

Inhaltsverzeichnis

Ganze Ringerweiterungen	3
1 Endliche Ringerweiterungen	4
2 Der ganze Abschluß von R in S	6
3 Der Körperfall	7
4 Der Noethersche Normalisierungssatz	8
Das Spektrum eines Ringes	11
5 Die Zariski Topologie	12
6 Eine Basis der offenen Mengen	14
7 Das Nilradikal	16
8 Radikal-Ideale	17
9 Zusammenhangskomponenten	18
10 Eine Anwendung	20
Maximale Ideale	23
11 Lokale Ringe	24
12 Das Jacobson Radikal	25
13 Der Hilbertsche Nullstellensatz	26
14 Endlich erzeugte R -Algebren	27
15 Eine Umformulierung	30
Noethersche Moduln und Ringe	32
16 Noethersche Ringe	33
17 Noethersche Räume	35
18 Generische Punkte	36
19 Primzyklische Moduln	37
20 Der Träger eines R -Moduls	40
21 P -Koprimäre Moduln	42
22 Koprimäre Moduln	44
23 Einbettbarkeit	44
24 Primärzerlegung	46

Dimensionstheorie	49
25 Höhe eines Primideals	50
26 Going Up	51
27 Polynomringe	52
Graduierte Ringe	55
28 Filtrationen	56
29 Graduierte Moduln	58
30 Hilbert–Dimension	59
31 Dimensionsvergleich	61
32 Reguläre lokale Ringe	63
Normale Ringe	65
33 Krull’s Hauptidealsatz	66
34 Faktorielle Ringe	66
35 Diskrete Bewertungen	68
36 Primärzerlegung von Hauptidealen	70
37 Reflexive Ideale	72
38 Die Klassengruppe	74
Ringe der Dimension 1	76
39 Dedekindringe	77
40 Zahlkörper	78
41 Kreiskörper	80
Komplettierungen	83
42 Vervollständigung	84
Ringe der Charakteristik p	88
43 Perfekte Ringe	89
44 Der Teichmüller Lift	90
45 Einige Beispiele	93
46 Der Kern der Perfektionierung	94
47 * Bewertungen	95
Wittringe	97
48 p -adische Entwicklungen	98
49 Rechnen mit Übertrag	99
50 Wittringe	100
51 Rekonstruktion	102
52 Konstruktion	104

Fontaine Ringe	106
53 Verdickungen	107
54 Neue Elemente	108
55 Der Kern von θ	110

Einleitung

Ist X ein kompakter topologischer Raum, dann ist der Ring $C(X)$ der stetigen reellwertigen Funktionen auf X ein kommutativer Ring mit 1. Für jeden Punkt $x \in X$ definiert die Auswertung $f \mapsto f(x)$ einen Ringhomomorphismus von $C(X)$ auf den Körper der reellen Zahlen. Das Bild ist der Körper \mathbb{R} , der Kern P_x dieser Auswertung ist also ein maximales Ideal in $C(X)$. Eine stetige Abbildung $g : X \rightarrow Y$ induziert einen Ringhomomorphismus

$$\varphi : C(Y) \rightarrow C(X) ,$$

den Pullback $f(y) \mapsto f(g(y))$. Das Urbild des maximalen Ideale $P_x \subset C(X)$ ist wieder maximal: $\varphi^{-1}(P_x) = P_{g(x)}$. Somit legt der Ringhomomorphismus φ die zugrunde liegende Abbildung g eindeutig fest.

Da die stetigen Funktionen die Punkte in X trennen (kompakte Räume sind normal), gibt es für $x, y \in X$ eine Funktion $f \in C(X)$ gibt mit $f(x) \neq f(y)$. Daher sind die Ideale P_x (für $x \in X$) alle verschieden voneinander. In der Tat liefert dies genau die Menge $X = \text{Specm}(R)$ aller maximalen Ideale des Rings $R = C(X)$. [Gäbe es ein weiteres maximales Ideal P in $C(X)$, dann gibt es zu jedem Punkt $x \in X$ ein $f_x \in C(X)$ mit $f_x \in P, f_x \notin P_x$. Das heißt $f_x(x) \neq 0$, obdA > 0 . Durch Multiplikation mit der stetigen Funktion $\max(0, f_x)$ kann dann obdA angenommen werden $f_x \geq 0$. Wegen Kompaktheit existiert eine endliche Menge $S \subset X$ mit $f = \sum_{x \in S} f_x > 0$. Einerseits ist $f \in P$. Andererseits ist $1/f$ in $C(X)$. Ein Widerspruch.]

In der kommutativen Algebra versucht man diesen Gedanken umzudrehen, indem man jedem kommutativen Ring R einen topologischen Raum $X = \text{Spec}(R)$ zuordnet. Eigentlich würde man gerne für X die Menge der maximalen Ideale von R nehmen. Ein Ringhomomorphismus $\varphi : R \rightarrow S$ hat aber im allgemeinen nicht mehr die Eigenschaft, daß Urbilder von maximalen Idealen maximal sind. Geht man aber von maximalen Idealen auf die größere Menge der Primideale oder gar Primär ideale über, dann ist die entsprechende Aussage aber erfüllt. Urbilder von Primidealen sind Primideale, Urbilder von Primär idealen sind Primär ideale. Man definiert daher $X = \text{Spec}(R)$ als die Menge der Primideale und versieht diese mit einer geeigneten Topologie, der Zariski Topologie.

Ganze Ringerweiterungen

1 Endliche Ringerweiterungen

Sei $\varphi : R \rightarrow S$ ein Ringhomomorphismus zwischen kommutativen Ringen mit Eins, im folgenden kurz Ringerweiterung genannt. Per Definition des Ringhomomorphismus werden die Einselemente aufeinander abgebildet. Wir schreiben dann $r \in S$ anstatt $\varphi(r) \in S$ für Elemente $r \in R$, obwohl φ nicht notwendigerweise injektiv sein muß.

Definition: Ein Element $s \in S$ heißt ganz über R (bezüglich einer Ringerweiterung $R \rightarrow S$), wenn es $r_1, \dots, r_n \in R$ gibt mit der Eigenschaft

$$s^n + r_1 s^{n-1} + \dots + r_n = 0$$

in S , d.h. s erfüllt eine sogenannte Ganzheitsgleichung.

Definition: Eine Ringerweiterung $R \rightarrow S$ heißt ganz, wenn jedes $s \in S$ ganz über R ist.

Es gibt einen engen Zusammenhang mit dem Begriff der endlichen Ringerweiterung

Definition: Eine Ringerweiterung $R \rightarrow S$ heißt endlich, wenn S als R -Modul endlich erzeugt ist.

Wie bei Körpererweiterungen zeigt man leicht

Satz: Sind $R \rightarrow S$, $S \rightarrow T$ endliche Ringhomomorphismen, dann ist die Zusammensetzung $R \rightarrow T$ wieder endlich.

Hilfssatz: Jede endliche Ringerweiterung $R \rightarrow S$ ist ganz.

Beweis: Seien b_1, \dots, b_n Erzeugende des R -Moduls S und obdA $b_1 = 1_S$. Dann gibt es $r_{ji} \in R$ mit

$$s \cdot b_j = \sum_{i=1}^n r_{ji} \cdot b_i .$$

Dies definiert eine Matrix $\mathbf{R} \in M_{nn}(R)$. Setzt man $\mathbf{M} = \mathbf{R} - s \cdot \mathbf{E}$ und ist $\tilde{\mathbf{M}}$ die Komplementärmatrix von $\mathbf{M} \in M_{nn}(S)$, dann gilt $\tilde{\mathbf{M}} \cdot \mathbf{M} = \det(\mathbf{M}) \cdot \mathbf{E}$ (Graßmannkalkül !). Die ursprünglichen Gleichungen

$$\sum_i M_{ji} \cdot b_i = 0$$

multipliziert mit \tilde{M}_{kj} liefern daher nach Summation über j die Gleichungen $\det(\mathbf{M}) \cdot b_k = 0$, für $k = 1$ wegen $b_1 = 1_S$ daher

$$\det(\mathbf{M}) = 0 .$$

Wegen $(-1)^n \det(\mathbf{M}) = s^n - \text{spur}(\mathbf{R})s^{n-1} \pm \dots + (-1)^n \det(\mathbf{R})$ ist dies eine Ganzheitsgleichung für s über R .

Eine ganze Ringerweiterung $R \rightarrow S$ ist nicht notwendig endlich, aber es gilt

Lemma 1.1. *Für $s \in S$ sind äquivalent*

- a) s ist ganz über R .
- b) Die von s und R in S erzeugte Teilalgebra $R[s] \subset S$ ist endlich über R .
- c) Die Ringerweiterung $R \rightarrow S$ faktorisiert $R \rightarrow \tilde{S} \rightarrow S$, wobei $R \rightarrow \tilde{S}$ eine endliche Ringerweiterung mit $s \in \tilde{S}$ (genauer im Bild von \tilde{S}).

Beweis: Klar. Außer dem Hilfssatz benutzt dies nur, daß $R[s]$ als R -Modul erzeugt wird von den Monomen $1, s, s^2, \dots, s^{n-1}$ im Fall einer Ganzheitsgleichung vom Grad n .

Korollar: *Sind $R \rightarrow S$ und $S \rightarrow T$ ganze Ringhomomorphismen, dann ist auch die Zusammensetzung $R \rightarrow S$ ganz.*

Beweis: Für $t \in T$ seien $s_1, \dots, s_n \in S$ die Koeffizienten einer Ganzheitsgleichung. Dann gilt

$$t \in R[s_1, \dots, s_n, t] .$$

Da $R[s_1]$ endlich über R , $R[s_1, s_2] = R[s_1][s_2]$ endlich über $R[s_1]$ etc., ist am Ende $R[s_1, \dots, s_n, t]$ endlich über R und somit t ganz über R . Benutze Lemma 1(c).

Zum Abschluß

Lemma 1.2. *Ist $R \rightarrow T$ ganz und S multiplikativ abgeschlossen in R . Dann ist auch die induzierte Ringerweiterung*

$$S^{-1}R \rightarrow S^{-1}T$$

(*universelle Eigenschaft der Lokalisierung !*) wieder ganz.

Beweis: Genügt t der Ganzheitsgleichung $t^n + r_1 t^{n-1} + \dots + r_n = 0$ über R , dann genügt t/s folgender Ganzheitsgleichung über $S^{-1}R$

$$(t/s)^n + (r_1/s)(t/s)^{n-1} + \dots + (r_n/s^n) = 0 .$$

2 Der ganze Abschluß von R in S

Sei $R \rightarrow S$ eine Ringerweiterung. Dann bilden die über R ganzen Elemente von S einen Teilring $\text{Int}_R(S)$ von S mit Eins

$$\begin{array}{ccc} \text{Int}_R(S) & \hookrightarrow & S \\ & \nwarrow \nearrow & \\ & R & \end{array} ,$$

den ganzen Abschluß von R in S .

Beweis: Sind s_1, s_2 ganz über R , dann sind $R[s_1]$ und $R[s_2]$ endlich über R in S . Somit ist auch $R[s_1, s_2] = R[s_1][s_2]$ endlich über R . Da $1, s_1 \cdot s_2, s_1 \pm s_2 \in R[s_1, s_2]$, sind diese Elemente wieder ganz über R wegen Lemma 1.1(c).

Beispiel: Ist L eine endliche Körpererweiterung von \mathbb{Q} , dann nennt man den ganzen Abschluß $\text{Int}_{\mathbb{Z}}(L)$ von \mathbb{Z} in L den Ring \mathcal{O}_L der ganzen Zahlen in L .

Offensichtlich ist die Bildung des ganzen Abschlußes funktoriell in folgendem Sinn. Ist

$$\begin{array}{ccc} S_1 & \xrightarrow{\sigma} & S_2 \\ \uparrow & & \uparrow \\ R_1 & \longrightarrow & R_2 \end{array}$$

ein kommutatives Diagramm von Ringerweiterungen, dann induziert die Einschränkung von σ ein kommutatives Diagramm

$$\begin{array}{ccc} \text{Int}_R(S_1) & \xrightarrow{\sigma} & \text{Int}_R(S_2) \\ \uparrow & & \uparrow \\ R_1 & \longrightarrow & R_2 \end{array}$$

Dies ist klar, denn das Bild $\sigma(s_1)$ von $s_1 \in \text{Int}_R(S_1)$ genügt in S_2 über R_2 ‘derselben’ Ganzheitsgleichung wie s_1 in S_1 über R_1 . Insbesondere gilt daher $\sigma(s_1) \in \text{Int}_R(S_2)$.

Lemma 2.1. *Sei R ein faktorieller Ring (= Integritätsbereich mit eindeutiger Primfaktorzerlegung) mit Quotientenkörper $K = \text{Quot}(R)$. Dann gilt*

$$\text{Int}_R(K) = R ,$$

d.h. R ist ein normaler Ring, d.h. nullteilerfrei und ganz abgeschlossen in K .

Dies zeigt, daß typischer Weise Lokalisierungen $R \rightarrow R_S$ nicht ganz sind. Wir werden das später noch genauer untersuchen.

Beweis: Sei $x = r/s \in \text{Int}_R(K)$ mit r, s aus R und $s \neq 0$. Aus der Existenz einer Ganzheitsgleichung für x folgt

$$r^n + s \cdot (r_1 \cdot r^{n-1} + \dots + s^{n-1} \cdot r_n) = 0 .$$

Somit gilt für jeden Primteiler π von s auch $\pi|r^n$, also dann auch $\pi|r$. Also folgt durch Kürzen obdA $s = 1$ beziehungsweise $x \in R$. Q.e.d.

Kriterium: Ist $R \subset K = R_S$ ein Ring mit Quotientenkörper K . Sei R nicht ganz abgeschlossen in K mit $x = r/s \in \text{Int}_R(K) \setminus R$. Dann folgt $[r] \neq 0$ in R/sR sowie $[r]^n = 0$ in R/sR (für ein $n \in \mathbb{N}$). Das heißt $[r]$ ist nilpotent in R/sR .

Lemma 2.2. *Sei K der Quotientenkörper eines faktoriellen Ringes R und $\text{Int}_R(L)$ der ganze Abschluß von R in einem endlichen Erweiterungskörper L von K . Dann existiert für jedes $x \in L$ ein $0 \neq m \in R$ mit $m \cdot x \in \text{Int}_R(L)$. Insbesondere gilt $L = \text{Quot}(\text{Int}_R(L))$.*

Beweis: Sei $x^n + r_1 x^{n-1} + \dots + r_n = 0$ eine Ganzheitsgleichung von x über K mit $r_1, \dots, r_n \in K$. Sei $0 \neq m \in R$ so gewählt, daß gilt $m \cdot r_i \in R$. Durch Multiplikation der Ganzheitsgleichung mit m^n folgt dann sofort $m \cdot x \in \text{Int}_R(L)$.

3 Der Körperfall

Sind R und S Körper, ist eine Ringerweiterung $R \rightarrow S$ genau dann endlich, wenn gilt $\dim_R(S) < \infty$, also wenn es sich um eine endliche Körpererweiterung handelt. Über einem Körper R ganze Elemente nennt man synonym auch über R algebraische Elemente.

Wir betrachten jetzt Fälle, wo entweder R oder S ein Körper ist. Hierbei nehmen wir obdA an

$$R \hookrightarrow S$$

sei injektiv.

Lemma 3.1. *Sei $R \rightarrow S$ eine injektive, ganze Ringerweiterung und sei S ein Körper. Dann ist R ein Teilkörper.*

Beweis: Sei $r \neq 0$ in R und $s = r^{-1} \in S$. Multipliziert man eine Ganzheitsgleichung von s über R (vom Grad n) mit r^{n-1} erhält man $r^{-1} \in R$ wegen

$$r^{-1} + (r_1 + r_2 \cdot r + \cdots + r_n \cdot r^{n-1}) = 0 .$$

Lemma 3.2. *Sei R ein Körper und S ein Integritätsbereich und $R \rightarrow S$ eine (injektive), ganze Ringerweiterung. Dann ist S ein Körper.*

Beweis: Für $s \in S$ ist $R \rightarrow R[s]$ endlich erzeugt, also ist $R[s]$ ein endlich dimensionaler R -Vektorraum. Multiplikation mit s ist ein injektiver (!) R -linearer Endomorphismus von $R[s]$, also wegen LAI auch surjektiv. Somit hat die Gleichung $s \cdot x = 1$ eine Lösung $x \in R[s] \subset S$. Dies liefert das Inverse $x = s^{-1} \in S$.

Aus dem im nächsten Abschnitt bewiesenen Noetherschen Normalisierungssatz folgt jetzt unmittelbar

Korollar 3.3. *Sei $K \rightarrow S$ eine Körpererweiterung und ist S als Ring von K und endlich vielen Elementen $s_1, \dots, s_n \in S$ erzeugt, dann ist S endlich über K .*

Beweis: Es gibt einen Polynomring R in r Variablen über K , welcher in S enthalten ist, so daß S endlich und damit auch ganz über R ist (Noethers Normalisierungssatz). Dann ist nach dem vorletzten Lemma R ein Körper. Dies impliziert $r = 0$ bzw. $R = K$. Also ist S endlich über K .

4 Der Noethersche Normalisierungssatz

Substitutionen: Für $M \in M_{n,n}(K)$ (K ein kommutativer Ring) induziert die Einsetzung $t_i \mapsto \sum_j M_{ij} t_j$ einen Ringhomomorphismus φ_M des Polynomrings $K[t_1, \dots, t_n]$ in sich. Ist M invertierbar, dann ist φ_M ein Automorphismus.

Der Körperfall: Sei jetzt K ein Körper mit unendlich vielen Elementen und

$$f(t_1, \dots, t_n) = c_0(t_2, \dots, t_n) \cdot t_1^m + c_1(t_2, \dots, t_n) \cdot t_1^{m-1} + \dots + c_m(t_2, \dots, t_n)$$

ein Polynom $f \in K[t_1, \dots, t_n]$. Per Induktion nach n findet man leicht ein

$$\lambda = (\lambda_1, \dots, \lambda_n) \in (K^*)^n$$

mit $f(\lambda) \neq 0$. Für die lineare Variablensubstitution M

$$t_1 \mapsto \lambda_1 \cdot t_1, \quad t_2 \mapsto t_2 + \lambda_2 \cdot t_1, \quad \dots, \quad t_n \mapsto t_n + \lambda_n \cdot t_1$$

gilt dann

$$f(t_1, \dots, t_n) \mapsto f(\lambda_1, \lambda_2, \dots, \lambda_n) \cdot t_1^N + \text{niedere Term in } t_1.$$

Der Koeffizient $f(\lambda) \neq 0$ der höchsten Potenz von t_1 hängt daher nicht von den anderen Variablen t_2, \dots, t_n ab.

Folgerung: *Ist K ein unendlicher Körper und $0 \neq f \in R = K[t_1, \dots, t_n]$, dann gibt es einen K -Automorphismus φ von R derart, daß nach Anwendung der Transformation φ auf f gilt*

$$\varphi(f) = c_0 \cdot t_1^N + c_1(t_2, \dots, t_n)t_1^{N-1} + \dots + c_N(t_2, \dots, t_n) \quad , \quad 0 \neq c_0 \in K^* .$$

Bemerkung: Ist K ein endlicher Körper, dann induziert die Substitution

$$t_1 \mapsto t_1, \quad t_2 \mapsto t_2 + \lambda_2 \cdot t_1^{m_2}, \quad \dots, \quad t_n \mapsto t_n + \lambda_n \cdot t_1^{m_n}$$

einen Ringautomorphismus von $K[t_1, \dots, t_n]$. Bei geeigneter Wahl der $\lambda_i \in K^*$ und $m_i \in N$ (zum Beispiel geeignete Potenzen der Charakteristik) überträgt sich die Aussage der obigen Folgerung.

Eine Ringerweiterung $R \rightarrow S$ heißt endlich erzeugt, wenn es endlich viele Elemente s_1, \dots, s_n in S gibt, so daß S als Ring von R und s_1, \dots, s_n erzeugt wird. Mit anderen Worten, der Einsetzungshomomorphismus

$$R[t_1, \dots, t_n] \rightarrow S$$

vom Polynomring, welcher die Variablen t_i auf $s_i \in S$ abbildet, ist surjektiv. Somit gilt $S \cong R[t_1, \dots, t_n]/I$ für ein Ideal $I \subset R[t_1, \dots, t_n]/I$. Umgekehrt sind alle Ringe dieser Gestalt endlich erzeugt über R .

Satz: *Ist R endlich erzeugt über einem Körper K , dann ist R eine endliche Ringerweiterung eines (geeigneten) Polynomrings $K[y_1, \dots, y_r] \subset R$.*

Beweis: Sei R über K von den Elementen $t_1, \dots, t_n \in R$ als Ring erzeugt. Dann ist entweder $R = K[t_1, \dots, t_n]$ isomorph zum Polynomring, oder (man kann

man durch Übergang zu neuen Erzeugern mittels einer Variablensubstitution obdA annehmen)

$$f(t_1, \dots, t_n) = c_0 \cdot t_1^N + c_1(t_2, \dots, t_n) \cdot t_1^{N-1} + \dots + c_N(t_2, \dots, t_n) = 0$$

für ein Polynom $f \neq 0$ mit $c_0 \in K^*$. Teilt man durch c_0 , dann erfüllt t_1 eine Ganzheitsgleichung über dem Teilring $K[t_2, \dots, t_n] \subset R$, und man schließt nun per Induktion nach der Zahl der Ringerzeuger.

Übungsaufgabe: Sei R endlich erzeugt über \mathbb{Z} und p eine Primzahl. Dann existiert ein $N \in \mathbb{Z}$ teilerfremd zu p , so daß die Lokalisierung R_N endlich ist über einem geeigneten Polynomring $\mathbb{Z}[\frac{1}{N}][y_1, \dots, y_r]$ in R_N .

Das Spektrum eines Ringes

5 Die Zariski Topologie

Für einen Ring R bezeichne $X = \text{Spec}(R)$ die Menge seiner Primideale und $|X| = \text{Specm}(R) \subset \text{Spec}(R)$ die Teilmenge der maximalen Ideale. Betrachtet man Ideale I mit $1 \notin I$, so folgt aus dem Zornschen Lemma: $\text{Specm}(R)$ ist nicht leer, genau dann wenn gilt $R \neq \{0\}$. Jeder Ringhomomorphismus

$$f : R \rightarrow S$$

induziert dann eine Abbildung

$$\text{Spec}(f) : \text{Spec}(S) \rightarrow \text{Spec}(R)$$

in der umgekehrten Richtung durch

$$P \mapsto f^{-1}(P).$$

Offensichtlich ist $f^{-1}(P)$ wegen $a \cdot b \in f^{-1}(P) \implies f(a) \cdot f(b) \in P \implies f(a) \in P$ oder $f(b) \in P \implies a$ oder $b \in P \implies a$ oder $b \in f^{-1}(P)$ wieder ein Primideal.

Klar ist auch, daß Spec einen kontravarianten Funktor von der Kategorie der Ringe mit 1 in die Kategorie der Mengen definiert.

Für Ideale I von R betrachten wir nun die Teilmengen

$$V(I) = \{P \supset I \mid P \text{ prim}\}$$

in $\text{Spec}(R)$. Das Symbol V steht für ‘Varietät’ und ‘Verschwinden’. Es gilt

Lemma:

- $X = V(\{0\})$
- $\emptyset = V(R)$, genauer $V(I) = \emptyset \iff I = R$
- $\bigcap_{\nu} V(I_{\nu}) = V(\text{ggT}(I_{\nu}))$
- $V(I_1) \cup \dots \cup V(I_n) = V(I_1 \cdot \dots \cdot I_n)$

Hierbei bezeichne $\text{ggT}(I_{\nu})$ das von allen I_{ν} aufgespannte Ideal in R . Für die letzte Beziehung beachte: Für Ideale I, J in R bezeichne $I \cdot J$ das von allen endlichen Summen $\sum_{\nu} i_{\nu} \cdot j_{\nu}$ ($i_{\nu} \in I, j_{\nu} \in J$) aufgespannte Ideal von R . Es gilt dann $(I \cdot J) \cdot K = I \cdot (J \cdot K)$. Die letzte Identität des Lemmas folgt aus

$$I_1 \cdot I_2 \subset P \text{ prim} \implies I_1 \subset P \text{ oder } I_2 \subset P$$

und somit $I_1 \cdot I_2 \subset P$. Nur die erste Implikation bedarf der Begründung. Dazu: Ist $I_1 \not\subset P$, dann existiert $i_1 \notin P$. Aus $i_1 \cdot i_2 \in P$ und der Primidealeigenschaft von P , folgt $i_2 \in P$ für alle $i_2 \in I_2$. Das heißt $I_2 \subset P$.

Folgerung: Die Teilmengen $V(I)$, $I \subset R$ Ideal definieren die abgeschlossenen Mengen einer Topologie auf $\text{Spec}(R)$, der sogenannten Zariskitopologie. Für diese Topologien sind die den Ringhomomorphismen $f : R \rightarrow S$ zugeordneten Abbildungen $\text{Spec}(f) : \text{Spec}(S) \rightarrow \text{Spec}(R)$ stetige Abbildungen.

Beweis: Klar wegen $\text{Spec}(f)^{-1}(V(I)) = V(J)$, wobei J das von den Elementen von $f(I)$ aufgespannte Ideal in S ist. Beachte für P prim in S und $I \subset R$ gilt: $P \in \text{Spec}(f)^{-1}(V(I)) \iff f^{-1}(P) \supseteq I \iff f^{-1}(P) \supseteq gT(I, \text{Kern}(f)) \iff P \supseteq f(I) \iff P \supseteq J$.

Jedes $V(I)$ besteht aus den Primidealen von R oberhalb des Ideals I . Diese Menge von Primidealen kann mit der Menge der Primideale des Quotientenrings $\pi : R \rightarrow R/I$ identifiziert werden. Somit gilt

$$\text{Spec}(\pi) : \text{Spec}(R/I) \xleftrightarrow{\sim} \text{Spec}(R) .$$

Im speziellen Fall der Abbildung $\text{Spec}(\pi)$ werden maximale Ideale auf maximale Ideale abgebildet (dies ist im allgemeinen nicht der Fall), und es gilt

$$\text{Spec}(\pi)(\text{Spec}(R/I)) = V(I) \subset \text{Spec}(R) .$$

Lokalisierung: Wir betrachten nun multiplikativ abgeschlossene Teilmengen S in R . Dazu gehört ein Lokalisierungs Homomorphismus

$$g : R \rightarrow R_S = S^{-1}R$$

und eine zugehörige Abbildung

$$\text{Spec}(g) : \text{Spec}(R_S) \rightarrow \text{Spec}(R) .$$

Wir nehmen an $0 \notin S$. Dann ist $R_S \neq \{0\}$ und somit $\text{Spec}(R_S) \neq \emptyset$.

Lemma: Die Abbildung $\text{Spec}(g)$ ist injektiv mit dem Bild

$$\boxed{\text{Bild}(g) = \{P \in \text{Spec}(R) \mid P \cap S = \emptyset\}} .$$

Beweis: Für Primideale P in R_S gilt

$$S \cap g^{-1}(P) = \emptyset ,$$

da Elemente von S Einheiten in R_S werden, und Einheiten wegen $P \neq R_S$ in keinem Primideal liegen können.

Sei umgekehrt p ein Primideal in R mit $p \cap S = \emptyset$. Setze $P = S^{-1}p = R_S \cdot g(p)$. Dann gilt

$$g^{-1}(P) = g^{-1}(S^{-1}p) = p .$$

Denn für $x = r/s$ mit $r \in p, s \in S$ impliziert $x \in R$ dann $s \cdot x \in p$ und somit $x \in p$ (wegen $s \notin p$). Außerdem ist P prim in R_S , denn für $r_1/s_1 \cdot r_2/s_2 = r/s$ impliziert $r \in p, s \in S$ (oder $r/s \in P$) dann $sr_1r_2 \in p$. Da p prim ist, folgt $sr_1 \in p$ oder $r_2 \in p$. Somit gilt entweder $r_1/s_1 \in S^{-1}p$ oder $r_2/s_2 \in S^{-1}p$. Also ist $P = S^{-1}p$ ein Primideal. (Bemerkung: Der Schluß $g^{-1}(S^{-1}I) = I$ überträgt sich auf primäre Ideale¹ I von R).

Injektivität: Seien P_1, P_2 Primideale von R_S mit $g^{-1}(P_1) = g^{-1}(P_2)$. Wir zeigen $P_1 = P_2$. Dazu genügt $P_1 \subset P_2$ wegen Symmetrie. Sei $x = r/s$ aus P_1 mit $r \in g^{-1}(P_1) = g^{-1}(P_2) =: p_2$. Es folgt $x \in S^{-1}p_2 = P_2$. Also $P_1 \subset P_2$. Damit ist das Lemma gezeigt.

Beachte: $P = S^{-1}g^{-1}(P)$.

6 Eine Basis der offenen Mengen

In gewisser Weise würde man die Elemente f des Rings R gerne als Funktionen auf dem Raum

$$X = \text{Spec}(R)$$

auffassen mit den Funktionswerten

$$f(P) := f \bmod P \in R/P .$$

Das macht natürlich keinen Sinn, da die Werte dieser ‘Funktion’ ja dann in den Ringen R/P liegen würde, was von Punkt zu Punkt variiert. Man muß dann schon $\bigoplus_P R/P$ als Bild wählen

$$f : X \rightarrow \bigoplus_P R/P .$$

Was aber dann in jedem Fall sinnvoll ist, ist die Aussage ob f in P eine Nullstelle besitzt. Gleichbedeutend mit $f(P) = 0$ ist dann $f \in P$ oder

¹D.h. Ideale $I \neq R$ mit $x \notin I, y \notin I, x \cdot y \in I \implies \exists N$ mit $x^N, y^N \in I$

$(f) = R \cdot f \subset P$. Die Menge der Nullstellen von f in $\text{Spec}(R)$ ist daher die abgeschlossene Teilmenge

$$V(I) \quad , \quad I = (f)$$

oder kurz $V(f)$ aller Primideale, welche das Hauptideal I enthalten.

Die erste interessante Beobachtung ist nun, daß für nilpotente Elemente $f \in R$, d.h. für die es ein $n \in \mathbb{N}$ mit $f^n = 0$ gibt, gilt

$$V(f) = X \text{ .}$$

Mit anderen Worten: Nilpotente f definieren die Nullfunktion auf $\text{Spec}(R)$! Dies ist klar, da nilpotente f auf nilpotente Elemente in R/P abgebildet werden. Da die Ringe R/P als Quotienten nach Primidealen nullteilerfrei sind, folgt aus $(f \bmod P)^n = 0$ aber $f \bmod P = 0$.

Sei nun f nicht nilpotent. Dann ist $S = \{1, f, f^2, \dots\}$ eine multiplikativ abgeschlossene Teilmenge von R . Da sie nach Annahme 0 nicht enthält, folgt $R_S \neq \{0\}$, insbesondere also

$$X_f := \text{Spec}(R_S) \neq \emptyset \text{ .}$$

Wir schreiben auch R_f anstelle von R_S . Wir behaupten jetzt $V(f) \neq X$. Dies folgt aus der allgemeinen disjunkten Zerlegung

$$\boxed{X = X_f \sqcup V(f)} \text{ .}$$

Beachte nämlich für $P \in \text{Spec}(R)$ gilt wegen des letzten Lemmas: $P \notin X_f \iff S \cap P \neq \emptyset \iff f^n \in P \iff f \in P \iff P \supseteq (f) \iff P \in V(f)$.

