Teil III. Dedekind Ringe.

Satz. *Sei R ein Integritätsbereich. Die folgenden Eigenschaften sind äquivalent:*

(i) *Die Halbgruppe der gebrochenen Ideale ist eine Gruppe.*

(ii) *Jedes gebrochene Ideal ist invertierbar (d.h. es gibt einen Untermodul I' von $\mathrm{Quot}(R)$ mit $II' = R$).*

(iii) *Jedes von Null verschiedene Ideal von R ist invertierbar.*

(iii′) *Jedes Ideal von R ist projektiver Modul.*

(iv) *Jedes von Null verschiedene Ideal ist Produkt von maximalen Idealen.*

(v) *Jedes von Null verschiedene Ideal ist Produkt von Primidealen.*

(vi) *Jedes von Null verschiedene Primideal P ist invertierbar.*

(vii) *R ist noethersch, R_M ist Hauptidealring für jedes maximale Ideal M von R.*

(viii) *R ist noethersch, ganz abgeschlossen und hat Krull-Dimension höchstens 1.*

Zusatz: *Die Darstellung eines Ideals als Produkt von invertierbaren Primidealen ist bis auf die Reihenfolge eindeutig.*

Beweis: (i) $\Longrightarrow$ (ii) $\Longrightarrow$ (iii): trivial. (ii) $\Longrightarrow$ (i): Wie wir gesehen haben, folgt aus $II' = R$, daß I' ebenfalls gebrochenes Ideal ist. (iii) $\Longrightarrow$ (ii). Sei I gebrochenes Ideal, etwa $\langle \frac{a}{\ } \subseteq I \subseteq \langle b\rangle$ mit $a, b \in K$. Sei $0 \neq r \in R$ mit $rb \in R$. Dann ist $Ir \subseteq \langle rb\rangle \subseteq R$ ein von Null verschiedenes Ideal von R. Es ist invertierbar, etwa $IrI' = R$. Also ist I invertierbar. Für (iii) $\Longleftrightarrow$ (iii') ist nur noch anzumerken, daß der Nullmodul natürlich projektiv ist.

(iv) $\Longrightarrow$ (iii). Sei M maximales Ideal, sei $0 \neq u \in M$. Schreibe $Ru = \prod_i M_i$ mit Prim-Idealen $M_1, \ldots, M_n$. Wegen $\prod M_i \subseteq M$ und M Primideal, folgt $M_i \subseteq M$ für ein i, also $M_i = M$. Wir können annehmen $i = 1$. Also $M \cdot \prod_{j\geq 2} M_j = Ru$, also $M \cdot (\prod_{j\geq 2} M_j)u^{-1} = R$. Dies zeigt, daß M invertierbar ist.

(iii) $\Longrightarrow$ (iv). Wir setzen also voraus, daß jedes von Null verschiedene Ideal I von R invertierbar ist. Insbesondere ist dann R noethersch. Angenommen, es gibt ein von Null verschiedenes Ideal, das sich nicht als Produkt von maximalen Idealen schreiben läßt; wähle I maximal mit dieser Eigenschaft. Das Ideal I ist ein echtes Ideal (denn nach Definition ist R Produkt von maximalen Idealen, mit 0 Faktoren), also in einem maximalen Ideal M enthalten, und zwar echt. Bilde $M^{-1}I$, dabei ist $M^{-1} = \{r \in K \mid rM \subseteq R\}$. Wegen $I \subseteq M$ ist $M^{-1}I \subseteq R$, also ein Ideal von R. Wegen $1 \in M^{-1}$ ist $I \subseteq M^{-1}I$. Wäre $I = M^{-1}I$, so wäre $MI = I$, dies ist aber unmöglich, wie wir gleich zeigen werden. Wegen $I \subset M^{-1}I$ läßt sich $M^{-1}I$ als Produkt maximaler Ideale schreiben, etwa $M^{-1}I = M_1 \cdots M_t$, also $I = M \cdot M_1 \cdots M_t$, ein Widerspruch zur Wahl von I.

