Bewertungsringe, Dedekindringe, diskrete Bewertungen und gebrochene Ideale

Markus Kirschmer

21. Dezember 2004

Nakayamas Lemma *Es sei R ein Ring und M ein endlich erzeugter R-Modul. Ist $\mathfrak{b} \subseteq \mathrm{Jac}(R) := \bigcap_{\mathfrak{m} \lhd_{max} R} \mathfrak{m}$ ein Ideal in R mit $\mathfrak{b}M = M$, dann folgt $M = \{0\}$.*

Beweis: Wir nehmen $M \neq \{0\}$ an. Ferner sei $M = \langle x_1, \ldots, x_r \rangle_R$ mit minimalem r. Dann ist $x_r = \sum_{i=1}^{r} b_i x_i$ mit $b_i \in \mathfrak{b}$. Daraus folgt $(1 - b_r)x_r = \sum_{i=1}^{r-1} b_i x_i$. Wäre $(1 - b_r) \notin R^*$, so würde ein maximales Ideal $\mathfrak{m}$ existieren mit $1 = (1 - b_r) + b_r \in \mathfrak{m}$. Also ist $(1 - b_r) \in R^*$. Aber dann kann r nicht minimal gewesen sein. Wir erhalten einen Widerspruch. □

1 Bewertungsringe

Definition 1.1 Sei R ein Integritätsbereich und $K = \mathrm{Quot}(R)$ sein Quotientenkörper. R heißt *Bewertungsring*, falls $x \in R$ oder $x^{-1} \in R$ für alle $x \in K$ gilt.

Proposition 1.2 Ist R ein Bewertungsring, so gelten

(a) R ist ein lokaler Ring.

(b) Ist R' ein Ring mit $R \subseteq R' \subseteq K$, dann ist auch R' ein Bewertungsring.

(c) R ist ganzabgeschlossen.

Beweis:

(a) Wir starten wie immer mit $\mathfrak{m} = \{x \in R \mid x \notin R^*\}$. Es seien $r \in R \setminus \{0\}$ und $x \in \mathfrak{m} \setminus \{0\}$. Angenommen es wäre $rx \notin \mathfrak{m}$, so würde $(rx)^{-1} \in R$ auch $x^{-1} = b(bx)^{-1} \in R$ implizieren, was $x \in \mathfrak{m}$ widerspricht. Daher ist $rx \in \mathfrak{m}$.
Sind nun $x, y \in \mathfrak{m} \setminus \{0\}$, dann können wir ohne Einschränkung annehmen, daß $xy^{-1} \in R$ gilt. Damit wird $x + y = (1 + xy^{-1})y \in R\mathfrak{m} \subseteq \mathfrak{m}$.
Also ist $\mathfrak{m}$ das einzige maximale Ideal von R.

(b) Klar.

(c) $x \in K$ ganz über $B \implies x^n = \sum_{k=0}^{n-1} r_k x^k$ mit $r_k \in R$. Nehmen wir nun $x \notin R$ an, so gilt $x^{-1} \in R$. Damit folgt $x = \sum_{k=0}^{n-1} r_k x^{k+1-n} \in R$. Ein Widerspruch. □

Definition 1.3 Eine *total geordnete abelsche Gruppe* $(\Gamma, +, \geq)$ ist eine abelsche Gruppe Γ mit einer totalen Ordnung „$\geq$“, so daß $x \geq y$ stets $x + z \geq y + z$ impliziere.

Bemerkung 1.4 Ist $(\Gamma, +, \geq)$ eine total geordnete abelsche Gruppe, so gelten

$$x,\, y \geq 0,\; z > 0 \implies x + y \geq 0 \text{ und } x + z > 0. \qquad (*)$$

Definition 1.5 Es sei K ein Körper und $(\Gamma, +, \geq)$ eine total geordnete abelsche Gruppe. Eine *Bewertung* auf K ist eine Abbildung $v\colon K \to \Gamma \cup \{\infty\}$ mit

(a) $v(x) = \infty \iff x = 0$

(b) $v(xy) = v(x) + v(y)$

(c) $v(x + y) \geq \min(v(x), v(y))$

Da $v\,|_{K^*}\colon K^* \to \Gamma$ offensichtlich ein Gruppenhomomorphismus ist, bildet $v(K^*) \leq \Gamma$ eine Untergruppe von Γ, die sogenannte *Bewertungsgruppe* von v.

Proposition 1.6 (Aufgabe AM 5.31) Ist K ein Körper und v eine Bewertung auf K, so bildet $R = \{x \in K \mid v(x) \geq 0\}$ einen Bewertungring in K, $\mathfrak{m} = \{x \in K \mid v(x) > 0\}$ ist sein maximales Ideal; $R^* = \{x \in K \mid v(x) = 0\}$ bilden die Einheiten.

Beweis: Sicher ist $0 \in R$. Da $v\,|_{K^*}$ ein Gruppenhomomorphismus ist, ist $v(1) = 0$. Damit folgt sofort $0 = v(1) = v(-1) + v(-1)$, was mit $(*)$ dann $v(-1) = 0$ impliziert.
Sind $x, y \in R$, so folgt wegen $v(xy) = v(x) + v(y) \geq 0$ und $v(x + y) \geq \min(v(x), v(y)) \geq 0$, daß $-x$, xy, $x + y \in R$ sind. Damit ist R ein Ring. Ist weiter $x \in K^*$, so gilt

$$0 = v(1) = v(x) + v(x^{-1}).$$

Wegen $(*)$ können nicht $0 > v(x)$ und $0 > v(x^{-1})$ zugleich gelten. Also ist $x \in R$ oder $x^{-1} \in R$. Außerdem folgt aus dieser Gleichung $x \in R^* \iff -v(x), v(x) \geq 0 \overset{(*)}{\iff} v(x) = 0$. Da R als Bewertungsring genau ein maximales Ideal besitzt, welches aus allen Nichteinheiten besteht, ist der Beweis damit beendet. □

Proposition 1.7 (Aufgabe AM 5.30) Es sei R ein Bewertungsring, $K = \mathrm{Quot}(R)$ sein Quotientenkörper und $\Gamma := K^*/R^*$. Dann liefert $xR^* \geq yR^* :\iff xy^{-1} \in R$ eine totale Ordnung auf Γ, mit den folgenden Eigenschaften:

(a) $(\Gamma, \cdot, \geq)$ ist eine total geordnete abelsche Gruppe.

(b) $v\colon K \to \Gamma \cup \{\infty\},\; x \mapsto \begin{cases} \infty & \text{falls } x = 0 \\ xR^* & \text{sonst} \end{cases}$ ist eine Bewertung auf K.

(c) R ist der zu v gehörende Bewertungsring und $\{x \in K \mid v(x) > R^*\}$ sein maximales Ideal.