Beachte $R_f = R_{f^n}$ und somit

$$X_f = X_{f^n} \text{ .}$$

X_f ist die Teilmenge, auf der f nicht verschwindet. Wir fassen zusammen

Lemma 6.1. *Die Teilmengen X_f , wobei f die Elemente des Rings R durchläuft, sind (für nicht nilpotentes f nichtleere) offene Teilmengen von $X = \text{Spec}(R)$ und bilden eine Basis der Topologie.*

Beweis: X_f ist offen, da das Komplement $V(f)$ abgeschlossen ist. Für eine beliebige offene Teilmenge $U = X \setminus V(I)$ gilt wegen $V(I) = \bigcap_{f \in I} V(f)$ aber

$$U = \bigcup_{f \in I} X_f \text{ .}$$

Für nilpotentes f gilt $X_f = \emptyset$.

Lemma 6.2. (Einheiten): Ist $f \in R$ ist genau dann eine Einheit $f \in R^*$ des Rings R , wenn $f \neq 0$ für alle Punkte $P \in X = \text{Spec}(R)$ – oder bereits $\text{Specm}(R)$ – gilt

$$f \in R^* \iff X_f = X .$$

Beweis: Für eine Einheit f existiert $r \in R$ mit $r \cdot f = 1$. Daraus folgt, daß auch die Restklasse von f in R/P eine Einheit ist. Somit folgt $f(P) \neq 0$.

Sei umgekehrt $f(P) \neq 0$ für alle $P \in \text{Spec}(R)$. Dann folgt $(f) = R$, denn anderenfalls gäbe es ein maximales Ideal P mit $(f) \subset P, 1 \notin P$ in dem f verschwindet. Aus $(f) = R$ folgt aber $f \in R^*$.

Punktetrennung: Sei P_1, \dots, P_r Primideale mit $P_i \not\subseteq P_j$ für $i \neq j$. Dann gibt es $f_i \in R$ mit $f_i(P_i) \neq 0$ aber $f_i(P_j) = 0$ für alle $j \neq i$. [Setze dazu $f_i = \prod_{j \neq i} f_{ij}$ für irgendwelche $f_{ij} \in R$ mit $f_{ij}(P_i) \neq 0$ und $f_{ij}(P_j) = 0$].

Lemma 6.3. $I \subset \bigcup_{i=1}^r P_i \implies I \subset P_i$ für ein i (I Ideal, P_1, \dots, P_r Primideale).

Beweis: Anderenfalls gäbe es $g_i \in I$ mit $g_i(P_i) \neq 0$ und $f = \sum_{i=1}^r g_i \cdot f_i$ wäre in I , aber $f(P_i) = 0, \forall P_i$. Widerspruch.

7 Das Nilradikal

Den Durchschnitt aller Primideale

$$\text{Nil}(R) = \bigcap_{P \in \text{Spec}(R)} P$$

nennt man das Nilradikal des Ringes R . Der Name erklärt sich aus folgendem

Lemma: f ist genau dann im Nilradikal von R , wenn f ein nilpotentes Element des Rings ist.

Beweis: Nilpotente f verschwinden auf $\text{Spec}(R)$. Somit $f \in P$ für alle P , d.h. $f \in \text{Nil}(R)$. Ist andererseits f nicht nilpotent, dann ist wie bereits gezeigt U_f nichtleer. Für $P \in U_f$ gilt dann $f \notin P$. Also $f \notin \text{Nil}(R)$.

Teilt man den Ring durch das Nilradikal, erhält man als Quotientenring den reduzierten Ring

$$R_{red} = R/Nil(R) .$$

Offensichtlich gilt

$$Nil(R_{red}) = \{0\},$$

denn aus $f^n \in Nil(R)$ folgt $(f^n)^m = 0$, also $f \in Nil(R)$. Die Bildung des reduzierten Rings ist funktoriell. Das heißt, man hat kommutative Diagramme

$$\begin{array}{ccc} R & \xrightarrow{f} & S \\ \pi \downarrow & & \downarrow \pi \\ R_{red} & \xrightarrow{f_{red}} & S_{red} \end{array}$$

8 Radikal-Ideale

Allgemeiner definiert man die Radikal-Ideale eines Ideals $I \subset R$ durch

$$Rad(I) = \bigcap_{P \in V(I)} P .$$

Offensichtlich ist $Rad(I)$ wieder ein Ideal und es gilt

$$I \subset Rad(I) .$$

Im Spezialfall $I = \{0\}$ gilt $Rad(0) = Nil(R)$. Offensichtlich gilt aber

$$V(I) = V(Rad(I)) .$$

Zum Beweis ersetzt man R durch den Quotient R/I und kann daher obdA annehmen $I = \{0\}$.

Lemma: $V(I_1) = V(I_2) \iff Rad(I_1) = Rad(I_2)$.

Beweis: Man kann obdA annehmen, daß $I_\nu = Rad(I_\nu)$ gilt. Aber solche Radikal-Ideale sind per Definition durch die Mengen $V(I_\nu)$ definiert.

Bemerkung: Im Fall $V(I) = \emptyset$ ist die Situation besonders einfach. Hier folgt immer $I = Rad(I) = R$, denn jedes Ideal $I \neq R$ besitzt ein Primideal $P \in V(I)$.

9 Zusammenhangskomponenten

Ringprodukte: Für kommutative Ringe R_i mit Eins (für $i = 0, 1$) setzen wir

$$R = R_0 \times R_1$$

mit komponentenweiser Multiplikation und Addition. Dann gilt $1_R = 1_{R_0} + 1_{R_1}$, $1_{R_0} \cdot 1_{R_1} = 0$ und R ist ein kommutativer Ring mit Eins. Die Elemente $e_i = 1_{R_i}$ bilden ein Paar von orthogonalen Idempotenten: $e_0^2 = e_0, e_1^2 = e_1$ und $e_0 e_1 = 0$ sowie $e_0 + e_1 = 1$. Weiterhin gilt $V(e_i) \cong \text{Spec}(R_{1-i})$. Orthogonale Idempotente: Ist umgekehrt $e_0 + e_1 = 1, e_0^2 = e_0, e_1^2 = e_1$ ein orthogonales Paar von Idempotenten eines Rings R . Dann sind $R_i = e_i \cdot R$ Ringe mit Einselement e_i . Es folgt $R = R_0 + R_1$ wegen $r = r_0 + r_1$ und $r_i = e_i \cdot r$. Die Zerlegung ist eindeutig wegen $R_0 \cap R_1 \subset R_0 \cdot R_1 = e_0 e_1 \cdot R = \{0\}$. Also $R = R_0 \oplus R_1$ und $(r_0 + r_1)(r'_0 + r'_1) = r_0 r'_0 + r_1 r'_1$ wegen $R_0 \cdot R_1 = 0$. Somit gilt

$$R = R_0 \times R_1 .$$

In der obigen Situation ist e_i eine Funktion auf $X = \text{Spec}(R)$ mit $e_i = 0$ auf $V(e_i)$. Wegen $1 = e_0 + e_1$ gilt daher $e_i = 0$ auf $A_i = V(e_i)$ und $e_i = 1$ auf $A_{1-i} = V(e_{1-i})$. Der Raum $X = \text{Spec}(R)$ zerfällt in die disjunkte Vereinigung zweier abgeschlossener Teilmengen

$$X = X_0 \sqcup X_1 \quad , \quad X_i = V(e_i) .$$

Da $e_1 - e_0 \in R$ auf X nirgendwo verschwindet, gilt $e_1 - e_0 \in R^*$.

Zerlegungen: Sei umgekehrt $X = \text{Spec}(R)$

$$X = X_0 \sqcup X_1$$

eine disjunkte Vereinigung von abgeschlossenen Teilmengen $A_i = V(I_i)$. Aus der Disjunktheit $X_0 \cap X_1 = \emptyset$ folgt dann $V(I_0 + I_1) = \emptyset$ und daher

$$I_0 + I_1 = R .$$

Aus $X_0 \cup X_1 = \text{Spec}(R)$ folgt

$$I_0 \cdot I_1 \subset \text{Nil}(R) .$$

Somit existieren Elemente $e_i \in I_i$ mit

$$e_0 + e_1 = 1$$

$$(e_0 \cdot e_1)^k = 0$$

für geeignetes $k \in \mathbb{N}$. Wir wollen durch absteigende Induktion nun zeigen, daß obdA hier $k = 1$ gewählt werden kann.

Ansatz: $\tilde{e}_0 = e_0 - x$, $\tilde{e}_1 = e_1 + x$ mit $x \in I_1 \cap I_2$.

Dieser Ansatz liefert $\tilde{e}_0 + \tilde{e}_1 = 1$ sowie $\tilde{e}_0 \cdot \tilde{e}_1 = e_0 \cdot e_1 + (e_1 - e_0)x - x^2$. Die Funktion $e_0 - e_1$ ist -1 auf A_0 und 1 auf A_1 , somit nirgends Null. Daher ist $e_0 - e_1$ eine Einheit in R . Wir setzen

$$x = -e_0 e_1 / (e_1 - e_0) \in I_0 \cdot I_1 .$$

Dann folgt $\tilde{e}_i \in I_i$ sowie $\tilde{e}_0 \cdot \tilde{e}_1 = -x^2$, also $(\tilde{e}_0 \cdot \tilde{e}_1)^{\lfloor k/2 \rfloor} = 0$. Wegen $\lfloor k/2 \rfloor < k$ für $k > 1$ können wir durch Iteration obdA von jetzt an $k = 1$ annehmen.

Wir nehmen nun $k = 1$ an: Dann sind e_0 und e_1 sogar Idempotente. Durch Multiplizieren mit e_i folgt $e_i^2 = e_i$. Also $R = R_0 \times R_1$ mit $R_i \subset I_i$ und $e_i \in I_i$. Wir behaupten, daß die Idempotenten e_i dadurch sogar eindeutig bestimmt sind.

Eindeutigkeit: Wäre $\tilde{e}_i \in I_i$ ein zweites Paar mit $1 = \tilde{e}_0 + \tilde{e}_1$, $\tilde{e}_i^2 = \tilde{e}_i$. Zerlegt man $R \ni \tilde{e}_0 = r_0 + r_1$ im obigen Sinn mit $r_i \in R_i \subset I_i$, dann sind auch $r_0 = e_0 \tilde{e}_0$ und $r_1 = e_1 \tilde{e}_0$ Idempotente. Andererseits ist $r_1 \in I_1 \cdot I_0 \subset \text{Nil}(R)$ nilpotent. Daraus folgt $r_1 = 0$. Es folgt $\tilde{r}_0 = r_0$. Ditto $\tilde{r}_1 = r_1$. Somit sind Zerlegung $R = R_1 \times R_2$ und Idempotente eindeutig durch die Bedingung $\text{Spec}(R_{1-i}) = X_i$ festgelegt. Also

Lemma 9.1. Disjunkte Zerlegungen $X = X_1 \sqcup X_2$ von $X = \text{Spec}(R)$ in abgeschlossene Teilmengen X_i entsprechen eindeutig Zerlegungen von R in direkte Produkte der Gestalt

$$\boxed{R = R_1 \times R_2} .$$

Hierbei gilt obdA $A_i \cong \text{Spec}(X_i)$.

Folgerung: $\text{Spec}(R)$ ist zusammenhängend genau dann wenn 0 und 1 die einzigen Idempotenten in R sind.

Beweis: Ein Idempotent e liefert Elemente $e_1 = e$ und $e_0 = 1 - e$ mit $e_0^2 = e_0$, $e_1^2 = e_1$ und $e_0 \cdot e_1 = 0$ und umgekehrt.

10 Eine Anwendung

Lemma 10.1. *Sind I_1, I_2 Ideale mit $I_1 + I_2 = R$, dann gilt $I_1 \cdot I_2 = I_1 \cap I_2$.*

Beweis: Die Inklusion \subset ist klar. Sei umgekehrt $x \in I_1 \cap I_2$ und $1 = i_1 + i_2$ mit $i_\nu \in I_\nu$. Dann ist $x = x \cdot i_1 + x \cdot i_2 \in I_1 \cdot I_2$.

Satz 10.2. *Ist K ein Körper und L eine endliche K -Algebra, dann gilt*

$$L \cong \bigoplus_i L_i \quad (\text{endliche Summe})$$

mit K -Algebren L_i , so daß alle $(L_i)_{\text{red}}$ endliche Körpererweiterungen von K sind.

Beweis: Schritt 1. Jedes Primideal P von L ist maximal, wegen Lemma 3.2 und $K \hookrightarrow L/P$. Daher ist $\{P\} = V(P)$ ein abgeschlossener Punkt (!) in $\text{Spec}(R)$.

Schritt 2. Für Primideale $P_i \neq P_j$ von L gilt wegen der Maximalität daher $P_i + P_j = L$ und somit (siehe obiges Lemma)

$$P_i \cap P_j = P_i \cdot P_j .$$

Schritt 3. Für Primideale P_1, \dots, P_r von L gilt

$$\bigcap_{i=1}^r P_i \subsetneq \bigcap_{i=1}^{r-1} P_i ,$$

denn andernfalls wäre $\bigcap_{i=1}^{r-1} P_i = P_1 \cdot \dots \cdot P_{r-1}$ [gilt per Induktion!] enthalten in P_r , und da P_r prim ist, wäre somit $P_i \subset P_r$ für ein $i = 1, \dots, r-1$ (siehe §5) im Widerspruch zu Schritt 1. [Induktionsschritt: Außerdem somit $P_r + \bigcap_{i=1}^{r-1} P_i = (1)$ wegen der Maximalität von P_r und daher $\bigcap_{i=1}^r P_i = P_1 \cdot \dots \cdot P_r$ wie in Schritt 2.]

Schritt 4. Jedes Primideal ist ein K -Vektorraum. Nach Schritt 3 folgt daher aus K -Dimensionsgründen, daß es nur endlich viele Primideale in L geben kann.

Schritt 5. Wie gezeigt ist $\text{Spec}(L)$ die endliche disjunkte Vereinigung von abgeschlossenen einpunktigen Mengen $\{P_i\}$. Somit wegen des letzten Paragraphen

$$L \cong \bigoplus_i L_i ,$$

wobei jetzt jedes L_i nur noch ein einziges Primideal besitzt. Also ist $(L_i)_{red}$ ein Körper, da Null sein (einziges) Primideal und gleichzeitig maximales Ideal ist.

Schritt 6. Die $L_i = L \cdot e_i$ sowie auch $(L_i)_{red}$ sind K -Vektorräume. Somit ist der Körper $(L_i)_{red}$ eine endliche Körpererweiterung von K . Q.e.d.

Bemerkung: L/K ist per Definition separabel, wenn die Kählerdifferentialie verschwinden: $\Omega(L/K) = 0$. Für L/K wie im letzten Satz ist dazu äquivalent $\Omega(L_i/K) = 0$ für alle i . $\Omega(L_i/K) = 0$ gilt genau dann, wenn $L_i = (L_i)_{red}$ ein Körper ist und L_i/K eine separable Körpererweiterung ist (siehe Appendix).

Beispiel: Sei M eine $n \times n$ -Matrix mit Koeffizienten in dem Körper $K = \mathbb{C}$. Sei L die von M in $M_{nn}(K)$ aufgespannte K -Unteralgebra. Wendet man das letzte Lemma in dieser Situation an, erhält man daraus die Zerlegung in Jordannormalformen. Insbesondere für eine Blockmatrix mit α auf der Diagonale und 1 in der unteren Nebendiagonale und Nullen sonst, gilt $\dim_K(L) = n$, aber

$$L_{red} = \mathbb{C}$$

sowie

$$M - \alpha \cdot E \in \text{Nil}(L) .$$

Dieser Zusammenhang mit der Eigenwerttheorie erklärt den Name Spektrum. Im allgemeinen entsprechen die Punkte von $\text{Spec}(L)$ den Jordanblöcken. Das Element $f = M \in L$ definiert die Funktion mit den Werten

$$f(P_i) = \alpha_i \in \mathbb{C} .$$

Appendix

Sei L eine endliche K -Algebra mit einelementigem Spektrum. Dann ist nach dem letzten Satz $L_{red} = L/I$ eine Körpererweiterung von K , wobei I das Radikal von L bezeichne. Man hat also folgende Ringerweiterungen

$$K \hookrightarrow S = K \cdot 1 \oplus I \hookrightarrow L .$$

Ist $I = 0$ und L_{red}/K separabel, dann ist L/K separabel. Die Umkehrung gilt auch

Lemma 10.3. *L/K ist genau dann separabel, wenn gilt $L = L_{red}$ und die Körpererweiterung L_{red}/K separabel ist.*

Beweis: Ist umgekehrt L/K separabel, dann ist L/S separabel (AI Lemma IX.3.5). Dann ist aber wegen $Der_S(L, M) = 0$ auch $Der_K(L_{red}, M) = 0$ für alle L_{red} -Vektorräume M . Also ist L_{red}/K separabel. Aus dem Satz vom primitiven Element für die separable Körpererweiterung L_{red}/K sowie AI Lemma IX.4.1 folgt dann schließlich: S/K ist separabel. Wir behaupten, dies impliziert $I = 0$, d.h. $L_{red} = L$. Wäre $I \neq 0$, dann folgt $I/I^2 \neq 0$ (benutze $I^n = 0$ für $n \gg 0$ oder das Nakayama Lemma in §12). Es genügt dann die Existenz von nichttrivialen K -Derivationen von S oder vom Quotienten S/I^2 , um einen Widerspruch abzuleiten. Wir können daher S durch S/I^2 ersetzen und obdA annehmen $I^2 = 0$. Dann gilt aber (!)

$$Der_K(S, M) = Hom_K(I, M)$$

für alle S -Moduln M . Ist S/K separabel, gilt per Definition $Der_K(S, M) = 0$ für alle M . Daher $I = 0$.

Maximale Ideale

11 Lokale Ringe

Ein Ring heißt lokaler Ring, wenn er ein einziges maximales Ideal besitzt.

Ist R ein beliebiger Ring und $P \in \text{Spec}(R)$, dann bilden die Elemente

$$S = R \setminus P$$

wegen der Primidealeigenschaft von P eine multiplikativ abgeschlossene Teilmenge von R . Die Lokalisierung R_S von R nennt man in diesem Fall die Lokalisierung nach dem Primideal P und schreibt R_P anstatt R_S

$$R \rightarrow R_P .$$

Lemma 11.1. R_P ist ein lokaler Ring. Bezüglich der von $R \rightarrow R_P$ induzierten Abbildung $\text{Spec}(R_P) \rightarrow \text{Spec}(R)$ wird das maximale Ideal von R_P gerade auf P abgebildet.

Genauer: Der Inklusionsverband der Primideale² von R_P entspricht dem Inklusionsverband der Primideale von R , welche in P enthalten sind.

Beweis: Ein Primideal P' von R liegt genau dann im Bild von $\text{Spec}(R_P)$, wenn gilt $P' \cap S = P' \cap (R \setminus P) = \emptyset$, d.h. aber

$$P' \subset P .$$

Mit anderen Worten: für $P \in X = \text{Spec}(R)$ gilt

$$\boxed{\text{Spec}(R_P) \cong \{P' \in X \mid P' \subset P\}} .$$

Q.e.d.

Wir bemerken an dieser Stelle, daß andererseits per Definition gilt

$$V(P) = \{P'' \in X \mid P \subset P''\} .$$

Dabei ist $V(P)$ die kleinste abgeschlossene Teilmenge von X , welche den Punkt $P \in X$ enthält. Also ist $V(P)$ der Abschluß der einpunktigen Menge $\{P\} \subset X$ in der Zariskitopologie

$$\boxed{\overline{\{P\}} = \{P'' \in X \mid P \subset P''\}} .$$

²Analog entsprechen die Primär Ideale von R_P den Primär Idealen von R , welche in P enthalten sind.

Folgerung: Ein Punkt $P \in X = \text{Spec}(R)$ ist genau dann abgeschlossen als Teilmenge von X , wenn P ein maximales Ideal von R ist.

Die lokalen Ringe R sind also genau jene, für die $\text{Spec}(R)$ genau einen abgeschlossenen Punkt besitzt. Aus Lemma 6.2 folgt weiterhin, daß für einen lokalen Ring R mit maximalem Ideal m gilt

$$R^* = R \setminus m .$$

12 Das Jacobson Radikal

Sei R ein von Null verschiedener Ring, dann ist das Jacobson Radikal definiert als der Durchschnitt

$$\text{Rad}_J(R) = \bigcap_{P \in \text{Specm}(R)} P$$

aller maximalen Ideale P . Offensichtlich gilt auf Grund der Definition $\text{Nil}(R) \subset \text{Rad}_J(R)$.

Jedes Element

$$1 + r \quad , \quad r \in \text{Rad}_J(R)$$

ist nach Lemma 6.2 eine Einheit.

Nakayama Lemma: Sei

$$I \subset \text{Rad}_J(R)$$

ein Ideal von R und M ein endlich erzeugter R -Modul. Dann gilt

$$I \cdot M = M \implies M = \{0\} .$$

Beispiel: Für lokal noethersches³ R mit maximalem Ideal I folgt $\bigcap_{n=0}^{\infty} I^n = 0$.

Durch Übergang zum Quotient M/N erhält man die

Variante: $M = N + I \cdot N'$ impliziert $M = N$ für Untermoduln N, N' . (Es genügt sogar nur anzunehmen, daß N' endlich erzeugt ist).

³siehe §16

Beweis: Sei e_1, \dots, e_n ein Erzeugendensystem von M von minimaler Länge. Aus $e_n = i_1 e_1 + \dots + i_n e_n$ ($i_\nu \in I$) folgt $e_n = (1 - i_n)^{-1}(i_1 e_1 + \dots + i_{n-1} e_{n-1})$ im Widerspruch zur Minimalität von n falls $M \neq 0$. Beachte, daß $1 - i_n$ eine Einheit ist wegen $i_n \in \text{Rad}_J(R)$.

13 Der Hilbertsche Nullstellensatz

Für jeden Ring gilt $\text{Nil}(R) \subset \text{Rad}_J(R)$. Im allgemeinen gilt hier aber nicht das Gleichheitszeichen. Das sieht man schon am Beispiel $R = \mathbb{Z}_{(p)}$ (Lokalisierung im Punkt p): Dann ist $\text{Nil}(R) = \{0\}$ und $\text{Rad}_J(R) = (p)$.

Man sagt daher: Der Hilbertsche Nullstellensatz gilt für R , wenn

$$\boxed{\text{Nil}(R) = \text{Rad}_J(R)}$$

erfüllt ist. Mit anderen Worten besagt der

Nullstellensatz: Eine ‘Funktion’ $f \in R$ verschwindet auf $X = \text{Spec}(R)$ bereits identisch, wenn f auf den abgeschlossenen Punkten verschwindet.

Annahme: *Der Ring R besitze folgende Eigenschaft: Die von $R \rightarrow R[t]$ (Polynomring über R) induzierte Abbildung*

$$\mathbb{A}_X = \text{Spec}(R[t]) \xrightarrow{\pi} X = \text{Spec}(R)$$

bildet abgeschlossene Punkte auf abgeschlossene Punkte ab.

Im nächsten Paragraphen geben wir Beispiele für solche Ringe R an.

Frage: Was geht schief im Fall $R = \mathbb{Z}_{(p)}$?

(Antwort: Das maximale Ideal $x = \text{Kern}(\varphi)$ des Kerns von $\varphi : \mathbb{Z}_{(p)}[t] \rightarrow \mathbb{Q}$ mit $\varphi(t) = 1/p$, wird auf das Primideal $P_x = \text{Kern}(\varphi|_{\mathbb{Z}_{(p)}}) = 0$ abgebildet. $P_x = 0$ ist prim, aber nicht mehr maximal!)

Lemma: *Ist obige Annahme für R erfüllt, dann gilt der Hilbertsche Nullstellensatz für den Ring R .*

Beweis: Andernfalls gäbe es ein $f \in R$, das Null auf $\text{Specm}(R)$ aber nicht nilpotent ist; insbesondere $R_f \neq 0$ sowie $\text{Specm}(R_f) \neq \emptyset$. Für ein maximales Ideal $x \in \text{Spec}(R_f) = X_f$ bezeichne $P_x \in \text{Spec}(R) = X$ das Bild in $\text{Spec}(R)$

$$X_f \hookrightarrow X \quad .$$

$$x \longmapsto P_x$$

Angenommen, P_x ist wieder ein maximales Ideal. Dann folgt – wegen der disjunkten Zerlegung $X = X_f \sqcup V(f)$ – also $(f) \not\subseteq P_x$ bzw $f \notin P_x$ im Widerspruch zu $f \in \text{Rad}_J(R) = \bigcap_{P \in \text{Specm}(R)} P$. Es genügt also die Maximalität von P_x zu zeigen.

Dazu benutzen wir eine neue Beschreibung der Lokalisierung R_f , nämlich

$$R_f \cong R[t]/(f \cdot t - 1)$$

(der Ring auf der rechten Seite erfüllt die universelle Eigenschaft der Lokalisierung!). Wegen $R \rightarrow R[t] \rightarrow R[t]/(f \cdot t - 1) = R_f$ faktorisiert daher die Einbettung $X_f \hookrightarrow X$ in der Form

$$\begin{array}{ccc} X_f & \xrightarrow{\iota} & \mathbb{A}_X \\ & \searrow & \downarrow \pi \\ & & X \end{array} \quad .$$

Die erste Abbildung ι bildet abgeschlossene Punkt auf abgeschlossene Punkte ab, da sie von einer Ringquotientenabbildung induziert wird; die zweite Abbildung π tut dies ebenfalls auf Grund unserer Annahme an R . Somit ist P_x abgeschlossener Punkt in $\text{Spec}(R)$, also P_x maximal.

14 Endlich erzeugte R -Algebren

Wir betrachten einen Ring R mit folgender Eigenschaft

Annahme: *Für jede Ringerweiterung*

$$\varphi : R \rightarrow L$$

von R in einen Körper L , so daß L als Ring endlich erzeugt über $\varphi(R)$ ist, ist das Bild von R ein Körper

$$K_\varphi = \varphi(R) .$$

(Beispielsweise: R ist selbst ein Körper).

Für einen solchen Ring R betrachten wir die Kategorie der endlich erzeugten R -Algebren. Objekte sind alle Ringerweiterungen $R \rightarrow A$, welche aus R durch Polynomringbildung und Quotientenbildung hervorgehen. Jede solche Ringerweiterung ist also ein Quotient des Polynomrings in n Unbestimmten für geeignetes $n \in \mathbb{N}$

$$R \rightarrow R[t_1, \dots, t_n]/I = A .$$

Morphismen sind die R -Algebrenhomomorphismen, also die Ringhomomorphismen über R . Die maximalen Ideale einer solchen R -Algebra A sind die maximalen Ideale des Polynomrings $R[t_1, \dots, t_n]$, welche das Ideal I enthalten.

Maximale Ideale des Polynomrings sind Kerne von surjektiven R -Algebren Homomorphismen

$$\varphi : R[t_1, \dots, t_n] \twoheadrightarrow L$$

auf Körpererweiterungen L von R . L ist dann als Ring endlich erzeugt über $\varphi(R)$ (mit n Erzeugenden). Nach obiger Annahme an R folgt daraus, daß $\varphi(R) = R/m$ selbst ein Körper ist. Das zugehörige durch φ bestimmte maximale Ideal m von R liefert eine Faktorisierung von φ

$$\begin{array}{ccc} R[t_1, \dots, t_n] & \xrightarrow{\varphi} & L \\ & \searrow \pi_m & \nearrow \exists! \\ & (R/m)[t_1, \dots, t_n] & \end{array}$$

Der recht untere Pfeil ist dabei ein Einsetzungshomomorphismus, welcher die Variablen t_i auf ihre Bilder $\alpha_i \in L$ abbildet

$$t_i \mapsto \alpha_i \quad (i = 1, \dots, n) .$$

Aus Korollar 3.3 folgt, daß alle α_i algebraisch über dem Körper R/m sind. Da die α_i den Körper L über R/m erzeugen, folgt

$$[L : (R/m)] < \infty .$$

Umgekehrt: Ist m ein maximales Ideal von R und $\alpha_1, \dots, \alpha_n$ algebraisch über R/m , L die davon erzeugte endliche Körpererweiterung von R/m , dann definiert der Kern des zugehörigen Einsetzungshomomorphismus $R[t_1, \dots, t_n] \twoheadrightarrow L$ ein maximales Ideal.

Aus dieser expliziten Beschreibung der maximalen Ideale, welche aus der oben gemachtem Annahme an R folgt, ergibt sich

Folgerung 14.1. *Die maximalen Ideale des Polynomrings $\mathbb{C}[t_1, \dots, t_n]$ entsprechen eineindeutig den Punkten $(\alpha_1, \dots, \alpha_n)$ des \mathbb{C}^n .*

$$\boxed{\text{Specm}(\mathbb{C}[t_1, \dots, t_n]) \cong \mathbb{C}^n} .$$

Folgerung 14.2. *Die von einem R -Algebrenhomomorphismus $\psi : A \rightarrow A'$ zwischen endlich erzeugten R -Algebren induzierte Abbildung*

$$\text{Spec}(\psi) : \text{Spec}(A') \rightarrow \text{Spec}(A)$$

bildet abgeschlossene Punkte auf abgeschlossene Punkte ab

$$\text{Spec}(\psi) : \text{Specm}(A') \rightarrow \text{Specm}(A) .$$

Beweis: ObdA kann $A = R[t_1, \dots, t_n]$ angenommen werden.

Sei $\varphi' : A' \twoheadrightarrow L'$ die Quotientenabbildung nach einem maximalen Ideal m'_x von A' für $x \in \text{Specm}(A')$. Der Kern der Zusammensetzung

$$\varphi' \circ \psi : R[t_1, \dots, t_n] \rightarrow L'$$

ist das Primideal $P = \text{Spec}(\psi)(x)$. Sei $L = \text{Bild}(\varphi' \circ \psi)$.

L ist ein endlich erzeugter Erweiterungsring des Körpers $R/(P \cap R) \cong R/(m \cap R)$ im Körper L' , also ein Integritätsbereich. Die Erzeugenden α_i liegen in der endlichen Körpererweiterung L' von $K_\varphi := R/(P \cap R)$, sind also algebraisch über dem Körper K_φ . Somit ist L also ganze integre Ringerweiterung des Körpers K_φ selbst ein Körper (Lemma 3.2). Also ist das Primideal P ein maximales Ideal. q.e.d.

Aus der Folgerung 14.2 und den Ausführungen des vorangegangenen Paragraphen folgt

Folgerung 14.3. *Gilt obige Annahme gilt für den Ring R , dann gilt der Hilbertsche Nullstellensatz für jede endlich erzeugte R -Algebra A .*

Korollar 14.4. *Für eine endlich erzeugte Algebra A über \mathbb{Z} oder über einem Körper gilt der Hilbertsche Nullstellensatz.*

Beweis: Wir müssen zeigen, daß unsere Annahme im Fall $R = \mathbb{Z}$ erfüllt ist. Dazu sei $\varphi : \mathbb{Z} \rightarrow L$ eine endlich erzeugte Ringerweiterung und L sei ein Körper. Es ist zu zeigen, daß φ über einen endlichen Quotient $\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$ faktorisiert, da dann gilt $\varphi(\mathbb{Z}) = \mathbb{F}_p$. Wir behaupten dies ist immer der Fall. Anderenfalls wäre nämlich $\varphi(\mathbb{Z}) = \mathbb{Z}$ ein Unterring von L . Somit gilt auch $\mathbb{Q} \subset L$ und L ist eine endlich erzeugte Körpererweiterung von \mathbb{Q} . Aus Korollar 3.3 folgt $[L : \mathbb{Q}] < \infty$. Seien $r_1, \dots, r_n \in L$ die endlich vielen Ringerzeuger von L über \mathbb{Z} . Es gibt dann ein $0 \neq N \in \mathbb{N}$ mit $N \cdot r_i \in \mathcal{O}_L$ (Lemma 2.2). Es folgt $\mathcal{O}_L[\frac{1}{N}] = L$. Aber $\mathcal{O}_L[\frac{1}{N}] \cap \mathbb{Q} = \mathbb{Z}[\frac{1}{N}]$ (Lemma 1.2 und 2.1) ist nicht $L \cap \mathbb{Q} = \mathbb{Q}$. Dies ist ein Widerspruch und zeigt die Behauptung.

