Dedekindringe in Funktionenkörpern

Vorlesung Algebraische Kurven SS2006

F. Heß

17. Juli 2006

In diesem Text sei F/k ein algebraischer Funktionenkörper in einer Variablen über dem exakten Konstantenkörper k . Mit $\mathbb{P}_F$ wird die Menge der Stellen von F bezeichnet. Die folgende Diskussion enthält ungefähr Abschnitt III.2 in Stichtenoth und beleuchtet dazu wesentlich genauer als dort die Verbindung zu Dedekindringen und algebraischen Kurven.

1 Dedekindringe in Funktionenkörpern

1 Lemma. Sei R ein Teilring von F mit $k \subseteq R$ und $R \subseteq \mathcal{O}_P$ für eine Stelle P von F . Dann ist $P \cap R$ ein maximales Ideal von R .

Beweis. Sei $\mathfrak{m} = P \cap R$. Die Einbettung $R \rightarrow \mathcal{O}_P$ verlängert sich zu $R \rightarrow \mathcal{O}_P/P$ und liefert eine Einbettung $R/\mathfrak{m} \rightarrow \mathcal{O}_P/P$. Mit $\mathcal{O}_P/P$ ist $R/\mathfrak{m}$ eine endliche Ringerweiterung von k und als solche (nach dem Satz, daß ganze Erweiterungen von Körpern wieder Körper sind) ein Körper. Also ist $\mathfrak{m}$ maximal. $\square$

2 Definition. Sei S eine Menge von Stellen. Dann definieren wir $\mathcal{O}_S = \bigcap_{P \in S} \mathcal{O}_P$ als den Ring der an den Stellen aus S ganzen Elemente, wobei der leere Schnitt gleich F gesetzt wird.

Man nennt die Ringe $\mathcal{O}_S$ auch Holomorphieringe. Ist $S = \mathbb{P}_F$ so gilt $\mathcal{O}_S = k$.

3 Lemma. Für $S, T \subseteq \mathbb{P}_F$ gilt $\mathcal{O}_S \subseteq \mathcal{O}_T$ genau dann, wenn $S \supseteq T$ ist.

Beweis. Für $S \supseteq T$ folgt $\mathcal{O}_S \subseteq \mathcal{O}_T$ direkt aus der Definition. Sei nun $\mathcal{O}_S \subseteq \mathcal{O}_T$ und $P \in T$. Falls $P \notin S$, so gibt es für ausreichend großes $m \in \mathbb{Z}$ ein $x \in \mathcal{L}(mP) \setminus k$. Dann gilt $x \in \mathcal{O}_S$ und $x \notin \mathcal{O}_T$, im Widerspruch zur Voraussetzung. Also ergibt sich $P \in S$. $\square$

Wir untersuchen nun den Bezug der Primideale von $\mathcal{O}_S$ zu den Stellen aus S . Für ein maximales Ideal $\mathfrak{m}$ von $\mathcal{O}_S$ bezeichnen wir die Lokalisierung $\mathcal{O}_S[(\mathcal{O}_S \setminus \mathfrak{m})^{-1}]$ mit $\mathcal{O}_{S,\mathfrak{m}}$.

4 Lemma. (i) Sei S eine Menge von Stellen mit $S \neq \mathbb{P}_F$ und P eine Stelle mit $\mathcal{O}_S \subseteq \mathcal{O}_P$. Dann ist $\mathfrak{m} = P \cap \mathcal{O}_S$ ein maximales Ideal von $\mathcal{O}_S$ und es gilt $\mathcal{O}_P = \mathcal{O}_{S,\mathfrak{m}}$, $P = \mathcal{O}_{S,\mathfrak{m}}\mathfrak{m}$ sowie $\mathcal{O}_P/P \cong \mathcal{O}_S/\mathfrak{m}$.

(ii) Sei S eine Menge von Stellen mit $S \neq \emptyset$ und $S \neq \mathbb{P}_F$ und $\mathfrak{m}$ ein maximales Ideal von $\mathcal{O}_S$. Dann gibt es eine Stelle $P \in S$ mit $\mathcal{O}_S \subseteq \mathcal{O}_P$ und $\mathfrak{m} = P \cap \mathcal{O}_S$.

Beweis. (i): Nach Lemma 1 wissen wir bereits, daß $\mathfrak{m}$ ein maximales Ideal von $\mathcal{O}_S$ ist.

Zum Beweis von $\mathcal{O}_P = \mathcal{O}_{S,\mathfrak{m}}$ bemerken wir zunächst $\mathcal{O}_P \supseteq \mathcal{O}_{S,\mathfrak{m}}$, da $\mathcal{O}_S \setminus \mathfrak{m} \subseteq \mathcal{O}_P \setminus P = \mathcal{O}_P^\times$ gilt. Zum Beweis der anderen Inklusion sei $x \in \mathcal{O}_P$. Nach dem starken Approximationssatz gibt es $y \in \mathcal{O}_S$ mit $v_P(y) = 0$ und $v_Q(y) = -v_Q(x)$ für alle Stellen $Q \in S$ mit $v_Q(x) < 0$. Dann gilt $xy \in \mathcal{O}_S$ und $y \notin \mathfrak{m}$ wegen $y \notin P$. Folglich $x \in \mathcal{O}_{S,\mathfrak{m}}$, $\mathcal{O}_P = \mathcal{O}_{S,\mathfrak{m}}$ und $P = \mathcal{O}_{S,\mathfrak{m}}\mathfrak{m}$, weil $\mathcal{O}_{S,\mathfrak{m}}\mathfrak{m}$ das maximale Ideal von $\mathcal{O}_{S,\mathfrak{m}} = \mathcal{O}_P$ ist.

Da Lokalisieren und Faktorisieren vertauschen und $\mathcal{O}_S/\mathfrak{m}$ ein Körper ist, folgt $\mathcal{O}_P/P \cong \mathcal{O}_S/\mathfrak{m}$. Diese Isomorphie kann man aber auch wie folgt beweisen: Der Homomorphismus $\phi : \mathcal{O}_S \rightarrow \mathcal{O}_P/P$ liefert eine Einbettung $\mathcal{O}_S/\mathfrak{m} \rightarrow \mathcal{O}_P/P$. Zu zeigen bleibt daher, daß ϕ surjektiv ist. Sei $x \in \mathcal{O}_P$. Wegen $\mathcal{O}_S \subseteq \mathcal{O}_P$ gilt $P \in S$ nach Lemma 3 (also auch $S \neq \emptyset$). Daher und wegen $S \neq \mathbb{P}_F$ können wir nach dem starken Approximationssatz ein $y \in \mathcal{O}_S$ mit $v_P(x - y) \geq 1$ finden. In $\mathcal{O}_P$ gilt dann $y \in x + P$ und damit $x = \phi(y)$. Also ist ϕ surjektiv.

(ii): Wegen des starken Approximationssatzes gibt es für $Q \in S$ ein $x \in \mathcal{O}_S$ mit $v_Q(x) = 1$. Dann folgt $x^{-1} \notin \mathcal{O}_S$ und $\mathcal{O}_S$ ist kein Körper. Daher gilt $\mathfrak{m} \neq \{0\}$. Nach Theorem I.1.18 in Stichtenoth und Lemma 3 existiert dann eine Stelle $P \in S$ mit $\mathcal{O}_S \subseteq \mathcal{O}_P$ und $\mathfrak{m} \subseteq P$. Da $P \cap \mathcal{O}_S$ ein maximales Ideal von $\mathcal{O}_S$ ist, welches $\mathfrak{m}$ enthält, folgt $P \cap \mathcal{O}_S = \mathfrak{m}$. $\square$

Zur Erinnerung: Sei R ein Dedekindring und $\mathfrak{p}$ ein Primideal von R . Für $x \in \text{Quot}(R)$ sei $v_{\mathfrak{p}}(x) \in \mathbb{Z}$ der genaue Exponent von $\mathfrak{p}$ in der Primidealfaktorisierung von Rx . Dies liefert eine diskrete, surjektive Bewertung auf $\text{Quot}(R)$. Die gebrochenen Ideale von R bilden eine freie, abelsche Gruppe $\mathcal{I}$. Die gebrochenen Hauptideale bilden eine Untergruppe $\mathcal{P}$ von $\mathcal{I}$. Die Klassengruppe oder Picardgruppe von R ist $\text{Pic}(R) = \mathcal{I}/\mathcal{P}$.

