Algebra II und algebraische Zahlentheorie
Algebra B4

Prof. Dr. Salma Kuhlmann

Sommersemester 2021

Inhaltsverzeichnis für das Gesamtskript
zur Vorlesung: Algebra II und algebraische Zahlentheorie
(Sommersemester 2021)

Kapitel 5 Norm, Spur, Diskriminante

Kapitel 6 Gitter in $\mathbb{R}^n$

Kapitel 7 Die Einheitsgruppe $\mathcal{O}_K^\times$

B4: Algebra II
Sommersemester 2021
Frau Prof. Dr. Salma Kuhlmann

1.Vorlesung

13. April 2021

Wir werden in diesem Skript die gleiche Notationen, Definitionen, Begriffe und Terminologie (von Skript B1, B2 und B3) implizit und stillschweigend beibehalten und verwenden.
In dieser Vorlesung B4; Algebra II werden wir die Einführung in die Algebra der B3 fortsetzen. Wir werden ***Moduln*** *über Hauptidealringe studieren, und die Theorie der Körpererweiterungen auf Ringerweiterungen übertragen. Insbesondere werden wir* ***Ganze Ringerweiterungen*** *sowie* ***Dedekindringe*** *genau untersuchen. Diese Themen dienen zur Vorbereitung zur algebraischen Zahlentheorie, wo diese algebraische Klassen eine wesentliche Rolle spielen. Als Motivation, Leitmotiv, und wichtiges Beispiel führen wir in Kapitel 1 quadratische Zahlkörper ein.*

Kapitel 1: Quadratische Zahlkörper

Definition 1.1 i) Ein Zahlkörper ist eine endliche Körpererweiterung 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 $m(\alpha) = 0$.

Bemerkung 1.1
Wir werden gleich zeigen dass die Menge $\mathcal{O}_K := \{\alpha \in K \mid \alpha \text{ ganz } \}$ ein Ring ist. Algebraische Zahlentheorie studiert die Arithmetik vom Zahlkörper K, den Ring $\mathcal{O}_K$, seine Ideale, Einheiten und Faktorisierungseigenschaften.

Proposition 1.1
Sei K ein Zahlkörper. Es gilt: $\alpha \in \mathcal{O}_K \iff \text{MinPol}_{\mathbb{Q}}(\alpha) \in \mathbb{Z}[x]$. Insbesondere ist $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.

Beweis. „$\Leftarrow$“: klar.

„$\Rightarrow$“: 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 $\text{MinPol}_{\mathbb{Q}}(\alpha)$ ergibt nun $f(x) = \text{MinPol}_{\mathbb{Q}}(\alpha) \in \mathbb{Z}[x]$.

Sei $\alpha = \frac{r}{s} \in \mathbb{Q}$, dann ist $\text{MinPol}_{\mathbb{Q}}(\alpha) = x - \frac{r}{s}$, $r, s \in \mathbb{Z}$, $ggT(r, s) = 1$. 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? Wir werden diese Frage für quadratische Zahlkörper (Zahlkörper vom Grad 2) untersuchen. Wir werden die folgende Definition benötigen.

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

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

Zusatz: wenn $F = \mathbb{Q}$ gilt, kann man o.E. $D \in \mathbb{Z}$ sogar 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 $\epsilon_i = 1$.

Diese Behauptung gilt 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 $K = \mathbb{Q}(\sqrt{D'})$. □

Proposition 1.2
Sei K ein quadratische Zahlkörper und setze also $K := \mathbb{Q}(\sqrt{D})$ mit D quadratfrei. 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. Bemerke dass $D \equiv 0 \bmod 4$ nicht möglich ist.
• Wir prüfen zunächst dass $\mathbb{Z}[\omega]$ ein Ring ist: $\mathbb{Z}[\omega]$ abgeschlossen unter Addition ist klar. Wenn $\omega = \sqrt{D}$ ist es auch klar, dass $\mathbb{Z}[\omega]$ abgeschlossen unter Multiplikation ist.
Wenn $\omega = \frac{1+\sqrt{D}}{2}$ 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 $\mathbb{Z}[\omega] \subseteq \mathcal{O}_K$. Bemerke dass wenn $\alpha \in K$, $\alpha \notin \mathbb{Q}$, dann ist $\alpha = a + b\sqrt{D}$ (mit $a, b \in \mathbb{Q}$), und $\mathrm{MinPol}_{\mathbb{Q}}(\alpha) = x^2 - 2ax + (a^2 - b^2 D)$.
Sei nun $\alpha = r + s\omega \in \mathbb{Z}[\omega]$, $r, s \in \mathbb{Z}$, o.E. $s \neq 0$. Es genügt zu zeigen, dass $\mathrm{MinPol}_{\mathbb{Q}}(\alpha) \in \mathbb{Z}[x]$ (s. Proposition 1.1).

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

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

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:

(1) $D \equiv 1, 2, 3 \bmod 4$ und x, y beide gerade

oder

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

Das heißt:

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

B4: Algebra II
Sommersemester 2021
Frau Prof. Dr. Salma Kuhlmann

2.Vorlesung

15. April 2021

In diesem Skript werden wir den Ring $\mathcal{O}_K$, wobei K ein quadratischer Zahlkörper ist, weiter untersuchen. Wir werden sehen, dass $\mathcal{O}_K$ nicht immer faktoriell ist, und werden alternative Eigenschaften erforschen. Wir werden Kapitel 1 mit einer Untersuchung der Gruppe der Einheiten $\mathcal{O}_K^\times$ beenden. Zum Schluß werden wir Kapitel 2 anfangen.

Sei $K = \mathbb{Q}(\sqrt{D})$ stets ein quadratischer Zahlkörper.

§Faktorisierung in $\mathcal{O}_K$

- Der fundamentaler Satz der Arithmetik besagt dass $\mathbb{Z} = \mathcal{O}_\mathbb{Q}$ faktoriell ist. Im Allgemeinen ist aber $\mathcal{O}_K$ nicht faktoriell:
- (ÜB) Betrachte $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Dann ist $3 \in \mathbb{Z}[\sqrt{-5}]$ irreduzibel aber nicht prim. Andererseits haben wir in der B3 gezeigt, dass in einem faktoriellen Ring irreduzibele sind prim. Also ist $\mathbb{Z}[\sqrt{-5}]$ nicht faktoriell.
- (ÜB) Wir werden zeigen, dass $\mathcal{O}_K$ "noethersch" ist und damit gilt die Existenz der Faktorisierung in irreduzibele Elemente. Was fehlt also i.A ist die Eindeutigkeit:
- (ÜB) In $\mathbb{Z}[\sqrt{-5}]$ gilt

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

  $2, 3, 1+\sqrt{-5}$ und $1-\sqrt{-5}$ sind alle irreduzibel und nicht assoziiert.

Erinnerung: Seien I, J Ideale,

$$IJ := \{ \underbrace{\sum_i a_i b_i}_{\text{endliche Summe}} \mid a_i \in I, b_i \in J\} .$$

Zum Beispiel $I =< a >$ und $J =< b > \Rightarrow IJ =< ab >$

Die Idee von Kummer und Dedekind ist eine Faktorisierung von Idealen zu betrachten.

Beispiel 2.1
Die Faktorisierung vom Hauptideal $< 6 >$ in $\mathbb{Z}[\sqrt{-5}]$ ist:

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

Um (‡) zu beweisen, genügt es wegen (†) zu zeigen dass:

Behauptung 1:

$$< 2, 1+\sqrt{-5} >< 2, 1-\sqrt{-5} >=< 2 > , \; < 3, 1+\sqrt{-5} >< 3, 1-\sqrt{-5} >=< 3 > .$$

Beweis von 1 für $< 2 >$: Wir berechnen

$$< 2, 1+\sqrt{-5} >< 2, 1-\sqrt{-5} >=< 4, 2+2\sqrt{-5}, 2-2\sqrt{-5}, 6 >$$

und 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

$$< 2 >\subseteq < 2, 1+\sqrt{-5} >< 2, 1-\sqrt{-5} > .$$

Der Beweis von 1 für $< 3 >$ ist analog (ÜA). Wie angekündigt erhalten wir nun durch (†):

$$< 2, 1+\sqrt{-5} >< 2, 1-\sqrt{-5} >< 3, 1+\sqrt{-5} >< 3, 1-\sqrt{-5} >=< 2 >< 3 >=< 6 > .$$

□

Behauptung 2: (ÜB) Alle vier Ideale sind Primideale. Wir argumentieren folgendermassen für $< 3, 1-\sqrt{-5} >$. Die Abbildung ϕ ist ein surjektiver Homomorphismus mit $ker(\phi) =< 3 >$

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

also ist $\mathbb{Z}[\sqrt{-5}]/ < 3, 1-\sqrt{-5} > \cong \mathbb{Z}/ < 3 >$ ein Körper.

Bemerkung 2.1
(ÜB) Man könnte auch zeigen dass

$$< 2, 1+\sqrt{-5} >< 3, 1+\sqrt{-5} >=< 1+\sqrt{-5} > , \; < 2, 1-\sqrt{-5} >< 3, 1-\sqrt{-5} >=< 1-\sqrt{-5} >$$

und die andere Faktorisierung von 6 in (†) ausnutzen.

§Einheiten

Wir berechnen nun explizit die Einheiten von $\mathcal{O}_K = \mathbb{Z}[\omega]$. Dafür führen wir die Norm ein:

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

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

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

(ii) Für $D \equiv 1 \bmod 4$, $\omega = \frac{1+\sqrt{D}}{2}$, $\alpha \in \mathbb{Z}[\omega]$, $\alpha = r + s\frac{1+\sqrt{D}}{2} = (r + \frac{s}{2}) + (\frac{s}{2})\sqrt{D}$, mit $r, s \in \mathbb{Z}$ und
$N(\alpha) = (r+\frac{s}{2})^2 - D(\frac{s}{2})^2$, also $N(\alpha) = r^2 + rs + \frac{1-D}{4}s^2 \in \mathbb{Z}$.

Wir haben bewiesen: $N(\alpha) \in \mathbb{Z}$ für alle $\alpha \in \mathbb{Z}[\omega]$.

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

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

(4) $r + s\overline{\omega} \in \mathbb{Z}[\omega]$ (ÜA).

(5) Die Norm ist multiplikativ (ÜA).

(6) **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 $N(r + s\omega) = \pm 1$, 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 2.2
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

§Moduln

R ist stets ein kommutativer Ring mit Eins.

Definition 2.1 (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 $RN \subseteq N$.

B4: Algebra II
Sommersemester 2021
Frau Prof. Dr. Salma Kuhlmann

3.Vorlesung

20. April 2021

Wir werden in Kapitel 2 grundsätzliche Aussagen über Moduln feststellen. Ähnliche Aussagen und Beweise haben wir in der B3 für Gruppen und Ringe etabliert, so dass hier einige Beweise als Übungsaufgaben erscheinen. In diesem Skript werden wir hauptsächlich Untermoduln sowie Homomorphiesätze für Moduln studieren.

Sei R ist stets ein kommutativer Ring mit Eins und M ein R-Modul.

Beispiel 3.1 (i) $M = R$ ist selbst ein R-Moduln. Ein Ideal von R ist dann ein Untermodul. Insbesondere ist $M = \{0\}$ der trivialer Modul.

(ii) Wenn $R = \mathbb{Z}$, dann ist ein $\mathbb{Z}$-Modul eine abelsche Gruppe und ein Untermodul eine Untergruppe.

(iii) Wenn $R = K$ ein Körper ist, dann ist ein K-Modul ein K-Vektorraum, und ein Untermodul ein Unterraum.

Definition 3.1
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) $\phi \in \mathrm{Hom}_R(M,N) \Rightarrow \ker(\phi) \leq M \wedge \ \mathrm{Im}\ (\phi) \leq N$.

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

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

ist ein R-Modul Homomorphismus (die Projektion).

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

Beweis. ÜA. □

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

Beweis. ÜA. □

Definition 3.2
Sei $A \subseteq M$.

(i) Für $a \in M$ sei $Ra := \{ra \mid r \in R\} \leq M$ der von a erzeugte Hauptmodul.

(ii) Die Summe $\sum_{i\in I} M_i \leq M$ einer Familie $(M_i)_{i\in I}$ von Untermoduln eines R-Moduls M ist der Untermodul

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

(iii) Eine lineare Kombination aus A ist ein $x \in M$, so dass $x = \sum_i r_i x_i$ (endliche Summe) mit $r_i \in R, x_i \in A$.

(iv) $\mathrm{Span}_R(A) := \{x \mid x \text{ lineare Kombination aus } A\} = \sum_{a\in A} Ra$.

(v) Der von A erzeugte Untermodul von M ist $\sum_{a\in A} Ra$.

(vi) 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 3.3 (i) Die direkte Summe einer Familie $(M_i)_{i\in I}$ von R-Moduln ist der R-Modul

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

versehen mit der koordinatenweise Summe $(x_i)_{i\in I} + (y_i)_{i\in I} := (x_i + y_i)_{i\in I}$ und für $r \in R$ der Skalarmultiplikation $r(x_i)_{i\in I} := (rx_i)_{i\in I}$.

(ii) Ein R-Modul M ist direkte Summe einer Familie $(M_i)_{i\in I}$ von seinen Untermoduln 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, dass heißt $\bigoplus_{i\in I} M_i \simeq \sum_{i\in I} M_i = M$.

Notation: In diesem Fall, werden wir oft einfach schreiben $M = \bigoplus_{i\in I} M_i$.

(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.

Lemma 3.4
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 3.2
$G = \mathbb{Z}_4$, $H =< 2 >$ hat kein Komplement im $\mathbb{Z}$-Modul G, weil die einzigen Untermoduln $\{0\}, H$ und G sind.

Lemma 3.5
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 □

B4: Algebra II
Sommersemester 2021
Frau Prof. Dr. Salma Kuhlmann

4.Vorlesung

22. April 2021

In diesem Skript werden wir die Begriffe von LA I für einen R- Moduln anstatt ein K-Vektorraum (insbesondere wenn der Ring R kein Körper K ist) anpassen. Dafür werden wir Torsionselemente in R, Torsionsfreie Moduln, sowie freie Moduln definieren. Wir werden dann lineare Unabhängigkeit, Basis und Dimension für freie Moduln studieren. Die Beweise hierfür sind wie in der LA I, deshalb werden einige im ÜB bearbeitet.

Sei R ist stets ein kommutativer Ring mit Eins und M ein R-Modul.

Definition 4.1 (i) $x \in M$ ist Torsionselement $\Leftrightarrow \exists r \in R$, r ist kein Nullteiler, mit $rx = 0$.

(ii) Setze $M_{\text{tor}} := \{x \in M \mid x \text{ Torsionselement}\}$. Dann ist M_{tor} ein Untermodul von M (ÜA), den wir Torsionsmodul von M nennen.

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

Definition 4.2
Eine Untermenge $S \subseteq M$ ist linear unabhängig, wenn für alle $r_i \in R$ und $x_i \in S$ gilt:

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

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

Beispiel 4.1
Es folgt aus Definition 4.1 dass $x \in M_{\text{tor}} \Rightarrow \{x\}$ ist nicht linear unbhängig.

Definition 4.3 (i) $S \subseteq M$ ist eine Basis $\Leftrightarrow S$ ist linear unabhängig und erzeugt M (i.e. $\text{Span}_R(S) = M$).

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

Bemerkung 4.1
Die Untermenge S ist genau dann eine Basis von M, wenn jedes $x \in M$ eine eindeutige Darstellung als lineare Kombination aus S hat (i.e. $x = \sum_{i \ I} r_i x_i$ für geeignete $r_i \in R$ und $x_i \in S$.)

Beispiel 4.2 (i) Jeder K-Vektorraum über ein Körper K hat eine Basis und ist also frei als K-Modul.

(ii) Betrachte aber $G := \mathbb{Z}_2 =< 1 >$, dann ist G nicht frei als $\mathbb{Z}$-Modul, weil $1 \in G_{\text{tor}}$.

Lemma 4.1 charakterisiert Basen von torsionsfreie Moduln, der Beweis folgt unmittelbar aus den Definitionen:

Lemma 4.1
Sei R ein Integritätsbereich, M torsionsfrei und $S \subseteq M$. Folgende Bedingungen sind äquivalent:

(1) M ist frei mit Basis S

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

Beweis. ÜA. □

Lemma 4.2
Sei $I \lhd R$, dann sind

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

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

Beweis. (1) Der Beweis folgt unmittelbar (ÜA).

(2) Die Verknüpfung Summe auf M/IM ist die Summe von Nebenklassen wie üblich. Betrachte nun die Verknüpfung

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

und verifiziere dafür die Axiome für Moduln (ÜA).

□

Lemma 4.3
Sei M frei als R-Modul mit Basis $\{x_j\}_{j \in J}$. Sei $I \lhd R$. Dann ist M/IM frei als R/I-Modul mit Basis $\{\overline{x}_j\}_{j \in J}$

Beweis. Bemerke dass $\{\overline{x}_j\}$ offensichtlich M/IM erzeugt (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 schreiben wir jedes $y_l = \sum_k r_{l,k} x_k$, und schreiben entsprechend $\sum_l t_l y_l$ um. Wir 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 4.4
Sei M ein freier R-Modul, und S eine Basis mit $|S| = n \in \mathbb{N}$. Dann haben alle anderen Basen Kardinalität n.

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

Korollar 4.5
M endlich erzeugt und frei$\Rightarrow$ 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 (für I maximales Ideal), also ist M/IM endlich dimensional und damit sind notwendigerweise alle Basen von M endlich. □

Bemerkung 4.2
Wir haben gezeigt: M frei mit $\{x_j\}_{j\in J}$ Basis, dann ist $|J|$ eindeutig definiert.

Definition 4.4
Sei M frei mit Basis $\{x_j\}_{j\in J}$. Wir definieren $\dim_R M := |J|$.

Bemerkung 4.3
Wir haben in Korollar 4.4 gezeigt:
$\dim_R M = \dim_K V$, wobei $K = R/I$ und $V = M/IM$, I ein maximales Ideal von R.

B4: Algebra II
Sommersemester 2021
Frau Prof. Dr. Salma Kuhlmann

5.Vorlesung

27. April 2021

In diesem Skript charakterisieren wir endlich erzeugte, beziehungsweise freie Moduln, und erklären den Zusammenhang zwischen freie und torsionsfreie Moduln. Im letztem Abschnitt setzen wir voraus, dass R ein Hauptidealbereich ist, und untersuchen endlich erzeugte, beziehungsweise freie Moduln und ihre Untermoduln.

Sei R ist stets ein kommutativer Ring mit Eins und M ein R-Modul.

Definition 5.1
Der Modul $R^n := \{(r_1, \dots, r_n) \mid r_i \in R\}$ mit Komponentenweise Addition und Skalarmultiplikation, und standard Basis: $\{e_i \mid i = 1, \dots, n\}$ ist der freie R-Modul vom Rang n.

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

Beweis. „$\Leftarrow$“ Lemma 3.5
„$\Rightarrow$“ Sei $\{x_1, \dots, x_n\} \subseteq M$ erzeugend. Betrachte

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

Dann ist ϕ ist ein surjektiver Homomorphismus mit $K := \ker(\phi)$ (ÜA). Die Behauptung folgt nun aus Proposition 3.2 (Homomorphiesatz für Moduln). □

Korollar 5.2
Sei $M \neq \{0\}$ endlich erzeugt, mit $\{x_1, \dots, x_n\}$ erzeugend, und ϕ der surjektiver Homomorphismus in Lemma 5.1. Dann gilt: M ist genau dann frei mit Basis $\{x_1, \dots, x_n\}$, wenn $\ker(\phi) = \{0\}$. Inbesondere für $x \neq 0$, $x \in M$, ist der Hauptmodul Rx genau dann frei mit Basis $\{x\}$, wenn $\{r \in R \mid rx = 0\} = \{0\}$.