15 Eine Umformulierung

Wir geben in diesem Abschnitt einige offensichtliche Umformulierungen des Hilbertschen Nullstellensatzes für Ringe vom Typ $\overline{R} = \mathbb{C}[t_1, \dots, t_n]/I$:

Seien f_1, \dots, f_r Polynome des Polynomrings $R = \mathbb{C}[t_1, \dots, t_n]$ und

$$I = (f_1, \dots, f_r)$$

das von diesen Polynomen erzeugte Ideal von R . Dann gilt

$$V(I) \cap \text{Specm}(R) = \{z \in \mathbb{C}^n \mid f_1(z) = \dots = f_r(z) = 0\}.$$

Dies entspricht gerade den abgeschlossenen Punkten z aus $\text{Spec}(\overline{R})$. Dies erlaubt es Punkte $z \in \text{Specm}(\overline{R})$ mit Lösungen des polynomialen Gleichungssystems

$$f_1(z) = f_2(z) = \dots = f_r(z) = 0 \quad , \quad z \in \mathbb{C}^n$$

zu identifizieren. Wir erhalten nunmehr folgende Verallgemeinerung des Fundamentalsatzes der Algebra.

Entweder gilt

$$1 = \sum_{i=1}^r g_i \cdot f_i$$

(für geeignete $g_i \in R$) oder mit anderen Worten $I = R$. Oder aber $\overline{R} \neq 0$ und $\exists z \in \text{Specm}(\overline{R}) \neq \emptyset$. In diesem Fall folgt also die Existenz einer Lösung $z \in \mathbb{C}^n$ des Gleichungssystems $f_1(z) = \dots = f_r(z) = 0$.

Folgerung: *Ein polynomiales Gleichungssystem $f_1(z) = \dots = f_r(z) = 0$ besitzt genau dann keine Lösung $z \in \mathbb{C}^n$ wenn es Polynome $g_1(z), \dots, g_r(z)$ gibt mit der Eigenschaft $\sum_i g_i(z) f_i(z) = 1$.*

Weiterhin: Für ein Polynom $f \in \mathbb{C}[t_1, \dots, t_n]$ sind die folgenden Aussagen äquivalent

- $f|V(I) = 0$
- $f_1(z) = \dots = f_r(z) = 0 \implies f(z) = 0$
- $\exists N \in \mathbb{N}, f^N \in I$, d.h. $f^N = \sum_{i=1}^r p_i(z) f_i(z)$.

Alle gemachten Aussagen gelten analog für einen beliebigen algebraisch abgeschlossenen Körper K anstelle von $K = \mathbb{C}$.

Noethersche Moduln und Ringe

16 Noethersche Ringe

Ein R -Modul M heißt noetherscher R -Modul, wenn sein R -Untermoduln alle endlich erzeugte R -Moduln sind.

Ein Ring R heißt noethersch, wenn R als R -Modul noethersch ist. Mit anderen Worten:

Definition: Ein Ring R heißt noethersch, wenn alle seine Ideale endlich erzeugte R -Moduln sind.

Beispiele: Körper und Hauptidealringe sind noethersche Ringe. Quotienten von noetherschen Ringen sind wieder noethersche Ringe. Quotienten- und Untermoduln eines noetherschen R -Moduls sind automatisch wieder noethersch. Es gilt auch folgende Umkehrung

Lemma 16.1. *Sei $(0 \rightarrow)N \rightarrow M \rightarrow N'(\rightarrow 0)$ eine exakte Sequenz von R -Moduln. Dann ist M noetherscher R -Modul, falls N, N' noethersche R -Moduln sind.*

Beweis: ObdA ist die linke Abbildung injektiv und die rechte surjektiv! Sind dann N', N noethersch und n'_1, \dots, n'_r sowie n_1, \dots, n_s R -Erzeugendensysteme von BN' resp. N . Dann ist $n_1, \dots, n_s, m_1, \dots, m_r$ ein R -Erzeugendensystem von M , falls $m_i \mapsto n'_i$. Das Argument überträgt sich sofort auf Untermoduln von M .

Korollar: *Für noethersches R sind endlich erzeugte R -Moduln noethersch. (Per Definition ist umgekehrt jeder noethersche Modul endlich erzeugt).*

Lemma 16.2. *Ist R ein noethersch, dann auch jede Lokalisierung $S^{-1}R$.*

Beweis: Ist I ein Ideal in $S^{-1}R$ und $f : R \rightarrow S^{-1}R$ die natürliche Abbildung, dann ist das R -Ideal $f^{-1}(I)$ endlich erzeugt. Aber für $r/s \in I$ folgt $r \in f^{-1}(I) = (r_1, \dots, r_n)$. Somit erzeugen r_1, \dots, r_n auch den $S^{-1}R$ -Modul I .

Lemma 16.3. *Ist R noethersch und normal (nullteilerfrei und ganz abgeschlossen in seinem Quotientenkörper K). Dann ist der ganze Abschluß S von R in einer endlichen separablen⁴ Körpererweiterung L von K wieder noethersch und normal.*

⁴Diese Annahme ist notwendig, wenn R nicht endlich erzeugt über einem Körper ist.

Beweis: Sei a ein (obdA über R ganzes) primitives Element von L/K . Ist $y = \sum_{i=0}^{[L:K]-1} x_i \cdot a^i$ ganz, dann auch seine Konjugierten. Sei D die Vandermonde Determinante der Konjugierten von a . Wegen Cramers Formel ist $D \cdot x_i \in S$ für alle $x_i \in K$. Wegen $D \in S$ und $D^2 \in R$ also $x_i \in D^{-2} \cdot R$. Somit ist S ein R -Untermodul des freien R -Moduls vom Rangs $[L : K]$, also noethersch.

Satz 16.4. *Ist R noethersch, dann auch der Polynomring $R[X]$.*

Beweis: Für ein Ideal I von $R[X]$ definieren die 'höchsten' Koeffizienten $a_0 = a_0(f)$ der $f = a_0 \cdot X^n + \dots + a_n \in I$ ein Ideal J von R

$$J = \{a_0(f) \mid f \in I\} .$$

Nach Annahme wird J von endlich vielen r_1, \dots, r_m als R -Modul erzeugt und es gibt Polynome $f_1, \dots, f_m \in I$ mit den führenden Koeffizienten r_1, \dots, r_m .

Es folgt: I wird von f_1, \dots, f_m und einem R -Erzeugendensystem des R -Moduls

$$M = I \cap (R + R \cdot X + \dots + R \cdot X^{N-1})$$

erzeugt, wobei $N = \max_i(\deg_X(f_i))$. Da M als R -Untermodul eines endlich erzeugten R -Moduls (mit N Erzeugenden) wieder endlich erzeugter R -Modul ist (letztes Korollar), ist daher I erst recht endlich erzeugt als $R[X]$ -Modul.

Per Induktion folgt

Korollar: Ist R noethersch, dann auch der Polynomring $R[X_1, \dots, X_n]$.

Bemerkung: Ein R -Modul M ist genau dann noethersch, wenn aufsteigende Ketten von R -Untermoduln

$$\dots \subset N_{i-1} \subset N_i \subset N_{i+1} \dots \subset M$$

stationär werden

$$N_i = N_{i+1} \text{ für } i \geq i_0 .$$

Begründung: Der R -Modul $N = \bigcup_i N_i$ ist im noetherschen Fall endlich erzeugt und alle Erzeugenden liegen daher in einem N_{i_0} .

Umgekehrt, gilt die Kettenbedingung, dann ist jeder R -Untermodul endlich erzeugt, da anderenfalls durch Hinzunahme immer neuer Erzeuger unendlich aufsteigende nicht stationäre Ketten entstehen würden.

17 Noethersche Räume

Ein topologischer Raum heißt noethersch, wenn jede absteigende Kette von abgeschlossenen Teilmengen stationär wird. Aus der Bemerkung des letzten Abschnitts folgt daher unmittelbar

Lemma: *Ist der Ring R noethersch, dann auch der topologische Raum $\text{Spec}(R)$.*

Ein topologischer Raum X heißt quasikompakt, wenn jede offene Überdeckung von X eine endliche Teilüberdeckung zulässt. Die duale dazu äquivalente Aussage ist: Ist ein Durchschnitt von abgeschlossenen Teilräumen leer, dann bereits ein endlicher Teildurchschnitt. Daraus folgt

Lemma: *Ein topologischer Raum X ist noethersch genau dann, wenn jede offene Teilmenge von X (mit der induzierten Topologie) quasikompakt ist.*

Beweis: Sei X noethersch und $U \subset X$ offen. Seien $A_\nu \subset U$ mit $\bigcap_\nu A_\nu = \emptyset$ abgeschlossene Teilmengen und $A = X \setminus U$. Da dann $A \cup A_\nu$ abgeschlossen in X ist [$U \setminus A_\nu = X \setminus (A \cup A_\nu)$ ist offen in U und offen in X , da U offen], folgt aus $\bigcap_\nu (A \cup A_\nu) = A$ bereits $\bigcap A_\nu = \emptyset$ für einen endlichen Teildurchschnitt, da man anderenfalls eine nicht stationäre zu A absteigende unendliche Kette von abgeschlossenen Teilmengen in X konstruieren könnte.

Ist umgekehrt jede offene Teilmenge $U \subset X$ quasikompakt, ist X noethersch. Sei $A_i \supseteq A_{i+1} \supseteq \dots$ eine absteigende Kette von abgeschlossenen Teilmengen in X mit Durchschnitt $A = \bigcap A_i$. Betrachte dann $U = X \setminus A$. Aus der Quasikompaktheit von U folgt, daß A bereits ein endlicher Teildurchschnitt der A_i ist. Die Kette der A_i wird daher stationär in X .

Abgeschlossene Teilmengen eines topologischen Raumes X heißen irreduzibel, falls sie nicht als Vereinigung von zwei abgeschlossenen echten Teilmengen geschrieben werden kann.

Lemma 17.1. *Sei X ein noetherscher topologischer Raum. Jede abgeschlossene Teilmenge Y von X kann als endliche Vereinigung von irreduziblen Mengen Y_ν geschrieben werden*

$$Y = Y_1 \cup \dots \cup Y_n .$$

Man kann obdA annehmen $Y_i \not\subseteq Y_j$ für $i \neq j$. In diesem Fall sind die irreduziblen Komponenten Y_ν eindeutig bestimmt.

ganze Erweiterung von Körper

Beweis: Die Eindeutigkeit folgt unmittelbar aus der Existenz.

Existenz (mittels noethersche Induktion): Sei E eine Eigenschaft der abgeschlossenen Mengen Y von X – etwa die oben relevante Eigenschaft ‘ Y ist Vereinigung endlich vieler irreduzibler Komponenten’ – und für E selbst sei folgendes vorausgesetzt:

- 1) E gelte für die leere Menge.
- 2) E gelte für Y , wenn E für alle echten abgeschlossenen Teilmengen von Y gilt.

Dann gilt (für noethersches X): E ist für alle abgeschlossenen $Y \subset X$ erfüllt.

Beweis: Anderenfalls gibt es eine nicht stationäre absteigende Kette von abgeschlossenen Mengen, für die E nicht gilt. Widerspruch!

18 Generische Punkte

Für $X = \text{Spec}(R) = \text{Spec}(R_{red})$, gilt:

- 1) Ist X irreduzibel und nicht leer, dann ist R_{red} nullteilerfrei:

$$f \cdot g = 0 \implies X = V(0) = V(f) \cup V(g) \implies V(f) = X \text{ oder } V(g) = X \text{ bzw. } f \in \text{Nil}(R_{red}) = 0 \text{ oder } g \in \text{Nil}(R_{red}) = 0.$$

- 2) Die Umkehrung:

Ist R nullteilerfrei, dann ist $X = \text{Spec}(R)$ irreduzibel und nicht leer: $X = V(I) \cup V(J) = V(I \cdot J)$ (I, J Ideale) $\implies I \cdot J \subset \text{Rad}(R) = \text{Nil}(R) = 0 \implies I = 0$ oder $J = 0$ bzw. $V(I) = X$ resp. $V(J) = X$.

- 3) Ist X irreduzibel, ist $\{0\}$ ein Primideal von R_{red} , das eindeutig bestimmte minimale Primideal des Ringes mit Zariski Abschluß $\overline{\{0\}} = X$.

Gibt es umgekehrt ein eindeutig bestimmtes minimales Primideal P . Dann gilt $\text{Rad}(R) = \bigcap_{P'} P' = P$. Somit ist das Radikal das minimale Primideal P und $R_{red} = R/P$ ist nullteilerfrei. Den zum Radikal gehörigen Punkt

$P \in X$ nennt man dann den generischen Punkt von X . Es ist der eindeutig bestimmte Punkt in X , dessen Abschluß ganz X ist.

Korollar: $X = \text{Spec}(R)$ ist irreduzibel und nicht leer genau dann, wenn X einen einzigsten generischen Punkt besitzt bzw. genau dann, wenn R_{red} nullteilerfrei ist.

Sei R ein noetherscher Ring und $X = \cup_{i=1}^n X_i$ die Zerlegung des Spektrums in seine irreduzible Komponenten. Die Komponenten $X_i = V(I_i)$ sind homöomorph zu $V(I_i) = \text{Spec}(R/I_i)$. Sie besitzen daher eindeutig bestimmte generische Punkte $P_i \in X_i$, deren Abschluß $\overline{\{P_i\}}$ gerade X_i ist. Die reduzierten Ringe $(R/P_i) = (R/I_i)_{\text{red}}$ sind nullteilerfrei. Sei

$$\text{GenSupp}(R) = \{P_1, \dots, P_n\}$$

die Menge der generischen Punkte, dann gilt

$$\text{Rad}(R) = \bigcap_{P \in \text{GenSupp}(R)} P.$$

19 Primzyklische Moduln

Allgemeine Begriffe: Sei M ein R -Modul. Die $r \in R$ mit $r \cdot M = 0$ definieren ein Ideal in R , den Annulator $\text{Ann}_R(M)$. Aus $N \subset M$ folgt $\text{Ann}_R(M) \subset \text{Ann}_R(N)$, da $rM = 0 \implies rN = 0$.

Beispiel: Für zyklische Moduln $M \cong R/I$ gilt

$$\text{Ann}_R(M) = \{r \in R \mid r \cdot [1] = [r] \in I\} = I.$$

M heißt primzyklisch, wenn I prim ist.

Lemma 19.1. Sei R/I zyklisch und R/P' primzyklisch. Dann gilt (a)

$$\text{Hom}_R(R/I, R/P') \neq 0 \iff I \subset P'.$$

(b) Ein injektiver Homomorphismus $\varphi \neq 0$ existiert genau dann wenn $I = P'$.

Beweis: Sei $\varphi : R/I \rightarrow R/P'$ R -linear. φ ist durch das Bild $[r]$ des Erzeugers $[1] \in R/I$ festgelegt. Aus $\varphi \neq 0$ folgt $r \notin P'$. Der Annulator von $[1] \in R/I$ ist I . Somit $I \subset \text{Ann}_R(\varphi([1])) = \text{Ann}_R([r])$. $[r] \neq 0$, wenn φ nicht null ist. Somit $\text{Ann}_R([r]) = P'$, da R/P' nullteilerfrei ist. Es folgt $I \subset P'$. Ist φ injektiv, dann gilt $\text{Ann}_R([1]_{R/I}) = \text{Ann}_R([r])$, also $I = P'$. Q.e.d.

Sei nun R ein noetherscher Ring und M ein endlich erzeugter R -Modul. Wir interessieren uns dann für

Zyklische Untermoduln: Ein zyklischer Untermodul $\langle m \rangle \subset M$ wird erzeugt von einem Element m . $\langle m \rangle$ ist ein Quotient von R . Somit gilt $\langle m \rangle \cong R/I$, für ein Ideal I . I ist der Annulator $I = \{r \in R \mid r \cdot m = 0\}$ des Elements m . I ist ungleich R , genau dann wenn gilt $m \neq 0$.

Im Inklusionsverband aller Annulatoren $I \neq R$ von Elementen m in M liegt jedes I in einem maximalen Elementannulator $\neq R$ (R ist noethersch!). Sei $I \neq R$ maximal in diesem Sinn. Dann ist I ein Primideal: Aus $r \cdot s \in I$ und $r \notin I$ (d.h. $m' = r \cdot m \neq 0$), $s \notin I$ folgt nämlich ein Widerspruch zur Maximalität von I :

$$\text{Ann}_R(m) \subsetneq \text{Ann}_R(m') \quad , \quad s \in \text{Ann}_R(m') \setminus \text{Ann}_R(m) .$$

Maximale Annulatoren $P \neq R$ von Elementen m aus M definieren daher nichttriviale primzyklische Untermoduln $R/P \cong \langle m \rangle \subset M$. Somit ist für $M \neq 0$ die folgende Menge nichtleer

$$\text{Ass}(M) = \{P \in \text{Spec}(R) \mid \exists R/P \hookrightarrow M\} .$$

Die Ideale $P \in \text{Ass}(M)$ nennt man die zu M assozierten Primideale. ein Primideal $P \in \text{Ass}(M)$ heißt isoliert, wenn $P \not\supseteq P'$ gilt für alle $P' \in \text{Ass}(M)$.

Folgerung 19.2. *Sei R noethersch und M ein noetherscher R -Modul. Dann existieren endliche aufsteigende Filtrationen*

$$M_0 = \{0\} \subsetneq \dots \subsetneq M_{i-1} \subsetneq M_i \subsetneq \dots \subsetneq M_n = M$$

gegeben durch R -Untermoduln M_i von M mit

$$M_i/M_{i-1} \cong R/P_i \quad (P_i \text{ prim}) .$$

ObdA kann angenommen werden, daß jeweils $P_i \in \text{Ass}(M/M_{i-1})$ isoliert sei.

Beweis: Wähle wie oben $R/P \hookrightarrow M$ nichttrivial und primzyklisch. Betrachte den Quotienten und iteriere das Verfahren bis es (wegen der Annahmen an R und M) abbricht. Q.e.d.

Sei $N \subset M$ ein R -Untermodul. Trivialerweise gilt $Ass(N) \subset Ass(M)$. Sei $P \in Ass(M) \setminus Ass(N)$. Dann erhält man eine injektive R -lineare Abbildung $\varphi: R/P \hookrightarrow M/N$ via

$$\begin{array}{ccccc} N & \hookrightarrow & M & \twoheadrightarrow & M/N \\ & & \uparrow & \nearrow \varphi & \\ & & R/P & & \end{array} .$$

Also $P \in Ass(M/N)$.

Begründung: [Für $0 \neq Kern(\varphi)$ existiert $P' \in Ass(Kern(\varphi))$. Also $R/P' \hookrightarrow Kern(\varphi) \hookrightarrow R/P$. Somit $P' = P$ (Lemma 19.1). Aber $R/P' \hookrightarrow Kern(\varphi) \hookrightarrow N$ im Widerspruch zu $P' = P \notin Ass(N)$.] Es folgt die erste Aussage von

Folgerung 19.3. *Seien R und M noethersch, und $N \subset M$ ein R -Untermodul. Dann gilt*

1. $Ass(N) \subset Ass(M) \subset Ass(N) \cup Ass(M/N)$
2. $Ass(R/P) = \{P\}$, für Primideale P .
3. $Ass(M)$ ist endlich und nichtleer für $M \neq 0$.

Beweis: 2. folgt aus Lemma 19.1(b). Aus 1., 2. und Folgerung 19.2 folgt 3.

$$Ass(M) \subset \bigcup_{i=0}^n Ass(R/P_i) = \bigcup_{i=0}^n \{P_i\} = \{P_1, \dots, P_n\} .$$

Ein $r \in R$ heißt Nullteiler von M , wenn $r \cdot m = 0$ gilt für ein $m \neq 0$ aus M .

Lemma 19.4. $\bigcup_{P \in Ass(M)} P$ ist die Menge der Nullteiler von M .

Beweis: \subset ist klar wegen $P \cdot \langle m \rangle = 0$ für $\langle m \rangle \cong R/P \hookrightarrow M$.

Sei andererseits r ein Nullteiler von M mit $r \cdot m = 0, m \neq 0$. Dann gilt $\langle m \rangle \cong R/I$, also $r \in I$. Für einen maximalen Elementannulator $P \neq R$, welcher I enthält, ist dann P prim, somit in $Ass(M)$, und es gilt $r \in I \subset P$.

Folgerung 19.5. *Besteht ein Ideal I eines noetherschen Rings R nur aus Nullteilern⁵, folgt $I \subset P$ für ein $P \in \text{Ass}(R)$. Ist R reduziert⁶, gilt $\text{Ass}(R) \subset \text{GenSupp}(R)$.*

Beweis: $r \notin P, \forall P \in \text{GenSupp}(R)$ und $r \cdot s = 0 \implies s \in P, \forall P \in \text{GenSupp}(R)$. Also $s \in \text{Nil}(R) = \{0\}$. Somit ist r kein Nullteiler und $\text{Ass}(R) \subset \text{GenSupp}(R)$.

20 Der Träger eines R -Moduls

Allgemeine Begriffe: Der Träger $\text{Supp}(M)$ eines R -Moduls M ist die abgeschlossene Teilmenge

$$\text{Supp}(M) = V(\text{Ann}_R(M))$$

von $X = \text{Spec}(R)$. Im zyklischen Fall $M = R/I$ ist $\text{Ann}_R(M) = I$, also

$$\text{Supp}(R/I) = V(I) .$$

Offensichtlich ist $\text{Supp}(M)$ für $M \neq \{0\}$ immer nicht leer. Weiterhin gilt $N \subset M \implies \text{Supp}(N) \subset \text{Supp}(M)$. Sei $N \subset M$ ein Untermodul. Sind I, I_1, I_2 die Annulatoren von $M, N, M/N$, dann gilt $I_1 \cdot I_2 \subset I$ sowie $I \subset I_1$ und $I \subset I_2$. Es folgt

$$\boxed{\text{Supp}(M) = \text{Supp}(N) \cup \text{Supp}(M/N)} .$$

Der noethersche Fall: Sei von nun an R und M noethersch. Sei

$$\text{GenSupp}(M) \subset X$$

die endliche Menge der generischen Punkte des Trägers $\text{Supp}(M)$. Deren Abschlüsse $V(P)$ liefern die irreduziblen Komponenten

$$\text{Supp}(M) = \bigcup_{P \in \text{GenSupp}(M)} V(P) .$$

⁵Lemma 6.3 und Lemma 19.4

⁶Nach Lemma 20.1 gilt dann sogar $\text{Ass}(R) = \text{GenSupp}(R)$.

Nach 19.2 besitzt M eine endliche Filtration mit primzyklische Subquotienten $M_i/M_{i-1} \cong R/P_i$ für alle i . Somit $Supp(M) = \bigcup_{i=0}^n Supp(R/P_i) = \bigcup_{i=0}^n V(P_i)$ sowie $Ass(M) \subset \bigcup_{i=0}^n Ass(R/P_i) = \bigcup_{i=0}^n \{P_i\}$ (Folgerung 19.3). Also

$$\boxed{Ass(M) \subset \{P_1, \dots, P_n\} \subset Supp(M)} .$$

Für $P \in Supp(M)$ ist $P \in V(P_i)$ (d.h. $P_i \subset P$) für mindestens ein i . Für minimale Primideale von $Supp(M)$, d.h. $P \in GenSupp(M)$, folgt daraus $P_i = P$

$$(*) \quad GenSupp(M) \subset \{P_1, \dots, P_n\} .$$

Lemma 20.1. (R, M noethersch) Die generischen Punkte⁷ von $Supp(M)$ liegen in $Ass(M)$

$$\boxed{GenSupp(M) \subset Ass(M)} .$$

Daraus folgt sogar, daß die minimalen Elemente innerhalb der Mengen $Ass(M)$ und $Supp(M)$ übereinstimmen. Dies charakterisiert die minimalen oder auch isoliert genannten Elemente von $Ass(M)$ als die generischen Punkte von $Supp(M)$. Im allgemeinen kann natürlich vorkommen $P \subsetneq P'$ für Elemente $P, P' \in Ass(M)$. Diese nicht isolierten Primideale P' von $Ass(M)$ nennt man 'eingebettet'.

Folgerung 20.2. (R, M noethersch). Sei P ein Primideal von R . Dann gilt

$$Ass(M) = \{P\} \implies Supp(M) = V(P) .$$

Somit gilt $P_i \supseteq P$ für die Subquotienten R/P_i einer primzyklischen Filtration von M .

Beweis: $Ass(M) = \{P\} \implies M \neq 0, GenSupp(M) \subset \{P\}$ nach Lemma 20.1. Also $GenSupp(M) = \{P\}$. Folglich $Supp(M) = V(P)$. Somit wegen $P_i \in Supp(M) = V(P)$ also $P \subset P_i$.

Beweis von Lemma 20.1: Für $P \in GenSupp(M)$ gilt obdA $P \notin Supp(M_{i-1})$ und $P = P_i$ für ein i im Sinne von Folgerung 19.2. Aus dem nächsten Lemma [für $M = M_i, N = M_{i-1}$ und $P = P_i$] folgt $P_i \in Ass(M_i) \subset Ass(M)$.

Lemma 20.3. ($R, N \subset M$ noethersch). Aus $Ass(M/N) \cap Supp(N) = \emptyset$ folgt

$$Ass(M) = Ass(N) \cup Ass(M/N) .$$

⁷Insbesondere gilt daher $Nil(R) = \bigcap_{P \in Ass(R)} P$.

Beweis: Die Inklusion \subset gilt nach Folgerung 19.3. Es bleibt $P \in \text{Ass}(M)$ zu zeigen für $P \in \text{Ass}(M/N)$. Ersetzt man M durch das Urbild eines $R/P \subset M/N$, kann obdA $M/N = R/P$ angenommen werden. Wähle ein Urbild $m \in M$ von $[1] \in R/P$

$$\begin{array}{ccccccc} 0 & \longrightarrow & N & \longrightarrow & M & \xrightarrow{\pi} & R/P \longrightarrow 0 \\ & & & & \uparrow & & \\ & & & & M' = J \cdot m & & \end{array}$$

$P \cdot m$ liegt in N und wird vom Annulator J von N annulliert. Es folgt

$$P \subset \text{Ann}_R(M')$$

für $M' = J \cdot m$ wegen $J \cdot (P \cdot m) = P \cdot (J \cdot m) = 0$. In dem Untermodul M' von M existiert ein m' mit $\pi(m') \neq 0$. Anderenfalls $J \subset P$ im Widerspruch zu $P \notin \text{Supp}(N)$. Der von m' aufgespannte zyklische Modul $\langle m' \rangle \cong R/I$ erfüllt als Untermodul von M' wegen $P \subset \text{Ann}_R(M') \subset I = \text{Ann}_R(m')$

$$P \subset I \quad , \quad R/I \hookrightarrow M \quad .$$

Andererseits gilt $\text{Hom}_R(R/I, R/P) \neq 0$ auf Grund der Wahl von m' . Aus Lemma 19.1 folgt $I \subset P$ und somit $I = P$. Dies impliziert $P \in \text{Ass}(M)$.

21 P -Koprimäre Moduln

Definition: Sei R ein noetherscher Ring und M ein noetherscher R -Modul. Gilt

$$\text{Ass}(M) = \{P\}$$

heißt M P -koprimär. Für einen koprimären Modul gilt nach Folgerung 20.2

$$\text{Supp}(M) = V(P) \quad .$$

Bemerkung: Primideale P sind Radikalideale. Aus $V(I) = V(P)$ für $I = \text{Ann}_R(M)$ folgt daher $\text{Rad}(I) = \text{Rad}(P) = P$. $P = (r_1, \dots, r_k)$ ist endlich erzeugt (R noethersch!). Für jeden Erzeuger r_i existiert ein m_i mit $(r_i)^{m_i} \in I$ (Radikalbedingung!). Also folgt $P^N \subset I \subset P$ für $N = \sum_{i=1}^k m_i$, denn $r = \sum_{i=1}^k \alpha_i \cdot r_i \in I \implies r^N = \sum_{i=1}^k \text{Binomialkoeffizient} \cdot (\alpha_1 \cdot r_1)^{e_1} \cdots (\alpha_k \cdot r_k)^{e_k}$. Für jeden Summanden gebe es mindestens ein i mit $e_i \geq m_i$. Also sind alle Summanden bereits einzeln in dem Ideal I . Es folgt $r^N \in I$. Man erhält

Lemma: Für einen P -koprimären Modul M sind folgende (für noethersches R zueinander äquivalente) Eigenschaften erfüllt

- $\text{Supp}(M) = V(P)$
- $P^N \subset \text{Ann}_R(M) \subset P$ für ein $N \in \mathbb{N}$
- $\text{Rad}(\text{Ann}_R(M)) = P$.

Folgerung 21.1. Für einen endlich erzeugten R -Modul $M \neq 0$ über einem noetherschen Ring R mit $P \in \text{Spec}(R)$ sind äquivalent:

1. $\text{Ass}(M) = \{P\}$, d.h. M ist P -koprimär
2. Für $r \in R$ ist die Multiplikationsabbildung

$$M \xrightarrow{r} M$$

injektiv für $r \notin P$ und nilpotent auf M für jedes $r \in P$ (eine Potenz von r induziert die Nullabbildung von M).

Beweis: 1. \implies 2.: Ist $\text{Kern}(r : M \rightarrow M) \neq 0$, dann ist r ein M -Nullteiler. Also $r \in \text{Ass}(M) = \{P\}$ (Lemma 19.4). Für $r \in P$ existiert N mit $r^N \in P^N \subset \text{Ann}_R(M)$ (für ein geeignetes N nach dem letzten Lemma). Daher ist $r^N = 0$ auf M , also r nilpotent auf M .

2. \implies 1.: Nilpotente Abbildungen sind nicht injektiv auf M wegen $M \neq 0$. Aus Annahme 2 folgt daher, daß P die Menge der M -Nullteiler ist. Also $\{P\} = \text{Ass}(M)$ nach Lemma 19.4.

Als Spezialfall von Folgerung 19.3 erhält man daher

Lemma 21.2. Sei N ein R -Untermodul von M . Sind N und M/N P -koprimär, dann auch M . Ist M P -koprimär, dann auch N .

Beispiel: Direkte Summen von P -koprimären Moduln sind somit P -koprimär. R/P ist P -koprimär. Achtung: Zwar ist R/P^n im allgemeinen⁸ nicht P -koprimär, aber es gilt $\text{GenSupp}(R/P^n) = \{P\}$.

⁸Für $R = \mathbb{Z} + (pt, t^2) \cdot \mathbb{Z}[t]$ in $\mathbb{Z}[t]$ ist $P = (pt, t^2) \cdot \mathbb{Z}[t]$ ein Primideal. Es gilt $R/P = \mathbb{Z}$ und $R/P^2 = \mathbb{Z} \oplus \mathbb{Z}pt \oplus (\mathbb{Z}/p^2) \cdot t^2 \oplus (\mathbb{Z}/p) \cdot t^3$. Also $I = \text{Ann}_R((\mathbb{Z}/p) \cdot t^3) = (p, pt, t^2)$ mit $R/I = \mathbb{F}_p$ und $I \in \text{Ass}(R/P^2) \setminus \text{Ass}(R/P)$.

22 Koprime Moduln

Definition: Ein noetherscher R -Modul M über einem noetherschen Ring R heißt koprime oder nullteilerarm, falls gilt: 1) $M \neq 0$. 2) Für $r \in R$ ist entweder $r : M \rightarrow M$ injektiv oder nilpotent auf M .

