Algebraische Zahlentheorie

frei nach

Cassels, J.W.S, Fröhlich, A. (ed): Algebraic number theory
Proceedings of an instructional conference organized by the London Mathematical Society
Academic Press, London and New York 1967

Dieses Vorlesungsmanuskript ersetzt nicht die Lektüre dieses Originals, sondern ist eher dazu gedacht, diese zu erleichtern.

Ich danke Andrea Schwetzler für ihr sorgfältiges Durcharbeiten des ersten Kapitels (Lokale Körper) und das Auffinden zahlreicher Fehler.

Bezeichnungen

Ab	Kategorie der abelschen Gruppen
Br(K)	Brauer-Gruppe des lokalen Körpers K, vgl. 5.2.8.4 oder 6.1.1.1
δ	Zusammenhangshomomorphismus der langen Kohomologie-Sequenz zu einer kurzen exakten Sequenz von Moduln über einer Gruppe, vgl. 4.1.6 oder auch 4.2.6
ε	Augementations-Homomorphismus, vgl. 4.2.1 oder 4.3.2
f	Grad des Resklassenkörpers k des lokalen Körpers K über dessen Primkörper, vgl. 6.0.1
F	Frobenius-Abbildung der maximalen unverzweigten Erweiterung eines lokalen Körpers, vgl. 6.1.1.1
G	eine Gruppe, vgl. 4.1.1
G(m)	die Gruppe der primen Restklassen modulo m, vgl. 3.1.2.
$G(E/F)=G_{E/F}$	Galois-Gruppe der Galois-Erweiterung E/F, vgl. 6.0.2
G°	die zu G entgegengesetzte Gruppe, vgl. Fußnote in 4.4.1.
$H^q(K)$	q-te Kohomologie des Komplexes K, vgl. 4.1.7
$H^q(F)$	q-the Kohomologie der absoluten Galois-Gruppe von F mit Werten in der mutliplikativen Gruppe der separablen Abschließung von F, vgl. 5.2.8.3
$H^q(G, M)$	q-te Kohomologie der Gruppe G mit Koeffizienten im G-Modul M, vgl. 4.1.9
$H_q(G,M)$	q-te Homologie der Gruppe G mit Koeffizienten im G-Modul M, vgl 4.3.5 und 4.3.7
$\hat{H}^0(G, M)$	0-te Tate-Kohomologie der endlichen Gruppe G mit Koeffizienten im G-Modul M, vgl. 4.6.2
$\hat{H}_0(G, M)$	0-te Tate-Kohomologie der endlichen Gruppe G mit Koeffizienten im G-Modul M, vgl. 4.6.2
$H^2(L/K)$	$:= H^2(G_{L/K}, L^*)$, vgl. 6.1.1.1
$H^2(L/K)_{nr}$	der Gruppe der über L zerfallenden Elemente von $H^2(L/K)$, vgl. 6.1.3.2.
Hom(M,N)	Gruppe der Gruppen-Homomorphismen der Gruppe M mit Werten in der Gruppe N, vgl. 4.1.2
$Hom_G(M,N)$	G-Modul der G-Modul-Homomorphismen des G-Moduls M mit Werten im G-Modul N. Dabei sei G eine Gruppe, vgl. 4.1.2
I_G	Augmentations-Ideal der Gruppe G, vgl. 4.3.2

inv_K	der Isomorphismus der Brauer-Gruppe eines lokalen Körpers mit $\mathbb{Q}/\mathbb{Z}$, vgl. 6.1.1.3 und 6.1.1.4
K	ein lokaler Körper, vgl. 6.0.1
K*	multiplikative Gruppe des lokalen Körpers K, vgl. 6.0.1
K_{nr}	maximale unverzweigte Erweiterung des lokalen Körpers K, vgl. 6.1.1.1
K_s	separable Abschließung von K, vgl. 6. 0.2
$\overline{K}$	algebraische Abschließung von K, vgl. 6.0.2
k	der Restklassenkörper des lokalen Körpers K, vgl. 6.0.1
$\overline{k}$	algebraische Abschließung des Körpers , vgl. 6.1.1.1
L_t	Links-Multiplikation mit dem Element t, vgl. 4.4.7
Λ	die ganzzahlige Gruppen-Algebra $\mathbb{Z}[G]$ der Gruppe G, vgl. 4.1.1
N = N(G)	Summe der Elemente der endlichen Gruppe G (im Gruppenring von G), bzw. die Multiplikation mit dieser Summe (betrachtet als Endomorphismus eines beliebigen G-Moduls), vgl. 4.6.1
$\mathcal{O}_K$	Ring der ganzen Zahlen des lokalen Körpers K, vgl. 6.0.1
$\mathcal{O}_v$	Ring der ganzen Zahlen der Vervollständigung k_v des Körpers k bezüglich der nicht-archimedischen Bewertung v von k, vgl. 1.14.1
P	Standard-Resolvente von $\mathbb{Z}$ über der Gruppe G, vgl. 4.2.1
p	Charakteristik des Restklassenkörpers des lokalen Körpers K, vgl. 6.0.1
q	Anzahl der Elemente des Restklassenkörpers k des lokalen Körpers K, vgl. 6.0.1
Res	Einschränkung der Kohomologie auf eine Untergruppe, vgl. 4.4.3.
σ_t	der innere Automorphismus einer Gruppe zum Gruppen-Element t, vgl. 4.4.6
T	die Differenz s-1, wobei s ein Erzeuger der betrachteten zyklischen Gruppe ist, vgl. 4.8.1. Die Multiplikation mit T wird ebenfalls mit T bezeichnet.
U_K	Gruppe der Einheiten des Rings $\mathcal{O}_K$ der ganzen Zahlen des lokalen Körpers K, vgl. 6.0.1
V_k	Adele-Ring des globalen Körpers k, vgl. 2.1.4.1
V_L	der L-Vektorraum, der aus V durch Basis-Wechsel nach L entsteht, vgl. 4.8.10.
#M	Anzahl der Elemente der Menge M
[y]	die Kohomologie-Klasse des Kozyklus y, vgl. 4.2.6
[x]	Restklasse des Elements x, vgl. 4.3.3
f*	der durch den Gruppen-Homomorphismus f induzierte Homomorphismus auf der Kohomologie, vgl. 4.4.3
f_*	der durch den Gruppen-Homomorphismus f induzierte Homomorphismus auf der Homologie, vgl. 4.4.5
G-Mod	Kategorie der linken Moduln über dem ganzzahligen Gruppenring $\Lambda = \mathbb{Z}[G]$ der Gruppe G
J(v)	Anzahl der Fortsetzungen der Bewertung v auf einen gegebenen Erweiterungskörper, vgl. 2.12.5
k_v	Vervollständigung des Körpers k bezüglich der Bewertung v von k, vgl. 2.12.5 und 2.14.1
M^G	Gruppe der invarianten Elemente des Moduls M über der Gruppe G, vgl. 4.1.3