In Definition 4.1 haben wir folgende definiert:

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

Lemma 5.3 (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 $\bar{x} = 0$.

□

Lemma 5.4 (i) M frei $\Rightarrow M$ torsionsfrei.

(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.

Beweis. Wir beweisen (i): Sei $x \in M_{\text{tor}}$ und $\{x_i\}_{i \in J}$ eine Basis von M. Schreibe $x = \sum r_i x_i$ und sei $r \in R$ kein Nullteiler, so dass $rx = 0$. Es folgt $\sum (rr_i)x_i = 0$. Aber $\{x_i\}$ linear unabhängig $\Rightarrow rr_i = 0 \, \forall i \; \Rightarrow r_i = 0 \, \forall i \; \Rightarrow x = 0$.
Beweise von (ii), (iii), (iv): ÜA.

□

Lemma 5.4 werden wir stillschweigend in den nächsten Abschnitt benutzen.

§Moduln über Hauptidealbereiche

Sei nun R stets ein Hauptidealbereich, M, F und N R- Moduln.

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 $M = M_n$). Da $x_1 \notin M_{\text{tor}}$, ist Rx_1 frei. Betrachte $M_1 = M \cap Rx_1$ und

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

• Da $M_1 \leq Rx_1$ ist $\phi^{-1}(M_1) \trianglelefteq R$, also ist $\phi^{-1}(M_1) =< a_1 >$ 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, $\dim M_m \leq m$.
Die Menge $\{a \in R \mid \exists x \in M, \text{ so dass } x = b_1 x_1 + \cdots + b_m x_m + a x_{m+1}\}$ 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 3.5 $\Rightarrow N = \Pi^{-1}(N)/K$ 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
$ay + b_1v_1 + \cdots + b_nv_n = 0$ 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

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

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

□

B4: Algebra II
Sommersemester 2021
Frau Prof. Dr. Salma Kuhlmann

6.Vorlesung

29. April 2021

Unser nächstes Ziel ist es, den Struktursatz für endlich erzeugte Moduln über Hauptidealbereiche zu beweisen (Satz 6.8). In diesem Skript bauen wir den Beweis schrittweise auf. Satz 6.2 ergibt eine Zerlegung als direkte Summe von frei und Torsionsmodul, Satz 6.6 untersucht die Struktur vom Torsionsmodul, und Satz 6.7 ergibt eine weitere Verfeinerung der Struktur. Für den Beweis vom Satz 6.7 brauchen wir einige Vorbereitung, die wir am Ende des Skriptes bringen. Satz 6.7 wird schließlich in Skript 7 zuende bewiesen.

Sei R stets ein kommutativer Ring mit Eins, und M ein R–Modul.

Lemma 6.1
Seien 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 $F := \operatorname{Span}_R\{x_i \mid i \in I\}$. Dann ist $\{x_i\}_{i\in I}$ linear unabhängig (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: $E = F + \ker(f)$.
Außerdem ist $F \cap \ker(f) = \{0\}$ (ÜA). □

Sei nun R ein Hauptidealbereich und M ein R–Modul.

Satz 6.2
Sei R ein Hauptidealbereich und M ein R–Modul. 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.

Beweis. 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 6.1 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. □

Definition 6.1
$\dim_R F$ im Satz 6.2 ist der (freier) Rang von M.

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

Definition 6.2 (a) Für $r \in R$ ist $M[r] := \{x \in M \mid rx = 0\}$ der r-Torsionsmodul.

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

Lemma 6.3
Sei M ein endlich erzeugter Torsionsmodul, dann $\exists a \in R, a \neq 0$ mit $aM = 0$.

Beweis. 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 6.4
Sei M endliche erzeugter Torsionsmodul und wähle $0 \neq a \in R$ mit $aM = 0$. Wenn $a = bc$ mit $ggT(b, c) = 1$, dann ist $M = M[b] \bigoplus M[c]$.

Beweis. Da R HIR ist, 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 $v = (xb + yc)v = xbv + ycv = 0$. □

Lemma 6.5
M endlich erzeugt $\Rightarrow |\{p \in R \mid p \text{ prim und } M[p^\infty] \neq 0\}| < \infty$.

Beweis. Wähle $a \neq 0$ mit $aM = 0$, $a \in R$. Da R HIR ist, ist R faktoriell. Wir können also die Primfaktorisierung von a ausnutzen, und Lemma 6.4 wirderholt anwenden. Die Induktion ergibt

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

□

Bemerkung 6.1
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 $M[q] = 0$

Wir können nun aus Lemma 6.5 folgern:

Satz 6.6
Sei $0 \neq M$ endlich erzeugter Torsionsmodul. Dann ist

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

Beweis. Sei $a \in R$ mit $aM = 0$. Da R HIR ist, ist R faktoriell. Wir können also die Primfaktorisierung von a ausnutzen, und Lemma 6.5 anwenden (ÜA). □

Wir wollen nun diese $M[p^\infty]$ weiter untersuchen. Den folgenden Satz werden wir im Skript 7 beweisen:

Satz 6.7
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 $M[p^\infty] \cong R/ < p^{\nu_1} > \oplus \cdots \oplus R/ < p^{\nu_s} >$.

Als Korollar zum Satz 6.7 erhalten wir sofort:

Satz 6.8
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 6.7 brauchen wir:

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 alle $a_1, \ldots, a_m \in R$.

   Bemerkung 6.2
   Wenn $y_1, \ldots, y_m \in M$ linear unabhängig sind, dann sind sie auch unabhängig; die Umkehrung dieser Aussage gilt für Torsionsfreie Moduln (ÜA).

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 Periode für x.

Bemerkung 6.3 (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 $l \leq \nu$.

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

(iii) Sei $x \in M$ mit Periode p^ν; setze $\overline{M} := M/Rx$. 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 $\mu \leq \nu$.

Beweis. (i): Nehme $l :=$ die kleinste natürliche Zahl, wofür es gilt $p^l x = 0$.

(ii), (iii), (iv): ÜA. □

B4: Algebra II
Sommersemester 2021
Frau Prof. Dr. Salma Kuhlmann

7.Vorlesung

4. Mai 2021

In diesem Skript beweisen wir Satz 6.7 und damit den Struktursatz für endlich erzeugte Moduln über Hauptidealbereiche Satz 6.8. Im nächstem Abschnitt untersuchen wir dann Noethersche Moduln und Ringe.

Sei R stets ein Hauptidealbereich und M ein R–Modul.

Wir müssen zuerst Lemma 7.1 beweisen. Wir werden dafür Bemerkung 6.3 stillschweigend gebrauchen.

Lemma 7.1
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 $x_1, y_1, \ldots, y_m \in M$ unabhängig sind.

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 es gibt $r \in R$ so dass $p^n y = rx_1 \in Rx_1$. Da R faktoriell ist, sei $c \in R, p \nmid c$, und $s \leq \nu$ so dass

$$(\dagger) \qquad p^n y = rx_1 = p^s c x_1 \,.$$

• 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.
• 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

$$(\ddagger) \qquad ax_1 + a_1 y_1 + \cdots + a_m y_m = 0$$

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 $a_i y_i = 0$ für alle i und damit ist (zurück in (‡)) auch $ax_1 = 0$.

□

Zur Erinnerung, wiederholen wir hier die Aussage vom Satz 6.7:

Satz 6.7 : Sei $0 \neq M$ endlich erzeugt; $p \in R$ prim mit $M[p^\infty] \neq 0$. Dann existiert eine eindeutige Folge $1 \leq \mu_1 \leq \cdots \leq \mu_s \in \mathbb{N}$, so dass $M[p^\infty] \cong R/ < p^{\mu_1} > \oplus \cdots \oplus R/ < p^{\mu_s} >$.

Beweis vom Satz 6.7. $M[p^\infty]$ endlich erzeugt$\Rightarrow$ O.E. $M = M[p^\infty]$ und (da M endlich erzeugt ist) $\exists x_1 \in M$ mit Periode p^ν, $\nu \in \mathbb{N}$ minimal so dass $M = M[p^\nu]$ (ÜA).
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: $\bar{a}_1 = \bar{a} \Rightarrow (a - a_1) = pa_2 \Rightarrow (a_1 - a)x = a_2 px = 0$.
Also ist $M[p]$ ein $R/ < p >$-Vektorraum.
Setze $\overline{M} := M/Rx_1$. Analog zeigt man dass $\overline{M}[p]$ ein $R/ < p >$-Vektorraum (ÜA).

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

Beweis. Seien $\bar{y}_1, \ldots \bar{y}_m \in \overline{M}[p]$ und $R/ < p >$-linear unabhängig. Lemma 7.1 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, und damit auch $R/ < p >$-linear unabhängig (ÜA). □

• Wir zeigen nun die Existenzaussage im Satz. Wir argumentieren per Induktion nach $\dim_{R/<p>} M[p]$. O.E. ist $\overline{M} \neq 0$ (sonst ist $M \cong Rx_1 \cong R/ < p^\nu >$).

Die Induktionsannahme impliziert dass

$$\overline{M} = \overline{M}[p^\infty] \cong R\bar{x}_2 \oplus \cdots \oplus R\bar{x}_s$$

und die Periode von $\bar{x}_i$ ist p^{n_i}, das heißt

$$R\bar{x}_i \cong R/ < p^{n_i} >, i = 2, \ldots, s\,.$$

Lemma 7.1 impliziert dass $\exists x_2, \ldots, x_s \in M$ so dass x_i Periode p^{n_i} hat und $x_1, \ldots, x_s$ unabhängig, das heißt:

$$M = M[p^\infty] \cong Rx_1 \oplus \cdots \oplus Rx_s \cong R/ < p^\nu > \oplus R/ < p^{n_2} > \oplus \cdots \oplus R/ < p^{n_s} >,$$

wie behauptet.

• Wir zeigen nun die Eindeutigkeit.
Sei

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

wobei $\mu_1 \leq \cdots \leq \mu_s$. Setze $\mu := \mu_s$. Aus $(*)$ folgt dass $M = M[p^\mu] \supsetneq M[p^{\mu-1}]$, i.e. μ ist minimal dafür dass $M = M[p^\mu]$, also ist μ **eindeutig**. Beachte, dass

$$M[p], M[p^2]/M[p], \ldots, M[p^\mu]/M[p^{\mu-1}]$$

alle $R/ < p >$-Vektorräume sind, und:

$$(\dagger) \qquad M[p] \cong < p^{\mu_1 - 1} > / < p^{\mu_1} > \oplus \cdots \oplus < p^{\mu_s - 1} > / < p^{\mu_s} > .$$

Diese letzte Behauptung $(\dagger)$ folgt aus $(*)$ und diese allgemeine Bemerkungen (ÜA):

$$(R/ < p^m >)[p] = < p^{m-1} > / < p^m > \text{ und } (N \oplus K)[p] \cong N[p] \oplus K[p]\,.$$

Bemerke auch dass die $\dim_{R/<p>} < p^{\mu_i - 1} > / < p^{\mu_i} >= 1$: die Abbildung

$$\begin{array}{rcl} R & \to & < p^{m-1} > / < p^m > \\ x & \mapsto & p^{m-1}x + < p^m > \end{array}$$

ist ein surjektiver Homomorphismus mit Kernel $< p >$.
Also folgt aus (†) dass

$$\dim_{R/<p>} M[p] = s = \sharp\{i \mid \mu_i \geq 1\} ,$$

damit ist s **eindeutig**.
Schreibe nun (folgt analog zum (†))

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

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

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

Da $< p^{m-2} > / < p^{m-1} > \cong R/ < p >$ und $\dim_{R/<p>} < p^{m-2} > / < p^{m-1} >= 1$ ist also

$$\dim_{R/<p>} M[p^2]/M[p] = \sharp\{i \mid \mu_i \geq 2\} .$$

Allgemeiner berechnen wir

$$(‡) \qquad \dim_{R/<p>} M[p^m]/M[p^{m-1}] = \sharp\{i \mid \mu_i \geq m\}, m = 1, 2, \ldots, \mu .$$

Insbesondere:

$$\dim_{R/<p>} M[p^\mu]/M[p^{\mu - 1}] = \sharp\{i \mid \mu_i \geq \mu\} = \sharp\{i \mid \mu_i = \mu\} .$$

Da s, und die größte natürliche Zahl μ der Folge $\mu_1 \leq \cdots \leq \mu_s$ eindeutig sind, folgt nun aus (‡) die Eindeutigkeit von μ_i für alle $i = 1, \cdots, s$ (ÜA). □

§Noethersche Moduln

Sei R ein Ring, M ein R-Modul.

Proposition 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. (1) $\Rightarrow$ (2): Setze $N := \bigcup_i N_i$, $N \leq M$.
Seien $x_1, \ldots, x_r \in N$ mit $N := \operatorname{Span}_R\{x_1, \ldots, x_r\}$ 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 $N' = \operatorname{Span}_R\{x_1, \ldots, x_r\}$ ein maximales Element von $\mathcal{U}$. Ist $N \supsetneq N'$, existiert dann $x \in N \backslash N'$ und $\operatorname{Span}_R\{x_1, \ldots, x_r, x\} \supsetneq N'$: Widerpsruch. $\square$

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

(b) Insbesondere: R ist ein noethersche Ring wenn jedes Ideal von R endlich erzeugt ist.

B4: Algebra II
Sommersemester 2021
Frau Prof. Dr. Salma Kuhlmann

8.Vorlesung

6. Mai 2021

In diesem Skript untersuchen wir Noethersche Moduln und Ringe weiter, insbesondere beweisen wir Hilbert's Basissatz und einige Korollare. Damit beenden wir Kapitel 2. Am Ende des Skriptes beginnen wir Kapitel 3 über Ganzheit.

Sei R stets ein kommutativer Ring mit Eins und M ein R–Modul.

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

Beweis. „$\Rightarrow$“ Sei $N' \leq N$, nun $N' \leq N \Rightarrow N' \leq M$, also ist N' endlich erzeugt. Damit haben wir gezeigt dass N noethersch ist. 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 (wegen Lemma 3.5).

„$\Leftarrow$“ Sei $A \leq M$. Wir nutzen dass $A + N/N \cong A/A \cap N$ (siehe ÜB).
Nun $A + N/N \leq M/N \Rightarrow A + N/N$ endlich erzeugt, es folgt $A/A \cap N$ ist endlich erzeugt.
Aber auch $A \cap N \leq N \Rightarrow A \cap N$ ist endlich erzeugt. Lemma 3.5 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 $\deg(f_i') = k+1$ (so dass f_i' und f_i den gleichen Leitkoeffizient haben). 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 $f \in< f_1, \ldots, f_n, g_1, \ldots, g_m >$ □

□

Per Induktion nach n bekommen wir nun:

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

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.

Für die weitere Untersuchung brauchen wir (vgl. Skript Lineare Algebra II; Satz 11.13):

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:

$$\det(C)x_j = \det(C_j) \forall j$$

B4: Algebra II
Sommersemester 2021
Frau Prof. Dr. Salma Kuhlmann

9.Vorlesung

11. Mai 2021

In diesem Skript untersuchen wir ganze Ringerweiterungen und den ganzen Abschluß. Wir beenden den Abschnitt mit dem wichtigem Satz 9.5. Im letztem Abschnitt studieren wir ganz abgeschlossene Integritätsbereiche und ihre Eigenschaften. Diese Begriffe werden wir in Kapitel 4 dieser Vorlesung, sowie allgemeiner in der Vorlesung algebraische Zahlentheorie benötigen.

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 $\alpha M \subseteq M$.

Beweis. „$\Rightarrow$“ Sei $\alpha^n + r_1\alpha^{n-1} + \cdots + r_n = 0$, $r_i \in R$. Wir können $M = R[\alpha]$ nehmen, i.e.:

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

Beweis. Wir haben: $\alpha^n \in \sum_{i=0}^{n-1} R\alpha^i$. Sei $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \in M$, berechne:

$$\alpha(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}) = \alpha a_0 + a_1\alpha^2 + \cdots + a_{n-2}\alpha^{n-1} + a_{n-1}\underbrace{\alpha^n}_{\in M} \in M\,.$$

□

„$\Leftarrow$“
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 geeignete $a_{ij} \in R$. 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 $C\underline{v} = \begin{pmatrix}0\\ \vdots\\ 0\end{pmatrix}$:

$$\det(C)v_j = \det(C_j) = 0$$

Nun gibt es mindestens ein j gibt mit $v_j \neq 0$ (weil $0 \neq M$). Außerdem sind $v_j \in S$ und $\det(C) \in S$ und S ist ein integritätsbereich. Es folgt: $\det(C) = 0$.
Das Berechnen dieser Determinante ergibt schließlich eine Gleichung
$\alpha^n + c\alpha^{n-1} + \cdots + c_n = 0\,, c_i \in R$ (ÜA).

□

Definition 9.1
Seien R, S integritätsbereiche, $R \subseteq S$. Der ganze Abschluss von R in S ist

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

Korollar 9.2
Seien $R \subseteq S$ Erweiterung von Integritätsbereichen. Der ganze Abschluss $\overline{R}^S$ von R in S ist ein Unterring von S (der R enthält).

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 $\{e_i f_j \mid i = 1, \ldots, m, j = 1, \ldots, n\}$ eben MN.

(c) MN ist abgeschlossen unter multiplikation durch $\alpha\beta$ und $\alpha \pm \beta$. Das heißt:

$$(\alpha\beta)MN \subseteq MN \text{ und } (\alpha \pm \beta)MN \subseteq MN$$

(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.

Beweis. Folgt aus Proposition 9.1 □

Unser nächses Ziel ist Satz 9.5 zu beweisen, brauchen wir noch diese:

Proposition 9.4
Sei R ein Integritätsbereich, $K := \mathrm{Quot}(R)$, 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 $a_i \in K = \mathrm{Quot}(R)$. 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

$$(d\alpha)^m + (a_1 d)(d\alpha)^{m-1} + \cdots + a_m d^m = 0\,.$$

□

Satz 9.5
Sei R ein Integritätsbereich, $K := \mathrm{Quot}(R)$, L/K eine algebraische Körpererweiterung und $\overline{R}^L$ der ganze Abschluss von R in L. Es gilt: $L = \mathrm{Quot}(\overline{R}^L)$.

Beweis. Sei $\alpha \in L$, Proposition 9.4 $\Rightarrow$ α lässt sich schreiben als $\alpha = \frac{d\alpha}{d}$, $d \in R, d\alpha \in \overline{R}^L$, das heißt $\alpha \in \mathrm{Quot}(\bar{R}^L)$, also $\mathrm{Quot}(\bar{R}^L) \supseteq L$. Da die Inklusion $\mathrm{Quot}(\bar{R}^L) \subseteq L$ offensichtlich ist (ÜA), ist der Satz bewiesen. □

§Ganz abgeschlossene Integritätsbereiche

Definition 9.2
Ein Integritätsbereich R ist ganz abgeschlossen $\Leftrightarrow \overline{R}^K = R$, wobei $K := \mathrm{Quot}(R)$

Beispiel 9.1
Faktorielle Integritätsbereiche sind ganz abgeschlossen (ÜB).