Es bleibt zu zeigen: *Sei I endlich erzeugtes Ideal in einem Integritätsbereich R, sei M maximales Ideal von R mit $MI = I$. Dann ist $I = 0$.* Beweis: Sei $I = \sum_{i=1}^n Rx_i$. Sei $I_j = \sum_{i=j}^n Rx_i$, für $0 \leq j \leq n$, also $I_1 = I$, und $I_{n+1} = 0$. Wir konstruieren induktiv Elemente $z_j \in M$ mit $(1 - z_j)I \subseteq I_j$. Für $i = 1$ nimm $z_1 = 0$. Sei nun z_j konstruiert, also $(1-z_j)I \subseteq I_j$. Wegen $I \subseteq MI$ ist $(1-z_j)I \subseteq (1-z_j)MI \subseteq MI_j$, also $(1 - z_j)x_j = \sum_{i=j}^n r_{ij}x_i$ mit $r_{ij} \in M$. Also ist $(1 - z_j - r_{jj})x_j \in I_{j+1}$, also

$(1 - z_j - r_{jj})I_j \in I_{j+1}$. Setze nun $(1 - z_{j+1}) = (1 - z_j - z_{jj})(1 - z_j)$. Es ist

$$(1 - z_{j+1})I = (1 - z_j - z_{jj})(1 - z_j)I \subseteq (1 - z_j - z_{jj})I_j \subseteq I_{j+1}.$$

Also erhalten wir mit $z = z_{n+1}$ ein Element in M mit $(1-z)I = 0$. Da R nullteilerfrei ist und $1 \neq z$, folgt $I = 0$.

(iv) $\implies$ (v): trivial. Bevor wir nun (v) $\implies$ (vi) zeigen, beweisen wir den Zusatz.

Beweis des Zusatzes: Sei $I = P_1 \cdots P_s = Q_1 \cdots Q_t$ mit invertierbaren Primidealen P_i, Q_j. Wähle P_i minimal unter den Idealen $P_1, \ldots P_s$. Wegen $Q_1 \cdots Q_t \subseteq P_1$ gibt es Q_j mit $Q_j \subseteq P_1$. Auch hier können wir annehmen $j = 1$. Wegen $P_1 \cdots P_s \subseteq Q_1$ gibt es P_i mit $P_i \subseteq Q_1$. Die Minimalität von P_1 und $P_i \subseteq Q_1 \subseteq P_1$ liefern $P_1 = Q_1$. Da wir voraussetzen, daß P_1 invertierbar ist, folgt nun $P_1 \cdots P_s = Q_2 \cdots Q_t$. Mit Induktion folgt die Behauptung.

Beweis der Implikation (v) $\implies$ (vi). Wir zeigen als erstes: Aus (v) folgt: *jedes invertierbare Primideal ist maximal.* Sei also P invertierbares Primideal. Sei $a \in R \setminus P$. Wir zeigen $P + Ra = R$ (dies impliziert, daß P maximal ist).

Schreibe die Ideale $P + Ra = P_i \cdots P_r$ und $P + Ra^2 = Q_1 \cdots Q_s$ mit Primidealen P_i, Q_j. Wegen $P \subseteq P_1 \cdots P_r \subseteq \bigcap P_i$ gilt $P \subseteq P_i$ für jedes i; entsprechend $P \subseteq Q_j$ für jedes j. Im Faktorring $\overline{R} = R/P$ sind die Ideale P_i/P und Q_j/P Primideale und es gilt $\overline{R}\overline{a} = P_1/P \cdots P_r/P$ und $\overline{R}\overline{a^2} = Q_1/P \cdots Q_s/P = (P_1/P)^2 \cdots (P_r/P)^2$, also ist $s = 2r$ und wir können annehmen $Q_{2i-1}/P = Q_{2i}/P = P_i/P$, also auch $Q_{2i-1} = Q_{2i} = P_i$. Daraus folgt:

$$P + Ra^2 = Q_1 \cdots Q_s = (P_1 \cdots P_r)^2 = (P + Ra)^2.$$

Also gilt

$$P \subseteq P + Ra^2 = (P + Ra)^2 \subseteq P^2 + Ra.$$

Es gilt sogar $P \subseteq P^2 + Pa$, denn ist $p \in P$, so schreibe $p = y + za$ mit $y \in P^2, z \in R$, also $za \in P$. Wegen $a \notin P$ folgt $z \in P$. Die umgekehrte Inklusion ist trivial, also gilt

$$P = P^2 + Pa.$$

Nun ist P invertierbar, also ist $R = P + Ra$.

Nun also der eigentliche Beweis von (v) $\implies$ (vi). Nimm ein Element $0 \neq p \in P$ und schreibe $Rp = \prod P_i$ mit Primidealen P_i. Alle diese Primideale P_i sind invertierbar (denn $Rp^{-1} \prod P_i = R$). Wegen $\prod P_i \subseteq P$ und P prim gibt es ein i mit $P_i \subseteq P$. Da P_i invertierbar ist, ist P_i maximal, also $P_i = P$ ist invertierbar.