M_G	:= $M/I_G M$, der größte Faktor-Modul des G-Moduls M, auf welchem die Gruppe G trivial operiert, vgl. 4.3.3
M^t	der Modul M über einer Gruppe G mit der durch den inneren Automorphismus zum Element $t \in G$ abgeänderten Modul-Struktur, vgl. 4.4.6
$M \otimes N$	Tensorprodukt der Moduln M und N über $\mathbb{Z}$, vgl. 4.3.1
$M \otimes_G N$	Tensorprodukt der G-Moduln M und N über dem Gruppenring $\Lambda = \mathbb{Z}[G]$ der Gruppe G, vgl. 4.3.1
${}^s\alpha$	Ergebnist der Anwendung des Automorphismus s auf das Element α des Definitionsbereiches von s, vgl. 6.0,1
$v \mid V$	die Einschränkung der Bewertung v ist äquivalent zur Bewertung V, vgl. 2.12.4

Inhalt

1 Lokale Körper (A. Fröhlich)

Bezeichnungen

Ab Kapitel 1.4 Erweiterungen

R	ein Dedekind-Ring
K	:= Q(R), Quotientenkörper von R
L	ein endlicher separabler Erweiterungskörper von K
S	die ganze Abschließung von R in L (d.h. der Ring der Elemente von L, welche ganz über R sind).

Ab Kapitel 1.5 Verzweigungen, Abschnitt 5.

R	ist ein diskreter Bewertungsring mit dem Bewertungsideal p
K	= Q(R) ist vollständig bezüglich der p-adischen Bewertung
S	ist ein diskreter Bewertungsring mit dem Bewertungsideal P
L	= Q(S) ist vollständig bezüglich der P-adischen Bewertung.

v_L	P-adische Bewertung des Körpers L
k_L	:= S/P, Resklassenkörper des Körpers L.
U_L	Gruppe der Einheiten des Rings S

k	$:= k_K$, Restklassenkörper zum Grundkörper.
Gitter	:= freier S-Teilmodul von L maximalen Rangs [L:K]
$[M:N]_R$	Index der Gitter $M,N \subseteq L$, $[M:N]= \det(\ell)R$ für $\ell: L \to L$ ein K-Automorphismen mit $\ell(M)=N$.
$D_R(M)$	Dual des Gitters M, $D(M) := \{x \in L \mid Tr_{L/K}(xM) \subseteq R\}$
$\delta_R(M)$	Diskrimante von M, $\delta := [D_R(M),M]_R$
$\mathcal{D}(L/K) := \mathcal{D}(S/R)$	Differente, $:= D_R(S)^{-1}$ $(\subset S)$
$\delta(L/K) := \delta(S/R)$	Diskriminante R, $\delta := N_{L/K}(\mathcal{D})$
$f(L/K) := f(S/R)$	Relativgrad, $f = [k_L : k_K]$
$e(L/K) := e(S/R)$	Verzweigungsindex, $v_L(x) = e \cdot v_K(x)$ für $x \in K$

Glossar

Unverzweigte Erweiterungen
$\Leftrightarrow$
1. $\text{char}(k_K) = 1$.
2. $k_K \subseteq k_L$ ist separable Körpererweiterung

$\Leftrightarrow \delta(L|K) = R$.

Zahm verzweigte Erweiterungen
$\Leftrightarrow$
1. $\text{char}(k_K)$ ist kein Teiler von $e(L|K)$
2. $k_K \subseteq k_L$ ist separable Körpererweiterung

$\Leftrightarrow Tr_{L/K}(S) = R$
$\Leftrightarrow v_L(\mathcal{D}) = e - 1$
($\Leftrightarrow S \cong R[G]$ über $R[G]$ im Fall von Galoiserweiterungen mit der Gruppe G)

Total verzweigte Erweiterungen
$\Leftrightarrow$
$e(L/K) = [L:K]$
$\Leftrightarrow f(L/K) = 1$
$\Leftrightarrow S = R[\prod]$ ist Eisensteinerweiterung

Zu jedem Verzweigungsindex gibt es eine total verzweigte Erweiterung.

1.1 Diskrete Bewertungsringe

1.1.1 Gebrochene Ideale

Sei R ein Integritätsbereich[1] mit dem Quotientenkörper K. Ein gebrochenes Ideal von R ist ein von Null verschiedener R-Teilmodul von K,

$$0 \neq I \subseteq K$$

mit der Eigenschaft, daß es ein $a \in K-\{0\}$ gibt mit $aI \subseteq R$.

Bemerkungen
(i) Man kann dann immer $a \in R-\{0\}$ wählen.
(ii) aI ist ein Ideal von R.

[1] d.h. ein kommutativer Ring ohne Nullteiler mit $1 \neq 0$.

1.1.2 Operationen mit R-Teilmoduln von Q(R)

Sei R ein Integritätsbereich mit dem Quotientenkörper K. Für R-Teilmoduln I_1, I_2 von K führen wir die folgenden Operationen ein.

$I_1 + I_2$ (Summe von Teilmoduln)

$I_1 \cap I_2$

$I_1 I_2$ (der kleinst Teilmodul, der alle Produkte ab mit $a \in I_1$ und $b \in I_2$ enthält)

$I^{-1} := \{x \in K \mid xI \subseteq R\}$

$R(I) := \{x \in K \mid xI \subseteq I\}$

1.1.3 Eigenschaften der Operationen

(i) Addition, Multiplikation und Durchschnittsbildung sind kommutativ und assoziativ auf der Menge der R-Teilmoduln von K.

(ii) $I \cdot (I_1 + I_2) = I \cdot I_1 + I \cdot I_2$

(iii) $R(I) \supseteq R \supseteq I \cdot I^{-1}$

(iv) $I \subseteq R \Rightarrow I^{-1} \supseteq R$

Beweis: trivial.
QED.

1.1.4 Der Fall gebrochener Ideale

Seien R ein Integritätsbereich und I, I_1, I_2 gebrochene Ideale von R. Dann sind auch

$$I_1 + I_2, \qquad I_1 \cap I_2, I_1 I_2, \quad I^{-1}, \quad R(I)$$

gebrochene Ideale.

Beweis. Für die ersten drei Operationen ist das trivial. Zum Beweis der Behauptung für die letzten beiden Moduln zeigen wir allgemeiner, daß für je zwei gebrochene Ideale I_1 und I_2 auch

$$J := \{x \in K \mid xI_2 \subseteq I_1\}$$

gebrochenes Ideal ist. Seien a, b∈K von Null verschiedene Elemente mit

$$aI_2 \subseteq R \text{ und } b \in I_1 \cap R.$$

Dann ist ab ein von Null verschiedenes Element mit $b \cdot aI_2 \subseteq bR \subseteq I_1$, d.h. es ist ab∈J, d.h.

$$J \neq 0.$$

Weiter seien c,d∈K von Null verschiedene Elemente mit

$$cI_1 \subseteq R, \; d \in I_2.$$

Dann gilt $cdJ \subseteq cI_1 \subseteq R$. Also ist J ein gebrochenes Ideal.