Beweis:

(a) „$\geq$“ ist offensichtlich reflexiv und wegen $xR^* = yR^* \iff xy^{-1} \in R^*$ auch wohldefiniert und symmetrisch.
Zur Transitivität: Gelten $xR^* \geq yR^*$ und $yR^* \geq zR^*$, so folgt xy^{-1}, $yz^{-1} \in R$. Also auch $xz^{-1} \in R$. Deswegen wird $xR^* \geq zR^*$.
Seien x, $y \in K$. Da R ein Bewertungring ist, gilt $xy^{-1} \in R$ oder $yx^{-1} \in R$. Mit anderen Worten, „$\geq$“ ist eine totale Ordnung.
Zum Beweis der Verträglichkeit mit der Gruppenstruktur seien $xR^* \geq yR^*$ und zR^* beliebig. Wegen $xy^{-1} \in R$ gilt dann auch $(xz^{-1})(zy^{-1}) \in R$. Anders ausgedrückt:
$xR^* \cdot zR^* = xzR^* \geq yzR^* = yR^* \cdot zR^*$. Damit ist $(\Gamma, \cdot, \geq)$ eine total geordnete abelsche Gruppe.

(b) $v(x) = \infty \iff x = 0$ ist klar. Auch $v(xy) = v(x) \cdot v(y)$ ist leicht zu erkennen. Seien nun x, $y \in K^*$. Ohne Einschränkung sei $xR^* \geq yR^*$. Dann ist $xy^{-1} \in R$ und somit $1 + xy^{-1} = (y + x)y^{-1} \in R$. Dies zeigt $v(x + y) = (x + y)R^* \geq yR^* = \min(v(x), v(y))$.

(c) $\{x \in K \mid v(x) \geq R^*\} \cup \{0\} = R$ ist klar. Mit der vorherigen Proposition folgt zu guter letzt auch die Aussage über das maximale Ideal. □

Beispiele 1.8 (Weitere Beispiele in Abschnitt 3.)

(a) Jeder Körper ist ein Bewertungsring. Er wird durch die triviale Bewertung
$v\colon K \to \mathbb{Z} \cup \{\infty\},\ x \mapsto \begin{cases} \infty & \text{falls } x = 0 \\ 0 & \text{sonst} \end{cases}$ induziert.

(b) Ist F ein Körper und $K = F(X)$. Für $f \in F[X]$ sei $w_X(f) := \max\{k \in \mathbb{N}_0 : X^k \mid f\}$. Dann liefert $v_X(\frac{f}{g}) := w_X(f) - w_X(g)$ eine Bewertung auf K mit Bewertungsring $F[X]_{(X)}$.

(c) Teil (b) liefert die Bewertung v_Y auf $\mathbb{C}(Y)$ und mit $F = \mathbb{C}(Y)$ den Bewertungsring $B_X := \mathbb{C}(Y)[X]_{(X)}$ in $K = \mathbb{C}(X, Y)$ und dazugehöriger Bewertung v_X.
Sei weiter $B := \left\{ \frac{\sum g_i X^i}{\sum h_j X^j} : g_i, h_j \in \mathbb{C}[Y],\ h_0 \neq 0,\ \frac{g_0}{h_0} \in \mathbb{C}[Y]_{(Y)} \right\} \subseteq K$. B ist sicher abgeschlossen bezüglich Multiplikation. Sind $f = \frac{\sum g_i X^i}{\sum h_j X^j}$, $f' = \frac{\sum g'_i X^i}{\sum h'_j X^j} \in B$, so ist $h_0 h'_0 \neq 0$ und $v_Y((f + f')(0, Y)) \geq \min\{v_Y(f(0, Y)), v_Y(f'(0, Y))\} \geq 0$. Damit gilt auch $f + f' \in B$. Also ist B ein Ring, der wegen $v_X(f) \geq 0$ auch B_X enthält. Sei nun $\varphi = \frac{\sum g_i X^i}{\sum h_j X^j} \in K^* \setminus B$ vollständig gekürzt. Ist $h_0 = 0$, so ist $g_0 \neq 0$. Ist $h_0 \neq 0$, so muß $\frac{g_0}{h_0} \notin \mathbb{C}[Y]_{(Y)}$ gelten. Damit ist $\frac{h_0}{g_0} \in \mathbb{C}[Y]_{(Y)}$. Was in beiden Fällen $\varphi^{-1} \in B$ impliziert. Damit ist B ein Bewertungsring in K. Wegen $Y^{-1} \in B_X \setminus B$ gilt $B \subsetneq B_X \subsetneq K$.

Für unser nächstes Ziel, eine Charakterisierung des ganzen Abschlusses eines Rings mittels Bewertungen zu geben, brauchen wir noch einige Ergebnisse:

Wir fixieren einen algebraisch abgeschlossenen Körper Ω sowie einen beliebigen Körper K. Weiter sei

$$\Sigma := \{(R, f) \mid R \text{ ist Teilring von } K,\ f\colon R \to \Omega \text{ ein Homomorphismus}\}.$$

Auf Σ liefert $(A_1, f_1) \leq (A_2, f_2) :\iff A_1 \subseteq A_2$ und $f_2|_{A_1} = f_1$ eine partielle Ordnung. Für eine aufsteigende Kette $\{(R_i, f_i) \mid i \in I\} \subseteq \Sigma$ setzen wir $R := \bigcup_{i \in I} R_i$ und $f\colon R \to \Omega,\ x \mapsto f_i(x)$, wobei i so gewählt sei, daß $x \in R_i$ gilt. Dies ist stets möglich und ist $x \in R_i \subseteq R_j$, so gilt $f_j(x) = f_i(x)$. Also ist $(R, f) \in \Sigma$ wohldefiniert und eine obere Schranke der Kette.
Damit können wir Zorns Lemma anwenden und erhalten ein maximales Element (B, g) von Σ.

Proposition 1.9 B ist ein lokaler Ring und $\mathfrak{m} := \ker(g)$ ist sein maximales Ideal.

Beweis: $B/\mathfrak{m} \cong g(B)$ ist Teilring von K, also Integritätsbereich. Damit ist $\mathfrak{m}$ prim.
Wir setzen nun $\overline{g}\colon B_{\mathfrak{m}} \to \Omega$ via $\overline{g}(\frac{b}{s}) = \frac{g(b)}{g(s)}$ für alle $b \in B,\ s \in B \setminus \mathfrak{m}$ und bemerken, daß $g(s) \neq 0$ gilt. Da B ein Integritätsbereich ist, ist $\overline{g}$ wohldefiniert, denn es gilt

$$\frac{a}{s} = \frac{a'}{s'} \iff as' = a's \implies g(a)g(s') = g(a')g(s) \iff \frac{g(a)}{g(s)} = \frac{g(a')}{g(s')}.$$

Fassen wir B als Teilmenge von $B_{\mathfrak{m}}$ auf, so wird g durch den Homomorphismus $\overline{g}$ fortgesetzt und daher gilt $(B,\, g) = (B_{\mathfrak{m}},\, \overline{g})$. B ist somit lokal und der Rest folgt mittels der Korrespondenz von Idealen unter Lokalisierung. □

Proposition 1.10 Für ein $x^{-1} \in K^*$ bezeichne $B[x]$ der von x erzeugte Teilring über B und $\mathfrak{m}[x] = B[x]\mathfrak{m}$. Dann gilt stets $\mathfrak{m}[x] \neq B[x]$ oder $\mathfrak{m}[x^{-1}] \neq B[x^{-1}]$.