Ein noetherscher Ring R heißt koprime oder nullteilerarm, wenn er als R -Modul koprime ist.

Mit anderen Worten: Ein Ring R ist nullteilerarm (koprime), wenn gilt $R \neq 0$ und

$$r \cdot s = 0 \text{ und } r \neq 0, s \neq 0 \implies r \text{ nilpotent und } s \text{ nilpotent.}$$

Das heißt: Die nilpotenten Elemente sind die einzigen Nullteiler von R .

Beispiel: Sei R ein lokaler Ring mit maximalem Ideal m und I ein Ideal von R , das eine Potenz von m enthält. Dann ist automatisch R/I koprime. Beachte $Ass(R/I) \subset Supp(R/I) = V(I) = V(m) = \{m\}$ wegen $m = Rad(I)$. Ist dagegen P ein nicht maximales Primideal, dann ist im allgemeinen R/I nicht einmal koprime für die Primidealepotenzen $I = P^n$.

Ein koprimer Modul ist P -koprime für ein eindeutig bestimmtes Primideal $P \in Spec(R)$. Denn für koprimes M ist

$$P = \{r \in R \mid r \text{ nilpotent auf } M\}$$

ein Ideal (Summen komm. nilpotenter Abbildungen sind nilpotent, Vielfache ebenso) und P ist prim (da die Komposition injektiver Abbildungen injektiv ist, und da injektive Abbildungen wegen $M \neq 0$ nicht nilpotent sind).

23 Einbettbarkeit

Jeder noethersche R -Modul M über einem noetherschen Ring R läßt sich in eine endliche direkte Summe von koprimeren R -Moduln einbetten läßt (wir zeigen dies weiter unten)

$$\boxed{M \hookrightarrow \bigoplus_{j=1}^r M'_j \quad , \quad M'_j \text{ koprime}} .$$

Die M'_j sind obdA koprimär zu paarweise verschiedenen Primidealen P_j wegen Lemma 21.2. Aus Korollar 19.3 folgt weiterhin

$$\text{Ass}(M) \subset \{P_1, \dots, P_r\} .$$

Ist r minimal gewählt, gilt Gleichheit

$$\boxed{\text{Ass}(M) = \{P_1, \dots, P_r\}} .$$

Beweis: Wegen der Minimalität von r ist $\pi_j : M \rightarrow \bigoplus_{i \neq j} M'_i$ nicht mehr injektiv. Als Untermodul von M'_j ist $\text{Kern}(\pi_j) = M \cap M'_j$ aber P_j -koprimär (Lemma 21.2): $\text{Ass}(\text{Kern}(\pi_j)) = \text{Ass}(M'_j) = \{P_j\}$. Es folgt $P_j \in \text{Ass}(M)$ wegen $\text{Kern}(\pi_j) \subset M$.

Beweis der Einbettbarkeit: (mittels Induktion nach der Länge l einer ‘primzyklischen’ Filtration $(M_i)_{i=0, \dots, l}$ von M wie in Folgerung 19.2). Zur Erinnerung $R/P_i \hookrightarrow M/M_{i-1}$ für isoliertes $P_i \in \text{Ass}(M/M_{i-1})$. Also $P_1 \in \text{GenSupp}(M) \subset \text{Ass}(M)$ (nach Lemma 20.1). Für $P = P_1$ und alle $i = 1, \dots, l$ gilt daher

$$P_i \neq P \implies P \not\subseteq P_i .$$

Induktionsschritt: Sei $P = P_1$. Betrachte $M_1 \cong R/P \hookrightarrow M$ mit Quotient $\pi : M \rightarrow N = M/M_1$. Per Induktion gibt es dann bereits eine Einbettung $\varphi : N \hookrightarrow N' = \bigoplus_i N_i$ (mit P_i -koprimären Moduln N_i). Es verbleibt daher nur noch eine R -lineare Abbildung

$$\psi : M \rightarrow M' \quad , \quad (M' \text{ koprimär})$$

zu finden, welche auf $\text{Kern}(\varphi) = R/P$ injektiv ist. Dann ist $\psi \oplus (\varphi \circ \pi) : M \hookrightarrow M' \oplus N'$ eine Injektion von M in eine direkte Summe von koprimären Moduln.

Konstruktion von ψ : Für die Subquotienten R/P_i der Filtration von M gilt

$$P_i \neq P \implies P \not\subseteq P_i \implies \exists r_i \in P_i \setminus P .$$

Das Produkt r aller so definierten r_i erfüllt

$$r \in P_i \quad \text{für alle } P_i \neq P \quad \text{sowie } r \notin P .$$

Die in Schritt 1 gesuchte Abbildung ist dann $\psi(m) = r^l \cdot m$

$$\psi : M \rightarrow M' \quad , \quad M' = r^l \cdot M .$$

Offensichtlich ist ψ auf dem Untermodul R/P injektiv wegen $r \notin P$ (Nullteilerfreiheit von R/P) und M' ist koprimär (siehe nächster Hilfsatz). Q.e.d.

Hilfssatz: Das Bild $M' = r^l \cdot M$ der l -fach angewendeten Multiplikation mit r ist ein P -koprimärer Modul.

Beweis (durch absteigende Induktion nach der Länge l): Die Multiplikation $M \xrightarrow{r} M$ für $r \in R$ respektiert Filtrationen $M_0 \subset \dots \subset M_i \subset \dots \subset M_l = M$

$$\begin{array}{ccccc} M_{l-1} \hookrightarrow & M_l & \xrightarrow{\pi} & R/P_l & \\ \downarrow r & \downarrow r & & \downarrow r & \\ M_{l-1} \hookrightarrow & M_l & \xrightarrow{\pi} & R/P_l & \end{array}$$

Der Fall $P \neq P_l$: Dann ist die rechte vertikale Abbildung Null. Somit $r : M_l \rightarrow M_{l-1}$ und $r^l M \subset r^{l-1} M_{l-1}$. Per Induktionsannahme ist $r^{l-1} M_{l-1}$ P -koprimär, und damit auch $M' = r^l M$ (Lemma 21.2).

Der Fall $P = P_l$: Dann ist $r^l : R/P \rightarrow R/P$ injektiv. Somit $r(r^{l-1} \cdot M_{l-1}) \subset r^l \cdot M_l$ mit Quotient $r^l \cdot (R/P)$ isomorph zu R/P . Beachte: $\pi(r^l M_l) = r^l (R/P)$ mit $\text{Kern}(\pi) \cap (r^l M_l) = r^l M_{l-1}$, da r^l kein Nullteiler von R/P ist. Somit ist $M' = r^l \cdot M_l$ wegen Lemma 21.2 und der Induktionsannahme wieder P -koprimär.

24 Primärzerlegung

Sei R ein noetherscher Ring und M ein noetherscher R -Modul.

Einen R -Untermodul N von M nennt man (P) -primären Untermodul, wenn der Quotient M/N ein (P) -koprimärer R -Modul ist

N (P) -primär $\iff M/N$ (P) -koprimär, d.h. nullteilerarm (bzgl. P).

Ein Ideal I in R heißt Primärideal (zum Primideal P), wenn der Quotient R/I nullteilerarm (ein P -koprimärer R -Modul) ist

$$I \text{ primär} \iff R/I \text{ nullteilerarm.}$$

Insbesondere gilt dann $P^N \subset I \subset P$ für ein geeignetes $N \in \mathbb{N}$.

Bemerkung: Für Ideale gilt: maximal \implies prim \implies primär $\implies V(I)$ irreduzibel.

Die Aussagen des letzten Abschnitts lassen sich wie folgt umformulieren:

Sei $\bigoplus_j \varphi_j : M \hookrightarrow \bigoplus_{j=1}^r M'_j$ eine Einbettung in eine direkte Summe von P_j -koprimären R -Moduln M'_j . Sei $M_j \subset M$ der Kern von $\varphi_j : M \rightarrow M'_j$. Da M'_j P_j -koprimär ist, ist auch der Untermodul $\text{Bild}(\varphi_j) \cong M/M_j$ ein P_j -koprimärer R -Modul. Somit ist M_j primär und es gilt

$$\{0\} = \bigcap_{j=1}^r M_j .$$

Wendet man dies auf einen Quotientenmodul M/N an, erhält man

Satz 24.1. *Sei R ein noetherscher Ring und M ein noetherscher R -Modul und $N \subset M$ ein R -Untermodul. Dann gibt es eine (nicht eindeutige) Darstellung*

$$N = \bigcap_{j=1}^r M_j$$

als Durchschnitt von P_j -primären R -Untermoduln $M_j \subset M$. Ist r minimal gewählt gilt

$$\text{Ass}(M/N) = \{P_1, \dots, P_r\} .$$

Bemerkung: Für $M = 0$ ist $N = 0$ der leere Durchschnitt.

Korollar: *Jedes Ideal $I \neq R$ eines noetherschen Rings R ist ein endlicher Durchschnitt von Primärideal zu den Primidealen $P \in \text{Ass}(R/I)$.*

1.Beispiel: Sei $R = \mathbb{C}[X, Y]$. Dann sind $I = (X^2, XY) = (X) \cap (X, Y)^2 = (X) \cap (X^2, Y)$ verschiedene Primärzerlegungen von I , wobei $\text{Ass}(R/I) = \{(X), (X, Y)\}$.

2.Beispiel: Ist $I = P^n$, dann ist P das einzige Primideal in $\text{GenSupp}(R/I)$. Wegen $\text{GenSupp}(R/I) \subset \text{Ass}(R/I)$ kommt ein P -primäres Ideal in der Primärzerlegung von I vor. Dieses Primärideal nennt man die n -te symbolische Potenz $P^{(n)}$ von P . Es gilt

$$P^n \subset P^{(n)} \subset P .$$

Die symbolische Potenz $P^{(n)}$ ist eindeutig bestimmt und hängt nicht ab von der Wahl der Primärzerlegung wegen

Satz 24.2. *Ist $P \in \text{GenSupp}(M/N)$, dann ist die zugehörige P -primäre Komponente M_i einer Primärzerlegung $N = \bigcap_{j=1}^r M_j$ eindeutig bestimmt.*

Beweis: ObdA $N \neq 0$. Seien $P = P_i$ eines der isolierten Primideale der Primärzerlegung wie im letzten Satz 24.1. Dann ist $M_i = \text{Kern}(\varphi_i)$ der maximale R -Untermodul U von M mit Träger in $Y = \bigcup_{j \neq i} V(P_j)$ (M ist noethersch!). Also ist M_i intrinsisch definiert.

Begründung: Der Aufspann von Untermoduln mit Träger in Y hat wieder Träger in Y . Somit ist U eindeutig bestimmt. Quotienten haben wieder Träger in Y . Wegen $M_i \subset U$ gilt $\text{Supp}(U/M_i) \subset Y$. P ist im Träger Y nicht enthalten (Minimalität von P !). Wäre $M_i \neq U$, ist $U/M_i \neq 0$ als Untermodul von M_i' wieder P -koprimal (Lemma 21.2). Somit $P \in \text{Ass}(U/M_i) \subset \text{Supp}(U/M_i)$ im Widerspruch zu obiger Feststellung. Es folgt $U = M_i$. Q.e.d.

Analog gibt es einen kanonischen Untermodul $N \subset M$

$$0 \rightarrow N \rightarrow M \rightarrow Q \rightarrow 0$$

mit $\text{Ass}(Q) = \text{Ass}(M)_{\text{isoliert}}$ und $\text{Ass}(N) = \text{Ass}(M)_{\text{eingebettet}}$.

Alternativer Beweis (via Lokalisierung): Für endliche Durchschnitte gilt allgemein (Übungsaufgabe!)

$$S^{-1} \bigcap_j I_j = \bigcap_j S^{-1} I_j .$$

Für Primär ideale I und $g : R \rightarrow S^{-1}R$ gilt $g^{-1}(S^{-1}I) = I$ (siehe §5). Für das Primärideal $I = P^{(n)}$ gilt $P^n = P^{(n)} \cap \bigcap_j I_j'$. Für $S = R \setminus P$ ist $S^{-1}I_j' = S^{-1}R$ für alle Primärkomponenten $I_j' \neq P^{(n)}$ wegen der Minimalität von $P \in \text{Ass}(R/P^n)$. Dies charakterisiert $P^{(n)}$ eindeutig:

$$g^{-1}(S^{-1}P^n) = g^{-1}(S^{-1}P^{(n)} \cap \bigcap_j S^{-1}I_j') = g^{-1}(S^{-1}P^{(n)}) = P^{(n)} .$$

Übungsaufgaben: Zeige $S^{-1}P^n = (S^{-1}P)^n$ und $S^{-1}(I + J) = S^{-1}I + S^{-1}J$.

Dimensionstheorie

25 Höhe eines Primideals

Sei R ein kommutativer Ring mit 1. Für ein Primideal P in $X = \text{Spec}(R)$ definieren wir die Höhe $h = h(P)$ als das Maximum der Längen von echt absteigenden Kette von Primidealen P_i in R mit

$$P \supsetneq P_1 \supsetneq \dots \supsetneq P_h .$$

Der Fall $h = \infty$ ist möglich.

Krulldimension: Wir setzen $\dim(R) = -\infty$ für den Nullring. Ansonsten

$$\dim(R) = \max_{P \in X} \left(h(P) \right) .$$

Die Krulldimension hängt offensichtlich nur von dem topologischen Raum X ab. Insbesondere $\dim(R) = \dim(R_{red})$.

Beispiele: 1) Sei R noethersch. Ist die Dimension Null, ist jeder Punkt im Spektrum X abgeschlossen. Somit sind die endlich vielen generischen Punkte abgeschlossene Punkte. Der Abschluß X ist die Vereinigung der endlich vielen generischen abgeschlossenen Punkte. Aus Lemma 9.1 folgt dann: R_{red} ist eine endliche direkte Summe von Körpern $\iff \dim(R) = 0$.

2) $\dim(\mathbb{Z}) = \dim(K[X]) = 1$ für Körper K .

3) Wir zeigen später $\dim(R) = 2$ für $R = \mathbb{Z}_{(p)}[X]$. Eine echte maximale Kette von Primidealen der Länge zwei für R ist etwa $\{0\} \subsetneq (X - p) \subsetneq (X, p)$. Dagegen ist $\{0\} \subsetneq (1 - pX)$ eine maximale Kette von Primidealen des Rings, deren Länge aber nur eins ist! Dies folgt aus dem später bewiesenen Krullschen Hauptidealsatz, da $\mathbb{Z}_{(p)}[X]/(1 - pX) = \mathbb{Q}$.

Eine Ungleichung: Offensichtlich gilt $\dim(R) \geq \dim(R/P) + h(P)$ für alle $P \in X$

$$\begin{array}{c} R \\ \left| \dim(R/P) \right. \\ P \\ \left| h(P) \right. \\ 0 \end{array} .$$

Im noetherschen Fall kann somit die Dimensionsbestimmung immer auf den Fall eines nullteilerfreier Ring durch Betrachten der irreduziblen Komponenten zurückgeführt werden. D.h. für noethersches R und Ideale $I \neq R$ gilt

$$\dim(R/I) = \max_P \left(\dim(R/P) \right)$$

für $P \in \text{GenSupp}(R/I)$. Offensichtlich gilt

$$\dim(R) = \max_{P \in \text{Spec}(R)} \left(\dim(R_P) \right) .$$

ObdA könnte man sich dabei auch auf die maximalen Ideale P beschränken (siehe Lemma 11.1 von §11).

Lemma 25.1. *Sei R noethersch und $0 \neq a \in R$ kein Nullteiler von R . Dann gilt*

$$\dim(R) \geq \dim(R/a) + 1 .$$

Beweis: ObdA $R/a \neq 0$. Wähle $\bar{P} \in \text{GenSupp}(R/a)$ mit Urbild P in R so, daß $\dim(R/a) = \dim(R/P)$. P kann nicht minimal in R sein. Wäre P minimal in R , wäre $a \in P$ wegen $P \in \text{GenSupp}(R) \subset \text{Ass}(R)$ (Lemma 20.1) ein Nullteiler in R (Lemma 19.4). Widerspruch! Also $h(P) \geq 1$. Daraus folgt $\dim(R) \geq \dim(R/P) + 1 = \dim(R/a) + 1$. Q.e.d.

26 Going Up

In diesem Paragraphen sei $R \hookrightarrow R'$ eine injektive, endliche Ringerweiterung. Es seien $X' = \text{Spec}(R')$ und $X = \text{Spec}(R)$ die zugehörigen Spektren und π die zugehörige Abbildung

$$\pi : X' \rightarrow X .$$

Dann gelten die folgenden Lemmata 26.1–26.4 (zum Beweis wird obdA $R \neq 0$ und damit $R' \neq 0$ angenommen).

Lemma 26.1. *Aus $P_2 \subset P_1$ und $P_1, P_2 \in X'$ sowie $\pi(P_1) = \pi(P_2)$ folgt $P_1 = P_2$.*

Beweis: Durch Division nach P_2 gilt obdA $P_2 = 0$ und $p = \pi(P_2) = R \cap P_2 = 0$. Somit sind R, R' nullteilerfrei. Für $0 \neq x \in P_1$ sei $x^n + a_1 x^{n-1} + \dots + a_n = 0$ eine Ganzheitsgleichung über R von minimalem Grad. Dann ist $a_n \neq 0$ (R' ist nullteilerfrei!). Andererseits ist $a_n \in P_1 \cap R = \pi(P_1) = p = 0$. Widerspruch! Es folgt $P_1 = 0$, also $P_1 = P_2$. Q.e.d.

Lemma 26.2. *π bildet maximale Ideale auf maximale Ideale ab*

$$\pi : |X'| \rightarrow |X| .$$

Beweis: : Lemma 3.1.

Lemma 26.3. $\pi : X' \rightarrow X$ ist surjektiv.

Beweis: Sei $p \in X$ und $S = R \setminus p$. Dann ist $S^{-1}R \rightarrow S^{-1}R'$ wieder injektiv(!) und endlich. Für $X_S = \text{Spec}(S^{-1}R)$ und $X'_S = \text{Spec}(S^{-1}R')$ gilt (siehe §5)

$$\begin{array}{ccccc} \emptyset \neq & |X'_S| \hookrightarrow & X'_S \hookrightarrow & X' & \\ & \downarrow \pi & \downarrow \pi & \downarrow \pi & \\ \{p\} & \longleftarrow |X_S| \hookrightarrow & X_S \hookrightarrow & X & \end{array}$$

Wegen $p \in \text{Bild}(X_S)$ kann man daher obdA durch Lokalisieren p als maximal und R als lokalen Ring annehmen. Es genügt dann, daß $\text{Specm}(R')$ (nicht leer!) auf $\text{Specm}(R)$ abgebildet wird (Lemma 26.2)!

Korollar 26.4. $\dim(R) = \dim(R')$.

Beweis: Wegen Lemma 26.1 ist $\dim(R) \geq \dim(R')$. Eine maximale Primidealkette von R kann andererseits geliftet werden. Es genügt zu zeigen daß für $p_i \not\subseteq p_{i+1}$ und $\pi(P_i) = p_i$ ein $P_{i+1} \supseteq P_i$ gefunden werden kann mit $\pi(P_{i+1}) = p_{i+1}$. ObdA $p_i = 0$ und $P_i = 0$ wie in Lemma 26.1. Dann folgt die Existenz von P_{i+1} sofort aus Lemma 26.3. Somit $\dim(R) = \dim(R')$.

Lemma 26.5. $\pi(P)$ ist maximal $\iff P$ maximal ist.

Beweis: \Leftarrow nach Lemma 26.2. Nach Lemma 26.3 existiert für $p \in |X| \subset X$ ein Urbild $P_2 \in X'$. Für maximales $P_1 \supset P_2$ gilt dann notwendiger Weise auch $\pi(P_2) = p$. Nach Lemma 26.1 ist dann $P_1 = P_2$ maximal.

27 Polynomringe

Ist K ein Körper und $R_n = K[X_1, \dots, X_n]$ der Polynomring. Dann ist $P_0 = 0$ das eindeutige minimale Primideal. Sei $P_d \supsetneq P_{d-1} \supsetneq \dots \supsetneq P_1 \supsetneq P_0$ irgend eine echte Kette von Primidealen in R_n , welche sich nicht weiter verfeinern läßt. Wähle $0 \neq f \in P_1$. Dann bilden die Quotienten \overline{P}_i (ab $i = 1$) eine nicht verfeinerbare echte Kette von Primidealen im Quotientenring $\overline{R} = R/f$ und umgekehrt. Es folgt

$$\dim(R_n) = \dim(\overline{R}) + 1 .$$

\overline{R} ist andererseits eine endliche Ringerweiterung eines Polynomrings $R_{n-1} \hookrightarrow \overline{R}$ (Noetherscher Normalisierungssatz). Somit folgt

$$\dim(\overline{R}) = \dim(R_{n-1}) ,$$

und durch Induktion nach n

Satz 27.1. $\boxed{\dim(K[X_1, \dots, X_n]) = n}$.

Allgemeiner folgt daraus

Satz 27.2. Für noethersche⁹ Ringe R gilt $\dim(R[X_1, \dots, X_n]) = \dim(R) + n$.

Der Fall $R = R_m$ ist klar. Den Fall einer endlich erzeugten K -Algebra R kann man durch Noether-Normalisierung und going up sofort auf den Fall $R = R_m$ zurückführen.

Beweisskizze: Den allgemeinen Fall reduziert man sofort auf die Situation R nullteilerfrei und $n = 1$. Dann folgt $\dim(R[X]) \geq \dim(R) + 1$, weil (X) ein Primideal mit Restklassenring R ist und $\{0\}$ ein Primideal mit Restklassenring $R[X]$ ist.

Für die nichttriviale Ungleichung

$$\dim(R[X]) \leq \dim(R) + 1$$

genügt es die Dimension einer Lokalisierung von $R' = R[X]$ nach einem beliebigen gewählten maximalen Ideal I' von R' zu betrachten. Sei I das Primideal $I = I' \cap R$ von R . Wir können daher zuerst R nach I lokalisieren wegen $R \setminus I \subset R[X] \setminus I'$. Ersetzt man R durch diese Lokalisierung, erlaubt es dies obdA R als lokal anzunehmen mit maximalem Ideal $I = I' \cap R$ und Restklassenkörper K . Wir betrachten nun wieder den Polynomring $R' = R[X]$ über dem lokalen Ring R (nicht seine Lokalisierung nach I'). Das abschließende Argument benutzt eine Technik des nächsten Kapitels, welche es erlaubt den noetherschen Ring R durch eine endlich erzeugte K -Algebra über einem Körper K zu ersetzen (und diesen Fall haben wir bereits bewiesen):

Der Ring $Gr_I(\mathbf{R}) = \bigoplus_n I^n / I^{n+1}$ ist eine endlich erzeugte K -Algebra. Er hat dieselbe Dimension wie R . (Siehe nächstes Kapitel, Korollar 31.1). Analog gilt, daß $R[X]$ dieselbe Dimension hat wie $Gr_{I'}(\mathbf{R}')$ (nach Lemma 29.1 ist es egal ob man R' zuerst nach I' lokalisiert oder nicht; wir lokalisieren daher nicht).

⁹Für nicht noethersches R ist dies im allgemeinen falsch.

Das maximale Ideal I' ist der Kern eines surjektiven Homomorphismus $\varphi : R' \rightarrow L$ auf einen Körper L . Hierbei wird R auf den Teilkörper $R/R \cap I' = R/I = K$ abgebildet. L ist algebraisch über K und von der Restklasse $[X]$ von X erzeugt (Korollar 3.3).

$$\begin{array}{ccccc} R[X] & \longrightarrow & K[X] & \xrightarrow{\pi} & L \\ \uparrow & & \uparrow & \nearrow & \\ R & \longrightarrow & K & & \end{array}$$

Der Kern von π wird vom K -Minimalpolynom von $[X] \in L$ erzeugt. Also ist der Kern I' von φ gleich

$$I' = (I, Y)$$

für ein Polynom $Y = X^n + a_1X^{-1} + \dots + a_n \in R[X]$, welches das Minimalpolynom liftet. Es folgt die Existenz eines surjektiven graduierten Homomorphismus

$$Gr_I(\mathbf{R})[Y] \twoheadrightarrow Gr_{I'}(\mathbf{R}') .$$

Wir erhalten $\dim(Gr_{I'}(\mathbf{R}')) \leq \dim(Gr_I(\mathbf{R})[Y]) = \dim(Gr_I(\mathbf{R})) + 1$. Also

$$\dim(R[X]) = \dim(Gr_{I'}(\mathbf{R}')) \leq \dim(Gr_I(\mathbf{R})) + 1 = \dim(R) + 1 .$$

Q.e.d.

Graduierte Ringe

28 Filtrationen

Eine Filtration auf einem R ist eine absteigende Kette von Idealen $R = I_0 \supseteq I_1 \supseteq I_2 \supseteq \dots$ mit der Eigenschaft $I_i \cdot I_j \subset I_{i+j}$ für alle $i, j \in \mathbb{N}$. Wir fixieren nun eine solche Filtration und erhalten ein filtrierten Ring \mathbf{R} .

Sei M ein R -Modul. Eine absteigende Kette $M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \dots$ von R -Modul definiert einen filtrierten Modul \mathbf{M} , falls gilt $I_i \cdot M_j \subset M_{i+j}$. Die filtrierten R -Moduln bilden eine Kategorie, deren Morphismen die R -linearen Abbildungen $f : \mathbf{M} \rightarrow \mathbf{N}$ sind mit der Eigenschaft $f(M_i) \subset N_i$ für alle i .

I -adische Filtration: Sei $I \subset R$ ein Ideal. $I_n = I^n$ definiert die I -adische Filtration \mathbf{R}^{I-ad} auf R . Ditto definiert $M_n = I^n \cdot M$ die I -adische Filtration \mathbf{M}^{I-ad} auf M .

Induzierte Filtrationen: Ist ein \mathbf{M} ein filtrierter R -Modul und

$$0 \rightarrow N \rightarrow M \rightarrow Q \rightarrow 0$$

eine kurze exakte Sequenz von R -Moduln. Dann definiert $N_n = M_n \cap N$ resp. $Bild(M_n)$ induzierte Filtrationen $\mathbf{N} = \mathbf{N}^{ind}$ und $\mathbf{Q} = \mathbf{Q}^{ind}$ auf N resp. Q . Ist die Filtration \mathbf{M} auf M I -adisch, dann auch die Filtration \mathbf{Q} auf Q ; im allgemeinen ist aber \mathbf{N} nicht I -adisch auf N , d.h. $\mathbf{N}^{ind} \neq \mathbf{N}^{I-ad}$.

Man definiert nun einen graduerten Erweiterungsring $R \rightarrow R^\bullet$

$$R^\bullet = R \oplus I_1 \oplus I_2 \oplus \dots$$

mit der graduerten Multiplikationsregel $I_i \cdot I_j \subset I_{i+j}$. Äquivalente Definition: $R^\bullet = R \oplus t \cdot I_1 \oplus t^2 \cdot I_2 \oplus \dots$ als Untertring des Polynomrings $R[t]$. Ein filtrierter R -Modul \mathbf{M} definiert den R^\bullet -Modul

$$M^\bullet = M_0 \oplus M_1 \oplus M_2 \oplus \dots$$

Alternativ: M^\bullet als Untermodul des $R[t]$ -Moduls $M[t] = \bigoplus_{i=0}^{\infty} t^i \cdot M_i$.

Der noethersche Fall: Ist R noethersch, und die Filtration auf R I -adisch, dann ist R^\bullet wieder ein noetherscher Ring (nämlich ein Quotient des Polynomrings $R[X_1, \dots, X_s]$ unter der Abbildung $X_i \mapsto t \cdot r_i$, wobei r_1, \dots, r_s Erzeugende des R -Moduls I sind).

Lemma 28.1. *Sei R noethersch und die Filtration \mathbf{R} I -adisch. Sei \mathbf{M} ein zugehöriger filtrierter, endlich erzeugter R -Modul (nicht notwendig selbst I -adisch). Dann sind äquivalent*

- 1) $M_{n+1} = I \cdot M_n$ für $n \geq n_0$.
 2) Der R^\bullet -Modul M^\bullet ist endlich erzeugt als R^\bullet -Modul.

Beweis: 1) \implies 2) ist klar, da dann $M^\bullet = R^\bullet \cdot M^{\leq n_0}$ gilt für den endlich erzeugten R -Untermodul

$$M^{\leq n_0} = \bigoplus_{i=0}^{n_0} t^i \cdot M_i .$$

Umgekehrt folgt aus 2., daß in M^\bullet jede aufsteigende Kette von R^\bullet -Moduln ab einem $n = n_0$ stationär wird. Angewandt auf die aufsteigende Kette $\subset R^\bullet \cdot M^{\leq n} \subset R^\bullet \cdot M^{\leq n+1} \subset \dots$ von R^\bullet -Untermoduln von M^\bullet

$$R^\bullet \cdot M^{\leq n} = M^{\leq n} \oplus t^{n+1}(I \cdot M_n) \oplus t^{n+2}(I^2 M_n) \oplus \dots$$

erhält man 1). Q.e.d.

Einen filtrierten R -Modul \mathbf{M} mit den beiden äquivalenten Eigenschaften des letzten Lemmas nennt man stabil. Da Untermoduln von noetherschen Moduln wieder noethersch sind, folgt aus dem letzten Lemma sofort die erste Aussage von

Lemma 28.2. (Artin-Rees) *Seien die Voraussetzungen wie im letzten Lemma, \mathbf{M} stabil filtriert und $N \subset M$ ein R -Untermodul. Dann ist die auf N induzierte Filtration \mathbf{N} stabil, d.h.*

$$\boxed{N \cap M_{n+k} = I^n \cdot (N \cap M_k) \quad , \quad k \geq k_0, \forall n} .$$

Zusatz: Für die I -adische Filtration $M_n = I^n \cdot M$ auf M folgt

$$\boxed{I^{n+k} \cdot N \subseteq N \cap (I^{n+k} \cdot M) \subseteq I^n \cdot N}$$

für alle n und ein geeignetes k .

Beweis: (Zusatz) Trivial ist die linke Inklusion, denn $I^{n+k} \cdot N \subset I^{n+k} \cdot M$ ist eine Teilmenge von N . Die rechte Inklusion folgt aus Artin-Rees $N \cap M_{n+k_0} = I^n \cdot (N \cap M_{k_0}) \subset I^n \cdot N$ für alle $n \geq 0$. Q.e.d.

29 Graduierte Moduln

Sei \mathbf{R} ein noetherscher Ring versehen mit der I -adischen Filtration. Im letzten Abschnitt haben wir einen Funktor konstruiert von der Kategorie der stabil filtrierten endlich erzeugten R -Moduln in die Kategorie der endlich erzeugten R^\bullet -Moduln

$$\mathbf{M} \mapsto M^\bullet .$$

Wegen $R \subset R^\bullet$ ist R^\bullet ein R -Modul. Sei $I \cdot R^\bullet$ das von I erzeugte R^\bullet -Ideal. Dann ist

$$Gr_I(\mathbf{R}) = R^\bullet / I \cdot R^\bullet$$

als Quotientenring des noetherschen Rings R^\bullet wieder noethersch. Beachte,

$$Gr_I(\mathbf{R}) = (R/I) \oplus (I/I^2) \oplus (I^2/I^3) \oplus \dots$$

ist ein R/I -Modul.

