei Γ ein Gitter mit erzeugender Menge $\{e_1, \ldots, e_n\}$.
$T := \{x \in \mathbb{R}^n \mid x = a_i \sum e_i, 0 \leq a_i < 1, a_i \in \mathbb{R}\}$ heißt fundamentaler Parallelotop von Γ.

Algebraische Zahlentheorie
Algebra B 4 - Sommersemester 2017
Prof'in Dr. Salma Kuhlmann

20.Vorlesung

13 Juli 2017

Sei Γ ein Gitter mit f.P. T.

Lemma 20.1
$\forall v \in \mathbb{R}^n, \exists! l \in \Gamma$, so daß $v \in T + l$

Beweis. Sei $\{e_1, \ldots, e_n\}$ eine Basis, schreibe $v = \sum b_i e_i$ und setze $z_i := \lfloor b_i \rfloor \in \mathbb{Z}, b_i \in \mathbb{R}$.
Dann ist $a_i := b_i - z_i \in \mathbb{R}$ mit $0 \leq a_i < 1$. Es ist $v = t + l$, wobei $t := \sum a_i e_i \in T$ und $l := \sum z_i e_i, l \in \Gamma$. □

Wir studieren nun die Faktorgruppe $(\mathbb{R}^n, +)/(\Gamma, +)$. Setze $S := \{z \in \mathbb{C} \mid |z| = 1\}$ (eine multiplikative Untergruppe).

Lemma 20.2
$(\mathbb{R}, +)/(\mathbb{Z}, +) \cong (S, \times)$.

Beweis. Betrachte $\begin{array}{rccc} \phi: & \mathbb{R} & \to & S \\ & a & \mapsto & e^{2ia\pi} \end{array}$

□

Allgemeiner setze $\mathbb{T}^n := \underbrace{S \times S \times \ldots S}_{n \text{ mal}}$ (n-dimensionaler Torus).

Satz 20.3
Sei Γ ein vollständiges Gitter in $\mathbb{R}^n$, dann ist $\mathbb{R}^n/\Gamma \cong \mathbb{T}^n$.

Beweis. Sei $\{e_1, \ldots, e_n\}$ eine Basis für Γ und betrachte $\phi : \mathbb{R}^n \to \mathbb{T}^n$ definiert durch $\phi(\sum a_i e_i) = (e^{2ia_1\pi}, \ldots, e^{2ia_n\pi})$. □

Lemma 20.4
$\phi_{|T} : T \to \mathbb{T}^n$ ist injektiv.

Beweis. Aus $\exp(2ia_j\pi) = \exp(2ib_j\pi)$ (für $0 \leq a_j < 1$, $0 \leq b_j < 1$) folgt $a_j = b_j$ □

Allgemeiner gilt

Satz 20.5
Sei $\Gamma \subseteq \mathbb{R}^n$ m-dimensional (also $m \leq n$), dann ist $\mathbb{R}^n/\Gamma \cong \mathbb{T}^m \times \mathbb{R}^{n-m}$.

Beweis. Setze $V := \text{Span}_{\mathbb{R}}(\Gamma)$ und $W \subseteq \mathbb{R}^n$, so daß $\mathbb{R}^n = V \bigoplus W$; dann ist
$\mathbb{R}^n = V \bigoplus W \underset{\text{Satz 20.3}}{\cong} \mathbb{T}^m \times \mathbb{R}^{n-m}$ □

Definition 20.1 (i) Sei $X \subseteq \mathbb{R}^n$ Lebesgue-meßbar. Definiere $v(X) = \int_X dx_1, \ldots, dx_n$ das Volumen von X (Lebesgue-Maß von X).

(ii) Sei $\Gamma \subseteq \mathbb{R}^n$ ein vollständiges Gitter (also $\mathbb{T}^n \cong \mathbb{R}^n/\Gamma$) und $X \subseteq \mathbb{T}^n$. Definiere das Volumen von X: $v(X) := v(\phi^{-1}(X))$

(iii) Ist $Y \subseteq T$, so ist $\phi(Y) \subseteq \mathbb{T}^n$ und $v(\phi(Y)) = v(Y)$.

Satz 20.6
Sei $X \subseteq \mathbb{R}^n$ beschränkt, so daß $v(X)$ existiert (d.h. beschränkt und Lebesgues-meßbar). Aus $v(\phi(X)) \neq v(X)$ folgt, daß $\phi_{|X}$ nicht injektiv ist.

Beweis. Sei $\phi_{|X}$ injektiv. Da X beschränkt ist, existieren $l_1, \ldots, l_s \in \Gamma$, so daß $l_i \neq l_j$ für $j \neq i$ und $X_{l_j} := X \cap (T + l_j) \neq \varnothing \quad \forall j = 1, \ldots, s$ (also $X = \bigsqcup_{j=1}^{s} X l_j$).
Für $j = 1, \ldots, s$, definiere $Y_{l_j} = X_{l_j} - l_j$, so daß $Y_{l_j} \subseteq T \subseteq \mathbb{R}^n$. Bemerke, daß die Y_{l_j} disjunkt sind (da $\phi_{|X}$ injektiv ist). Außerdem gelten:

(a) $v(Y_{l_j}) = v(X_{l_j})$ (weil das Lebesgue-Maß invariant unter Translation ist).

(b) $\phi(X_{l_j}) = \phi(Y_{l_j})$ (weil $\Gamma = \ker \phi$).

(c) $v(\phi(Y_{l_j})) = v(Y_{l_j})$ (da $Y_{l_j} \subset T$).

Wir berechnen nun $v(\phi(X)) = v(\phi(\bigcup_j X_{l_j})) = v(\bigsqcup_j Y_{l_j}) = \sum_j v(Y_{l_j}) = \sum v(X_{l_j}) = v(X)$ □

Definition 20.2 (i) $X \subseteq \mathbb{R}^n$ ist <u>konvex</u>, wenn $\forall x, y \in X$ und $\forall \lambda \in \mathbb{R}$ mit $0 \leq \lambda \leq 1$ gilt $\lambda x + (1 - \lambda) y \in X$.

(ii) X ist <u>symmetrisch</u>, wenn gilt: $x \in X \Rightarrow -x \in X$.

Satz 20.7 (Minkowski)
Sei Γ ein vollständiges Gitter in $\mathbb{R}^n$ mit f.P. T und sei $X \subseteq \mathbb{R}^n$ beschränkt symmetrisch konvex (und Lebesgue-meßbar). Wenn $v(X) > 2^n v(T)$, gilt dann: $\exists \gamma \neq 0, \gamma \in \Gamma \cap X$.

Bemerkung
Da Γ diskret ist, gibt es nur endlich viele solche γ.

Beweis. Betrachte, das Gitter 2Γ mit f.P $2T$ und Volumen $v(2T) = 2^n v(T)$. Betrachte das Torus $\mathbb{T}^n = \mathbb{R}^n / 2\Gamma$.
Berechne $v(\mathbb{T}^n) = v(2T) = 2^n v(T)$. $\phi : \mathbb{R}^n \to \mathbb{T}^n$, $\ker \phi = 2\Gamma$, $\phi(X) \subseteq \mathbb{T}^n$ und
$v(\phi(X)) \leq v(\mathbb{T}^n) = 2^n v(T) < v(X)$
Aus Satz 20.6 folgt: $\phi_{|X}$ ist nicht injektiv. Also $\exists x_1, \neq x_2$, $x_1, x_2 \in X$, so daß $\phi(x_1) = \phi(x_2)$ oder $(x_1 - x_2) \in \ker \phi$, d.h. $x_1 - x_2 \in 2\Gamma$. Also $\frac{1}{2}(x_1 - x_2) \in \Gamma$. Nun $x_2 \in X \Rightarrow -x_2 \in X$ und $\frac{1}{2} x_1 + \frac{1}{2}(-x_2) \in X$, d.h. $\frac{1}{2}(x_1 - x_2) \in X$. □

§<u>Geometrische Darstellung von algebraischen Zahlen</u>

<u>Ansatz/Ziel</u>: Sei $L/\mathbb{Q}$ ein Zahlkörper von Grad n. Wir wissen, daß $L = \mathrm{Quot}(\mathcal{O}_L)$ (Satz 9.4). <u>Wir wollen</u> den gebrochenen Idealen von L Gittern in $\mathbb{R}^n$ zuordnen.
Sei θ ein primitives Element, so daß $L = \mathbb{Q}(\theta)$ (θ algebraische Zahl) und seien $\sigma_1, \ldots, \sigma_n$ die n verschiedenen Einbettungen von L in $\Omega := \mathbb{C}$.
Ist $\sigma_j(L) \subseteq \mathbb{R}$ (also $\sigma_i(\theta) \in \mathbb{R}$), so heißt σ_j reell. Sonst heißt σ_j komplex (also ist auch $\bar{\sigma}_j$ komplex).
Es ist $n = s + 2t$, wobei $s := \sharp$reelle Einbettungen und $2t := \sharp$ komplexe Einbettungen (also $\sigma_1, \ldots, \sigma_s, \sigma_{s+1}, \bar{\sigma}_{s+1}, \ldots, \sigma_{s+t}, \bar{\sigma}_{s+t}$ sind alle n verschiedene Einbettungen.)
Setze $L_{\mathbb{R}} := \mathbb{R}^S \times \mathbb{C}^t$. Siehe Fortsetzung in der 22. Vorlesung.