Beweis: Angenommen, es gilt beidesmal Gleichheit, dann existieren $u_i, v_i \in \mathfrak{m}$ mit

$$(1) \qquad 1 = \sum_{i=0}^{m} u_i x^i \qquad \text{und} \qquad (2) \qquad 1 = \sum_{i=0}^{n} v_i x^{-i}$$

Ohne Einschränkung sind $m \geq n$ minimal gewählt. Multiplizieren wir Gleichung (2) mit x^n, so erhalten wir $x^n = \sum_{i=0}^{n} v_i x^{n-i}$ und daher $x^n(1 - v_0) = \sum_{i=1}^{n} v_i x^{n-i}$. Wäre $(1 - v_0) \notin B^*$, dann würde $1 = (1 - v_0) + v_0 \in \mathfrak{m}$ folgen, was nicht sein kann. Also ist $(1 - v_0) \in B^*$. Dann kann m in (1) aber nicht minimal gewesen sein. □

Satz 1.11 *Sei $(B,\, g)$ wie oben. Dann ist B ein Bewertungsring in K.*

Beweis: Sei $\mathfrak{m} = \ker(g)$ und $x \in K^*$. Ohne Einschränkung gilt $1 \notin \mathfrak{m}[x] \lhd B[x] =: B'$. Daher existiert ein maximales Ideal $\mathfrak{m}' \lhd B'$ welches $\mathfrak{m}$ umfasst. Wegen $\mathfrak{m}' \cap B \lhd B$ und $\mathfrak{m} \subseteq \mathfrak{m}' \cap B$ wird $\mathfrak{m} = \mathfrak{m}' \cap B$. Damit ist $\ker(B \hookrightarrow B' \twoheadrightarrow B'/\mathfrak{m}') = \mathfrak{m}$. Wir können also $k := B/\mathfrak{m}$ als Teilmenge von $k' := B'/\mathfrak{m}'$ auffassen. Mit $\overline{x} = x + \mathfrak{m}'$ gilt dann $k[\overline{x}] = k'$, d.h. k'/k ist eine endliche Körpererweiterung. Der Homomorphismus $\overline{g}\colon k \hookrightarrow \Omega$ aus dem Beweis von Proposition 1.9 läßt sich daher fortsetzen zu $\overline{g}\colon k' \hookrightarrow \Omega$ (Algebra I). Dies liefert einen Homomorphismus $h\colon B' \to k' \hookrightarrow \Omega$ mit $h|_B = g$. Es folgt $(B,\, g) = (B',\, h)$ und somit $x \in B$. □

Proposition 1.12 Sei R ein Teilring von K und $\overline{R}$ der ganze Abschluß von R in K. Mit $\mathfrak{B} = \{R \subseteq B \subseteq K \mid B \text{ ist ein Bewertungsring in } K\}$ gilt dann $\overline{R} = \bigcap_{B \in \mathfrak{B}} B$.

Beweis: „$\supseteq$“: Sei $B \supseteq R$ ein Bewertungsring. Dann ist B ganzabgeschlossen und somit $\overline{R} \subseteq B$.
„$\subseteq$“: Sei $x \in K \setminus \overline{R}$. Dann ist sicher $x \notin R' := R[x^{-1}]$ und deshalb gilt $x^{-1} \notin R'^*$. Also existiert ein $\mathfrak{m}' \underset{\max}{\lhd} R'$ mit $x \in \mathfrak{m}'$. Bezeichne Ω den algebraischen Abschluß von $R'/\mathfrak{m}'$ und $f\colon R' \twoheadrightarrow R'/\mathfrak{m}' \hookrightarrow \Omega$. Dann existiert eine maximale Fortsetzung $(B,\, g)$ von $(R,\, f|_R)$ und B ist ein Bewertungsring nach dem vorangegangenen Satz. Wegen $x^{-1} \in \mathfrak{m}' \subseteq \ker(g)$ folgt $x^{-1} \notin B^*$ also $x \notin B$. □

Satz 1.13 *Seien Ω ein algebraisch abgeschlossener Körper, $R \subseteq R'$ Integritätsbereiche und R' sei endlich erzeugt über R. Dann existiert zu jedem $v \in R \setminus \{0\}$ ein $u \in R \setminus \{0\}$ so daß sich jeder Homomorphismus $f\colon R \to \Omega$ mit $f(u) \neq 0$ fortsetzen läßt zu einem Homomorphismus $g\colon R' \to \Omega$ mit $g(v) \neq 0$.*

Beweis: Es genügt die Behauptung für $R' = R[x]$ zu zeigen. Wir unterscheiden nun zwei Fälle.
1. Fall: x ist transzendent über R.
Sei $v = \sum_{i=0}^{n} r_i x^i$ mit $r_n \neq 0$, dann setzen wir $u := r_n$. Sei f nun wie oben gegeben, so existiert ein $z \in \Omega^*$ mit $0 \neq \sum_{i=0}^{n} f(r_i) z^i$, da ein Polynom vom Grad n in $\Omega[T]$ nur n Nullstellen hat. Der Homomorphismus $g\colon B \to \Omega,\ \sum r'_i x^i \mapsto \sum f(r'_i) z^i$ setzt f auf B fort mit $g(u) = f(r_n) z^n \neq 0$.

2. Fall: x ist algebraisch über $\mathrm{Quot}(R)$.
Dann sind v und damit auch v^{-1} algebraisch über R. Daher existieren $r_i, \tilde{r}_i \in R$ mit
$0 = \sum_{i=0}^{m} r_m x^m,\ 0 = \sum_{i=0}^{n} \tilde{r}_i v^{-i}$ und $r_m, \tilde{r}_n \neq 0$. Sei nun $u := r_m \tilde{r}_n \neq 0$ und f wie oben gegeben. Wegen $f(u) \neq 0$ induziert $f(u^{-1}) := f(u)^{-1}$ eine Fortsetzung $f\colon R[u^{-1}] \to \Omega$. Mit Satz 1.11 läßt sich f erweitern zu $h\colon B \to \Omega$, mit einem Bewertungsring $B \supseteq R[u^{-1}]$. Wegen der Wahl von u sind x und v^{-1} ganz über $R[u^{-1}]$. Dies impliziert $R' \subseteq B$ und $v \in B^*$. Damit ist $h(v) = 0$ ausgeschlossen. $g := h|_{R'}$ besitzt somit die gewünschten Eigenschaften. □

Satz 1.14 (Hilberts Nullstellensatz) *Sei K ein Körper und A eine endlich erzeugte K-Algebra. Ist A zusätzlich ein Körper, dann ist A/K eine endliche algebraische Erweiterung.*

Beweis: Bezeichne $\overline{K}$ den algebraischen Abschluß von K. Nach dem vorangegangenen Satz läßt sich (mit $v = 1$) die Einbettung $f\colon K \hookrightarrow \overline{K}$ fortsetzen zu einem Homomorphismus $g\colon A \to \overline{K}$. Da A einfach ist, ist g injektiv. □

2 Dedekindringe

Definition 2.1 Eine *Dedekindring* ist ein ganzabgeschlossener, noetherscher Integritätsbereich, in dem jedes von (0) verschiedene Primideal maximal ist.

Satz 2.2 *Jedes von* (0) *verschiedene Ideal eines Dedekindrings ist ein endliches Produkt von Primidealen und die Darstellung ist eindeutig bis auf Anordnung der Faktoren.*

Zum Beweis dieses wichtigen Satzes benötigen wir zwei Lemmata.