Beweis (vi) $\implies$ (iii). Sei $\mathcal{U}$ die Menge der von Null verschiedenen Ideale, die nicht invertierbar sind. Angenommen $\mathcal{U} \neq \emptyset$. Ist $(U_\lambda)_\lambda$ eine Kette (bezüglich Inklusion) in $\mathcal{U}$, so gehört auch $U = \bigcup U_\lambda$ zu $\mathcal{U}$ (denn wäre U invertierbar, so endlich erzeugt, also gleicbh einem U_λ, Widerspruch). Also wähle $U \in \mathcal{U}$ maximal

(Zorn). Da U nicht invertierbar ist, ist U ein echtes Ideal von R. Da alle Primideale invertierbar sind, ist U kein Primideal. Also gibt es $a, b \in R \setminus U$ mit $ab \in U$. Setze $U' = \{x \in R \mid xa \in U\}$, dies ist ein Ideal von R mit $U \subseteq U'$. Wegen $b \in U' \setminus U$ gilt $U \subset U'$. Also ist U' invertierbar. Entsprechend ist $U \subset U + Ra$, also ist auch $U + Ra$ invertierbar. Mit U' ist auch $U'a$ als Produkt zweiter invertierbarer Ideale invertierbar. Andererseits ist $U'a = U \cap Ra$ (denn $U'a \subseteq U$ und $U'a \subseteq Ra$ folgen beide aus der Definition von U', Ist andererseits $u \in U \cap Ra$, etwa $u = ra$ mit $r \in R$, so ist $r \in U'$, also $u = ra \in U'a$.

Wir erhalten eine exakte Folge der Form

$$0 \to U \cap Ra \to U \oplus Ra \to U + Ra \to 0.$$

Da $U + Ra$ invertierbar, also projektiv ist, zerfällt die Folge und es gilt $U \oplus Ra \simeq (U \cap Ra) \oplus (U + Ra)$. Der rechte Modul ist projektiv, also ist auch U projektiv, Widerspruch.

Vorbemerkungen zum Beweis: (iii) $\implies$ (vii). Wir betrachten zuerst den Fall eines lokalen Rings.

Lemma. Sei R ein lokaler Integritätsbereich. Genau dann ist jedes von Null verschiedene Ideal invertierbar, wenn R ein Hauptidealring (also ein diskreter Bewertungsring oder ein Körper) ist.

Beweis: In Hauptidealbereichen ist jedes von Null verschiedene Ideal invertierbar. Umgekehrt sei jedes von Null verschiedene Ideal von R invertierbar. Dann ist jedes Ideal endlich erzeugt, also R ist noethersch. Es reicht zu zeigen: Sind x, y von Null verschiedene Elemente des Rings, so ist $x \in Ry$ oder $y \in Rx$. Sei $I = \langle x, y\rangle$ und $II' = R$, also $1 = xx' + yy'$ mit $x', y' \in I$. Wir sehen, daß gilt $Rxx' + Ryy' = R$, also, da R lokal ist, ist etwa $Ryy' = R$. Daraus folgt einerseits $Ryy'x = Rx$, andererseits ist $Rxy' \subseteq R$ und demnach $Rxy'y \subseteq Ry$. Insgesamt sehen wir also $Rx \subseteq Ry$.

Lemma. *Sei R Integritätsbereich mit* (iii). *Sei Σ multiplikative Menge von R. Dann gilt* (iii) *auch in $R\Sigma^{-1}$.*

Beweis: Sei I ein von Null verschiedenes Ideal von $S = R\Sigma^{-1}$. Dann ist $I = (I \cap R)\Sigma^{-1}$ (denn $\supseteq$ ist trivial, und ist $x = \frac{r}{s} \in I$ mit $r \in R, s \in \Sigma$, so ist $r = \frac{r}{s}s$ in $I \cap R$, also $\frac{r}{s} = rs^{-1} \in (I \cap R)\Sigma^{-1}$). Es ist $I \cap R$ ein von Null verschiedenes Ideal von R, also invertierbar: es gibt also einen R-Untermodul J mit $(I \cap R)J = R$. Also $R\Sigma^{-1} = (I \cap R)\Sigma^{-1}J\Sigma^{-1} = I \cdot J\Sigma^{-1}$ zeigt, daß I invertierbar ist.