QED.

1.1.5 Gebrochene Ideale noetherscher Integritätsbereiche

Sei R ein noetherschen Integritätsbereich und I⊆Q(R) ein von Null verschiedener R-Teilmodul. Dann sind folgende Aussagen äquivalent.

(i) I ist gebrochenes Ideal.

(ii) I ist endlich erzeugt.

Beweis. (i) ⇒ (ii). Es gilt aI⊆R für ein a∈K-{0}, d.h. aI ist ein Ideal von R und damit endlich erzeugt.

(ii) ⇒ (i). Wählen wir ein endliches Erzeugendensystem für I,

$$I = Rc_1 + \ldots + Rc_n \text{ mit } c_i \in K.$$

Es gibt ein von Null verschiedenes Element $a \in R$ mit $ac_i \in R$ für alle i. Dann gilt aber auch $aI \subseteq R$.
QED.

1.1.6 Diskrete (additive) Bewertungen

Seien K ein Körper und K* die multiplikative Gruppe von K. Eine diskrete Bewertung von K ist eine Abbildung

$$v: K \to \mathbb{Z} \cup \{\infty\}$$

mit folgenden Eigenschaften.

1. v induziert einen surjektiven Gruppenhomomorphismus $K^* \to \mathbb{Z}$.
2. $v(0) = \infty$.
3. $v(x+y) \geq \inf\{v(x), v(y)\}$.

Bemerkungen

(i) $R_v := \{x \in K \mid v(x) \geq 0\}$ ist ein Teilring von K und heißt Bewertungsring zur Bewertung v. Es gilt $Q(R_v) = K$.

(ii) $m_v := \{x \in K \mid v(x) > 0\}$ ist das einzige maximale Ideal von R_v und heißt Bewertungsideal zur Bewertung v.

(iii) In Fall $v(x) \neq v(y)$ gilt $v(x+y) = \inf(v(x), v(y))$.

Beweis. Zu (i). Die Ringeigenschaft von R_v folgt unmittelbar aus der Definition von v.

Man beachte für $x \in K^*$ gilt $v(x) \geq 0$ oder $v(x^{-1}) \geq 0$, also $x \in R_v$ oder $x^{-1} \in R_v$. Also ist

$$Q(R_v) = K.$$

Zu (ii). Trivialerweise ist m_v ein Ideal. Es ist ein echtes Ideal wegen $v(1) = 0$, also

$$1 \in R_v - m_v.$$

Für jedes Element $x \in R_v - m_v$ gilt $v(x) = 0$, also $v(x^{-1}) = 0$, also $x^{-1} \in R_v$, d.h. x ist Einheit in R_v. Dann ist aber m_v das einzige maximale Ideal von R_v.

Zu (iii). OBdA sei $v(x) > v(y)$. Angenommen es ist $v(x+y) > \inf(v(x), v(y))$. Dann gilt

$$(*) \qquad v(y) < v(x+y) = v(y) + v\left(1+\frac{x}{y}\right).$$

Wegen $v(x) > v(y)$ gilt $v\left(\frac{x}{y}\right) > 0$, also $\frac{x}{y} \in m_v$. Nach (*) ist $v\left(1+\frac{x}{y}\right) > 0$, also auch $1+\frac{x}{y} \in m_v$ und damit $1 \in m_v$, im Widerspruch zu (ii).

QED.

1.1.7 Multiplikative Bewertungen (vom Rang 1)

Sei K ein Körper. Eine multiplikative Bewertung von K ist eine Abbildung

$$K \to \mathbb{R}_{\geq 0} := \{x \in \mathbb{R} \mid x \geq 0\}, \; x \mapsto |x|,$$

mit folgenden Eigenschaften.

1. $|x| = 0 \Leftrightarrow x = 0$.
2. $|xy| = |x| \cdot |y|$.
3. Es gibt eine Konstante C mit $|1+x| \leq C$ für alle x mit $|x| \leq 1$.

Bemerkungen

(i) Die multiplikative Bewertung mit $|x| = 1$ heißt triviale Bewertung von K. Die triviale Bewertung wird bei den meisten Betrachtungen ausgeschlossen.

(ii) Aus Axiom 2 folgt $|1| = |1| \cdot |1|$, also ist $|1| = 1$.

(iii) Wenn für eine Potenz des Elements x gilt $x^n = 1$, so ist $|x| = 1$. Insbesondere ist die einzige multiplikative Bewertung eines endlichen Körpers die triviale.

(iv) Aus Axiom 2 folgt $|1| = |-1|\cdot|-1|$, also ist $|-1| = 1$ und damit
$$|-x| = |x| \text{ für alle } x.$$
(v) Zwei Bewertungen $|\ |_1$ und $|\ |_2$ des Körpers K heißen äquivalent, wenn es ein $c>0$ gibt mit $|x|_2 = |x|_1^c$ für alle $x\in K$. Auf diese Weise ist eine Äquivalenzrelation für multiplikative Bewertungen definiert.
(vi) Eine multiplikative Bewertung, welche äquivalent zu einer Bewertung mit C=1 ist heißt nicht-archimedisch. Für Bewertungen mit C=1 gilt die folgende Verschärfte Variante der Dreiecksungleichung.
$$|x+y| \le \max\{|x|,|y|\}$$
(vii) Eine multiplikative Bewertung des Köpers K ist genau nicht-archimedisch, wenn gilt
$$|n\cdot 1_K| \le 1 \text{ für } n=1,2,3,...$$

Beweis von (vi) und (vii). Zu (vi). OBdA sei $|x| \ge |y|$. Dann hat $c := \frac{y}{x}$ einen Wert ≤ 1, d.h. es ist
$$|x+y| = |x|\cdot|1+c| \le |x| = \max\{|x|,|y|\}.$$
Zu (vii). Offensichtlich ist die Bedingung für Bewertungen mit C=1 erfüllt. Sei jetzt umgekehrt eine Bewertung gegeben mit
$$|n\cdot 1_K| \le 1 \text{ für } n=1,2,3,...$$
Es reicht zu zeigen, $|1+x| \le 1$ für jedes $x\in K$ mit $|x|\le 1$. Auf jeden Fall gilt
$$|1+x|^n = |\sum_{j=0}^{n} \binom{n}{j} x^j| = \sum_{j=0}^{n} |\binom{n}{j}\cdot 1_K|\cdot|x^j| = \sum_{j=0}^{n} |x^j| \le n+1$$
Wir ziehen die n-te Wurzel und lassen n gegen ∞ gehen und erhalten $|1+x| \le 1$, d.h. wir haben eine Bewertung mit C=1 vorliegen.
QED.