Lemma 2.3 *Es sei R ein Dedekindring und $(0) \neq \mathfrak{a} \trianglelefteq R$. Dann existieren maximale Ideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ mit $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_n \subseteq \mathfrak{a}$.*

Beweis: Sei $\mathfrak{M} = \{(0) \neq \mathfrak{a} \trianglelefteq R \mid \mathfrak{a} \text{ verletzt die Behauptung}\}$. Ist diese Menge leer, so wäre das Lemma bewiesen. Andernfalls existiert, da R noethersch ist, ein Ideal $\mathfrak{a}$, welches in $\mathfrak{M}$ maximal ist. Sicherlich ist $\mathfrak{a}$ kein Primideal. Daher existieren $a_1,\ a_2 \in R \setminus \mathfrak{a}$ mit $a_1 a_2 \in \mathfrak{a}$.
Setzen wir nun $\mathfrak{a}_i := (a_i) + \mathfrak{a},\ (i = 1, 2)$, so gilt $\mathfrak{a} \subsetneq \mathfrak{a}_i$. Aus der Maximalität von $\mathfrak{a}$ folgt, daß $\mathfrak{a}_1$ und $\mathfrak{a}_2$ Produkte maximaler Ideale enthalten.
Wegen $\mathfrak{a}_1 \mathfrak{a}_2 \subseteq (\mathfrak{a},\ a_1\mathfrak{a},\ a_2\mathfrak{a},\ a_1 a_2) \subseteq \mathfrak{a}$ gilt dies dann aber auch für $\mathfrak{a}$. Ein Widerspruch. □

Definition 2.4 Ist R ein Dedekindring und $(0) \neq \mathfrak{a} \trianglelefteq R$ ein Ideal, dann bezeichne $\mathfrak{a}^{-1} := \{x \in K \mid x\mathfrak{a} \subseteq R\}$ das zu $\mathfrak{a}$ *inverse Ideal*. (Warum es „Ideal“ heißt, obwohl es im Allgemeinen kein Ideal von R im uns bekannten Sinne ist, wird erst später klar werden.)

Lemma 2.5 *Es sei R ein Dedekindring und $\mathfrak{p} \underset{max}{\lhd} R$ ein Primideal. Dann gilt $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1}$ für alle $(0) \neq \mathfrak{a} \trianglelefteq R$.*

Beweis: „$\subseteq$“ ist klar, da offensichtlich $1 \in \mathfrak{p}^{-1}$ liegt.
„$\neq$“: Wir zeigen die Behauptung zuerst für $\mathfrak{a} = R$:
Sei $a \in \mathfrak{p} \setminus \{0\}$ und $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \subseteq (a) \subseteq \mathfrak{p}$ mit minimalem r. Wäre $\mathfrak{p}_i \nsubseteq \mathfrak{p}$ für alle i, dann gäbe es $x_i \in \mathfrak{p}_i \setminus \mathfrak{p}$ mit $\prod_i x_i \in \mathfrak{p}$, was sicher nicht sein kann. Wir können also annehmen, daß $\mathfrak{p}_1 \subseteq \mathfrak{p}$ gilt, was wegen der Maximalität $\mathfrak{p}_1 = \mathfrak{p}$ impliziert.
Wegen der Minimalität von r ist $\mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r \nsubseteq (a)$, also existiert ein $b \in \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r$ mit $a^{-1}b \notin R$. Aber es gilt $\mathfrak{p}b \subseteq \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r \subseteq (a)$, d.h. $a^{-1}b \in \mathfrak{p}^{-1}$. Dies zeigt $\mathfrak{p}^{-1} \neq R$.

Sei nun $(0) \neq \mathfrak{a} \trianglelefteq R$ beliebig mit $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$.
Da R noethersch ist, existiert ein Erzeugendensystem $(\alpha_1, \ldots, \alpha_n)$ von $\mathfrak{a}$. Für jedes $x \in \mathfrak{p}^{-1}$ existieren dann $a_{ij} \in R$, so daß $x\alpha_i = \sum_j a_{ij}\alpha_j$ gilt.
Mit $A := xI_n - (a_{ij}) \in R^{n\times n}$ und $\alpha = (\alpha_1, \ldots, \alpha_n)^{tr}$ gilt weiter $A \cdot \alpha = 0$. Bezeichnet A^* die zu A adjungierte Matrix, so gilt $0 = A^*A\alpha = I_n \cdot \det(A)\alpha$. Da R ein Integritätsbereich ist und nicht alle $\alpha_i = 0$ sein können, folgt $\det(A) = 0$.
Also ist x eine Nullstelle von $\det(XI_n - (a_{ij})) \in R[X]$. Damit sind aber alle $x \in \mathfrak{p}^{-1}$ ganz über R. Mit $1 \in \mathfrak{p}^{-1}$ impliziert dies aber $\mathfrak{p}^{-1} = R$, was wir schon vorab ausgeschlossen haben. Daher ist das Lemma bewiesen. □

Bemerkung 2.6 Ist R ein Dedekindring und $\mathfrak{p} \underset{\max}{\lhd} R$, so gilt $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1} \subseteq R$. Aus der Maximalität von $\mathfrak{p}$ folgt $\mathfrak{p}\mathfrak{p}^{-1} = R$.

Die Bemerkung bleibt auch richtig für beliebige Ideale, wenn wir Satz 2.2 bemühen und die Tatsache, daß $(\mathfrak{p}_1\mathfrak{p}_2)^{-1} = \mathfrak{p}_1^{-1}\mathfrak{p}_2^{-1}$. Später dazu mehr.

Beweis (von Satz 2.2): Existenz: Wir setzen

$$\mathfrak{M} = \{\mathfrak{a} \trianglelefteq R \mid (0) \neq \mathfrak{a} \text{ und } \mathfrak{a} \text{ ist kein endliches Produkt von Primidealen}\}.$$

Ist die Menge leer, so ist die Existenzaussage bewiesen. Nehmen wir daher $\mathfrak{M} \neq \emptyset$ an, und wählen $\mathfrak{a}$ ein maximales Element in $\mathfrak{M}$. Dann existiert ein maximales Ideal $\mathfrak{p} \lhd R$ mit $\mathfrak{a} \subsetneq \mathfrak{p}$. Nach dem vorherigen Lemma gilt aber $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} = R$. Somit ist $\mathfrak{a}\mathfrak{p}^{-1} \notin \mathfrak{M}$, d.h. $\mathfrak{a}\mathfrak{p}^{-1}$ ist ein endliches Produkt von Primidealen. Aber dann gilt dasselbe auch für $\mathfrak{a}$. Widerspruch.

Eindeutigkeit: Definieren wir $\mathfrak{a} \mid \mathfrak{b} :\iff \mathfrak{b} \subseteq \mathfrak{a}$, so können wir dem bekannten Beweis in $\mathbb{Z}$ folgen.
Angenommen, wir hätten $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_n = \mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_m$. Dann ist $\mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_m \subseteq \mathfrak{p}_1$. Wie schon zuvor folgt $\mathfrak{q}_i \subseteq \mathfrak{p}_1$ für ein i und letztlich $\mathfrak{q}_i = \mathfrak{p}_1$.
Jetzt macht man (nach Umnummerierung) mit $\mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_n = \mathfrak{q}_2 \cdot \ldots \cdot \mathfrak{q}_m$ weiter .... □

Definition 2.7 Ein *algebraischer Zahlkörper* K ist eine endliche Körpererweiterung von $\mathbb{Q}$. Der ganze Abschluss $\mathbb{Z}_K$ von $\mathbb{Z}$ in K wird auch *Ring der ganzen Zahlen von* K genannt.

