Prof. Dr. H. Brenner | Osnabrück WS 2020/2021

Algebraische Zahlentheorie

Vorlesung 19

Kähler-Differentiale

Wir besprechen eine weitere Möglichkeit, Verzweigung zu erfassen, nämlich mit der Hilfe von Kähler-Differentialen. Dies ist ein sehr allgemeines Konzept, das dazu dient, die geometrische Idee eines Tangentialraumes bzw. Tangentialbündels algebraisch zu realisieren. Wir erwähnen hier nur die Grundzüge der Konstruktion und die wesentlichen Eigenschaften ohne Beweis. Beweise finden sich im Anhang.

Definition 19.1. Es sei R ein kommutativer Ring und A eine kommutative R-Algebra. Der von allen Symbolen $d(a)$, $a \in A$, erzeugte A-Modul, modulo den Identifizierungen

$$d(ab) = ad(b) + bd(a) \text{ für alle } a, b \in A$$

und

$$d(ra + sb) = rd(a) + sd(b) \text{ für alle } r, s \in R \text{ und } a, b \in A\,,$$

heißt *Modul der Kähler-Differentiale* von A über R. Er wird mit

$$\Omega_{A|R}$$

bezeichnet.

Bei dieser Konstruktion startet man also mit dem freien A-Modul F mit da, $a \in A$ als Basis und bildet den A-Restklassenmodul zu demjenigen Untermodul, der von den Elementen

$$d(ab) - ad(b) - bd(a)\, (a, b \in A)$$

und

$$d(ra + sb) - rd(a) - sd(b)\, (r, s \in R \text{ und } a, b \in A)$$

erzeugt wird. Die Abbildung

$$d\colon A \longrightarrow \Omega_{A|R},\, a \longmapsto d(a) = da,$$

heißt die *universelle Derivation.* Man prüft sofort nach, dass es sich um eine R-Derivation handelt.

Grundlage für konkrete Berechnungen bilden die folgenden Lemmata.

Lemma 19.2. *Es sei R ein kommutativer Ring und $A = R[X_1, \ldots, X_n]$ der Polynomring in n Variablen über R. Dann ist der Modul der Kähler-Differentiale der freie A-Modul zur Basis*

$$dX_1, dX_2, \ldots, dX_n\,.$$

Die universelle Derivation ist bezüglich dieser Basis durch

$$A \longrightarrow AdX_1 \oplus \cdots \oplus AdX_n,\ F \longmapsto dF = \frac{\partial F}{\partial X_1} dX_1 + \cdots + \frac{\partial F}{\partial X_n} dX_n,$$

gegeben.

LEMMA 19.3. *Es sei R ein kommutativer Ring und es seien A und B kommutative R-Algebren und*

$$\varphi\colon\ A \longrightarrow B$$

ein R-Algebrahomomorphismus. Dann ist die Sequenz

$$\Omega_{A|R} \otimes_A B \longrightarrow \Omega_{B|R} \longrightarrow \Omega_{B|A} \longrightarrow 0$$

von B-Moduln exakt. Dabei geht $da \otimes b$ auf $bd\varphi(a)$ und db (in $\Omega_{B|R}$) auf db (in $\Omega_{B|A}$).

LEMMA 19.4. *Es sei R ein kommutativer Ring und es sei A eine kommutative endlich erzeugte R-Algebra, die als*

$$A = R[X_1, \ldots, X_n]/(F_1, \ldots, F_k)$$

gegeben sei. Dann ist

$$\Omega_{A|R} = \bigoplus_{i=1}^{n} AdX_i/(dF_1, \ldots, dF_k).$$

KOROLLAR 19.5. *Es sei K ein Körper, $P \in K[X]$ ein nichtkonstantes Polynom und*

$$K[Y] \longrightarrow K[X] \cong K[Y][X]/(Y - P(X)),\ Y \longmapsto P(X),$$

der zugehörige Einsetzungshomomorphismus. Dann gilt für den Modul der Kähler-Differentiale die Beschreibung

$$\Omega_{K[X]|K[Y]} \cong K[X]/(P').$$

Beweis. Nach Korollar 19.4 ist (mit $R = K[Y]$ und $A = R[X]/(Y - P(X))$)

$$\Omega_{K[X]|K[Y]} = \Omega_{K[Y][X]/(Y-P(X))|K[Y]} = K[X]/d(Y - P(X)) = K[X]/(P').$$

□

Diese Isomorphie ist so zu verstehen, dass die 1 in $K[X]/(P')$ dem Differential dX entspricht. Man könnte den Sachverhalt auch als die Gleichung

$$\Omega_{K[X]|K[Y]} = K[X]/(P')dX$$

ausdrücken.