1.1.8 Äquivalente multiplikative Bewertungen

(i) Ist $|\ |$ eine multiplikative Bewertung des Körpers K und ist $c>0$, so ist auch $|x|^c$ eine multiplikative Bewertung.
(ii) Jede multiplikative Bewertung ist äquivalent zu einer mit C=2.
(iii) Für multiplikative Bewertungen mit C=2 ist das dritte Axiom äquivalent zur Dreiecksungleichung,
$$|x+y| \le |x| + |y|.$$
(iv) Für multiplikative Bewertungen, die der Dreicksungleichung genügen, gilt auch
$$||x| - |y|| \le |x-y|.$$

Beweis. Zu (i). trivial.
Zu (ii). trivial.
Zu (iii). Sei
$$|1+x| \le 2 \text{ für } |x|\le 1.$$
Dann gilt auch[2]
(1) $$|x+y| \le 2\cdot\max\{|x|, |y|\} \text{ für beliebige } x,y\in K.$$
Induktiv ergibt sich aus (1)
(2) $$|\sum_{j=1}^{2^r} x_j| \le 2^r \max\{x_1,...,x_{2^r}\}$$
und damit für $2^{r-1} < n \le 2^r$
(3) $$|\sum_{j=1}^{n} x_j| \le 2^r \max\{x_1,...,x_n\} \le 2n\cdot\max\{x_1,...,x_{2^r}\}$$

[2] Sei OBdA $|x|\ge|y|$ und $y = xc$. Dann ist $|x+y| = |x|\cdot(|1+c|) \le 2\cdot|x| = 2\cdot\max\{|x|, |y|\}$.

(wir addieren Summanden die Null sind). Insbesondere ergibt sich aus (3)

(4) $$|n| \le 2n\cdot|1| = 2n$$

für alle $n>0$. Damit ist aber

$$\begin{aligned}
|x+y|^n &= |\sum_{j=1}^{n}\binom{n}{j}x^j y^{n-j}| \\
&\le 2(n+1)\cdot\max\{|\binom{n}{j}x^j y^{n-j}| : j=0,...,n\} \qquad \text{(nach (3))} \\
&\le 4(n+1)\cdot\max\{\binom{n}{j}\cdot|x|^j\cdot|y|^{n-j} : j=0,...,n\} \text{(nach (4))} \\
&\le 4(n+1)\cdot\sum_{j=1}^{n}\binom{n}{j}\cdot|x|^j\cdot|y|^{n-j} \\
&\le 4(n+1)(|x| + |y|)^n.
\end{aligned}$$

Wir ziehen die n-te Wurzel,gehen zum Limes $n\to\infty$ über und erhalten die Dreiecksungleichung.

Zu (iv). Mit $z = x-y$ gilt $x = y+z$ also

$$|x| = |y+z| \le |y| + |z|,$$

also

$$|x| - |y| \le |z| = |x-y|.$$

Damit ist aber auch

$$-(|x|-|y|) = |y| - |x| \le |y-x| = |x-y|,$$

zusammen ist also $||x| - |y|| \le |x-y|$.

QED.

1.1.9 Additive und multiplikative Bewertungen

Ist $v:K\to\mathbb{Z}\cup\{\infty\}$ eine diskrete Bewertung von K und $\rho\in(0,1)$ eine reelle Zahl, so ist durch

$$|x|_v := \rho^{v(x)}$$

eine multiplikative Bewertung gegeben. Diese heißt die durch v gegebene diskrete multiplikative Bewertung.

Beweis. Es gilt

$$0 = |x|_v = \rho^{v(x)} \Leftrightarrow v(x) = \infty \Leftrightarrow x = 0.$$

Die Multiplikativität von $|x|_v$ folgt aus der Additivität von v. Zur dritten Eigenschaft:

$$|1+x|_v = \rho^{v(1+x)} \le 1 \text{ für } v(1+x)\ge 0,$$

also für $x\in R_v$, d.h. für $v(x)\ge 0$, d.h. $|x|_v = \rho^{v(x)}\le 1$.

QED.

Bemerkungen

(i) Jede diskrete Bewertung definiert über die zugehörige multiplikative Bewertung eine Topologie auf K. Bezüglich dieser Topologie kann man K vervollständigen.

(ii) Wir werden später sehen, die zugehörige Vervollständigung $\bar{K}$ von K ist wieder ein Körper mit einer eindeutig bestimmten multiplikativen Bewertung, welche die gegebene Bewertung fortsetzt. Diese kommt von einer diskreten Bewertung im oben angegebenen Sinne.

(iii) Insbesondere läßt sich damit jede diskrete Bewertung v von K auf genau eine Weise auf die Vervollständigung $\bar{K}$ von K fortsetzen.

1.1.10 Beispiel: formale Laurentreihen

Seien F ein Körper und

$$K := F((t)) := \{ \sum_{n=n_0}^{\infty} a_n t^n \mid a_n \in F \}$$

der Körper der formalen Laurentreihen mit Koeffizienten aus F. Die diskrete Standard-Bewertung von K ist gegeben durch

$$v(\sum_{n=n_0}^{\infty} a_n t^n) = \inf \{n \mid a_n \neq 0\}.$$

Der Körper K ist vollständig bezüglich dieser Bewertung.

1.1.11 Einheitengruppe und Uniformisierenden

Sei $v: K \to \mathbb{Z} \cup \{\infty\}$ eine diskrete Bewertung des Körpers K. Dann heißt

$$U := U_0 := \{x \in K \mid v(x) = 0\} = (R_v)^*$$

die Einheitengruppe der Bewertung v. Sie ist identisch mit der Gruppe der Einheiten des Bewertungsrings R_v. Sei $\pi \in K$ ein Element mit $v(\pi) = 1$. Dann läßt sich jedes Element $x \in K^*$ auf genau eine Weise in der Gestalt

$$x = u \cdot \pi^n \text{ mit } u \in U_0 \text{ und } n := v(x) \in \mathbb{Z}$$

schreiben. Ein Element π mit $v(\pi) = 1$ heißt auch lokale Uniformisierende bezüglich v. Für jedes gebrochene Ideal I des Ringes R_v setzen wir

$$v(I) := \inf \{v(x) \mid x \in I\}$$

1.1.12 Die Ideale des Bewertungsrings R_v

Seien $v: K \to \mathbb{Z} \cup \{\infty\}$ eine diskrete Bewertung des Körpers K und $\pi \in R_v$. Dann gilt

(i) Das maximale Ideal des Bewertungsrings R_v wird von π erzeugt,

$$m_v := \pi R_v .$$

(ii) Die gebrochenen Ideale von R_v sind gerade die Ideale der Gestalt

$$I = \pi^n R_v \text{ mit } n \in \mathbb{Z}$$

(genauer ist $n = v(I)$).

Beweis. Zu (ii). Da $\pi^n R_v$ ein von Null verschiedener R_v-Teilmodul von K ist und die Multiplikation mit einer hohen Potenz von π ein Ideal von R_v liefert, ist $\pi^n R_v$ gebrochenes Ideal von R_v.