Algebraische Zahlentheorie
Algebra B 4 - Sommersemester 2017
Prof'in Dr. Salma Kuhlmann

21.Vorlesung

17 Juli 2017

§Idealnorm und Eigenschaften

Erinnerung: Sei $L/\mathbb{Q}$ ein Zahlkörper, $\mathcal{O}_L = \overline{\mathbb{Z}}^L$, $\mathcal{O}_L$ ist Dedekindring.

Definition 21.1
Sei $0 \neq \mathfrak{a} \lhd \mathcal{O}_L$, definiere
$N(\mathfrak{a}) := [\mathcal{O}_L : \mathfrak{a}] = |(\mathcal{O}_L, +)/(\mathfrak{a}, +)|$ (endlich oder ∞)

Satz 21.1 1. Sei $\mathfrak{b} \neq 0$, $\mathfrak{b} \lhd \mathcal{O}_L$, dann ist $N(\mathfrak{b}) < \infty$

2. $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$ für $\neq 0$ Ideale $\mathfrak{a}, \mathfrak{b} \lhd \mathcal{O}_L$

Beweis. Wir zeigen (1) und daß

$$(**) \qquad N(\mathfrak{ap}) = N(\mathfrak{a})N(\mathfrak{p})$$

für $\mathfrak{p} \lhd \mathcal{O}_L$ ein Primideal.
(2. folgt aus $(**)$ wegen Primfaktorisierung von Idealen in Dedekindringen).
Zu 1.: Sei $0 \neq \alpha \in \mathfrak{b}$ und Ω die normale Hülle von $L/\mathbb{Q}$, $n := \deg L$ und $\sigma_1, \ldots, \sigma_n$ die n verschiedenen Einbettungen von L in Ω. Setze $0 \neq \alpha = \sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ und
$n_\alpha := N_{L/\mathbb{Q}}(\alpha) \underset{\text{Satz 11.4}}{=} \prod_{i=1}^n \sigma_i(\alpha) = \alpha \prod_{i=2}^n \sigma_i(\alpha)$.
(Bemerke, daß (Korollar 12.1) $n_\alpha \in \mathbb{Z}$, da $\alpha \in \mathcal{O}_L$), also ist $\prod_{i=2}^n \sigma_i(\alpha) = n_\alpha \alpha^{-1} \in L$. Außerdem sind alle $\sigma_i(\alpha)$ ganz über $\mathbb{Z}$, also ist $\prod_{i=2}^n \sigma_i(\alpha)$ ganz über $\mathbb{Z}$, und somit ist $\prod_{i=2}^n \sigma_i(\alpha) \in \mathcal{O}_L$.
Nun ist $n_\alpha = \underbrace{\alpha}_{\in \mathfrak{b}} \underbrace{\prod_{i=2}^{n} \sigma_i(\alpha)}_{\in \mathcal{O}_L} \in \mathfrak{b}$ (weil $\mathfrak{b} \lhd \mathcal{O}_L$), also ist $< n_\alpha >= \mathcal{O}_L n_\alpha \subseteq \mathfrak{b}$. (und wir haben einen surjektiven Homomorphismus $\psi : \mathcal{O}_L/ < n_\alpha > \to \mathcal{O}_L/\mathfrak{b}$). Nun ist $\mathcal{O}_L$ ein freier $\mathbb{Z}$-Modul vom Rang n, insbesondere ist $\mathcal{O}_L$ ein endlich erzeugter $\mathbb{Z}$-Modul und so ist auch $\mathcal{O}_L/ < n_\alpha >$. Außerdem ist $\mathcal{O}_L/ < n_\alpha >= (\mathcal{O}_L/ < n_\alpha)_{\text{tor}}$ ein Torsionsmodul (5. Vorlesung), und ein endlich erzeugter Torsionsmodul über $\mathbb{Z}$ ist endlich (folgt aus Struktursatz für endlich erzeugte Moduln über HIR in 6. Vorlesung). Insbesondere ist $\mathcal{O}_L/\mathfrak{b}$ auch endlich (als Bild von ψ).
Zu $(**)$: Wir zeigen, daß

(a) $|\mathcal{O}_L/\mathfrak{ap}| = |\mathcal{O}_L/\mathfrak{a}||\mathfrak{a}/\mathfrak{ap}|$
und

(b) $|\mathfrak{a}/\mathfrak{ap}| = |\mathcal{O}_L/\mathfrak{p}|$

(a) ist klar (3. Isomorphiesatz für Gruppen):
$\mathcal{O}_L/\mathfrak{ap} \to \mathcal{O}_L/\mathfrak{a}$, $x + \mathfrak{ap} \mapsto x + \mathfrak{a}$ ist ein surjektiver Homomorphismus von Gruppen mit Kern $\mathfrak{a}/\mathfrak{ap}$, also $\mathcal{O}_L/\mathfrak{a} \cong (\mathcal{O}_L/\mathfrak{ap})/(\mathfrak{a}/\mathfrak{ap})$, also ist $|\mathcal{O}_L/\mathfrak{a}| = \frac{|\mathcal{O}_L/\mathfrak{ap}|}{|\mathfrak{a}/\mathfrak{ap}|}$ (Lagrange).
Zu (b): Bemerke, daß $\mathfrak{ap} \subsetneq \mathfrak{a}$ (Eindeutigkeit der Primfaktorisierung).

Behauptung: Sei $I \lhd \mathcal{O}_L$, so daß $\mathfrak{ap} \subseteq I \subseteq \mathfrak{a}$, dann ist $I = \mathfrak{ap}$ oder $I = \mathfrak{a}$.

Beweis. $\mathfrak{a}^{-1}\mathfrak{ap} \subseteq \mathfrak{a}^{-1}I \subseteq \mathcal{O}_L$, d.h $\mathfrak{p} \subseteq \mathfrak{a}^{-1}I \subseteq \mathcal{O}_L$,
$\mathfrak{p}$ maximal $\Rightarrow \mathfrak{p} = \mathfrak{a}^{-1}I$ (d.h $\mathfrak{ap} = I$) oder $\mathcal{O}_L = \mathfrak{a}^{-1}I$ (d.h.: $\mathfrak{a} = I$). □

Sei nun $x \in \mathfrak{a}$, $x \notin \mathfrak{ap}$ und betrachte $\mathfrak{ap} + < x >$. Wir haben $\mathfrak{ap} \subsetneq \mathfrak{ap} + < x > \subseteq \mathfrak{a}$, also $\mathfrak{ap} + < x > = \mathfrak{a}$. Wir definieren einen Homomorphismus

$$\begin{array}{rccc} : & \mathcal{O}_L & \to & \mathfrak{a}/\mathfrak{ap} \\ & y & \mapsto & \underbrace{yx}_{\in\mathfrak{a}} + \mathfrak{ap} \end{array}$$

Da $\mathfrak{ap} + < x > = \mathfrak{a}$, ist ψ surjektiv mit $\ker\psi \supseteq \mathfrak{p}$. Da $\mathfrak{p}$ maximal ist, und $\mathfrak{ap} \neq \mathfrak{a}, \ker\psi \neq \mathcal{O}_L$, folgt $\mathfrak{p} = \ker\psi$. D.h. $\mathcal{O}_L/\mathfrak{p} \cong \mathfrak{a}/\mathfrak{ap}$

□

Als Nächstes wollen wir die folgende Proposition Zeigen:

Proposition 21.2
Sei $0 \neq \beta \in \mathcal{O}_L$. Es ist $\underbrace{N(< \beta >)}_{\in\mathbb{N}} = |\underbrace{N_{L/\mathbb{Q}}(\beta)}_{\in\mathbb{Z}}|$.

Bevor wir die Proposition 21.2 beweisen, brauchen wir :

Bemerkung (i) Sei N ein freier $\mathbb{Z}$-Modul vom Rang n und $M \leq N$ ein Untermodul (dann ist M frei vom Rang $\leq n$, da $\mathbb{Z}$ ein HIR ist).

Dann ist: $[N : M] < \infty \Leftrightarrow \dim_{\mathbb{Z}} M = n$

Beweis von (i).