Wenn K algebraisch abgeschlossen ist, so ist $P' = (X - a_1) \cdots (X - a_s)$ und $K[X]/(P') \cong K^s$. Die vorstehende Aussage zeigt somit insbesondere, dass der Modul der Kähler-Differentiale nur lokalisiert in den maximalen Idealen $(X - a_j)$, die den Nullstellen der Ableitung entsprechen, von 0 verschieden ist. Ein entsprechendes Verhalten gilt generell im Fall einer separablen Erweiterung von Dedekindbereichen.

Lemma 19.6. *Es sei $R \subseteq S$ eine endliche Erweiterung von Dedekindbereichen derart, dass die Körpererweiterung $Q(R) \subseteq Q(S)$ der Quotientenkörper separabel sei. Dann gelten folgende Aussagen.*

(1) *Es ist $\left(\Omega_{S|R}\right)_{S\setminus\{0\}} = 0$.*
(2) *Es gibt ein $s \in S$, $s \neq 0$, mit $\left(\Omega_{S|R}\right)_s = 0$.*
(3) *Es gibt ein $r \in R$, $r \neq 0$, mit $\left(\Omega_{S|R}\right)_r = 0$.*
(4) *Es gibt endlich viele Primideale $\mathfrak{q} \in \operatorname{Spek}(S)$ mit $\left(\Omega_{S|R}\right)_{\mathfrak{q}} \neq 0$.*
(5) *Es gibt ein $r \in R$, $r \neq 0$, und ein $m \in \mathbb{N}$ mit $r^m\left(\Omega_{S|R}\right) = 0$. Insbesondere ist $\Omega_{S|R}$ ein S/r^mS-Modul.*

Beweis. (1) Nach Lemma Anhang 9.6 ist

$$\left(\Omega_{S|R}\right)_{S\setminus\{0\}} = \Omega_{Q(S)|R} = \Omega_{Q(S)|Q(R)}.$$

Somit folgt die Aussage aus dem Satz vom primitiven Element in Verbindung mit Korollar 19.4.

(2) Folgt aus (1) aufgrund der endlichen Erzeugtheit von $\Omega_{S|R}$.
(3) Folgt aus (2), man kann für r die Norm von s nehmen, die ja nach Korollar 10.8 (im zahlentheoretischen Kontext) ein Vielfaches von s ist.
(4) Folgt aus (2) und daraus, dass es in einem Dedekindbereich nur endlich viele Primideale oberhalb eines Elementes $\neq 0$ gibt.
(5) Folgt aus (3) und der endlichen Erzeugtheit.

□

In der Aussage Lemma 19.6 (5) könnte man auf den Exponenten m verzichten, wenn man r abändert. Aber aus Teil (3) ergibt sich die Aussage mit dem Exponenten. Man denke bei r an eine Primzahl aus $\mathbb{Z}$, man versucht dann, eine annullierende Potenz mit einem möglichst kleinen Exponenten zu finden.

Lemma 19.7. *Es sei $D \neq 0, 1$ eine quadratfreie Zahl und R der zugehörige quadratische Zahlbereich. Dann ist*

$$\Omega_{R|\mathbb{Z}} \cong R/\left(2\sqrt{D}\right)$$

bei $D = 2, 3 \mod 4$ *und*

$$\Omega_{R|\mathbb{Z}} \cong R/\left(\sqrt{D}\right)$$

bei $D = 1 \mod 4$.