Sei jetzt umgekehrt I ein gebrochenes Ideal von R_v. Wir wählen ein Element $a \in R_v$ mit $aI \subseteq R_v$. Für jedes Element $x \in I$ gilt dann $ax \in R_v$, also

$$v(ax) \geq 0.$$

Sei jetzt $b = u \cdot \pi^n \in I$ ein Element, für welches v(xb) minimal wird. Dann gilt für jedes $a \in I$ die Ungleichung

$$0 \leq v(ax) - v(bx) = v(a/b),$$

d.h. $\frac{a}{b} \in R_v$ also $a \in bR_v$. Wir haben gezeigt

$$I \subseteq bR_v \subseteq I$$

(die zweite Inklusion gilt wegen $b \in I$). Damit ist aber $I = bR_v = \pi^n R_v$.

Zu (i). Das gebrochene Ideal $\pi^n R_v$ liegt genau dann in R_v, wenn $n \geq 0$ gilt, und ist genau dann echtes Ideal von R_v, wenn $n > 0$. Für $n=1$ erhalten wir also das maximale Ideal.

QED.

1.1.13 Der Begriff des diskreten Bewertungsrings

Ein diskreter Bewertungsring ist ein (nullteilerfreier) Hauptidealring[3] R mit genau einem von Null verschiedenen Primideal.

1.1.14 Charakterisierung der Ringe R_v

(i) Sei $v: K \to \mathbb{Z} \cup \{\infty\}$ eine diskrete Bewertung des Körpers K. Dann ist R_v ein diskreter Bewertungsring.

(ii) Zu jedem diskreten Bewertungsring R gibt es eine Bewertung v des Quotientenkörpers Q(R) mit $R = R_v$.

Beweis. Zu (i). Folgt aus 1.1.12 und der Definition von R_v in Bemerkung 1.1.6(i).

Zu (ii). Sei m das maximale Ideal von R. Da R ein Hauptidealring ist, gilt

$$m = \pi R$$

mit einem von Null verschiedenen Element $\pi \in R$. Da jedes Primelment ein von Null verschiedenes Primideal erzeugt, gibt es (bis auf Assozierte) in R nur ein Primelement, nämlich π.
Sei jetzt $x \in R-\{0\}$ beliebig. Die Primzerlegung von x hat die Gestalt

$$x = u \cdot \pi^n$$

mit einer eindeutig bestimmten nicht-negativen ganzen Zahl n und einer eindeutigbestimmten Einheit u von R.
Die Elemente $\neq 0$ des Quotientenkörpers K:= Q(R) habe damit die Gestalt

$$x = u \cdot \pi^n \text{ mit } n \in \mathbb{Z}.$$

Wir setzen

$$v(u \cdot \pi^n) := n \text{ und } v(0) := \infty.$$

Damit ist eine Bewertung von K definiert und es gilt

$$v(u \cdot \pi^n) \geq 0 \Leftrightarrow n \geq 0$$

d.h.

$$R_v = R.$$

Der Ring R ist somit wirklich von der behaupteten Gestalt.
QED.

1.1.15 Charakterisierung der Bewertungsringe

Sei R ein Integritätsbereich. Dann sind folgende Aussagen äquivalent.

(i) R ist ein Bewertungsring.

(ii) R ist noethersch[4], ganz abgeschlossen[5] und 1-dimensional[6] und lokal[7].

---

[3] R soll kommutativ sind und ein Einselement haben.

[4] Jedes Ideal wird von endlich vielen Elementen erzeugt.

[5] Jedes Element $x \in Q(R)$, welches einer Gleichung der Gestalt $x^n + a_1 x^{n-1} + \ldots + a_n = 0$ mit $a_1, \ldots, a_n \in R$ genügt, liegt selbst schon in R. Ein Element x aus einem den Ring R enthaltenden Ring, welches einer solchen Gleichung genügt, heißt ganz über R. Ganze Abgeschlossenheit bedeutet also, jedes über R ganze Element von Q(R) liegt selbst schon in R.

[6] Jedes von Null verschiedene Primideal ist maximal.

[7] Es gibt genau ein maximales Ideal.

Beweis.(i) $\Rightarrow$ (ii).
Wir haben bereits gesehen, ein Bewertungring ist ein Hauptidealring (also erst recht noethersch), ist 1-dimensional und lokal. Sei jetzt $x \in Q(R)-\{0\}$ ein Element mit

(*) $$x^n + a_1 x^{n-1} + \ldots + a_n = 0 \ , \ a_1, \ldots, a_n \in R.$$

Da R eine ZPE-Ring ist, können wir x in der Gestalt

$$x = \frac{a}{b}, \text{ a und b teilerfremd,}$$

schreiben. Einsetzen in die Identität (*) und Multiplizieren mit dem Hauptnenner liefert

$$a^n + a_1 a^{n-1} b + \ldots + a_n b^n = 0$$

Die Glieder auf der linken Seite sind mit Ausnahme des ersten sämtlich durch b teilbar, also ist auch a^n durch b teilbar. Da a und b teilerfremd sind, muß b eine Einheit sein. Also gilt $x = \frac{a}{b} \in R$.

(ii) $\Rightarrow$ (i). 1. Schritt. Für jedes gebrochene Ideal I von R gilt R(I) = R.
Zur Erinnerung, R(I) ist definiert als das gebrochene Ideal

$$R(I) := \{x \in K \mid xI \subseteq I\}.$$

Wegen $R \subseteq R(I)$ können wir R(I) auch als kommutativen Ring mit 1 ansehen. Für jedes $x \in R(I)$ gilt

$$R[x] \subseteq R(I).$$

Als gebrochenes Ideal ist R(I) ein endlich erzeugter R-Modul. Da R noethersch ist, ist dann aber auch der R-Teilmodul R[x] von R(I) endlich erzeugt,d.h. R[x] wird von endlich vielen Potenzen von x erzeugt. Insbesondere gibt es eine Potenz von x, welche eine R-Linearkombination niedrigerer Potenzen ist. Das bedeutet aber, x ist ganz über R. Da R ganz abgeschlossen ist, folgt $x \in R$. Wir haben damit gezeigt, R = R(I).

2. Schritt. Für das einzige von Null verschiedene Primideal m von R gilt $m^{-1} \neq R$.

Wir beachten zunächst, es gibt in R von Null verschiedene Ideal $I \subseteq R$ mit $I^{-1} \neq R$. Zum Beispiel kann man

$$I = aR$$

setzen mit $a \in m-\{0\}$. Dann liegt nämlich $\frac{1}{a} \in I^{-1}-R$.

Sei J maximal unter allen Ideal von R, für welche $I^{-1} \neq R$ gilt. Ein solches Ideal existiert, weil R noethersch ist. Zum Beweis der Aussage des zweiten Schrittes genügt es zu zeigen, J ist ein Primideal.

Seien $x,y \in R$ Elemente mit $xy \in J$ und $x \notin J$. Wir haben zu zeigen $y \in J$.