Ist M^\bullet als R^\bullet -Modul endlich erzeugt, dann ist

$$M^\bullet / I \cdot R^\bullet M^\bullet = (M_0 / IM_0) \oplus (M_1 / IM_1) \oplus \dots$$

ein endlich erzeugter $Gr_I(\mathbf{R})$ -Modul. Ebenso der $Gr_I(R)$ -Modul

$$Gr_I(\mathbf{M}) = \bigoplus_n M_n / M_{n+1} ,$$

da \mathbf{M} nach Annahme eine stabile Filtration ist, gilt $M_n / M_{n+1} = M_n / I \cdot M_n$ für fast alle n . Somit stimmen beide Quotienten nach Artin-Rees für fast alle n überein (Lemma 28.1) und $Gr_I(\mathbf{M})$ ist ein Quotient von $M^\bullet / I \cdot R^\bullet M^\bullet$.

Lemma 29.1. Für maximale Ideale $I \in \text{Specm}(R)$ sei $R \rightarrow S^{-1}R$ die Lokalisierung nach I . Dann gilt

$$\boxed{Gr_I(\mathbf{R}) \cong Gr_{S^{-1}I}(\mathbf{S}^{-1}\mathbf{R})} .$$

Beweis: $(S^{-1}I)^n = S^{-1}I^n$ und $S^{-1}I^n = I^n + S^{-1}I^{n+1}$ (Exaktheit der Lokalisierung). I^{n+1} ist I -koprämär, da I ein maximales Ideal ist. Es folgt $(S^{-1}I^{n+1}) \cap R = I^{n+1}$ nach §5. Somit $(S^{-1}I)^n / (S^{-1}I)^{n+1} = I^n / (I^n \cap S^{-1}I^{n+1}) = I^n / I^{n+1}$.

30 Hilbert–Dimension

Sei R noethersch (nicht notwendig lokal) mit maximalem Ideal I . Dann ist $K = R/I$ ein Körper. Somit ist $Gr_I(\mathbf{R})$ eine K -Algebra.

$Gr_I(\mathbf{R})$ ist endlich erzeugt über K : Sind x_1, \dots, x_r Erzeugende des Ideals I , dann ist R^\bullet ein Quotient von $R[X_1, \dots, X_r]$. Somit ist $Gr_I(\mathbf{R})$ ein Quotient von $K[X_1, \dots, X_r]$.

Weiterhin: Wegen des noetherschen Normalisierungssatzes kann man die Erzeugenden x_1, \dots, x_r von I so wählen, daß die ersten s Variablen X_1, X_2, \dots, X_s einen K -Polynomring in $Gr_I(\mathbf{R})$ aufspannen, über dem $Gr_I(\mathbf{R})$ eine endliche injektive Ringerweiterung von graduierten Ringen ist

$$\boxed{K[X_1, \dots, X_s] \hookrightarrow Gr_I(\mathbf{R}) \quad \text{endlich}} .$$

Insbesondere hat man nach Going Up Dimensionsgleichheit.

Definition-Folgerung: Für R noethersch lokal mit I maximal und der I -adischen Filtration \mathbf{R} ist $s = s(R)$ die Dimension von $Gr_I(\mathbf{R})$, und $s(R)$ nennt man die Hilbert-Dimension des lokalen noetherschen Rings R .

Da die K -Dimension des Raums P_s^n der Polynome in X_1, \dots, X_s vom Grad $\leq n$ gleich $\binom{n+s}{s}$ ist [wegen $P_s^n/X_1 \cdot P_s^{n-1} \cong P_{s-1}^n$ sowie $\binom{n+(s-1)}{(s-1)} + \binom{(n-1)+s}{s} = \binom{n+s}{s}$], ist $\binom{n+s-1}{s-1}$ die Dimension der Polynome vom genauen Grad n .

Korollar 30.1. Im Fall $s \geq 1$ gilt für alle $n \in \mathbb{N}$

$$\boxed{\frac{1}{(s-1)!} \cdot n^{s-1} \leq \dim_K(I^n/I^{n+1}) \leq C \cdot n^{s-1}}$$

bezüglich einer geeigneten Konstante C .

Bemerkung: Sei $G = \bigoplus_{n=n_0}^{\infty} G^n$ ein endlich erzeugter graduierter Modul über dem Polynomring $K[X_1, \dots, X_s]$. Nach Hilbert gibt es dann ein Polynom $P_G(t)$ vom Grad $\leq s-1$, so daß gilt

$$\dim_K(G^n) = P_G(n) \quad , \quad \forall n \geq n_0 .$$

Dies beweist man durch Induktion nach s : Betrachte die Multiplikation $X_s : G^\bullet \rightarrow G^{\bullet+1}$. Kern und Kokern sind endliche graduierte Moduln über $K[X_1, \dots, X_{s-1}]$ und man erhält $P_G(n+1) - P_G(n) = P_{\text{Koker}}(n+1) - P_{\text{Ker}}(n)$. Die rechte Seite $p(n)$ ist nach Induktionsannahme polynomial vom Grad

$\leq s - 2$ (für $n \gg 0$). Benutze nun, daß für jedes Polynom $p(n)$ auch $P(n) = \sum_{i=0}^{n-1} p(i)$ ein Polynom ist.

Daraus folgt: Sei R ein noetherscher lokaler Ring mit maximalem Ideal I und Restklassenkörper $K = R/I$. Sei M ein noetherscher R -Modul versehen mit einer stabilen Filtration $\mathbf{M} = (M_n)_{n \in \mathbb{N}}$. Dann sind die Subquotienten M_i/M_{i+1} endlich dimensionale K -Vektorräume. Setze $l(M/M_n) = \sum_{i=0}^{n-1} \dim_K(M_i/M_{i+1})$. Dann gibt es eindeutig bestimmte Polynome $Q_{\mathbf{M}}(t)$, $P_{\mathbf{M}}(t)$ mit

$$l(M/M_n) = Q_{\mathbf{M}}(n) \quad , \quad \dim_K(M_n/M_n) = P_{\mathbf{M}}(n)$$

für alle $n \geq n_0(\mathbf{M})$. Offensichtlich gilt $Q_{\mathbf{M}}(t+1) - Q_{\mathbf{M}}(t) = P_{\mathbf{M}}(t)$. Aus 30.1 folgt daher

Folgerung: Die Hilbert-Dimension eines lokalen noetherschen Rings R ist gleich dem Grad des Polynoms $Q_{\mathbf{R}}(t)$

$$\boxed{s(R) = \deg(Q_{\mathbf{R}}(t))} .$$

Additivität

Ist $N \subset M$ ein R -Untermodul von M und versieht man N und M/N mit den von \mathbf{M} induzierten Filtrationen, so erhält man aus der Kern-Kokern Sequenz die folgenden exakten Sequenzen

$$0 \longrightarrow N_i/N_{i+1} \longrightarrow M_i/M_{i+1} \longrightarrow (M/N)_i/(M/N)_{i+1} \longrightarrow 0$$

Daraus folgt $P_{\mathbf{N}}(t) + P_{\mathbf{M}/\mathbf{N}}(t) = P_{\mathbf{M}}(t)$ und durch Aufaddieren dieser Beträge zu den Längen folgt die Längenadditivität $l(N/M_n \cap N) + l(M/(N + M_n)) = l(M/M_n)$. Also

$$Q_{\mathbf{N}}(t) + Q_{\mathbf{M}/\mathbf{N}}(t) = Q_{\mathbf{M}}(t) .$$

Lemma 30.2. Die Länge $l(M/M_n)$ hängt nur von $M_n \subset M$ und nicht von der Filtration ab. Aus $M_n \subset M'_n$ folgt $l(M/M_n) \geq l(M/M'_n)$.

Beweis: Sei \mathbf{M} fixiert und $M'_r \subset \dots \subset M'_1 \subset M'_0 = M$ eine zweite Filtration. Die Filtration \mathbf{M} induziert Filtration auf den Untermoduln M'_i und den Subquotienten. Wir nehmen an $M_n \subset M'_r$. Bezüglich dieser induzierten Filtrationen folgt aus der Additivität der Längen

$$l_{\mathbf{M}}(M/M_n) = \sum_{i=0}^{r-1} l_{\mathbf{M}}(M'_i/M'_{i+1}) + l_{\mathbf{M}}(M'_r/M_n) .$$

Der Index $l_{\mathbf{M}}$ soll daran erinnern, daß es sich um von \mathbf{M} induzierte Längen handelt. Der letzte Term $l_{\mathbf{M}}(M'_r/M_n)$ ist ≥ 0 . Es genügt daher für den Beweis zu zeigen $l_{\mathbf{M}}(M'_i/M'_{i+1}) = \dim_K(M'_i/M'_{i+1})$. Somit ist die Aussage des Lemmas auf den Fall von R -Moduln reduziert, auf denen I trivial operiert. R -Untermoduln sind dann aber nichts anderes als K -Untervektorräume. Die von M induzierte Filtration ist ein Filtration durch K -Untervektorräume und die Aussage folgt aus der Dimensionsformel für Kern und Bild.

31 Dimensionsvergleich

Sei R ein lokaler noetherscher Ringe mit maximalem Ideal I und I -adischer Filtration \mathbf{R} . Wir vergleichen die Hilbert-Dimension mit der Krull-Dimension und zeigen Gleichheit.

Korollar 31.1. *Für noethersche lokale Ringe mit maximalem Ideal I gilt*

$$\boxed{\dim(R) = \dim(\text{Gr}_I(\mathbf{R})) = s(R)} .$$

Beweis: Induktion nach $s = \dim(\text{Gr}_I(\mathbf{R}))$. Sei $\dim(\text{Gr}_I(\mathbf{R})) = 0$ (Induktionsanfang). Also $I^n/I^{n+1} = 0$ für fast alle n , d.h. $I \cdot I^n = I^n$. Daher $I^n = 0$ für $n \gg 0$ (Nakayama Lemma). Also $I = \text{Nil}(R)$. Daher ist $R_{\text{red}} = R/I = K$ ein Körper. Es folgt $\dim(R) = \dim(R_{\text{red}}) = \dim(K) = 0$. Die Umkehrung gilt auch.

Also können wir daher annehmen $\dim(R) \geq 1$. Zum Beweis von $\dim(R) = \dim(\text{Gr}_I(\mathbf{R}))$ können wir R durch R_{red} ersetzen. Dies ändert weder die Dimension noch die Hilbert-Dimension, da $G_{I_{\text{red}}}(\mathbf{R}_{\text{red}})$ ein Quotient von $G_I(\mathbf{R})$ mit nilpotentem Kern ist. Dadurch ist nun R obdA reduziert und $I \neq 0$.

Wähle $P \in \text{GenSupp}(R)$ mit $\dim(R) = \dim(R/P)$ und ein $P' \subsetneq P$ mit $\dim(R) - 1 = \dim(R/P')$. Das Ideal P' enthält nach Folgerung 19.5 einen Nichtnullteiler x des Rings R . Setze $\bar{R} = R/x \cdot R$. Die induzierte Filtration $\bar{\mathbf{R}}$ ist die \bar{I} -adische für das maximale Ideal $\bar{I} = \text{Bild}(I)$ von \bar{R} .

Wegen $(x) \subset P'$ gilt $\dim(\bar{R}) \geq \dim(R/P') = \dim(R/P) - 1 = \dim(R) - 1$. Wegen Lemma 25.1 gilt $\dim(R) - 1 \geq \dim(\bar{R})$, da x kein Nullteiler in R ist. Also

$$\dim(\bar{R}) = \dim(R) - 1 .$$

Aus dem nächsten Lemma 31.2 folgt $\dim(G_{\bar{I}}(\bar{\mathbf{R}})) = \dim(G_I(\mathbf{R})) - 1$. Wegen der Induktionsannahme gilt daher $\dim(R) = \dim(\text{Gr}_I(\mathbf{R}))$. Q.e.d.

Lemma 31.2. *Sei R lokaler noetherscher Ring und $x \in I$, I maximal. Dann gilt für die Hilbert-Dimensionen s resp. \bar{s} von R resp. $\bar{R} = R/xR$ die Ungleichung $s - 1 \leq \bar{s}$. Ist $x \in I$ kein Nullteiler in R gilt $\bar{s} = s - 1$.*

Beweis 1. $0 \rightarrow (xR \cap I^n)/(xR \cap I^{n+1}) \rightarrow (I^n/I^{n+1}) \rightarrow (\bar{I}^n/\bar{I}^{n+1}) \rightarrow 0$ ist exakt (Kern-Kokern Sequenz). Somit $\bar{s} \leq s$ und durch Aufaddieren für $n \gg 0$

$$Q_R(n) - Q_{\bar{R}}(n) = Q_{xR}^{ind}(n) .$$

2. Aus $I^n/I^{n+1} \rightarrow xI^n/xI^{n+1}$ folgt durch Aufaddieren

$$Q_{xR}^{I-ad}(n) \leq Q_R(n)$$

für $n \gg 0$. Ist x kein Nullteiler in R , gilt sogar $Q_{xR}^{I-ad}(n) = Q_R(n)$ wegen $I^n/I^{n+1} \cong xI^n/xI^{n+1}$.

3. Wegen $x \in I$ ist $xI^n \subset xR \cap I^{n+1} \subset R$. Somit folgt für alle $n \gg 0$ genügend groß $Q_{xR}^{ind}(n+1) \leq Q_{xR}^{I-ad}(n)$ (Lemma 30.2). Daraus folgen zusammen mit 2. und 3. folgende Ungleichungen $Q_R(n+1) - Q_{\bar{R}}(n+1) = Q_{xR}^{ind}(n+1) \leq Q_{xR}^{I-ad}(n) \leq Q_R(n)$. Die äußere Ungleichung liefert

$$Q_R(n+1) - Q_R(n) \leq Q_{\bar{R}}(n+1) .$$

Also $\deg(Q_{\bar{R}}) \geq \deg(Q_R) - 1$, da der führende Koeffizient von $Q_R(n)$ positiv ist. Das heißt: $\bar{s} \geq s - 1$.

4. Nach Artin-Rees gilt $xR \cap I^{n+k} \subset xI^n \subset xR$. Also $Q_{xR}^{ind}(n+k) \geq Q_{xR}^{I-ad}(n)$ für $n \gg 0$ (Lemma 30.2). Ist x kein Nullteiler, folgt nach 1. und 2. daraus $Q_R(n+k) - Q_{\bar{R}}(n+k) \geq Q_R(n)$ oder $Q_{\bar{R}}(n+k) \leq Q_R(n+k) - Q_R(n)$. Somit $\bar{s} \leq s - 1$, da der führende Koeffizient von $Q_{\bar{R}}(n)$ positiv ist. Zusammen mit der Ungleichung aus 3. folgt $\bar{s} = s - 1$. Q.e.d.

Korollar 31.3. *Sei R lokaler noetherscher Ring mit maximalem Ideal I . Für $x \in I$ gilt dann*

$$\dim(R) \leq \dim(R/xR) + 1$$

mit Gleichheit, wenn x kein Nullteiler von R ist.

32 Reguläre lokale Ringe

Sei R noethersch, lokal mit Restklassenkörper $K = R/I$. Jedes minimale Erzeugendensystem x_1, \dots, x_r des Ideals I muß I/I^2 als K -Vektorraum erzeugen. Elemente $x_1, \dots, x_r \in I$ mit $I = Rx_1 + \dots + Rx_r \pmod{I^2}$ tun dies andererseits (Nakayama Lemma). Es folgt $r = \dim_K(I/I^2)$. Nach §30 galt für die Hilbert-Dimension $s(R)$ immer $s(R) \leq r$. Wegen $s(R) = \dim(R)$ folgt daraus

$$\dim(R) \leq \dim_K(I/I^2).$$

Wird für einen noetherschen lokalen Ring R die Gleichheit

$$\boxed{\dim(R) = \dim_K(I/I^2)}$$

angenommen, heißt R regulär.

Wir bemerken an dieser Stelle, daß der Quotient I/I^2 eine geometrische Bedeutung besitzt. Man nennt den K -Vektorraum I/I^2 den Kotangentenraum des lokalen Rings (R, I) .

Für reguläre lokale Ringe ist die in §30 konstruierte Injektion

$$K[X_1, \dots, X_s] \hookrightarrow Gr_I(\mathbf{R})$$

wegen $s = \dim(R)$ (Korollar 31.1) eine Bijektion. Nämlich $I/I^2 = K \cdot X_1 + \dots + K \cdot X_s$. I^n/I^{n+1} wird dann von den Monomen vom Grad n in X_1, \dots, X_s erzeugt.

Korollar 32.1. *Für einen regulären lokalen Ring R der Dimension s mit Restklassenkörper $K = R/I$ gilt*

$$Gr_I(\mathbf{R}) = K[X_1, \dots, X_s].$$

Bemerkung: Sei R lokal noethersch mit maximalem Ideal und sei $Gr_I(\mathbf{R})$ nullteilerfrei und ganz abgeschlossen in seinem Quotientenkörper. Dann ist auch R nullteilerfrei und ganz abgeschlossen in seinem Quotientenkörper. Beachte, $\nu(x) = \min_\nu(x \notin I^{\nu+1})$ ist eine diskrete Bewertung¹⁰ auf R . Somit ist R nullteilerfrei. Sei r/s ganz über R . Dann folgt durch Betrachtung der graduierten Ganzheitsgleichung $r \in a \cdot s + I^{\nu(r)+1}$ für ein $a \in R$. Auch $r'/s' = r/s - a = (r - as)/s$ ist ganz über R . Iteriert man das Argument, folgt $r \in (s) + I^n$ für alle $n \in \mathbb{N}$. Aber $\bigcap_{n=0}^{\infty} ((s) + I^n) = (s)$. [Nakayama Lemma für den lokalen Ring $R/(s)$]. Es folgt $r \in (s)$ bzw. $r/s \in R$.

¹⁰Siehe §35

Korollar 32.2. *Reguläre lokale Ringe R sind normal, d.h. nullteilerfrei und ganz abgeschlossen in ihrem Quotientenkörper.*

Beweis: $K[X_1, \dots, X_s]$ ist nullteilerfrei und ganz abgeschlossen in seinem Quotientenkörper.

Korollar 32.3. *Ist R regulär lokal und $x \in I \setminus I^2$, dann ist auch R/x regulär lokal und von der Dimension $\dim(R/x) = \dim(R) - 1$.*

Normale Ringe

33 Krull's Hauptidealsatz

Satz 33.1. *Sei R noethersch und $a \in R$. Für jedes $P \in \text{GenSupp}(R/(a))$ gilt $h(P) \leq 1$. Ist R nullteilerfrei und $a \neq 0$, gilt $h(P) = 1$.*

Beweis: ObdA R lokal mit maximalem Ideal P ; ersetze dazu R durch die Lokalisierung nach P . Noethersch bleibt nach §16 erhalten! (Ist R nullteilerfrei, dann auch die Lokalisierung; $a \neq 0 \implies a/1 \neq 0$ in diesem Fall). Aus Korollar 31.3 folgt $\dim(R) - \dim(R/a) \leq 1$. Wegen $h(P) \leq \dim(R) - \dim(R/a)$ folgt also $h(P) \leq 1$. (Ist R nullteilerfrei und $a \neq 0$, gilt $h(P) = 1$ wegen $P \neq \{0\}$).

Bemerkung: Analog $h(P) \leq r$ für $P \in \text{GenSupp}(R/(a_1, \dots, a_r))$ und beliebige Elemente $a_1, \dots, a_r \in R$.

34 Faktorielle Ringe

Ein kommutativer Ring mit 1 heißt faktoriell, wenn R nullteilerfrei ist, und wenn jedes Element $0 \neq a$ aus R eine eindeutige Zerlegung der Form

$$a = \varepsilon \cdot \pi_1^{e_1} \cdots \pi_r^{e_r} \quad , \quad \varepsilon \in R^*$$

mit Primelementen $\pi_1, \dots, \pi_r \in R$ besitzt. Ein Element $0 \neq \pi \in R, \pi \notin R^*$ heißt prim oder Primelement, wenn für jede Zerlegung $\pi = a \cdot b$ entweder a oder b eine Einheit ist.

Existenz: Ist R noethersch, dann besitzt jedes Element ein Primfaktorzerlegung. Dies folgt unmittelbar aus dem Abbrechen aufsteigender Idealketten. Siehe LA-II-Skript. Im allgemeinen ist diese Primfaktorzerlegung aber nicht eindeutig!

Beispiel: $R = \mathbb{Z}[\sqrt{-5}] = \mathbb{Z}[X]/(X^2 + 5)$ ist nicht faktoriell wegen

$$2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$$

für Primelemente $2, 3, 1 \pm \sqrt{-5}$ von R , deren Hauptideale – wie man durch Normbildung leicht sieht – paarweise verschieden sind. Die aufgespannten

Hauptideale (2) , (3) , $(1 \pm \sqrt{-5})$ sind jedoch keine Primideale. Die darüber Primideale sind

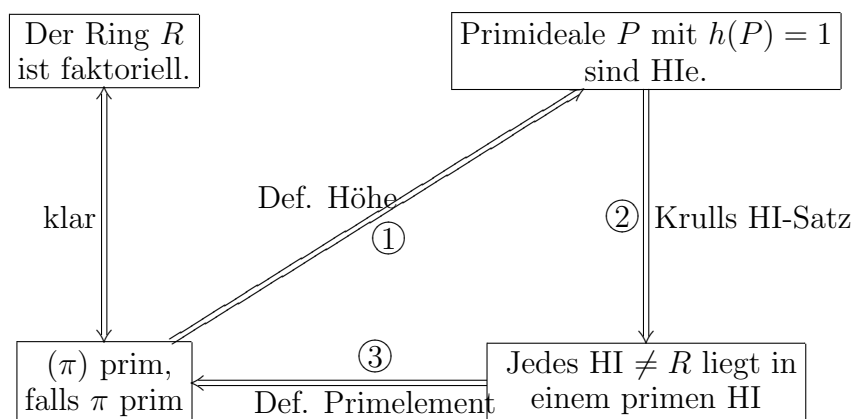
$$(2, 1 \pm \sqrt{-5}) \text{ sowie } (3, 1 + \sqrt{-5}) \text{ und } (3, 1 - \sqrt{-5}).$$

Eindeutigkeit: Sei R faktoriell. Sei $\pi \in R$ prim. Aus $\pi|a \cdot b$ folgt durch Primfaktorzerlegung von a und b sofort $\pi|a$ oder $\pi|b$. Somit ist das Hauptideal (π) des Primelements π ein Primideal.

Sei umgekehrt R ein (noetherscher) Ring, in dem für jedes prime Element $\pi \in R$ das zugehörige Hauptideal (π) ein Primideal ist. Dann folgt die Eindeutigkeit von Primfaktorzerlegungen in R . Man zeigt dies durch Induktion nach der Länge einer Primfaktor-Zerlegung wie im Fall euklidischer Ringe (LA-II Skript).

Lemma 34.1. Sei R ein nullteilerfreier, noetherscher Ring. Dann sind äquivalent

Bezeichnung (HI = Hauptideal)



Beweis: 1) Def.Höhe: Sei R faktoriell, d.h. (π) sei prim für jedes Primelement $\pi \in R$. Sei P ein Primideal der Höhe 1 in R . Wähle $0 \neq a \in P$ mit Primfaktorzerlegung $a = \varepsilon \cdot \prod_i \pi_i \in P$. Da P Primideal ist folgt $\pi \in P$ für mindestens einen Primfaktor $\pi = \pi_i$ von a . Also $\{0\} \subset (a) \subset (\pi) \subset P$. Da $\{0\}$ und (π) Primideale sind, folgt dann $P = (\pi)$ wegen $h(P) = 1$. Somit ist P ein Hauptideal.

2) Krulls HI-Satz: Sei $(a) \neq R$ ein Hauptideal. ObdA $a \neq 0, a \notin R^*$. Die minimalen Primideale P über (a) haben dann Höhe $h(P) = 1$ nach Krulls Hauptidealsatz 33.1. Somit sind sie nach Annahme Hauptideale.

3) Def. Primelement: Sei π ein Primelement. Nach Annahme existiert ein primes Hauptideal (a) mit $(\pi) \subset (a)$. Also $\pi = r \cdot a$. Da π Primelement ist, folgt $r \in R^*$ wegen $a \notin R^*$ (sonst wäre $(a) = R$ kein Primideal!). Es folgt $(\pi) = (a)$. Also ist (π) ein Primideal. Q.e.d.

Wir erinnern abschließend an den Satz von Gauß (siehe Algebra I)

Satz 34.2. *Ist R faktoriell, dann auch der Polynomring $R[X]$.*

Als Konsequenz

Korollar 34.3. *Polynomringe über \mathbb{Z} oder einem Körper K sind faktoriell.*

35 Diskrete Bewertungen

Sei R noethersch lokal mit maximalem Ideal I . Für einen lokalen Ring R mit maximalem Ideal I gilt $R \setminus I = R^*$ (§11). Weiterhin gilt $\bigcap_{n=0}^{\infty} I^n = 0$ (Nakayama's Lemma). Für $0 \neq x \in I$ sei $n = v(x)$ das minimale $n \in \mathbb{N}$ mit $x \notin I^{n+1}$. Für $x \in R \setminus I = R^*$ setzen wir $v(x) = 0$. Dann gilt $x = \varepsilon \cdot a^{v(x)}$. Setze noch formal $v(0) := \infty$.

Ist a kein Nullteiler in R , ist der so definierte Exponent $v(x)$ eindeutig durch x bestimmt. Insbesondere ist dann $R = \bigcup_{\nu=0}^{\infty} R^* \cdot a^{\nu}$ nullteilerfrei.

Lemma 35.1. *Sei R noethersch lokal und das maximale Ideal sei ein Hauptideal $I = (a)$. Dann hat jedes Ideal J die Gestalt $J = (a^n)$. R ist ein Hauptidealring der Dimension ≤ 1 .*

Beweis: $0 \neq x \in R$ schreibt sich in der Form $x = a^{v(x)} \cdot \varepsilon$ mit $\varepsilon \in R^* = R \setminus I$. Es folgt $J = (x_1, \dots, x_r) = (a^n)$ für $n = \min(v(x_1), \dots, v(x_r))$. Q.e.d.

Bewertungsringe: Erfüllt R die Annahmen von Lemma 35.1 und ist a kein Nullteiler in R , dann ist R ein regulärer lokaler Ring von der Dimension $\dim(R) = 1$. Die Umkehrung gilt offensichtlich auch. Ein solcher Ring ist insbesondere nullteilerfrei. Erfüllt R die Annahmen von Lemma 35.1 und

ist nullteilerfrei, dann nennt man R einen diskreten Bewertungsring. Die Zuordnung $x \mapsto v(x)$ definiert eine diskrete Bewertung, also eine Funktion

$$v : R \rightarrow \mathbb{Z} \cup \{\infty\}$$

mit den Eigenschaften

- 1) $v(x \cdot y) = v(x) + v(y)$
- 2) $v(x + y) \geq \min(v(x), v(y))$
- 3) $v(x) = \infty \iff x = 0$.

Eine Bewertung v eines nullteilerfreien Rings R kann mittels $v(x/y) = v(x) - v(y)$ auf den Quotientenkörper $K = \text{Quot}(R)$ fortgesetzt werden. Für einen diskreten Bewertungsring (im obigen Sinn) gilt dann sogar $K^* = a^{\mathbb{Z}} \cdot R^*$ (oder $\dim(R) = 0$ und R ist bereits ein Körper). Die Eigenschaften 1) und 2) bleiben erhalten, und es gilt: Für $x \in K$ sind äquivalent $x \in R$ und $v(x) \geq 0$.

Bemerkung: Ein diskreter Bewertungsring R ist normal, d.h. nullteilerfrei und ganz abgeschlossen in seinem Quotientenkörper. Nullteilerfreiheit folgt aus 1) und 3). Aus $x^n + r_1 \cdot x^{n-1} + \dots + r_n = 0$ und $r_i \in R$ folgt andererseits $n \cdot v(x) \geq \min((n-1)v(x), \dots, v(x), 0)$, also $v(x) \geq 0$ bzw. $x \in R$. [Unter der zusätzlichen Annahme $\dim(R) = 1$ ist R dann ein regulärer lokaler Ring der Dimension 1. Dies folgt aus dem nächsten Lemma 35.2 wegen (iii) \implies (ii).

Das duale Ideal I^*

Sei R ein nullteilerfreier Ring und I ein Ideal in R . Die Menge I^* aller x in $\text{Quot}(R)$ mit $x \cdot I \subset R$ ist ein R -Modul. Per Definition gilt $I^*I \subset R$ und $R \subset I^*$.

Lemma 35.2. *Sei R ein lokaler noetherscher normaler Ring mit maximalem Ideal I . Dann sind äquivalent*

- (i) $I^* \neq R$.
- (ii) I ist Hauptideal und somit R ein diskreter Bewertungsring.
- (iii) $\dim(R) \leq 1$.
- (iv) $I \in \text{Ass}(R/(a))$ für ein $a \in R$.

Beweis: Angenommen es gilt (i). Aus $I^*I \subset R$ und $R \subset I^*$ folgt $I \subset I^*I \subset R$. Da I ein maximales Ideal ist, folgt

$$\boxed{I^*I = R}.$$

[$I^*I = I$ ist ausgeschlossen. I^* wäre ganz über R (I ist ein endlich erzeugter R -Modul), also wäre $I^* = R$ entgegen der Annahme (i).]

Wähle $a \in I$ (obdA $a \notin I^2$ wegen des Nakayama Lemmas, denn der Körperfall $I = 0$ ist trivial). Dann ist $I^*a \subset I^*I = R$. Somit gilt entweder $I^*a \subset I$ (also $(a) = II^*a \subset I^2$ im Widerspruch zu $a \notin I^2$) oder daher $I^*a = R$. Letzteres impliziert $(a) = (II^*)a = I(I^*a) = I$, also $I = (a)$. Die Implikationen (i) \implies (ii) \implies (iii) folgen daher aus Lemma 35.1.

(iii) \implies (iv): Wegen $\dim(R) \leq 1$ und der Nullteilerfreiheit von R sind $\{0\}$ und I die einzigen Primideale von R . ObdA können wir annehmen $I \neq \{0\}$, da der Körperfall trivial ist. Für $0 \neq a \in I$ ist dann $\text{Ass}(R/a) \subset \text{Supp}(R/a) = \{I\}$.

(iv) \implies (i): Sei $I \in \text{Ass}(R/a)$. Dann existiert $R/I \cong \langle m \rangle$ zyklisch in R/a mit $I = \text{Ann}(m) = \{r \in R \mid r \cdot x \in (a)\}$ für ein Urbild $x \in R$ von $m \in R/a$. Also $\xi \cdot I \subset R$ für $\xi = x/a$, bzw $\xi \in I^*$. Genauer

$$\boxed{\xi = x/a \in I^* \setminus R}$$

wegen $x \notin (a) \iff m \neq 0 \in R/(a)$. Also $I^* \neq R$. Q.e.d.

36 Primärzerlegung von Hauptidealen

Sei R ein noetherscher normaler Ring mit Quotientenkörper $K = \text{Quot}(R)$.

Lokalisierungen: Für jedes Primideal $P \in X$ ist die Lokalisierung R_P dann wieder noethersch und normal in K : Dafür müssen wir zeigen, daß R_P wieder ganz abgeschlossen in K ist. Sei $(\xi)^n + (r_1/s_1)(\xi)^{n-1} + \dots + (r_n/s_n) = 0$ eine Ganzheitsgleichung von $\xi \in K$ über $S^{-1}R = R_P$, dann genügt $\xi \cdot \prod_{i=1}^n s_i \in K$ einer Ganzheitsgleichung über R und liegt somit in R . Also $\xi \in R_P$.

Wir behaupten

Lemma 36.1. *Sei R noethersch. Ist R normal dann gilt¹¹ für alle $a \in R$*

$$\text{Ass}(R/a) = \text{GenSupp}(R/a)$$

¹¹Umgekehrt folgt die Normalität von R aus diesen Eigenschaften, indem man damit direkt Lemma 38.3 zeigt. Ein Durchschnitt von Bewertungsringen ist nämlich normal.

und jedes P in $\text{GenSupp}(R/a)$ ist ein Primideal in R (der Höhe 1), dessen lokaler Ring R_P ein diskreter Bewertungsring ist.