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 beweisen nun dass alle Nullstellen von $f(x)$ ganz über R sind:

Beweis. Sei α' eine Nullstelle, dann gibt es eine Isomorphie: $K(\alpha) \xrightarrow{\sigma}_{\sim} K(\alpha')$ mit $\sigma_{|K} = \ \mathrm{Id}$ und $\alpha \mapsto \alpha'$. Anwendung von σ auf $(*)$ ergibt nun: $(\alpha')^m + a_1(\alpha')^{m-1} + \cdots + a_m = 0$. □

Nun sind die Koeffizienten von $f(x)$ *elementare symmetrische Polynome in den Nullstellen* von $f(x)$ (ÜB). Da die Menge aller ganzen Elementen ein Teilring ist, folgt dass alle Koeffizienten von $f(x)$ ganz über R sind. Diese Koeffiziente sind andererseits in K. Da R ganz abgeschlossen ist folgt nun: alle Koeffiziente von f sind $\in R$. □

Unser nächstes Ziel ist die *Transitivität von Ganzheit* zu zeigen. Für den Beweis brauchen wir:

Lemma 9.7
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 (ÜA). □

B4: Algebra II
Sommersemester 2021
Frau Prof. Dr. Salma Kuhlmann

10.Vorlesung

18. Mai 2021

In diesem Skript werden wir zunächst Ganzheit weiter untersuchen und dann Kapitel 3 mit einer Diskussion über Ganzheit und Lokalisierung beenden. Danach werden wir unser letztes Kapitel (Kapitel 4) beginnen.

Wir betrachten stets kommutative Ringe mit Eins.

Für den Beweis von Proposition 10.2 brauchen wir noch:

Lemma 10.1
Sei $B = A[\beta_1, \dots, \beta_m]$ eine Ringerweiterung, wobei β_j ganz über A ist $\forall j = 1, \dots, m$. Dann ist B endlich erzeugt als A-Modul, und ganz über A.

Beweis. Beweis per Induktion nach m.

• Induktionsanfang: $m = 1$
Setze $\beta := \beta_1$, wobei β ganz über A ist. Da $B = A[\beta]$ ist B ganz über A wegen Korollar 9.3.
Wir zeigen daß B endlich erzeugt als A-Modul ist. Seien $n \in \mathbb{N}$, und $a_i \in A\,;\ i = 1, \cdots, n$, so daß $\beta^n + \cdots + a_n = 0$

Behauptung: $1, \beta, \beta^2, \dots, \beta^{n-1}$ erzeugen B als A-Modul.

Beweis. In der Tat, sei $b \in A[\beta]$ beliebig, d.h. es gibt $N \in \mathbb{N}$ und $c_i \in A\,;\ i = 1, \cdots, N$ so daß

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

Da $\beta^n \in \sum_{i=0}^{n-1} A\beta^i$, kann man b umschreiben, indem man $c_N\beta^N$ als A-lineare Kombination der $1, \dots, \beta^{n-1}$ schreibt und in $(*)$ ersetzt. □

• Induktionsschritt: schreibe $B = A[\beta_1, \dots, \beta_{m-1}, \beta_m] = \underbrace{A[\beta_1, \dots, \beta_{m-1}]}_{:=D}[\beta_m]$
D ist endlich erzeugt als A-Modul per Induktionsannahme und $B = D[\beta_m]$. Da β_m (a fortiori) auch ganz über D ist, ist B endlich erzeugt als D-Modul per Induktionsanfang.
Also sind $A \subseteq D \subseteq B$ wie in Lemma 9.7 und damit ist B endlich erzeugt als A-Modul. Außerdem gilt auch daß B ganz über A ist (wegen Korollar 9.3). □

Proposition 10.2 (Transitivität von Ganzheit)
Seien $A \subseteq B \subseteq C$ Integritätsbereiche. Wenn B ganz über A und C ganz über B sind, dann ist C ganz über A.

Beweis. Seien $\gamma \in C$ und $b_i \in B$, so daß $\gamma^n + b_1\gamma^{n-1} + \cdots + b_n = 0$
Setze $B' := A[b_1, \dots, b_n]$. Da die b_i ganz über A sind, ist B' endlich erzeugt als A-Modul (s. Lemma 10.1). Nun ist γ bereits ganz über B' (Wahl der b_i), also ist $B'[\gamma]$ endlich erzeugt als B'-Modul (s. Lemma 10.1). Also ist $B'[\gamma]$ endlich erzeugt als A-Modul (s. Lemma 9.7). Damit ist γ ganz über A (wegen Korollar 9.3). □

Korollar 10.3
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

$$R \underset{\text{ganz}}{\subseteq} \overline{R}^S \underset{\text{ganz (wegen Lemma 10.1)}}{\subseteq} \overline{R}^S[\gamma] \,.$$

Damit gilt nach Proposition 10.2 daß auch $R \underset{\text{ganz}}{\subseteq} \overline{R}^S[\gamma]$. Somit ist $\gamma \in \overline{R}^S$. □

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

Lokalisierung und Ganzheit
Für eine Erinnerung an Lokalisierung siehe Skript 3 und 4 der Algebra 1 (B3) Vorlesung. Sei R stets ein kommutativer Ring mit Eins.

Notation (Erinnerung) i) Wir bezeichnen $\text{Spec}(R) :=$ Menge aller Primideale von R.

ii) Für $\mathfrak{p} \lhd R$ Primideal, ist $R_\mathfrak{p} := \{\frac{r}{d} \mid r \in R, d \notin \mathfrak{p}\}$ die Lokalisierung von R nach $\mathfrak{p}$.

iii) R ist lokal, wenn R nur ein maximales Ideal besitzt.

Die Beweise von Lemma 10.5, Proposition 10.6 und Proposition 10.7 sind ÜA.

Lemma 10.5
R ist lokal $\Leftrightarrow R \backslash R^\times$ ist ein Ideal.

Beweis. siehe ÜB. □

Proposition 10.6
Sei $I \lhd R$ und $D \subseteq R$ multiplikativ mit $0 \notin D$.

a) Setze $I^e := D^{-1}RI$ das von I in $D^{-1}R$ erzeugte Ideal. Es gilt: $I^e = \{\frac{a}{d} \mid a \in I, d \in D\}$.

b) Sei nun $I \lhd D^{-1}R$. Betrachte das Ideal $I^c := I \cap R \lhd R$. Es gelten

(i) $I \lhd D^{-1}R \Rightarrow I^{ce} = I$

(ii) $I \lhd R$ prim und $I \cap D = \varnothing \Rightarrow I^{ec} = I$

c) Die Abbildung $\mathfrak{p} \mapsto \mathfrak{p}^e$ definiert eine inklusionserhaltende Bijektion zwischen

$$\{\mathfrak{p} \in \text{Spec}(R) : p \cap D = \varnothing\} \text{ und } \text{Spec}(D^{-1}R) \,.$$

d) Sei $\mathfrak{p} \lhd R$ prim. Die Abbildung $\mathfrak{q} \mapsto \mathfrak{q}R_\mathfrak{p}$ definiert eine inklusionserhaltende Bijektion zwischen

$$\{\mathfrak{q} \in \text{Spec}(R) \mid \mathfrak{q} \subseteq \mathfrak{p}\} \text{ und } \text{Spec}(R_\mathfrak{p}) \,.$$

e) Insbesondere besitzt $R_\mathfrak{p}$ nur ein maximales Ideal, nämlich $\mathfrak{p}R_\mathfrak{p}$.

Beweis. ÜA. Siehe Aufgabe 3.4* in ÜB 3 der Algebra 1 Vorlesung (B3) im WiSe 2020/2021. □

Proposition 10.7
Sei $D \subseteq R$ multiplikativ mit $0 \notin D$

(i) R noethersch $\Rightarrow D^{-1}R$ noethersch.

(ii) R ganz abgeschlossen$\Rightarrow D^{-1}R$ ganz abgeschlossen.

(iii) $R \subseteq R'$ ganze Erweiterung$\Rightarrow D^{-1}R \subseteq D^{-1}R'$ ganze Erweiterung.

Beweis. siehe ÜB. □

Kapitel 4: Dedekindringe

In diesem Kapitel werden wir Dedekindringe einführen und charakterisieren. Ein Hauptziel von diesem Kapitel ist zu zeigen daß wenn R ein Dedekindring ist mit Quotientenkörper K und L/K eine endlich separable Erweiterung ist, dann ist $\overline{R}^L$ ein Dedekindring. Ein weiteres Ziel ist gebrochene Ideale und die Klassengruppe von R einzuführen. Diese Resultate werden wir in der Vorlesung algebraische Zahlentheorie unbedingt benotigen.

Wir betrachten stets kommutative Ringe mit Eins.

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

Beispiel 10.1
Wenn $I =< x >$ und $J =< y >$, dann ist $IJ =< xy >$.

Definition 10.1
Ein Ring R ist ein Dedekindring, wenn R ein Integritätsbereich ist und jedes Ideal ein (endliches) Produkt von Primidealen ist.

Beispiel 10.2 (i) Sei R faktoriell. Dann ist jedes Hauptideal ein (endliches) Produkt von Primidealen. Insbesondere ist jeder Hauptidealring ein Dedekindring. Wir werden später die Umkehrung zeigen.

(ii) R Dedekindring und $0 \neq S \subseteq R$ multiplikativ $\Rightarrow S^{-1}R$ Dedekindring. Folgt aus Proposition 10.6 und 10.7 (ÜA). Wir werden einen anderen Beweis später liefern.

B4: Algebra II
Sommersemester 2021
Frau Prof. Dr. Salma Kuhlmann

11.Vorlesung

20. Mai 2021

In diesem Skript werden wir gebrochene Ideale einführen, und ihre Eigenschaften studieren. Unser Hauptziel für diese Vorlesung ist Satz 11.6 für Dedekindringe zu beweisen. Der wird uns später ermöglichen, die Gruppenstruktur der Klassengruppe zu definieren.

Sei R stets ein kommutativer integer Ring mit Eins.

Definition 11.1 (i) Sei $K = \text{Quot}(R)$. 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: wenn $I, J \lhd R$ sind so dass $B = (\frac{1}{d})I$ und $B' = (\frac{1}{d'})J$, dann ist $BB' = (\frac{1}{dd'})IJ$.

Definition 11.2
Das gebrochene Ideal B ist invertierbar, wenn es ein gebrochenes Ideal B' gibt mit

$$BB' = R \qquad (*)$$

Bemerkung 11.1 (i) B invertierbar$\Rightarrow \exists! B'$, das $(*)$ erfüllt, d.h. $BB' = BB'' = R \Rightarrow B' = B''$. 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 11.1
Sei A ein invertierbares gebrochenes Ideal, dann ist $A^{-1} = (R : A)$.
(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 11.2
Wenn jedes ganzes Ideal$\neq 0$ invertierbar ist, dann ist 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 11.3
Ein invertierbares gebrochenes Ideal ist ein endlich erzeugter R-Modul.

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

Lemma 11.4
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. $B^{-1}(\prod_i A_i) = R \Rightarrow A_i \underbrace{(B^{-1} \prod_{j \neq i} A_j)}_{:= A_i^{-1}} = R$ □

Bemerkung 11.2
Sei $\mathfrak{p} \lhd R$ ein Primideal und $I, J \lhd R$. Es ist: $\mathfrak{p} \supseteq IJ \Rightarrow \mathfrak{p} \supseteq I$ oder $\mathfrak{p} \supseteq J$.

Lemma 11.5
Für Produkte von invertierbaren (ganzen) Primidealen ist die Faktorisierung als Produkt von Primidealen eindeutig.

Beweis. Sei $A = \prod_i \mathfrak{p}_i$, $\mathfrak{p}_i$ invertierbare Primideale. Sei $A = \prod_j \mathfrak{q}_j$, wobei $\mathfrak{q}_j$ 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. $\mathfrak{q}_1 \subseteq \mathfrak{p}_1$ (Bemerkung 11.2). 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 11.6
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

$$\mathfrak{p} + Ra = \prod_{i=1}^{n} \mathfrak{p}_i \text{ und } \mathfrak{p} + Ra^2 = \prod_{j=1}^{m} \mathfrak{q}_j$$

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 (Bemerkung 11.1) und es folgt (Lemma 11.4): $\mathfrak{p}_i/\mathfrak{p}$ und $\mathfrak{q}_j/\mathfrak{p}$ sind alle invertierbar. Aber

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

Wir folgern aus Lemma 11.5 und einem Vergleich von $(*)$, $(**)$ und $(***)$: Für jedes $j = 1, \cdots, m$ ist das Ideal $\mathfrak{q}_j/\mathfrak{p}$ ist in der Menge $\{\mathfrak{p}_i/\mathfrak{p}\}$ und wird zweimal wiederholt, 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 für Idealsummen, 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 $\mathfrak{p}Ra + \mathfrak{p}Ra = \mathfrak{p}Ra$ (da $I + I = I$ immer gilt).
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 $0 \neq b \in \mathfrak{p}$. Da R Dedekindring ist; schreibe $Rb = \prod_i \mathfrak{p}_i$ mit $\mathfrak{p}_i$ Primideal. Aus Lemma 11.4 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 $\mathfrak{p} \supseteq \mathfrak{p}_1$ (Bemerkung 11.2) und damit $\mathfrak{p} = \mathfrak{p}_1$ und $\mathfrak{p}$ ist invertierbar. □

□

B4: Algebra II
Sommersemester 2021
Frau Prof. Dr. Salma Kuhlmann

12.Vorlesung

25. Mai 2021

Unser Hauptsatz in diesem Skript ist Satz 12.4. Danach beweisen wir mehrere Lemmata, die wir für die Charakterisierung von Dedekindringe im Skript 13 brauchen.

Sei R stets ein kommutativer integer Ring mit Eins.

Korollar 12.1
Sei R ein Dedekindring, dann ist die Faktorisierung von Idealen (als Produkt von Primidealen) eindeutig.

Beweis. Folgt unmittelbar aus Lemma 11.5 und Satz 11.6 □

Korollar 12.2
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 11.2) ist auch jedes gebrochenes Ideal $\neq 0$ invertierbar. □

Für den Beweis vom Satz 12.4 brauchen wir ein

Lemma 12.3
Seien $\mathfrak{a}, \mathfrak{m}$ Ideale in R so daß $\mathfrak{a}$ endlich erzeugt ist und $\mathfrak{m}\mathfrak{a} = \mathfrak{a}$. Dann:

(i) $\exists z \in \mathfrak{m}$, so daß $(1-z)\mathfrak{a} = 0$.

(ii) Es folgt: Wenn R ein Integritätsbereich ist, $1 \notin \mathfrak{m}$ und $\mathfrak{a} \neq 0$, dann ist $\mathfrak{m}\mathfrak{a} \neq \mathfrak{a}$.

Beweis. (i) Sei $\{x_1, \ldots, x_n\}$ erzeugend für $\mathfrak{a}$. Für jedes $i = 1, \cdots, n$, setze $\mathfrak{a}_i := < x_i, \ldots, x_n >$ (das von $\{x_i, \ldots, x_n\}$ erzeugte Ideal). Also ist $\mathfrak{a} = \mathfrak{a}_1$. Setze $\mathfrak{a}_{n+1} = \{0\}$.

Wir zeigen (per Induktion) daß:

$$\forall i = 1, \cdots, n+1 \; \exists z_i \in \mathfrak{m} \text{ so daß } (1-z_i)\mathfrak{a} \subseteq \mathfrak{a}_i \qquad (\dagger)$$

- Für $i = 1$ setze $z_1 = 0$.
- Aus $(1-z_i)\mathfrak{a} \subseteq \mathfrak{a}_i$ und $\mathfrak{a} \subseteq \mathfrak{m}\mathfrak{a}$ folgt $(1-z_i)\mathfrak{a} \subseteq \mathfrak{m}\mathfrak{a}_i$. Insbesondere gilt

$$(1-z_i)x_i = \sum_{j=i}^{n} z_{ij}x_j \text{ für geeignete } z_{ij} \in \mathfrak{m} \qquad (*)$$

Also ist

$$(1 - z_i - z_{ii})x_i \in \mathfrak{a}_{i+1} \qquad (**)$$

Per Definition von $\mathfrak{a}_{i+1}$ ist außerdem $(1 - z_i - z_{ii})x_j \in \mathfrak{a}_{i+1}$ für alle $j = i + 1, \cdots, n$.

Setze:

$$1 - z_{i+1} := (1 - z_i)(1 - z_i - z_{ii}) \qquad (***)$$

Aus (*) (**) und (***) folgt nun daß $(1 - z_{i+1})\mathfrak{a} \subseteq \mathfrak{a}_{i+1}$.

• Wir haben (†) bewiesen. Nun ist $z := z_{n+1}$ das gesuchte Element.

(ii) ÜA.

□

Satz 12.4
Sei R ein Integritätsbereich. Es ist:
R ist ein Dedekindring$\Leftrightarrow$ jedes Ideal $\neq 0$ in R ist invertierbar.

Beweis. "$\Rightarrow$" folgt aus Korollar 12.2.
"$\Leftarrow$" Lemma 11.3 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 Lemma 12.3(ii) 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 $\mathfrak{a}$.

□

Wir beweisen nun die Hilfslemmata für noethersche Ringe.

Hilfslemma 12.1
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 12.2
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 12.3
Sei R ein ganz abgeschlossener noetherscher Integritätsbereich, $K = \mathrm{Quot}(R)$, $I \subseteq K$ ein gebrochenes Ideal von R; dann ist $S := \{x \in K \mid xI \subseteq I\} = R$

Beweis. Wegen Hilfslemma 12.1 ist I ein endlich erzeugter R-Modul. Sei nun $x \in S$. 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 $R = S$. □

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

Hilfslemma 12.4
Sei R ein noetherscher Integritätsbereich, so daß jedes $\neq 0$ Primideal ein Maximalideal ist. Sei $I \lhd R$. Dann ist $I^* \supsetneq R$.

Beweis. Wir zeigen $I^* \neq R$. Sei $a \neq 0, a \in I$, so daß $R \supseteq I \supseteq aR$. Hilfslemma 12.2 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. Also 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 $I^* \supsetneq R$. □

Hilfslemma 12.5
Sei D ein Integritätsbereich, $k \subseteq D$ ein Unterkörper, so daß D/k algebraisch ist. Dann ist D ein Körper.

Beweis. 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 $\beta\beta' = 1 \in k[\beta]$ □

B4: Algebra II
Sommersemester 2021
Frau Prof. Dr. Salma Kuhlmann

13.Vorlesung

27. Mai 2021

In diesem Skript führen wir in Definition 13.1 die Klassengruppe (vgl. Korollar 12.2) und Klassenzahl von einem Dedekingring ein. Diese Begriffe werden wir in der nächster Vorlesung gleich gebrauchen. Wir beweisen außerdem weitere wichtige Sätze über Dedekindringe. Satz 13.1 ergibt eine allgemeine Charakterisierung für Dedekindringe (vgl. Satz 12.4), Satz 13.2 eine Charakterisierung für faktorielle Dedekindringe, und Satz 13.3 die eindeutige Faktorisierung für gebrochene Ideale in einem Dedekindring. Wir beenden das Skript (und damit die Vorlesung Algebra 2) mit Satz 13.5, den wir direkt in der nächster Vorlesung verwenden wollen.

Definition 13.1
Sei R ein Dedekindbereich. Die Menge $\mathrm{Id}(R)$ der $\neq 0$ gebrochenen Ideale von R (versehen mit der Verknüpfung *Idealprodukt*) ist eine abelsche Gruppe. Sie enthält die Untergruppe $H(R)$ der gebrochenen Hauptideale. Die Faktorgruppe $\mathcal{K}l(R) := \mathrm{Id}(R)/H(R)$ heißt die Ideal Klassengruppe von R. Ihre Ordnung $|\mathcal{K}l(R)| \in \mathbb{N} \cup \{\infty\}$ heißt die Klassenzahl von R.