Behauptung 1: Sei $\{y_1, \ldots, y_m\}$ eine $\mathbb{Z}$-Basis für M. Schreibe $A := \begin{pmatrix} y_1 \\ \ldots \\ y_m \end{pmatrix}$, $y_j \in \mathbb{Z}^n$.

$A \in M_{m\times n}(\mathbb{Z})$

Nun zeigt ÜB, daß elementare Zeilen- und Spaltenumformungen eine Matrix B mit folgender Eigenschaft ergeben:

$\mathbb{Z}^n/\ \mathrm{Span}_{\mathbb{Z}}(B) \cong \mathbb{Z}^n/\ \mathrm{Span}_{\mathbb{Z}}(A) = \mathbb{Z}^n/M$

Behauptung 2: Zeilen-und Spaltenumformungen ergeben B der Form $B := \begin{pmatrix} d_1 & \ldots & 0 & * \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \ldots & d_m & * \end{pmatrix}$

$d_i \in \mathbb{Z}, d_i \neq 0$ (da$\{y_1, \ldots, y_m\}$ $\mathbb{Z}$-linear unabhängig sind).

Mit Behauptung 1 und Behauptung 2 können wir nun die Äquivalenz in (i) zeigen:

„$\Rightarrow$“ wir nehmen an, $m < n$ und zeigen $[\mathbb{Z}^n : M] = \infty$.

Setze $v_z := (\underbrace{0, \ldots, 0}_{m}, \underbrace{z}_{\in\mathbb{Z}}, 0, \ldots, 0)$. Aus $z_1 \neq z_2$ folgt $v_{z_1} \neq v_{z_2}$ mod $\mathrm{Span}_{\mathbb{Z}}B$

(weil $v_{z_1} - v_{z_2} = v_{z_1 - z_2}, z = z_1 - z_2 \neq 0 \Rightarrow v_z \notin \mathrm{Span}_{\mathbb{Z}}B$).

„$\Leftarrow$“ Wir nehmen nun an, daß $\dim_{\mathbb{Z}} M = n$, d.h. $n = m$. Dann ist $B = \begin{pmatrix} d_1 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & d_n \end{pmatrix}$,

$d_i \neq 0$, und

$\mathbb{Z}^n/\operatorname{Span}_{\mathbb{Z}} B \cong \mathbb{Z}^n/M$.

Wir berechnen

$|\mathbb{Z}^n/\operatorname{Span}_{\mathbb{Z}} B| = |\mathbb{Z}/d_1\mathbb{Z} \bigoplus \cdots \bigoplus \mathbb{Z}/d_n\mathbb{Z}| = \prod_{i=1}^n |d_i| < \infty$

□

(ii) Wir sehen außerdem, daß $n = m \Rightarrow |\mathbb{Z}^n/M| = |\det B| = |\det A|$, d.h

$n = m \Rightarrow [\mathbb{Z}^n : M] = |\det A|$, wobei

$A = \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix}$ für eine Basis $\{y_1, \ldots, y_n\} \subseteq M$ von M über $\mathbb{Z}$.

Um Proposition 21.2 zu beweisen, brauchen wir noch eine Berechnung:

Proposition 21.3
Sei $L/\mathbb{Q}$ Zahlkörper vom Grad n, $0 \neq \mathfrak{a} \lhd \mathcal{O}_L$, $\{y_1, \ldots, y_n\}$ eine $\mathbb{Z}$-Basis für $\mathfrak{a}$. Es ist:
$D(\mathcal{O}_L/\mathbb{Z})N(\mathfrak{a})^2 = D(y_1, \ldots, y_n)$.

Beweis. Wir wissen, daß $\mathcal{O}_L$ ein freier $\mathbb{Z}$-Modul vom Rang n ist, und außerdem, daß $[\mathcal{O}_L : \mathfrak{a}] < \infty$. Es folgt aus Bemerkung (i), daß $\mathfrak{a}$ ein freier $\mathbb{Z}$-Modul vom Rang n ist.
Sei $\{e_1, \ldots, e_n\}$ eine $\mathbb{Z}$-Basis für $\mathcal{O}_L$ und $\{y_1, \ldots, y_n\}$ eine $\mathbb{Z}$-Basis für $\mathfrak{a}$. Schreibe $y_i = \sum y_{ij} e_j, y_{ij} \in \mathbb{Z}$ und sei A die Matrix mit y_{ij} als ij-te Eintrag. Wir berechnen:
$D(y_1, \ldots, y_n) \underset{14.Vor.}{=} \det A^2 D(e_1, \ldots, e_n) = \det A^2 D(\mathcal{O}_L/\mathbb{Z})$.
Andererseits folgt aus Bemerkung (ii), daß
$|\det A| = [\mathcal{O}_L : \mathfrak{a}]$.
Alles zusammen ergibt: $D(y_1, \ldots, y_n) = N(\mathfrak{a})^2 D(\mathcal{O}_L/\mathbb{Z})$ □

Beweis von Proposition 21.2. Sei $\{e_1, \ldots, e_n\}$ eine $\mathbb{Z}$-Basis für $\mathcal{O}_L$, dann ist $\{\beta e_1, \ldots, \beta e_n\}$ eine $\mathbb{Z}$-Basis für $< \beta >$. Aus Proposition 21.3 folgern wir, daß
$D(\beta e_1, \ldots, \beta e_n) = D(\mathcal{O}_L/\mathbb{Z})N(< \beta >)^2$. Andererseits wissen wir, daß
$D(\beta e_1, \ldots, \beta e_n) = \det(B_{L/\mathbb{Q}}(\beta e_i, \beta e_j))$. Wir berechnen:
$\det(B_{L/\mathbb{Q}}(\beta e_i, \beta e_j)) = (\det((\sigma_i(\beta e_j))_{ij}))^2 = (\det((\sigma_i(\beta)\sigma_i(e_j))_{ij}))^2$. Nun ist
$\det((\sigma_i(\beta)\sigma_i(e_j))_{ij}) = \sigma_1(\beta) \ldots \sigma_n(\beta) \det(\sigma_i(e_j))_{ij} = N_{L/\mathbb{Q}}(\beta) \det(\sigma_i(e_j)_{ij})$. Alles zusammen ergibt:

$$D(\beta e_1, \ldots, \beta e_n) = (N_{L/\mathbb{Q}}(\beta))^2 (\det(\sigma_i(e_j))_{ij})^2 = (N_{L/\mathbb{Q}}(\beta))^2 D(e_1, \ldots, e_n) \underset{\text{Prop 21.3}}{=} N(< \beta >)^2 D(e_1, \ldots, e_n)$$

□

Algebraische Zahlentheorie
Algebra B 4 - Sommersemester 2017
Prof'in Dr. Salma Kuhlmann

22.Vorlesung

20 Juli 2017

Ziel: Endlichkeit der Klassenzahl

Satz 22.1
Sei L ein Zahlkörper vom Grad n und $s \in \mathbb{N}$ fest. Dann ist $|\{I \mid I \lhd \mathcal{O}_L, N(I) = s\}| < \infty$

Beweis.

Behauptung 1: Sei $J \lhd \mathcal{O}_L$. Dann ist $N(J) \in J$.

Beweis. $N(J) = |\mathcal{O}_L/J| \Rightarrow \forall x \in \mathcal{O}_L, N(J)x \in J.$ □

Behauptung 2: Seien $I, J \lhd \mathcal{O}_L, I \neq 0, J \neq 0$.
Es ist $I \subseteq J \Rightarrow IJ^{-1} \lhd \mathcal{O}_L$.