Dazu wählen wir ein Element $z \in J^{-1}-R$. Es gilt

$$zy(xR+J) \subseteq R,$$

also[8]

$$zy \in (xR+J)^{-1} \subseteq R$$

also

$$z(yR+J) \subseteq R$$

also $z \in (yR+J)^{-1}$. Insbesondere ist also $(yR+J)^{-1} \neq R$. Wegen der Maximalität von J kann (yR+J) nicht echt größer sein als J, d.h. es gilt $y \in J$. Damit ist gezeigt, J ist ein Primideal.

3. Schritt. $m \cdot m^{-1} = R$.

Nach dem 2. Schritt gilt $m^{-1} \supseteq R$, also

$$R \supseteq m \cdot m^{-1} \supseteq m \cdot R \supseteq m.$$

---

[8] Die Enthaltenseinsrelation ergibt aus der Maximalität von J und der Tatsache, daß xR+J echt größer ist als J.

Da m maximales Ideal von R ist, folgt $m \cdot m^{-1} = R$ oder $m \cdot m^{-1} = m$. Aus der zweiten Identität würde nach Definition von R(I) und dem ersten Schritt folgen

$$m^{-1} \subseteq R(m) = R$$

im Widersprung zu 2. Schritt. Also gilt $m \cdot m^{-1} = R$.

4. Schritt. $\cap_{n=1}^{\infty} m^n = 0$ (Durchschnittssatz von Krull).

Wegen des 3. Schrittes gilt $m^{-1} \cdot m^n \subseteq m^{n-1}$, also liegt

$$m^{-1} \cdot \cap_{n=1}^{\infty} m^n$$

in jeder Potenz von m, d.h. es gilt $m^{-1} \cdot \cap_{n=1}^{\infty} m^n \subseteq \cap_{n=1}^{\infty} m^n$ und damit

$$m^{-1} \subseteq R(\cap_{n=1}^{\infty} m^n).$$

Das mit dem 1. Schritt nur dann vereinbar, wenn $\cap_{n=1}^{\infty} m^n = 0$ gilt.

5. Schritt. m ist ein Hauptideal.

Wegen des 4. Schrittes muß m^2 echt kleiner sein als m. Wir wählen ein Element

$$\pi \in m - m^2.$$

Dann gilt

$$\pi m^{-1} \subseteq m \cdot m^{-1} \subseteq R.$$

Außerdem kann unmöglich $\pi m^{-1} \subseteq m$ gelten,denn dann wäre nach dem 3. Schritt

$$\pi \in \pi R = \pi m \cdot m^{-1} \subseteq m^2,$$

im Widerspruch zur Wahl von π. Da m das einzige maximale Ideal von R ist, folgt[9]

$$\pi m^{-1} = R.$$

Multiplikation dieser Identität mit m liefert nach dem 3.Schritt $\pi R = m$.

6. Schritt. Abschluß des Beweises.

Für jedes von Null verschiedene Element $a \in R$ gibt es nach dem 3.Schritt eine nicht-negative ganze Zahl n mit $a \in m^n - m^{n+1}$. Insbesondere gilt

$$a = u \cdot \pi^n \text{ für ein } u \in R - m.$$

Das Element u ist eine Einheit von R. Die Elemente von K:= Q(R) haben entsprechend die Gestalt

$$x = u \cdot \pi^n,\ n \in \mathbb{Z},\ u \text{ Einheit von } R,$$

und durch $v(u \cdot \pi^n) = n$ ist eine Bewertung von K definiert mit $R_v = R$. Mit anderen Worten R ist ein Bewertungsring.

QED.

1.1.16 Die Topologie von K und K*, Einheitengruppen

Seien $v: K \to \mathbb{Z} \cup \{\infty\}$ eine diskrete Bewertung des Körpers K und ρ eine reelle Zahl mit

$$0 < \rho < 1$$

Wir führen die multiplikative Bewertung

$$|x| = |x|_v := \rho^{v(x)}$$

und versehen K mit der durch diese Bewertung definierten Topologie. Es gilt

$$|x| < \rho^n \Leftrightarrow v(x) > n$$

---

[9] πm^{-1} liegt in R aber nicht in m.

$$|x| \leq \rho^n \Leftrightarrow v(x) \geq n$$

also

$$m^n = \{x \in K \mid |x| < \rho^{n-1}\} = \{x \in K \mid |x| \leq \rho^n\}.$$

Insbesondere sind die Potenzen

$$m^n, n \in \mathbb{Z},$$

offene und gleichzeitig abgeschlossenen Untergruppen der additiven Gruppe von K. Sie bilden eine Umgebungsbasis der $0 \in K$. Die Separiertheit der Topologie drückt sich dadurch aus, daß gilt

$$\cap_{n=0}^{\infty} m^n = 0.$$

Die Addition

$$K \times K \to K, (x,y) \mapsto x+y,$$

ist eine stetige Abbildung, denn es ist $(x+m^r)+(y+m^r) \subseteq (x+y)+m^r$.
Analog bilden die Untergruppen[10]

$$U_n := 1+m^n, n \geq 1,$$

der multiplikativen Gruppe K* von K eine Umgebungsbasis der 1. Die Separiertheit der Topologie von K* drückt sich dadurch aus, daß gilt

$$\cap_{n=0}^{\infty} (1+m^n) = 1.$$

Die Multiplikation

$$K^* \times K^* \to K^*, (x,y) \mapsto xy,$$

ist eine stetige Abbildung, denn es ist $(x+m^r)(y+m^r) \subseteq xy+m^r$. Die Elemente von U_n heißen n-Einheiten.

1.1.17 Einige Isomorphismen

Sei R ein diskreter Bewertungsring mit dem Quotientenkörper K, dem maximalen Ideal $m=\pi R$, dem Restklassenkörper $k := R/m$ und der Gruppe der n-Einheiten $U_n = 1 + m^n$.
Dann gilt:

(i) Die Multiplikation $R \to R$ mit π^n induziert einen Isomorphismus von k-Moduln

$$k \to m^n/m^{n+1}, c \mapsto (c\pi^n \bmod m^{n+1}).$$

(ii) Die natürliche Abbildung $R \to k$ induzierte einen Isomorphismus von multiplikativen abelschen Gruppen

$$U/U_1 \to k^*, u \mapsto (u \bmod m).$$

(iii) Die Abbildung $U_n \to m^n$, $u \mapsto u-1$, induziert einen Isomorphismus von abelschen Gruppen

$$U_n/U_{n+1} \to m^n/m^{n+1}.$$

(iv) Es gibt für jedes $n \geq 1$ einen Isomorphismus abelscher Gruppen

$$U_n/U_{n+1} \to k, u \mapsto \frac{u-1}{\pi^n}.$$

Beweis. Zu (i). Die die Multiplikation mit π^n induziert eine R-lineare Abbildung

---

[10] Dies sind tatsächlich Untergruppen: Es gilt $(1+m^n)\cdot(1+m^n)=1+m^n$ und jedes $x=1+a \in 1+m^n$ ist eine Einheit von R, d.h. es gibt eine $1+b \in R$ mit $1 = (1+a)(1+b) = 1 + a+b+ab$. Insbesondere ist $0 = a+b+ab$, also $b = a(-1-b) \in m^n$, d.h das Inverse zu $1+a$ liegt ebensfalls in $1+m^n$.

$$R \to m^n \to m^n/m^{n+1}.$$

Diese ist surjektiv, weil m^n von π^n erzeugt wird und hat als Kern die Vielfachen von π, d.h. m. Also induziert sie einen Isomorphismus $k = R/m \to m^n/m^{n+1}$.