Satz 13.1
Sei R ein Integritätsbereich. Dann ist R ein Dedekindring genau dann, wenn R die folgende drei Bedingungen erfüllt:

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

Beweis. „⇒“

1. folgt aus Korollar 12.2 und Lemma 11.3.
2. folgt aus Satz 11.6.
3. Setze $K := \mathrm{Quot}(R)$, sei $a \in K$ und $f(x) \in R[x]$ normiert mit $f(a) = 0$, $\deg(f) = n$. Schreibe $a = \frac{b}{c}$, b , $c \in R, c \neq 0$ und setze $M := R + Ra + \cdots + Ra^{n-1}$. Es ist $c^{n-1}M \subseteq R$ (und somit ist M ein gebrochenes Ideal), und $M^2 = M$ (ÜA). Da M gebrochenes Ideal, und R Dedekind ist, existiert M^{-1}. Also ist $M^{-1}M^2 = R$, d.h $M = R$. Da $a \in M$, gilt nun $a \in R$.

„⇐“ Wir zeigen 1.+2.+3.⇒ jedes $\neq 0$ gebrochenes Ideal ist invertierbar.

Sei also I ein gebrochenes Ideal.
Setze $I^* := (R : I)$, und prüfe daß (vgl. [Skript 12; Erinnerung s. 3]):

$$II^*(II^*)^* \subseteq R \text{ , also } I(I^*(II^*)^*) \subseteq R \text{ , also } I^*(II^*)^* \subseteq I^*$$

per Definition von I^* .

Setze $S := \{x \in K \mid xI^* \subseteq I^*\}$. Es ist: $S \subseteq R$ (siehe Hilfslemma 12.3). Wir bekommen also aufjedenfall daß :

$$(II^*)^* \subseteq S \subseteq R \qquad (\dagger)$$

• Wenn $II^* = R$ gilt, ist I invertierbar und wir sind fertig.

• Sonst ist $II^* \lhd R$, aber dann ist (Hilfslemma 12.4) $(II^*)^* \supsetneq R$: Widerspruch zum (†). □

Beispiel 13.1 (i) Ein Hauptidealring ist ein Dedekindring. Die Klassengruppe ist trivial und die Klassenzahl 1.

Folgt aus Proposition 5.12 in Skript 5 der Algebra 1 Vorlesung WiSe 2020/2021, und Beispiel 9.1 oder Aufgabe 5.1 ÜB 5 (ÜA).

(ii) R Dedekindring und $0 \neq S \subseteq R$ multiplikativ $\Rightarrow S^{-1}R$ Dedekindring. Folgt aus Proposition 10.6 und 10.7 (ÜA).

(iii) $\mathbb{Q}[x, y]$ ist faktoriell, ist jedoch kein Dedekindring, da das Ideal $< x >$ prim aber nicht maximal ist (ÜA).

Satz 13.2
Sei R ein Dedekindbereich, R ist genau dann faktoriell, wenn er ein Hauptidealbereich ist. Das heißt: Ein Dedekindbereich ist genau dann faktoriell, wenn $|\mathcal{K}l(R)| = 1$.

Beweis. „⇐“ Jedes Hauptidealbereich 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 (Satz 11.6). □

Satz 13.3 (Gebrochene Ideale in einem Dedekindbereich)
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 (Korollar 12.1)

$$d\mathfrak{a} = p_1^{r_1} \dots p_m^{r_m} \qquad \text{wobei die } p_i \text{ Primideale sind und } r_i \in \mathbb{N}_0$$

und

$$< d >= p_1^{s_1} \dots p_m^{s_m}, \qquad \text{wobei } s_i \in \mathbb{N}_0 \,.$$

Dann ist

$$\mathfrak{a} = \prod_{i=1}^{m} p_i^{r_i - s_i}, \qquad \text{wobei } r_i - s_i \in \mathbb{Z} \,.$$

□

Für den Beweis vom Satz 13.5 brauchen wir den Satz 13.4. Wir werden allerdings diesen Satz erst in der Folgevorlesung beweisen können.

Satz 13.4
Sei R ein ganz abgeschlossener Integritätsbereich, $K = \mathrm{Quot}(R)$, 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 $M \subseteq S \subseteq M'$.

Satz 13.5
Sei R ein Dedekindbereich, $K = \mathrm{Quot}(R)$, L/K eine endliche separable Erweiterung. Dann ist $\overline{R}^L$ ein Dedekindbereich.

Beweis. Wir zeigen, daß $\overline{R}^L$ $1. + 2. + 3.$ von Satz 13.1 erfüllt.

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

   Satz 13.4 $\Rightarrow M \subseteq \overline{R}^L \subseteq M'$, 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 10.4

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 $\beta^n + a_1\beta^{n-1} + \cdots + a_n = 0$ 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

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

   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 Hilfslemma 12.5, daß $\overline{R}^L/\mathfrak{q}$ ein Körper ist. Es folgt: $\mathfrak{q}$ ist maximal.

□

B4: Algebraische Zahlentheorie
Sommersemester 2021
Frau Prof. Dr. Salma Kuhlmann

14.Vorlesung

8. Juni 2021

Wir werden in diesem Skript die gleiche Notationen, Definitionen, Begriffe und Terminologie (von Skript B1, B2, B3, B4; Algebra II) implizit und stillschweigend beibehalten und verwenden. In dieser Vorlesung B4; Algebraische Zahlentheorie werden wir die Ergebnisse der Algebra II auf Zahlkörper L und deren Ringe $\mathcal{O}_L$ (ganze algebraisch Zahlen) anwenden. Wir werden zunächst ***Norm, Spur, Diskriminante*** *studieren, um die Theorie der Körpererweiterungen und unseren Werkzeugkasten zu ergänzen. Danach werden wir* ***Gitter*** *in $\mathbb{R}^n$ und* Idealnorm *einführen um* die Endlichkeit der Klassenzahl *zu etablieren. Im letztem Kapitel werden wir die* Gruppe der Einheiten $\mathcal{O}_L^\times$ *studieren und* ***Dirichlet's Einheitensatz*** *beweisen.*

In Skript 14 führen wir die Norm und die Spur ein, und fangen damit an ihre Eigenschaften zu studieren. Dafür erinnern wir kurz an gewählte und benötigte Begriffe und Ergebnisse der LA I und LA II.

Kapitel 5: Norm, Spur, Diskriminante

Sei L/K stets eine endliche Körpererweiterung (das heißt $\dim_K L < \infty$).

Erinnerung aus LA I und LA II:

- Wir bezeichnen mit $\mathcal{L}_K(L,L)$ den K-Vektorraum

$$\mathcal{L}_K(L,L) := \{\mu \,:\, L \longrightarrow L \,;\, \mu \text{ ist eine } K- \text{ lineare Abbildung } \}$$

- Für $\mu \in \mathcal{L}_K(L,L)$ bezeichnet $\text{Spur}(\mu)$ die Spur (Trace) von μ :

  für M eine Matrix Darstellung von μ, ist $\text{Spur}(\mu) := \text{Spur}(M) :=$ die Summe der Einträge M_{ii} der Hauptdiagonale von M.

Definition und Notation
Sei $\alpha \in L$. Betrachte die Abbildung

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

Diese Abbildung ist offensichtlich K-linear, das heißt $\mu_{\alpha,L} \in \mathcal{L}_K(L,L)$. Wir bezeichnen:

- $\chi_{\alpha,L} :=$ CharPol von $\mu_{\alpha,L}$
- $f_{\alpha,L} :=$ MinPol von $\mu_{\alpha,L}$
- $N_{L/K}(\alpha) := \det(\mu_{\alpha,L}) \in K$.

  $N_{L/K}(\alpha)$ heißt die (L/K)-Norm von α.
- $Sp_{L/K}(\alpha) := \mathrm{Spur}(\mu_{\alpha,L}) \in K$.

  $Sp_{L/K}(\alpha)$ heißt die (L/K)-Spur von α.

Das folgende Lemma erklärt den Zusammenhang zum Minimalpolynom von $\alpha \in L$ über K:

Lemma 14.1
Es gelten:

(i) $f_{\alpha,L} = \mathrm{MinPol}_K(\alpha)$.

(ii) Für $L = K(\alpha)$ bezeichne $f_\alpha := f_{\alpha,K(\alpha)}$. Insbesondere gilt dann:

$$f_\alpha = \chi_{\alpha,K(\alpha)} = \mathrm{MinPol}_K(\alpha) .$$

(iii) Setze $m := [L : K(\alpha)]$. Dann gilt allgemeiner

$$\chi_{\alpha,L} = f_{\alpha,L}^m .$$

Beweis. (i) Es ist leicht zu prüfen, daß $f(\mu_{\alpha,L}) = 0 \Leftrightarrow f(\alpha) = 0 \, \forall f \in K[x]$.

Die Aussage von (i) folgt nun unmittelbar aus den Definitionen (ÜA).

(ii) Wir berechnen: $\deg \chi_{\alpha,K(\alpha)} = [K(\alpha) : K] = \deg \mathrm{MinPol}_K(\alpha) = \deg f_\alpha$.

Damit sind die Polynome gleich.

(iii) 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 $\mu_{\alpha,L}$-invariante K-Unterräume, und

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

(ÜA).

• Betrachte nun die folgende Abbildungen:
$\mu_{\alpha,L} : L \to L$
$\mu_{\alpha,K(\alpha)} : K(\alpha) \to K(\alpha)$

und für jedes $i = 1, \cdots, m$ die K-Vektorräume Isomorphie: $\begin{array}{ccc} K(\alpha) & \overset{\omega_i}{\tilde{\to}} & W_i \\ x & \mapsto & x\lambda_i \end{array}$

• Für jedes $i = 1, \cdots, m$ erfüllt ω_i die folgende Gleichung auf $K(\alpha)$:

$$\omega_i \circ \mu_{\alpha,K(\alpha)} = \mu_{\alpha,L} \circ \omega_i \text{ auf } K(\alpha)\,.$$

Folgt per Definitionen (ÜA).

(Diese Gleichungen kann man zusammenfassen als: $\mu_{\alpha,L} = \bigoplus_{i=1}^{m} \mu_{\alpha,K(\alpha)}$).

Außerdem gilt:

$(***)$ $$\underbrace{\mu_{\alpha,L} \restriction W_i = \omega_i \circ (\mu_{\alpha,K(\alpha)}) \circ \omega_i^{-1}}_{\textbf{ähnliche lineare Transformationen}}\,.$$

(ÜA)

Wegen $(**)$ und $(***)$ berechnen wir nun (siehe LA II), daß

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

□

Wir werden nun weitere Eigenschaften von Norm und Spur untersuchen.

Lemma 14.2
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. $N_{L/K}(\lambda) = \lambda^n$ und $Sp_{L/K}(\lambda) = n\lambda$
4. Sei $f_{\alpha,L} = x^\nu + a_{\nu-1}x^{\nu-1} + \cdots + a_0, \quad a_i \in K.$

Also ist $\nu = [K(\alpha) : K] = \deg \text{MinPol}_K(\alpha)$. Setze $\mu := [L : K(\alpha)] = \frac{n}{\nu}$. Es gilt:

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

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

Lemma 14.2 beweisen wir im Skript 15. Dafür fassen wir zusammen benötigte **Erinnerungen als LA I und LA II:**

- Die Determinante ist multiplikativ.
- Die Spur ist additiv.
- Sei $A \in M_{n\times n}(K)$, setze $\mathrm{CharPol}(A) = \det(xI - A) = x^n + b_{n-1}x^{n-1} + \cdots + b_0$. Es ist

$$b_0 = (-1)^n \det A \text{ und } b_{n-1} = -\mathrm{Spur}(A)\,.$$

B4: Algebraische Zahlentheorie
Sommersemester 2021
Frau Prof. Dr. Salma Kuhlmann

15.Vorlesung

10. Juni 2021

In diesem Skript werden wir die Eigenschaften von Norm und Spur weiter entwickeln. Dafür werden wir (hier sowie in die folgende Skripte) weitere Elemente der Galoistheorie einbauen, die wir in der Algebra I nicht fertig gebracht haben.

Sei L/K stets eine endliche Körpererweiterung (das heißt $\dim_K L < \infty$).

Wir fangen an mit dem Beweis von Lemma 14.2

Beweis. 1. Wir bemerken zunächst daß $\mu_{\alpha\beta,L} = \mu_{\alpha,L} \circ \mu_{\beta,L}$ per Definition (ÜA). Wir berechnen nun: $N_{L/K}(\alpha\beta) = \det(\mu_{\alpha\beta,L}) = \det(\mu_{\alpha,L} \circ \mu_{\beta,L}) = \det(\mu_{\alpha,L}) \det(\mu_{\beta,L})$ (weil die Determinante multiplikativ ist).

2. Wir bemerken zunächst daß $\mu_{\lambda\alpha+\beta,L} = \lambda\mu_{\alpha,L} + \mu_{\beta,L}$ per Definition (ÜA). Wir argumentieren (analog wie in 1, und die Tatsache daß die Spur additiv ist) (ÜA).

3. Wir bemerken zunächst daß $\mu_{\lambda,L} = \lambda \operatorname{Id}_L$ per Definition (ÜA). Wir berechnen nun: $N_{L/K}(\lambda) = \det(\mu_{\lambda,L}) = \det(\lambda \operatorname{Id}_L) = \lambda^n$. Analog $Sp_{L/K}(\lambda) = \operatorname{Spur}(\lambda \operatorname{Id}_L) = n\lambda$.

4. (i) Wir haben $\nu = [K(\alpha) : K], \quad \mu = [L : K(\alpha)], \quad n = \nu\mu$. Setze

   (†) $$\chi_{\alpha,L} = x^n + b_{n-1}x^{n-1} + \cdots + b_0.$$

   Wir berechnen nun $N_{L/K}(\alpha) = \det(\mu_{\alpha,L})$. Wir wissen (Erinnerung LA I + LA II) daß $(-1)^n \det(\mu_{\alpha,L}) = b_0$. Außerdem ist (wegen Lemma 14.1):

   (‡) $$\chi_{\alpha,L} = (f_\alpha)^\mu.$$

   Ein Koeffizientenvergleich in (†) und (‡) ergibt nun $b_0 = a_0^\mu$.

   (ii) Wir wissen (Erinnerung LA I + LA II) daß $b_{n-1} = -\operatorname{Spur}(\mu_{\alpha,L}) = -Sp_{L/K}(\alpha)$ per Definition. Wir berechnen: der Koeffizient von x^{n-1} (das heißt der Koeffizient von $x^{\nu\mu-1}$) in $(f_\alpha)^\mu$ ist $\mu a_{\nu-1}$ (ÜA). Wir vergleichen nun die Koeffizienten in (†) und (‡) und bekommen $b_{n-1} = \mu a_{\nu-1}$.

□

Proposition 15.1
Setze $n = [L : K]$. Sei $\beta \in L, f(x) := \text{ MinPol}_K(\beta)$, $\deg f := m = [K(\beta) : K]$. Setze $r := \frac{n}{m} = [L : K(\beta)]$. Seien $\beta = \beta_1, \beta_2, \ldots, \beta_m$ alle Nullstellen von f (in einem Zerfällungskörper). Es ist

$$N_{L/K}(\beta) = (\prod \beta_i)^r \text{ und } Sp_{L/K}(\beta) = r \sum \beta_i \, .$$

Beweis. Setze $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0$, $a_i \in K$. Wir wissen daß $\prod \beta_i = (-1)^m a_0$ und $\sum \beta_i = -a_{m-1}$ (siehe ÜB).
Wir berechnen (mit Anwendung von Lemma 14.2 4-(i) und 4-(ii)):

$$(\prod \beta_i)^r = (-1)^{mr} a_0^r \overset{(i)}{=} N_{L/K}(\beta)$$

und

$$r \sum \beta_i = -r a_{m-1} \overset{(ii)}{=} Sp_{L/K}(\beta) \, .$$

□

Korollar 15.2
Sei R ein ganz abgeschlossener Integritätsbereich, $K := \text{Quot}(R)$, und 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. Da $\beta \in \overline{R}^L$ wissen wir daß $\text{ MinPol}_K(\beta) \in R[x]$. Nun seien $\beta = \beta_1, \ldots, \beta_m$ seine Nullstellen. Es folgt daß auch $\beta_1, \ldots, \beta_m \in \overline{R}^L$. Setze $r := [L : K(\beta)]$. Nun sind per Definition $N_{L/K}(\beta)$, $Sp_{L/K}(\beta) \in K$. Außerdem wegen Proposition 15.1 sind $N_{L/K}(\beta) = (\prod \beta_i)^r$ und $Sp_{L/K}(\beta) = r \sum \beta_i$. Also sind $N_{L/K}(\beta) \in \overline{R}^L$ und $Sp_{L/K} \in \overline{R}^L$. Nun ist aber R ganz abgeschlossen, also folgt die Behauptung. □

In Satz 15.4 führen wir eine genauere Berechnung wenn L/K separabel ist. Dafür brauchen wir einen weiteren Satz der Galoistheorie:

Satz 15.3
Sei L/K separabel, und Ω die normale Hülle von L/K. Setze $[L : K] = n$. Dann gelten:

1. $\exists \sigma_1, \ldots, \sigma_n$ verschiedene Einbettungen von L/K in Ω.
2. Sei $\beta \in L$ und setze $[K(\beta) : K] = m = \frac{n}{r}$ und $[L : K(\beta)] = r$. Dann gilt

$$\forall \sigma \in \{\sigma_1, \ldots, \sigma_n\} \, : \, \sigma(\beta) \text{ kommt genau } r \text{ mal in der Folge } (\sigma_1(\beta), \ldots, \sigma_n(\beta)) \text{ vor} \, .$$

Beweis. Da L/K separabel ist, ist sie eine einfache Erweiterung, also

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

$$\begin{array}{ccc} L & \overset{\sigma_k}{\hookrightarrow} & \Omega \\ \gamma & \mapsto & \gamma_k \end{array}$$

$$K \overset{\sigma_k|K}{\underset{=Id}{\longrightarrow}} K \quad \text{(Isomorphismus } K(\gamma) \cong K[x]/ < g(x) > \cong K(\gamma_k) \text{ aus Algebra BIII)}$$

(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:

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

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

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

Im Zeichen:

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

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

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

Es ist klar, daß $(\tilde{\mu}_j \circ \lambda_i)$ Einbettung von L über K in 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

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

und

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

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

□

Satz 15.4
Setze $[L : K] = n$. Sei L/K separabel, 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

$$N_{L/K}(\beta) = \prod_{k=1}^{n} \sigma_k(\beta) \text{ und } Sp_{L/K}(\beta) = \sum_{k=1}^{n} \sigma_k(\beta) \,.$$

Beweis. Seien $\sigma_1, \ldots \sigma_n$ wie in Satz 15.3. 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.

• Es folgt aus Satz 15.3 daß: Für $i = 1, \ldots, m$ gibt es genau r Einbettungen von L in Ω, die β auf β_i absenden. Das heißt: β_i erscheint genau r mal in der Folge $(\sigma_k(\beta))_k$.

• Nun folgt aus Prop 15.1, daß
$N_{L/K}(\beta) = (\prod_{i=1}^{m} \beta_i)^r = \prod_{i=1}^{n} \sigma_i(\beta)$ und $Sp_{L/K}(\beta) = r(\sum_{i=1}^{m} \beta_i) = \sum_{i=1}^{n} \sigma_i(\beta)$. □

B4: Algebraische Zahlentheorie
Sommersemester 2021
Frau Prof. Dr. Salma Kuhlmann

16.Vorlesung

15. Juni 2021

Im Korollar 16.1 werden wir die Norm und Spur für eine Zwischenerweiterung untersuchen. Danach werden wir Erinnerungen an Dualraum, und Bilineare Formen aus der LA I und LA II aufrufen. Diese Begriffe werden wir ebenfalls in die folgende Skripte stark benötigen, um den dritten Begriff des Kapitels, die Diskriminante, einzuführen. Im letztem Abschnitt werden wir eine besondere bilineare Form einführen.