Satz 2.8 *Ist K ein algebraischer Zahlkörper, so ist $\mathbb{Z}_K$ ein Dedekindring.*

Beweis: $K/\mathbb{Q}$ ist separabel. Aus Proposition AM 5.17 folgt, daß $\mathbb{Z}_K$ ein Teilmodul eines endlich erzeugten freien $\mathbb{Z}$-Moduls ist. Da $\mathbb{Z}$ ein Hauptidealbereich ist, ist jedes Ideal von $\mathbb{Z}_K$ endlich erzeugt. Also ist $\mathbb{Z}_K$ noethersch und als ganzer Abschluss von $\mathbb{Z}$ auch ganzabgeschlossen.
Es sei nun $(0) \neq \mathfrak{p} \underset{\text{prim}}{\lhd} R$. Dann gibt es eine Primzahl p mit $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Da $p\mathbb{Z}$ maximal ist, gilt dies auch für $\mathfrak{p}$. □

Historisch gesehen waren dies die ersten Ringe, in denen die eindeutige Faktorisierung von Idealen in Primideale studiert wurde.
Ursprünglich hatte man geglaubt, *Fermats Letzten Satz* mittels den algebraischen Zahlkörpern $\mathbb{Q}[\zeta_p]$ bewiesen zu haben. Dabei sei p eine Primzahl und ζ_p eine primitive p-te Einheitswurzel. Der Beweis ruhte aber auf der Annahme, daß alle diese $\mathbb{Z}[\zeta_p]$ faktoriell (d.h. ZPE-Ringe) sind. Eduard Kummer erkannte diesen Fehler und konnte, indem er zu Idealen überging, den Beweis für eine große Klasse von Primzahlen retten, welche er *regulär* nannte.

3 Diskrete Bewertungen

Definition 3.1 Es sei K ein Körper. Eine Abbildung $v\colon K \to \mathbb{Z} \cup \{\infty\}$ heißt *diskrete Bewertung*, falls folgende Bedingungen erfüllt sind:

(a) $v(x) = \infty \iff x = 0$

(b) $v(xy) = v(x) + v(y)$

(c) $v(x + y) \geq \min(v(x), v(y))$

(d) v ist surjektiv.

$R = \{x \in K \mid v(x) \geq 0\}$ ist der *Bewertungsring* von v und ein Ring A heißt *diskreter Bewertungsring*, falls es eine diskrete Bewertung auf $\mathrm{Quot}(A)$ gibt, die A als ihren Bewertungsring besitzt.

Beispiele 3.2 (Eine Verallgemeinerung der Beispiele (a) und (b) liefert Korollar 4.7.)

(a) v_X und v_Y in Beispiel 1.8 waren diskret.

(b) Der Fundamentalsatz der Arithmetik liefert eine eindeutige Faktorisierung

$$\mathbb{Z}n = \prod_{p \in \mathbb{P}} \mathbb{Z}p^{w_p(n)} \qquad \text{mit } w_p(n) \in \mathbb{N}_0 \text{ und } w_p(n) \neq 0 \text{ nur endlich oft.}$$

wobei $\mathbb{P}$ die Menge aller Primzahlen bezeichne. Für jede Primzahl p liefert die Abbildung

$$v_p\colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}, \frac{n}{m} \mapsto \begin{cases} \infty & \text{falls } \frac{n}{m} = 0 \\ w_p(n) - w_p(m) & \text{sonst} \end{cases}$$

eine diskrete Bewertung auf $\mathbb{Q}$. Wir beweisen Eigenschaft (c):

$$\begin{aligned} v\left(\frac{n}{m}+\frac{n'}{m'}\right) &= w(nm'+n'm)-w(mm') \\ &\overset{(*)}{\geq} \min\{w(nm'),\, w(n'm)\}-w(mm') \\ &= \min\{w(nm')-w(mm'),\, w(n'm)-w(mm')\} \\ &= \min\left\{v\left(\frac{n}{m}\right),\, \left(\frac{n'}{m'}\right)\right\} \end{aligned}$$

$(*)$ ist richtig, da $p^k \mid a$ und $p^l \mid b$ impliziert $p^{\min(k,l)} \mid a+b$.

(c) $v\colon \mathbb{C}(X) \to \mathbb{Z}, \frac{f}{g} \mapsto \deg(g)-\deg(f)$ induziert ebenfalls eine diskrete Bewertung auf $\mathbb{C}(X)$. Wir zeigen (ein letzes Mal) Eigenschaft (c):

$$\begin{aligned} v\left(\frac{f}{g}+\frac{f'}{g'}\right) &= \deg(gg')-\deg(fg'+f'g) \\ &\geq \deg(gg')+\min\{-\deg(fg'),\, -\deg(f'g)\} \\ &= \min\{\deg(gg')-\deg(fg'),\, \deg(gg')-\deg(f'g)\} \\ &= \min\left\{v\left(\frac{f}{g}\right),\, v\left(\frac{f'}{g'}\right)\right\} \end{aligned}$$

Bemerkung 3.3

(a) Jede diskrete Bewertung ist eine Bewertung.

(b) Bedingung (d) ist eine Normierung. Denn ist v eine beliebige Abbildung, die die Bedingungen (a)-(c) erfüllt und nicht die triviale Bewertung ist (d.h. $v(K^*) \neq \{0\}$ vgl. Beispiel 1.8), dann ist $v(K^*) = n\mathbb{Z}$ mit $n \in \mathbb{Z}_{>0}$. Nach Reskalierung mit $\frac{1}{n}$ erhalten wir eine Abbildung, die alle obigen Bedingungen erfüllt und denselben Bewertungsring liefert.

(c) Ein *nicht-archimedischer Absolutbetrag* von K ist eine Abbildung $v'\colon K \to \mathbb{R}_{\geq 0}$ mit

(a)' $v'(x)=0 \iff x=0$

(b)' $v'(xy)=v'(x)v'(y)$

(c)' $v'(x+y) \leq \max(v'(x), v'(y))$

v' induziert dann kanonisch eine Ultrametrik auf K. Die Bedingung (c)' ist eine Verschärfung der Dreiecksungleichung. Jede diskrete Bewertung v geht via $v'(x) := \exp(-v(x))$ in einen nicht-archimedischen Absolutbetrag über und ist $v'(K^*)$ eine diskrete Teilmenge von R, so gilt auch die Umkehrung dieser Aussage.
Ist anstatt (c)' nur die Dreiecksungleichung erfüllt, so heißt v' *archimedischer Absolutbetrag*. In diesem Fall wird lediglich eine Metrik induziert.
Ein Beispiel dafür sind die Betragsabbildungen auf $\mathbb{R}$ oder $\mathbb{C}$ oder etwas allgemeiner: Ist K ein algebraischer Zahlkörper, so liefert jede Einbettung $\sigma\colon K \to \mathbb{C}$ einen archimedischen Absolutbetrag $x \mapsto |\sigma(x)|$.
In diesem Zusammenhang sollte Bedingung (c) verstanden werden.

