Universität Regensburg
Fakultät für Mathematik

Wintersemester 2016/2017

Seminar zum Thema:

Gröbnerbasen und Regularität

Multiplikative Idealtheorie

vorgelegt von:

Selina Strathmeyer

Seminarleitung

Prof. Dr. Moritz Kerz
Dr. Florian Strunk

Termin:

14. Dezember 2016

Vorwort In dieser schriftlichen Ausarbeitung des Abschnittes 2 aus Kapitel 14 in [Kem11] zum Thema „Multiplikative Idealtheorie“ im Rahmen des Seminars über Gröbnerbasen und Regularität bei Prof. Dr. Moritz Kerz und Dr. Florian Strunk werden gebrochene Ideale eingeführt, welche unsere klassische Vorstellung von Idealen erweitern. Dabei wird der Frage nachgegangen, wann ein gebrochenes Ideal invertierbar ist. Es wird sich herausstellen, dass dies eng damit verknüpft ist, dass ein Ideal von der Höhe 1 ist. Gebrochene Ideale spielen etwa bei der Untersuchung von Dedekindbereichen eine entscheidende Rolle, wie im weiteren Verlauf des Seminars noch thematisiert werden wird.
Die Nummerierung in [ ] bezieht sich auf die originale Nummerierung in [Kem11]. Soweit nicht anders vermerkt, wird die originale Nummerierung von Aussagen und Beispielen, die in anderen Kapiteln von [Kem11] eingeführt wurden, beibehalten.

Multiplikative Idealtheorie

In diesem Abschnitt sei R ein beliebiger Ring.

Wir erinnern zunächst an das Produkt von Idealen.

1.1 Definition [2.5] Sei R ein kommutativer Ring, $I \subseteq R$ ein Ideal und M ein R-Modul.

a) Das **Produkt** von I und M ist definiert als die abelsche Gruppe erzeugt von allen Produkten $a \cdot m$ von Elementen aus I und aus M. Es gilt somit
$$I \cdot M = \left\{ \sum_{i=1}^{n} a_i m_i \mid n \in \mathbb{N}, a_i \in I, m_i \in M \right\}$$
Dabei ist $I \cdot M \subseteq M$ ein Untermodul.

b) Im Falle $M = J$, für $J \subseteq R$ ein weiteres Ideal von R, gilt, dass das Idealprodukt kommutativ und assoziativ ist.

1.2 Bemerkung Die Menge der Ideale $I \subseteq R$ zusammen mit dem Idealprodukt aus Definition 1.1 bildet einen abelschen Monoid, wobei R kommutativ sei. Dies folgt daraus, dass jedes Ideal bereits eine additive Untergruppe von R ist und dass das Idealprodukt assoziativ und kommutativ ist. Aus den Idealeigenschaften erhält man für ein Ideal I, dass
$$R \cdot I = \left\{ \sum_{i=1}^{n} r_i a_i \mid n \in \mathbb{N}, a_i \in I, r_i \in R \right\} = I$$
und somit R das zugehörige neutrale Element ist.
Das einzige invertierbare Element in diesem Monoid ist dabei R selbst.

Dabei werden diese Aussagen umso interessanter, wenn der Blickwinkel erweitert wird. Daher werden wir im Folgenden gebrochene Ideale betrachten, basierend auf Definition 1.3:

1.3 Definition [14.4] Sei R ein Integritätsring und $K := \mathrm{Quot}(R)$ der zugehörige Quotientenkörper.

a) Ein **gebrochenes Ideal** ist ein R-Untermodul $I \subseteq K$.

b) Das **Produkt zweier gebrochener Ideale** ist definiert wie das Produkt gewöhnlicher Ideale und macht die Menge der gebrochenen Ideale damit zu einem abelschen Monoid mit Neutralelement R.

c) Ein gebrochenes Ideal I ist **invertierbar**, wenn ein gebrochenes Ideal J existiert, sodass $I \cdot J = R$.
Damit bilden die invertierbaren gebrochenen Ideale eine abelsche Gruppe, die wir mit $C(R)$ bezeichnen. (Die Begründung für diese Bezeichnung folgt später.)

1.4 Bemerkung zu Definition 1.3 a)

a) Einige Autoren wie etwa Neukirch fordern, dass gebrochene Ideale $I \neq (0)$ sind und/oder verlangen zusätzlich, dass ein $a \in R \setminus \{0\}$ existiert mit $a \cdot I \subseteq R$ (vgl. [Neu92], S. 22).

b) Ein gebrochenes Ideal I ist dabei nicht zwangsläufig ein Ideal von R, da $I \subseteq K$ nicht notwendigerweise eine Teilmenge von R selbst sein muss.

c) Es ist möglich, die obige Definition auf Ringe, die keine Integritätsbereiche sind, zu verallgemeinern, indem man den Totalquotientenring statt dem Quotientenkörper betrachtet. Dabei ist ein **Totalquotientenring** Q eines Ringes R definiert als die Lokalisierung von R an die Menge der Nichtnullteiler von R (vgl.[Har77], S.140). Ist R dabei ein Integritätsring, so ist der Totalquotientenring nach Definition der Quotientenkörper von R.
Betrachtet man etwa den Restklassenring $\mathbb{Z}/6\mathbb{Z}$, so ist dieser kein Integritätsbereich, da er nicht nullteilerfrei ist, da $2 \cdot 3 \equiv 6 \equiv 0 \mod 6$, aber 2 und 3 selbst nicht null sind in $\mathbb{Z}/6\mathbb{Z}$. Die Menge S der Nicht-Nullteiler in diesem Ring setzt sich aus den Restklassen von 1 und 5 zusammen und somit wäre hier der Totalquotientenring gegeben als $Q = S^{-1}(\mathbb{Z}/6\mathbb{Z})$. Dies würde uns erlauben, gebrochene Ideale in $\mathbb{Z}/6\mathbb{Z}$ zu betrachten.

Im Folgenden nehmen wir nun an, dass R ein Integritätsbereich ist und $K := \mathrm{Quot}(R)$ der zugehörige Quotientenkörper.

1.5 Bemerkung

a) Ein Produkt von gebrochenen Idealen $I \cdot J$ ist genau dann invertierbar, wenn es auch I und J sind.

Beweis: Seien I und J invertierbare gebrochene Ideale. $\Leftrightarrow$ Es existieren $I', J' \subset K$ mit $I \cdot I' = R$ und $J \cdot J' = R$. $\Leftrightarrow$ $R = R \cdot R = (I \cdot I') \cdot (J \cdot J') = (I \cdot J) \cdot (I' \cdot J')$, da R als Integritätsring kommutativ ist. $\Leftrightarrow$ $I \cdot J$ ist ein invertierbares Produkt von gebrochenen Idealen. $\square$

b) Für jedes $a \in K = \mathrm{Quot}(R), a \neq 0$ ist das gebrochene Hauptideal $(a)_R \subseteq K$ invertierbar. Dabei ist das zugehörige Inverse $(a^{-1})_R$, denn:
Sei $a \in \mathrm{Quot}(R) \setminus \{0\}$. Dann existiert ein $a^{-1} \in \mathrm{Quot}(R)$, sodass $a \cdot a^{-1} = 1$. Nun gilt, dass $(a^{-1})_R = \{y \cdot a^{-1} \,|\, y \in R\}$. Damit erhält man nach der Definition des Idealprodukts $(a)_R \cdot (a^{-1})_R = \{z \cdot a \cdot a^{-1} \,|\, z \in R\} = \{z \cdot 1 \,|\, z \in R\} = R$, da R als Integritätsbereich assoziativ ist.
Dies liefert einen Homomorphismus

$$\phi : K^* \longrightarrow C(R),\, a \longmapsto (a)_R$$

mit $\ker(\phi) = \{q \in \mathrm{Quot}(R) \setminus \{0\} \,|\, (q)_R = (1)_R\} = R^*$.
Im Allgemeinen ist ϕ nicht surjektiv, z.B. könnten invertierbare gebrochenen Ideale existieren, die keine Hauptideale sind, wie das folgende Beispiel zeigt:

1.6 Beispiel [14.5] Betrachte im Folgenden den Ring

$$R := \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \,|\, a, b \in \mathbb{Z}\} \subset \mathbb{C}$$

zusammen mit der Norm

$$N : \mathbb{Z}[\sqrt{-5}] \longrightarrow \mathbb{N},\, a + b\sqrt{-5} \longmapsto a^2 + 5b^2$$

sowie das Ideal $I = (2, 1 + \sqrt{-5})_R \subseteq R$. Mit $J := \left(1, \frac{1-\sqrt{-5}}{2}\right)_R \subseteq \mathrm{Quot}(R)$, erhält man

$$I \cdot J = \left(2, 1 - \sqrt{-5}, 1 + \sqrt{-5}, 3\right)_R = R$$

und daher ist I nach 1.3 invertierbar.
Allerdings ist I kein Hauptideal. Tatsächlich lässt sich von der Annahme $I = (z)_R$ mit $z =$

$a + b\sqrt{-5},\ a, b \in \mathbb{Z}$ folgern, dass 2 und $1 + \sqrt{-5} \in (z)_R$ gilt und somit $N(z) \mid N(2) = 4$ und $N(z) \mid N(1 + \sqrt{-5}) = 6$, also

$$a^2 + 5b^2 \mid 4 \text{ und } a^2 + 5b^2 \mid 6.$$

Dies impliziert, dass $a = \pm 1$ und $b = 0$ und somit $I = R$. Allerdings gilt $I = \{x + y\sqrt{-5} \mid x, y \in \mathbb{Z}, x \equiv y \bmod 2\} \neq R$. Dabei folgt diese Darstellung von I aus der Überlegung, dass ein Element $a \in I$ in der Form $a = 2\alpha + \beta + \beta\sqrt{-5}$ mit $\alpha, \beta \in \mathbb{Z}$ dargestellt werden kann und indem man $x := 2\alpha + \beta$ und $y := \beta$ setzt, was dann wiederum $x \equiv y \bmod 2$ liefert.
Dieser Ring war bereits Gegenstand von Beispiel 8.9(3) und wir haben dort gesehen, dass dieser normal, aber nicht faktoriell ist.