Beweis. Im ersten Fall ist nach Satz 9.8 $R \cong \mathbb{Z}[X]/(X^2 - D)$ und daher nach Korollar 19.4

$$\Omega_{R|\mathbb{Z}} = RdX/d\left(X^2 - D\right) = RdX/2XdX \cong R/2X = R/2\sqrt{D}.$$

Im zweiten Fall ist

$$R \cong \mathbb{Z}[Y]/\Big(Y^2 - Y - \frac{D-1}{4}\Big)$$

mit $Y = \frac{1+\sqrt{D}}{2}$. Somit ist

$$\begin{aligned} \Omega_{R|\mathbb{Z}} &= RdY/d\Big(Y^2 - Y - \frac{D-1}{4}\Big) \\ &= RdY/(2Y-1)dY \\ &= RdY/\sqrt{D}dY \\ &\cong R/\sqrt{D}. \end{aligned}$$

□

Beispiel 19.8. Es sei p eine Primzahl und R der p-te Kreisteilungsring, also

$$R = \mathbb{Z}[X]/\big(X^{p-1} + X^{p-2} + \cdots + X^2 + X + 1\big)$$

nach Lemma 17.14. Nach Korollar 19.4 ist der Modul der Kähler-Differentiale gleich

$$\begin{aligned} \Omega_{R|\mathbb{Z}} &\cong R/\big((p-1)X^{p-2} + (p-2)X^{p-2} + \cdots + 3X^2 + 2X + 1\big) \\ &\cong \mathbb{Z}[X]/\big(X^{p-1} + X^{p-2} + \cdots + X^2 + X + 1, \\ &\quad (p-1)X^{p-2} + (p-2)X^{p-3} + \cdots + 3X^2 + 2X + 1\big). \end{aligned}$$

Das beschreibende Ideal ist auf den ersten Blick schwer zu durchschauen. Da $X^p - 1$ zum Ideal des Kreisteilungsringes gehört, gehört auch die Ableitung zum beschreibenden Ideal des Kählermoduls. Es ist ja

$$X^p - 1 = (X-1)\big(X^{p-1} + X^{p-2} + \cdots + X^2 + X + 1\big)$$

und somit

$$\begin{aligned} pX^{p-1}dX &= d(X^p - 1) \\ &= d\big((X-1)\big(X^{p-1} + X^{p-2} + \cdots + X^2 + X + 1\big)\big) \\ &= \big(X^{p-1} + X^{p-2} + \cdots + X^2 + X + 1\big)dX + (X-1) \\ &\quad \big((p-1)X^{p-2} + (p-2)X^{p-3} + \cdots + 3X^2 + 2X + 1\big)dX. \end{aligned}$$

Damit ist insbesondere

$$pdX = 0$$

in $\Omega_{R_p|\mathbb{Z}}$, da ja X eine Einheit ist. Somit ist der Kählermodul ein R_p/pR_p-Modul und insbesondere ein $\mathbb{Z}/(p)$-Modul. Daher und wegen Lemma Anhang 9.11 ist

$$\Omega_{R_p|\mathbb{Z}} = \Omega_{R_p|\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Z}/(p) = \Omega_{R_p/pR_p|\mathbb{Z}/(p)}.$$

Da der Faserring über p die Form

$$R_p/pR_p = \mathbb{Z}/(p)[X]/\big((X-1)^{p-1}\big) = \mathbb{Z}/(p)[Y]/\big(Y^{p-1}\big)$$

besitzt, ist wegen $\big(Y^{p-1}\big)' = -Y^{p-2}$ insgesamt

$$\Omega_{R_p|\mathbb{Z}} = \Omega_{\mathbb{Z}/(p)[Y]/(Y^{p-1})|\mathbb{Z}/(p)} \cong \mathbb{Z}/(p)[Y]/\big(Y^{p-2}\big).$$

Dies ist ein freier $\mathbb{Z}/(p)$-Modul mit der (in X geschriebenen) Basis $dX, XdX, \ldots, X^{p-3}dX$ (also vom Rang $p-2$).

Beispiel 19.9. Es sei p eine Primzahl und $R = \mathbb{Z}[X]/(X^p - p)$, vergleiche Beispiel 18.11. Der Modul der Kähler-Differentiale ist

$$\Omega_{R|\mathbb{Z}} \,=\, R/\big(px^{p-1}\big)dx$$

und das annullierende Ideal ist

$$\big(px^{p-1}\big) \,=\, \big(x^{2p-1}\big).$$

Die Norm von deshalb ist die Anzahl der Elemente im Modul der Kähler-Differentiale gleich p^{2p-1}.