Bemerkung 3.4 Sei R ein diskreter Bewertungsring mit Bewertung v und $\pi \in R$ eine *Uniformisierende*, d.h. $v(\pi) = 1$. Dann gelten:

(a) $R^* = \{x \in K \mid v(x) = 0\}$.

(b) Alle Ideale $\neq (0)$ sind gegeben durch $(\pi^k) \quad (k \in \mathbb{N}_0)$.

(c) R ist ein noetherscher, ganzabgeschlossener lokaler Hauptidealbereich mit maximalem Ideal $\mathfrak{m} := (\pi)$.

(d) Jedes $x \in R \setminus \{0\}$ besitzt eine eindeutige Faktorisierung $x = \pi^k u$ mit $k \in \mathbb{N}_0$ und $u \in R^*$.

Beweis:

(a) Dies gilt für jede Bewertung.

(b) Sei $(0) \neq \mathfrak{a} \trianglelefteq R$ und $x \in \mathfrak{a}$ ein Element mit minimaler Bewertung. Ist $v(x) = k$, so gilt $v(\pi^k x^{-1}) = 0$. Also ist $\pi^k x^{-1} \in R^*$, was $(\pi^k) = (x) \subseteq \mathfrak{a}$ impliziert.
Ist umgekehrt $y \in \mathfrak{a}$, so gilt $k \leq v(y) = v(x(x^{-1}y)) = k + v(x^{-1}y)$. Damit ist $v(x^{-1}y) \geq 0$ und somit $x^{-1}y \in R$. Zusammen folgt $\mathfrak{a} = (x) = (\pi^k)$.

(c) Folgt aus (b) und den Eigenschaften von Bewertungsringen.

(d) Sei $x \in R\setminus\{0\}$. Dann ist $(x) = (\pi^k)$ für ein $k \in \mathbb{N}_0$. Dies ist die Existenz. Die Eindeutigkeit ist klar, denn sind $\pi^k u = \pi^{k'} u'$ mit $k \geq k'$, so folgt $\pi^{k-k'} \in R^*$ und damit $k = k'$. Nun muß auch $u = u'$ gelten, da R ein Integritätsbereich ist. □

Satz 3.5 *Es sei R ein Ring, der aber kein Körper ist. Dann sind folgende Aussagen äquivalent.*

(a) R ist diskreter Bewertungsring.

(b) R ist Hauptidealbereich mit genau einem Primideal.

(c) R ist ein lokaler Hauptidealbereich.

(d) R ist ein noetherscher, lokaler Integritätsbereich und das maximale Ideal ist Hauptideal.

(e) R ist Integritätsbereich und es existiert ein $\pi \in R$, so daß jedes $x \in R\setminus\{0\}$ eine eindeutige Faktorisierung $x = \pi^k u$ mit $k \in \mathbb{N}_0$ und $u \in R^*$ besitzt.

(f) R ist lokaler Integritätsbereich und das maximale Ideal $\mathfrak{m}$ ist Hauptideal mit $\bigcap_{k=0}^{\infty} \mathfrak{m}^k = (0)$.

(g) R ist lokaler Dedekindring

(h) R ist lokaler noetherscher Integritätsbereich und $\mathfrak{m}$ sein maximales Ideal. Weiter bilden $\mathfrak{m}^k$ $(k \in \mathbb{N}_0)$ alle von (0) verschiedenen R-Ideale.

(i) R ist noetherscher Bewertungsring.

Beweis: Aus Bem. 3.4 folgen $(a) \Longrightarrow (b)$ und $(a) \Longrightarrow (g)$. Auch $(b) \Longrightarrow (c) \Longrightarrow (d)$ ist klar.
$(d) \Longrightarrow (e)$ Sei (π) das maximale Ideal. Ist $x \in R \setminus \{0\}$, so setze $k := \max\{k \in \mathbb{N}_0 : x \in \pi^k\}$. Ist $k = \infty$, so wäre $x = r_1\pi = r_2\pi^2 = \ldots$, also $(r_i) = (r_{i+1}\pi) \subseteq (r_{i+1})$ für alle i. Da R noethersch ist, muß diese Kette stationär werden, sagen wir bei (r_l). Wegen $r_{l+1} = r \cdot r_l = r \cdot \pi \cdot r_{l+1}$ für ein $r \in R$ folgt $1 = r \cdot \pi$ und somit $\pi \in R^*$ was Nonsens ist. Damit ist k endlich. Die Eindeutigkeit zeigt man wie in Bemerkung 3.4.

$(e) \Longrightarrow (a)$ R ist Bewertungsring der diskreten Bewertung $\frac{\pi^k u}{\pi^l u'} \mapsto k-l \quad (k,\, l \in \mathbb{N}_0,\ u,\, u' \in R^*)$.

$(e) \Longrightarrow (f)$ Offensichtlich besteht $\mathfrak{m} := (\pi)$ gerade aus allen Nichteinheiten von R und ist somit das einzige maximale Ideal. Wegen $\pi^k u \notin \mathfrak{m}^{k+1}$ ist $\bigcap_{k=0}^{\infty} \mathfrak{m}^k = (0)$.

$(f) \Longrightarrow (e)$ Sei $\mathfrak{m} = (\pi)$ das maximale Ideal. Für ein $x \in R$ sei $k := \max\{l \in \mathbb{N}_0 \mid x \in (\pi^l)\}$. Nach Voraussetzung ist k endlich und liefert $x = \pi^k u$ mit einer Einheit u.

$(g) \Longrightarrow (h)$ Klar, denn (0) ist nicht maximal und jedes Ideal $\neq (0)$ ist ein eindeutiges Produkt von Primidealen.

$(h) \Longrightarrow (i)$ Angenommen, es gäbe ein $k \in \mathbb{N}$ mit $\mathfrak{m}^k = \mathfrak{m}^{k+1}$, so wäre $\mathfrak{m}^k = (0)$ nach Nakayama. Ist nun $x \in \mathfrak{m}$, so folgt $x^k \in \mathfrak{m}^k = (0)$. Da R ein Integritätsbereich ist, folgt $x = 0$. Also ist $\mathfrak{m} = (0)$. Dies ist aber unmöglich, da R ja kein Körper sein sollte. Zu jedem $x \in R$ existiert daher genau ein $w(x) \in \mathbb{N}_0$ mit $(x) = \mathfrak{m}^{w(x)}$. $\frac{x}{y} \mapsto w(x) - w(y)$ liefert eine (diskrete) Bewertung auf K mit Bewertungsring R.

$(i) \Longrightarrow (d)$ Sei $\mathfrak{m}$ das maximale Ideal von R. Dieses ist endlich erzeugt, sagen wir $\mathfrak{m} = (x_1, \ldots, x_r)$ mit r minimal. Wäre $r > 1$, so gilt $x_1 x_2^{-1} \in R$ oder $x_2 x_1^{-1} \in R$. Also war r nicht minimal. □

Satz 3.6 *Es sei R ein noetherscher Integritätsbereich (aber kein Körper), in dem jedes Primideal maximal ist. Äquivalent sind:*

(a) R ist ganzabgeschlossen (also ein Dedekindring).

(b) $R_\mathfrak{p}$ ist ein diskreter Bewertungsring für alle $\mathfrak{p} \underset{max}{\lhd} R$.