Wie die folgende Proposition nun zeigen wird, sind invertierbare gebrochene Ideale nicht sehr weit davon entfernt, die Eigenschaften eines Hauptideals zu besitzen:

1.7 Proposition [14.6] (Invertierbare gebrochene Ideale sind lokal Hauptideale)
Sei R ein Integritätsbereich und $I \subseteq K := \mathrm{Quot}(R)$ ein gebrochenes Ideal. Dann sind die folgenden Aussagen äquivalent:

a) I ist invertierbar.

b) Mit $I' := \{a \in K \mid aI \subseteq R\}$ erhält man $I \cdot I' = R$.

c) Es ist $I \neq (0)$, endlich erzeugt und für jedes Primideal $P \in \mathrm{Spec}(R)$ existiert ein $a \in I$, sodass die Lokalisierung von I

$$I_P = (a)_{R_P}$$

genügt.
Man sagt dann, I **ist lokal ein Hauptideal**.

Beweis:

a)$\Rightarrow$ c) Da I nach Voraussetzung invertierbar ist, existiert ein gebrochenes Ideal $J \subseteq K$ mit $I \cdot J = R$ nach Definition. Insbesondere erhalten wir $1 = \sum_{i=1}^n a_i b_i$ mit $a_i \in I$ und $b_i \in J$ für alle $i = 1, \ldots, n$. Damit erfüllt jedes $x \in I$

$$x = 1 \cdot x = \sum_{i=1}^n a_i b_i x = \sum_{i=1}^n a_i x b_i$$

und damit folgt für $x \in I$, $b_i \in J$, dass $xb_i \in I \cdot J = R$ für alle $i = 1, \ldots, n$. Daher wird I von $a_1, \ldots, a_n$ erzeugt. Da I invertierbar, gilt offensichtlich $I \neq \{0\}$.
Weiterhin existiert für jedes $P \in \mathrm{Spec}(R)$ ein $a \in I$ und $y \in J$ mit $ay \in R \setminus P$. Wäre $ay \in P \subsetneq R$ für beliebige $a \in I, y \in J$, so würde daraus folgen, dass $I \cdot J \subsetneq R$. Allerdings gilt $I \cdot J = R$ und $P \subsetneq R$.
Für ein beliebiges Element $\frac{b}{u} \in I_P$ mit $b \in I$ und $u \in R \setminus P$ erhalten wir

$$\frac{b}{u} = \frac{by}{uay} \cdot a \in (a)_{R_P},$$

da $by \in I \cdot J = R$ und $uay \in R \setminus P$.
Daher ist I lokal ein Hauptideal und es folgt c).

c) $\Rightarrow$ b) Nach Definition von I' ist $I \cdot I' \subseteq R$ ein Ideal von R. Für einen Widerspruchsbeweis nehmen wir nun an, dass $I \cdot I' \subsetneq R$. Dann existiert ein maximales Ideal $P \in \mathrm{Spec}(R)$ mit $I \cdot I' \subseteq P$ nach dem Zorn'schen Lemma. Nach Annahme c) existiert ein $a \in I$ mit $I_P = (a)_{R_P}$ und

$I = (a_1, \dots, a_n)$, da I endlich erzeugt. Da $a_i \in I$ für alle i folgt insbesondere, dass $a_i \in I_P = (a)_{R_P}$. Somit können alle a_i dargestellt werden als $a_i = \frac{\alpha_i}{u_i} \cdot a$ für $\alpha_i \in R, u_i \in R \setminus P$, $i = 1 \dots, n$. Daraus folgt, dass ein $u \in R \setminus P$ existiert mit $ua_i \in (a)_R$ für alle $i = 1, \dots, n$, sodass $uI \subseteq (a)_R$.
Da $I \neq \{0\}$, ist $a \neq 0$ und es folgt, dass $\frac{u}{a} \in I'$ und somit $u = a \cdot \frac{u}{a} \in I \cdot I'$, was im Widerspruch steht zu $I \cdot I' \subseteq P$. Dies impliziert b).

b) $\Rightarrow$ a) Da I nach Voraussetzung ein gebrochenes Ideal ist und da nach b) ein $I' := \{a \in K \mid aI \subseteq R\}$ mit $I \cdot I' = R$ existiert, ist I nach Definition invertierbar und es folgt a). Dabei ist I' ebenfalls ein gebrochenes Ideal nach Definition.

□

1.8 Bemerkung In obigem Beweis kann man b) auch leicht aus a) folgern, indem man nutzt, dass die Invertierbarkeit von I die Existenz eines gebrochenen Ideals J impliziert mit $I \cdot J = R$.

1.9 Definition Ausgehend von 1.7b) der obigen Proposition definieren wir

$$I^{-1} := \{a \in \mathrm{Quot}(R) \mid aI \subseteq R\}$$

für ein beliebiges gebrochenes invertierbares Ideal I eines Integritätsbereichs R.