Beweis. $J^{-1} = (\mathcal{O}_L : J) = \{x \in L \mid xJ \subseteq \mathcal{O}_L\}$ □

Sei nun $J \lhd \mathcal{O}_L$ mit $N(J) = s$. Dann ist
$< s > \subseteq J$, also ist $< s > J^{-1} \lhd \mathcal{O}_L$. Setze $I :=< s > J^{-1}$. Wir haben $< s >= IJ$. Die Eindeutigkeit der Primfaktorisierung zeigt, daß die Menge der Primideale, die in der Faktorisierung von J erscheinen, eine Untermenge von der Menge der Primideale, die in der Faktorisierung von $< s >$ erscheinen, ist. Außerdem: Wenn für $\mathfrak{p}$ Primideal $\mathfrak{p}^\nu$ in der Faktorisierung von J und P^μ in der Faktorisierung von $< s >$ erscheint $(\mu, \nu \in \mathbb{N})$, ist dann $\nu \leq \mu$.
Setze $\mu := v_\mathfrak{p}(< s >)$. Wir sehen also, daß es höchstens $\prod_{\mathfrak{p}|<s>}(v_\mathfrak{p}(< s >) + 1)$ Möglichkeiten für J gibt, insbesondere endlich viele. □

Satz 22.2 (Minkowski Schranke)
Sei $L/\mathbb{Q}$ ein Zahlkörper. Dann gibt es $c_L \in \mathbb{R}_+$, so daß: $\forall 0 \neq \mathfrak{a} \lhd \mathcal{O}_L \exists 0 \neq \alpha \in \mathfrak{a}$ mit

$$(\dagger) \qquad N(< \alpha >) \leq c_L N(\mathfrak{a})$$

Beweis. Später (siehe 23. Vorlesung). □

Korollar 22.3
Sei $L/\mathbb{Q}$ ein Zahlkörper. Es gilt:

$$\forall \bar{\mathfrak{q}} \in \mathcal{K}l(L) := \mathcal{K}l(\mathcal{O}_L) \quad \exists \mathfrak{a} \lhd \mathcal{O}_L, \text{ so daß } \bar{\mathfrak{a}} = \bar{\mathfrak{q}} \text{ und } N(\mathfrak{a}) \leq C_L$$

Erinnerung: $\mathcal{K}l(L) = \mathrm{Id}(\mathcal{O}_L)/H(\mathcal{O}_L) = \mathcal{K}l(\mathcal{O}_L)$ ist die Klassengruppe des Zahlkörpers L, wobei $\mathrm{Id}(\mathcal{O}_L) =$ die Gruppe der gebrochenen Ideale unf $H(\mathcal{O}_L) =$ die Untergruppe der gebrochenen Hauptideale.

Beweis. Sei $\bar{\mathfrak{q}} = \mathfrak{q}H(\mathcal{O}_L)$, $\mathfrak{q} \in \mathrm{Id}(\mathcal{O}_L) \Rightarrow \exists d \neq 0, d \in \mathcal{O}_L$ und $\mathfrak{b} \lhd \mathcal{O}_L$, so daß

$$(*) \qquad \mathfrak{q}^{-1} = \frac{1}{d}\mathfrak{b}$$

Satz 22.2 $\Rightarrow \exists \beta \in \mathfrak{b}$, so daß

$$(\dagger) \qquad |N_{L/\mathbb{Q}}(\beta)| \leq c_L N(\mathfrak{b})$$

Betrachte

$$(**) \qquad \mathfrak{a} := \beta\mathfrak{b}^{-1},$$

da $< \beta > \subseteq \mathfrak{b}$ gilt $\mathfrak{a} \lhd \mathcal{O}_L$. Also ist $\mathfrak{q} \overset{(*)}{=} d\mathfrak{b}^{-1} \overset{(**)}{=} d\beta^{-1}\mathfrak{a}$ d.h $\mathfrak{q}\mathfrak{a}^{-1} = \mathcal{O}_L(d\beta^{-1}) \in H(\mathcal{O}_L)$. Wir berechnen $N(\mathfrak{a})N(\mathfrak{b}) = N(\mathfrak{a}\mathfrak{b}) \underset{(**)}{=} N(< \beta >) \underset{(\dagger)}{\leq} c_L N(\mathfrak{b})$, es folgt $N(\mathfrak{a}) \leq c_L$.

□

Erinnerung: $h_L := |\mathcal{K}l(L)|$ ist die Klassenzahl des Zahlkörpers L.

Satz 22.4 (Endlichkeit der Klassenzahl)
$\mathcal{K}l(L)$ ist endlich (d.h. $h_L \in \mathbb{N}$)

Beweis. Sei $\bar{\mathfrak{q}} \in \mathcal{K}l(L)$ und $\mathfrak{a} \lhd \mathcal{O}_L$ mit $N(\mathfrak{a}) \leq c_L$ und $\bar{\mathfrak{q}} = \bar{\mathfrak{a}}$. Dann ist $0 < N(\mathfrak{a}) \leq \lfloor c_L \rfloor$. Wir bekommen eine surjektive Abbildung von $\{\mathfrak{a} \lhd \mathcal{O}_L \mid N(\mathfrak{a}) \leq \lfloor c_L \rfloor\}$ nach $\mathcal{K}l(L)$ und
$\{\mathfrak{a} \lhd \mathcal{O}_L \mid N(\mathfrak{a}) \leq \lfloor c_L \rfloor\} = \bigcup_{s=1}^{\lfloor c_L \rfloor} \{\mathfrak{a} \lhd \mathcal{O}_L \mid N(\mathfrak{a}) = s\}$ ist endlich wegen Satz 22.1 □

Wir wollen nun (†) beweisen. Dafür kehren wir zum Ansatz am Ende der 20. Vorlesung und definieren eine Abbildung $\sigma : L \to L_{\mathbb{R}}$ wie folgt: $\sigma(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_s(\alpha), \sigma_{s+1}(\alpha), \ldots, \sigma_{s+t}(\alpha))$.

Bemerkung
σ ist $\mathbb{Q}$-linear

Satz 22.5
Sei $0 \neq \mathfrak{a} \lhd \mathcal{O}_L$, dann ist $\sigma(\mathfrak{a})$ ein vollständiges Gitter.

Beweis. Sei $\{\alpha_1, \ldots, \alpha_n\} \subseteq \mathcal{O}_L$ eine Basis für $L/\mathbb{Q}$.

Behauptung: $\{\sigma(\alpha_1), \ldots, \sigma(\alpha_n)\}$ ist eine Basis für $L_{\mathbb{R}}$ als $\mathbb{R}$-Vektorraum.

Beweis. Setze für $i = 1, \ldots, n$
$v_i := (\sigma_1(\alpha_i), \ldots, \sigma_s(\alpha_i);\ \mathrm{Re}\ \sigma_{s+1}(\alpha_i),\ \mathrm{Im}\ \sigma_{s+1}(\alpha_i), \ldots,\ \mathrm{Re}\ \sigma_{s+t}(\alpha_i),\ \mathrm{Im}\ \sigma_{s+t}(\alpha_i)) \in \mathbb{R}^{s+2t}$.
Vergleiche $A = \begin{pmatrix} v_1 \\ \ldots \\ v_n \end{pmatrix}$
mit $\mathcal{V}$(13. Vorlesung).

Erinnerung: $\mathcal{V} = \begin{pmatrix} \sigma_1(\alpha_1) & \ldots \sigma_s(\alpha_1) & \sigma_{s+1}(\alpha_1) & \overline{\sigma_{s+1}(\alpha_1)} & \ldots & \sigma_{s+t}(\alpha_1) & \overline{\sigma_{s+t}(\alpha_1)} \\ & \vdots & \vdots & & & & \\ \sigma_1(\alpha_n) & \ldots \sigma_s(\alpha_n) & \sigma_{s+1}(\alpha_n) & \overline{\sigma_{s+1}(\alpha_n)} & \ldots & \sigma_{s+t}(\alpha_n) & \overline{\sigma_{s+t}(\alpha_n)} \end{pmatrix}$

In ÜB haben wir berechnet: $0 \neq (\det \mathcal{V})^2 = D(\alpha_1, \ldots, \alpha_n)$ (da $\{\alpha_1, \ldots, \alpha_n\}$ Basis ist). Aber man kann A durch elementare Spaltenumformungen aus $\mathcal{V}$ bekommen (siehe Berechnung weiter unten), also ist auch $\det A \neq 0$. □

Nun ist $\mathfrak{a}$ ein freier $\mathbb{Z}$-Modul vom Rang n (21. Vorlesung), also wählen wir nun $\{\alpha_1, \ldots, \alpha_n\} \subseteq \mathfrak{a}$. Wir haben $\sigma(\mathfrak{a}) = \mathrm{Span}_{\mathbb{Z}}\{\sigma(\alpha_1, \ldots, \sigma(\alpha_n)\}$ (da σ $\mathbb{Q}$-linear ist) ein vollständiges Gitter.

□

Wir berechnen nun genau $\det A = ?$.