Sei L/K stets eine endliche Körpererweiterung (das heißt $\dim_K L < \infty$).

Korollar 16.1
Sei L/K separabel, $[L:K] = n$, und $K \subseteq E \subseteq L$. Sei $\alpha \in L$. 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. Wir argumentieren wie im Beweis vom Satz 15.3. und benutzen dabei ebenfalls die gleiche Bezeichnungen wie im Beweis vom Satz 15.3.

(i) Aus Satz 15.4 folgt:

$$N_{L/K}(\alpha) = \prod_{k=1}^{n} \sigma_k(\alpha)\,,$$

wobei $\{\sigma_1, \ldots, \sigma_n\}$ die Einbettungen von L/K in Ω sind.

• Sei nun β ein primitives Element für E/K, also $E = K(\beta)$ und setze $[K(\beta) : K] = m = \frac{n}{r}$ und $[L : K(\beta)] = r$. Aus $(*)$ und $(**)$ im Beweis vom Satz 15.3. wissen wir daß $\{\tilde{\mu}_j \circ \lambda_i \mid j = 1, \ldots, m, i = 1, \ldots, r\} = \{\sigma_1, \ldots, \sigma_n\}$.

• Also $\forall k, \exists i, \exists j$, so daß $\sigma_k = \tilde{\mu}_j \circ \lambda_i$. Da alle vorkommene Abbildungen Homomorphismen sind, berechnen wir:

$$N_{L/K}(\alpha) = \prod_{i,j} (\tilde{\mu}_j \circ \lambda_i)(\alpha) \overset{\text{Hom}}{=} \prod_{j=1}^{m} \tilde{\mu}_j (\prod_{i=1}^{r} \lambda_i(\alpha))\,.$$

• Nun folgt ebenfalls aus Satz 15.4 daß:

$$\prod_{i=1}^{r} \lambda_i(\alpha) = N_{L/E}(\alpha)$$

(Anwendung für L/E und die r Einbettungen von L über E in Ω').

- Da aber per Definition $N_{L/E}(\alpha) \in E$ ist, folgt aus der Definition von $\tilde{\mu}$ daß

$$\tilde{\mu}_j(\prod_{i=1}^{r} \lambda_i(\alpha)) = \mu_j(\prod_{i=1}^{r} \lambda_i(\alpha)) \, .$$

- Eine nochmalige Anwendung vom Satz 15.4 ergibt schließlich daß:

$$N_{L/K}(\alpha) = \prod_{j=1}^{m} \mu_j(N_{L/E}(\alpha)) = N_{E/K}(N_{L/E}(\alpha))$$

(Anwendung für E/K und die m Einbettungen von E über K in Ω').

(ii) Analog (ÜA).

□

Erinnerung: Bilineare Formen.

1. Sei V ein endlichdimensionaler Vektorraum über K, $\dim_K V = n$ und $\mathcal{B} := \{v_i \mid i = 1, \ldots, n\}$ eine K-Basis für V.

   Sei $B : V \times V \to K$ eine bilineare Form.

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

3. Die Matrix-Darstellung $\mathbb{B}$ von B bezüglich der Basis $\mathcal{B}$ 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. Sei $\mathbb{B}'$ die Darstellung von B bezüglich einer Basis $\{v_i' \mid i = 1, \ldots, n\}$ und P die Basiswechselmatrix. Es gilt: $\mathbb{B}' = P^t \mathbb{B} P$.

Definition 16.1
Sei V ein endlichdimensionaler Vektorraum über K und $\mathcal{B} := \{v_i \mid i = 1, \ldots, n\}$ eine K-Basis für V, $\mathcal{B}^*$ die Dualbasis. Sei $B : V \times V \to K$ bilinear und 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 <u>nicht ausgeartet</u>, wenn: $\forall x \in V, x \neq 0 \Rightarrow B_x \neq 0$.

Bemerkung 16.1 (i) $B_x \in V^*$

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

(iii) B ist nicht ausgeartet $\Leftrightarrow$ Kern $\phi_B = \{0\}$ wobei ϕ_B ist die lineare Abbildung

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

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

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

(v) Sei B nicht ausgeartet. Setze für jedes $i = 1, \ldots, n$

$$w_i := \phi_B^{-1}(v_i^*) \, .$$

Dann gilt $\forall i, j$:

$$B(v_i, w_j) = \delta_{ij} \, .$$

Diese Basis $\{w_i \mid i = 1, \ldots, n\}$ von V heißt die zu $\mathcal{B}$ B-duale Basis für V. Die B-duale Basis hat die folgende nützliche Eigenschaft:

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

Beweis. ÜA. □

§Die Spur bilineare Form

Bemerkung 16.2
Sei L/K eine endliche separable Körpererweiterung.

(i) Die Abbildung

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

definiert eine symmetrische bilineare Form.

(ii) $B_{L/K}$ ist nicht ausgeartet.

Beweis. (i) ÜA.

(ii) Setze $[L : K] = n$. Sei $\gamma \in L$, so daß $L := K(\gamma)$ (Satz vom Primitivelement). Dann ist $\{\gamma^0, \ldots, \gamma^{n-1}\}$ eine K-Basis für L.

• Wir berechnen die Matrixdarstellung $\mathbb{B}$ der bilinearen Form $B_{L/K}$ bezüglich dieser Basis:

$$\forall i, j \,:\, \mathbb{B}_{ij} = Sp_{L/K}(\gamma^{i+j}) \overset{\text{Satz}}{\underset{15.4}{=}} \sum_{k=1}^{n} \sigma_k(\gamma^{i+j}) \overset{\text{Hom}}{=} \sum_{k=1}^{n} \sigma_k(\gamma)^{i+j} \,,$$

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 $\mathrm{MinPol}_K(\gamma)$, also ist $\{\gamma_1, \ldots, \gamma_n\} = \{\sigma_1(\gamma), \ldots, \sigma_n(\gamma)\}$. Wir schreiben um

$$\mathbb{B}_{ij} = \sum_{k=1}^{n} \gamma_k^{i+j} \qquad (\dagger)$$

• Wir zeigen daß $\det \mathbb{B} \neq 0$. Aus (†) sehen wir, daß $\mathbb{B}$ das Produkt

$$\mathbb{B} = \mathcal{V}^t \mathcal{V}$$

wobei $\mathcal{V}$ die Vandermonde Matrix ist:

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

(ÜA).

Wir berechnen nun: $\det \mathbb{B} = (\det \mathcal{V})^2$. 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.

□

B4: Algebraische Zahlentheorie
Sommersemester 2021
Frau Prof. Dr. Salma Kuhlmann

17.Vorlesung

17. Juni 2021

In diesem Skript werden wir den folgenden Anstaz studieren:

R ganz abgeschloßen Integer Ring , $K = QuotR, L/K$ eine endliche separable Körpererweiterung .

Wir werden den ganzen Abschluß $\overline{R}^L$ beschreiben und wie (in der Algebra II Vorlesung) vorangekündigt Satz 13.4 (Satz 17.1 hier) beweisen. Wir wollen schließlich in Korollar 17.4 diese Ergebnisse auf

$$R = \mathbb{Z}, L/\mathbb{Q} \text{ ein Zahlkörper, und } \overline{\mathbb{Z}}^L = \mathcal{O}_L$$

anwenden. Danach werden wir die Diskriminante einführen, um Ganzheitbasen zu berechnen.

Ansatz und Bezeichnungen weiterhin wie im Skript 16.

Bemerkung 17.1 (ÜA)
Im Beweis von Bemerkung 16.2 können wir 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. Sei $\mathcal{V}_{ij} := \sigma_i(v_j)$ für alle i, j, und $\mathbb{B}$ die Matrix von $B_{L/K}$ bezüglich $\{v_1, \ldots, v_n\}$. Dann ist $\mathbb{B} = \mathcal{V}^t\mathcal{V}$, also ist $\det \mathbb{B} = (\det \mathcal{V})^2$.

Satz 17.1
Sei R ein ganz abgeschlossener Integritätsbereich, $K = \mathrm{Quot}(R)$, 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. • Betrachte

$$B_{L/K} : L \times L \to K \ , \ B_{L/K}(x, y) = Sp_{L/K}(xy).$$

Bemerke daß die Einschränkung von $B_{L/K}$ auf $S \times S$ hat Werte in R (Korollar 15.2).

• Sei $\{\nu_1, \ldots, \nu_n\}$ eine Basis für L/K. O.E. $\{\nu_1, \ldots, \nu_n\} \subseteq S$ (weil $\forall \alpha \in L \, \exists r \in R$ mit $r\alpha \in S$, s. Proposition 9.4).

• Sei $\{\mu_1, \ldots, \mu_n\}$ die $B_{L/K}$-duale Basis ($B_{L/K}(\nu_i, \mu_j) = \delta_{ij}$) wie im Bemerkung 16.1.
Setze

$$M := \bigoplus R\nu_i \text{ und } M' = \bigoplus R\mu_i \, .$$

M und M' sind frei und haben Dimension gleich n (da $\{\nu_1, \ldots, \nu_n\}$ und $\{\mu_1, \ldots, \mu_n\}$ a fortiori linear unabhängig über R sind). Es ist klar, dass $M \subseteq S$. Wir zeigen $S \subseteq M'$. Sei $\alpha \in S$, schreibe $\alpha = \sum c_i\mu_i$. Aber $c_i = B_{L/K}(\alpha, \nu_i) \in R$ (Bemerkung 16.1 und Korollar 15.2). □

Korollar 17.2
Sei R ein ganz abgeschlossener Integritätsbereich, $K = \mathrm{Quot}(R)$, L/K eine endliche separable Erweiterung. Wenn R noethersch ist, dann ist $\overline{R}^L$ ein endlich erzeugter R-Modul.

Beweis. Sei M' wie in Satz 17.1, M' ist ein endlich erzeugter Modul über einem noetherschen Ring, also ist M' ein noetherscher R-Modul (s. Korollar 8.3), und damit ist jeder Untermodul endlich erzeugt.

□

Korollar 17.3
Sei R ein Hauptidealbereich, L/K eine endliche separable Körpererweiterung und $n = [L : K]$. Dann ist $\overline{R}^L$ ein freier R-Modul der Dimension n.

Beweis. Ein Untermodul (über einem HIR) von einem freiem Modul der Dimension $= n$ ist frei der Dimension $\leq n$ (s. Satz 5.1). Sei M' wie in Satz 17.1. Es gelten:

$$S \subseteq M' \Rightarrow S \text{ frei der Dimension } \leq n$$

und

$$M \subseteq S \Rightarrow \dim_R M = n \leq \dim_R S \leq n \Rightarrow \dim_R S = n\,.$$

□

Korollar 17.4
$R = \mathbb{Z}$. L ist ein Zahlkörper $\Rightarrow \mathcal{O}_L$ ist ein freier $\mathbb{Z}$-Modul der Dimension $[L : K]$.

§Ganzheitsbasen

Definition 17.1
Sei R ein Hauptidealbereich, $K = \mathrm{Quot}(R)$, L/K separable Erweiterung, $n = [L : K]$. Dann ist $S = \overline{R}^L$ 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.

Kurzbezeichnung: Sei V ein n-dimensionaler K-Vektorraum, B eine bilinerare Form, $\mathcal{B} = \{v_1, \ldots, v_n\} \subseteq V$, wir bezeichnen hierunten mit $B(v_i, v_j)$ die $n \times n$ Matrix Darstellung von B bzgl $\mathcal{B}$.

Bemerkung 17.2
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. „⇒“ Siehe Bemerkung 16.1.
„⇐“Sei $\{w_1, \ldots, w_n\}$ eine Basis für V über K. Setze $v_i = \sum_j c_{ij} w_j$, $P := [c_{ij}]$, $P \in M_{n\times n}(K)$. 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 nun analog vorgehen wie in Bemerkung 17.2 um R-Basen von S zu bestimmen:

Ansatz wie oben.

Diskriminante der Ringerweiterung S/R:
Wir haben (wegen Korollar 15.2)

$$B_{L/K} : S \times S \to R\,.$$

Für $\{\nu_1, \ldots, \nu_n\} \subseteq S$ definiere $D(\nu_1, \ldots, \nu_n) := \det(B_{L/K}(\nu_i, \nu_j))$. Es ist: $D(\nu_1, \ldots, \nu_n) \in R$.

Lemma 17.1
Seien $\{v_1, \ldots, v_n\}$ und $\{\mu_1, \ldots, \mu_n\}$ Basen für S als R-Modul. Dann ist

$$D(\nu_1, \ldots, \nu_n) = \pi^2 D(\mu_1, \ldots, \mu_n)$$

für ein geeignetes $\pi \in R^\times$.

Beweis. Wir argumentieren wie im Beweis von Bemerkung 17.2. 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 $\pi := \det P \in R^\times$. □

Bevor wir die Diskriminante der Ringerweiterung S/R definieren können, müssen wir noch eine Äquivalenzrelation einführen. Wir definieren für $x, y \in R : x \sim y \Leftrightarrow x = \pi^2 y$ für ein $\pi \in R^\times$. Lemma 17.1 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 17.2
$D(S/R) := [D(\nu_1, \ldots, \nu_n)]_\sim$ für eine (alle) Basis $\{\nu_1, \ldots, \nu_n\} \subseteq S$ von S als R-Modul.

Bemerkung 17.3
$R = \mathbb{Z} \Rightarrow \mathbb{Z}^\times = \{\pm 1\}$, 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 17.2
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. „⇒“ folgt aus Lemma 17.1.
„⇐“ Sei $\mathcal{B} := \{\nu_1, \ldots, \nu_n\}$ eine Basis von S als R-Modul, so daß
$\det[B_{L/K}(\gamma_i, \gamma_j)] = D(\gamma_1, \ldots, \gamma_n) = \pi^2 D(\nu_1, \ldots, \nu_n) = \pi^2 \det[B_{L/K}(\nu_i, \nu_j)]$ mit $\pi \in R^\times$. Betrachte

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

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

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

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 auch ein C invertierbarer R-Homomorphismus, d.h $\{\gamma_1, \ldots, \gamma_n\}$ ist eine Basis. □

B4: Algebraische Zahlentheorie
Sommersemester 2021
Frau Prof. Dr. Salma Kuhlmann

18.Vorlesung

22. Juni 2021

In diesem Skript werden wir unsere bisherige Ergebnisse anwenden, um Ganzheitsbasen für Zahlkörper zu berechnen. Wir fassen zusammen hier unseren ***Ansatz*** *aus Skript 16 und 17:*

- $R = \mathbb{Z}$, $L/\mathbb{Q}$ *ist ein Zahlkörper,* α *ist ein primitives Element für die Erweiterung, so daß* $L = \mathbb{Q}(\alpha)$, $f :=$ *MinPol*$_{\mathbb{Q}}(\alpha)$, $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ *die verschiedene Nullstellen von* f.
- $\mathcal{O}_L = \overline{\mathbb{Z}}^L$, *ohne Einschränkung* $\alpha \in \mathcal{O}_L$, $\mathcal{O}_L$ *ist frei vom Rang* $n = [L : \mathbb{Q}]$, *und* $D(\mathcal{O}_L/\mathbb{Z}) \in \mathbb{Z}$ *ist die Diskriminante des Zahlkörpers* L .
- *Unsere Fragestellung: Sei* $\mathcal{B}$ *eine Basis für* $L/\mathbb{Q}$, *so daß* $\mathcal{B} \subseteq \mathcal{O}_L$. *Wann ist* $\mathcal{B}$ *eine Basis (eine Ganzheitsbasis) für* $\mathcal{O}_L$ *als* $\mathbb{Z}$*-Modul?*

Wir benutzen weiterhin die Kurzbezeichnung die wir in der 17. Vorlesung eingeführt haben: Sei V *ein* n*-dimensionaler* K*-Vektorraum,* B *eine bilinerare Form,* $\mathcal{B} = \{v_1, \ldots, v_n\} \subseteq V$, *wir bezeichnen hierunten mit* $B(v_i, v_j)$ *die* $n \times n$ *Matrix Darstellung von* B *bzgl* $\mathcal{B}$.

Besondere Fragestellung: Betrachte die Basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$ für $L/\mathbb{Q}$. Dann ist $\{1, \alpha, \ldots, \alpha^{n-1}\} \subseteq \mathcal{O}_L$, und $\{1, \alpha, \ldots, \alpha^{n-1}\}$ ist insbesondere $\mathbb{Z}$-linear unabhängig. Wann ist $\{1, \alpha, \ldots, \alpha^{n-1}\}$ sogar erzeugend für $\mathcal{O}_L$ als $\mathbb{Z}$-Modul? Also wann ist $\{1, \alpha, \ldots, \alpha^{n-1}\}$ sogar eine *Basis* (eine Ganzheitsbasis) für $\mathcal{O}_L$ als $\mathbb{Z}$-Modul?

Um diese Frage zu beantworten, wollen wir Satz 17.2 anwenden. Dafür müssen wir zunächst berechnen:

$$\begin{aligned} D(1, \alpha, \ldots, \alpha^{n-1}) &= \det[B_{L/\mathbb{Q}}(\alpha^i, \alpha^j)] \\ &\overset{\text{Bem. 16.2}}{=} (\text{Vandermonde Determinante})^2 \\ &\overset{\text{Bem. 17.1}}{=} [\prod_{i<j}(\alpha_i - \alpha_j)]^2 \end{aligned}$$

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

Diese Berechnung motiviert die folgende allgemeine Definition:

Definition 18.1
Sei $g \in \mathbb{Q}[x]$ irreduzibel und $\alpha_1, \ldots, \alpha_n$ alle Nullstellen von g. Die Diskriminante von g ist $D(g) := \prod_{i<j}(\alpha_i - \alpha_j)^2$.

Bemerkung 18.1
Sei $\{\beta_1, \ldots, \beta_n\}$ eine Ganzheitsbasis für $\mathcal{O}_L$ als $\mathbb{Z}$-Modul. Sei P wie in $(*)$ im Beweis vom Satz 17.2. Wir berechnen $D(f) \in \mathbb{Z}$ mithilfe der $(**)$ im Beweis vom Satz 17.2:

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

Diese Gleichung (†) ist sehr hilfreich weil:

(i) Aus (†) und Satz 17.2 folgt daß 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 und $\{1, \alpha, \ldots, \alpha^{n-1}\}$ ist eine Ganzheitsbasis.

(iii) Wenn $D(f)$ nicht quadratfrei ist, benutzen wir den **Satz von Stickelberger**.

Satz 18.1 (Satz von Stickelberger)
$D(\mathcal{O}_L/\mathbb{Z}) \equiv 0, 1 \bmod 4$, also ist $D(\mathcal{O}_L/\mathbb{Z})$ ein Quadrat mod 4.

Bevor wir den Satz von Stickelberger beweisen, wollen wir eine Anwendung der Bemerkung 18.1 auf die Berechnung von Ganzheitsbasen für quadratische Zahlkörper bringen (vgl. Algebra 2; Kapitel 1).

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

Fall 1: Wenn $d \equiv 2, 3 \bmod 4$, dann ist $\{1, \sqrt{d}\}$ ist eine Ganzheitsbasis

(und somit ist $\mathcal{O}_L = \mathbb{Z}[\sqrt{d}]$).

Hier haben wir $\alpha = \sqrt{d}$ das primitive Element, $d \in \mathcal{O}_L$ und $f(x) = \text{ MinPol}_{\mathbb{Q}}(\alpha) = x^2 - d$. Die Nullstellen von f sind

$$x_{1,2} := \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} .$$

Also ist $D(f) = (x_1 - x_2)^2 = 4d$. Nun ist $4d = \underbrace{(\det P)^2}_{\in \mathbb{Z}} \quad \underbrace{D(\mathcal{O}_L/\mathbb{Z})}_{\equiv 0,1 \bmod 4 (s.\ Satz\ 18.1)}$

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 $\{1, \sqrt{d}\}$ eine Ganzheitsbasis.