Beweis: „$\Longrightarrow$“ $R_\mathfrak{p}$ ist ein lokaler Dedekindring, also ein diskreter Bewertungsring nach dem vorherigen Satz.
„$\Longleftarrow$“ R ist nach Proposition AM 5.13 ganzabgeschlossen, da dies lokalisiert an allen maximalen Idealen gilt. □

4 Gebrochene Ideale

Definition 4.1 Es sei R ein Integritätsbereich und $K = \mathrm{Quot}(R)$. Ein R-Untermodul I von K heißt *gebrochenes Ideal* von R, falls es ein $c \in R$ gibt mit $cI \subseteq R$.
Weiter sei dann $I^{-1} := \{x \in K \mid xI \subseteq R\}$.

Jeder endlich erzeugte R-Teilmodul von K ist ein gebrochenes Ideal. (Wegen der Existenz von „Hauptnennern“.) Ist umgekehrt R noethersch, so ist jedes gebrochene Ideal I endlich erzeugt und es existiert ein $c \in R$ sowie ein $\mathfrak{a} \trianglelefteq R$ mit $I = c^{-1}\mathfrak{a}$.

Definition 4.2 Es sei R ein Integritätsbereich und $K = \mathrm{Quot}(R)$. Ein R-Untermodul I von K heißt *invertierbar*, falls es einen R-Untermodul J von K gibt mit $IJ = R$.

Ist I invertierbar und J ein R-Teilmodul von K mit $IJ = R$, so gilt sicher $J \subseteq I^{-1}$. Umgekehrt folgt $I^{-1} = (I^{-1}I)J \subseteq J$. Also ist $J = I^{-1}$. D.h. Inverse sind eindeutig bestimmt.
Weiter ist dann $1 = \sum_{i=1}^{n} x_i y_i$ mit $x_i \in I^{-1},\ y_i \in I$. Damit ist $x = \sum (x_i x) y_i \in (I^{-1}I)I = R \cdot I$ für jedes $x \in I$. Insbesondere ist I (und auch I^{-1}) endlich erzeugt. Dies erklärt warum wir I^{-1} in Definition 2.4 als inverses Ideal bezeichnet haben.

Zum Beispiel hat jedes Hauptideal $(0) \neq (x) := xR$ gerade (x^{-1}) als sein Inverses.

Weiter wird nun für invertierbare Moduln die Rechenregel $(I_1 I_2)^{-1} = I_1^{-1} I_2^{-1}$ klar.

Proposition 4.3 Die Menge der invertierbaren gebrochenen Ideale bilden mit der Idealmultiplikation eine abelsche Gruppe. Darin ist R das neutrale Element und zu jedem Ideal I ist I^{-1} das eindeutig bestimmte Inverse.

Proposition 4.4 Es sei R ein Integritätsbereich, $K = \mathrm{Quot}(R)$ und I ein gebrochenes Ideal. Dann sind äquivalent:

(a) I ist invertierbar.

(b) I ist endlich erzeugt und $I_\mathfrak{p}$ ist invertierbar für jedes $(0) \neq \mathfrak{p} \underset{\text{prim}}{\lhd} R$.

(c) I ist endlich erzeugt und $I_\mathfrak{m}$ ist invertierbar für jedes $\mathfrak{m} \underset{\max}{\lhd} R$.

Beweis:
$(a) \Longrightarrow (b)$ Wir wissen schon, daß I endlich erzeugt ist. Weiter folgt aus $I^{-1}I = R$ natürlich $(I^{-1})_\mathfrak{p} I_\mathfrak{p} = R_\mathfrak{p}$ da die Lokalisation mit der Multiplikation verträglich ist.

$(b) \Longrightarrow (c)$ Ist klar.

$(c) \Longrightarrow (a)$ Sei $\mathfrak{m} \underset{\max}{\lhd} R$ und $I = \langle x_1, \ldots, x_r \rangle_R$. Damit gilt auch $I_\mathfrak{m} = \langle x_1, \ldots, x_r \rangle_{R_\mathfrak{m}}$. Wir zeigen zunächst $(I^{-1})_\mathfrak{m} \supseteq (I_\mathfrak{m})^{-1}$:
Sei $x \in (I_\mathfrak{m})^{-1}$, dann ist $x x_i = \frac{r_i}{s_i}$ mit $r_i \in R$ und $s_i \in R \setminus \mathfrak{m}$. Setzen wir $s := \prod_i s_i$, so gilt $s x x_i \in R$ und somit $sx \in I^{-1}$. Wegen $s \in R \setminus \mathfrak{m}$ folgt hiermit $x = \frac{sx}{s} \in (I^{-1})_\mathfrak{m}$. Damit ist die Behauptung bewiesen.
Nun zum eigentlichen Beweis: Setze $\mathfrak{a} := I^{-1}I \subseteq R$. Dies ist ein ganzes Ideal in R. Dann gilt aber $\mathfrak{a}_\mathfrak{m} = (I^{-1})_\mathfrak{m} I_\mathfrak{m} \supseteq (I_\mathfrak{m})^{-1} I_\mathfrak{m} = R_\mathfrak{m}$ für jedes maximale Ideal $\mathfrak{m}$. Damit ist $\mathfrak{a} = R$, da $\mathfrak{a}$ in keinem maximalen Ideal enthalten sein kann. □

Proposition 4.5 Sei R ein lokaler Integritätsbereich. R ist ein diskreter Bewertungsring genau dann, wenn alle gebrochenen Ideale $\neq (0)$ invertierbar sind.

Beweis: „$\Longrightarrow$“ Sei π eine Uniformisierende und I ein gebrochenes Ideal von R. Weiter sei $c \in R$ so, daß $cI \subseteq R$ ein ganzes Ideal ist. Dann ist $cI = (\pi)^k$ und $(c) = (\pi)^l$ für $k, l \in \mathbb{N}_0$. Dies impliziert $R = (\pi)^{-k}(\pi)^k = (\pi)^{-k}(c) \cdot I = (\pi)^{l-k} I$. Also ist I invertierbar.
„$\Longleftarrow$“ Alle (ganzen) Ideale sind endlich erzeugt, somit ist R noethersch. Bezeichne $\mathfrak{m}$ das maximale Ideal von R, so genügt es wegen Satz 3.5 zu zeigen, daß $\{\mathfrak{m}^k \mid k \in \mathbb{N}_0\} \cup \{(0)\}$ alle (ganzen) Ideale von R sind:

Dazu sei $\Gamma = \{\mathfrak{a} \lhd R \mid \mathfrak{a} \neq (0) \text{ und } \mathfrak{a} \neq \mathfrak{m}^k \quad \forall\, k \in \mathbb{N}_0\}$. Diese Menge als nichtleer angenommen, so existiert darin ein maximales Element $\mathfrak{a}$. Wegen $\mathfrak{a} \subsetneq \mathfrak{m}$ ist $\mathfrak{m}^{-1}\mathfrak{a} \subsetneq \mathfrak{m}^{-1}\mathfrak{m} = R$ ein echtes ganzes Ideal in R. Außerdem gilt $\mathfrak{a} \subseteq \mathfrak{m}^{-1}\mathfrak{a}$.
Würde $\mathfrak{m}\mathfrak{a} = \mathfrak{a}$ gelten, dann wäre $\mathfrak{a} = (0)$ mit Nakayamas Lemma was nicht sein kann. Also gilt $\mathfrak{a} \subsetneq \mathfrak{m}^{-1}\mathfrak{a}$ und damit $\mathfrak{m}\mathfrak{a} = \mathfrak{m}^k$ für ein $k \in \mathbb{N}_0$, da $\mathfrak{a}$ maximal gewählt war. Widerspruch. □

Proposition 4.6 Ist R ein Integritätsbereich, so ist R ein Dedekindring genau dann, wenn jedes von (0) verschiedene gebrochene Ideal invertierbar ist.