Beweis: ObdA $a \neq 0$. Für $\bar{P} \in \text{Ass}(R/a)$ sei P das Urbild in R mit $a \in P$ und $R_P = S^{-1}R$ die Lokalisierung von R nach P mit dem maximalem Ideal $I = S^{-1}P$. Dann ist $I \in \text{Ass}(R_P/a)$. [Für $m \in R/a$ mit $\text{Ann}_R(m) = P$ gilt $s \cdot m \neq 0$ für alle $s \in S = R \setminus P$. Also $m/1 \neq 0$ in R_P/a . Somit $\text{Ann}_{R_P}(m/1) \neq R_P$. Andererseits gilt $P \cdot m = 0$, also $I \cdot m/1 = 0$ und daher $\text{Ann}_{R_P}(m/1) = I$]. Somit ist jetzt obdA R lokal, noethersch, normal mit maximalem Ideal und $I \in \text{Ass}(R/a)$. Daraus folgt $\dim(R_P) = 1$ wegen der Implikation (iv) \implies (iii) von Lemma 35.2. Wegen $\dim(R_P) = 1$ ist dann aber P ein minimales Primideal über (a) (nach dem Krullschen Hauptidealsatz). Es folgt $\text{Ass}(R/a) \subset \text{GenSupp}(R/a)$. Die andere Inklusion gilt nach Lemma 20.1. Q.e.d.

Folgerung 36.2. *Sei R noethersch und normal. Dann besitzt jedes Hauptideal $(a) \neq R$ eine eindeutige Primärzerlegung als endlicher Durchschnitt von symbolischen Potenzen $P^{(n)}$ von Primidealen P der Höhe 1*

$$(a) = \bigcap_{P_i \in X^1} P_i^{(n_i)} \quad , \quad n_i = v_{P_i}(a) \quad .$$

Beweis: Die Primärzerlegung $(a) = \bigcap_i Q_i$ in primäre Ideale Q_i ist eindeutig wegen Lemma 36.1 und Satz 24.2. Die Ideale Q_i sind primär zu Primidealen P_i der Höhe 1 nach Lemma 36.1. Nach Abschnitt §5 entsprechen die P_i -primären Ideale genau den $S^{-1}P_i$ -primären Idealen der Lokalisierung $R_{P_i} = S^{-1}R$. Da dieser lokale Ring ein diskreter Bewertungsring ist, sind die von Null verschiedenen Ideale dieses lokalen Rings die Potenzen des maximalen Ideals. Daraus folgt, daß $Q_i = P_i^{(n)}$ eine symbolische Potenz des Primideals P_i ist. Siehe §24.

Korollar 36.3. *Endliche Durchschnitte von Hauptidealen schreiben sich in der Form*

$$\bigcap_{a \in J} (a) = \bigcap_{P_i \in X^1} P_i^{(n_i)} \quad , \quad n_i = \max_{a \in J} (v_{P_i}(a)) \quad .$$

Im nächsten Abschnitt geben wir einen von der Primärzerlegung unabhängigen Zugang zu den obigen Resultaten.

37 Reflexive Ideale

In diesem Paragraphen sei R ein nullteilerfreier noetherscher Ring und K der Quotientenkörper von R . Ein endlich erzeugter R -Untermodul $I \neq 0$ von K heißt gebrochenes Ideal von R . Es gibt dann ein $r \in R$ mit $r \cdot I \subset R$. Also sind die gebrochenen Ideale die R -Moduln der Gestalt $\xi \cdot I$ für $\xi \in K^*$ und Ideale I in R . Zwei gebrochene Ideale I_1, I_2 heißen äquivalent, wenn $\xi \cdot I_1 = I_2$ gilt für ein $\xi \in K^*$. Jedes gebrochene Ideal ist dann äquivalent zu einem Ideal in R . Jedes Ideal in R ist äquivalent zu einem gebrochenen Ideal das 1 und damit R enthält. Ein gebrochenes Ideal der Gestalt $(\xi) = \xi \cdot R$ heißt (gebrochenes) Hauptideal. Für ein gebrochenes Ideal sei

$$I^* = \{x \in K \mid x \cdot I \subset R\} .$$

Offensichtlich gilt $R^* = R$ und $(\xi \cdot I)^* = \xi^{-1} \cdot I^*$. Aus $I_1 \subset I_2$ folgt $I_2^* \subset I_1^*$. Aus $I \supset R$ folgt $I^* \subset R$, also ist I^* wieder ein gebrochenes Ideal. Daraus folgt aber durch Übergang zur Äquivalenzklasse, daß I^* für beliebige gebrochene Ideale I wieder ein gebrochenes Ideal ist.

Allgemein gilt $I \subset I^{**} = (I^*)^*$. Gilt dann $I = (I^*)^*$, nennt man das gebrochene Ideal I reflexiv. Beispiel: Von Null verschiedene Hauptideale sind reflexiv. Allgemein gilt $\xi \in (I^*)^* \iff \xi \cdot y \in R$ für alle $y \in K \setminus 0$ mit $y \cdot I \subset R$. Dazu äquivalent ist $\xi \in (y^{-1})$ falls $I \subset (y^{-1})$. Also

$$I^{**} = \bigcap_{x \in K, I \subset (x)} (x) .$$

Durchschnitte: Diese Formel für I^{**} impliziert für reflexive Ideale I_j sofort $(\bigcap_j I_j)^{**} \subset \bigcap_j (\bigcap_{x \in K, I_j \subset (x)} (x)) = \bigcap_j I_j^{**} = \bigcap_j I_j$ und somit wegen der umgekehrten trivialen Inklusion beim Doppeldual

$$\left(\bigcap_j I_j\right)^{**} = \bigcap_j I_j .$$

Es folgt

Lemma 37.1. *Ein gebrochenes Ideal I eines nullteilerfreien noetherschen Rings ist genau dann reflexiv, wenn I ein endlicher¹² Durchschnitt von (gebrochenen) Hauptidealen ist.*

Bemerkung: Für jedes gebrochene Ideal I ist I^* reflexiv: Einerseits gilt $I^* \supset (I^{**})^*$ wegen $I \subset I^{**}$. Andererseits gilt $I^* \subset (I^*)^{**}$. Es folgt $I^* = I^{***}$.

Übungsaufgabe: Es gilt $I^* = \text{Hom}_R(I, R)$. Benutze, jedes $\varphi \in \text{Hom}_R(I, R)$ ist von der Gestalt $\varphi(a) = x \cdot a$ für ein $x \in K$.

¹² $I \mapsto I^*$ transferiert absteigende Ketten reflexiver Ideale in aufsteigende Ketten.

* Appendix

Wir zeigen für nullteilerfreie noethersche Ringe R die folgende Verschärfung¹³ des Krullschen Hauptidealsatzes:

Sei $I' \subset R$ reflexiv. Da R noethersch ist gibt es unter den reflexiven Idealen I mit der Eigenschaft $1 \notin I$ und $I' \subset I \subset R$ ein maximales. Ist I maximal in diesem Sinn, dann ist I ein Primideal. Genauer

Satz 37.2. *Maximale reflexive Oberideale $I \subsetneq R$ eines gegebenen reflexiven Ideals in R sind Primideale. Sie haben Höhe 1 und sind von der Gestalt $I = (x) \cap (1)$ für ein $x \in K^*$.*

Beweis: $I = \bigcap_{x \in J} (x)$ (Reflexivität). ObdA $1 \in J$ und dann obdA $(x) \cap (1) \neq (1)$ für $x \in J$. Dadurch gilt entweder $J \subset R$, und wegen der Maximalität von I somit $\#J = 1$ und $I = (x) = (x) \cap (1)$. Oder wegen der Maximalität von I gilt $I = (x) \cap (1)$ für ein einziges $x \in J \setminus R$. Damit ist bereits die letzte Aussage gezeigt.

Aus $I \subsetneq R$ folgt $I \subset P \subsetneq R$ für ein $P \in \text{Spec}(R)$. Sei $a \cdot b \in I$ für $a, b \in R$.

Der Fall $(a^{-1}x) \cap (1) \subseteq P$: Hier gilt $I = (x) \cap (1) \subset (a^{-1}x) \cap (1) \subset P \subset R$. Wegen der Maximalität von I ist daher $I = (a^{-1}x) \cap (1)$. Andererseits gilt $b \in (a^{-1}x) \cap (a^{-1})$ und $b \in (1)$. Also $b \in (a^{-1}x) \cap (1) = I$.

Der Fall $(a^{-1}x) \cap (1) \not\subseteq P$: Dann existiert ein $c \in R$ mit $c \notin P$ und $c \in (a^{-1}x) \cap (1)$. Somit $a \cdot c \in (x) \cap (c) \subset (x) \cap (1)$. Also $a \in (c^{-1}x) \cap (c^{-1})$ sowie $a \in (1)$. Es folgt

$$a \in (c^{-1}x) \cap (1) .$$

Aber $c \cdot [(c^{-1}x) \cap (1)] \subset (x) \cap (c) \subset (x) \cap (1) \subset P$. Da P ein Primideal ist und da $c \notin P$, folgt daraus $(c^{-1}x) \cap (1) \subset P \subsetneq R$. Aus der Maximalität von I und der Reflexivität von $(c^{-1}x) \cap (1)$ folgt $(c^{-1}x) \cap (1) = I$ und damit $a \in I$.

Somit gilt entweder $a \in I$ oder $b \in I$. Also ist I ein Primideal in R .

Da I reflexiv ist, gilt $h(I) \leq 1$. [Benutze Lokalisierung nach I ! Reflexivität bleibt erhalten – also $I^* \neq R$ – und I wird maximal. Aus Lemma 35.2 folgt dann $h(I) = \dim(R_I) \leq 1$]. Q.e.d.

¹³Der Beweis ist unabhängig vom Beweis in 33

38 Die Klassengruppe

In diesem Paragraph sei R noethersch und normal. Sei $X = \text{Spec}(R)$ und

$$X^1 \subset X$$

die Menge der Primideale P von R der Höhe $h(P) = 1$. Wie bereits in §36 gezeigt gilt

Lemma 38.1. *Ist R noethersch und normal, dann ist auch jede Lokalisierung R_P nach einem Primideal P von R noethersch und normal.*

Sei $P \neq 0$ minimal, also $P \in X^1$. Dann gilt $\dim(R_P) = 1$ für den lokalen und noetherschen normalen Ring R_P . Wir erhalten nach Lemma 35.2

Lemma 38.2. *Sei R noethersch, normal mit $K = \text{Quot}(R)$ und $P \in X^1$ ein Primideal mit $h(P) = 1$. Dann ist die Lokalisierung R_P ein diskreter Bewertungsring. D.h. es existiert eine diskrete Bewertung $v = v_P$ von K mit $R_P = \{x \in K \mid v(x) \geq 0\}$ und maximalem Ideal $\{x \in K \mid v(x) > 0\}$.*

Sei

$$\text{Div}(R) = \bigoplus_{P \in X^1} \mathbb{Z} \cdot P .$$

Jedem Element $x \in K^*$ ist ein Divisor in $\text{Div}(R)$ zugeordnet durch

$$\text{Div}(x) = \sum_{P \in X^1} v_P(x) \cdot P .$$

Fast alle $v_P(x)$ sind Null; dazu kann obdA $x \in R$ angenommen werden. Dann liegen nur endliche Primideale der Höhe 1 über dem Hauptideal (x) (die generischen Punkte von $R/(x)$ wegen des Krullschen Hauptidealsatzes).

Notation: Wir schreiben $D_1 = \sum_{P \in X^1} n_P \cdot P \geq D_2 = \sum_{P \in X^1} m_P \cdot P$ für Divisoren D_1, D_2 , wenn $n_P \geq m_P$ für alle $P \in X^1$ gilt.

Lemma 38.3. *Unter den Voraussetzungen von 38.2 gilt $R = \bigcap_{P \in X^1} R_P$, d.h. für $x \in K^*$ sind äquivalent*

$$x \in R \iff \text{Div}(x) \geq 0 .$$

Beweis: Die Inklusion \subset ist trivial. Sei umgekehrt $x = \frac{r}{s} \in K^*$ gegeben mit $v(x) \geq 0$ für alle $P \in X^1$. Das heißt $\max(v_P(r), v_P(s)) = v_P(r)$ für alle $P \in X^1$. Aus 36.3 und $\text{Div}(x) \geq 0 \iff \text{Div}(r) \geq \text{Div}(s)$ folgt $(s) \cap (r) = (r)$, also $r \in (s)$, d.h. $x \in R$. Q.e.d.

Alternativer Beweis: Das Ideal $I = (x^{-1}) \cap (1)$ in R ist reflexiv. Wäre $I \subsetneq R$, gibt es ein $P \in X^1$ mit $I \subset P$ nach Satz 37.2. Also $(s) \cap (r) \subset r \cdot P$ (alternativ folgt dies auch aus Folgerung 36.2). Durch Lokalisieren nach P folgt $S^{-1}[(s) \cap (r)] = S^{-1}(s) \cap S^{-1}(r) \subset S^{-1}r \cdot P \subsetneq S^{-1}R = R_P$. Da R_P ein Bewertungsring ist folgt $\max(v_P(s), v_P(r)) \geq v_P(r) + 1$. Ein Widerspruch. Somit gilt $(x^{-1}) \cap (1) = R$ und $1 = t \cdot x^{-1}$ für ein $t \in R$. Somit $x = t \in R$. Q.e.d.

Korollar 38.4. *Ein Element in K^* ist genau dann eine Einheit von R , wenn für alle $P \in X^1$ gilt $v_P(x) = 0$.*

Man erhält daher eine exakte Sequenz

$$0 \rightarrow R^* \rightarrow K^* \rightarrow \text{Div}(R) \rightarrow \text{Cl}(R) \rightarrow 0 .$$

Den Kokern $\text{Cl}(R)$ der Divisorenabbildung nennt man die Klassengruppe des Rings R . Nach Lemma 34.1 ist der Ring R genau dann faktoriell, wenn gilt $\text{Cl}(R) = 0$.

Bemerkung: Jeder Divisor $D \in \text{Div}(R)$ definiert ein gebrochenes Ideal

$$I(D) = \{x \in K \mid v_P(x) \geq D\} .$$

Beachte, für jedes D existiert ein $\xi \in R$ mit $\text{Div}(\xi) + D \geq 0$. Somit $\xi \cdot I(D) \subset I(0) = R$. Offensichtlich gilt $I(D)^* = I(-D)$. Insbesondere ist daher $I(D)$ reflexiv. Für Hauptdivisoren $D = (\xi)$ folgt weiterhin $I(D) = (\xi)$. Wegen $\bigcap_{i=1}^r I(D_i) = I(D)$ für $D = \sup_i(D_i)$, ist daher dann sogar jedes reflexive Ideal I von der Gestalt $I = I(D)$ wegen Lemma 37.1.

Die Primideale $P \in X^1$ sind Spezialfälle. Beachte $P = \{x \in R \mid v_P(x) \geq 1\}$ wegen¹⁴ $P = g^{-1}(S^{-1}P) = R \cap (P \cdot R_P)$. Aus Lemma 38.3 folgt somit

$$I(P) = P .$$

Folgerung: Ist R noethersch und normal, dann sind die Primideale $P \in X^1$ reflexiv. Nach Satz 37.2 sind dies genau die reflexiven Primideale von R .

¹⁴Bezeichnungen wie in §5.

Ringe der Dimension 1

39 Dedekindringe

Ein noetherscher, normaler Ring der Dimension ≤ 1 heißt Dedekindring. Die Primideale $P \neq \{0\}$ eines Dedekindrings sind wegen $\dim(R) = 1$ alle maximal und haben die Höhe 1. Insbesondere sind sie daher reflexiv.

Lokalisierungen von Dedekindringen sind wieder Dedekindringe.

Beispiele: \mathbb{Z} und $K[X]$ für Körper K sind Dedekindringe. Für jede endliche¹⁵ Körpererweiterung L von \mathbb{Q} (Zahlkörper) bzw. von $K(t)$ (Funktionskörper) ist der ganze Abschluß von \mathbb{Z} resp. $K[t]$ in L wieder ein Dedekindring.

Sei $I \neq 0$ ein Ideal eines Dedekindrings R und sei $I = \bigcap_{i=1}^r Q_i$ sei seine Primärzerlegung. Hierbei sind Q_i P_i -koprimäre Ideale; die P_i sind notwendig maximale Ideale von R . Dann bedeutet P_i -koprimär aber gerade

$$P_i^n \subset Q_i \subset P_i$$

für ein geeignetes $n \in \mathbb{N}$. Genauer gilt für Dedekindringe dann aber sogar $Q_i = P_i^n$ für geeignetes n , denn die P_i -primären Ideale entsprechen eindeutig den P_i -primären Idealen der Lokalisierung R_{P_i} (siehe §5). In der Lokalisierung ist jedes Ideal eine Potenz des maximalen Ideals (Lemma 35.2 und Lemma 35.1). Aus dieser verfeinerten Primärzerlegung folgt

$$I = \bigcap_{i=1}^r P_i^{n_i} .$$

Hierbei sind obdA die P_i paarweise verschieden, indem man überflüssige Terme streicht. Da es für jeden Divisor $D \in \text{Div}(R)$ ein reflexives Ideal $I(D)$ gibt, folgt durch Vergleich sofort

$$I = I(D) \quad , \quad D = \sum_{i=1}^r n_i \cdot P_i .$$

Folgerung 39.1. *Jedes (gebrochene) Ideal $I \neq 0$ eines Dedekindrings ist reflexiv und einem eindeutig bestimmten Divisor D zugeordnet: $I = I(D)$.*

Sein nun $\dim(R) = 1$, d.h. R kein Körper. Sind P_i und P_j verschiedene maximale Ideale des Dedekindrings, dann gilt $I = R$ für das Ideal $I :=$

¹⁵Für den inseparablen Fall siehe Zariski-Samuel

$P_i^{n_i} + P_j^{n_j}$ (für beliebige $n_i > 0, n_j > 0$). [Beachte $V(I) = V(P_i^{n_i}) \cap V(P_j^{n_j}) = \{P_i\} \cap \{P_j\} = \emptyset$, also $I = R$]. Somit

$$P_i^{n_i} \cap P_j^{n_j} = P_i^{n_i} \cdot P_j^{n_j}$$

nach Lemma 10.1. Dieser Schluß verallgemeinert sich sofort auf endliche Produkte. Es folgt

Korollar 39.2. *Jedes Ideal $I \neq 0$ eines Dedekindringes R schreibt sich auf eindeutige Weise als ein Produkt von Primidealpotenzen*

$$I = \prod_{i=1}^r P_i^{n_i}$$

für paarweise verschiedene maximale Ideale P_i von R (die auftretenden Primideale P_i sind die Elemente von $\text{Ass}(R/I)$).

Die gebrochenen Ideale bilden daher von sich aus eine Gruppe, welche man mit der Divisorengruppe identifizieren kann.

Beispiel: Im Ring $R = \mathbb{Z}[\sqrt{-5}]$ gilt $(2, 1 + \sqrt{-5}) = (2, 1 - \sqrt{-5})$ sowie $2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$. Somit

$$(2, 1 + \sqrt{-5})^2 = (2)$$

$$(3, 1 + \sqrt{-5}) \cdot (3, 1 - \sqrt{-5}) = (3)$$

$$(2, 1 + \sqrt{-5}) \cdot (3, 1 - \sqrt{-5}) = (1 - \sqrt{-5})$$

$$(2, 1 + \sqrt{-5}) \cdot (3, 1 + \sqrt{-5}) = (1 + \sqrt{-5})$$

wegen $(2, 1 + \sqrt{-5}) \cdot (2, 1 - \sqrt{-5}) = (4, 2(1 \pm \sqrt{-5}), 6) = (2)$. Wegen $(9, 3(1 + \sqrt{-5}), 3(1 - \sqrt{-5}), 6) = (3)$. Wegen $(6, 2(1 - \sqrt{-5}), 3(1 + \sqrt{-5}), 6) = (6, 2(1 - \sqrt{-5}), 3(1 - \sqrt{-5})) = (1 - \sqrt{-5})$ und wegen $(2, 1 - \sqrt{-5}) \cdot (3, 1 + \sqrt{-5}) = (1 + \sqrt{-5})$.

40 Zahlkörper

Sei L/\mathbb{Q} eine endliche Körpererweiterung. Der ganze Abschluß $R = \mathcal{O}_L$ von \mathbb{Z} in L ist ein Dedekindring. Going up liefert eine Surjektion

$$\pi : \text{Spec}(R) \twoheadrightarrow \text{Spec}(\mathbb{Z})$$

mit Fasern $Y = \pi^{-1}(p)$.

Beispiel Der Ring $R = \mathbb{Z}[\sqrt{-5}]$ ist normal in L . Also $R = \mathcal{O}_L$ und es gilt

$$\pi^{-1}(\{(2)\}) = \{ (2, 1 + \sqrt{-5}) \} .$$

Weiterhin $\pi^{-1}(\{(3)\}) = \{ (3, 1 + \sqrt{-5}), (3, 1 - \sqrt{-5}) \}$.

Zur Erinnerung: Die Primideale $P \in Y$ von über einem maximalen Ideal $p \subset \mathbb{Z}$ sind die Primideale von R mit der Eigenschaft $P \cap \mathbb{Z} = p$ oder $P \supseteq p \cdot R$. Es folgt

$$Y \cong \text{Spec}(R/pR) .$$

Zerlegungsgesetz: Das Hauptideal $p \cdot R$ schreibt sich nach Kor.39.2 als Produkt

$$p \cdot R = \prod_{i=1}^g P_i^{e_i} .$$

Das Produkt erstreckt sich über die Primideale $P_1, \dots, P_g \in \text{Ass}(R/pR)$. Wegen $\dim(R) = 1$ ist jedes Primideal in $\text{Ass}(R/pR)$ isoliert. Es folgt

$$\text{Ass}(R/pR) = \text{GenSupp}(R/pR) = \text{Spec}(R/pR) = Y .$$

Beispiel: Für $R = \mathbb{Z}[\sqrt{-5}]$ ist $2 \cdot R = (2, 1 + \sqrt{-5})^2$. Dagegen $3 \cdot R = (3, 1 + \sqrt{-5}) \cdot (3, 1 - \sqrt{-5})$.

Man zeigt nun ohne Mühe, daß R als Untermodul eines freien \mathbb{Z} -Moduls (siehe §16) selbst ein freier \mathbb{Z} -Modul ist. Also

Lemma 40.1. *R ist ein freier \mathbb{Z} -Modul vom Rang $[L : \mathbb{Q}]$.*

R/pR ist also eine \mathbb{F}_p -Algebra der Dimension $[L : \mathbb{Q}]$ und zerfällt nach Satz 10.2 in eine direkte Summe lokaler \mathbb{F}_p -Algebren R_i

$$R/pR \cong \bigoplus_{P_i \in Y} R_i .$$

Restklassengrad: $R/P_i = (R_i)_{\text{red}}$ ist der Restklassenkörper von P_i , ein endlicher Erweiterungskörper von \mathbb{F}_p mit Restklassengrad $f_i = [R/P_i : \mathbb{F}_p]$.

Verzweigungsindex: Beachte $R_i \cong R/P_i^{e_i}$. Der Verzweigungsindex e_i ist die Länge des R -Moduls $R/P_i^{e_i}$. Es gilt $\dim_{\mathbb{F}_p}(R_i) = e_i \cdot [R/P_i : \mathbb{F}_p]$ (wegen Lemma 38.2 ist die P_i -Lokalisierung von R ein Bewertungsring).

Dimensionsformel: Aus der Summenzerlegung von R/pR folgt

$$[L : \mathbb{Q}] = \sum_{P \in Y} e_P \cdot f_P .$$

Idealnormen: Definiere für maximale Ideale P von R die Norm

$$N(P) = \#(R/P) .$$

Für P über $p \cdot R$ gilt $N(P) = p^f$ für $f = [R/P : \mathbb{F}_p]$. Es folgt

Korollar 40.2. *Sei p eine Primzahl und $p \cdot \mathcal{O}_L = \prod_P P^{e_P}$ seine Faktorisierung in \mathcal{O}_L . Dann gilt die Normen*

$$p^{[L:\mathbb{Q}]} = \prod_P N(P)^{e_P} .$$

Das Produkt durchläuft die Primideale von \mathcal{O}_L über p , und es gilt $e_P \geq 1$.

Galois Fall: Sei L/\mathbb{Q} galoisch mit Galoisgruppe G . G operiert auf $\text{Spec}(\mathcal{O}_L)$ und $Y = \pi^{-1}((p))$. Sei $Y = \coprod Y_j$ die Zerlegung in G -Orbits. Wähle $f \in R$ mit $f \in P = P_1 \in Y_1$ und $f \notin P_i, i \geq 2$ (Punktetrennung). Es folgt $N(f) = \prod_{\sigma \in G} \sigma(f) \in P$ für alle $P \in Y_1$, und $N(f) \notin P$ für die $P \in Y \setminus Y_1$. Aber $N(f) \in \mathbb{Z}$ liegt in (p) und somit in allen $P \in Y$. Es folgt $Y = Y_1$ und somit

Lemma 40.3. *Ist L/\mathbb{Q} galoisch, dann operiert die Galoisgruppe transitiv auf den Fortsetzungen P des Primideals (p) . Die Restklassengrade f_P und die Verzweigungszahlen e_P hängen nur ab von p . Setzt man $g_p := \#Y$, gilt*

$$\#G = e_p \cdot f_p \cdot g_p .$$

41 Kreiskörper

Sei die Situation wie im letzten Paragraph, aber nun speziell

$$L = \mathbb{Q}(\zeta_{p^n})$$

für eine primitive p^n -te Einheitswurzel ζ_{p^n} . L ist der Zerfällungskörper des über \mathbb{Q} irreduziblen ganzzahligen Kreispolynoms

$$\Phi_{p^n}(X) = X^{(p-1)p^{n-1}} + \dots + 1 .$$

Also ist ζ_{p^n} ganz über \mathbb{Z} wegen $\Phi_{p^n}(\zeta_{p^n}) = 0$ (Ganzheitsgleichung). Somit ist

$$R = \mathbb{Z}[\zeta_{p^n}] = \mathbb{Z}[X]/(\Phi_{p^n}(X)) .$$

ein Unterring von \mathcal{O}_L .

Lemma 41.1. $R = \mathcal{O}_L$.

Beweis: 1) $L = S^{-1}R$ für $S = \mathbb{Z} \setminus \{0\}$. Wir zeigen, R ist ganz abgeschlossen in L . Angenommen es gäbe $x = r/s$ in $\mathcal{O}_L \setminus R$ mit $r \in R, s \in S$. Wir zeigen einen Widerspruch.

2) Wählt man x mit $|s|$ minimal, ist $s = l$ notwendig prim in \mathbb{Z} . Nach §2 ist $0 \neq [r] \in R/lR$ nilpotent. Daraus folgt $l = p$, denn $R/lR = \mathbb{F}_l[X]/\overline{\Phi}_{p^n}(X)$ ist reduziert für primes $l \neq p$. Beachte $\overline{\Phi}(X) | X^{p^n} - 1$ und $X^{p^n} - 1$ ist separabel im Fall $l \neq p$. Benutze den Appendix von §10!

3) Es folgt $l = p$. Insbesondere liegt x nicht in der Lokalisierung $R_{(p)}$ von R nach $\mathbb{Z} \setminus (p)$. $R_{(p)}$ wäre somit nicht ganz abgeschlossen in L . Ein Widerspruch! Nach Schritt 4) ist nämlich $R_{(p)}$ noethersch lokal mit einem maximalen Ideal I , das ein Hauptideal ist

$$I = (1 - \zeta_{p^n}) .$$

Somit ist $R_{(p)}$ ein diskreter Bewertungsring (Lemma 35.1), insbesondere also ganz abgeschlossen in seinem Quotientenkörper. Der Widerspruch zeigt daher $R = \mathcal{O}_L$.

4) Es gilt $R/pR = R_{(p)}/pR_{(p)}$ (dies gilt für \mathbb{Z} und R ist frei als \mathbb{Z} -Modul). Die maximalen Ideale in $R_{(p)}$ entsprechen den Primidealen von R über pR respektive den Primidealen von $R/pR = \mathbb{F}_p[X]/\overline{\Phi}_{p^n}(X)$. In $\mathbb{F}_p[X]$ gilt

$$\overline{\Phi}(X) \cdot (X^{p^{n-1}} - 1) = (X^{p^n} - 1) .$$

Die Variablensubstitution $X = Y + 1$ und der kleine Fermat liefern daher

$$R/pR \cong \mathbb{F}_p[Y]/(Y^{(p-1)p^{n-1}}) .$$

Insbesondere ist $(R/pR)_{red} \cong \mathbb{F}_p[Y]/(Y) = \mathbb{F}_p$ ein Körper. Somit ist R/pR ein lokaler Ring. Sein maximales Ideal wird von $Y = [\zeta_{p^n}] - 1$ erzeugt. Folglich ist $R_{(p)}$ ein lokaler Ring mit dem maximalem Ideal $I = (\zeta_{p^n} - 1, p)$. Aber $N(\zeta_{p^n} - 1) = p$ wegen $\Phi_{p^n}(Y + 1) = Y^{(p-1)p^{n-1}} + \dots + p$. Daraus folgt $p = (\zeta_{p^n} - 1) \cdot \prod_{\sigma \neq 1} \sigma(\zeta_{p^n} - 1) \in (\zeta_{p^n} - 1)$, also $I = (1 - \zeta_{p^n})$. Q.e.d.

Korollar 41.2. *Für die Verzweigungszahlen der Erweiterung $\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}$ gilt:*

(i) $e_l = 1$ für Primzahlen $l \neq p$.

(ii) $e_l = [\mathbb{Q}(\zeta_{p^n}) : \mathbb{Q}]$ für $l = p$.

Somit $f_p = g_p = 1$ und $p \cdot R = (N(\zeta_{p^n} - 1)) = P^{e_P}$. Das eindeutig bestimmte Primideal P über p ist das Hauptideal

$$P = (1 - \zeta_{p^n}) .$$

Komplettierungen

42 Vervollständigung

Gegeben sei ein projektives System von abelschen Gruppen (Ring, R -Modul), also ein System A_0, A_1, \dots von abelschen Gruppen (kommutative Ring, R -Modul etc.) mit (Ring, R -Modul) Homomorphismen

$$\pi_j : A_j \rightarrow A_{j-1} .$$

Sei $\theta : \prod_j A_j \rightarrow \prod_j A_j$ der Homomorphismus

$$\theta(x_0, x_1, \dots, x_n, \dots) = (\pi_1(x_1), \pi_2(x_2), \dots, \pi_{n+1}(x_{n+1}), \dots) .$$

Definition: Der projektive Limes $\lim_{\leftarrow} A_j$ ist $\text{Kern}(1 - \theta) \subset \prod_j A_j$. Elemente in $\lim_{\leftarrow} A_n$ haben die Form (a_0, a_1, a_2, \dots) mit $\pi_j(a_j) = a_{j-1}$ für alle $j \geq 1$. Der Kokern $\text{Kokern}(1 - \theta)$ wird mit $\lim_{\leftarrow}^1 A_j$ bezeichnet.

Für kurze exakte Sequenzen mit kommutativen Quadraten

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_j & \longrightarrow & B_j & \longrightarrow & C_j & \longrightarrow & 0 \\ & & \pi_j \downarrow & & \pi_j \downarrow & & \pi_j \downarrow & & \\ 0 & \longrightarrow & A_{j-1} & \longrightarrow & B_{j-1} & \longrightarrow & C_{j-1} & \longrightarrow & 0 \end{array}$$

liefert die Kern-Kokern Sequenz eine 6-Term exakte Sequenz zwischen den projektiven und höheren projektiven Limiten der Gruppen. Man erhält sogar kurze exakte Sequenzen

$$0 \rightarrow \lim_{\leftarrow} A_j \rightarrow \lim_{\leftarrow} B_j \rightarrow \lim_{\leftarrow} C_j \rightarrow 0 ,$$

wenn (fast) alle $\pi_j : A_j \rightarrow A_{j-1}$ surjektiv sind. Dann ist $\text{Kokern}(1 - \theta_A) = 0$.