Beispiel 19.10. Es sei $q = \pm 1 \mod 9$ eine Primzahl und $R = \mathbb{Z}[x,z] \subset \mathbb{Q}[X]/(X^3 - q)$ mit $z = \frac{1+qx+x^2}{3}$ der Ganzheitsring, vergleiche Satz 16.1. Der Modul der Kähler-Differentiale wird als R-Modul von dx und dz erzeugt. Wir behaupten, dass der Erzeuger dz überflüssig ist, obwohl er als Algebraerzeuger nicht überflüssig ist. Dabei gilt

$$3dz \,=\, d3z \,=\, d\big(1+qx+x^2\big) \,=\, qdx + 2xdx \,=\, (q+2x)dx.$$

Ferner ist unter Verwendung von Aufgabe 16.7

$$xdz + zdx \,=\, dxz \,=\, d\left(\frac{1-q^2}{3}x + qz\right) \,=\, \frac{1-q^2}{3}dx + qdz,$$

woraus wir

$$(x-q)dz \,=\, -zdx - \frac{1-q^2}{3}dx \,=\, -\left(z + \frac{1-q^2}{3}\right)dx$$

gewinnen. Schließlich ist

$$2zdz \,=\, dz^2 \,=\, d\left(\frac{q^2-1}{9} + \frac{-q^3-q}{9}x + \frac{q^2+2}{3}z\right) \,=\, \frac{-q^3-q}{9}dx + \frac{q^2+2}{3}dz,$$

woraus wir

$$\left(2z - \frac{q^2+2}{3}\right)dz \,=\, \frac{-q^3-q}{9}dx$$

gewinnen. Wir können also verschiedene Vielfache von dz als Vielfache von dx ausdrücken. Wir betrachten das von den Vorfaktoren erzeugte Ideal in R, also

$$\left(3, x-q, 2z - \frac{q^2+2}{3}\right).$$

Dieses Ideal enthält $q^3 - q$ und Im Restklassenring wird also x zu q und z wird zu

$$\frac{1+qx+x^2}{3} \,=\, \frac{1+2q^2}{3}.$$

Somit enthält das Ideal die Zahlen $3, q^3 - q$ und

$$2\frac{1+2q^2}{3} - \frac{q^2+2}{3} \,=\, q^2.$$

Da 3 und q teilerfremd ist, enthält es auch die 1 und somit gibt es auch eine Darstellung von dz als Vielfaches von dx.

Verzweigung und Differentiale

Lemma 19.11. *Es sei K ein vollkommener Körper und A eine lokale endlichdimensionale K-Algebra. Dann ist A genau dann reduziert (also ein Körper) wenn der Modul der Kählerdifferentiale $\Omega_{A|K}$ gleich 0 ist.*

Beweis. Wenn R reduziert ist, so liegt eine endliche Körpererweiterung $K \subseteq A$ vor, die wegen der Vollkommenheit des Grundkörpers separabel ist und deshalb nach dem Satz vom primitiven Element von einem Elment erzeugt ist, sagen wir $A = K[x] = K[X]/(F)$. Nach Lemma Anhang 8.3 erzeugen F und F' das Einheitsideal und somit folgt aus $F'(x)dx = 0$, dass sogar $dx = 0$ ist. Somit folgt die Aussage aus Korollar 19.4.

Sei nun angenommen, dass A nicht reduziert ist. Es ist zu zeigen, dass es nichttriviale Kählerdifferentiale gibt. Da A eine lokale Algebra ist, ist ein Element darin entweder eine Einheit oder gehört zum maximalen Ideal. Zu einer Einheit $x \in A$, $x \notin K$, ist $K[x]$ ein Erweiterungskörper von K. Indem wir so den Grundkörper vergrößern, können wir wegen Lemma 19.3 annehmen, dass nur die Elemente aus $K \setminus 0$ Einheiten in A sind. Dann ist

$$A = K[x_1, \ldots, x_n]$$

und die x_i gehören zum maximalen Ideal $\mathfrak{m}$. Indem wir die Restklassenabbildung

$$A \longrightarrow A/\mathfrak{m}^2$$

betrachten und Lemma Anhang 9.8 heranziehen, können wir davon ausgehen, dass die Situation

$$A = K[X_1, \ldots, X_n]/(X_iX_j,\, 1 \leq i \leq j \leq n)$$

vorliegt, wobei mindestens ein Erzeuger $x_1 \neq 0$ ist. Mit dem gleichen Lemma können wir modulo $(x_2, \ldots, x_n)$ gehen und erhalten die Situation $K[X]/(X^2)$. Dafür zeigt Korollar 19.4, dass $dx \neq 0$ ist. □