5 Satz. Sei S eine Menge von Stellen mit $S \neq \emptyset$ und $S \neq \mathbb{P}_F$.

- (i) Der Ring $\mathcal{O}_S$ ist ein Dedekindring mit $\text{Quot}(\mathcal{O}_S) = F$.
- (ii) Die Abbildung $P \mapsto P \cap \mathcal{O}_S$ liefert eine bijektive Abbildung von S auf die Menge der Primideale von $\mathcal{O}_S$ mit der Inversen $\mathfrak{m} \mapsto \mathcal{O}_{S,\mathfrak{m}}$ und es gilt $\mathcal{O}_P/P \cong \mathcal{O}_S/(P \cap \mathcal{O}_S)$. Die Bewertung v_P stimmt mit der durch $P \cap \mathcal{O}_S$ definierten Bewertung $v_{P \cap \mathcal{O}_S}$ auf F überein.

Sei T eine weitere Menge von Stellen mit $T \neq \emptyset$, $T \neq \mathbb{P}_F$ und $T \subseteq S$.

- (iii) Ist I ein Ideal von $\mathcal{O}_S$ und $I = \prod_{P \in S} (P \cap \mathcal{O}_S)^{e_P}$ die Primidealfaktorisierung von I in $\mathcal{O}_S$, so ist $\mathcal{O}_T I = \prod_{P \in T} (P \cap \mathcal{O}_T)^{e_P}$ die Primidealfaktorisierung von $\mathcal{O}_T I$ in $\mathcal{O}_T$.

Ist J ein Ideal von $\mathcal{O}_T$ und $J = \prod_{P \in T} (P \cap \mathcal{O}_T)^{e_P}$ die Primidealfaktorisierung von J in $\mathcal{O}_T$, so ist $J \cap \mathcal{O}_S = \prod_{P \in T} (P \cap \mathcal{O}_S)^{e_P}$ die Primidealfaktorisierung von $J \cap \mathcal{O}_S$ in $\mathcal{O}_S$.

- (iv) Die Abbildungen $\phi : I \mapsto \mathcal{O}_T I$ und $\psi : J \mapsto J \cap \mathcal{O}_S$ sind multiplikativ und erfüllen $\phi \circ \psi = \text{id}$. Für $P \in S$ gilt $\phi(P \cap \mathcal{O}_S) = P \cap \mathcal{O}_T$, falls $P \in T$, und $\phi(P \cap \mathcal{O}_S) = \mathcal{O}_T$ andernfalls.
- (v) Die Abbildungen $\phi : I \mapsto \mathcal{O}_T I$ setzt sich zu einem Epimorphismus $\phi : \mathcal{I}_S \rightarrow \mathcal{I}_T$ der Gruppen der gebrochenen Ideale $\mathcal{I}_S$ von $\mathcal{O}_S$ und $\mathcal{I}_T$ von $\mathcal{O}_T$ fort und liefert einen Epimorphismus $\text{Pic}(\mathcal{O}_S) \rightarrow \text{Pic}(\mathcal{O}_T)$.

Beweis. (i): Nach Lemma 4, (ii) ist $\mathcal{O}_{S,\mathfrak{m}}$ für jedes maximale Ideal $\mathfrak{m}$ von $\mathcal{O}_S$ der Bewertungsring einer Stelle. Daher folgt $\text{Quot}(\mathcal{O}_S) = \text{Quot}(\mathcal{O}_{S,\mathfrak{m}}) = F$ nach Definition I.1.4 in Stichtenoth.

Zum Beweis, daß $\mathcal{O}_S$ ein Dedekindring ist, verwenden wir die folgende Aussage. Ein noetherscher Integritätsring R ist genau dann ein Dedekindring, wenn $R_{\mathfrak{m}}$ ein diskreter Bewertungsring für alle maximalen Ideale $\mathfrak{m}$ von R ist. Es ist klar, daß Dedekindringe diese Eigenschaft erfüllen. Umgekehrt bleibt nach Algebra 2 zu zeigen, daß R die Dimension 1 hat. Sei $\mathfrak{p} \neq 0$ ein Primideal von R und $\mathfrak{m}$ ein maximales Ideal von R mit $\mathfrak{p} \subseteq \mathfrak{m}$. Dann ist $R_{\mathfrak{m}}\mathfrak{p}$ ein Primideal von $R_{\mathfrak{m}}$ mit $R_{\mathfrak{m}}\mathfrak{p} \neq 0$, wie man direkt nachrechnet. Da $R_{\mathfrak{m}}$ ein diskreter Bewertungsring ist, gilt $R_{\mathfrak{m}}\mathfrak{p} = R_{\mathfrak{m}}\mathfrak{m}$, und hieraus ergibt sich $\mathfrak{p} = \mathfrak{m}$, wie man ebenfalls leicht nachrechnet. Also sind Primideale maximal und es gilt $\dim(R) = 1$.

Um diese Aussage auf $R = \mathcal{O}_S$ anzuwenden, müssen wir jetzt nur noch zeigen, daß $\mathcal{O}_S$ noethersch ist. Seien $0 \neq I_1 \subseteq I_2 \subseteq \dots$ eine aufsteigende Kette von Idealen in $\mathcal{O}_S$. Es gibt nur endlich viele maximale Ideale $\mathfrak{m}$ von $\mathcal{O}_S$ mit $\mathfrak{m} \supseteq I_1$, denn sonst gäbe es Elemente $\neq 0$ in $I_1 \subseteq F$ mit unendlich

vielen Nullstellen. Wir bezeichnen die Menge dieser $\mathfrak{m}$ mit M . Für jedes $\mathfrak{m}$ wird die Kette $\mathcal{O}_{S,\mathfrak{m}}I_1 \subseteq \mathcal{O}_{S,\mathfrak{m}}I_2 \subseteq \dots$ stationär, denn $\mathcal{O}_{S,\mathfrak{m}}$ ist noethersch. Sei $i \in \mathbb{Z}$, so daß $\mathcal{O}_{S,\mathfrak{m}}I_j = \mathcal{O}_{S,\mathfrak{m}}I_i$ für alle $j \geq i$ und alle $\mathfrak{m} \in M$ gilt. Für alle maximalen Ideale $\mathfrak{n}$ von $\mathcal{O}_S$ mit $\mathfrak{n} \notin M$ gilt dazu $\mathcal{O}_{S,\mathfrak{n}}I_j = \mathcal{O}_{S,\mathfrak{n}}I_i = \mathcal{O}_{S,\mathfrak{n}}$. Es folgt $I_j = I_i$ in $\mathcal{O}_S$ für alle $j \geq i$ und $\mathcal{O}_S$ ist noethersch.

Insgesamt ergibt sich, daß $\mathcal{O}_S$ ein Dedekindring ist.

(ii): Sei $\phi : P \mapsto P \cap \mathcal{O}_S$ und $\psi : \mathfrak{m} \mapsto \mathcal{O}_{S,\mathfrak{m}}\mathfrak{m}$. Nach Lemma 4, (i) folgt $\psi \circ \phi = \text{id}$. Die Surjektivität von ϕ ergibt sich aus (i), da damit jedes Primideal maximal ist, und aus Lemma 4, (ii). Die Aussage über die Bewertungen folgt, da die Bewertungen bezüglich des Primideals $\mathfrak{m} = P \cap \mathcal{O}_S$ von $\mathcal{O}_S$ und des diskreten Bewertungsrings $\mathcal{O}_{S,\mathfrak{m}}$ gleich sind und letztere gerade die Bewertung der Stelle P ist.

(iii): Die erste Aussage folgt aus Teil (iv) (ohne „ $\phi \circ \psi = \text{id}$ “) und der eindeutigen Faktorisierung in Primideale.

Die zweite Aussage folgt mit Hilfe von Bewertungsbetrachtungen. Für $x \in F$ gilt $x \in J$ genau dann, wenn $v_P(x) \geq e_P$ für alle $P \in T$. Damit $x \in J \cap \mathcal{O}_S$ genau dann, wenn $v_P(x) \geq e_P$ für alle $P \in T$ und $v_P(x) \geq 0$ für alle $P \in S \setminus T$. Dies gilt wiederum genau dann, wenn $x \in \prod_{P \in T} (P \cap \mathcal{O}_S)^{e_P}$ ist.

