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

18.Vorlesung

6 Juli 2017

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

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

Beweis. „$\Rightarrow$“

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

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

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

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

Wir beweisen nun die Hilfslemmata.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

□

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

19