Beweis von (iii) $\implies$ (vii): Ist jedes von Null verschiedene Ideal von R invertierbar, so R noethersch. Und für jedes maximale Ideal M von R gilt die Bedingung (iii) im Ring $R_M = R(R \setminus M)^{-1}$, also ist R_M ein Hauptidealring.

Vorbemerkungen zum Beweis (vii) $\implies$ (viii). Ganz allgemein gilt:

Lemma. *Sei R Integritätsbereich. Dann ist $R = \bigcup_M R_M$, wobei M alle maximalen Ideale durchläuft.*

Beweis: Eine Inklusion ist trivial. Sei also $x \in \bigcup R_M$. Sei $I = \{y \in R \mid yx \in R\}$, dies ist ein Ideal von R. Wäre dies ein echtes Ideal, so wäre es in einem maximalen Ideal enthälten, etwa in M. Da $x \in R_M$, schreiben wir $x = \frac{r}{s}$ mit $r \in R$ und $s \in R \setminus M$. Es ist $s \in I$, denn $sx = s\frac{r}{s} = r \in R\}$, also $s \in T \subseteq M$, Widerspruch. Demnach ist $I = R$, also $1 \in I$, also $x \in R$.

Lemma. *Ist R Integritätsbereich, und sind multiplikative Mengen Σ_i gegeben, mit $R = \bigcup R\Sigma_i^{-1}$, so gilt: Sind alle Ringe $R\Sigma_i^{-1}$ ganz abgeschlossen, so ist auch R ganz abegschlossen.*

Beweis: Sei $f(T) \in R[T]$ normiertes Polynom, sei $x \in K$ Nullstelle von $f(T)$. Dies ist ein normiertes Polynom in $R\Sigma_i^{-1}[T]$ und $x \in \mathrm{Quot}(R\Sigma_i - 1)$. Da der Ring $R\Sigma_i^{-1}$ ganz abgeschlossen ist, ist $x \in R\Sigma_i^{-1}$, also im Durchschnitt dieser Unterringe, also in R.

Nun der Beweis (vii) $\implies$ (viii): Die beiden Lemmata zeigen, daß aus R_M ganz abgeschlossen für alle M folgt, daß auch R ganz abgeschlossen ist. Jede Primidealkette liefert eine entsprechend lange Primidealkette in einem Ring R_M. Da alle Ringe R_M Krull-Dimension höchstens 1 haben, hat auch R Krull-Dimension höchstens 1.

Beweis von (viii) $\implies$ (vi). Sei $P \neq 0$ Primideal von R, sei $0 \neq a \in P$. In einem noetherschen Ring enthält jedes Ideal ein Produkt von Primidealen, die von Null verschieden sind. Also gibt es Primideale $P_1, \ldots, P_t$ mit $P_1 \cdots P_t \subseteq Ra$. Wähle eine solche Darstellung mit t minimal. Wegen $P_1 \cdots P_t \subseteq Ra \subseteq P$ und P prim gibt können wir annehmen $P_1 \subseteq P$. Wegen Krull-Dimension höchstens 1 ist P_1 maximales Ideal, also $P_1 = P$. Die Minimalität von t besagt $P_2 \ldots P_t \not\subseteq Ra$, also gibt es $b \in P_1 \cdots P_t$ mit $b \notin Ra$.

Wegen $bP \subseteq Ra$ ist $a^{-1}bP \subseteq R$. Sei $I = \{x \in K \mid xP \subseteq R\}$. Es ist $P \subseteq IP$ (wegen $1 \in I$) und $IP \subseteq R$ (nach Definition von I). Da P maximal ist, gibt es nur die Möglichkeiten $P = IP$ und $IP = R$. Letzteres hätten wir gern, denn dies zeigt ja, daß P invertierbar ist. Angenommen, $P = IP$. Da $a^{-1}b \in I$, gilt $a^{-1}bP \subseteq P$, aber dann ist $a^{-1}b$ ganz über R (daran sei gleich noch erinnert), gehört also zu R und demnach ist $b = (a^{-1}b)a \in Ra$, ein Widerspruch.

Erinnerung. *Sei $R \subseteq S$ eine Inklusion von Integritätsbereichen und sei $U \neq 0$ ein endlich erzeugter R-Untermodul von S. Ist $s \in S$ mit $sU \subseteq U$, so ist s ganz über R.*

Beweis: Sei $u_1, \ldots, u_n$ ein R-Erzeugendensystem von U, schreibe $cu_i = \sum r_{ij}u_j$ mit $r_{ij} \in R$, also $\sum(c\delta_{ij} - r_{ij})u_j =$. Betrachte die Matrix $A = (r_{ij})$ und auch $(cI - A)$ Multiplizieren wir mit der klassischen Adjunkten $\mathrm{adj}(cI - A)$, so erhalten wir $\chi_A(c)u_j = 0$, für alle j. Da $U \neq 0$, gilt $u_j \neq 0$ für mindestens ein j und demnach $\chi_A(c) = 0$, also ist c Nullstelle des charakteristischen Polynoms der Matrix A.

Bemerkung (ohne Beweis): "Jedes Ideal ist projektiv" bedeutet: Jeder Untermodul von ${}_RR$ ist projektiv. Daraus folgt ganz allgemein: Jeder Untermodul eines projektiven Moduls ist projektiv; man nennt derartige Ringe *erblich.*

Ist R Dedekind-Ring, so ist die Gruppe der gebrochenen Ideale freie abelsche Gruppe mit Basis die Menge der maximalen Ideale. (Freie abelsche Gruppe = freier $\mathbb{Z}$-Modul).

Dies folgt aus der Eindeutigkeit der Darstellung als Produkt invertierbarer Primideale.

Zerlegungssatz: Weitreichende Verallgemeinerung des Fundamentalsatzes der Algebra und des Fundamentalsatzes der elementaren Zahlentheorie.

In einem Dedekind-Ring bezeichnet man die Faktorgruppe der Gruppe der gebrochenen Ideale modulo der Untergruppe der zyklischen gebrochenen Ideale als *Idealklassengruppe,* ihre Ordnung die *Klassenzahl.* Wichtig in der Zahlentheorie: *Die Idealklassengruppe ist eine endliche Gruppe.* Natürlich gilt: Genau dann ist die Idealklassengruppe trivial, wenn R ein Hauptidealring ist. Die Idealklassengruppe mißt die Abweichung, ein Hauptidealring zu sein.

Sei $h(m)$ die Klassenzahl des imaginär-quadratischen Zahlkörpers $K = \mathbb{Q}[\sqrt{m}]$. Genau dann ist $h(m) = 1$, wenn gilt

$$|m| = 1, 2, 3, 7, 11, 19, 43, 67, 163$$

(die List der zugehörenden "Diskriminanten" ist $|d| = 3, 4, 7, 8, 11, 19, 43, 76, 163$). (Ferner gibt es genau 18 Fälle mit Klassenzahl 2.) Es gibt viele, möglicherweise unendlich viele reell-quadratische Zahlkörper mit Klassenzahl 1.

Lemma. (Fast wie oben) *Ist $I \subseteq K$ ein Untermodul, so ist jeder R-Homomorphismus $f\colon I \to K$ von der Form $f(x) = x \cdot b$ mit $b \in K$.*

Beweis: Ist $I = 0$, so nimm $b = 0$. Sei also $I \neq 0$. Dann ist auch $I \cap R \neq 0$ and wir wählen ein Element $0 \neq u \in I \cap R$. Ist $y \in I$, etwa $y = \frac{r}{s}$ mit $r, s \in R$, so ist

$$suf(\frac{r}{s}) = f(su\frac{r}{s}) = f(ur) = rf(u),$$

also gilt für $b = \frac{f(u)}{u}$

$$f(y) = f(\frac{r}{s}) = \frac{r}{s} \cdot \frac{f(u)}{u} = y \cdot b.$$

Die invertierbaren gebrochenen Ideale sind gerade die "projektiven Moduln vom Rang 1", wir sehen also: Zwei projektive Moduln vom Rang 1 sind genau dann isomorph, wenn sie zur gleichen Restklasse modulo der Untergruppe der zyklischen gebrochenen Ideale gehören (und die Multiplikation entspricht gerade dem Tensor-Produkt). Man bezeichnet mit $\mathrm{Pic}(R)$ die Gruppe der Isomorphieklassen projektiver Moduln vom Rang 1 bezüglich des Tensorprodukts. Wir sehen also: *Für einen Integritätsbereich R gilt:* $\mathrm{Pic}(R)$ *ist gleich der Restklassengruppe der invertierbaren gebrochenen Ideale modulo der Untergruppe der zyklischen gebrochenen Ideale.*