Fall 2: Wenn $d \equiv 1 \bmod 4$, dann ist $\{1, \frac{1+\sqrt{d}}{2}\}$ ist eine Ganzheitsbasis

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

Beweis. $f = \text{ MinPol}_{\mathbb{Q}}(\omega) = x^2 - x + [\frac{1-d}{4}] \in \mathbb{Z}[x]$ und $D(f) = 1 - [4(\frac{1-d}{4})] = d$, d quadratfrei, also folgt nun unsere Behauptung aus Bemerkung 18.1(ii). □

B4: Algebraische Zahlentheorie
Sommersemester 2021
Frau Prof. Dr. Salma Kuhlmann

19.Vorlesung

24. Juni 2021

In diesem Skript werden wir die Sätze von Stickelberger und von Brill beweisen. Wir werden diese Ergebnisse anwenden zur Berechnung der Diskriminante.

Ansatz und Notation wie in Skript 16, 17 und 18.

Erinnerung (Bem. 17.1; ÜB)**:** Sei L/K eine endliche separable Erweiterung, $n = [L : K]$, $\{\mu_1, \dots, \mu_n\}$ eine Basis für L/K, $\sigma_1, \dots, \sigma_n$ die verschiedene Einbettungen von L über K in Ω; dann gilt

$$\det(B_{L/K}(\mu_i, \mu_j)) = \underbrace{(\det(\sigma_i(\mu_j))^2}_{\neq 0} \in \mathbb{Z}\,.$$

Beweis von Stickelberger. Sei nun $\{\mu_1, \dots, \mu_n\}$ eine Ganzheitsbasis von $\mathcal{O}_L$ über $\mathbb{Z}$. Nach Definition von $D(\mathcal{O}_L/\mathbb{Z})$ berechnen wir:

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

wobei

$$G := \sum_{\pi\in A_n} \operatorname{sign}(\pi)\sigma_{\pi(1)}(\mu_1)\dots\sigma_{\pi(n)}(\mu_n)$$

und

$$U := -(\sum_{\pi\in S_n\setminus A_n} \operatorname{sign}(\pi)\sigma_{\pi(1)}(\mu_1)\dots\sigma_{\pi(n)}(\mu_n)\,)\,.$$

• Aus den Definitionen folgt daß $G, U \in \mathcal{O}_L$, $\mathcal{O}_L \subseteq \Omega$, $\mathbb{Q} \subseteq L \subseteq \Omega$ ist Galois Erweiterung.

• Sei nun $\tau \in \operatorname{Gal}(\Omega/\mathbb{Q})$. Für jedes $i \in \{1, \dots, n\}$ haben wir die Einbettungen σ_i und $\tau \circ \sigma_i$:

$$\sigma_i : L \hookrightarrow \Omega \text{ und } L \xrightarrow{\sigma_i} \Omega \xrightarrow{\tau} \Omega\,.$$

Es folgt daß $\forall i \in \{1, \dots, n\}\ \exists j \in \{1, \dots, n\}$, so daß $\tau \circ \sigma_i = \sigma_j$.
Also ist die Abbildung

$$\rho : i \mapsto j \text{ definiert durch } \rho(i) = j \Leftrightarrow \tau \circ \sigma_i = \sigma_j$$

eine Permutation, das heißt $\rho \in S_n$.

• Per Definition von ρ berechnen wir nun für jedes $\pi \in S_n$:

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

• Wir betrachten nun zwei Fälle und in jedem Fall:

(i) $\rho \in A_n \Rightarrow \tau(G) = G, \tau(U) = U$ oder

(ii) $\rho \in S_n \backslash A_n \Rightarrow \tau(G) = U, \tau(U) = G$.

Somit ist

$$(*) \qquad \tau(G+U) = G+U \text{ und } \tau(GU) = GU \quad \forall \tau \in \mathrm{Gal}(\Omega/\mathbb{Q})\,.$$

• Es folgt nun aus $(*)$ und Hauptsatz der Galoistheorie (B3, Skript 24, Satz 24.5) daß

$$G+U, GU \in \mathrm{Inv}(\Omega/\mathbb{Q}) \underset{HSGT}{=} \mathbb{Q}\,.$$

Also sind $G+U, GU \in \mathbb{Q}$ und $\mathbb{Z}$ ist ganz abgeschlossen$\Rightarrow G+U, GU \in \mathbb{Z}$.

• Schließlich berechnen wir:

$$D(\mathcal{O}_L/\mathbb{Z}) = (G-U)^2 = \underbrace{(G+U)^2}_{\in\mathbb{Z}} - \underbrace{4GU}_{\in 4\mathbb{Z}} \Rightarrow (G-U)^2 \equiv (G+U)^2 \bmod 4 \text{ in } \mathbb{Z}\,.$$

Also ist $D(\mathcal{O}_L/\mathbb{Z})$ ein Quadrat mod 4 wie behauptet. □

Definition 19.1
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.

Erinnerung: Setze $L = \mathbb{Q}(\alpha)$, $[L:\mathbb{Q}] = n$, $f(x) := \mathrm{MinPol}_{\mathbb{Q}}(\alpha)$. Dann ist (Fundamentaler Satz der Algebra) $f(x) = \prod(x-\alpha_i) \in \mathbb{C}[x]$ mit r reellen Nullstellen und $2s$ komplexen Nullstellen, so daß $n = 2s+r$. L hat genau r relle Einbettungen in $\mathbb{C}$ und $2s$ komplexe Einbettungen in $\mathbb{C}$. **Bezeichnung:** $\mathbb{R}_+ = \mathbb{R}^{>0}, \mathbb{R}_- := \mathbb{R}^{<0}$.

Satz 19.1 (Satz von Brill)
Es gilt $\mathrm{sign} D(\mathcal{O}_L/\mathbb{Z}) = (-1)^s$

Beweis. $L = \mathbb{Q}(\alpha)$, $[L:\mathbb{Q}] = n$, $f := \mathrm{MinPol}_{\mathbb{Q}}(\alpha)$. Sei $\{\alpha_1,\dots,\alpha_n\} \subseteq \mathcal{O}_L$ Basis für $L/\mathbb{Q}$ [1].
Sei P wie im Beweis vom Satz 17.2.[2] Es ist:

$$D(\alpha_1,\dots,\alpha_n) = (\det P)^2 D(\mathcal{O}_L/\mathbb{Z})$$

Insbesondere ist aufjedenfall $\mathrm{sign} D(\alpha_1,\dots,\alpha_n) = \mathrm{sign} D(\mathcal{O}_L/\mathbb{Z})$.

[1] Wir haben schon gesehen daß es immer möglich ist, solch eine Basis zu finden, z.B. für ein primitives Element α in $\mathcal{O}_L$ setze $\alpha_i := \alpha^i$.

[2] $P \in M_{n\times n}(\mathbb{Z})$, $\det P \neq 0$ aber nicht unbedingt invertierbar in $\mathbb{Z}$.

Wir berechnen nun $\text{sign}D(1, \alpha, \ldots, \alpha^{n-1})$, d.h wir berechnen $\text{sign}D(f)$.

Seien $\beta_1, \ldots, \beta_r, z_1, \ldots, z_s, \bar{z}_1, \ldots, \bar{z}_s$ alle Nullstellen von f in $\mathbb{C}$. Also gilt die Faktorisierung:

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

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

.

Wir untersuchen diese Produkte genau und bestimmen das Signum:

- $\prod_{i<j} (\beta_i - \beta_j)^2 \in \mathbb{R}^2 > 0$ (da $\beta_i \neq \beta_j$) also $\in \mathbb{R}_+$.
- $\underbrace{\prod_{i,k} (\beta_i - z_k)^2}_{:=w} \underbrace{\prod_{i,k} (\beta_i - \bar{z}_k)^2}_{\bar{w}} = w\bar{w} \in \mathbb{R}_+$.
- 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 tatsächlich die Faktoren $z_k - \bar{z}_l$ sowie $z_l - \bar{z}_k$ im Produkt, also

$$(z_k - \bar{z}_l)^2 (z_l - \bar{z}_k)^2 = [- \underbrace{(z_k - \bar{z}_l)(\bar{z}_k - z_l)}_{\in \mathbb{R}^+}]^2 \in \mathbb{R}_+$$

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 Signum $(-1)^s$. $\square$

B4: Algebraische Zahlentheorie
Sommersemester 2021
Frau Prof. Dr. Salma Kuhlmann

20.Vorlesung

29. Juni 2021

In diesem Skript werden wir weitere Berechnungen für Diskriminante führen und damit Kapitel 5 beenden. Wir werden dann Kapitel 6 über Gitter und die Geometrie der Zahlen anfangen, mit dem Ziel, die Endlichkeit der Klassenzahl für Zahlkörper zu beweisen.

Ansatz und Bezeichnung weiterhin wie im Skript 14, 15, 16, 17, 18, 19.

Proposition 20.1
Sei L/K eine endliche separable Körpererweiterung, $[L:K]=n$, α primitives Element, $f = \text{MinPol}_K(\alpha)$. Es ist

$$D(f) = (-1)^{\frac{n(n-1)}{2}} N_{L/K}(f'(\alpha))$$

Beweis. Seien $\alpha_1, \ldots, \alpha_n$ die verschiedenen Nullstellen von f, und $\sigma_1, \ldots, \sigma_n$ die Einbettungen von L über K in Ω. Schreibe $f(x) = \prod(x-\alpha_i)$ und berechne

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

• Per Definition von $N_{L/K}$ und Satz 15.4 haben wir

$$(\ddagger) \qquad N_{L/K}(f'(\alpha)) = \prod_{k=1}^{n} \sigma_k(f'(\alpha)) = \prod_{k=1}^{n} (f'(\sigma_k(\alpha))) = \prod_{k=1}^{n} f'(\alpha_k)\,.$$

• Einsetzen von α_k in $(\dagger)$ und von $f'(\alpha_k)$ in $(\ddagger)$ ergibt:

$$f'(\alpha_k) = \prod_{j\neq k} (\alpha_k - \alpha_j)$$

und

$$(*) \quad N_{L/K}(f'(\alpha)) = \prod_{k=1}^{n} \prod_{j\neq k} (\alpha_k - \alpha_j)\,.$$

• Per Definition haben wir:

$$(**) \quad D(f) = \prod_{j<k} (\alpha_k - \alpha_j)^2\,.$$

• Wir vergleichen nun das Produkt im $(*)$ mit $(**)$:
In $N_{L/K}(f'(\alpha))$ wie in $(*)$ erscheint jede Differenz $(\alpha_k - \alpha_j)$ zweimal und zwar für (j,k) und (k,j), d.h. $(\alpha_j - \alpha_k)(\alpha_k - \alpha_j) = -(\alpha_j - \alpha_k)^2$ erscheint im $(*)$.
Dagegen erscheint für jedes $k = 1, \ldots, n$, mit $j < k$ der Faktor $(\alpha_j - \alpha_k)^2$ wie in $(**)$ in $D(f)$.

Zusammengefasst: $\forall k = 1, \ldots, n$ und $j < k$ wird ein Faktor (-1) beigetragen, insgesamt also $(n-1) + (n-2) + \cdots + 0$ Beiträge. Also weicht $(**)$ von $(*)$ mit dem Faktor $(-1)^{\frac{n(n-1)}{2}}$ ab. □

Proposition/Beispiel
Sei $f(x) = x^n + ax + b \in \mathbb{Q}[x]$ irreduzibel, α eine Nullstelle, setze $L := \mathbb{Q}(\alpha)$, $n = [L : \mathbb{Q}]$.
Wir wollen Proposition 20.1 anwenden und $D(f)$ berechnen. Setze $\gamma := f'(\alpha) = n\alpha^{n-1} + a$. Wir müssen $N_{L/\mathbb{Q}}(\gamma)$ berechnen.
Dafür werden wir das minimal Polynom von γ berechnen und dann Lemma 14.2 4 (i) anwenden.

Nun erfüllt α die Gleichung $\alpha^n + a\alpha + b = 0$. 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 $n = [\mathbb{Q}(\gamma) : \mathbb{Q}]$.
Setze $y = \frac{-nb}{x+(n-1)a} \in \mathbb{Q}(x)$ und betrachte die rationale Funktion $f(y) = \frac{p(x)}{q(x)} \in \mathbb{Q}(x)$. Einsetzen von $x = \gamma$ in y ergibt:

$$0 = f(\alpha) = \frac{p(\gamma)}{q(\gamma)} = 0\,.$$

Somit muss $p(\gamma) = 0$. Wenn wir $f(y) = y^n + ay + b$ direkt berechnen und als Quotient umschreiben bekommen wir

$$p(x) = (x + (n-1)a)^n - na(x + (n-1)a)^{n-1} + (-1)^n n^n b^{n-1}$$

und der konstante Koeffizient a_0 von $p(x)$ ist

$$(n-1)^n a^n - na(n-1)^{n-1}a^{n-1} + (-1)^n n^n b^{n-1}$$

(ÜA).
Da $p(x) \in \mathbb{Q}[x]$ normiert ist, $\deg p = n$ und $p(\gamma) = 0$, folgt nun $p(x)$ ist das $\mathrm{MinPol}_{\mathbb{Q}}(\gamma)$.
Wir berechnen nun wegen Lemma 14.2 4 (i):

$$N_{L/\mathbb{Q}}(\gamma) = (-1)^n a_0 = (-1)^n (n-1)^n a^n - na(n-1)^{n-1}a^{n-1} + (-1)^n n^n b^{n-1}\,.$$

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 20.1
$f(x) = x^3 - x - 1$ 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 $\mathcal{O}_L = \mathbb{Z}[\alpha]$.

Kapitel 6: Gitter in $\mathbb{R}^n$

Wir behalten die Bezeichnungen der LA I und LA II, zum Beispiel: $||x||$ ist die euklisdische Norm für $x \in \mathbb{R}^n$.

Definition 20.1 (i) Sei $\{e_1, \ldots, e_m\} \subseteq \mathbb{R}^n$ linear unabhängig über $\mathbb{R}$ (also $m \leq n$). Die von $\{e_1, \ldots, e_m\}$ erzeugte additive Gruppe Γ ist ein Gitter der Dimension m. Das heißt

$$\Gamma := \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_m$$

ist eine freie abelsche Gruppe vom Rang m.

Wenn $m = n$ heißt Γ vollständiges Gitter

(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 $r \in \mathbb{R}_+$.

Definition 20.2
Sei Γ ein Gitter mit erzeugender Menge $\{e_1, \ldots, e_n\}$.
$T := \{x \in \mathbb{R}^n \mid x = \sum a_i e_i, 0 \leq a_i < 1, a_i \in \mathbb{R}\}$ heißt fundamentaler Parallelotop von Γ.

B4: Algebraische Zahlentheorie
Sommersemester 2021
Frau Prof. Dr. Salma Kuhlmann

21.Vorlesung

01. Juli 2021

In diesem Skript werden wir Gitter und Ihre fundamentale Parallelotope untersuchen und den Satz von Minkowski 21.8 beweisen. Den Satz werden wir ab Skript 22 aufrufen, um die Endlichkeit der Klassenzahl zu beweisen.

Das folgende Lemma 21.1 erklärt die Rolle von fundamentale Parallelotope (f.P.) T.

Lemma 21.1
Sei Γ ein Gitter, T f.P von Γ. Es gilt: $\forall v \in \mathbb{R}^n, \exists! l \in \Gamma$, so daß $v \in T + l$

Beweis. Sei $\{e_1, \ldots, e_n\}$ eine Basis von $\mathbb{R}^n$ die Γ erzeugt und sei $v \in \mathbb{R}^n$. Schreibe

$$v = \sum b_i e_i \text{ mit } b_i \in \mathbb{R}$$

und setze

$$z_i := \lfloor b_i \rfloor \in \mathbb{Z}\,.$$

Dann ist

$$a_i := b_i - z_i \in \mathbb{R} \text{ und } 0 \leq a_i < 1\,.$$

Es ist $v = t + l$, wobei $t := \sum a_i e_i \in T$ und $l := \sum z_i e_i, l \in \Gamma$. □

Satz 21.2
Eine additive Untergruppe Γ von $(\mathbb{R}^n, +)$ ist genau dann ein Gitter, wenn Γ diskret ist.

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

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

Es ist klar daß : $f(B_r(0))$ ist beschränkt (ÜA), 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.

„⇐“ 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. Das heißt: 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:

$$T := \{x \in \Gamma \mid x = \sum_{i=1}^{m} a_i g_i, a_i \in \mathbb{R}, 0 \leq a_i < 1, i = 1, \ldots, m-1 \text{ und } 0 \leq a_m \leq 1\} .$$

Es ist: T ist beschränkt (ÜA). Also ist T endlich, da Γ diskret ist.

• Wähle also $x' \in T, x' = \sum_{i=1}^{m} b_i g_i$ mit b_m kleinste $\neq 0$ Koeffizient von g_m.

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

Beweis. Es ist klar, daß diese Menge immernoch linear unabhängig ist (ÜA). 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 (vgl. Lemma 1). Aus der Wahl von x' gilt nun: dieser Koeffizient ist 0, also ist $g' \in \Gamma_0$. □

□

Wir studieren nun die Faktorgruppe $(\mathbb{R}^n, +)/(\Gamma, +)$.

• Wir fangen an mit dem Fall $n = 1$. Setze

$$S := \{z \in \mathbb{C} \mid |z| = 1\} .$$

S ist eine multiplikative Untergruppe von $\mathbb{C}$.
Erinnerung: $i = \sqrt{-1} \in \mathbb{C}$.

Lemma 21.3
$(\mathbb{R}, +)/(\mathbb{Z}, +) \cong (S, \times)$.

Beweis. Betrachte die surjektive Abbildung

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

ϕ ist ein Homomorphismus und $\ker(\phi) = (\mathbb{Z}, +)$ (ÜA). □

• Allgemeiner für $n \in \mathbb{N}$ setze

$$\mathbb{T}^n := \underbrace{S \times S \times \ldots S}_{n \text{ mal}}$$

(der n-dimensionaler Torus).

Satz 21.4
Sei Γ ein vollständiges Gitter in $\mathbb{R}^n$, dann ist $(\mathbb{R}^n, +)/(\Gamma, +) \cong (\mathbb{T}^n, \times)$.

Beweis. Sei $\{e_1, \ldots, e_n\}$ eine Basis für Γ und betrachte $\phi : (\mathbb{R}^n, +) \to (\mathbb{T}^n, \times)$ definiert durch $\phi(\sum a_i e_i) = (e^{2ia_1\pi}, \ldots, e^{2ia_n\pi})$. ϕ ist surjektiver Homomorphismus mit $\ker(\phi) = \Gamma$. (ÜA). □

Lemma 21.5
$\phi_{|T} : T \to \mathbb{T}^n$ ist injektiv.

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

Allgemeiner gilt für beliebige Gitter

Satz 21.6
Sei $\Gamma \subseteq \mathbb{R}^n$ ein m-dimensionales Gitter (also $m \le n$), 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
$\mathbb{R}^n = V \bigoplus W \underset{\text{Satz 21.4}}{\cong} \mathbb{T}^m \times \mathbb{R}^{n-m}$ □

Definition 21.1 (i) Sei $X \subseteq \mathbb{R}^n$ Lebesgue-meßbar. Definiere $v(X) = \int_X dx_1 \dots dx_n$ das Volumen von X (Lebesgue-Maß von X).