1.10 Bemerkung Die Endlichkeitsbedingung in 1.7c) darf dabei nicht vernachlässigt werden, damit die Äquivalenzen in Proposition 1.7 gelten: Auch wenn es zunächst unwahrscheinlich erscheint, gibt es Beispiele von noetherschen Integritätsbereichen und gebrochenen Idealen, die lokal Hauptideale sind, aber nicht endlich erzeugt und damit auch nicht invertierbar. Betrachte dazu $I \subseteq \mathbb{Q}$, welcher der Untermodul von $\mathbb{Q}$ sei, der von allen Elementen der Form $\frac{1}{p}$ erzeugt wird, wobei p Primzahlen seien. Dann ist I nicht endlich erzeugt, da das kleinste gemeinsame Vielfache der Nenner eines endlichen Erzeugendensystems das Produkt aller Primzahlen wäre. Andererseits gilt für $P = (p) \in \mathrm{Spec}(\mathbb{Z})$ für p Primzahl, dass

$$\frac{1}{q} = \frac{p}{q} \cdot \frac{1}{p} \in \mathbb{Z}_P \cdot \frac{1}{p}$$

für alle Primzahlen q und somit folgt $I_P = (\frac{1}{p})_{\mathbb{Z}_P}$ und für $P = \{0\}$ erhält man $\mathbb{Z}_P = \mathbb{Q}$, also $I_P = (1)_{\mathbb{Q}}$.
Somit ist I also ein gebrochenes Ideal in $\mathbb{Q}$, das nicht endlich erzeugt ist, aber dennoch lokal ein Hauptideal ist. Da allerdings die Endlichkeitsbedingung aus 1.7c) nicht erfüllt ist, ist I nicht invertierbar.

1.11 Erinnerung Sei R ein Ring und $P \subset R$ ein Primideal

a) Die **Höhe** von P ist definiert als

$$\mathrm{ht}(P) := \dim(R_P) \in \mathbb{N}_0 \cup \infty.$$

Damit entspricht $\mathrm{ht}(P)$ der maximale Länge n einer Kette

$$P_0 \subsetneq P_1 \subsetneq \dots \subsetneq P_n = P$$

von Primidealen $P_i \in \mathrm{Spec}(R)$, welche mit P endet.

b) P ist **minimal** über einem Ideal $I \subseteq R$, wenn P ein minimales Element von $\mathcal{V}_{\mathrm{Spec}(R)}(I) = \{P \in \mathrm{Spec}(R) \mid I \subseteq P\}$ ist, d.h. $I \subseteq P$, aber kein echtes Unter-Primideal von P enthält I.

Wir können aus Proposition 1.7 Folgendes schließen:

1.12 Korollar [14.7] (Eigenschaften invertierbarer gebrochener Ideale)
Sei $I \in C(R)$ ein invertierbares gebrochenes Ideal in einem noetherschen Integritätsbereich R. Dann gilt:

a) Es existieren invertierbare, nicht-gebrochene Ideale $J_1, J_2 \subseteq R$ mit

$$I = J_1 \cdot J_2^{-1}.$$

b) Ist $I \subseteq R$ ein nicht-gebrochenes Ideal, dann hat jedes Primideal $P \in \operatorname{Spec}(R)$, welches über I minimal ist, Höhe 1.

c) Ist $I =: P$ ein Primideal von R, dann hat P Höhe 1 und R_P ist regulär.

Beweis:

zu a): Nach Prop. 1.7 ist I endlich erzeugt. Wenn $a \in R \setminus \{0\}$ ein gemeinsamer Nenner aller Elemente im Erzeugendensystem ist, dann gilt

$$J_1 := I \cdot (a)_R \subseteq R$$

und $I = J_1 \cdot (a)_R^{-1}$. Da

$$J_2 := (a)_R$$

und I invertierbar sind, trifft dies auch auf J_1 zu und wir erhalten $I = J_1 \cdot J_2^{-1}$.

zu b): Sei $P \in \operatorname{Spec}(R)$ minimal über I. Dann ist auch P_P minimal über I_P (Inklusionen bleiben unter Lokalisierung erhalten), was nach Prop. 1.7 ein Hauptideal ist. Somit gilt $\operatorname{ht}(P_P) \leq 1$ nach dem Hauptidealtheorem 7.4. Da $\{0\} \neq I \subseteq P_P$, muss die Höhe von P_P gleich 1 sein. Also gilt ht $(P) =$ ht (P_P), da Inklusionen unter Lokalisierung erhalten bleiben und die Höhe als die maximale Länge einer Kette von Primidealen, welche mit P beziehungsweise hier P_P endet, definiert war. Da $\operatorname{ht}(P_P) = 1$ gilt, folgt die Behauptung.

zu c): Nach Teil b) hat P Höhe 1 und somit $\dim(R_P) = 1$. Da R_P ein lokaler Ring ist, existiert genau ein Maximalideal und nach Prop. 1.7c) ist das Maximalideal von R_p daher ein Hauptideal und somit ist R_P regulär. □

Basierend auf diesem Korollar stellt man fest, dass Primideale von anderer Höhe als 1 nicht invertierbar sind. Die Frage ist nun, unter welchen Bedingungen alle Primideale der Höhe 1 invertierbar sind.
Nach obigem Korollar scheint eine notwendige Bedingung dafür Regularität mit Kodimension 1 zu sein (Dies beschreibt die Eigenschaft, dass R_P regulär ist für alle $P \in \operatorname{Spec}(R)$ mit $\operatorname{ht}(P) \leq 1$ (vgl. [Kem11], S. 209)). Da für einen normalen noetherschen Ring R gilt, dass R_P für alle $P \in \operatorname{Spec}(R)$ normal und somit regulär ist, wäre ein normaler noetherscher Integritätsbereich ein guter Kandidat.
Allerdings zeigt Beispiel 1.13 einen normalen noetherschen Integritätsbereich auf, der ein Primideal von Höhe 1 besitzt, das nicht invertierbar ist.

1.13 Beispiel Wir betrachten im Folgenden den Ring $R := \mathbb{Z}[x, \frac{x^2}{2}] \subset \mathbb{Q}[x]$.
Zunächst ist zu zeigen, dass R ein normaler noetherscher Integritätsbereich ist. Es gilt, dass R eine endlich erzeugte $\mathbb{Z}$-Unteralgebra von $\mathbb{Q}[x]$ ist und somit ist R ein noetherscher Integritätsbereich. Betrachte nun die Abbildung

$$\begin{aligned} \varphi: \ S := \mathbb{Z}[x, \sqrt{2x}] &\longrightarrow R, \\ x \longmapsto \tfrac{x^2}{2} \text{ und } \sqrt{2x} &\longmapsto x \end{aligned}$$

welche ein Isomorphismus von $\mathbb{Z}$-Algebren ist. Daher genügt es zu zeigen, dass S normal ist.
Betrachte daher ein $f \in \mathrm{Quot}(S)$ mit $f = a + b\sqrt{2x}$, wobei $a, b \in \mathbb{Q}(x)$. Sei nun f ganz über S, also $f \in \bar{S}$. Da S ganz über $\mathbb{Z}[x]$ ist, ist f auch ganz über $\mathbb{Z}[x]$ und daher gilt dies auch für $\hat{f} := a - b\sqrt{2x}$. Daraus folgt, dass $f + \hat{f} = 2a$ und $f \cdot \hat{f} = a^2 - 2b^2x$ auch ganz über $\mathbb{Z}[x]$ sind. Da $\mathbb{Z}[x]$ ganz abgeschlossen ist nach Proposition 8.8, folgt $2a \in \mathbb{Z}[x]$ und $4 \cdot f \cdot \hat{f} = (2a)^2 - 2x(2b)^2 \in 4\mathbb{Z}[x]$. Daraus folgt sowohl $2b \in \mathbb{Z}[x]$ als auch $(2a)^2 \in 2\mathbb{Z}[x]$, was wiederum impliziert, dass $2a$ gerade Koeffizienten hat und somit gilt $a \in \mathbb{Z}[x]$. Aus diesem Result kann man nun folgern, dass $2x(2b)^2 \in 4\mathbb{Z}[x]$ gilt und deshalb $b \in \mathbb{Z}$. Insgesamt folgt somit, dass $f \in S$ und daher ist S normal.
Im nächsten Schritt ist zu zeigen, dass das Ideal $P := (x, \frac{x^2}{2})_R$ ein Primideal von Höhe 1 ist. P ist der Schnitt von $(x)_{\mathbb{Q}[x]} \in \mathrm{Spec}(\mathbb{Q}[x])$ mit $R = \mathbb{Z}[x, \frac{x^2}{2}]$ und somit ist P ein Primideal. Weiterhin gilt, dass jedes Primideal $Q \in \mathrm{Spec}(R)$, welches $\frac{x^2}{2}$ enthält, auch x enthält und somit gilt $P \subseteq Q$. Daraus folgt, dass P minimal über dem Hauptideal $(\frac{x^2}{2})$ ist und nach 7.4 gilt daher $\mathrm{ht}(P) \leq 1$. Da $P \neq \{0\}$, folgt $\mathrm{ht}(P) = 1$.
Es bleibt zu zeigen, dass P nicht invertierbar ist. Sei dazu $f \in P^{-1}$. Dann gilt $x \cdot f \in R \subset \mathbb{Q}[x]$ und es folgt $f = \frac{a}{x} + g$ mit $a \in \mathbb{Q}, g \in \mathbb{Q}[x]$. Weiter gilt $\frac{a}{2} \cdot x + g \cdot \frac{x^2}{2} = f \cdot \frac{x^2}{2} \in R$ und daher ist a gerade und ein Element aus $\mathbb{Z}$. Dies liefert, dass die konstanten Koeffizienten von $x \cdot f$ und von $\frac{x^2}{2} \cdot f$ gerade sind. Somit haben alle Elemente von $P \cdot P^{-1}$ einen geraden konstanten Koeffizienten, woraus folgt, dass $P \cdot P^{-1} \neq R = \mathbb{Z}[x, \frac{x^2}{2}]$ gilt. Daher ist P nicht invertierbar.