Bemerkung: Wenn alle π_j Isomorphismen sind für $j > n$, dann definiert die Projektion $(a_0, a_1, \dots) \mapsto a_n$ einen Isomorphismus $(\lim_{\leftarrow} A_j) \cong A_n$.

Der Ringfall: Sei R ein filtrierter Ring. Sei $R = I_0 \supseteq I_1 \supseteq I_2 \supseteq \dots$ die zugehörige Filtration durch Ideale I_j mit der Eigenschaft $I_i \cdot I_j \subset I_{i+j}$. Man hat dann Ringhomomorphismen $\pi_j : (R/I_j) \rightarrow (R/I_{j-1})$ und dies definiert

den projektiven Limes $\hat{R} = \varprojlim (R/I_j)$ als Ring. Man hat einen Ringhomomorphismus

$$i: R \rightarrow \hat{R} = \varprojlim (R/I_j)$$

definiert durch $i(x) = ([x], [x], [x], \dots)$. Analog definiert man den projektiven Limes $\hat{M} = \varprojlim M/M_j$ eines gefilterten R -Moduls M . Die Abbildung $i: M \rightarrow \hat{M}$ ist im allgemeinen weder injektiv noch surjektiv. Ihr Kern wird beschrieben durch folgende exakte Sequenz

$$0 \rightarrow \bigcap_{\nu=0}^{\infty} M_{\nu} \rightarrow M \rightarrow \hat{M} \quad .$$

Definition: Ist $i: R \rightarrow \hat{R}$ bijektiv, dann heißt R vollständig.

Begründung: Sei $q > 1$. Dann ist $d(r, r') = q^{-\max\{j \mid r' - r \in I_j\}}$ eine Pseudometrik auf R . Es gilt die scharfe Dreiecksungleichung

$$d(r, r'') \leq \max(d(r, r'), d(r', r'')) \quad .$$

Die offenen Kugeln um Null sind gerade die I_j . Gilt $\bigcap_j I_j = 0$, dann ist $d(\cdot, \cdot)$ eine Metrik. Das heißt $d(r, r') = 0 \iff r = r'$ sowie $R \hookrightarrow \hat{R}$. Für $x = (x_0, x_1, \dots) \in \hat{R}$ sei $j = v(x)$ maximal mit $x_i = 0$ (in R/I_i) für $i \leq j$. Dann ist $\hat{d}(x, x') = q^{-v(x'-x)}$ eine Fortsetzung der Metrik d von R auf \hat{R} . Addition und Multiplikation sind stetige Abbildungen auf \hat{R} bzw. R . Der Ring R liegt dicht in \hat{R} : Für $x \in \hat{R}$ und $\varepsilon > 0$ gibt es $r \in R$ mit $d(x, i(r)) < \varepsilon$. Der metrische Ring (\hat{R}, \hat{d}) ist die (isomorph zu der) Cauchy-Vervollständigung des metrischen Rings (R, d) (= metrische Ring der Cauchyfolgen von R modulo dem Ideal der Nullfolgen von R).

[Beachte: Für $x = (x_0, \dots)$ und Repräsentanten $y_j \in R$ von $x_j \in R/I_j$ ist y_j eine Cauchyfolge in R : $d(y_i, y_j) \leq q^{-\max(i, j)}$. Ist umgekehrt y'_j eine Cauchyfolge in R , dann ist $x_j := y'_j \bmod I_j$ unabhängig von i für $i \gg 0$. Dies definiert ein Element $x = (x_0, x_1, \dots) \in \hat{R}$. Ändert man (y'_i) ab um eine Nullfolge, ändert dies nichts am Wert $x \in \hat{R}$ und $y'_j - y_j$ ist eine Nullfolge.]

Man kann auch Reihenkonvergenz untersuchen. Auf Grund der scharfen Dreiecksungleichung gilt sogar

Lemma 42.1. *Für eine Folge y_n in \hat{R} sind äquivalent: 1) y_n ist eine Nullfolge. 2) Die Reihe $\sum_{n=0}^{\infty} y_n$ konvergiert.*

Äquivalente Filtrationen: Zwei Filtrationen M_j, M'_j auf einem R -Modul heißen äquivalent, wenn für ein geeignetes festes $k \in \mathbb{N}$ für alle $j \in \mathbb{N}$ gilt

$$M_j \subset M'_{j-k} \quad , \quad M'_j \subset M_{j-k} .$$

Beispiel: Seien M, R noethersch und sei $N \subset M$ ein R -Untermodul. Nach Artin-Rees ist die I -adische Filtration $N_j = I^j \cdot N$ auf N äquivalent zu der von der I -adischen Filtration auf M induzierten Filtration $N'_j = N \cap (I^j \cdot M)$.

Äquivalente Filtrationen definieren dieselbe Topologie auf M und haben denselben projektiven Limes: Die Abbildungen

$$(M/M'_j) \twoheadrightarrow (M/M_{n-k}) \quad \text{und} \quad (M/M_{n-k}) \twoheadrightarrow (M/M_{n-2k})$$

induzieren Abbildungen der projektiven Limiten

$$\varprojlim (M/M'_j) \rightarrow \varprojlim (M/M_{j-k}) \quad , \quad \varprojlim (M/M_{j-k}) \rightarrow \varprojlim (M/M'_{j-2k}) ,$$

deren Zusammensetzung die Identität von \hat{M}' ist. Sie wird induziert von

$$(x_0, \dots, x_{2k}, x_{2k+1}, \dots) \mapsto (x_{2k} \bmod M'_0, \dots) = (x_0, x_1, \dots) .$$

Ditto in der umgekehrten Richtung.

Wichtige Beispiele: Sei $R = \mathbb{Z}$ und $I_j = p^j \cdot \mathbb{Z}$, dann bezeichnet man die zugehörige Kompletierung von \mathbb{Z} als p -adische Kompletierung und $\hat{\mathbb{Z}}$ als den Ring der p -adischen ganzen Zahlen \mathbb{Z}_p .

Ist $R = \mathbb{Z}$ und $I_j = (j!)$, dann bezeichnet man die zugehörige Kompletierung als den Ring \mathbb{Z}_{fin} der ganzen Adele. Es gilt

$$\mathbb{Z}_{fin} \cong \prod_{p \text{ prim}} \mathbb{Z}_p .$$

Die Lokalisierung von \mathbb{Z}_{fin} nach $\mathbb{Z} \setminus 0$ ist der Ring der endlichen Adele \mathbb{A}_{fin} . Der Ring $\mathbb{A} = \mathbb{R} \times \mathbb{A}_{fin}$ heißt Ring der Adele. Dieser Ring spielt eine fundamentale Rolle in der algebraischen Zahlentheorie.

π -adische Entwicklungen: Sei $I = (\pi)$ ein Hauptideal und sei π kein Nullteiler von R . Sei $\mathcal{R} \subset R$ ein Repräsentantensystem von R/I . Dann gibt es für $a \in R$ ein $\delta^0 \in \mathcal{R}$ mit $a - \delta^0 = a_1 \cdot \pi$. Da π kein Nullteiler ist, ist $a_1 \in R$ durch a eindeutig bestimmt. Somit gilt $a_1 = \delta^1 + a_2 \cdot \pi$ usw. Rekursiv enthält man eine eindeutige π -adische Entwicklung

$$a = \delta^0 + \delta^1 \cdot \pi + \delta^2 \cdot \pi^2 + \dots + \delta^n \cdot \pi^n + (\pi^{n+1}) \quad , \quad (\delta^i \in \mathcal{R}) .$$

Beispiel: Im Fall $R = \mathbb{Z}_p$ kann man $\mathcal{R} = \{0, \dots, p-1\}$ wählen und $\pi = p$. Wir werden im nächsten Kapitel zeigen, daß \mathbb{Z}_p die $(p-1)$ -ten Einheitswurzeln enthält. Zusammen mit Null bildet dies ein multiplikatives Repräsentantensystem \mathcal{R} von $\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$ in \mathbb{Z}_p .

Trivialerweise folgt durch Rechnen mit den π -adischen Entwicklungen

Lemma 42.2. *Ist $R/(\pi)$ nullteilerfrei und $\bigcap_{i=0}^{\infty} (\pi^i) = \{0\}$, dann ist auch R nullteilerfrei.*

Insbesondere ist also der Ring \mathbb{Z}_p der p -adischen Zahlen nullteilerfrei und sein Quotientenkörper ist der Körper \mathbb{Q}_p der sogenannten p -adischen Zahlen.

Ringe der Charakteristik p

43 Perfekte Ringe

In einem Ring R der Charakteristik p gilt $p \cdot R = 0$. Der Frobenius $Frob_R : R \rightarrow R$ ist i.a. weder injektiv noch surjektiv. Ist $Frob_R$ bijektiv (surjektiv), heißt R perfekt (semiperfekt).

Lemma: Für einen Ring R der Charakteristik p gibt es einen perfekten Ring $P(R)$ – die Perfektionierung von R – und einen Ringhomomorphismus $\rho : P(R) \rightarrow R$, so daß $(P(R), \rho)$ in folgendem Sinn universell ist:

Jeder Ringhomomorphismus φ eines perfekten Rings R' nach R faktorisiert eindeutig über ρ

$$\begin{array}{ccc} R' & \xrightarrow{\varphi} & R \\ & \searrow \exists! \psi & \uparrow \rho \\ & & P(R) \end{array} .$$

Zusatz: Ist $Frob_R$ surjektiv (injektiv), dann ist ρ surjektiv (injektiv). Ist R perfekt, dann ist ρ ein Isomorphismus.

Beweis: Sei $P(R)$

$$P(R) = \lim (R \xleftarrow{Frob} R \xleftarrow{Frob} R \xleftarrow{Frob} R \xleftarrow{Frob} R \cdots) .$$

der projektive Limes bezüglich des Frobenius Homomorphismus $Frob_R$. Die Elemente von $P(R)$ sind somit Folgen $(x_n)_{n \geq 0}$ von Ringelementen $x_n \in R$ mit der Eigenschaft $(x_n)^p = x_{n-1}$. $P(R)$ ist ein Ring mit komponentenweiser Addition und Multiplikation.

$P(R)$ ist ein Ring der Charakteristik p . Sein Frobenius homomorphismus

$$Frob_{P(R)}((x_n)_{n \geq 0}) = (x_{n-1})_{n \geq 0} \quad (\text{mit } x_{-1} := x_0^p)$$

ist bijektiv mit $Frob_{P(R)}^{-1}((x_n)_{n \geq 0}) = (x_{n+1})_{n \geq 0}$ (voilà !). Also ist $P(R)$ perfekt.

Setze nun $\rho((x_n)_{n \geq 0}) := x_0$. Offensichtlich ist ρ surjektiv, wenn $Frob_R$ surjektiv ist (wähle $x_1 \in R$ mit $Frob_R(x_1) = x_0$ usw.). Ist $Frob_R$ injektiv, ist auch ρ injektiv (aus $x_0 = 0$ folgt $x_1 = 0$ etc.).

Die Konstruktion von $P(R)$ ist funktoriell: Ein Ringhomomorphismus $\varphi : R' \rightarrow R$ induziert auf offensichtliche Weise ein kommutatives Diagramm

$$\begin{array}{ccc} R' & \xrightarrow{\varphi} & R \\ \uparrow \rho & & \uparrow \rho \\ P(R') & \xrightarrow{P(\varphi)} & P(R) \end{array}$$

via $(x_n)_{n \geq 0} \mapsto (\varphi(x_n))_{n \geq 0}$. Ist R' perfekt, gilt $\rho : P(R') = R'$. Dies zeigt die universelle Eigenschaft. Beachte $\psi(x)_n = \rho(\text{Frob}_{P(R)}^{-n} \psi(x)) = \rho(\psi(\text{Frob}_{R'}^{-n}(x))) = \varphi(\text{Frob}_{R'}^{-n}(x))$. Also ist ψ eindeutig bestimmt.

44 Der Teichmüller Lift

In diesem Paragraph sei p eine Primzahl und A ein kommutativer Ring mit 1, und sei I-vollständig

$$A = \varprojlim A/I^n$$

für ein Ideal I mit der Eigenschaft $p \in I$. Dann ist A/I ein Ring der Charakteristik p . Für $a \in A$ bezeichne \bar{a} die Restklasse in A/I .

Betrachte: $Z_I(A) = \{x = (x_0, x_1, \dots) \mid x_n \in A \text{ mit } (x_n)^p = x_{n-1} \text{ mod } I\}$. Offensichtlich definiert diesen einen Ring. Im Fall $I = (p)$ schreiben wir $Z(A)$ für diesen Ring anstatt $Z_I(A)$.

Ersetzt man die Kongruenzbedingungen $(x_n)^p = x_{n-1} \text{ mod } I$ in der Definition von $Z_I(A)$ durch die rigidener Bedingungen $(x_n)^p = x_{n-1}$ erhält man a priori keinen Ring mehr. Dies definiert erst einmal nur einen multiplikativen Untermonoid $P(A) \xrightarrow{i} Z_I(A)$

$$P(A) = \{x = (x_0, x_1, \dots) \mid x_n \in A \text{ mit } (x_n)^p = x_{n-1}\}.$$

Ziel dieses Abschnitts ist es zu zeigen, daß man $(P(A), \cdot)$ dennoch als den multiplikativen Monoid einer Ringstruktur auf $P(A)$ auffassen kann. Dazu genügt es zu zeigen (siehe Satz 44.3), daß die Reduktionsabbildung $A \rightarrow A/I$ einen Monoidisomorphismus $P(A) \rightarrow P(A/I)$ induziert. Denn nun ist $A' = A/I$ ein Ring der Charakteristik p . Und für Ringe A' der Charakteristik p ist $P(A')$ in natürlicher Weise ein Ring. $P(A') = Z(A')$ ist dann nämlich

die Perfektionierung des Rings A' , genauer $(P(A'), \cdot)$ ist der multiplikative Monoid dieses Ringes.

Wie gesagt gilt per Definition

$$Z(A/I) = P(A/I)$$

und Reduktion modulo I liefert das kommutative Diagramm

$$\begin{array}{ccc} Z_I(A) & \xleftarrow{i} & P(A) \\ \pi_Z \downarrow & & \downarrow \pi \\ Z_I(A/I) & \xlongequal{\quad} & P(A/p) \end{array}$$

für $i : (x_0, x_1, \dots) \mapsto (x_0, x_1, \dots)$, wegen $\lim_n (x_{n+i})^{p^n} = \lim_n (x_i) = x_i$.

Lemma 44.1. *Für $x \in Z_I(A)$ existiert in A der Limes*

$$[x]_0 = \lim_{n \rightarrow \infty} (x_n)^{p^n} .$$

Beweis: $[x]_0 = x_0 + (x_1^p - x_0) + (x_2^{p^2} - x_1^p) + \dots$ konvergiert, denn der kleine Fermat liefert

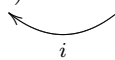
$$\boxed{x'_i = x_i \pmod{I^r} \implies (x'_i)^p = (x_i)^p \pmod{I^{r+1}}} .$$

Für $x'_i = (x_{i+1})^p$ ist daher $(x_{i+1}^{p^{i+1}} - x_i^{p^i}) = (x'_i)^{p^i} - (x_i)^{p^i}$ in I^i . Q.e.d.

Bemerkung: Analog existiert dann

$$[x]_i = \lim_{n \rightarrow \infty} (x_{n+i})^{p^n}$$

(durch Verschieben). Dies definiert einen Monoidhomomorphismus, die surjektive Retraktion $[\cdot] : x = (x_0, x_1, \dots) \mapsto [x] = ([x]_0, [x]_1, \dots)$ mit

$$Z_I(A) \xrightarrow{[\cdot]} P(A) \quad , \quad [\cdot] \circ i = id_{P(A)} .$$


Lemma 44.2. *Die Limiten $[x]_i$ hängen nur ab von $(x_n \pmod{I})_{n \geq 0}$.*

Beweis: $x_n = x'_n \bmod I \implies (x_n)^{p^n} = (x'_n)^{p^n} \bmod I^{n+1} \implies [x]_0 = [x']_0$.
Es genügt obdA $i = 0$. Q.e.d.

Wegen Lemma 44.2 faktorisiert die Retraktion $[\cdot]$ über die Reduktion π_Z modulo I . Dabei ist die Reduktion $\pi_Z : Z_I(A) \rightarrow Z_I(A/I)$ definiert durch $\pi_Z(x_0, x_1, \dots) = (\bar{x}_0, \bar{x}_1, \dots)$. Diese Faktorisierung definiert eine Monoidabbildung, den Teichmüller-Lift $\psi : P(A/I) \rightarrow P(A)$

$$\begin{array}{ccc} Z_I(A) & \xrightarrow{[\cdot]} & P(A) \\ \pi_Z \downarrow & & \uparrow \exists! \psi \\ Z_I(A/I) & \xlongequal{\quad} & P(A/I) \end{array}$$

- 1) ψ ist surjektiv, da die Retraktion surjektiv ist.
- 2) ψ ist injektiv wegen

$$\pi \circ \psi = id_{P(A/I)} \quad \text{für} \quad \pi : P(A) \rightarrow P(A/I) .$$

Nämlich $(\pi \circ \psi)((\bar{x}_n)_{n \geq 0}) = \pi((\lim_i (x_{n+i})_{n \geq 0})^{p^i}) = \lim_i ((\bar{x}_{n+i})_{n \geq 0})^{p^i} = (\bar{x}_n)_{n \geq 0}$.

Satz 44.3. *Sei A I -vollständig für ein Ideal I mit $p \in I$. Dann sind der Teichmüller Lift ψ und die Reduktion $\pi : P(A) \rightarrow P(A/I)$ modulo I invers zueinander. π und ψ definieren Bijektionen*

$$\boxed{P(A) \cong P(A/I)} .$$

Da A/I Charakteristik p besitzt ist $P(A/I)$ ein Ring (die Perfektionierung von A/I). Obige Bijektion induziert auf $P(A)$ wie bereits erläutert eine natürliche Ringstruktur, welche die gegebene multiplikative Monoidstruktur induziert. Der so definierte Ring $P(A)$ ist funktoriell bezüglich (A, I) .

Ist A/I perfekt, dann gilt $P(A/I) = A/I$ und es folgt

Korollar 44.4. *Ist der Restklassenring A/I sogar perfekt, dann gibt es einen Isomorphismus multiplikativer Monoide*

$$\boxed{\psi : (A/I, \cdot) \cong (P(A), \cdot)} .$$

Die Zuordnung, welche jeder Restklasse $\bar{x} \in A/I$ die nullte Komponente $[\bar{x}] = \psi(\bar{x})_0 \in A$ zuordnet, ist multiplikativ

$$[\bar{x} \cdot \bar{y}] = [\bar{x}] \cdot [\bar{y}]$$

und erfüllt

$$[\bar{x}] \equiv \bar{x} \text{ modulo } I .$$

Man nennt $[\bar{x}]$ den Teichmüller-Repräsentant, und $\mathcal{R} = \{[\bar{x}] \mid \bar{x} \in A/I\}$ das multiplikative Restklassensystem von A/I in A .

45 Einige Beispiele

Beispiel 1): $P(\mathbb{F}_q) = \mathbb{F}_q$.

Beispiel 2): $P(\mathbb{F}_q[t]) = \mathbb{F}_q$.

Beispiel 3): $P(\mathbb{Z}_p) \cong P(\mathbb{Z}_p/p\mathbb{Z}_p) = P(\mathbb{F}_p) = \mathbb{F}_q$ ist ein multiplikativer Monoid in \mathbb{Z}_p . Somit sind die $p - 1$ -ten Einheitswurzeln in \mathbb{Z}_p^* . Es gilt

$$\mathbb{Z}_p^* = \mu_{p-1} \times (1 + p\mathbb{Z}_p) .$$

Beachte $(1 + px)^{-1} = 1 - px + p^2x^2 \dots$ konvergiert.

Wie in Beispiel 3 zeigt man allgemeiner

Lemma 45.1. *Ist A/I perfekt, dann gilt $A^* \cong (A/I)^* \times (1 + I)$.*

Beispiel 4): Sei $A = \mathcal{O}_{\mathbb{R}_p}$ die p -adische Kompletierung (nicht die Bewertungskompletierung) des zyklotomischen Rings¹⁶ aller p -Potenzeinheitswurzeln ζ_{p^n} über \mathbb{Z}_p . A erfüllt unsere Annahmen und

$$\boxed{\zeta = (1, \zeta_p, \zeta_{p^2}, \dots) \in P(A)}$$

für geeignete primitive p^n -te Einheitswurzeln ζ_{p^n} . Identifiziert man $P(A) = P(A/p)$ und betrachtet anstelle von ζ das Element

$$\boxed{\bar{\zeta} = (1, \bar{\zeta}_p, \bar{\zeta}_{p^2}, \dots) \in P(A/p)},$$

so ist in dem Ring $P(A/p)$ das Element

$$\bar{\zeta} - 1 = (0, \bar{\pi}_1, \bar{\pi}_2, \dots) \in P(A/pA)$$

erklärt. Es wird representiert von den Elementen $\pi_n = \zeta_{p^n} - 1 \in A$ mit der p -adischen Bewertung $v(\pi_n) = \frac{p^{1-n}}{p-1}$. Offensichtlich ist $\bar{\zeta} - 1$ ein nichttriviales Element im Kern

$$\bar{\zeta} - 1 \in \text{Kern}(\rho : P(A/p) \rightarrow A/p) .$$

¹⁶Es gilt $\Phi_{p^n}(Y + 1) \equiv Y^{(p-1)p^{n-1}} \pmod{p}$. Für $\mathcal{O} = \mathbb{Z}[\zeta_{p^n}] = \mathbb{Z}[X]/\Phi_{p^n}(X)$ folgt $\mathcal{O}/p\mathcal{O} \cong \mathbb{F}_p[Y]/Y^{(p-1)p^{n-1}}$. Also $A/pA = \mathbb{F}_p[t^{p^{-\infty}}]/(t^{p-1})$ für $A = \mathcal{O}_{\mathbb{R}_p}$. Notation: $\mathbb{F}_p[t^{p^{-\infty}}] := \mathbb{F}_p[t, t^{p^{-1}}, t^{p^{-2}}, \dots]$ und $t = Y^{1/(p-1)}$.

46 Der Kern der Perfektionierung

Sei A und die Bezeichnungen wie im letzten Paragraph. A/I ist ein Ring der Charakteristik p . Der Einfachheit halber sei $p \neq 2$. Betrachte die Perfektionierung

$$\rho : P(A/I) \rightarrow A/I .$$

Der Kern $K = \rho^{-1}(0_{A/I})$ kann mit $1 + K = \rho^{-1}(1_{A/I})$ identifiziert werden.

Einheitswurzeln: Liegt $(\bar{\varepsilon} - 1)$ in K , dann auch $\bar{\varepsilon}^p - 1$. Elemente $\bar{\varepsilon} = (\bar{\varepsilon}_n)_{n \geq 0}$ in $1 + K$ erfüllen $\bar{\varepsilon}_n^{p^n} = \bar{\varepsilon}_{n-1}^{p^{n-1}} = \dots = \bar{\varepsilon}_1^p = 1$. Die $\bar{\varepsilon}_n$ sind p^n -te Einheitswurzeln in A/I . Betrachte $\psi(\bar{\varepsilon})$ in $P(A)$. Es gilt $\psi(\bar{\varepsilon})_0 = \lim_n \varepsilon_n^{p^n} = 1$. Die Komponenten $[\bar{\varepsilon}]_n \in A$ von $\psi(\bar{\varepsilon})$ sind daher p^n -te Einheitswurzeln des Quotientenkörpers $Quot(A)$, falls A nullteilerfrei ist. Ist $\bar{\varepsilon} \neq 1$ in $P(A/I)$, dann ist $\psi(\bar{\varepsilon}) \neq 1$ in $P(A)$. Somit erfüllt eine geeignete Potenz von $\psi(\bar{\varepsilon})$ außerdem $[\bar{\varepsilon}]_0 = 1, [\bar{\varepsilon}]_1 \neq 1$. Dann sind alle $[\bar{\varepsilon}]_n = \zeta_{p^n}$ primitive n -te Einheitswurzeln in A . Fixiere ein solches $\bar{\varepsilon} = \bar{\zeta}$, welches auch im Kern von ρ liegt.

Folgerung 46.1. *Sei A nullteilerfrei. Dann ist $P(A/I)$ nullteilerfrei und es gilt genau dann*

$$Kern(\rho : P(A/I) \rightarrow A/I) \neq 0 ,$$

wenn A alle primitiven p -Potenz-Einheitswurzeln enthält (d.h A enthält die I -adische Vervollständigung $\mathcal{O}_{\mathbb{R}_p}$ des p^∞ -zyklotomischen Rings !).

Zusatz: *Im letzteren Fall gilt*

$$Kern(\rho) = (1 - \bar{\zeta}) \cdot P(A/I) \quad , \quad \bigcap_{i=0}^{\infty} (1 - \bar{\zeta})^i = \{0\}$$

und $Bild(\rho)$ enthält $\mathbb{F}_p[\bar{\zeta}_p, \bar{\zeta}_{p^2}, \dots]$ wegen $\rho(Frob^{-n}(\bar{\zeta})) = \bar{\zeta}_{p^n}$.

Beweis (des Zusatzes): Ist A nullteilerfrei, dann ist es auch der Monoid $P(A)$. Wegen $P(A/I) \cong P(A)$ ist daher die multiplikative Gruppe des Rings $P(A/I)$ nullteilerfrei. Für $\bar{x} \in (1 - \bar{\zeta})^{p^n}$ gilt $\bar{x}_0 = \bar{x}_1 = \dots = \bar{x}_{n-1} = 0$. Somit ist der Durchschnitt aller Potenzen des Ideals $(1 - \bar{\zeta})$ gleich Null.

Für $\bar{\varepsilon} \in 1 + K$ ist $\bar{\varepsilon} \in (\bar{\zeta} - 1) \cdot P(A/I)$ zu zeigen. Es gilt $\bar{\varepsilon} = (1, \bar{\varepsilon}_p, \bar{\varepsilon}_{p^2}, \dots)$ für p^n -te Einheitswurzeln ε_{p^n} . Somit existieren $n_i \in \mathbb{Z}/p^i\mathbb{Z}$ mit

$$\varepsilon_{p^i} = (\zeta_{p^i})^{n_i} .$$

Behauptung:

$$(\bar{\zeta} - 1) = (\bar{\varepsilon} - 1) \cdot (n_1, \sum_{\nu=0}^{n_1-1} (\bar{\zeta}_p)^\nu, \sum_{\nu=0}^{n_2-1} (\bar{\zeta}_p^2)^\nu, \dots)$$

liegt im Hauptideal $(\bar{\zeta} - 1) \cdot P(A/I)$.

Beweis: Wir wissen $n_{r+1} = n_r \bmod p^r$ und müssen zeigen

$$\text{Frob} \left(\sum_{\nu=0}^{n_{r+1}} (\bar{\zeta}_{p^{r+1}})^\nu \right) = \sum_{\nu=0}^{n_r} (\bar{\zeta}_{p^r})^\nu$$

modulo I . Dazu genügt wegen $p \in I$

Lemma 46.2. Für $r \geq 1$ und $n = m \bmod p^r$ gilt $\sum_{\nu=0}^n \zeta_{p^r}^\nu = \sum_{\nu=0}^m \zeta_{p^r}^\nu \bmod p$.

Beweis: ObdA $m - n = p^r \cdot k \geq 0$. Zeige also $\sum_{\nu=n+1}^m \zeta_{p^r}^\nu = 0 \bmod p$ oder $\zeta_{p^r}^{n+1} \cdot \sum_{\nu=0}^{kp^r-1} \zeta_{p^r}^\nu = 0 \bmod p$. Dazu genügt $\sum_{\nu=0}^{p^r-1} \zeta_{p^r}^\nu = 0 \bmod p$. Dies folgt aus $\prod_{\nu=0}^{p^r-1} (X - \zeta_{p^r}^\nu) = X^{p^r} - 1$ (betrachte den Term X^{p^r-1}).

Korollar 46.3. Für $\bar{x} = (\bar{x}_0, \bar{x}_1, \dots) \in P(A/I)$ sind äquivalent

- (1) Es gilt $\bar{x}_i = 0$ für alle $i = 0, \dots, n$.
- (2) Es gilt $\bar{x} \in (1 - \bar{\zeta})^{p^n} \cdot P(A/I)$.

Beweis: Es gilt

$$(1 - \bar{\zeta})^{p^n} = (0, \dots, 0, 1 - \bar{\zeta}_p, 1 - \bar{\zeta}_{p^2}, \dots) \in P(A/I).$$

Somit überträgt sich der Beweis von Folgerung 46.1.

47 * Bewertungen

Sei A I -vollständig mit $p \in I$, nullteilerfrei und habe eine Bewertung $v : A \rightarrow \mathbb{R} \cup \{\infty\}$, für welche $e^{-v(\cdot)}$ stetig ist bezüglich der I -adischen Topologie, z.B.

wenn gilt $v(p) = 1$ im Fall $I = (p)$. Wir setzen dann für $x = (\bar{x}_0, \bar{x}_1, \dots) \neq 0$ aus $P(A/p)$ mit Teichmüller Lift $\psi(x) = (x_0, x_1, \dots)$

$$\bar{v}\left((\bar{x}_0, \bar{x}_1, \dots)\right) = v(x_0) .$$

Dies ist wohldefiniert. Sind $a_n \in A$ irgendwelche Repräsentanten der $\bar{x}_n \in A/I$, dann gilt wegen der Stetigkeit

$$\bar{v}(a_0 \bmod I, a_1 \bmod I, \dots) = v\left(\lim_{n \rightarrow \infty} (a_n)^{p^n}\right) = \lim_{n \rightarrow \infty} p^n \cdot v(a_n) .$$

Es gilt weiterhin

$$\begin{aligned} \bar{v}(x \cdot y) &= \bar{v}(x) + \bar{v}(y) \\ \bar{v}(x + y) &\geq \min(\bar{v}(x), \bar{v}(y)) , \end{aligned}$$

wenn man formal $\bar{v}(0) = \infty$ setzt.

Korollar 47.1. *Sei A I -vollständig mit $p \in I$, nullteilerfrei und habe eine Bewertung $v : A \rightarrow \mathbb{R} \cup \{\infty\}$, für welche $e^{-v(\cdot)}$ stetig ist bezüglich der I -adischen Topologie, dann ist $P(A/p)$ ein bewerteter perfekter Ring.*

Beispiel: Sei $x = (p, p^{1/p}, p^{1/p^2}, \dots)$ in $P(A)$ bzw. $x = (0 \bmod p, p^{1/p} \bmod p, \dots)$ in $P(A/p)$ für $A = \mathcal{O}_{\mathbb{C}_p}$ mit $\bar{v}(x) = 1$. Frage: Liegt $x \in P(A_0)$ für $A_0 = \mathcal{O}_{\mathbb{R}_p}$?

Analog für $\bar{\zeta} - 1 = (0 \bmod p, \zeta_p - 1 \bmod p, \zeta_{p^2} - 1 \bmod p, \dots)$ ist dann

$$\bar{v}(\bar{\zeta} - 1) = p^r \cdot v(\zeta_{p^r} - 1) = \frac{p}{p-1} .$$

Wittringe

48 p -adische Entwicklungen

Ein Ring A heißt p -vollständig, wenn A vollständig ist bezüglich der Kompletterung nach den Potenzen des Ideals $I = (p)$.