(iv): Die Multiplikativität von ψ folgt aus der zweiten Aussage von (iii) und der eindeutigen Faktorisierung in Primideale.

Die Multiplikativität von ϕ ist unmittelbar einsichtig.

Sei $P \in S$ und $I = P \cap \mathcal{O}_S$. Falls $P \in T$, so gilt $I \subseteq \mathcal{O}_T I \cap \mathcal{O}_S$ wegen $I \subseteq \mathcal{O}_S$, und $\mathcal{O}_T I \cap \mathcal{O}_S \subseteq P \cap \mathcal{O}_S = I$ wegen $\mathcal{O}_P(\mathcal{O}_T I) = \mathcal{O}_P I = P$ und damit $\mathcal{O}_T I \subseteq P$. Es folgt $\mathcal{O}_T I \cap \mathcal{O}_S = I$. Wegen der Multiplikativität von ψ beziehungsweise der zweiten Aussage von (iii) folgt $\mathcal{O}_T I = P \cap \mathcal{O}_T$, wie gewünscht.

Falls $P \notin T$, so sei $\mathfrak{m}$ ein maximales Ideal von $\mathcal{O}_T$ mit $\mathfrak{m} \supseteq \mathcal{O}_T I$. Dann gibt es eine Stelle $Q \in T$ mit $\mathfrak{m} \subseteq Q$, also $I = P \cap \mathcal{O}_S \subseteq Q \cap \mathcal{O}_S$. Da sowohl $P \cap \mathcal{O}_S$ als auch $Q \cap \mathcal{O}_S$ maximale Ideale sind, folgt $P \cap \mathcal{O}_S = Q \cap \mathcal{O}_S$. Nach Lemma 4, (i) folgt $P = Q$ und $P \in T$ wegen $Q \in T$, im Widerspruch zur Annahme. Also gibt es kein maximales Ideal $\mathfrak{m}$ von $\mathcal{O}_T$ mit $\mathfrak{m} \supseteq \mathcal{O}_T I$ und es folgt $\mathcal{O}_T I = \mathcal{O}_T$, wie gewünscht.

Damit ist auch die erste Aussage in (iii) bewiesen.

Schließlich folgt $\phi \circ \psi = \text{id}$ aus den beiden Aussagen von (iii).

(v): Klar mit (iii) und (iv), und da ϕ Hauptideale auf Hauptideale abbildet. $\square$

6 Satz. *Sei S eine endliche Menge von Stellen. Dann ist der Dedekindring $\mathcal{O}_S$ ein Hauptidealring.*

Beweis. Sei $I = \prod_{P \in S} (P \cap \mathcal{O}_S)^{e_P}$ die Primfaktorisierung von I . Nach dem schwachen Approximationssatz gibt es $x \in \mathcal{O}_S$ mit $v_P(x) = e_P$ für alle $P \in S$. Dann gilt $I = \mathcal{O}_S x$. Denn für $y \in I$ ist $v_P(y/x) \geq 0$ für alle $P \in S$, also $y/x \in \mathcal{O}_S$. $\square$

Ein Ring R heißt semilokal, wenn er nur endlich viele maximale Ideale besitzt. Da der schwache Approximationssatz allgemein für Dedekindringe R gilt, sind semilokale Dedekindringe R Hauptidealringe.

2 Divisoren von Funktionenkörpern und Ideale in Dedekindringen

Wir wollen jetzt Divisoren D und Riemann-Roch-Räume $\mathcal{L}(D)$ mit Hilfe der Dedekindringe $\mathcal{O}_S$ und gebrochener Ideale darstellen. Wegen $\mathcal{O}_{\mathbb{P}_F} = k$ ist es leider nicht möglich, sämtliche Stellen als Primideale eines $\mathcal{O}_S$ darzustellen. Für $S_1, S_2 \subsetneq \mathbb{P}_F$ mit $S_1 \cup S_2 = \mathbb{P}_F$ und $S_1 \cap S_2 = \emptyset$ können wir aber jede Stelle nach Satz 5 durch genau ein Primideal in einem der Ringe $\mathcal{O}_{S_1}$ und $\mathcal{O}_{S_2}$ darstellen.

Seien $\mathcal{D}_F$ die Gruppe der Divisoren von F und $\mathcal{I}_1, \mathcal{I}_2$ die Idealgruppen von $\mathcal{O}_{S_1}$ und $\mathcal{O}_{S_2}$. Wir definieren $\phi : \mathcal{D}_F \rightarrow \mathcal{I}_1 \times \mathcal{I}_2$ durch $\sum_P e_P P \mapsto (\prod_{P \in S_1} (P \cap \mathcal{O}_{S_1})^{e_P}, \prod_{P \in S_2} (P \cap \mathcal{O}_{S_2})^{e_P})$. Wegen der Dedekindringeneigenschaft und der eindeutigen Korrespondenz der Stellen zu Primidealen in $\mathcal{O}_{S_1}$ und $\mathcal{O}_{S_2}$ ist ϕ ein Isomorphismus. Das Bild der Gruppe der Hauptdivisoren ist aber beispielsweise nicht gleich dem Produkt der Gruppen der Hauptideale von $\mathcal{O}_{S_1}$ und $\mathcal{O}_{S_2}$. Seien I_1, I_2 Ideale mit $(I_1, I_2) = \phi(D)$. Aufgrund der Definitionen und unter Betrachtung der Bewertungsbedingungen ergibt sich schließlich $\mathcal{L}(D) = I_1^{-1} \cap I_2^{-1}$.

Um die etwas künstliche Aufteilung $\mathbb{P}_F = S_1 \cup S_2$ zu vermeiden, geht man wie folgt vor. Wir setzen $X = \mathbb{P}_F$ und betrachten zunächst „offene, affine“ Mengen U mit $0 < \#(X \setminus U) < \infty$ (vormals mit S bezeichnet). Wir erhalten eine Schaar von „echten“ Dedekindringen $\mathcal{O}_X : U \mapsto \mathcal{O}_U = \bigcap_{P \in U} \mathcal{O}_P$ und allgemeiner zu einem Divisor D eine Schaar von (gebrochenen) Idealen $\mathcal{O}_X(D) : U \mapsto \prod_{P \in U} (P \cap \mathcal{O}_U)^{-v_P(D)}$, die man praktischerweise gleich invertiert. Es gilt $\mathcal{O}_X(\cup_i U_i) = \bigcap_i \mathcal{O}_X(U_i)$ und allgemeiner $\mathcal{O}_X(D)(\cup_i U_i) = \bigcap_i \mathcal{O}_X(D)(U_i)$ wegen Satz 5 (beziehungsweise unter Beachtung der Tatsache, daß sich Bewertungsbedingungen in Schnitten mit „und“ verknüpfen), sofern $\cup_i U_i \neq X$, da sonst die linke Seite nicht definiert ist. Für $\cup_i U_i = X$ nehmen wir dies als Möglichkeit, $\mathcal{O}_X(X)$ und $\mathcal{O}_X(D)(X)$ zu definieren. Dann gilt $\mathcal{O}_X(X) = k$ und $\mathcal{O}_X(D)(X) = \mathcal{L}(D)$. Wir beschreiben den Funktionenkörper F und insbesondere Divisoren D durch die Schaaren $\mathcal{O}_X$ und $\mathcal{O}_X(D)$.

3 Verbindungen zu algebraischen Kurven

Punktmengen. Der Koordinatenring $k[C]$ einer irreduziblen glatten affinen Kurve C über einem algebraisch abgeschlossenen Körper k ist ein Dedekindring und die Primideale von $k[C]$ entsprechen den Punkten von C . Ist $F = k(C)$ der Funktionenkörper von C und $X = \mathbb{P}_F$, so gilt $k[C] = \mathcal{O}_X(U)$ für $U = \{P \in X \mid k[C] \subseteq \mathcal{O}_P\}$ aufgrund der Dedekindringeigenschaft von $k[C]$. Also entsprechen auch die Stellen in U den Punkten von C .

Umgekehrt können wir die Stellen in U beziehungsweise die Primideale jedes $\mathcal{O}_X(U)$ mit $0 < \#(X \setminus U) < \infty$ als Punkte einer affinen Kurve C wie folgt auffassen. Nach dem starken Approximationssatz gibt es $x \in F$ mit $v_P(x) \geq 0$ für alle $P \in U$ und $v_P(x) < 0$ für alle $P \in X \setminus U$. Ohne Beweis merken wir an, daß x so gewählt werden kann, daß $F/k(x)$ separabel ist. Nach Satz 7 und Satz 9 wissen wir dann $\text{Cl}(k[x], F) = \mathcal{O}_X(U)$ und $\text{Cl}(k[x], F) = k[x, \omega_1, \dots, \omega_n]$ für $\omega_1, \dots, \omega_n \in \text{Cl}(k[x], F)$ (die ω_i sind eine Basis der $k[x]$ -Maximalordnung $\text{Cl}(k[x], F)$). Also ist $\text{Cl}(k[x], F)$ eine nullteilerfreie affine k -Algebra. Die Erzeuger des Relationenideals von $x, \omega_1, \dots, \omega_n$ liefern die Gleichungen für eine irreduzible, glatte affine Kurve C mit $k[C] = k[x, \omega_1, \dots, \omega_n] = \mathcal{O}_X(U)$.

Die Primideale von $\mathcal{O}_X(U)$ entsprechen genau den Stellen in $U \subseteq X$. Aber wir erhalten nicht alle Stellen in X als Punkte einer einzigen affinen Kurve. Da die U beliebig mit $0 < \#(X \setminus U) < \infty$ gewählt werden können und somit X überdecken, können wir insgesamt X als eine abstrakte Kurve auffassen und die Stellen aus X als Punkte dieser Kurve. Man nennt X manchmal auch abstrakte Riemannsche Fläche.

Die Verbindung zu projektiven Kurven ist die folgende. Haben wir eine irreduzible glatte projektive Kurve C über einem algebraisch abgeschlossenen Körper k , so entsprechen die Stellen des Funktionenkörpers von $k(C)$ bijektiv den Punkten von C .

Die Mengen U mit $0 < \#(X \setminus U) < \infty$ sind gerade die in der Zariskitopologie offenen Mengen (wegen Dimension 1) (diese U sind/heißten affin, da die Primideale in $\mathcal{O}_X(U)$ genau den Punkten in U entsprechen).

Eine irreduzible glatte projektive Kurve C ist dann in folgendem Sinn vollständig: Jede nicht konstante Funktion $x \in k(C)$ besitzt genau $[k(C) : k(x)]$ Nullstellen und Polstellen.

Funktionen. Bei einer irreduziblen glatten affinen Kurve C über einem algebraisch abgeschlossenen Körper k haben wir die Elemente von $k[C]$ sowohl als abstrakte Ringelemente als auch als Funktionen $C \rightarrow k$ aufgefasst. Die Elemente von $\mathcal{O}_X(U)$ können wir ebenfalls als Funktionen auffassen: Für $f \in \mathcal{O}_X(U)$ sei $f : U \rightarrow k$ durch $P \mapsto f(P)$ definiert. Da k algebraisch abgeschlossen ist, gilt $f(P) \in k(P) = k$, wie erforderlich. Wegen $\#U = \infty$

ist dieser Funktionenring isomorph zu $\mathcal{O}_X(U)$ (wegen des Hilbertschen Nullstellensatzes, oder da eine Funktion $\neq 0$ nur endlich viele Nullstellen hat). Wenn man sich die Definitionen anschaut, sieht man, daß die Kurven- und die Funktionenkörperbeschreibung äquivalent sind.

Bei nicht algebraisch abgeschlossenem Konstantenkörper gibt es Probleme mit der Definition $f : P \mapsto f(P)$, da die Bildwerte nicht mehr in k liegen. Das können wir wie folgt beheben. Sei $A = \cup_P k(P)$ die disjunkte Vereinigung der Restklassenkörper. Dann definieren wir $f : U \rightarrow A$ durch $P \mapsto f(P)$. Bezüglich koordinatenweiser Addition und Multiplikation bilden die Funktionen wieder einen Ring, den wir für den Moment mit $\mathcal{O}_X(U)'$ bezeichnen. Ist $f \in \mathcal{O}_X(U)'$ die Nullfunktion, so hat f als Element von $\mathcal{O}_X(U)$ beziehungsweise F unendlich viele Nullstellen und ist folglich Null in $\mathcal{O}_X(U)$. Daher ist $f \in \mathcal{O}_X(U)'$ ebenfalls Null und es gilt $\mathcal{O}_X(U)' \cong \mathcal{O}_X(U)$. Eine andere Möglichkeit ist die folgende: Sei $A = \cup_P \mathcal{O}_P$ die disjunkte Vereinigung der Bewertungsringe. Dann definieren wir $f : U \rightarrow A$ durch $P \mapsto f$ als Element von $\mathcal{O}_P$. Wie man direkt sieht, handelt es sich bei diesem Ring $\mathcal{O}_X(U)'$ im wesentlichen um das Bild von $\mathcal{O}_X(U)$ im Adelering A_F . Mit diesen Definitionen stellt sich die Inklusion $\mathcal{O}_X(U) \subseteq \mathcal{O}_X(V)$ beziehungsweise $\mathcal{O}_X(U)' \subseteq \mathcal{O}_X(V)'$ für $U \supseteq V$ als Einschränkung von Funktionen von U auf V dar.

Sei $U = \cup_i U_i$ und $f'_i \in \mathcal{O}_X(U_i)'$ mit $f'_i = f'_j$ auf $U_i \cap U_j$ für alle i, j . Dann gibt es ein eindeutig bestimmtes $f' \in \mathcal{O}_X(U)'$ mit $f' = f'_i$ auf U_i für alle i . Als reine Funktion auf U ist die Existenz und Eindeutigkeit von f' klar, für die Existenz muß man hier aber noch zeigen, dass f' auch von der Form $P \mapsto f(P)$ für ein $f \in \mathcal{O}_X(U)$ ist. Die f'_i entsprechen aber eindeutig Elementen f_i aus $\mathcal{O}_X(U_i) \subseteq F$ und es gilt wegen $f'_i = f'_j$ auf $U_i \cap U_j$ auch $f_i = f_j$ in F . Also gilt $f_i \in \cap_j \mathcal{O}_X(U_j) = \mathcal{O}_X(U)$ und $f = f_i$ liefert das gesuchte Element (alternativ und im allgemeinen erforderlich kann man die Funktionen auch lokal definieren, dann ist die Existenz unmittelbar klar, aber man muß nun den chinesischen Restsatz anwenden, um die Isomorphie der Funktionenräume $\mathcal{O}_X(U)'$ mit $\mathcal{O}_X(U)$ zu zeigen). Analoge Überlegungen sind auch für $\mathcal{O}_X(D)$ richtig. Solche Schaaren von Funktionsringen bilden Beispiele von sogenannten Garben, die in der algebraischen Geometrie überall vorkommen.

4 Ganze Abschlüsse und Ordnungen

Wir wollen Teilringe von F und insbesondere die Ringe $\mathcal{O}_S$ noch etwas genauer untersuchen.

7 Satz. Sei A ein Teilring und kein Teilkörper von F mit $k \subseteq A$. Sei $S(A) = \{P \in \mathbb{P}_F \mid A \subseteq \mathcal{O}_P\}$. Dann gilt

- (i) $S(A) \neq \emptyset$ und $S(A) \neq \mathbb{P}_F$.
- (ii) $\text{Cl}(A, F) = \mathcal{O}_{S(A)}$.

Beweis. Siehe Stichtenoth III.2.6 auf Seite 69:

(i): Da A kein Körper ist, gibt es ein maximales Ideal $\mathfrak{m} \neq 0$ von A . Dann gibt es nach Stichtenoth I.1.18 eine Stelle $P \in \mathbb{P}_F$ mit $A \subseteq \mathcal{O}_P$ und $\mathfrak{m} \subseteq P$. Also gilt $S(A) \neq \emptyset$. Wegen $k \subseteq A$ und $\bigcap_{P \in \mathbb{P}_F} \mathcal{O}_P = k$ gilt auch $S(A) \neq \mathbb{P}_F$.

(ii): Da $A \subseteq \mathcal{O}_{S(A)}$ gilt und $\mathcal{O}_{S(A)}$ ganz abgeschlossen ist, folgt $\text{Cl}(A, F) \subseteq \text{Cl}(\mathcal{O}_{S(A)}, F) = \mathcal{O}_{S(A)}$.

Sei $z \in \mathcal{O}_{S(A)}$. Dann gilt $z^{-1}A[z^{-1}] = A[z^{-1}]$. Denn andernfalls gibt es nach Stichtenoth I.1.18 eine Stelle $Q \in \mathbb{P}_F$ mit $A[z^{-1}] \subseteq \mathcal{O}_Q$ und $z^{-1} \in Q$, also $Q \in S(A)$ und $z \notin \mathcal{O}_Q$ im Widerspruch zu $z \in \mathcal{O}_{S(A)} \subseteq \mathcal{O}_Q$.

Nun ist z^{-1} eine Einheit in $A[z^{-1}]$, es gibt also $a_i \in A$ mit $1 = z^{-1} \cdot \sum_{i=0}^s a_i (z^{-1})^i$. Multiplikation mit z^{s+1} liefert eine Ganzheitsgleichung für z über A , also $z \in \text{Cl}(A, F)$. $\square$

Sei F/k ein Funktionenkörper und F'/F eine endliche Erweiterung. Dann ist F'/k ebenfalls ein Funktionenkörper, wobei k allerdings nicht mehr exakt zu sein braucht. Sei A ein Teilring von F mit $\text{Quot}(A) = F$ und B ein Teilring von F' mit $\text{Quot}(B) = F'$ und $A \subseteq B$, so daß B endlich über A ist. Dann nennen wir B eine A -Ordnung von F' . Da B endlich über A ist, ist jedes Element aus B ganz über A . Gilt $B' \subseteq B$ für jede A -Ordnung B' von F' , so heißt B eine A -Maximalordnung von F' .

8 Lemma. Sei $B = \text{Cl}(A, F')$. Dann gibt es eine F -Basis von F' bestehend aus Elementen aus B . Daher gilt auch $F' = \text{Quot}(B) = B[U^{-1}]$ mit $U = A \setminus \{0\}$.

Beweis. Sei $b \in F'$ und $f \in F[t]$ normiert mit $\deg(f) \geq 1$ und $f(b) = 0$. Sei $d \in A$ das Produkt der in den Koeffizienten von f auftretenden Nenner. Setze $g = d^{\deg(f)} f(t/d)$. Dann ist g normiert und es gilt $g \in A[t]$. Wegen $g(db) = d^{\deg(f)} f(b) = 0$ ist $db \in B$.

Indem wir eine F -Basis von F' mit geeigneten $d \in A$ multiplizieren, erhalten wir also eine F -Basis von F' bestehend aus Elementen aus B . Speziell läßt sich jedes Element $b \in F'$ in der Form $b = a/d$ mit $a \in B$ und $d \in F$ schreiben, was die zweite Aussage zeigt. $\square$

9 Satz. Sei zusätzlich A noethersch und F'/F separabel. Dann gibt es genau eine A -Maximalordnung B von F' , nämlich $B = \text{Cl}(A, F')$.

Beweis. Sei B' eine beliebige A -Ordnung. Nach Lemma 8 gilt $\text{Quot}(B) = F$. Da B' endlich und somit ganz über A ist, gilt weiter $B' \subseteq B = \text{Cl}(A, F')$. Daher bleibt nur zu zeigen (und das ist der Knackpunkt), daß B endlich über A ist.

Ist M ein A -Untermodul von F' , so definieren wir den dualen Modul $M^\# = \{x \in F' \mid \text{Tr}_{F'/F}(xy) \in A \text{ für alle } y \in M\}$. Für $M \subseteq N$ folgt $M^\# \supseteq N^\#$. Außerdem gilt $B^\# \supseteq B$.

Nach Lemma 8 gibt es eine in B gelegene F -Basis $b_1, \dots, b_n$ von F' . Sei M der von einer solchen Basis erzeugte A -Untermodul von B . Dann gilt $M \subseteq B \subseteq B^\# \subseteq M^\#$. Sei $\phi : M^\# \rightarrow A^n$ der durch $x \mapsto (\text{Tr}_{F'/F}(xb_1), \dots, \text{Tr}_{F'/F}(xb_n))$ definierte A -Modulhomomorphismus. Da F'/F separabel ist, ist ϕ nach Satz ??, (iii) injektiv. Folglich kann B als A -Untermodul von A^n aufgefaßt werden. Da A noethersch ist, sind A^n und B nach Satz ?? noethersch. Also ist B auch ein endlich erzeugter A -Modul. $\square$

Im Beweis wurde nur verwendet, daß F'/F separabel und A noethersch ist. Der Satz gilt hier aber auch ohne die Voraussetzung, daß F'/F separabel sein soll, denn in unserer Situation haben wir zusätzlich $\dim(A) \leq 1$ (Satz von Krull-Akizuki).

Wir haben oben im Vorgriff von Satz 9 gezeigt, daß die Ringe $\mathcal{O}_X(U)$ für $0 < \#(X \setminus U) < \infty$ $k[x]$ -Ordnungen für geeignete $x \in \mathcal{O}_X(U)$ sind.

Ist A ein Hauptidealring, so besitzt jede A -Ordnung B von F' nach dem Hauptsatz über endlich erzeugte Moduln über Hauptidealringen eine A -Basis bestehend aus $[F' : F]$ Elementen. Die Basis von $\text{Cl}(A, F')$ nennt man eine A -Ganzheitsbasis.

Sind die $\omega_1, \dots, \omega_n$ eine A -Basis von B , so können die Elemente von B als Linearkombinationen der ω_i , also als Vektoren aus A^n dargestellt werden. Addition geschieht dann komponentenweise. Für die Multiplikation benötigt man nur noch Elemente $\lambda_{i,j,\nu} \in A$ mit $\omega_i \omega_j = \sum_{\nu=1}^n \lambda_{i,j,\nu} \omega_\nu$. Solche $\lambda_{i,j,\nu}$ heißen Multiplikationstabelle oder Strukturkonstanten der A -Ordnung B .

Sei B eine A -Ordnung. Ist A noethersch, so ist auch B noethersch, denn B ist als A -Modul isomorph zu einem Faktormodul von A^n . Für $\dim(A) = 1$ folgt $\dim(B) = 1$. Denn ist $\mathfrak{p}$ ein Primideal von B , so ist $A \cap \mathfrak{p}$ ein Primideal und wegen $\dim(A) = 1$ ein maximales Ideal von A . Dann ist $B/\mathfrak{p}$ eine endliche Erweiterung des Körpers $A/(A \cap \mathfrak{p})$ und somit ein Körper. Also ist $\mathfrak{p}$ ein maximales Ideal von B und somit $\dim(B) = 1$. Man kann allgemein $\dim(A) = \dim(B)$ zeigen, da B ganz über A ist.

5 Diskriminanten und Index

Man kann den Satz 9 aus dem vorigen Abschnitt auch etwas anders beweisen, in dem man den Ordnungen noch gewisse Invarianten, die Diskriminanten, zuordnet. Diese sind aber auch anderweitig von Nutzen. Wir nehmen der Einfachheit halber an, daß A ein Hauptidealring ist. Das geht dann wie folgt.

Jede A -Basis von B ist linear unabhängig über F und liefert damit eine F -Basis von F' . Sei $\omega_1, \dots, \omega_n$ eine F -Basis von F' . Wir definieren $\text{disc}(\omega_1, \dots, \omega_n) = \det((\text{Tr}_{F'/F}(\omega_i \omega_j))_{i,j})$. Da F'/F separabel ist, ist die Spur nicht ausgeartet und es gilt $\text{disc}(\omega_1, \dots, \omega_n) \neq 0$. Sind die ω_i ganz über A , so gilt $\text{disc}(\omega_1, \dots, \omega_n) \in A$. Ist $\omega'_1, \dots, \omega'_n \in F$ eine weitere F -Basis von F' , so gibt es ein invertierbares $U \in F^{n \times n}$ mit $(\omega'_1, \dots, \omega'_n) = (\omega_1, \dots, \omega_n)U$. Die Linearität der Spur liefert $\text{disc}(\omega'_1, \dots, \omega'_n) = \det(U)^2 \text{disc}(\omega_1, \dots, \omega_n)$. Sind die ω'_i eine Basis einer A -Ordnung B' und die ω_i eine Basis einer A -Ordnung B mit $B' \subseteq B$, so gilt $U \in A^{n \times n}$. Speziell gilt hier nun $B = B'$ genau dann, wenn U unimodular, also $\det(U) \in A^\times$ ist.