Erinnerung: Für $z \in \mathbb{C}$, $i = \sqrt{-1}$, $\operatorname{Re} z = \frac{z+\bar{z}}{2}$ und $\operatorname{Im} z = \frac{z-\bar{z}}{2i}$

Wir analysieren die Spaltenumformungen auf $\mathcal{V}$:

$$\begin{pmatrix} \dots & \sigma_{s+1}(\alpha_1) & \overline{\sigma_{s+1}(\alpha_1)} & \dots \\ & \vdots & \vdots & \\ \dots & \sigma_{s+1}(\alpha_n) & \overline{\sigma_{s+1}(\alpha_n)} & \dots \end{pmatrix} \overset{I+II}{\longrightarrow} \begin{pmatrix} \dots & \operatorname{Re}\sigma_{s+1}(\alpha_1) & \overline{\sigma_{s+1}(\alpha_1)} & \dots \\ & \vdots & \vdots & \\ \dots & \operatorname{Re}\sigma_{s+1}(\alpha_n) & \overline{\sigma_{s+1}(\alpha_n)} & \dots \end{pmatrix}$$

wobei:
I: $(s+1)$-te Spalte von $\mathcal{V}$ wird mit $\frac{1}{2}$ multipliziert.
II: Addiere die $(s+2)$-te Spalte zur $(s+1)$-te Spalte.

$$\overset{III+IV}{\longrightarrow} \begin{pmatrix} \dots & \operatorname{Re}\sigma_{s+1}(\alpha_1) & \operatorname{Im}\sigma_{s+1}(\alpha_1) & \dots \\ & \vdots & \vdots & \\ \dots & \operatorname{Re}\sigma_{s+1}(\alpha_n) & \operatorname{Im}\sigma_{s+1}(\alpha_n) & \dots \end{pmatrix}$$

Wobei :
III: $(s+2)$-te Spalte minus $(s+1)$-te Spalte.
IV: multipliziere mit i.
Wiederhole für $(s+3)$-te bis $(s+t)$-te Spalte, insgesamt t mal. Alles zusammen ergibt:
$\det A = (\frac{1}{2}i)^t \det \mathcal{V}$.

Algebraische Zahlentheorie
Algebra B 4 - Sommersemester 2017
Prof'in Dr. Salma Kuhlmann

23.Vorlesung

21 Juli 2017

Sei $L/\mathbb{Q}$ ein Zahlkörper vom Grad n. Ansatz wie in der 22. Vorlesung. Wir wollen nun das Gitter $\sigma(\mathfrak{a}) \subseteq L_{\mathbb{R}}$. studieren.

Bemerkung 23.1
Sei $\Gamma \subseteq \mathbb{R}^n$ ein vollständiges Gitter mit Basis $\{v_1, \ldots, v_n\}$ und f.P. T_Γ.
Es ist $v(T_\Gamma) = |\det \begin{pmatrix} v_1 \\ \ldots \\ v_n \end{pmatrix}|$ (ÜB)

Wir können Bemerkung 23.1 anwenden mit $\Gamma = \sigma(\mathfrak{a})$. Wir berechnen:
$v(T_{\sigma(\mathfrak{a})}) = |\det A| = |(\frac{1}{2}(i))^t \det \mathcal{V}|$. Andererseits ist $(\det \mathcal{V})^2 \underset{\text{ÜB}}{=} D(\alpha_1, \ldots, \alpha_n) \underset{\text{Prop. 21.3}}{=} N(\mathfrak{a})^2 D(\mathcal{O}_L/\mathbb{Z})$.
Alles zusammen ergibt: $v(T_{\sigma(\mathfrak{a})}) = 2^{-t} N(\mathfrak{a}) \sqrt{|D(\mathcal{O}_L/\mathbb{Z})|}$

Bemerkung 23.2
Sei $\tau \in \mathbb{R}_+$ und setze $X_\tau := \{(x_1, \ldots, x_s, z_1, \ldots, z_t) \in L_{\mathbb{R}} \mid \sum_{i=1}^s |x_i| + 2\sum_{j=1}^t |z_j| < \tau\}$.
Dann ist X_τ beschränkt, konvex, symmetrisch und $v(X_\tau) = 2^s (\frac{\pi}{2})^t \frac{\tau^n}{n!}$ (ÜB)

Wir können nun eine genauere Aussage über die Minkowski Schranke (Satz 22.2) zeigen.

Satz 23.1 (Explizite Minkowski Schranke)
Sei $0 \neq \mathfrak{a} \lhd \mathcal{O}_L$,. Es gibt $0 \neq \alpha \in \mathfrak{a}$, so daß

$$|N_{L/\mathbb{Q}}(\alpha)| \leq \underbrace{(\frac{4}{\pi})^t \frac{n!}{n^n} \sqrt{|D(\mathcal{O}_L/\mathbb{Z})|}}_{:=C_L} N(\mathfrak{a})$$

Beweis. Wir wollen Satz 20.7 auf $\Gamma := \sigma(\mathfrak{a})$ und $X_\tau \subseteq L_{\mathbb{R}}$ für ein geeignetes τ anwenden.
Wir bemerken jetzt schon: wenn

(1) $v(X_\tau) > 2^n v(T_{\sigma(\mathfrak{a})})$ dann

(2) $\exists \alpha \neq 0, \alpha \in \mathfrak{a}$, so daß $\sigma(\alpha) \in X_\tau$, d.h so daß $(\sigma_1(\alpha), \ldots, \sigma_s(\alpha), \sigma_{s+1}(\alpha), \ldots, \sigma_{s+t}(\alpha)) \in X_\tau$, d.h.

$$(*) \qquad \sum_{i=1}^s |\sigma_i(\alpha)| + 2\sum_{j=1}^t |\sigma_{s+j}(\alpha)| < \tau$$

Erinnerung (AGU)**:** Seien $a_1, \ldots, a_n \in \mathbb{R}_+$, $n \in \mathbb{N}$. Es ist

$$(\prod_{i=1}^n a_i)^{\frac{1}{n}} \leq \frac{1}{n}(\sum_{i=1}^n a_i)$$

Setze $a_j := |\sigma_j(\alpha)|$, $j = 1, \ldots, s$ und $a_{s+1} = a_{s+2} = |\sigma_{s+1}(\alpha)|$ und
$\vdots$
$\underbrace{a_{s+2t-1}}_{=a_{n-1}} = \underbrace{a_{s+2t}}_{a_n} = |\sigma_{s+t}(\alpha)|$
$(*)$ bedeutet $\sum_{l=1}^{n} a_l < \tau$. Die AGU impliziert nun, daß $n(a_1 \ldots a_n)^{\frac{1}{n}} < \tau$, d.h. $\prod_{l=1}^{n} a_l < \frac{\tau^n}{n^n}$, d.h. $|N_{L/\mathbb{Q}}(\alpha)| = \prod_{l=1}^{n} a_l < \frac{\tau^n}{n^n}$.
(Begründung: $\prod a_l = \prod_{i=1}^{s} |\sigma_i(\alpha)| \prod_{j=1}^{t} |\sigma_{s+j}(\alpha)|^2$. Andererseits ist $|\sigma_{s+j}(\alpha)|^2 = |\sigma_{s+j}(\alpha)|.|\overline{\sigma_{s+j}(\alpha)}|$, so daß

$$\begin{aligned}\prod a_l &= |\prod_{i=1}^{s} \sigma_i(\alpha) \prod_{j=1}^{t} \sigma_{s+j}(\alpha)\overline{\sigma}_{s+j}(\alpha)| \\ &= |\prod_{i=1}^{s} \sigma_i(\alpha) \prod_{j=1}^{t} \sigma_{s+j}(\alpha) \prod_{j=1}^{t} \overline{\sigma}_{s+j}(\alpha)| \\ &= |N_{L/\mathbb{Q}}(\alpha)|\end{aligned}$$

Weil $\sigma_1, \ldots, \sigma_s, \sigma_{s+1}, \bar{\sigma}_{s+1}, \ldots, \sigma_{s+t}, \bar{\sigma}_{s+t}$ alle Einbettungen über $\mathbb{Q}$ von L in $\mathbb{C}$ sind.)
Zusammenfassung:

(1) Ist $v(X_\tau) > 2^n v(T_{\sigma(\mathfrak{a})})$, dann

(2) $\exists 0 \neq \alpha \in \mathfrak{a}$, so daß $|N_{L/\mathbb{Q}}(\alpha)| < \frac{\tau^n}{n^n}$

oder
(1) Ist $2^s(\frac{\pi}{2})^t \frac{\tau^n}{n!} > 2^n 2^{-t} N(\mathfrak{a}) \sqrt{|D(\mathcal{O}_L/\mathbb{Z})|}$ dann gilt (2). Wir analysieren die Bedingung (1) genauer:

$$\begin{aligned}(1) &\Leftrightarrow \tau^n > n! 2^{-s} 2^n 2^{-t} 2^t \pi^{-t} N(\mathfrak{a}) \sqrt{|D(\mathcal{O}_L/\mathbb{Z})|} \\ &\text{d.h. } \tau^n > n! 2^{n-s} \pi^{-t} N(\mathfrak{a}) \sqrt{|D(\mathcal{O}_L/\mathbb{Z})|} \\ &\text{d.h. } \tau^n > n! 2^{2t} \pi^{-t} N(\mathfrak{a}) \sqrt{|D(\mathcal{O}_L/\mathbb{Z})|}\end{aligned}$$

Wir haben bewiesen:
Ist $\tau^n > n!(\frac{4}{\pi})^t N(\mathfrak{a}) \sqrt{|D(\mathcal{O}_L/\mathbb{Z})|}$ (1), dann $\exists 0 \neq \alpha \in \mathfrak{a}$ mit $|N_{L/\mathbb{Q}}(\alpha)| < \frac{\tau^n}{n^n}$ (2).
Für jedes τ wie in (1) definieren wir
$A_\tau := \{0 \neq \alpha \in \mathfrak{a} \mid |N_{L/\mathbb{Q}}(\alpha)| < \frac{\tau^n}{n^n}\}$. Dann ist $A_\tau \neq \varnothing$, $|A_\tau| < \infty$ (da $\sigma(\alpha) \in X_\tau \cap \sigma(\mathfrak{a})$), $\tau_1 < \tau_2 \Rightarrow A_{\tau_1} \subseteq A_{\tau_2}$. Aus diesen Eigenschaften folgern wir, daß $\bigcap_{\tau \text{ erfüllt (1)}} A_\tau \neq \varnothing$: Sei τ_0, so daß $|A_{\tau_0}| \leq |A_\tau|$ für alle τ, die (1) erfüllen. Dann ist $\cap A_\tau = A_{\tau_0} \neq \varnothing$.
Sei nun $\alpha \in \cap A_\tau$. Wir behaupten, daß $|N_{L/\mathbb{Q}}(\alpha)| \leq C_L N(\mathfrak{a})$: da $0 \neq \alpha \in \cap A_\tau$ ist, gilt $|N_{L/\mathbb{Q}}(\alpha)| < \frac{\tau^n}{n^n}$, für alle τ, die (1) erfüllen . Es folgt : $|N_{L/\mathbb{Q}}(\alpha)| \leq \inf_{\tau \text{ erfüllt (1)}} \{\frac{\tau^n}{n^n}\} = \frac{1}{n^n} \inf_{\tau \text{ erfüllt (1)}} \tau^n$
Nun ist $\inf_{\tau \text{ erfüllt (1)}} \tau^n = n!(\frac{4}{\pi})^t N(\mathfrak{a}) \sqrt{|D(\mathcal{O}_L/\mathbb{Z})|}$. □

Algebraische Zahlentheorie
Algebra B 4 - Sommersemester 2017
Prof'in Dr. Salma Kuhlmann

24.Vorlesung

24 Juli 2017

§Die Einheitsgruppe $\mathcal{O}_L^\times$

Ansatz wie in den 22. und 23. Vorlesungen.

Satz 24.1 (Dirichletsche Einheitssatz)
$\mathcal{O}_L^\times$ ist eine endlich erzeugte abelsche Gruppe mit freiem Rang $s+t-1$.

Beweis. Später. □

Bemerkung
Aus D.E.S können wir folgern, daß

(i) $\mathcal{O}_L^\times = F \times (\mathcal{O}_L^\times)_{\text{tor}}$, F freie abelsche Gruppe vom Rang $s+t-1$ (siehe Satz 5.4)

(ii) $\mu(L) := (\mathcal{O}_L^\times)_{\text{tor}} = \{x \neq 0, x \in \mathcal{O}_L, \exists \mu \in \mathbb{N}, x^\mu = 1\}$ besteht aus Einheitswurzeln in $\mathcal{O}_L^\times$, d.h. $\mu(L)$:=die Gruppe der Einheitswurzeln in L.

(iii) $\mathcal{O}_L^\times$ ist endlich erzeugt⇒ $(\mathcal{O}_L^\times)_{\text{tor}}$ ist endlich erzeugt, also ist $(\mathcal{O}_L^\times)_{\text{tor}}$ eine endliche Gruppe. Andererseits ist eine endliche Untergruppe von $L^\times$ zyklisch (siehe B3), insbesondere ist $(\mathcal{O}_L^\times)_{\text{tor}}$ eine endliche zyklische Gruppe mit Erzeuger eine Einheitswurzel $\mu \in L^\times$.

Für den Beweis von D.E.S brauchen wir zwei Schlüßelergebnisse:

Lemma 24.2
Sei $\alpha \in L$. Dann ist $\alpha \in \mathcal{O}_L^\times \Leftrightarrow \alpha \in \mathcal{O}_L$ und $N_{L/\mathbb{Q}}(\alpha) = \pm 1$.

Beweis. „⇒“

$$\begin{aligned} \alpha \in \mathcal{O}_L^\times &\Rightarrow \beta = \alpha^{-1} \in \mathcal{O}_L \\ &\Rightarrow N_{L/\mathbb{Q}}(\alpha\beta) = \underbrace{N_{L/\mathbb{Q}}(\alpha)}_{\in\mathbb{Z}} \underbrace{N_{L/\mathbb{Q}}(\beta)}_{\in\mathbb{Z}} = 1 \\ &\Rightarrow N_{L/\mathbb{Q}}(\alpha) = \pm 1 \end{aligned}$$

„⇐“ Es ist: $\prod_{i=1}^n \sigma_i(\alpha) = \alpha \prod_{i=2}^n \sigma_i(\alpha) = \pm 1$ also $\alpha^{-1} = \pm \prod_{i=2}^n \sigma_i(\alpha)$, also ist α^{-1} ganz über $\mathbb{Z}$, außerdem ist $\alpha^{-1} \in L$. Also $\alpha^{-1} \in \mathcal{O}_L$ □

Proposition 24.3
Seien $m, M \in \mathbb{N}$ fest. Es ist: Die Menge der komplexen algebraischen Zahlen $A_{m,M} = \{\alpha \in \mathcal{O}_{\mathbb{C}} \mid \deg \text{ MinPol}_{\mathbb{Z}}(\alpha) \leq m$ und $|\alpha'| \leq M$ für alle konjugierte α' zu $\alpha\}$ ist endlich.

Beweis. α ist ganz über $\mathbb{Z}$. Es genügt zu zeigen: es gibt nur endlich viele normierte irreduzible Polynome in $\mathbb{Z}[X]$, die als $\mathrm{MinPol}_{\mathbb{Z}}(\alpha)$ fungieren können (für solche $\alpha \in A_{m,M}$). Nun ist deg $\mathrm{MinPol}_{\mathbb{Z}}(\alpha) \leq m$. Wir behaupten: die Koeffiziente sind auch beschränkt, d.h $\exists M_m \in \mathbb{N}$, so daß alle Koeffiziente im Absolutbetrag $< M_m$ sind. In der Tat sind die Koeffiziente elementare symmetrische Funktionen in den Nullstellen, und die Nullstellen sind im Absolutbetrag $\leq M$ per Annahme. Genauer erklärt, sei z.B. $\mathrm{MinPol}_{\mathbb{Z}}(\alpha) = x^m + z_{m-1}x^{m-1} + \cdots + z_0$, $z_i \in \mathbb{Z}$ mit Nullstellen $\alpha_1, \ldots, \alpha_m$. Es ist

$$z_{m-1} = -\sum_{i=1}^{m} \alpha_i \Rightarrow |z_{m-1}| \leq \sum_{i=1}^{m} |\alpha_i| \leq mM = \binom{m}{1} M$$

$$z_{m-2} = \sum_{i<j} \alpha_i\alpha_j \Rightarrow |z_{m-2}| \leq \sum_{i<j} |\alpha_i\alpha_j| \leq \binom{m}{2} M^2$$

$$\vdots$$

$$z_{m-k} = (-1)^k \sum \alpha_{i_1} \ldots \alpha_{i_k} \Rightarrow |z_{m-k}| \leq \sum |\alpha_{i_1} \ldots \alpha_{i_k}| \leq \binom{m}{k} M^k$$

Da $\mathbb{Z}^m$ ein Gitter ist, und jedes normierte irreduzible Polynom in $\mathbb{Z}[x]$ vom deg $\leq m$ ein Vektor in $\mathbb{Z}^m$ ist (Vektor der Koeffiziente), ist der Durchschnitt mit der beschränkten Menge endlich wie behauptet.

□

Korollar 24.4
Sei $\alpha \in \mathbb{C}$ eine ganze algebraische Zahl, so daß $|\alpha'| = 1$ für alle α' zu α konjugiert (d.h. für alle Nullstellen α' von $\mathrm{MinPol}_{\mathbb{Z}}(\alpha)$). Dann gibt es $\mu \in \mathbb{N}$, so daß $\alpha^\mu = 1$ (d.h.: α ist eine Einheitswurzel).