Zu (ii). Die Einschränkung der natürlichen Abbildung $R \longrightarrow k$ auf U induziert einen Homomorphismus

$$U \to k^*$$

multiplikativer Gruppen. Dieser ist surjektiv. Zwei Einheiten $u,u' \in U$ haben genau dann dasselbe Bild, wenn sie sich um ein Element auf m unterscheiden, $u-u' \in m$. Insbesondere liegt u genau dann im Kern, wenn $u-1 \in m$ gilt. Mit anderen Worten,

$$\mathrm{Ker}(U \to k^*) = 1+m.$$

Die Behauptung folgt jetzt aus dem Homomorphiesatz.

Zu (iii). Wegen $U_n = 1 + m^n = 1+ \pi^n R$ ist die folgenden Abbildung wohldefiniert.

$$f: U_n \to k,\ 1+ r\cdot\pi^n \mapsto (r \bmod m).$$

Offensichtlich ist sie auch surjektiv. Für das Bild eines Produktes erhalten wir

$$\begin{aligned} f((1+ r\cdot\pi^n)(1+ s\cdot\pi^n)) &= f(1+(r+s)\pi^n+rs\cdot\pi^{2n}) \\ &= (r+s) \bmod m \\ &= f(1+ r\cdot\pi^n) + f(1+ s\cdot\pi^n). \end{aligned}$$

Mit anderen Worten, f ist ein Gruppenhomomorphismus. Berechnen wir den Kern von f. Es gilt

$$f(1+ r\cdot\pi^n) = 0 \Leftrightarrow r \in m \Leftrightarrow 1+ r\cdot\pi^n \in U_{n+1}.$$

Die Behauptung ist nun eine Folge des Homomorphiesatzes.
Zu (iv). Folgt aus (i) und (iii).
QED.

1.1.18 Inklusionen zwischen Einheitengruppen, Automorphismen

Sei R ein diskreter Bewertungsring mit dem Quotientenkörper K, dem maximalen Ideal $m=\pi R$, dem Restklassenkörper $k:= R/m$ und der Gruppe der n-Einheiten $U_n = 1 + m^n$.

Dann gilt:

(i) Hat k eine positive Charakteristik $\mathrm{char}(k) = p > 0$, so besteht für jedes $n \geq 1$ die Inklusion

$$U_n^p \subseteq U_{n+1}.$$

(ii) Ist K vollständig und i kein Vielfaches von char(k), so ist für jedes $n \geq 1$ die Abbildung

$$U_n \to U_n,\ u \mapsto u^i,$$

ein Automorphismus der Gruppe U_n.

Beweis. Zu (i). Betrachten wir den Isomorphismus

$$U_n/U_{n+1} \to k$$

abelscher Gruppen von 1.1.17(iv). Die Zusammensetzung

$$f: U_n \to U_n/U_{n+1} \to k$$

mit der natürlichen Abbildung $U_n \to U_n/U_{n+1}$ hat den Kern U_{n+1}. Die Abbildung f bildet das Produkt zweier Elemente in die Summen ihrer Bilder ab. Insbesondere wird die p-te Potenz eines Elementes in das p-fache des Bildes abgebildet, also in 0. Damit gilt

$$(U_n)^p \subseteq \mathrm{Ker}(f) = U_{n+1}.$$

Zu (ii). Wir betrachten weiter den Isomorphismus $U_n/U_{n+1} \to k$. Der Gruppenendomorphismus

(*) $$U_n/U_{n+1} \to U_n/U_{n+1},\ u \mapsto u^i,$$

entspricht bei diesem Isomorphismus der Multiplikationsabbildung $k \to k$ mit i. Da i nach Voraussetzung kein Vielfaches der Charakteristik von k ist, ist diese Multiplikationsabbildung ein Isomorphismus. Damit ist aber auch (*) ein Isomorphismus.
Der Homomorphismus

$$f:U_n \to U_n,\ u \mapsto u^i,$$

hat damit einen Kern, der in jeder der Gruppe U_j mit $j \geq n$ enthalten ist. Nach 1.1.16 ist f injektiv. Aus der Bijektivität von (*) folgt weiter, daß es für jedes $y \in U_j$ ein $x \in U_j$ gibt mit[11]

$$y\text{-}f(x) \in U_{j+1}.$$

Wendet man diese Aussage auf $y' := y\text{-}f(x)$ mit j+1 anstelle von j an, so erhält man durch Wiederholung dieses Schlusses für jedes $y \in U_n$ eine Folge von Elementen $x_j \in U_j$ mit

$$y\text{-}f(x_n + x_{n+1} + \ldots + x_j) \in U_{j+1} \text{ für } j = n, n+1, \ldots$$

Da die U_k eine Umgebungsbasis von 1 bilden und K vollständig ist, konvergiert die Reihe

$$\sum_{j=n}^{\infty} x_j = x$$

gegen ein Element $x \in U_n$ (man beachte U_n ist abgeschlossen). Außerdem gilt

$$f(x_n + x_{n+1} + \ldots + x_j) \to y \text{ für } j \to \infty.$$

Wegen $f(U_j) \subseteq U_j$ gilt $f(xU_j) \subseteq xU_j$ für jedes j, d.h. f ist stetig im Punkt s. Damit ist aber

$$f(x) = f(\lim_{j\to\infty} x_n + x_{n+1} + \ldots + x_j) = \lim_{j\to\infty} f(x_n + x_{n+1} + \ldots + x_j) = y.$$

Wir haben gezeigt, f ist surjektiv.
QED.

Bemerkungen zur Konvergenz der Reihe $\sum_{j=1}^{\infty} x_j$ in K und U.

Bezeichne $v:K \to \mathbb{Z} \cup \{\infty\}$ die diskrete Bewertung mit dem Bewertungsring R und

$$|x| := \rho^{v(x)},\ 0 < \rho < 1,$$

die eine zugehörige multiplikative Bewertung von K.

(i) Die Bewertung |x| ist nicht-archimedisch.

Es gilt $|x+y| = \rho^{v(x+y)} \leq \rho^{\min\{v(x),(y)\}} = \max\{|x|,|y|\}$.