Die Diskriminante $\text{disc}(B)$ einer A -Ordnung wird definiert als $\text{disc}(\omega_1, \dots, \omega_n)$ für eine Basis $\omega_1, \dots, \omega_n$ von B und bis ist auf Skalierung mit Quadraten aus $A^\times$ ein wohldefiniertes Element aus A . Das Ideal $\text{disc}(B)A$ ist daher eindeutig bestimmt. Für $B' \subseteq B$ gilt $B' = B$ genau dann, wenn $\text{disc}(B')A = \text{disc}(B)A$ ist.

Sei $y \in F'$ mit $F' = F(y)$. Ein solches y existiert nach dem Satz vom primitiven Element, da F'/F separabel ist. Durch Multiplikation mit Elementen aus A können wir erreichen, daß y ganz über A wird. Dann ist $A[y]$ eine A -Ordnung. Sei z_i eine Folge von Elementen aus $\text{Cl}(A, F')$ und $R_i = A[y, z_1, \dots, z_i]$. Für die A -Ordnungen R_i gilt dann $R_1 \subseteq R_2 \subseteq \dots$ und $\text{disc}(R_1)A \subseteq \text{disc}(R_2)A \subseteq \dots$. Da A auch noethersch ist, wird die Folge der R_i stationär. Daher gibt es $z_1, \dots, z_r \in \text{Cl}(A, F')$ mit $\text{Cl}(A, F') = A[y, z_1, \dots, z_r]$. Also ist $\text{Cl}(A, F')$ endlich über A und damit eine A -Ordnung.

Die A -Ordnung $A[y]$ aus dem Beweis wird häufig eine A -Gleichungsordnung genannt, wobei die Gleichung $f(y) = 0$ und f das Minimalpolynom von y über F mit Koeffizienten in A ist. Es gilt $\text{disc}(A)A = \text{disc}(f)A$ unter Verwendung einer van der Mondeischen Determinante. Dies sieht man wie folgt. Zunächst gilt $(\text{Tr}_{F'/F}(\omega_i \omega_j))_{i,j} = M^{tr}M$ mit $M = (\sigma_i(\omega_j))_{i,j}$, wobei die σ_i die n verschiedenen F -linearen Einbettungen von F' in einen algebraischen Abschluß von F bezeichnen. Für $\omega_i = y^{i-1}$ ist $\det(M) = \prod_{i < j} (\sigma_i(y) - \sigma_j(y))$ die van der Mondeische Determinante und wir erhalten $\text{disc}(1, y, \dots, y^{n-1}) = \det(M^{tr}M) = \det(M)^2 = \prod_{i < j} (\sigma_i(y) - \sigma_j(y))^2 = \text{disc}(f)$.

Seien $B' \subseteq B$ zwei A -Ordnungen und A ein Hauptidealring. Ist $U \in A^{n \times n}$ die Transformationsmatrix einer Basis von B in eine Basis von B' , so nennen wir $\det(U)$ den Index von B' in B . Der Index ist wieder bis auf Einheiten

eindeutig bestimmt. Fassen wir B' und B nur als A -Moduln auf, so folgt für den Index $\det(U)B \subseteq B'$. Es gilt weiter $\text{disc}(B) \det(U)^2 A = \text{disc}(B)A$.

6 Führer

Seien B, B' Integritätsringe mit $B \subseteq B'$ und $\text{Quot}(B) = \text{Quot}(B') = F'$. Der Führer von B in B' ist definiert als $\mathcal{F} = \{x \in F' \mid xB' \subseteq B\}$. Der Führer ist das größte gemeinsame Ideal von B und B' . In der Tat, wegen $1 \in B'$ gilt $\mathcal{F} \subseteq B$ und es ist klar, daß $\mathcal{F}$ ein Ideal von B ist. Es gilt aber auch $B'\mathcal{F} \subseteq \mathcal{F}$, denn $(B'\mathcal{F})B' \subseteq B'B'\mathcal{F} \subseteq B'\mathcal{F} \subseteq B$. Analog zeigt man für jedes gemeinsame Ideal I von B und B' , daß $I \subseteq \mathcal{F}$ gilt.

Der Index von A -Ordnungen B' in B ist ein Element von $\mathcal{F}$. Dies zeigt insbesondere $\mathcal{F} \neq \{0\}$ in diesem Fall.

Wir definieren $\mathcal{I}_{B,\mathcal{F}} = \{I \mid I \text{ Ideal von } B \text{ mit } \mathcal{F} + I = B\}$ und analog $\mathcal{I}_{B',\mathcal{F}}$ für B' . Desweiteren seien $\phi : \mathcal{I}_{B,\mathcal{F}} \rightarrow \mathcal{I}_{B',\mathcal{F}}$ und $\psi : \mathcal{I}_{B',\mathcal{F}} \rightarrow \mathcal{I}_{B,\mathcal{F}}$ definiert durch $I \mapsto B'I$ und $J \mapsto J \cap B$.

10 Satz. *Sei $B \subseteq B'$ eine Ringerweiterung, so daß $\text{Quot}(B) = \text{Quot}(B')$ und $\dim(B) = \dim(B') = 1$ gilt, B' ein Dedekindring ist, und B den Führer $\mathcal{F}$ in B' hat.*

- (i) $\mathcal{I}_{B,\mathcal{F}}$ und $\mathcal{I}_{B',\mathcal{F}}$ sind bezüglich Idealmultiplikation Monoide mit Kürzungsregel. Die Abbildungen ϕ und ψ sind zueinander inverse Isomorphismen von $\mathcal{I}_{B,\mathcal{F}}$ und $\mathcal{I}_{B',\mathcal{F}}$.
- (ii) Für $J \in \mathcal{I}_{B',\mathcal{F}}$ gilt $B/(J \cap B) \cong B'/J$.
- (iii) Für ein Primideal P von B gilt $P \in \mathcal{I}_{B,\mathcal{F}}$ genau dann, wenn B_P ein diskreter Bewertungsring ist.
- (iv) Die Ideale aus $\mathcal{I}_{B,\mathcal{F}}$ sind invertierbar und können eindeutig in Primideale faktorisiert werden.

Beweis. (i): Sei $I \in \mathcal{I}_{B,\mathcal{F}}$. Dann gilt $B' \supseteq B'I + \mathcal{F} \supseteq B'(I + \mathcal{F}) = B'B = B'$, also $\phi(I) = B'I \in \mathcal{I}_{B',\mathcal{F}}$. Sei $J \in \mathcal{I}_{B',\mathcal{F}}$. Dann gilt $B' = J + \mathcal{F}$, und wegen $\mathcal{F} \subseteq B$ auch $B = (J \cap B) + \mathcal{F}$, also $\psi(J) = J \cap B \in \mathcal{I}_{B,\mathcal{F}}$.

Zum Beweis von $\psi \circ \phi = \text{id}$ sei $I \in \mathcal{I}_{B,\mathcal{F}}$. Dann gilt in der Tat $I \subseteq B'I \cap B = B'I \cap (I + \mathcal{F}) \subseteq I + (B'I \cap \mathcal{F}) \subseteq I + B'IF \subseteq I$.

Zum Beweis von $\phi \circ \psi = \text{id}$ sei $J \in \mathcal{I}_{B',\mathcal{F}}$. Dann gilt $J\mathcal{F} = J \cap \mathcal{F} = (J \cap B) \cap \mathcal{F} = (J \cap B)\mathcal{F}$ und damit $J = JB = J((J \cap B) + \mathcal{F}) = J(J \cap B) + J\mathcal{F} = J(J \cap B) + (J \cap B)\mathcal{F} = (J \cap B)(J + \mathcal{F}) = (J \cap B)B'$.

Die Homomorphieeigenschaft von ϕ und damit auch von ψ ist klar.