Basierend auf obigem Beispiel schließen wir, das für das Gewünschte mehr Bedingungen erfüllt sein müssen.
Aus Proposition 8.8 ist bekannt, dass aus faktoriell normal folgt. Weiterhin liegt nach Prop. 8.10 die Eigenschaft, dass jede Lokalisierung nach einem Primideal faktoriell ist, genau zwischen den beiden, indem man die Äquivalenz zwischen der Normalität eines Integritätsbereiches R und der Normalität der Lokalisierung $R_\mathfrak{m}$ nach einem beliebigen Maximalideal $\mathfrak{m} \in \mathrm{Spec}_{max}(R)$ ausnutzt.
Ausgehend von diesen Überlegungen ergeben sich die nächsten Aussagen:

1.14 Definition Wir nennen einen Integritätsbereich R **lokal faktoriell**, wenn R_P faktoriell ist für jedes $P \in \mathrm{Spec}(R)$.

1.15 Theorem [14.8] (Invertierbare Ideale in einem lokal faktoriellem Ring)
Sei R ein noetherscher Integritätsbereich.

a) Wenn R lokal faktoriell ist, dann ist jedes Primideal der Höhe 1 von R invertierbar.

b) Wenn jedes Primideal der Höhe 1 von R invertierbar ist, dann gilt für ein Ideal $I \subseteq R$: I ist genau dann invertierbar, wenn I ein endliches Produkt von Primidealen der Höhe 1 ist. Dabei sei $I = R$ als leeres Produkt definiert.

1.16 Bemerkung Wir können nun ausnutzen, dass reguläre Ringe die Eigenschaft besitzen, dass ihre Lokalisierung nach einem Primideal einen regulären lokalen Ring liefert (vgl. Def. 13.2b)), welcher wiederum faktoriell ist (vgl. Anmerkung zu Kor. 13.6b)). Somit ist basierend auf Definition 1.14 jeder reguläre Ring lokal faktoriell.
Dies wurde für Ringe mit dim ≤ 1 gezeigt (vgl. [Kem11], S.207 beziehungsweise die Erläuterungen zu Kor. 13.6b)). Somit kann das Theorem 1.15 auf reguläre Bereiche angewandt werden.

Für den Beweis von Theorem 1.15 benötigen wir folgendes Lemma:

1.17 Lemma [14.9] Sei R ein noetherscher Integritätsbereich und $I \subseteq R$ ein Ideal $\neq (0)$, welches in einem invertierbaren Primideal P enthalten ist. Dann gilt

$$I \subsetneq I \cdot P^{-1} \subseteq R.$$

Beweis: Aus $I \subseteq P$ folgt $J := I \cdot P^{-1} \subseteq P \cdot P^{-1} = R$. Weiterhin gilt $I = J \cdot P \subseteq J$.
Angenommen es sei nun $I = J$. Dann gilt $I = P \cdot I$, was lokalisiert $I_P = P_P \cdot I_P$ ergibt. Nun kann man auf den lokalen Ring R_P mit zugehörigem Maximalideal P_P Nakayamas Lemma (7.3) anwenden, was $I_P = \{0\}$ liefert. Nachdem in R als noetherscher Integritätsbereich keine Nullteiler existieren, folgt $I = \{0\}$ im Widerspruch zur Annahme. □

Zum Beweis von Theorem 1.15:

zu a): Sei $Q \subset R$ ein beliebiges Primideal der Höhe 1 von R. Wir wenden nun Prop. 1.7 darauf an. Q ist als Ideal der Höhe 1 offensichtlich endlich erzeugt und als Primideal der Höhe 1 ungleich 0, daher müssen wir nur noch zeigen, dass $Q_P \subseteq R_P$ ein Hauptideal ist für alle $P \in \text{Spec}\,(R)$ und dann folgt mit Prop. 1.7a), dass Q invertierbar ist.
Falls $Q \nsubseteq P$, dann enthält Q Elemente, die in R_P invertierbar sind und somit ist $Q_P = (1)_{R_P}$ ein Hauptideal.
Andererseits, falls $Q \subseteq P$ gilt, dann folgt aus Theorem 6.5, dass Q_P ein Primideal von R_P ist von Höhe 1. Da R lokal faktoriell und somit R_P faktoriell ist, folgt nach Lemma 5.14, dass Q_P auch in diesem Fall ein Hauptideal ist.

zu b): „$\Leftarrow$“: Dies folgt direkt aus der Annahme.

„$\Rightarrow$“: Nutze für diese Richtung Noethersche Induktion. Wir nehmen an, dass ein invertierbares Ideal I existiert, welches kein Produkt von Primidealen der Höhe 1 ist. Aufgrund der Noethereigenschaft von R können wir I so wählen, dass es unter allen Gegenbeispielen maximal ist. R selbst ist kein Gegenbeispiel und daher gilt $I \neq R$ und es existiert ein Primideal $P \in \text{Spec}\,(R)$, das über I minimal ist. Nach Korollar 1.12 b) hat P Höhe 1 und ist daher nach 1.15a) invertierbar. Mit Lemma 1.17 erhalten wir

$$I \subsetneq J := I \cdot P^{-1} \subseteq R.$$

Da I invertierbar ist, ist es auch J. Aus der Maximalität von I folgt, dass J eine Produkt von Primidealen von Höhe 1 ist. Daher gilt dies auch für $I = J \cdot P$ und es folgt die Behauptung.

□

1.18 Proposition [14.10] (Eindeutige Faktorisierung von invertierbaren Idealen)
Sei R ein Integritätsbereich und $I \subseteq R$ ein invertierbares Ideal, welches die Zerlegung

$$I = P_1 \cdot \ldots \cdot P_n$$

in Primideale P_i mit $i = 1, \ldots, n$ besitzt. Dabei tritt der Fall $n = 0$ auf, wenn $I = R$ gilt. Diese Faktorisierung ist dann eindeutig bis auf Permutation.

Beweis: Der Beweis erfolgt per Induktion nach n. Sei dazu $I = Q_1 \cdot \ldots \cdot Q_m$ eine weitere Faktorisierung von I mit $Q_j \in \text{Spec}(R)$ mit $j = 1, \ldots, m$.

$n = 0$ Dann gilt auch $m = 0$, da sonst $I \subseteq Q_1 \subsetneq R = I$ gelten würde.

$n > 0$ Nach Umnummerierung können wir annehmen, dass P_1 unter den P_i minimal ist. Wegen $I \subseteq P_1$, gilt $I = Q_1 \cdot \ldots \cdot Q_m \subseteq P_1$. Aus der Primidealeigenschaft folgt, dass ein j existiert, sodass $Q_j \subseteq P_1$. Nach Umnummerierung können wir hier annehmen, dass $j = 1$ und $Q_1 \subseteq P_1$.
Da ebenfalls $P_1 \cdot \ldots \cdot P_n \subseteq Q_1$ gilt, existiert ein i, sodass $P_i \subseteq Q_1$ und damit $P_i \subseteq Q_1 \subseteq P_1$. Aus der Minimalität von P_1 folgt $P_1 = Q_1$.
Da I invertierbar ist, sind auch alle P_i und Q_j invertierbar. Multiplizieren von

$$I = P_1 \cdot \ldots \cdot P_n = Q_1 \cdot \ldots \cdot Q_m$$

mit $P_1^{-1} = Q_1^{-1}$ liefert $P_2 \cdot \ldots \cdot P_n = Q_2 \cdot \ldots \cdot Q_m$ und per Induktion folgt $n = m$ sowie $P_i = Q_j$ nach einer geeigneten Permutation der Indizes. □

Sei nun R ein lokal faktorieller, noetherscher Integritätsbereich oder allgemeiner ein noetherscher Integritätsbereich, in dem alle Primideale der Höhe 1 invertierbar sind. Wir können dann Theorem 1.15b) und Proposition 1.18 auf invertierbare gebrochene Ideale erweitern:

1.19 Korollar Sei $\mathcal{M} \subseteq \operatorname{Spec}(R)$ die Menge aller Primideale der Höhe 1 von R. Dann ist ein gebrochenes Ideal I genau dann invertierbar, wenn es eine Darstellung

$$I = \prod_{Q \in \mathcal{M}} Q^{e_{I,Q}} \tag{1}$$

mit $e_{I,Q} \in \mathbb{Z}$ besitzt, bei welcher alle bis auf endlich viele $e_{I,Q}$ gleich 0 sind. Dabei sind die $e_{I,Q}$ eindeutig.

Beweis:

„$\Rightarrow$“ Sei also $I \subseteq \operatorname{Quot}(R)$ ein invertierbares gebrochenes Ideal. Dann gilt nach Korollar 1.10a) und Theorem 1.15b), dass I als endliches Produkt von Primidealen der Höhe 1 und Inversen von Primidealen der Höhe 1 geschrieben werden kann. Dies liefert insbesondere, dass $e_{I,Q} \in \mathbb{Z}$ sowie die Endlichkeit des Produkts.

„$\Leftarrow$“ Es habe nun ein gebrochenes Ideal $I \subseteq \operatorname{Quot}(R)$ die Darstellung $I = \prod_{Q \in \mathcal{M}} Q^{e_{I,Q}}$ mit $e_{I,Q} \in \mathbb{Z}$. Nach Voraussetzung ist R ein lokal faktorieller, noetherscher Integritätsbereich beziehungsweise ein noetherscher Integritätsbereich, in dem alle Primideale der Höhe 1 invertierbar sind. Somit sind alle $Q \in \mathcal{M}$ invertierbar unter Verwendung von 1.15b) beziehungsweise der Voraussetzung. Weiterhin ist bekannt, dass die invertierbaren gebrochenen Ideale die Gruppe $C(R)$ bilden und somit folgt aus der Invertierbarkeit der einzelnen Faktoren nach der Gruppeneigenschaft auch die Invertierbarkeit des Produkts und somit von I.

Nach Proposition 1.18 folgt, dass die $e_{I,Q}$ eindeutig sind. Würden zwei verschiedene Faktorisierungen existieren, so könnte man beide mit Primidealen der Höhe 1 multiplizieren bis man zwei Zerlegungen eines nicht-gebrochenen Ideals erreicht. Dies würde allerdings Proposition 1.18 widersprechen. □

1.20 Bemerkung

a) Es gilt, dass $I \subseteq R$ genau dann, wenn alle $e_{I,Q} \geq 0$.