Beweis: „$\Longrightarrow$“ Sei $(0) \neq I$ ein gebrochenes R-Ideal. Dieses ist endlich erzeugt. Für alle $\mathfrak{p} \underset{\max}{\lhd} R$ ist $I_\mathfrak{p}$ ein gebrochenes $R_\mathfrak{p}$-Ideal und als solches invertierbar. Mit der vorangegangenen Proposition ist I damit invertierbar.
„$\Longleftarrow$“ Alle (ganzen) Ideale sind invertierbar, also insbesondere endlich erzeugt. Damit ist R noethersch.
Seien $(0) \neq \mathfrak{p} \underset{\text{prim}}{\lhd} R$ und $(0) \neq \widetilde{I} \trianglelefteq R_\mathfrak{p}$ beliebig. Dann ist $\widetilde{I} \cap R$ ein ganzes Ideal in R und somit invertierbar. Damit gilt dies auch für $\widetilde{I}$. Nach Proposition 4.5 ist $R_\mathfrak{p}$ somit ein diskreter Bewertungsring und nach Satz 3.5 ein Dedekindring. □

Korollar 4.7 *Sei R ein Dedekindring, die eindeutige Faktorisierung der ganzen Ideale setzt sich fort auf die Menge der gebrochenen Ideale und liefert mittels*

$$(x) = \prod_{\mathfrak{p} \underset{max}{\lhd} R} \mathfrak{p}^{v_\mathfrak{p}(x)} \qquad \textit{mit } v_\mathfrak{p}(x) \in \mathbb{Z} \textit{ und } v_\mathfrak{p}(x) \neq 0 \textit{ nur endlich oft}$$

für jedes von (0) verschiedene Primideal $\mathfrak{p}$ eine diskrete Bewertung $x \mapsto v_\mathfrak{p}(x)$ auf $\mathrm{Quot}(R)$. *Insbesondere gilt dies für algebraische Zahlkörper.*

Korollar 4.8 *Sei R ein Dedekindring, so bilden die von (0) verschiedenen gebrochenen R-Ideale eine freie abelsche Gruppe $\mathcal{J}$, die von den Primidealen in R erzeugt wird.*

Wir wollen das Kapitel 9 in Atiyah-MacDonald und diesen Vortrag mit einem kleinen Ausblick auf die algebraische Zahlentheorie beenden.

Bezeichne $\mathcal{H} = \{xR \mid x \in K^*\} \trianglelefteq \mathcal{J}$ die Menge der gebrochenen Hauptideale, so erhalten wir mittels

$$\varphi\colon K^* \to \mathcal{J},\ x \mapsto (x) = xR$$

die exakte Sequenz

$$1 \to R^* \hookrightarrow K^* \xrightarrow{\varphi} \mathcal{J} \twoheadrightarrow \mathcal{H} \to 1.$$

Sei nun K ein algebraischer Zahlkörper und $\mathbb{Z}_K$ der Ring der ganze Zahlen von K.

Die Gruppe $\mathcal{J}$ ist dann stets unendlich, aber die *Klassenzahl* $h_K := \#\mathcal{J}/\mathcal{H}$ ist endlich. Dies zeigt man in der algebraischen Zahlentheorie mittels den von Hermann Minkowski entwickelten Methoden (Minkowskischer Gitterpunktsatz). Diese werden heute mit dem Begriff „Geometrie der Zahlen“ umschrieben. Weiter ist $\mathbb{Z}_K$ ein Hauptidealbereich genau dann wenn $h_K = 1$ gilt.

Die Einbettungen $\sigma\colon K \hookrightarrow \mathbb{C}$ zerfallen in zwei Klassen: reelle ($\sigma(K) \subset \mathbb{R}$) und nicht reelle, welche wir komplex nennen wollen. Sind deren Anzahlen r respektive $2s$, so sagt man K hätte die *Signatur* $(r,\, s)$. Es ist sicher $[K : \mathbb{Q}] = r + 2s$.

Bezeichnet $\mu(\mathbb{Z}_K) := \{x \in \mathbb{Z}_K \mid x^n = 1 \text{ für ein } n \in \mathbb{Z}_{>0}\}$ die zyklische Gruppe der Einheitswurzeln in $\mathbb{Z}_K$, so besagt der *Dirichletsche Einheitensatz*, daß $\mathbb{Z}_K^*/\mu(\mathbb{Z}_K)$ frei von Ordnung $r+s-1$ ist.

Zum Abschluß noch ein paar Beispiele:

(a) $K = \mathbb{Q}[i]$ besitzt $\mathbb{Z}_K = \mathbb{Z}[i]$. Es gilt $r = 0$, $s = 1$. $\mathbb{Z}_K$ ist ein Hauptidealbereich und somit gilt $h_K = 1$. Außerdem ist $< i >= \{\pm 1, \pm i\} = \mathbb{Z}_K^* = \mu(\mathbb{Z}_K) \cong \mathbb{Z}/4\mathbb{Z}$.

(b) $K = \mathbb{Q}[\sqrt{2}]$. Dann ist $Z_K = \mathbb{Z}[\sqrt{2}]$ und $r = 2$, $s = 0$. Wieder ist die Klassenzahl $h_K = 1$ und es gilt $\mathbb{Z}_K^* = \{\pm 1\} \times < 1 + \sqrt{2} > \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.

(c) $K = \mathbb{Q}[\sqrt{-5}]$. Es ist $\mathbb{Z}_K = \mathbb{Z}[\sqrt{-5}]$, $r = 0$, $s = 1$ und $\mathbb{Z}_K^* = \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$. $\mathbb{Z}_K$ ist kein Hauptidealbereich, da $(2, 1 + \sqrt{-5})$ kein Hauptideal ist. Ferner ist $h_K = 2$ und konkret gilt $\mathcal{J}/\mathcal{H} =< \overline{(2, 1 + \sqrt{-5})} > \cong \mathbb{Z}/2\mathbb{Z}$.

(d) $K = \mathbb{Q}[\sqrt{5}]$. Hier ist $\mathbb{Z}_K = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ (und nicht $\mathbb{Z}[\sqrt{5}]$ wie man meinen könnte). Es wird $r = 2$, $s = 0$, $h_K = 1$ und $\mathbb{Z}_K^* = \{\pm 1\} \times < \frac{1+\sqrt{5}}{2} > \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.

Dies waren allesamt quadratische Zahlkörper, also $K = \mathbb{Q}[\sqrt{d}]$ für ein quadratfreies $d \in \mathbb{Z}$. Ist $d < 0$, so tritt $h_K = 1$ nur in den neun Fällen $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$ auf. Für positive d wird vermutet, daß dies unendlich oft der Fall ist. Insgesamt ist jedoch nicht einmal bekannt, ob es unter allen algebraischen Zahlkörper unendlich viele mit Klassenzahl 1 gibt.