Für $J_1, J_2 \in \mathcal{I}_{B', \mathcal{F}}$ gilt $B' = (J_1 + \mathcal{F})(J_2 + \mathcal{F}) \subseteq J_1 J_2 + \mathcal{F} \subseteq B'$, also $J_1 J_2 \in \mathcal{I}_{B', \mathcal{F}}$. Der Rest folgt aus der Dedekindringeigenschaft von B' und da ϕ, ψ Isomorphismen sind.

(ii): Die Inklusion liefert eine Einbettung $h : B/(J \cap B) \rightarrow B'/J$. Sei $x \in B'$. Wegen $B' = J + \mathcal{F}$ gibt es $x' \in J$ und $z \in \mathcal{F} \subseteq B$ mit $x = x' + z$. Es folgt $h(z + (J \cap B)) = x + B$ und h ist surjektiv.

(iii): Sei $U = B \setminus P$. Der Führer von $B_P = B[U^{-1}]$ in $B'[U^{-1}]$ ist gleich $\mathcal{F}B_P$, wie man direkt nachrechnet. Nun gilt $P + \mathcal{F} = B$ genau dann, wenn $\mathcal{F}B_P = B_P$ ist. Denn für $x + y = 1$ mit $x \in P$ und $y \in \mathcal{F}$ ist $y = 1 - x \in \mathcal{F} \cap B_P^\times$, und für $y/u = 1$ mit $y \in \mathcal{F}$ und $u \in B \setminus P$ folgt $y = u \notin P$ und damit $\mathcal{F} \not\subseteq P$ und $\mathcal{F} + P = B$, da $\dim(B) = 1$.

Für $P \in \mathcal{I}_{B, \mathcal{F}}$ folgt also $\mathcal{F}B_P = B_P$ und damit $B_P = B'[U^{-1}]$. Folglich ist B_P ein Dedekindring mit genau einem Primideal $\neq 0$, also ein diskreter Bewertungsring.

Ist umgekehrt B_P ein diskreter Bewertungsring, so gilt $B_P = B'[U^{-1}]$ wegen $\dim(B') = 1$ und der Maximalität von diskreten Bewertungsringen (Stichtenoth I.1.12 c)), also $\mathcal{F}B_P = B_P$ und damit $P + \mathcal{F} = B$.

(iv): Die eindeutige Primidealfaktorisierung folgt aus (i). Primideale aus $\mathcal{I}_{B, \mathcal{F}}$ sind wegen (iii) invertierbar, und damit wegen der Primidealfaktorisierung dann alle Ideale aus $\mathcal{I}_{B, \mathcal{F}}$. $\square$

Man kann den Satz dann auch auf gebrochene Ideale von B und B' verallgemeinern.

11 Satz. *Sei A ein Dedekindring und seien $B \subseteq B'$ zwei A -Ordnungen von F' mit $B = A[y]$ und $B' = \text{Cl}(A, F')$. Sei $f \in A[t]$ normiert mit $f(y) = 0$. Sei $\mathcal{F}$ der Führer von B in B' und P ein Primideal von A mit $BP + \mathcal{F} = B$. Dann gibt es Primideale P_i von B' mit $P = \prod_{i=1}^r P_i^{e_i}$, wobei die P_i , e_i , r und die Indizes $[B'/P_i : A/P]$ wie folgt erhalten werden.*

Die Faktorisierung von f modulo P ist $f \equiv \prod_{i=1}^r f_i^{e_i} \pmod{P}$. Es gilt $P_i = B'P + B'f_i(y)$ und $[B'/P_i : A/P] = \deg(f_i)$.

Beweis. Mit $BP + \mathcal{F} = B$ gilt auch $B'P + \mathcal{F} = B'$ und umgekehrt. Nach Satz 10 genügt es, die Aussagen für die Primidealfaktorisierung von BP in B zu beweisen.

Die Primideale P_i über BP entsprechen den Primidealen von $B/BP \cong A[t]/(PA[t] + f(t)A[t]) \cong (A/P)[t]/(\bar{f})$, wobei $\bar{f}$ das Bild von f in $(A/P)[t]$ bezeichnet. Da A/P ein Körper ist, haben wir eine Faktorisierung $\bar{f} = \prod_{i=1}^r \bar{f}_i^{e_i}$ mit $f_i \in A[t]$. Die Primideale von $(A/P)[t]/(\bar{f})$ sind dann $\bar{P}_i = (\bar{f}_i)$. Seien die P_i die Urbilder der $\bar{P}_i$ in B . Dann gilt $P_i = BP + Bf_i$, und wir erhalten so alle Primideale, welche BP enthalten. Es gilt $\prod_{i=1}^r P_i^{e_i} \subseteq BP$ nach Konstruktion. Ersetzen wir die e_i durch Werte $d_i \leq e_i$ mit $d_j < e_j$

für mindestens ein j , so gilt $\prod_{i=1}^r P_i^{d_i} \not\subseteq BP$ nach Konstruktion. Da BP eine Primidealfaktorisierung in die P_i wegen Satz 10 besitzt, folgt $\prod_{i=1}^r P_i^{e_i} = BP$. Außerdem gilt $[B/P_i : A/P] = \deg(f_i)$. $\square$

Um den Satz anzuwenden, benötigt man den Führer $\mathcal{F}$, dessen Bestimmung umständlich sein kann. Es gilt aber $\text{disc}(A[y]) \in \mathcal{F}$, so daß man den Satz auf jeden Fall auf solche P anwenden kann, für die $A = \text{disc}(A[y])A + P$ gilt.

7 Beispiel

Sei k ein vollkommener Körper mit $\text{char}(k) \neq 2$ und $C : y^2 = f(x)$ mit $f \in k[x]$ quadratfrei und $\deg(f) = 2d + 1$ ungerade. Dann ist C eine irreduzible affine Kurve. Wir betrachten den Funktionenkörper $k(C)$ von C .

Der Koordinatenring $k[x, y]$ von C ist ein Dedekindring. Dies können wir auf zwei Weisen, einer „geometrischen“ und einer „algebraischen“, testen.

Für die geometrische Weise stellen wir fest, daß es nach Voraussetzung keine Punkte $(x_0, y_0) \in C(\bar{k})$ mit $2y_0 = 0$ und $f'(x_0) = 0$ gibt. Also ist C glatt und $k[x, y]$ damit ein Dedekindring. Anders ausgedrückt ist das durch $2y$ und $f'(x)$ erzeugte Ideal I von $k[x, y]$ gleich $k[x, y]$ selbst.

Für die algebraische Weise berechnen wir die Diskriminante von $y^2 - f(x)$ als univariates Polynom in y und erhalten $\text{disc}(f) = 4f(x)$. Daher gilt auch $\text{disc}(k[x][y]) = 4f(x)$ für die $k[x]$ -Gleichungsordnung $k[x][y] = k[x, y]$. Da $f(x)$ quadratfrei ist, muß $k[x][y]$ bereits die $k[x]$ -Maximalordnung von F sein, ist also ein Dedekindring.

Sei $\wp$ das durch $x - x_0$ definierte Primideal von $k[x]$. Es gibt dann drei Fälle: 1. $k[x, y]\wp = \mathfrak{p}_1\mathfrak{p}_2$ mit $\mathfrak{p}_1 \neq \mathfrak{p}_2$ genau dann, wenn $y^2 - f(x_0)$ eine Nullstelle $y_0 \neq 0$ in k besitzt, also $f(x_0) \neq 0$ ein Quadrat in k ist. Dann ist $\mathfrak{p}_1 = k[x, y]\wp + k[x, y](y - y_0)$ und $\mathfrak{p}_2 = k[x, y]\wp + k[x, y](y + y_0)$. Man sagt, $\wp$ ist total zerlegt in $k[x, y]$. 2. $k[x, y]\wp = \mathfrak{p}^2$ genau dann, wenn $y_0 = 0$ in 1. gilt, wenn also $f(x_0) = 0$ gilt. Dann ist $\mathfrak{p} = k[x, y]\wp + k[x, y]y$. Man sagt, daß $\wp$ total verzweigt in $k[x, y]$ ist. 3. $k[x, y]\wp = \mathfrak{p}$ genau dann, wenn $y^2 - f(x_0)$ keine Nullstelle in k besitzt, also $f(x_0)$ kein Quadrat in k ist. Dann gilt $[k[x, y]/\mathfrak{p} : k[x]/\wp] = 2$. Man sagt, daß $\wp$ träge in $k[x, y]$ ist.