Lazardbedingung: Sei A p -vollständig, sei p kein Nullteiler in A und sei $R = A/p$ perfekt.

Unter dieser Bedingung gilt $A/pA = P(A/pA)$, und die Teichmüllerabbildung definiert eine Abbildung $\psi : A/pA \rightarrow P(A)$. Die nullte Komponente $\psi(\bar{a})_0 \in A$ nennt man den Teichmüller Repräsentant $[\bar{a}]$ von \bar{a} in A .

Damit besitzt jedes $a \in A$ eine kanonische Taylorentwicklung

$$a = \delta^0(a) + p \cdot \delta^1(a) + p^2 \cdot \delta^2(a) + \dots$$

mit $\delta^0(a) = \psi(a \bmod p)_0$ (Teichmüller Repräsentant). Dann ist $\delta^0(a) = a \bmod p$. Also $\exists!$ $a_1 \in A$ (p ist kein Nullteiler) mit $a - \delta^0(a) = p \cdot a_1$. Setze $\delta^1(a) = \psi(a_1)_0$ usw. Die Terme $\delta^i(a)$ verhalten sich ähnlich wie Ableitungen¹⁷.

Folgerung: a ist somit eindeutig eine Folge zugeordnet

$$(\alpha_0, \alpha_1, \alpha_2, \dots) \in \prod_{i=0}^{\infty} A/p$$

mit $\alpha_i = a_i \bmod p$ und $\delta^i(a) = \psi(\alpha_i)$.

Rechnet man in dem Restklassenring $A/p^{n+1}A$, dann bricht die Taylorentwicklung obdA an der $n+1$ -sten Stelle ab. Nach Lemma 44.1 (Beweis) gilt modulo $p^{n+1}A$

$$\begin{aligned} \delta^0(a) &\equiv \text{Lift}(\text{Frob}^{-n}(\alpha_0))^{p^n} \\ p \cdot \delta^1(a) &\equiv p \cdot \text{Lift}(\text{Frob}^{-n+1}(\alpha_1))^{p^{n-1}} \\ &\dots \\ p^n \cdot \delta^n(a) &\equiv p^n \cdot \text{Lift}(\alpha_n) . \end{aligned}$$

$\text{Lift}(\alpha)$ steht für ‘irgendein Urbild von $\alpha \in A/pA$ ’ in A . Mit den Abkürzungen $X_0 = \text{Lift}(\text{Frob}^{-n}(\alpha_0))$, $X_1 = \text{Lift}(\text{Frob}^{-n+1}(\alpha_1))$, ..., $X_n = \text{Lift}(\alpha_n)$ für diese Elemente aus A erhält man

$$a \equiv X_0^{p^n} + p \cdot X_1^{p^{n-1}} + \dots + p^n \cdot X_n \pmod{p^{n+1}A} .$$

¹⁷z.B. $\delta^1(a+b) = \delta^1(a) + \delta^1(b) + (\delta^0(a)^p + \delta^0(b)^p - (\delta^0(a) + \delta^0(b))^p)/p$ und $\delta^1(a \cdot b) = \delta^0(a)\delta^1(b) + \delta^1(a)\delta^0(b) + p\delta^1(a)\delta^1(b)$

Beachte: $p^i \cdot X_i^{p^{n-i}}$ modulo $p^{n+1}A$ hängt nur ab von der Restklasse X_i mod pA .

49 Rechnen mit Übertrag

Seien X_0, X_1, X_2, \dots abzählbar viele Unbestimmte. Setze

$$\begin{aligned} w_0 &= X_0 \\ w_1 &= X_0^p + p \cdot X_1 \\ &\dots \\ w_n &= X_0^{p^n} + p \cdot X_1^{p^{n-1}} + \dots + p^n \cdot X_n. \end{aligned}$$

im Polynomring $\mathbb{Z}[X_0, X_1, \dots]$. Dann gilt

$$\mathbb{Q}[X_0, X_1, \dots, X_n] = \mathbb{Q}[w_0, w_1, \dots, w_n].$$

Etwa $X_1 = (w_1 - w_0^p)/p$ etc. Sind dann Y_0, Y_1, \dots weitere Unbestimmte und \tilde{w}_n die entsprechenden Polynome in den Y_i . Wir schreiben auch $w_i = w_i(X)$ und $\tilde{w}_i = w_i(Y)$. Induktiv findet sofort rekursiv Polynome $U_0, U_1, \dots, V_0, V_1, \dots$ in $\mathbb{Q}[X_0, X_1, \dots, Y_0, Y_1, \dots]$ mit

$$\begin{aligned} w_0(X) + w_0(Y) &= w_0(U) & \text{resp} & & w_0(X) \cdot w_0(Y) &= w_0(V) \\ w_1(X) + w_1(Y) &= w_1(U) & \text{resp} & & w_1(X) \cdot w_1(Y) &= w_1(U) \\ &\dots & & & & \\ w_n(X) + w_n(Y) &= w_n(U) & \text{resp.} & & w_n(X) \cdot w_n(Y) &= w_n(U). \end{aligned}$$

Die Polynome $U_i(X, Y), V_i(X, Y)$ hängen nur von $X_0, \dots, X_i, Y_0, \dots, Y_i$. Die Koeffizienten der Polynome sind a priori rationale Zahlen mit p -Potenzennennern.

Beispiel: $U_0 = X_0 + Y_0, V_0 = X_0 Y_0$ sowie $U_1 = X_1 + Y_1 + (X_0^p + Y_0^p - (X_0 + Y_0)^p)/p$ und $V_1 = X_0 Y_1 + X_1 Y_0 + p X_1 Y_1$, etc.

Lemma 49.1. *Die Polynome $U_i(X, Y), V_i(X, Y)$ sind für alle i ganzzahlig.*

Beweis: Dies ist ziemlich klar, da diese Polynome das Rechnen mit Übertrag (Addition und Multiplikation) in dem Ring

$$A_0 = \mathbb{Z}_p[X_0^{1/p^\infty}, X_1^{1/p^\infty}, \dots, Y_0^{1/p^\infty}, Y_1^{1/p^\infty}, \dots]$$

regulieren (X^{1/p^∞} steht für alle sukzessiven p -Potenz Wurzeln von X ; dies liefert abzählbar viele Elemente). Sei A die p -adische Kompletierung von A_0 . A ist p -vollständig, p ist kein Nullteiler in A , und A/p ist perfekt. Die U_i, V_i ergeben sich daher wie im vorigen Abschnitt als Potenzreihen mit p -adisch ganzen Koeffizienten (in \mathbb{Z}_p). Sie sind die Phantomkomponenten von der Summe bzw. dem Produkt von $\sum_{i=0}^n p^i X_i$ und $\sum_{i=0}^n p^i Y_i$. Beachte $X_i = \psi(X_i)$ und $Y_i = \psi(Y_i)!$ Andererseits sind sie Polynome mit rationalen Koeffizienten, deren Nenner höchsten p -Potenzen sind. Durch Koeffizienten Vergleich folgt, daß alle Koeffizienten ganz sind.

50 Wittringe

Sei A ein beliebiger kommutativer Ring mit 1. Betrachte die Abbildung W

$$\begin{aligned} W(A) = \prod_{i=0}^{\infty} A &\xrightarrow{W} \prod_{i=0}^{\infty} A \\ x = (x_0, x_1, \dots) &\longmapsto (w_0(x), w_1(x), \dots) \end{aligned}$$

welche durch die Polynome $w_i(x_0, x_1, \dots)$ des letzten Paragraphen definiert wird. Erklärt man die Addition und Multiplikation im rechten Produkt komponentenweise, im linken Produkt dagegen durch

$$(x + y)_n := U_n(x_0, \dots, x_n, y_0, \dots, y_n)$$

$$(x \cdot y)_n := V_n(x_0, \dots, x_n, y_0, \dots, y_n),$$

für $n = 0, 1, \dots$, dann wird W ein Ringhomomorphismus. $W(A)$ wird nämlich durch diese Definition zu einem Ring mit $1_{W(A)} = (1, 0, 0, \dots)$, der sogenannte Wittring von A (zur Primzahl p).

Reduktion auf den universellen Fall: Das Assoziativ-, Distributivgesetz etc. genügt es in geeigneten universellen Situationen zu prüfen (Ringe vom Typ des Rings A_0 aus dem letzten Paragraph, nur eventuell mehr Variablen). Für diese Ringe ist die Aussage klar nach §39. Für einen beliebigen Ring A involviert das Nachprüfen der Axiome immer nur endlich viele Elemente des

Rings A . Diese kann man in einen über \mathbb{Z} endlich erzeugten Unterring $B \subset A$ einbetten. B ist ein Quotient eines Polynomrings über \mathbb{Z} . Diesen kann man in einen universellen Ring vom Typ A_0 einbetten und so das Axiom durch Reduktion auf den universellen Fall verifizieren.

Implizit bei dieser Verifikation haben wir folgende Tatsache ausgenutzt

Lemma 50.1. *Ist $\varphi : A \rightarrow A'$ ein Ringhomomorphismus, dann definiert*

$$\varphi(x_0, x_1, \dots) := (\varphi(x_0), \varphi(x_1), \dots)$$

einen Ringhomomorphismus $\varphi : W(A) \rightarrow W(A')$.

Beweis: $\varphi(x+y) = \varphi(U_0(x, y), \dots) = (\varphi(U_0(x, y)), \dots) = (U_0(\varphi(x), \varphi(y)), \dots) = \varphi(x) + \varphi(y)$. Q.e.d.

Bemerkung: Ist p kein Nullteiler in A , ist die Abbildung $W : W(A) \rightarrow \prod_{i=0}^{\infty} A$ injektiv, im Fall $p \in A^*$ sogar ein Ringisomorphismus. Dies folgt unmittelbar aus den Formeln, welche die w_i durch die x_i ausdrücken. Um allgemeine Identitäten auf dem Witttringe zu prüfen, genügt es diese in Ringen A zu prüfen, in denen p kein Nullteiler oder eine Einheit ist.

Variante: Die Projektion $W(A) = \prod_{i=0}^{\infty} A \rightarrow W_n(A) = \prod_{i=0}^n A$ definiert einen Quotientenring $W(A) \twoheadrightarrow W_n(A)$ mit einem Ringhomomorphismus

$$W : W_n(A) \rightarrow \prod_{i=0}^n A .$$

Beachte, daß die Polynome U_i, V_i, w_i nur von $X_0, \dots, X_i, Y_0, \dots, Y_i$ abhängen. Lemma 40.1 und die Bemerkung übertragen auf diesen Fall.

Die Verschiebung

Die injektive Verschiebung $V : W(A) \hookrightarrow W(A)$ ist definiert durch

$$V(x_0, x_1, \dots) = (0, x_0, x_1, \dots) .$$

Lemma 50.2. *Die Verschiebung V ist (nur !) additiv auf $W(A)$. Ist A ein Ring der Charakteristik p , dann gilt*

$$\boxed{V \cdot F = F \cdot V = p \cdot id_{W(A)}} ,$$

insbesondere dann also $p \cdot 1_{W(A)} = (0, 1, 0, \dots)$. Hierbei bezeichne F den vom Frobenius $Frob_A$ induzierten Ringhomomorphismus von $W(A)$

$$F(x_0, x_1, \dots) = (x_0^p, x_1^p, \dots) .$$

Beweis: Die erste Aussage folgt durch Reduktion auf den universellen Fall. Die zweite durch Reduktion auf $A = A_0/p$, d.h. den universellen Fall mod p . Hier ist A perfekt und die Aussage folgt aus den Formeln für das Rechnen mit Übertrag.

Korollar 50.3. *Ist A ein Ring der Charakteristik p und $Frob_A$ injektiv, dann ist p kein Nullteiler in $W(A)$. Ist $Frob_A$ surjektiv, dann ist $V^{n+1}(W(A)) = p^{n+1} \cdot W(A)$ das von p^{n+1} erzeugte Hauptideal und es gilt*

$$W(A)/p^{n+1}W(A) \cong W_n(A) .$$

Beweis: $p \cdot x = 0$ impliziert $VF(x) = 0$, also $F(x) = 0$. Daraus folgt $x_i^p = 0$ für alle Komponenten $x_i \in A$ von x . Somit $x = 0$ für injektiven Frobenius. Die zweite Aussage folgt aus $FV = VF$, $FV = p$ sowie $F^n(W(A)) = W(A)$ (im surjektiven Fall).

Übungsaufgabe: Es gibt einen Ringhomomorphismus $F : W(A) \rightarrow W(A)$, welcher unter $W : W(A) \rightarrow \prod_{i=0}^{\infty} A$ mit dem Shift $(x_0, x_1, \dots) \mapsto (x_1, x_2, \dots)$ von $\prod_{i=0}^{\infty} A$ kommutiert. $F(x_0, x_1, \dots) = (f_0(x), f_1(x), \dots)$ mit ganzzahligen Polynomen $f_i(x) \equiv x_i^p$ modulo pA . Also induziert F den Frobenius im Fall $p \cdot A = 0$. Allgemein gilt $V(F(x) \cdot y) = x \cdot V(y)$ und $FV = p$. (Universelle Reduktion). Somit $VF = FV \iff V(1) = p \iff p \cdot A = 0$. (Für \implies benutze $W(0, 1, 0, \dots) = (0, p, p, \dots)$ sowie $W(p) = (p, p, p, \dots)$, für \impliedby dagegen Kor.50.2).

51 Rekonstruktion

Für jeden Ring A existiert ein kommutatives Diagramm

$$\begin{array}{ccc} W_n(A) & \xrightarrow{w_n} & A \\ \downarrow & & \downarrow \\ W_n(A/pA) & \xrightarrow{\exists! \theta_n} & A/p^{n+1}A \end{array}$$

Die Zusammensetzung des Ringhomomorphismus w_n mit der Projektion von A auf $A/p^{n+1}A$ bildet $(x_0, \dots, x_n) \in W_n(A)$ auf

$$a \equiv x_0^{p^n} + p \cdot x_1^{p^{n-1}} + \dots + p^n \cdot x_n \pmod{p^{n+1} \cdot A}$$

ab. Nach §48 hängt dieser Wert modulo $p^{n+1}A$ nur von den Restklassen $(\bar{x}_0, \dots, \bar{x}_n) \in W(A/p)$ ab. Somit faktorisiert dieser Homomorphismus über einen Homomorphismus $\theta_n : W(A/pA) \rightarrow A/p^{n+1}A$.

Lemma 51.1. *Sei A p -vollständig, p kein Nullteiler in A . Ist $\text{Frob}_{A/p}$ surjektiv (resp. injektiv), dann ist θ_n surjektiv (resp. injektiv). Ist A/p perfekt – das heißt die Lazardbedingungen seien erfüllt – dann induziert*

$$\theta_n(\bar{x}_0, \dots, \bar{x}_n) = x_0^{p^n} + \dots + p^n x_n$$

einen Ringisomorphismus

$$\boxed{\theta_n : W_n(A/pA) \xrightarrow{\sim} A/p^{n+1}A} .$$

Beweis: Nach §48 ist die Abbildung θ_n surjektiv (p -Entwicklung von $a \in A$), im perfekten Fall aber auch injektiv. Aus $\theta_n(\bar{x}_0, \dots, \bar{x}_n)$ folgt $\bar{x}_0^{p^n} = 0$ in A/pA . Wenn A/pA perfekt ist, folgt $\bar{x}_0 = 0$ und obdA also $x_0 = 0$. Da p kein Nullteiler in A ist folgt $x_1^{p^{n-1}} + \dots + p^{n-1}x_n \in p^n A$ und induktiv damit $\bar{x}_1 = \dots = \bar{x}_n = 0$ in A/pA .

Nach Konstruktion hat man kommutative Diagramme

$$\begin{array}{ccc} W_n(A/pA) & \xrightarrow{\theta_n} & A/p^{n+1}A \\ F \downarrow & & \downarrow \\ W_{n-1}(A/pA) & \xrightarrow{\theta_{n-1}} & A/p^n A \end{array}$$

für den Frobenius $F(\bar{x}_0, \dots, \bar{x}_n) = (\bar{x}_0^p, \dots, \bar{x}_{n-1}^p)$. Die rechte vertikale Abbildung ist die natürliche Quotientenabbildung.

Sei nun A/pA perfekt: Setzt man $\pi_n = W_n(\text{Frob}^{-n}) \circ \text{proj}(W \rightarrow W_n)$ und $\theta(\bar{x}_0, \dots) = \sum_{i=0}^{\infty} p^i \cdot \psi(\text{Frob}^{-i}\bar{x}_i)$, dann erhält man ein kommutatives Diagramm

$$\begin{array}{ccc} W(A/pA) & \xrightarrow{\theta} & A \\ \pi_n \downarrow & & \downarrow \\ W_n(A/pA) & \xrightarrow{\theta_n} & A/p^{n+1}A \end{array}$$

Die $W_n(\text{Frob}^{-n})$ sind Isomorphismen. Somit induzieren die Abbildungen π_n einen Ringisomorphismus

$$W(A) \cong \lim_{\leftarrow F} W_n(A/pA)$$

sowie θ einen Ringhomomorphismus

$$W(A) \rightarrow \lim_{\leftarrow} A/p^{n+1}A .$$

Aus Lemma 51.1 folgt

Lemma 51.2. *Sei A p -vollständig und ist A/pA perfekt. Dann definiert*

$$\theta(\bar{x}_0, \bar{x}_1, \dots) = \sum_{i=0}^{\infty} p^i \cdot \psi(\text{Frob}_{A/pA}^{-i}(\bar{x}_i))_0$$

einen Ringhomomorphismus $\theta : W(A/pA) \rightarrow A$. Ist die Lazardbedingung erfüllt – d.h. zusätzlich sei p kein Nullteiler in A – dann ist θ ein Ringisomorphismus

$$W(A/pA) \cong A .$$

Bemerkung: $\delta^i(\theta(x)) = \psi(\text{Frob}_{A/pA}^{-i}(\bar{x}_i))$ im Sinn von §48.

Bemerkung: Wegen Lemma 50.2 gilt

$$\theta(x) = \sum_{i=0}^{\infty} \psi(V^i(x)_0) .$$

52 Konstruktion

Sei R ein Ring der Charakteristik p . Dann besitzt $A = W(R)$ einen surjektiven Restklassenhomomorphismus

$$w_0 : A = W(R) \rightarrow R$$

welcher $(x_0, x_1, \dots) \in W(R)$ auf $x_0 \in R$ abbildet. Ist R semiperfekt, dann ist $\text{Kern}(w_0)$ das von p erzeugte Hauptideal von $W(R)$ und $W(R)$ ist p -vollständig wegen $W(R) = \lim_n W_n(R) = \lim_n W(R)/p^n \cdot W(R)$ (nach Korollar 50.3). Ist R perfekt, erfüllt $A = W(R)$ die Lazardbedingung (wieder Korollar 50.3).

Korollar 52.1. *Zu jedem perfekten Ring R der Charakteristik p gibt es einen Ring A , welcher die Lazardbedingung (d.h. A ist p -vollständig und p ist kein Nullteiler in A) erfüllt, so daß weiterhin gilt*

$$A/pA = R .$$

Der Ring A ist dadurch eindeutig bestimmt bis auf Isomorphie und es gilt

$$A \cong W(R) .$$

Der Frobenius Automorphismus Frob_R besitzt eine Fortsetzung F auf A .

Aus Lemma 42.2 folgt

Lemma 52.2. *Ist R nullteilerfrei und perfekt von der Charakteristik p , dann ist auch $W(R)$ nullteilerfrei.*

Beispiel 1: Es gilt $W(\mathbb{F}_p) = \mathbb{Z}_p$ (nach Lemma 51.2 für $A = \mathbb{Z}_p$)

Beispiel 2: Sei $R = \mathbb{F}_q$ eine endliche Körpererweiterung von \mathbb{F}_p . R ist perfekt und $\text{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ wird vom Frobenius erzeugt. Der Ring $W(\mathbb{F}_q)$ ist ein Erweiterungsring von $W(\mathbb{F}_p) = \mathbb{Z}_p$ und enthält die $(q-1)$ -sten Einheitswurzeln als Teichmüller Repräsentanten. Mittels der p -adischen Entwicklung (Lemma 51.2) folgt dann sofort

$$W(\mathbb{F}_q) = \mathbb{Z}_p[\zeta_{q-1}] .$$

$W(\mathbb{F}_q)$ ist ein regulärer lokaler Ring mit maximalem Ideal (p) , somit ganz abgeschlossen in seinem Quotientenkörper \mathbb{Q}_q .

Fontaine Ringe

53 Verdickungen

Sei A p -vollständig. Dann ist A/p ein Ring der Charakteristik p . Sei $P(A/p)$ seine Perfektionierung. Dies ist ein perfekter Ring der Charakteristik p . Als multiplikativer Monopoid kann er mit dem Monoid $P(A) \subset (A, \cdot)$ der Teichmüllerrepräsentanten in A identifiziert werden. Der Witttring $WP(A)$ des perfekten Rings hat die Eigenschaft $WP(A)/p = P(A)$ und es gilt

$$P(P(A/p)) = P(A/p)$$

Die linke Seite kann mit $P(WP(A))$, gewissen Folgen von Teichmüller Repräsentanten in $WP(A)$, die rechte Seite mit $P(A)$, gewissen Folgen von Teichmüller Repräsentanten in A , identifiziert werden

$$\prod_{j=0}^{\infty} WP(A) \supseteq P(WP(A)) \longleftrightarrow P(A) \subseteq \prod_{j=0}^{\infty} A.$$

Der Ringhomomorphismus ρ der Perfektionierung $P(A/p) \rightarrow A/p$ induziert Ringhomomorphismen $W_n(P(A/p)) \rightarrow W_n(A/p)$. Die Zusammensetzung mit den Abbildungen $\theta_n : W_n(A/p) \rightarrow A/p^n$ (siehe Anfang von §51) liefert Ringhomomorphismen $W_n(P(A/p)) \rightarrow A/p^n$, und im projektiven Limes einen Ringhomomorphismus $\theta : WP(A) \rightarrow A$ zusammen mit einem kommutativen Reduktionsdiagramm

$$\begin{array}{ccc} WP(A) & \xrightarrow{\theta} & A \\ \text{mod } p \downarrow & & \downarrow \text{mod } p \\ P(A/p) & \xrightarrow{\rho} & A/p \end{array}$$

Explizite Beschreibung von θ : Elemente $x = (\bar{x}_0, \bar{x}_1, \dots)$ im Witttring $WP(A)$ können auch durch

$$x = \sum_i p^i \cdot \psi_{WP(A)}(\text{Frob}_{P(A/p)}^{-i}(\bar{x}_i))_0$$

repräsentiert werden (Lemma 51.2). Jede Komponente \bar{x}_i ist in $P(A/p)$, also selber repräsentiert durch eine Sequenz

$$\bar{x}_i = \begin{pmatrix} \bar{x}_{0i} \\ \bar{x}_{1i} \\ \dots \end{pmatrix}, \quad (\bar{x}_{ji} \in A/pA)$$

mit $(\bar{x}_{ji})^p = \bar{x}_{j-1i}$. Andererseits kann x mit einer Sequenz

$$x_i = \begin{pmatrix} x_{0i} \\ x_{1i} \\ \dots \end{pmatrix} \in P(A) = P(A/p)$$

identifiziert werden (Satz 44.3). Zur Erinnerung: Dann gilt $x_{ji} \in A$ mit $x_{ji}^p = x_{j-1i}$. Man hat also die bijektive Zuordnung

$$WP(A) \ni (\bar{x}_{ji}) \mapsto (x_{ji}) \in \prod_{j,i} A$$

und die Teichmüller Repräsentanten

$$\psi_{WP(A)}(\text{Frob}_{P(A/p)}^{-i}(\bar{x}_i))_0 = \psi_{WP(A)}\left(\begin{pmatrix} \bar{x}_{ii} \\ \bar{x}_{i+1i} \\ \dots \end{pmatrix}\right)_0$$

in $WP(A)$ respektive die Teichmüller Repräsentanten

$$\psi_A(\text{Frob}_{P(A/p)}^{-i}(\bar{x}_i))_0 = x_{ii}$$

in A .

Lemma 53.1. *Der kanonische Homomorphismus*

$$\boxed{\theta : WP(A) \rightarrow A}$$

ist gegeben durch:

$$x = \sum_i p^i \cdot \left[\begin{pmatrix} \bar{x}_{ii} \\ \bar{x}_{i+1i} \\ \dots \end{pmatrix} \right] \mapsto \theta(x) = \sum_i p^i \cdot x_{ii} .$$

Ist A/p semiperfekt, dann ist θ surjektiv.

54 Neue Elemente

Sei A p -vollständiger Teilring eines Körpers und es seien alle p^n -ten Einheitswurzeln in A . Der Einfachheit halber sei $p \neq 2$. Dann gilt

$$\bar{\zeta} = (1, \bar{\zeta}_p, \bar{\zeta}_{p^2}, \dots) \in P(A/p)$$

mit primitiven p^n -ten Einheitswurzeln $\zeta_{p^n} \in A$. Identifiziert man $P(A) = P(A/p)$ wie im letzten Abschnitt, kann man $\bar{\zeta}$ als Element in $P(A)$ auffassen. Es ist gegeben durch eine Folge von Elementen in A wie folgt

$$\bar{\zeta} = (1, \zeta_p, \zeta_{p^2}, \dots) \in P(A) \subset \prod_j A .$$

Andererseits kann man den multiplikativen Teichmüller Repräsentant

$$e^{(2\pi i)_p} := [\bar{\zeta}] \in WP(A)$$

von $\bar{\zeta} \in P(A/p) = WP(A)/p$ betrachten. Dieser ist gerade der Wittvektor

$$e^{(2\pi i)_p} = (\bar{\zeta}, 0, 0, \dots) \in \prod_i P(A/p) = W(P(A/p)) = WP(A) .$$

Notation: $\boxed{\zeta = e^{(2\pi i)_p}}$.

Es gilt $\theta(e^{(2\pi i)_p}) = p^0 \cdot 1 = 1 \in A$. Das heißt $1 - e^{(2\pi i)_p} \in \text{Kern}(\theta)$.

Notation: $\boxed{\zeta_{p^n} = e^{\frac{(2\pi i)_p}{p^n}}}$ bezeichne den Teichmüllerlift von $(F^{-n}(\bar{\zeta}), 0, \dots)$.

Beachte $\zeta_{p^n}^{p^n} = \zeta$ sowie $\theta(e^{\frac{(2\pi i)_p}{p^n}}) = \zeta_{p^n}$ und $\zeta_{p^n} = F^{-n}(\zeta)$.

Frage: *Liegen die p^n -ten Einheitswurzeln in $WP(A)$?*

Antwort: *Nur wenn der Ring A der Nullring ist.*

Beweis: Eine Einheitswurzeln der Ordnung p^n in $WP(A)$ hat die Gestalt

$$\zeta_{p^n} = e^{\frac{(2\pi i)_p}{p^n}} + y \cdot (1 - e^{(2\pi i)_p}) \quad , \quad y \in WP(A) .$$

Hierbei benutzen wir, daß der Kern von θ das von $(1 - e^{(2\pi i)_p})$ aufgespannte Hauptideal ist. Dies wird im nächsten Paragraph gezeigt. Durch Potenzieren mit p^n folgt dann

$$1 \equiv e^{(2\pi i)_p} + p^n \zeta_{p^n}^{p^n-1} y \cdot (1 - e^{(2\pi i)_p}) \quad \text{modulo} \quad (1 - e^{(2\pi i)_p})^2 \cdot WP(A) .$$

Nach Kürzen von $(1 - e^{(2\pi i)_p})$ – benutze das nächste Lemma – müßte also gelten $p^n \zeta_{p^n}^{p^n-1} y \equiv 1 \quad \text{modulo} \quad (1 - e^{(2\pi i)_p}) \cdot WP(A)$, und somit

$$\theta(y) = p^{-n} \cdot \zeta_{p^n} .$$

Das postulierte Element y hat aber sein Bild $\theta(y) \in A$. Wegen $\zeta_{p^n} \in A^*$ folgt $p \in A^*$. Da A p -vollständig ist, folgt daraus $A = 0$. Q.e.d.

Lemma 54.1. *Ist A nullteilerfrei, dann auch $WP(A)$.*

Beweis: Beachte $P(A/p)$ ist nullteilerfreier Untermonoid von A . Somit folgt die Behauptung wegen Lemma 42.2.

55 Der Kern von θ

Sei A p -vollständiger Teilring eines Körpers, insbesondere also nullteilerfrei. Der Einfachheit halber sei $p \neq 2$. Man hat dann den kanonischen Homomorphismus

$$\theta : WP(A) \rightarrow A .$$

Wir bestimmen den Kern von θ : Elemente $x = \sum_i p^i [F^{-i}(\bar{x}_i)] \in WP(A)$ mit $\theta(x) = 0$ erfüllen per Definition $\sum_i p^i x_{ii} = 0$ in A . Da x_{ii} Teichmüller Repräsentanten der Restklassen $\bar{x}_{ii} \in A/pA$ in A sind, ist daher $x_{ii} = 0$ resp. $\bar{x}_{ii} = 0$ für alle i mittels p -adischer Entwicklung gleichbedeutend mit $\theta(x) = 0$. Nach Lemma 46.3 sind diese Bedingungen – wegen $p \neq 2$ – äquivalent zu $\bar{x}_i \in (1 - \bar{\zeta})^{p^i} \cdot \bar{y}_i$ ($\bar{y}_i \in P(A/p)$) für alle i . Hierbei ist $\bar{\zeta}$ definiert wie in Kapitel 46. [$\bar{\zeta} = 0$, außer wenn alle p^n -ten Einheitswurzeln in A/p (oder äquivalent dazu in A) liegen].

Mit anderen Worten: $\theta(x) = 0 \iff x = \sum_i p^i [1 - \bar{\zeta}] \cdot [F^{-i} \bar{y}_i] \in [1 - \bar{\zeta}] \cdot WP(A)$. Beachte $[F^{-i}((1 - \bar{\zeta})^{p^i} \cdot \bar{y}_i)] = [(1 - \bar{\zeta}) \cdot F^{-i}(\bar{y}_i)] = [1 - \bar{\zeta}] \cdot [F^{-i}(\bar{y}_i)]$. Setze $e^{(2\pi i)_p} := [\bar{\zeta}]$.

Behauptung: Für $p \neq 2$ gilt $[1 - \bar{\zeta}] = \alpha \cdot (1 - e^{(2\pi i)_p})$ für eine Einheit $\alpha \in WP(A)^*$.

Korollar 55.1. *Sei $p \neq 2$. Der Kern von $\theta : WP(A) \rightarrow A$ ist das von $(1 - e^{(2\pi i)_p})$ erzeugte Hauptideal von $WP(A)$, wenn A alle p^n -ten Einheitswurzeln enthält. Anderenfalls ist θ injektiv.*

Beweis der Behauptung: Aus $\theta([\bar{\zeta}] - 1) = 0$ folgt $[\bar{\zeta}] - 1 = \alpha \cdot [1 - \bar{\zeta}]$ für ein $\alpha \in WP(A)$, wie bereits oben gezeigt. Da $WP(A)$ p -vollständig ist, gilt $WP(A)^* = [P(A/p)^*] \times (1 + p \cdot WP(A))$. Somit ist α eine Einheit genau dann, wenn die nullte Wittkomponente $\bar{\alpha}_0 \in P(A/p)$ von α eine Einheit in $P(A/p)$ ist. Dies können wir durch Reduktion nach p bestimmen. Dies liefert $(\bar{\zeta} - 1) = \bar{\alpha} \cdot (\bar{\zeta} - 1)$. Da $P(A/p)$ nach 46.1 nullteilerfrei ist, folgt $\bar{\alpha} = 1$. Q.e.d.