Beweis. Sei $m := \deg \mathrm{MinPol}_{\mathbb{Q}}(\alpha)$. Bemerke, daß $\{1, \alpha, \alpha^2, \ldots\} \subseteq A_{m,1}$, also ist es endlich, d.h. es gibt l, k mit $\alpha^l = \alpha^k$ oder $\alpha^{l-k} = 1$. □

Wir können nun direkt zeigen, daß:

Korollar 24.5
$\mu(L) = (\mathcal{O}_L^\times)_{\mathrm{tor}}$ ist endlich.
(Vergleiche mit Bemerkung (iii))

Beweis. Setze $n = \deg L/\mathbb{Q}$, $N = 1$, $\mu(L) \subseteq A_{n,1}$ □

Ansatz weiterhin wie in der 22. und 23. Vorlesung. Für den Beweis von D.E.S brauchen wir außerdem noch eine „Hilfsabbildung“ $\lambda : L^\times \to \mathbb{R}^{s+t}$
$\alpha \mapsto (\log|\sigma_1(\alpha)|, \ldots \log|\sigma_s(\alpha)|, \log|\sigma_{s+1}(\alpha)|, \log|\sigma_{s+2}(\alpha)|, \ldots, \log|\sigma_{s+t}(\alpha)|)$
λ ist ein Homomorphismus (der multiplikativen Gruppe $L^\times$ auf die additive Gruppe $\mathbb{R}^s \times \mathbb{R}^t$). Bemerke, daß

$$\begin{aligned} \alpha \in \mathcal{O}_L^\times &\Rightarrow |N_{L/\mathbb{Q}}(\alpha)| = 1 \\ &\Rightarrow \prod_{i=1}^{s} |\sigma_i(\alpha)| \prod_{j=1}^{t} |\sigma_{s+j}(\alpha)|^2 = 1 \\ (*) \qquad &\Rightarrow \sum_{i=1}^{s} \log|\sigma_i(\alpha)| + 2\sum_{j=1}^{t} \log|\sigma_{s+j}(\alpha)| = 0 \end{aligned}$$

und umgekehrt auch: für $\alpha \in \mathcal{O}_L$, $(*) \Rightarrow N_{L/\mathbb{Q}}(\alpha) = \pm 1$ also $\alpha \in \mathcal{O}_L^\times$, d.h.:
$\forall \alpha \in \mathcal{O}_L, \alpha \in \mathcal{O}_L^\times \Leftrightarrow (*)$ gilt für α.
Betrachte die Untermenge von $\mathbb{R}^s \times \mathbb{R}^t$: $H := \{x \in \mathbb{R}^s \times \mathbb{R}^t \mid \sum_{i=1}^{s} x_i + 2\sum_{j=1}^{t} x_{s+j} = 0\}$. Eigentlich ist H ein Unterraum der Dimension $s + t - 1$ (Lösungsraum von einem homogenen Gleichungssystem mit einer Gleichung und in $s + t$ Unbekannten). Mit dieser Notation gilt: $\mathcal{O}_L^\times = \{\alpha \in \mathcal{O}_L \mid \lambda(\alpha) \in H\}$.

Proposition 24.6
$\lambda(\mathcal{O}_L^\times)$ ist ein Gitter in $\mathbb{R}^{s+t}$

Beweis. Später □

Korollar 24.7
$\mathcal{O}_L^\times$ ist endlich erzeugt mit freiem Rang $\leq s+t-1$

Beweis. $\lambda(\mathcal{O}_L^\times)$ ist ein Gitter $\subseteq H$, also ist $\lambda(\mathcal{O}_L^\times)$ eine freie abelsche Gruppe vom Rang $\leq s+t-1$. Betrachte: $\lambda_{|\mathcal{O}_L^\times} : \mathcal{O}_L^\times \to H$ und berechne dessen Kern:

$$\begin{aligned}\alpha \in \ker\lambda &\Leftrightarrow \log|\sigma_l(\alpha)| = 0 \quad \forall l = 1,\dots,s+t\\ &\Leftrightarrow |\sigma_l(\alpha)| = 1 \quad \forall l = 1,\dots,s+t\\ &\Leftrightarrow |\alpha'| = 1 \text{ für alle konjugierte } \alpha' \text{ zu } \alpha\\ &\Leftrightarrow \alpha \text{ ist Einheitswurzel} \Leftrightarrow \alpha \in \mu(L)\end{aligned}$$

Wir haben gezeigt: $\ker\lambda = \mu(L)$ ist eine endliche Gruppe. Zusammenfassend:

$$\begin{array}{rccc}\lambda: & \mathcal{O}_L^\times & \to & \lambda(\mathcal{O}_L^\times)\\ & \mathcal{O}_L^\times/\underbrace{\mu(L)}_{\text{endlich}} & \cong & \underbrace{\lambda(\mathcal{O}_L^\times)}_{\text{endlich erzeugt}}\end{array} \Rightarrow \mathcal{O}_L^\times \text{ ist eine endlich erzeugte abelsche Gruppe}$$

Ferner ist $\mu(L) = (\mathcal{O}_L^\times)_{\text{tor}}$ und der freie Rang von $\mathcal{O}_L^\times$ ist dann
$\dim_{\mathbb{Z}}(\mathcal{O}_L^\times/(\mathcal{O}_L^\times)_{\text{tor}}) = \dim_{\mathbb{Z}}\lambda(\mathcal{O}_L^\times) \leq s+t-1$.

□

Bemerkung
Um D.E.S vollständig zu zeigen, müssen wir nur noch beweisen, daß $\lambda(\mathcal{O}_L^\times)$ ein vollständiges Gitter in H ist.

Beweis von Proposition 24.6. z.z.: $\lambda(\mathcal{O}_L^\times)$ ist diskret. Dafür genügt es zu zeigen, dass:
$\forall c \in \mathbb{R}_+$ existieren endlich viele $\alpha \in \mathcal{O}_L^\times$ mit $|\log|\sigma_l(\alpha)|| \leq c \quad \forall l = 1,\dots,s+t$. Aber
$\log|\sigma_l(\alpha)| \leq c \Leftrightarrow |\sigma_l(\alpha)| \leq \exp c$. Also $\alpha \in \mathcal{O}_L^\times$ mit $|\log|\sigma_l(\alpha)|| \leq c \Rightarrow \alpha \in \underbrace{A_{n,\lceil\exp c\rceil}}_{\text{endlich wegen Prop.24.3}}$

□

Algebraische Zahlentheorie
Algebra B 4 - Sommersemester 2017
Prof'in Dr. Salma Kuhlmann

25.Vorlesung

27 Juli 2017

Ziel: $\lambda(\mathcal{O}_L^\times) \subseteq H$ ist ein vollständiges Gitter. Es genügt dafür, $\epsilon_1, \ldots, \epsilon_{s+t-1} \in \mathcal{O}_L^\times$ zu finden, so daß $\{\lambda(\epsilon_1), \ldots, \lambda(\epsilon_{s+t-1})\} \subseteq H$ $\mathbb{R}$-linear unabhängig ist. Diese letzte Vorlesung hat als Hauptziel, die folgende Proposition 25.1 zu beweisen und daraus D.E.S zu folgern.

Proposition 25.1
$\exists \epsilon_1, \ldots, \epsilon_{s+t-1} \in \mathcal{O}_L^\times$, so daß $|\sigma_l(\epsilon_k)| < 1$ für $l \neq k, l = 1, \ldots, s+t, k = 1, \ldots, s+t-1$.

Beweis. Später. □

Wir können nun schon Aufgrund von Proposition 25.1 den Beweis für D.E.S fortsetzen. Seien $\epsilon_1, \ldots, \epsilon_{s+t-1}$ wie in Proposition 25.1. Wir zeigen:

$(*)$ $\{\lambda(\epsilon_1), \ldots, \lambda(\epsilon_{s+t-1})\}$ ist linear unabhängig.

Betrachte die Matrix A mit (k,l)-tem Eintrag
$A_{k,l} := \log|\sigma_l(\epsilon_k)|$, $k = 1, \ldots, s+t-1$, $l = 1, \ldots, s+t-1$.
Um $(*)$ zu beweisen, genügt es zu zeigen, daß A invertierbar ist. Durch elementare Spaltenumformungen (multipliziere die letzte $t-1$ Spalten mit 2) bekommen wie eine Matrix A' mit den folgenden Eigenschaften:

(i) $A'_{kl} < 0$ für $k \neq l$ ($|\sigma_l(\epsilon_k)| < 1 \Rightarrow \log|\sigma_l(\epsilon_k)| < 0$)

(ii) $\sum_l A'_{kl} > 0$ ($\sum_l A'_{kl} = \sum_{l=1}^{s} \log|\sigma_l(\epsilon_k)| + 2\sum_{l=s+1}^{s+t-1} \log|\sigma_l(\epsilon_k)| = -2\log|\sigma_{s+t}(\epsilon_k)|$, da $\lambda(\epsilon_k) \in H$.

Nun ist aber $\log|\sigma_{s+t}(\epsilon_k)| < 0$, also $-2\log|\sigma_{s+t}(\epsilon_k)| > 0$.)

Hilfslemma
Sei A' eine $m \times m$ matrix, die die Eigenschaften (i)+(ii) erfüllt. Dann ist A' invertierbar.

Beweis. ÜA □

Damit ist D.E.S bewiesen.

Wir müßen nur noch Proposition 25.1 beweisen. Ansatz wie in der 22 und 23 Vorlesung.

Bemerkung 1. $L_\mathbb{R}$ ist nicht nur ein $\mathbb{R}$-Vektorraum, sondern eine $\mathbb{R}$-Algebra (mit Komponentenweise Multiplikation versehen).

2. Für $x \in L_\mathbb{R}$ definiere die "Norm von x" wie folgt:
$N(x) := \prod_{i=1}^{s} x_i \prod_{j=1}^{t} x_{s+j}\bar{x}_{s+j} = \prod_{i=1}^{s} x_i \prod_{j=1}^{t} |x_{s+j}|^2$.
(Bemerke, daß $N_{L/\mathbb{Q}}(\alpha) = N(\sigma(\alpha)) \forall \alpha \in L$, dies begründet die Terminologie "Norm von x".)

Unsere **Hauptbehauptung** nun ist: $\exists c > 0, c \in \mathbb{R}$ so daß $\forall x \in L_{\mathbb{R}}$ mit $\frac{1}{2} \leq |N(x)| \leq 1$, $\exists \epsilon \in \mathcal{O}_L^{\times}$, so daß $|x_l \sigma_l(\epsilon)| < \epsilon \quad \forall l = 1, \ldots, s+t$.

Bemerke, daß **Hauptbehauptung**⇒Proposition 25.1:

Beweis. für jedes $k = 1, \ldots, s+t-1$ wähle $x \in L_{\mathbb{R}}$ mit $|N(x)| = 1$ aber $|x_l| > c$ für $l \neq k$ (ausgleichen mit dem k-te Komponente). Unsere Hauptbehauptung liefert $\epsilon_k \in \mathcal{O}_L^{\times}$, so daß $|x_l \sigma_l(\epsilon_k)| < c \quad \forall l$. Insbesondere wenn $l \neq k$, ist $|\sigma_l(\epsilon_k)| < c/|x_l| < 1$ wie erwnüscht. □

Wir bemühen uns letztendlich darum, die **Hauptbehauptung** zu beweisen. Wir werden dafür Minkowski's Satz anwenden.
Sei $x \in L_{\mathbb{R}}$ mit $N(x) \neq 0$. Wir zeigen zunächst, daß $x\sigma(\mathcal{O}_L)$ ein vollständiges Gitter in $L_{\mathbb{R}}$ ist.
Bemerke: Da $\mathcal{O}_L \lhd \mathcal{O}_L$ ist, wissen wir schon, daß $\sigma(\mathcal{O}_L)$ ein vollständiges Gitter in $L_{\mathbb{R}}$ ist (siehe 22. Vorlesung), also daß $x\sigma(\mathcal{O}_L)$ ein vollständiges Gitter für $x = (1, \ldots, 1)$ ist.
Sei $\{\alpha_1, \ldots, \alpha_n\}$ eine $\mathbb{Z}$-Basis für $\mathcal{O}_L$, also $\{\sigma(\alpha_1), \ldots, \sigma(\alpha_n)\}$ ist $\mathbb{R}$-linear unabhängig und $x\sigma(\mathcal{O}_L) = x\sigma(\alpha_1)\mathbb{Z} \oplus \cdots \oplus x\sigma(\alpha_n)\mathbb{Z}$.
Wir zeigen: $\{x\sigma(\alpha_1), \ldots, x\sigma(\alpha_n)\}$ ist $\mathbb{R}$-linear unabhängig. Dafür betrachten wir wie immer die Matrix
$A = \begin{pmatrix} x\sigma(\alpha_1) \\ \vdots \\ x\sigma(\alpha_n) \end{pmatrix} \in \mathrm{Mat}_{n\times n}(\mathbb{R})$. Analogue Berechnungen wie früher zeigen, daß
$|\det(A)| = 2^{-t}|\det \chi|$, wobei χ die Matrix mit i-te Zeile gleich

$$x_1\sigma_1(\alpha_i) \ldots x_s\sigma_s(\alpha_i) \quad x_{s+1}\sigma_{s+1}(\alpha_i) \quad \bar{x}_{s+1}\overline{\sigma_{s+1}(\alpha_i)} \ldots$$

ist. Wir wollen also $\det \chi$ berechnen. Jede Spalte hat einen gemeinsamen Faktor, und zwar entweder x_j oder $\bar{x}_j$, wir sehen also, daß $\det \chi = N(x) \det \mathcal{V}$, wobei wie immer $V_{ij} = \sigma_i(\alpha_j)$. Wir bekommen außerdem $0 \neq |\det(A)| = 2^{-t}|N(x)|\sqrt{|D(\mathcal{O}_L/\mathbb{Z})|}$ (siehe 21. Vorlesung). Also ist $x\sigma(\mathcal{O}_L)$ ein vollständiges Gitter und analogue Berechnungen wie in der 22. Vorlesung ergeben: $v(T_x) = |\det A| = 2^{-t}|N(x)|\sqrt{|D(\mathcal{O}_L/\mathbb{Z})|}$ (wobei $T_x :=$ f.P von $x\sigma(\mathcal{O}_L)$). Insbesondere wenn $\frac{1}{2} \leq |N(x)| \leq 1$, dann ist

$$(**) \qquad v(T_x) \leq 2^{-t}\sqrt{|D(\mathcal{O}_L/\mathbb{Z})|}$$

(unabhängig von x)

- Sei nun $X \subseteq L_{\mathbb{R}}$ konvex symmetrisch beschränkt, so daß $v(X) > 2^n 2^{-t}\sqrt{|D(\mathcal{O}_L/\mathbb{Z})|}$ (z.B. $X = B_R(0)$ mit R groß genug)
- Sei $R \in \mathbb{R}_+$, so daß $|N(y)| < R \quad \forall y \in X$.
- Minkowski und $(**)$ ergeben:

$$(***) \qquad \forall x \in L_{\mathbb{R}} \text{ mit } \frac{1}{2} \leq |N(x)| \leq 1, \exists 0 \neq \alpha \in \mathcal{O}_L, \text{ so daß } x\sigma(\alpha) \in X$$

(Minkowski mit Gitter $x\sigma(\mathcal{O}_L)$ und X anwenden)

- Betrachte nun $\mathcal{I} := \{\alpha\mathcal{O}_L \lhd \mathcal{O}_L \mid \exists x \in L_{\mathbb{R}}, \frac{1}{2} \leq |N(x)| \leq 1 \text{ und } x\sigma(\alpha) \in X\}$ ($\mathcal{I}$ ist wegen $(***)$ eine nicht leere Menge von Hauptidealen.)
- Wir berechnen: $\alpha\mathcal{O}_L \in \mathcal{I} \Rightarrow \exists x \in L_{\mathbb{R}}$, so daß $\frac{1}{2} \leq |N(x)| \leq 1$
  $|N(x\sigma(\alpha))| < R \Rightarrow |N(x)||N(\sigma(\alpha))| < R \Rightarrow |N(\sigma(\alpha))| < R/\frac{1}{2} = 2R$

- Wir haben berechnet : $\forall \alpha\mathcal{O}_L \in \mathcal{I}$ gilt $N(\alpha\mathcal{O}_L) < 2R$.
- Also ist $\mathcal{I}$ eine endliche Menge, d.h. $\mathcal{I} = \{\beta_1\mathcal{O}_L, \ldots, \beta_m\mathcal{O}_L\}$, $\beta_k \neq 0$.
- Sein nun $x \in L_{\mathbb{R}}$ mit $\frac{1}{2} \leq |N(x)| \leq 1$. $(***)$ liefert $0 \neq \alpha \in \mathcal{O}_L$, so daß $\alpha\mathcal{O}_L \in \mathcal{I}$, d.h. $\exists k$, so daß $\alpha\mathcal{O}_L = \beta_k\mathcal{O}_L$.
- Setze $\epsilon = \alpha\beta_k^{-1}$. Dann ist $x\sigma(\epsilon) = \underbrace{x\sigma(\alpha)}_{\in X}\sigma(\beta_k^{-1}) \in \sigma(\beta_k^{-1})X$.
- Wir haben gezeigt: $\forall x \in L_{\mathbb{R}}$ mit $\frac{1}{2} \leq |N(x)| \leq 1$, $\exists \epsilon \in \mathcal{O}_L^{\times}$, so daß $x\sigma(\epsilon) \in \bigcup_{k=1}^{m} \sigma(\beta_k^{-1})X$.
- Da X beschränkt ist, so ist $\sigma(\beta_k^{-1})X \quad \forall k = 1, \ldots, m$.
- Es folgt: $\bigcup_{k=1}^{m} \sigma(\beta_k^{-1})X$ ist beschränkt.
- Endlich wählen wir eine Schranke c für diese beschränkte Menge.