Entsprechend geht man vor, wenn $x - x_0$ durch ein Primpolynom höheren Grades ersetzt wird. Damit können wir alle Primideale von $k[x, y]$ und somit alle Stellen von F bestimmen, an denen x keine Pole besitzt.

Um auch die Pole von x zu finden, betrachten wir $\tilde{x} = x^{-1}$ anstelle von x . Division mit x^{2g+2} liefert $(y/x^{g+1})^2 = f(x)/x^{2g+2}$ in F . Für $\tilde{y} = y/x^{g+1}$ gilt dann $\tilde{y}^2 = c\tilde{x} + O(\tilde{x}^2)$, wobei c der Leitkoeffizient von $f(x)$ ist. Wir

erhalten eine andere irreduzible affine Kurve mit Koordinatenring $k[\tilde{x}, \tilde{y}]$ und interessieren uns jetzt nur noch für die Nullstellen von $\tilde{x}$ in F . Sei $k[\tilde{x}]_{(\tilde{x})}$ die Lokalisierung bezüglich des Primideals $(\tilde{x})$. Wir wollen zeigen, daß die $k[\tilde{x}]_{(\tilde{x})}$ -Gleichungsordnung $k[\tilde{x}]_{(\tilde{x})}[\tilde{y}]$ bereits maximal ist. Das einzige Primelement von $k[\tilde{x}]_{(\tilde{x})}$ ist $\tilde{x}$. Da $\text{disc}(k[\tilde{x}]_{(\tilde{x})}[\tilde{y}]) = 4(c\tilde{x} + O(\tilde{x}^2))$ demnach quadratfrei in $k[\tilde{x}]_{(\tilde{x})}$ ist, folgt die Behauptung wie oben. Wir erhalten $k[\tilde{x}]_{(\tilde{x})}[\tilde{y}]\tilde{x} = \tilde{\mathfrak{p}}^2$ mit $\tilde{\mathfrak{p}} = k[\tilde{x}]_{(\tilde{x})}[\tilde{y}]\tilde{x} + k[\tilde{x}]_{(\tilde{x})}[\tilde{y}]\tilde{y}$.

Also ergibt sich $(x)_\infty = 2\infty$, wobei die zum Primideal $\tilde{\mathfrak{p}}$ gehörige Stelle mit ∞ bezeichnet sei und Grad eins hat. Durch Bewertungsvergleich ergibt sich $(y)_\infty = 2d + 1$. Wir können $k[x, y]$ dann als „Polynomring“ mit $\deg(x) = 2$ und $\deg(y) = 2d + 1$ auffassen.

Dies wiederum hilft bei der Bestimmung der Fehlzahlen bei ∞ : Man sieht direkt, daß die ersten d ungeraden Zahlen genau die Fehlzahlen bei ∞ sind. Damit ergibt sich $g = d = (\deg(f) - 1)/2$ für das Geschlecht von C beziehungsweise F .

Es gilt $\dim(2\infty) \geq 2$ wegen $1, x \in \mathcal{L}(2\infty)$. Sei F/k umgekehrt ein Funktionenkörper mit einer Stelle P vom Grad eins und $\mathcal{L}(2P) \geq 2$. Für $x \in \mathcal{L}(2P) \setminus k$ gilt dann $(x)_\infty = 2P$. Sei $y \in \mathcal{L}((2d+1)P)$ mit d minimal. Dann gilt $(y)_\infty = (2d+1)P$ und es gibt genau d Fehlzahlen bei P , also ist das Geschlecht g von F wie eben gleich d . Wir haben $x^i, x^j y, y^2 \in \mathcal{L}((4g+2)P)$ für $0 \leq i \leq 2g+1$ und $0 \leq j \leq g$. Das sind $3g+4$ Elemente. Nach Riemann-Roch gilt aber $\dim((4g+2)P) = 4g+2+1-g+0 = 3g+3$, denn $(4g+2)P$ ist nicht speziell. Also sind die $x^i, x^j y, y^2$ linear abhängig über k . Wir erhalten $h, f \in k[x]$ und $a \in k$ mit $ay^2 + h(x)y + f(x) = 0$. Wegen $\deg((x)_\infty) = 2$ gilt $a \neq 0$ und ohne Einschränkung $a = 1$. Wegen $\deg((y)_\infty) = 2g+1$ gilt $\deg(f) = 2g+1$. Nach Konstruktion gilt $\deg(h) \leq g$. Indem wir als Erzeuger $y + h(x)/2$ statt y wählen, erhalten wir $y^2 + f(x) = 0$ für ein neues $f \in k[x]$ mit $\deg(f) = 2g+1$.

12 Definition. Ein Funktionenkörper F/k mit $g = 1$ und einer Stelle vom Grad eins heißt elliptischer Funktionenkörper.

Ein Funktionenkörper F/k mit $g \geq 2$ und einem Divisor D vom Grad zwei und der Dimension ≥ 2 heißt hyperelliptischer Funktionenkörper.

Ist die Charakteristik $\neq 2$ und $D = 2P$, so ist F/k Funktionenkörper einer Kurve $C : y^2 = f(x)$ mit $\deg(f) = 2g+1$. Für $g = 1$ nennt man C elliptische Kurve und für $g \geq 2$ hyperelliptische Kurve.

Aufgabe: Setze die Fälle $D = P$ und $D = P_1 + P_2$ und $C : y^2 = f(x)$ mit $\deg(f) = 2d+2$ analog wie oben in Beziehung zueinander.

Sei $C : y^2 = x(x-a)^2$. Dann ist der Koordinatenring $k[C] = k[x, y]$ nicht maximal. Das Element $y/(x-a)$ ist nämlich wegen $(y/(x-a))^2 = x$ ganz über

$k[x]$, befindet sich aber nicht in $k[x, y]$. Dann ist $k[x, y/(x-a)]$ maximal, da die Diskriminante von $t^2 - x$ kein Quadrat enthält. Wegen $k(C) = k(y/(x-a))$ ist $k(C)$ ein rationaler Funktionenkörper und hat daher Geschlecht 0. Speziell gilt $k[x, y/(x-a)] = k[y/(x-a)]$ und $k[x, y/(x-a)]$ ist daher ein Polynomring.

Dies liefert auch ein Beispiel für die Zerlegung von Primidealen, die nicht teilerfremd zum Führer sind. In $k[x, y]$ gilt $\mathfrak{p}^2 \subseteq k[x, y](x-a)$ mit $\mathfrak{p} = k[x, y](x-a) + k[x, y]y$. In $k[x, y/(x-a)]$ gilt aber $\mathfrak{p}_1\mathfrak{p}_2 = k[x, y/(x-a)](x-a)$ mit $\pi = k[x, y/(x-a)](x-a) + (y/(x-a)) \pm \sqrt{a}k[x, y/(x-a)]$. Konkret ist $k[x, y/(x-a)]\mathfrak{p} = \mathfrak{p}_1\mathfrak{p}_2$, also das von $\mathfrak{p}$ in $k[x, y/(x-a)]$ erzeugte Ideal kein Primideal mehr.

In der Notation von Satz 11 sind also die Ideale $B'P_i$ nicht unbedingt Primideale von B' , falls $P_i + \mathcal{F} \neq B$. Man kann allgemein zeigen, daß für $B'P = \sum_{i=1}^r P_i^{e_i}$ gilt $n = \sum_{i=1}^r e_i f_i$ mit $n = [F' : F] = \deg(f)$ und $f_i = [B'/P_i' : A/P]$. Ist P_j' ein Primideal von B' , welches $B'P_i$ teilt, so gilt $B/P_i \subseteq B'/P_j'$. Haben wir also in B ein Produkt der Form $\prod_{i=1}^r P_i^{e_i} \subseteq BP$ entsprechend der Faktorisierung von f modulo P , so ändert sich die Primidealfaktorisierung in B' höchstens dahingehend, daß r und die f_i größer werden, und die e_i entsprechend kleiner werden, so daß zum Schluß aber immer noch $n = \sum_i e_i f_i$ gilt. Für die genaueren Verhältnisse in konkreten Beispielen verwendet man am besten geeignete Algorithmen zur Idealfaktorisierung (Stichwort Indexteilerfaktorisierung).