(ii) Sei $\Gamma \subseteq \mathbb{R}^n$ ein vollständiges Gitter, $X \subseteq \mathbb{T}^n$, und $\phi := \phi_{|T}$ wie im Lemma 21.5. 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 21.7
Sei $X \subseteq \mathbb{R}^n$ beschränkt, so daß $v(X)$ existiert (d.h. X ist beschränkt und Lebesgues-meßbar). Aus $v(\phi(X)) \neq v(X)$ folgt, daß $\phi_{|X}$ nicht injektiv ist.

Beweis. Sei X beschränkt und $\phi_{|X}$ injektiv. Es existieren $l_1, \dots, l_s \in \Gamma$, so daß $l_i \neq l_j$ für $j \neq i$ und $X_{l_j} := X \cap (T + l_j) \neq \varnothing \quad \forall j = 1, \dots, s$. Also $X = \bigsqcup_{j=1}^{s} X_{l_j}$ (folgt aus Lemma 1, ÜA).
Für $j = 1, \dots, s$, 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 $Y_{l_j} \subseteq T$).

Wir berechnen nun

$$v(\phi(X)) = v(\phi(\bigsqcup_j X_{l_j})) \underset{(b),(c)}{=} v(\bigsqcup_j Y_{l_j}) = \sum_j v(Y_{l_j}) \underset{(a)}{=} \sum_j v(X_{l_j}) = v(X) \,.$$

□

Definition 21.2 (i) $X \subseteq \mathbb{R}^n$ ist <u>konvex</u>, wenn $\forall x, y \in X$ und $\forall \lambda \in \mathbb{R}$ mit $0 \le \lambda \le 1$ gilt $\lambda x + (1-\lambda)y \in X$.

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

Satz 21.8 (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 den Torus $\mathbb{T}^n = \mathbb{R}^n/2\Gamma$.
Berechne $v(\mathbb{T}^n) = v(2T) = 2^n v(T)$. Für $\phi : \mathbb{R}^n \to \mathbb{T}^n$ ist $\ker \phi = 2\Gamma$ und $\phi(X) \subseteq \mathbb{T}^n$, also

$$v(\phi(X)) \le v(\mathbb{T}^n) = 2^n v(T) < v(X) \,.$$

Aus Satz 21.7 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. $\frac{1}{2}(x_1 - x_2) \in X$. □

B4: Algebraische Zahlentheorie
Sommersemester 2021
Frau Prof. Dr. Salma Kuhlmann

22.Vorlesung

06. Juli 2021

Wir betrachten den folgenden Ansatz: $L/\mathbb{Q}$ ein Zahlkörper von Grad n, $\mathcal{O}_L = \overline{\mathbb{Z}}^L$. Wir wissen, daß $L = Quot(\mathcal{O}_L)$ (Satz 9.5) und daß $\mathcal{O}_L$ ein Dedekindring ist (Satz 13.5). Wir verfolgen das folgende Ziel: Wir wollen den gebrochenen Idealen von $\mathcal{O}_L$ Gittern in $\mathbb{R}^n$ zuordnen. Wir werden dabei, oft stillschweigend, die Ergebnisse von [Algebra II; Kapitel 4] (insbesondere bezüglich der Klassengruppe) benutzen.

Erinnerung: • Sei θ ein primitives Element für L, i.e. $L = \mathbb{Q}(\theta)$ und seien $\sigma_1, \ldots, \sigma_n$ die n verschiedenen Einbettungen von L in $\Omega := \mathbb{C}$.

• Ist $\sigma_i(\theta) \in \mathbb{R}$ (also $\sigma_j(L) \subseteq \mathbb{R}$), so heißt σ_j reell. Sonst heißt σ_j komplex.
In diesem Fall ist auch $\bar{\sigma}_j$ komplex.

• Sei $s := \sharp$reelle Einbettungen und $2t := \sharp$ komplexe Einbettungen. Es ist $n = s + 2t$, und

$$\sigma_1, \ldots, \sigma_s \; ; \; \sigma_{s+1}, \bar{\sigma}_{s+1}, \; \cdots \; , \; \sigma_{s+t}, \bar{\sigma}_{s+t}$$

sind die n verschiedene Einbettungen.

• Setze $L_{\mathbb{R}} := \mathbb{R}^S \times \mathbb{C}^t = \mathbb{R}^S \times \mathbb{R}^{2t}$.

§Idealnorm und Eigenschaften

Definition 22.1
Sei $0 \neq \mathfrak{a} \lhd \mathcal{O}_L$, definiere
$N(\mathfrak{a}) := [\mathcal{O}_L : \mathfrak{a}] = |(\mathcal{O}_L, +)/(\mathfrak{a}, +)|$
($N(\mathfrak{a})$ ist a priori endlich oder ∞).

Satz 22.1
Seien $\mathfrak{a}, \mathfrak{b} \lhd \mathcal{O}_L$, $\mathfrak{a} \neq 0$, $\mathfrak{b} \neq 0$.

(1) Es ist $N(\mathfrak{b}) < \infty$

(2) $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$

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 dann aus $(**)$ wegen Primfaktorisierung von Idealen in Dedekindringen.

Zu (1): Sei $0 \neq \alpha \in \mathfrak{b}$ und betrachte $\alpha := \sigma_1(\alpha)$ sowie $\sigma_2(\alpha) \ldots, \sigma_n(\alpha)$. Berechne:

$$n_\alpha := N_{L/\mathbb{Q}}(\alpha) \underset{\text{Satz 15.4}}{=} \prod_{i=1}^{n} \sigma_i(\alpha) = \alpha \prod_{i=2}^{n} \sigma_i(\alpha) \,.$$

• Da $\alpha \in \mathcal{O}_L$, ist $n_\alpha \in \mathbb{Z}$ (Korollar 15.2). 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 das Hauptideal $< n_\alpha >= \mathcal{O}_L n_\alpha \subseteq \mathfrak{b}$.

• Wir haben also 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 (Satz 17.3), insbesondere ist $\mathcal{O}_L$ ein endlich erzeugter $\mathbb{Z}$-Modul. Also ist auch $\mathcal{O}_L / < n_\alpha >$ endlich erzeugt.

• Da $n_\alpha \in \mathbb{Z}$ ist außerdem $\mathcal{O}_L / < n_\alpha >= (\mathcal{O}_L / < n_\alpha >)_{\text{tor}}$ ein Torsionsmodul (ÜA). Ein endlich erzeugter Torsionsmodul über $\mathbb{Z}$ ist endlich (folgt aus Struktursatz für endlich erzeugte Moduln über HIR). Insbesondere ist $\mathcal{O}_L/\mathfrak{b}$ auch endlich (als Bild von ψ).

Zu $(**)$: Dafür genügt es zu zeigen, daß

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

und

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

• Zu (a): $\mathcal{O}_L/\mathfrak{ap} \to \mathcal{O}_L/\mathfrak{a}$, $x + \mathfrak{ap} \mapsto x + \mathfrak{a}$ 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 $|\mathcal{O}_L/\mathfrak{a}| = \frac{|\mathcal{O}_L/\mathfrak{ap}|}{|\mathfrak{a}/\mathfrak{ap}|}$ (wegen Lagrange).

• Zu (b): Bemerke, daß $\mathfrak{ap} \subsetneq \mathfrak{a}$ (wegen Eindeutigkeit der Primfaktorisierung).

Behauptung: Sei $I \lhd \mathcal{O}_L$. Wenn $\mathfrak{ap} \subseteq I \subseteq \mathfrak{a}$, 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 $\mathfrak{p} \subseteq \mathfrak{a}^{-1}I \subseteq \mathcal{O}_L$.
Nun $\mathfrak{p}$ maximal $\Rightarrow \mathfrak{p} = \mathfrak{a}^{-1}I$ (in diesem Fall $\mathfrak{ap} = I$) oder $\mathcal{O}_L = \mathfrak{a}^{-1}I$ (in diesem Fall $\mathfrak{a} = I$). □

Wähle nun $x \in \mathfrak{a}$ so daß $x \notin \mathfrak{ap}$ 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

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

Da $\mathfrak{ap} + < x >= \mathfrak{a}$, ist ψ surjektiv mit $\mathfrak{p} \subseteq \ker\psi \subseteq \mathcal{O}_L$, und da $\mathfrak{ap} \neq \mathfrak{a}$ ist $\ker\psi \neq \mathcal{O}_L$ (ÜA). Da $\mathfrak{p}$ maximal ist, folgt nun $\mathfrak{p} = \ker\psi$. Es folgt: $\mathcal{O}_L/\mathfrak{p} \cong \mathfrak{a}/\mathfrak{ap}$ □

Bevor wir die nächste Propositionen beweisen, fassen wir zusammen allgemeine ergänzende Bemerkungen:

Bemerkung 22.1 (i) Sei N ein freier $\mathbb{Z}$-Modul vom Rang n (i.e. $N \simeq \mathbb{Z}^n$) und $M \leq N$ ein Untermodul. Da $\mathbb{Z}$ ein HIR ist, wissen wir daß M frei vom Rang $m \leq n$ ist. Wir behaupten daß:

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

Beweis von (i).

Behauptung 1: Sei $\{y_1, \dots, y_m\} \subseteq \mathbb{Z}^n$ eine $\mathbb{Z}$-Basis für M. Betrachte die Matrix $A \in M_{m\times n}(\mathbb{Z})$ mit Zeilen $\{y_1, \dots, y_m\}$, also $A := \begin{pmatrix} y_1 \\ \dots \\ y_m \end{pmatrix}$.

Man kann zeigen, daß elementare Zeilen- und Spaltenumformungen eine Matrix $B \in M_{m\times n}(\mathbb{Z})$ mit folgender Eigenschaft ergeben:

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

(ÜA).

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

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

• 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 $v_z := (\underbrace{0, \dots, 0}_{m}, \underbrace{z}_{\in\mathbb{Z}}, 0, \dots, 0)$. Bemerke daß $v_z \notin \operatorname{Span}_{\mathbb{Z}}B$ wenn $z \neq 0$ (ÜA).

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

„$\Leftarrow$“ Wir nehmen nun an, daß $\dim_{\mathbb{Z}} M = n$, d.h. $n = m$. Dann ist $B = \begin{pmatrix} d_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & d_n \end{pmatrix}$,
$d_i \neq 0$, 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) Zusatz: Wir sehen außerdem, daß $n = m \Rightarrow |\mathbb{Z}^n/M| = |\det B| = |\det A|$, d.h
$n = m \Rightarrow [\mathbb{Z}^n : M] = |\det A|$.

B4: Algebraische Zahlentheorie
Sommersemester 2021
Frau Prof. Dr. Salma Kuhlmann

23.Vorlesung

08. Juli 2021

In diesem Skript ist der Ansatz weiterhin im Skript 22. Wir werden, oft stillschweigend, die Notationen und Ergebnisse von [Algebra II; Kapitel 4] (insbesondere bezüglich der Klassengruppe), sowie die Eigenschaften der Norm und Diskriminante (Skripte 15,16,17) benutzen. Wir werden zunächst in Propositionen 23.1 und 23.2 zwei weitere Schlüssel Eigenschaften von Idealnorm erklären. Dann werden wir Satz 23.3 beweisen. Um unser Hauptziel (Satz 23.6; Endlichkeit der Klassenzahl) zu erreichen werden wir Satz 23.4 (Minkowski Schranke) aussagen und gleich anwenden. Den Beweis vom Satz 23.4 werden wir erst im Skript 24 führen.

Proposition 23.1
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. Bemerke zunächst daß die Aussage sinnvoll ist: 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 22.1(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:
$D(y_1, \ldots, y_n) \underset{17.Vor.}{=} \det A^2 D(e_1, \ldots, e_n) = \det A^2 D(\mathcal{O}_L/\mathbb{Z})$.
Andererseits folgt aus Bemerkung 22.1 (ii), daß
$|\det A| = [\mathcal{O}_L : \mathfrak{a}]$.
Alles zusammen ergibt: $D(y_1, \ldots, y_n) = N(\mathfrak{a})^2 D(\mathcal{O}_L/\mathbb{Z})$ □

Proposition 23.2
Sei $0 \neq \beta \in \mathcal{O}_L$. Es ist $\underbrace{N(<\beta>)}_{\in\mathbb{N}} = |\underbrace{N_{L/\mathbb{Q}}(\beta)}_{\in\mathbb{Z}}|$.

Beweis. • 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 23.1 folgern wir, daß

$$D(\beta e_1, \ldots, \beta e_n) = D(\mathcal{O}_L/\mathbb{Z})N(<\beta>)^2\,.$$

Andererseits per Definition wissen wir, daß

$$D(\beta e_1, \ldots, \beta e_n) = \det(B_{L/\mathbb{Q}}(\beta e_i, \beta e_j))\,.$$

• Wir berechnen (ÜA, ÜB):

$$\det(B_{L/\mathbb{Q}}(\beta e_i, \beta e_j)) = (\det((\sigma_i(\beta e_j))_{ij}))^2 = (\det((\sigma_i(\beta)\sigma_i(e_j))_{ij}))^2 .$$

• Nun ist (ÜA, Eigenschaften von Determinanten)

$$\det((\sigma_i(\beta)\sigma_i(e_j))_{ij}) = \sigma_1(\beta)\dots\sigma_n(\beta)\det(\sigma_i(e_j)_{ij}) = N_{L/\mathbb{Q}}(\beta)\det(\sigma_i(e_j)_{ij}) .$$

Alles zusammen ergibt:

$$D(\beta e_1, \dots, \beta e_n) = (N_{L/\mathbb{Q}}(\beta))^2(\det(\sigma_i(e_j))_{ij})^2 = (N_{L/\mathbb{Q}}(\beta))^2 D(e_1, \dots, e_n) \underset{\text{Prop 23.1}}{=} N(<\beta>)^2 D(e_1, \dots, e_n)$$

□

Satz 23.3
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. $N(J) = |\mathcal{O}_L/J| \underset{\text{Lagrange}}{\Rightarrow} \forall x \in \mathcal{O}_L, N(J)x \in J$. Insbesondere gilt das für $x = 1$. □

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 $\mathfrak{p}^\mu$ 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 23.4 (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 24. Vorlesung). □

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 und $H(\mathcal{O}_L)$ = die Untergruppe der gebrochenen Hauptideale. $h_L := |\mathcal{K}l(L)|$ ist die Klassenzahl des Zahlkörpers L.

Korollar 23.5
Sei $L/\mathbb{Q}$ ein Zahlkörper und c_L wie in Satz 23.4. Es gilt:

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

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 23.4 $\Rightarrow \exists \beta \in \mathfrak{b}$, 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 (s. Beh. 2 S.2) $\mathfrak{a} \lhd \mathcal{O}_L$. Also ist

$$\mathfrak{q} \overset{(*)}{=} d\mathfrak{b}^{-1} \overset{(**)}{=} d\beta^{-1}\mathfrak{a}\,.$$

Das heißt:

$$\mathfrak{q}\mathfrak{a}^{-1} = \mathcal{O}_L(d\beta^{-1}) \in H(\mathcal{O}_L)\,.$$

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 $N(\mathfrak{a}) \leq c_L$.

□

Satz 23.6 (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 23.3 □

B4: Algebraische Zahlentheorie
Sommersemester 2021
Frau Prof. Dr. Salma Kuhlmann

24.Vorlesung

13. Juli 2021

Sei $L/\mathbb{Q}$ ein Zahlkörper mit $[L:\mathbb{Q}] = n$. Unser Ziel ist es Satz 23.4 (†) beweisen. Wir werden sogar eine explizite Minkowski Schranke c_L in Satz 24.2 angeben. Hier werden wir in Satz 24.1 wie angekündigt Im Skript 22 den Idealen von $\mathcal{O}_L$ Gittern in $\mathbb{R}^n$ zuordnen. Dann werden wir genaue Volumen Berechnungen anstellen. Wir werden weiterhin, oft stillschweigend, die Notationen und Ergebnisse von [Algebra II], sowie die Eigenschaften der Norm und Diskriminante benutzen. Damit werden wir schließlich für den Beweis vom Satz 24.2 Minkowski's Satz 21.8 aufrufen können. Den Beweis von Satz 24.2 werden wir in Skript 25 ausführen.

Ansatz wie am Anfang der 22. Vorlesung (Erinnerung).

Wir definieren nun eine $\mathbb{Q}$-lineare Abbildung σ wie folgt:

$$\sigma : L \to L_{\mathbb{R}} \; ; \; \sigma(\alpha) := (\sigma_1(\alpha), \dots, \sigma_s(\alpha), \sigma_{s+1}(\alpha), \dots, \sigma_{s+t}(\alpha)) \; .$$

Wir erinnern an die Notation:
$(*)$ Für $z \in \mathbb{C}$ und $i = \sqrt{-1}$, ist $\text{Re } z = \frac{z+\bar{z}}{2}$ und $\text{Im } z = \frac{z-\bar{z}}{2i}$.

Satz 24.1
Sei $0 \neq \mathfrak{a} \lhd \mathcal{O}_L$, dann ist $\sigma(\mathfrak{a})$ ein vollständiges Gitter.

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

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

Beweis. Setze für $i = 1, \dots, n$

$$v_i := (\sigma_1(\alpha_i), \dots, \sigma_s(\alpha_i); \; \text{Re } \sigma_{s+1}(\alpha_i), \; \text{Im } \sigma_{s+1}(\alpha_i), \dots, \; \text{Re } \sigma_{s+t}(\alpha_i), \; \text{Im } \sigma_{s+t}(\alpha_i)) \in \mathbb{R}^{s+2t} \; .$$

Nun definiere entsprechend die Matrix $A := \begin{pmatrix} v_1 \\ \dots \\ v_n \end{pmatrix}$.

Andererseits erinnern wir an die Matrix (die wir schon im ÜB untersucht haben):

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

Da $\{\alpha_1, \ldots, \alpha_n\}$ Basis ist haben wir (wie wir im ÜB berechnet haben):

$$0 \neq (\det \mathcal{V})^2 = D(\alpha_1, \ldots, \alpha_n) \,.$$

Wir vergleichen nun die Matrix A mit der Matrix $\mathcal{V}$: wir können A durch elementare Spaltenumformungen aus $\mathcal{V}$ bekommen (siehe Berechnungsaufstellung in $(**)$ weiter unten Seite 2), also ist auch $\det A \neq 0$. □

Nun ist $\mathfrak{a}$ ein freier $\mathbb{Z}$-Modul vom Rang n, also wählen wir nun $\{\alpha_1, \ldots, \alpha_n\} \subseteq \mathfrak{a}$ (Satz und Bemerkung 22.1). Also ist $\sigma(\mathfrak{a}) = \operatorname{Span}_{\mathbb{Z}}\{\sigma(\alpha_1), \ldots, \sigma(\alpha_n)\}$ ein vollständiges Gitter. □

$(**)$ Wir skizzieren nun die Berechnung zwischen A und $\mathcal{V}$, beziehungsweise zwischen $\det A$ und $\det \mathcal{V}$ (bitte die Details prüfen).

Wir durchführen die folgende Spaltenumformungen auf $\mathcal{V}$ (wofür wir $(*)$ ausnutzen):

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

wobei I und II die folgende Umformungen sind:

- 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.

Dann

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

wobei III und IV die folgende Umformungen sind:

- III: $(s+2)$-te Spalte minus $(s+1)$-te Spalte.
- IV: multipliziere mit i.