Beweis:

„$\Leftarrow$" Sei $I = Q_1^{e_{I,Q_1}} \cdot \ldots \cdot Q_n^{e_{I,Q_n}}$ eine Zerlegung von I, wobei $n \in \mathbb{N}$. Da die Zerlegung eindeutig ist, gilt $Q_i \neq Q_j$ für $i \neq j$ und insbesondere $Q_i^{e_{I,Q_i}} \neq Q_j^{e_{I,Q_j}}$ für $i \neq j$ Da $e_{I,Q_i} \geq 0$ für alle i, folgt $Q_i^{e_{I,Q_i}} \subseteq R$ und damit insgesamt $I \subseteq R$.

„$\Rightarrow$" Sei $I \subseteq R$. Angenommen es existiert eine Zerlegung von I mit

$$I = Q_1^{e_{I,Q_1}} \cdot \ldots \cdot Q_n^{e_{I,Q_n}},$$

wobei $e_{I,Q_i} < 0$ für gewisse i gelte. Sei dies ohne Einschränkung $i = 1$, also $e_{I,Q_1} < 0$. Schreibe dann I als

$$I = \frac{1}{Q_1^{e_{I,Q_1}}} \cdot \ldots \cdot Q_n^{e_{I,Q_n}}.$$

Dann ist $\frac{1}{Q_1^{e_{I,Q_1}}} \subseteq \mathrm{Quot}(R)$ und damit insgesamt $I \subseteq \mathrm{Quot}(R)$, was im Widerspruch steht zur Voraussetzung. $\square$

b) Multipliziert man zwei invertierbare gebrochene Ideale, so werden die zugehörigen Exponenten in (1) addiert, denn für $I = \prod_{Q \in \mathcal{M}} Q^{e_{I,Q}}$ und $J = \prod_{Q \in \mathcal{M}} Q^{e_{J,Q}}$ mit $e_{I,Q}, e_{J,Q} \in \mathbb{Z}$ gilt

$$I \cdot J = \prod_{Q \in \mathcal{M}} Q^{e_{I,Q}} \cdot \prod_{Q \in \mathcal{M}} Q^{e_{J,Q}} = \prod_{Q \in \mathcal{M}} Q^{e_{I,Q}+e_{J,Q}}.$$

1.21 Definition Für einen beliebigen Ring R ist $\mathrm{Div}(R)$, die Gruppe der **Weil-Divisoren**, definiert als die freie abelsche Gruppe, welche von Primidealen der Höhe 1 erzeugt wird.
Im Gegensatz zu $C(R)$ wird die Gruppe der Weil-Divisoren üblicherweise additiv geschrieben, da ein Weil-Divisor D eine „formale" $\mathbb{Z}$-linear Kombination von Primidealen der Höhe 1 ist, d.h

$$D = \sum_{Q \in \mathcal{M}} n_q Q$$

mit $n_q \in \mathbb{Z}$.
Insbesondere wenn R der Koordinatenring einer affinen Kurve ist, kann ein Weil-Divisor als eine formale $\mathbb{Z}$-linear Kombination von Punkten geschrieben werden.

1.22 Bemerkung In diesem Kontext wird ein invertierbares gebrochenes Ideal I eines Integritätsbereiches R **Cartier-Divisor** genannt und $C(R)$ ist die Gruppe der Cartier-Divisoren. Damit erklärt sich auch die Verwendung des Buchstaben C. (Die übliche Notation von Cartier-Divisoren ist allerdings eine andere. Vergleiche dazu [Har77], S.141.)

1.23 Ausblick Ist R ein lokal faktorieller, noetherscher Integritätsbereich (oder allgemeiner ein noetherscher Integritätsbereich, in dem alle Primideale der Höhe 1 invertierbar sind), erhalten wir nach Obigem einen Isomorphismus

$$\varphi : C(R) \longrightarrow \mathrm{Div}(R),\ I \longmapsto \sum_{Q \in \mathcal{M}} e_{I,Q} \cdot Q.$$

Dabei ist φ surjektiv, da nach Kor. 1.19 und der Darstellung (1) für alle $D \in \mathrm{Div}(R)$ ein $I \in C(R)$ existiert mit $\varphi(I) = D = \sum_{Q \in \mathcal{M}} e_{I,Q} \cdot Q$. Weiterhin folgt die Injektivität von φ aus der Eindeutigkeit der $e_{I,Q}$.
Indem wir diesen Isomorphismus benutzen, können wir davon sprechen, dass ein Weil-Divisor zu einem invertierbaren Ideal oder einem Element $a \in R \setminus \{0\}$ assoziiert ist. Bei letzterem nutzen wir, dass für ein $a \neq 0$ das davon erzeugte Hauptideal $(a)_R$ Höhe 1 hat und gilt $(a)_R = \prod_{i=1}^{n} P_i^{e_i}$ für P_i Primideale der Höhe 1 und $e_i \in \mathbb{Z}$.

Literatur

[Har77] Hartshorne, Robin. *Algebraic Geometry.* New York [u.a.]: Springer-Verlag, 1977.

[Kem11] Kemper, Gregor. *A Course in Commutative Algebra. Graduate Texts in Mathematics*, Vol. 256. Heidelberg [u.a.]: Springer-Verlag, 2011.

[Neu92] Neukirch, Jürgen. *Algebraische Zahlentheorie* Berlin [u.a.]: Springer-Verlag, 1992.