Satz 19.12. *Es sei R ein Zahlbereich. Dann ist die Ringerweiterung $\mathbb{Z} \subseteq R$ in einem Primideal $\mathfrak{q} \in \operatorname{Spek}(R)$ genau dann verzweigt, wenn*

$$\left(\Omega_{R|\mathbb{Z}}\right)_{\mathfrak{q}} \neq 0$$

ist.

Beweis. Es sei $\mathfrak{p} = \mathbb{Z} \cap \mathfrak{q}$, und wir können wegen Lemma Anhang 9.6 direkt zu

$$B = \mathbb{Z}_{\mathfrak{p}} \longrightarrow A = R_{\mathbb{Z} \setminus \mathfrak{p}}$$

übergehen. Die Bedingung

$$\left(\Omega_{R|\mathbb{Z}}\right)_{\mathfrak{q}} = \left(\Omega_{A|B}\right)_{\mathfrak{q}} = \Omega_{A_{\mathfrak{q}}|B} \neq 0$$

ist äquivalent zu

$$\Omega_{A|B} \otimes_A A/\mathfrak{q} \;=\; \Omega_{A_\mathfrak{q}|B} \otimes_{A_\mathfrak{q}} A_\mathfrak{q}/\mathfrak{q} \;\neq\; 0,$$

da ja $\Omega_{A_\mathfrak{q}|B}$ ein endlicher erzeugter $A_\mathfrak{q}$-Modul über dem lokalen Ring $A_\mathfrak{q}$ ist. Wegen der natürlichen Surjektion

$$A_\mathfrak{q}/\mathfrak{p}A_\mathfrak{q} \longrightarrow A_\mathfrak{q}/\mathfrak{q}$$

ist dies auch äquivalent zu

$$\Omega_{A_\mathfrak{q}|B} \otimes_{A_\mathfrak{q}} A_\mathfrak{q}/\mathfrak{p}A_\mathfrak{q} \;\neq\; 0.$$

Nach Lemma Anhang 9.11 angewendet auf

$$\begin{array}{ccc} A_\mathfrak{q} & \longrightarrow & A_\mathfrak{q}/\mathfrak{p}A_\mathfrak{q} \\ \uparrow & & \uparrow \\ B & \longrightarrow & B/\mathfrak{p} = \kappa(\mathfrak{p}) \end{array}$$

ist

$$\Omega_{A_\mathfrak{q}|B} \otimes_{A_\mathfrak{q}} A_\mathfrak{q}/\mathfrak{p}A_\mathfrak{q} \;=\; \Omega_{A_\mathfrak{q}/\mathfrak{p}A_\mathfrak{q}|B/\mathfrak{p}}$$

und dies ist die Lokalisierung von $\Omega_{A/\mathfrak{p}|B/\mathfrak{p}}$ an $\mathfrak{q}$. Somit ist die Lokalisierung von $\Omega_{A|B}$ an $\mathfrak{q}$ genau dann von 0 verschieden, wenn $\Omega_{A/A\mathfrak{p}|B/\mathfrak{p}}$ lokalisiert an $\mathfrak{q}$ von 0 verschieden ist. Die Bedingung an den Modul der Kähler-Differentiale spielt sich somit allein in der speziellen Faser über $\mathfrak{p}$ ab. Nach (dem Beweis zu) Satz 18.10 liegt in $\mathfrak{q}$ genau dann Verzweigung vor, wenn $R/\mathfrak{q} = A/\mathfrak{q}$ nicht reduziert ist. Deshalb folgt die Aussage aus Lemma 19.11. $\square$

Abbildungsverzeichnis