Dann wiederhole für $(s+3)$-te bis $(s+t)$-te Spalte, insgesamt t mal. Alles zusammen ergibt:

$$\det A = (\frac{1}{2}i)^t \det \mathcal{V} \,.$$

Als nächstes wollen wir nun das Gitter $\sigma(\mathfrak{a}) \subseteq L_{\mathbb{R}}$ und $T_{\sigma(\mathfrak{a})}$ studieren. Wir brauchen einige Bemerkungen:

Bemerkung 24.1
Sei $\Gamma \subseteq \mathbb{R}^n$ ein vollständiges Gitter mit Basis $\{v_1, \ldots, v_n\}$ und f.P. T_Γ.
Es ist $v(T_\Gamma) = |\det \begin{pmatrix} v_1 \\ \ldots \\ v_n \end{pmatrix}|$

Beweis. Siehe ÜB. □

Bemerkung 24.2
Wir wollen Bemerkung 24.1 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

$$(\det \mathcal{V})^2 \underset{\text{ÜB}}{=} D(\alpha_1, \ldots, \alpha_n) \underset{\text{Prop. 23.1}}{=} N(\mathfrak{a})^2 D(\mathcal{O}_L/\mathbb{Z}) \,.$$

Alles zusammen ergibt:

$$v(T_{\sigma(\mathfrak{a})}) = 2^{-t} N(\mathfrak{a}) \sqrt{|D(\mathcal{O}_L/\mathbb{Z})|} \,.$$

Bemerkung 24.3
Sei $\tau \in \mathbb{R}_+$ und setze

$$X_\tau := \{(x_1, \ldots, x_s, z_1, \ldots, z_t) \in L_{\mathbb{R}} \;;\; \sum_{i=1}^{s} |x_i| + 2 \sum_{j=1}^{t} |z_j| < \tau\} \,.$$

Dann ist X_τ beschränkt, konvex, symmetrisch und

$$v(X_\tau) = 2^s (\frac{\pi}{2})^t \frac{\tau^n}{n!}$$

Beweis. Siehe ÜB. □

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

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

Wir können nun eine genauere Aussage über die Minkowski Schranke (Satz 23.4) schreiben.

Satz 24.2 (Explizite Minkowski Schranke)
Sei $L/\mathbb{Q}$ ein Zahlkörper mit $[L : \mathbb{Q}] = n$. Setze

$$c_L := (\frac{4}{\pi})^t \frac{n!}{n^n} \sqrt{|D(\mathcal{O}_L/\mathbb{Z})|} \,.$$

Dann gilt:

$$\forall\, 0 \neq \mathfrak{a} \lhd \mathcal{O}_L \; \exists 0 \neq \alpha \in \mathfrak{a}$$

so daß

$$|N_{L/\mathbb{Q}}(\alpha)| \leq c_L N(\mathfrak{a})$$

Beweis. Folgt im Skript 25. □

B4: Algebraische Zahlentheorie
Sommersemester 2021
Frau Prof. Dr. Salma Kuhlmann

25.Vorlesung

15. Juli 2021

In diesem Skript werden wir Satz 24.2 beweisen (damit ist die Endlichkeit der Klassenzahl vollständig bewiesen) und Kapitel 6 beenden. Danach werden wir unser letztes Kapitel 7 anfangen. Der Hauptsatz im Kapitel 7 ist der Dirichletsche Einheitssatz, womit die Struktur der Einheitengruppe $\mathcal{O}_L^\times$ als $\mathbb{Z}$-Modul erklärt wird.

Für den Beweis vom Satz 24.2, behalten wir den Ansatz und Notation vom Skript 24. Wir benutzen, oft stillschweigend, die Ergebnisse vom Skript 24.

Beweis. Die Beweisstrategie ist folgend. Wir wollen Satz 21.8 anwenden auf

$$\Gamma = \sigma(\mathfrak{a}) \text{ und } X_\tau \subseteq L_{\mathbb{R}} .$$

Wir werden uns nun darum bemühen, *ein geeignetes $\tau \in \mathbb{R}_+$ zu finden.*

• Aus Satz 21.8 folgt, für ein beliebiges $\tau \in \mathbb{R}_+$, daß *wenn*

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

(2) $\exists \alpha \neq 0, \alpha \in \mathfrak{a}$, so daß $\sigma(\alpha) \in X_\tau$, das heißt so daß

$$(\sigma_1(\alpha), \ldots, \sigma_s(\alpha), \sigma_{s+1}(\alpha), \ldots, \sigma_{s+t}(\alpha)) \in X_\tau$$

das heißt so daß

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

• 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 daß $\sum_{l=1}^{n} a_l < \tau$. Die AGU impliziert nun, daß

$$n(a_1 \ldots a_n)^{\frac{1}{n}} < \tau , \text{ d.h. } \prod_{l=1}^{n} a_l < \frac{\tau^n}{n^n} .$$

Daraus folgt daß

$$|N_{L/\mathbb{Q}}(\alpha)| = \prod_{l=1}^{n} a_l < \frac{\tau^n}{n^n} .$$

[Wir prüfen hier kurz, daß $|N_{L/\mathbb{Q}}(\alpha)| = \prod_{l=1}^{n} a_l$. Wir berechnen:

$$\prod a_l = \prod_{i=1}^{s} |\sigma_i(\alpha)| \prod_{j=1}^{t} |\sigma_{s+j}(\alpha)|^2 .$$

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: für ein beliebiges $\tau \in \mathbb{R}_+$, *wenn*

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

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

• Anders formuliert (s. Bem. 24.2 und 24.3): für ein beliebiges $\tau \in \mathbb{R}_+$, *wenn*

(1) $2^s(\frac{\pi}{2})^t \frac{\tau^n}{n!} > 2^n 2^{-t} N(\mathfrak{a})\sqrt{|D(\mathcal{O}_L/\mathbb{Z})|}$, *dann gilt*

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

• Wir analysieren nun die Bedingung (1) genauer:

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

• Wir haben bewiesen: für ein beliebiges $\tau \in \mathbb{R}_+$, *wenn*

(1) $\tau^n > n!(\frac{4}{\pi})^t N(\mathfrak{a})\sqrt{|D(\mathcal{O}_L/\mathbb{Z})|}$, *dann*

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

• Für jedes τ wie in (1) definieren wir

$$A_\tau := \{0 \neq \alpha \in \mathfrak{a} \,;\, |N_{L/\mathbb{Q}}(\alpha)| < \frac{\tau^n}{n^n}\} .$$

Wegen (1) und (2) gelten folgende Eigenschaften (ÜA):

- $A_\tau \neq \varnothing$,
- $|A_\tau| < \infty$ (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

$$\bigcap_{\tau \in \mathbb{R}_+ \text{ , und } \tau \text{ erfüllt (1)}} A_\tau \neq \varnothing \, .$$

(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

$$|N_{L/\mathbb{Q}}(\alpha)| \leq c_L N(\mathfrak{a}) \quad .$$

In der Tat, da $0 \neq \alpha \in \cap A_\tau$ ist, gilt

$$|N_{L/\mathbb{Q}}(\alpha)| < \frac{\tau^n}{n^n} \, , \forall \, \tau \textbf{ die (1) erfüllen} \, .$$

Es folgt :

$$|N_{L/\mathbb{Q}}(\alpha)| \leq \inf_{\tau \textbf{ erfüllt (1)}} \{\frac{\tau^n}{n^n}\} = \frac{1}{n^n} \inf_{\tau \textbf{ erfüllt (1)}} \tau^n \, .$$

Nun ist aber

$$\inf_{\tau \textbf{ erfüllt (1)}} \tau^n = n! (\frac{4}{\pi})^t \sqrt{|D(\mathcal{O}_L/\mathbb{Z})|} \, N(\mathfrak{a}) \, .$$

□

Kapitel 7: Die Einheitsgruppe $\mathcal{O}_L^\times$

Ansatz wie in der 20. Vorlesung (Erinnerung).

Satz 25.1 (Dirichletsche Einheitssatz)
$\mathcal{O}_L^\times$ ist eine endlich erzeugte abelsche Gruppe mit freiem Rang $s + t - 1$.

Beweis. Im Skript 26. □

Bemerkung 25.1
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 [Algebra II ; Satz 6.2]).

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

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

B4: Algebraische Zahlentheorie
Sommersemester 2021
Frau Prof. Dr. Salma Kuhlmann

26.Vorlesung

20. Juli 2021

In diesem Skript werden wir die erste Ungleichung für Satz 25.1 zeigen (siehe Korollar 26.6). Dafür werden wir einige technische Lemmata beweisen und die Hilfsabbildung λ einführen. Wir werden, oft stillschweigend, die Ergebnisse vom Kapitel 6 aufrufen.

Ansatz und Notation wie im Skript 25. Für den Beweis von D.E.S brauchen wir zwei Schlüßelergebnisse. Lemma 26.1 ist eine Verallgemeinerung von [Skript 2 ; Behauptung (6) S. 3].

Lemma 26.1
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. „$\Rightarrow$“

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

„$\Leftarrow$“ 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 26.2
Seien $m, M \in \mathbb{N}$ fest. Es ist: Die Menge der ganzen komplexen algebraischen Zahlen

$$A_{m,M} = \{\alpha \in \mathcal{O}_{\mathbb{C}} \mid \deg \ \mathrm{MinPol}_{\mathbb{Z}}(\alpha) \leq m \text{ und } |\alpha'| \leq M \text{ für alle konjugierte } \alpha' \text{ zu } \alpha\}$$

ist endlich.

Beweis. Sei $\alpha \in A_{m,M}$ (d.h. für alle Nullstellen α' von $\mathrm{MinPol}_{\mathbb{Z}}(\alpha)$ gilt $|\alpha'| \leq M$).

• Es genügt zu zeigen: für $\alpha \in A_{m,M}$ gibt es nur endlich viele normierte irreduzible Polynome in $\mathbb{Z}[x]$, die als $\mathrm{MinPol}_{\mathbb{Z}}(\alpha)$ fungieren können.

• Wir behaupten: die Koeffiziente von $\mathrm{MinPol}_{\mathbb{Z}}(\alpha)$ sind auch beschränkt, d.h $\exists M_m \in \mathbb{N}$, so daß alle Koeffiziente von $\mathrm{MinPol}_{\mathbb{Z}}(\alpha)$ im Absolutbetrag $< M_m$ sind.

• *Beweis der Behauptung:* die Behauptung gilt weil einerseits sind die Koeffiziente elementare symmetrische Funktionen in den Nullstellen (ÜB), und andererseits sind die Nullstellen im Absolutbetrag $\leq M$ per Annahme. Genauer erklärt, sei

$$\mathrm{MinPol}_{\mathbb{Z}}(\alpha) = x^m + z_{m-1}x^{m-1} + \cdots + z_0, z_i \in \mathbb{Z} \text{ mit Nullstellen } \alpha_1, \ldots, \alpha_m \, .$$

Wir berechnen

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

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

$\vdots$

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

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

Korollar 26.3
Sei $\alpha \in \mathbb{C}$ eine ganze algebraische Zahl, so daß $|\alpha'| = 1$ für alle konjugierte α' zu α. Dann ist α ist eine Einheitswurzel, d.h. es gibt $\mu \in \mathbb{N}$, so daß $\alpha^\mu = 1$.

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

Bemerkung 25.1 (iii) können wir hier nochmal direkt zeigen:

Korollar 26.4
$\mu(L) = (\mathcal{O}_L^\times)_{\mathrm{tor}}$ ist endlich.

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

Für den Beweis von D.E.S brauchen wir außerdem noch diese „Hilfsabbildung“ λ (Ansatz weiterhin wie im Skript 22 - 24):

$$\lambda : L^\times \to \mathbb{R}^{s+t} \,;\, \alpha \mapsto (\log|\sigma_1(\alpha)|, \dots \log|\sigma_s(\alpha)|, \log|\sigma_{s+1}(\alpha)|, \log|\sigma_{s+2}(\alpha)|, \dots, \log|\sigma_{s+t}(\alpha)|)$$

- λ ist ein Homomorphismus von der multiplikativen Gruppe $L^\times$ auf die additive Gruppe $\mathbb{R}^s \times \mathbb{R}^t$.
- Bemerke, daß

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

- umgekehrt: 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 diese Untermenge von $\mathbb{R}^s \times \mathbb{R}^t$:

$$H := \{x \in \mathbb{R}^s \times \mathbb{R}^t \mid \sum_{i=1}^{s} x_i + 2\sum_{j=1}^{t} x_{s+j} = 0\} \,.$$

Also ist H der Lösungsraum von einem homogenen Gleichungssystem mit einer Gleichung und in $s+t$ Unbekannten, H ist ein Unterraum der Dimension $s+t-1$.

- Mit dieser Notation gilt: $\mathcal{O}_L^\times = \{\alpha \in \mathcal{O}_L \mid \lambda(\alpha) \in H\}$.

Proposition 26.5
$\lambda(\mathcal{O}_L^\times)$ ist ein Gitter in $\mathbb{R}^{s+t}$

Beweis. Wir zeigen: $\lambda(\mathcal{O}_L^\times)$ ist diskret. Dafür genügt es zu zeigen, dass:

$$\forall c \in \mathbb{R}_+ \; \exists \text{ nur endlich viele } \alpha \in \mathcal{O}_L^\times \text{ wofür gilt } |\log|\sigma_l(\alpha)|| \leq c \quad \forall l = 1, \ldots, s+t\,.$$

Nun ist

$$\log|\sigma_l(\alpha)| \leq c \Leftrightarrow |\sigma_l(\alpha)| \leq \exp c\,.$$

Also

$$\alpha \in \mathcal{O}_L^\times \text{ mit } |\log|\sigma_l(\alpha)|| \leq c \quad \forall l = 1, \ldots, s+t \Rightarrow \alpha \in A_{n,\lceil \exp c \rceil}\,.$$

Aber $A_{n,\lceil \exp c \rceil}$ ist eine endliche Menge wegen Prop.26.2.

□

Korollar 26.6
$\mathcal{O}_L^\times$ 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:

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

Es folgt (Korollar 26.3 und 26.4) daß $\ker\lambda = \mu(L)$ eine endliche Gruppe ist.
Zusammenfassend:

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

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.

B4: Algebraische Zahlentheorie
Sommersemester 2021
Frau Prof. Dr. Salma Kuhlmann

27.Vorlesung

22. Juli 2021

Fortsetzung vom Skript 26. Um D.E.S. müssen wir nur noch zeigen daß:

$$\lambda(\mathcal{O}_L^\times) \subseteq H \text{ ein vollständiges Gitter ist.}$$

Es genügt dafür zu finden,

$$(*) \qquad \epsilon_1, \ldots, \epsilon_{s+t-1} \in \mathcal{O}_L^\times \text{ so daß } \{\lambda(\epsilon_1), \ldots, \lambda(\epsilon_{s+t-1})\} \qquad \mathbb{R}- \text{ linear unabhängig ist.}$$

Diese letzte Vorlesung hat als Hauptziel, die folgende Proposition 27.1 zu beweisen und daraus schließlich $(*)$ zu folgern.

Ansatz und Notationen wie in den 20-26 Vorlesungen. Wir werden, oft stillschweigend, die bisherige Ergebnisse aufrufen.

Proposition 27.1
$\exists \epsilon_1, \ldots, \epsilon_{s+t-1} \in \mathcal{O}_L^\times$, so daß $|\sigma_l(\epsilon_k)| < 1$ für alle $l \neq k, l = 1, \ldots, s+t, k = 1, \ldots, s+t-1$.

Für den Beweis brauchen wir eine Vorbereitung:

Bemerkung 27.1

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

2. Wir führen eine vorübergehende Terminologie ein.
   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 $N_{L/\mathbb{Q}}(\alpha) = N(\sigma(\alpha)) \quad \forall \alpha \in L$ (ÜA), dies begründet die Terminologie "Norm von x".

3. Unsere **Hauptbehauptung** nun ist:

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

4. Bemerke, daß **Hauptbehauptung** $\Rightarrow$ Proposition 27.1:

Beweis. für jedes $k = 1, \dots, s+t-1$ 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 erwünscht. □

Wir bemühen uns nun darum, die **Hauptbehauptung** zu beweisen. Wir wollen und werden dafür Minkowski's Satz anwenden. Dies benötigt einige technische Berechnungen.

• Da $\mathcal{O}_L \trianglelefteq \mathcal{O}_L$ ist, wissen wir, daß $\sigma(\mathcal{O}_L)$ ein vollständiges Gitter in $L_{\mathbb{R}}$ ist , also daß $x\sigma(\mathcal{O}_L)$ ein vollständiges Gitter für $x = (1, \dots, 1) \in L_{\mathbb{R}}$ ist. Allgemeiner für $x \in L_{\mathbb{R}}$ mit $N(x) \neq 0$, werden nun zeigen, daß $x\sigma(\mathcal{O}_L)$ ein vollständiges Gitter in $L_{\mathbb{R}}$ ist.

• Sei $\{\alpha_1, \dots, \alpha_n\}$ eine $\mathbb{Z}$-Basis für $\mathcal{O}_L$. Also ist $\{\sigma(\alpha_1), \dots, \sigma(\alpha_n)\}$ $\mathbb{R}$-linear unabhängig und

$$x\sigma(\mathcal{O}_L) = x\sigma(\alpha_1)\mathbb{Z} \oplus \cdots \oplus x\sigma(\alpha_n)\mathbb{Z}\,.$$

Wir behaupten: $\{x\sigma(\alpha_1), \dots, x\sigma(\alpha_n)\}$ ist $\mathbb{R}$-linear unabhängig. Dafür betrachten wir die Determinante der Matrix

$$A = \begin{pmatrix} x\sigma(\alpha_1) \\ \vdots \\ x\sigma(\alpha_n) \end{pmatrix} \in \mathrm{Mat}_{n\times n}(\mathbb{R})$$

Übliche Berechnungen ergeben, daß

$$|\det(A)| = 2^{-t}|\det \chi|$$

wobei χ die Matrix mit i-te Zeile gleich

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

ist (ÜA).

• Wir müssen 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 üblich

$$\mathcal{V}_{ij} = \sigma_i(\alpha_j)\,; \forall i, j = 1, \cdots, n\,.$$

Wir berechnen wie üblich

$$0 \neq |\det(A)| = 2^{-t}|N(x)|\sqrt{|D(\mathcal{O}_L/\mathbb{Z})|}$$

Also ist $x\sigma(\mathcal{O}_L)$ ein vollständiges Gitter, setze $T_x :=$ f.P von $x\sigma(\mathcal{O}_L)$. Wir berechnen wie üblich:

$$v(T_x) = |\det A| = 2^{-t}|N(x)|\sqrt{|D(\mathcal{O}_L/\mathbb{Z})|}\,.$$

(ÜA).

• Insbesondere wenn $\frac{1}{2} \leq |N(x)| \leq 1$, dann gilt, **unabhängig von** x, daß

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

- 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's Satz und $(**)$ ergeben (Minkowski's Satz für das Gitter $x\sigma(\mathcal{O}_L)$ und die Menge X anwenden):

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

- Betrachte nun

$$\mathcal{I} := \{\alpha\mathcal{O}_L \trianglelefteq \mathcal{O}_L \mid \exists x \in L_{\mathbb{R}}, \frac{1}{2} \leq |N(x)| \leq 1 \text{ und } x\sigma(\alpha) \in X\}$$

  Bemerke daß $\mathcal{I}$ 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:

$$\forall x \in L_{\mathbb{R}} \text{ mit } \frac{1}{2} \leq |N(x)| \leq 1, \exists \epsilon \in \mathcal{O}_L^{\times}, \text{ so daß } x\sigma(\epsilon) \in \bigcup_{k=1}^{m} \sigma(\beta_k^{-1})X \, .$$

- 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. $\square$(Hauptbehauptung)

$\square$(Proposition 27.1).

Wir können nun schon Aufgrund von Proposition 27.1 den Beweis für D.E.S beenden: Seien $\epsilon_1, \ldots, \epsilon_{s+t-1}$ wie in Proposition 27.1. Wir zeigen:

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

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 $k \neq l$

(weil $|\sigma_l(\epsilon_k)| < 1 \Rightarrow \log|\sigma_l(\epsilon_k)| < 0$.)

(ii) $\sum_l A'_{kl} > 0$

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

Zuletzt ist zu prüfen daß:

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.