(ii) Die Reihe $\sum_{j=1}^{\infty} x_j$ in K konvergiert genau dann, wenn $\{x_j\}$ eine Nullfolge ist.

---

[11] Die Gruppenoperation der abelschen Gruppe U wollen wir hier vorübergehend mit + bezeichnen und ihr inverses mit -. Diese beiden Gruppenoperationen sind natürlich gerade die Multiplikation und die Division des Körpers K.

Die Nullfolgeneigenschaft als Folge der Konvergenz der Reihe ist trivial. Zeigen wir die umgekehrt Implikation. Sei also $\{x_j\}$ ein Nullfolge. Und sein ein $\varepsilon>0$ vorgegeben. Wir haben zu zeigen, es gibt ein $N = N(\varepsilon)$ mit

$$|\sum_{j=m}^{n} x_j| < \varepsilon \text{ für alle m und n mit } n \geq m \geq N.$$

Da die Bewertung nicht-archimetisch ist, läßt sich die Summe links wie folgt abschätzen.

$$|\sum_{j=m}^{n} x_j| \leq \max\{|x_m|,...,|x_n|\}.$$

Da $\{x_j\}$ eine Nullfolge ist, läßt sich das Maximum rechts beliebig klein machen.

(iii) Die Differenz von je zwei Elementen $x,y \in U_n$ liegt in m^n. Ihr Abstand ist deshalb

$$|x-y| \leq |\pi|^n.$$

Dabei ist $q:= |\pi|$ eine reelle Zahl < 1. Insbesondere hat jedes Element $x \in U_1$ eine Abstand von 1,

$$|1-x| < 1.$$

Für $x,y \in U_1$ gilt

$$(1-x)(1-y) = 1- x - y + xy = (1-x)+(1-y) - (1-xy)$$

also

$$\begin{aligned} |1-xy| &= |(1-x)+(1-y) - (1-x)(1-y)| \\ &\leq \max\{|1-x|,|1-y|,|1-x|\cdot|1-y|\} \\ &\leq \max\{|1-x|,|1-y|\} \end{aligned}$$

Durch Iteration erhält man

(*) $$|1-x_1\cdot...\cdot x_n| \leq \max\{|1-x_j| , j=1,...,n\} \text{ für } x_j \in U_1$$

(vi) Im obigen Beweis ist die Reihe $\sum_{j=n}^{\infty} x_j$ in Wirklichkeit ein unendliches Produkt. Zum Beweis ihrer Konvergenz gehen wir zur multiplikativen Schreibweise über. Es gilt wegen $x_j \in U_j$ für $u \leq v$:

$$|\prod_{j=n}^{v} x_j - \prod_{j=n}^{u} x_j| = \prod_{j=n}^{u} |x_j| \cdot |1 - \prod_{j=u+1}^{v} x_j|$$

$$= |1- \prod_{j=u+1}^{v} x_j| \quad \text{(die Element von } U_1 \text{ haben den Wert 1)}$$

$$\leq \max\{|1-x_{u+1}|,...,|1-x_v|\}$$

Da die x_j gegen 1 konvergieren, kann man das Maximum rechts beliebig klein machen, indem man nur u und v hinreichend groß wählt. Also ist die Folge $\{\prod_{j=n}^{v} x_j\}$ eine Cauchy-Folge.

1.2 Dedekindsche Ringe

1.2.1 Bezeichnungen

In diesem Abschnitt bezeichne R einen Integritätsbereich und K dessen Quotientenkörper. Für jedes Primideal $p \subseteq R$ betrachten wir die Lokalisierung

$$R_p := \{\frac{r}{s} \mid r,s \in R,\ s \notin p\}$$

von R im Primideal p. R_p ist ein lokaler Ring mit dem maximalen Ideal pR_p. Ein gebrochenes Ideal I von R heißt umkehrbar, wenn $I \cdot I^{-1} = R$ gilt.

1.2.2 Relationen zwischen den Idealen von R und der Lokalisierung von R

Sei p ein Ideal des Integritätsbereiches R. Dann gilt:

(i) Es gilt $p = pR_p \cap R$ für jedes Primideal von p von R.

(ii) Für beliebige Ideale J von R_p gilt $(J \cap R)R_p = J$.

Beweis. Zu (i). Die Inklusion "$\subseteq$" ist trivial. Sei jetzt $x \in pR_p \cap R$, d.h. $x = \frac{r}{s}$ mit $r,s \in R$ und s nicht in p. Dann gilt $sx \in p$ und, da p Primideal ist, $x \in p$.

Zu (ii). Die Inklusion "$\subseteq$" ist trivial. Sei jetzt $\frac{r}{s} \in J$. Dann gilt $r \in J \cap R$, also $r \in (J \cap R)R_p$. Wegen $s \notin p$ ist s eine Einheit in R_p. Also gilt $\frac{r}{s} = \frac{1}{s} r \in (J \cap R)R_p$.

QED.

1.2.3 Charakterisierung der Dedekind-Ringe

Sei R ein Integritätsbereich. Dann sind folgende Aussagen äquivalent.

(i) R ist noethersch, ganz abgeschlossen und 1-dimensional.

(ii) R ist noethersch und für jedes von 0 verschiedene Primideal p ist R_p ein diskreter Bewertungsring.

(iii) Alle gebrochenen Ideal von R sind umkehrbar.

Ein Dedekind-Ring ist ein Integritätsbereich, der den obigen Bedingungen genügt.

Beispiel

Ein nullteilerfreier Haupidealring ist ein Dedekind-Ring, denn er genügt der Bedingung (iii).

Beweis der Äquivalenz von (i)-(iii).

(i) $\Rightarrow$ (ii). Sei p ein von Null verschiedenes Primideal. Wir werden gleich sehen, R_p ist ein lokaler Ring. Auf Grund der Charakterisierung 1.1.15 der Bewertungsringe, genügt es zu zeigen, die Eigenschaften von R, noethersch, ganzabgeschlossen und 1-dimensional zu sein, bleiben beim Übergang zu R_p erhalten.

Nach 1.2.2 (ii) hat jedes Ideal von R_p die Gestalt IR_p mit einem Ideal I von R. Da I von endlich vielen Elementen erzeugt wird, gilt dasselbe von IR_p, d.h. R_p ist noethersch.

Sei x ein Element aus dem Quotientenkörper von R_p, welches ganz ist über R_p, d.h. es gelte

$$x^n + b_1 x^{n-1} + \ldots + b_n = 0$$

für gewissen $b_i \in R_p$. Wir schreiben die b_i in der Gestalt $b_i := \frac{a_i}{b}$ mit $a_i, b \in R, b \notin p$ und erhalten durch Multiplikation der obigen Identität mit b^n:

$$(bx)^n + ba_1(bx)^{n-1} + \ldots + b^n b_n = 0.$$

Mit anderern Worten, bx ist ganz über R, liegt also schon selbst in R. Wegen $b \notin p$ gilt dann aber auch $x = \frac{bx}{b} \in R_p$. