Algebraische Zahlentheorie
– Kuhlmann –
SS 2013

18. Vorlesung am 24.06.2013

• Erinnerung: in 17. Vor Satz 2 wurde gezeigt: R Dedekind $\Leftrightarrow$ jedes $\neq 0$ gebr. Id. ist invert.

Satz 1. Sei R Integritätsbereich.
Dann ist R Dedekindring $\Leftrightarrow$ R erfüllt:

1) R ist noethersch
2) jedes echtes Primideal ist maximal
3) R ist ganz abgeschlossen.

Beweis. "$\Rightarrow$" 1) folgt aus Kor 2 17. Vor. und Lemma 3 16. Vor.
2) folgt aus Satz 1 17. Vor
3) setze $K := \mathrm{Quot}(R)$; sei $a \in K$ und $f(x) \in R[x]$ normiert mit $f(a) = 0$, $\deg f = n$.

setze $M := R + Ra + \dots + Ra^{n-1}$;
schreibe $a = b/c$ $\quad b, c \in R$.
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

Setze $I^* := (R : I)$ für I gebrochenes Ideal

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

Betrachte das (ganze) Ideal $I^* I$. Es gelten:

$I I^* (I I^*)^* \subseteq R$ also $I(I^* (I I^*)^*) \subseteq R$

also $I^* (I I^*)^* \subseteq I^*$ per Definition von I^*.

Setze $S := \{ x \in K \mid x I^* \subseteq I^* \}$

Es ist: $S \subseteq R$ (siehe Hilfslemma 3 hier weiter unten).

Wir bekommen also:

$$(I I^*)^* \subseteq S \subseteq R.$$

Wenn $I I^* = R$ ist I invertierbar und wir sind fertig, sonst ist $I I^* \underset{\neq}{\triangleleft} R$ aber dann ist (wegen Hilfslemma 4 hier weiter unten) $(I I^*)^* \underset{\neq}{\supseteq} R$. Widerspruch. $\blacksquare$

Wir beweisen nun die Hilfslemmata.

<u>Hilfslemma 1:</u> Ein gebrochenes Ideal von einem noetherschem Integritätsbereich R ist ein endl. erz. R-Modul

<u>Beweis.</u> Setze $I = \frac{1}{d} I'$ wobei $d \in R$, $d \neq 0$ und $I' \triangleleft R$

R noethersch $\Rightarrow$ I' endl. erz mit Erzeugende menge $\{x_1, \ldots, x_t\}$

dann ist offensichtlich $\{ x_1/d, \dots, x_r/d \}$ Erzeugend für I. $\blacksquare$

<u>Hilfslemma 2.</u> Ein $0 \neq$ Ideal in einem noetherschem Ring enthält ein Produkt von $\neq 0$ Primidealen.

<u>Beweis.</u> Sonst ist die Menge der $0 \neq$ 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 $I_2 \supsetneq I$ (e.g. $\exists\, a, b \in R$ 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. Widerspricht die Wahl von I. $\blacksquare$

Hilfslemma 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. Sei $x \in S$. Wegen Hilfslemma 1 ist I endl. erz. R-Modul. Aus $xI \subseteq I$ und Prop 1.9. Vor 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 $R = S$. $\boxed{}$

Hilfslemma 4. Sei R ein noetherscher Integritätsbereich so daß: jedes $0 \neq$ Primideal Maximalideal ist.

Sei $I \underset{\neq}{\triangleleft} R$. Dann ist $I^* \underset{\neq}{\supset} R$.

Bemerkung: Da $I \triangleleft R$ 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 2 liefert $aR \supseteq P_1 \dots P_m$ $\quad P_i \neq 0$

P_i Primideale; sei m minimal.

Sei $P \supseteq I$ Maximalideal so

$$P \supseteq I \supseteq aR \supseteq \prod_{i=1}^{m} P_i$$

Da beide P und P_i Primideale sind folgt aus

unsere Annahme daß $P = P_i$ für geeignetes i

(P Primideal und $P \supseteq \prod P_i \Rightarrow \exists i$ s.d. $P \supseteq P_i$,

aber P_i Maximalideal $\Rightarrow P = P_i$).

Also OE ist $P = P_1$

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 $aR \not\supseteq P_2 \cdots P_m$

per Minimalität von m, wähle $b \in \prod_{i=2}^{m} P_i$, aber $b \notin aR$,

und setze $c := a^{-1} b$. Dann ist $\boxed{c \notin R}$

und $cI \subseteq cP = a^{-1} b P \subseteq a^{-1} P \prod_{i=2}^{m} P_i$

$\subseteq a^{-1}(aR) = R$. Wir haben gezeigt: $\boxed{c \in I^*}$,

also $I^* \supsetneq R$. ☒

Satz 2. Sei R ein Dedekindbereich, $K = \mathrm{Quot}(R)$ $L|K$ endl. separable Erweiterung. Dann ist $\overline{R}^L$ ein Dedekindbereich.

Bemerkung: Wir zeigen daß $\overline{R}^L$ 1) + 2) + 3) von Satz 1.

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

Satz 13. Vor. $\Rightarrow$ $M \subseteq \overline{R}^L \subseteq M'$ also ist $\overline{R}^L$ enthalten in einem endl. erz. R-Modul M', und da R noethersch ist, folgt (aus Kor 3 8. Vor.) daß M' ist ein noethersche R-Modul.

D.h: $\overline{R}^L$ ist Untermodul eines noetherschen R-Modul. Es folgt: jedes Ideal in $\overline{R}^L$ ist endl. erz. als R-Modul (und a fortiori als $\overline{R}^L$-Modul) d.h $\overline{R}^L$ ist noethersch.

2) $\overline{R}^L$ ist ganz abgeschlossen: (Kor 2 10. Vor.).

3) Jedes $0 \neq$ Primideal von $\overline{R}^L$ ist Maximalideal:

Sei $0 \neq \mathfrak{q}$ Primideal, $\beta \neq 0$, $\beta \in \mathfrak{q}$, β ganz über R

$\exists\, a_i \in R$ s.d. $\beta^n + a_1\beta^{n-1} + \dots + a_n = 0$ 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

so $\mathfrak{p}$ Maximalideal in R, so $R/\mathfrak{p}$ ist Körper.

Nun ist $\overline{R}^L/\mathfrak{q}$ Integritätsbereich und die

Einbettung

$$R/\mathfrak{p} \xhookrightarrow{\sim} \overline{R}^L/\mathfrak{q}$$

$$a+\mathfrak{p} \longmapsto a+\mathfrak{q}$$

liefert: $R/\mathfrak{p}$ ist (isomorph zu) 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 ~~das~~ nächste **Hilfslemma**

daß $\overline{R}^L/\mathfrak{q}$ ein Körper ist, $\mathfrak{q}$ ist maximal. ∎

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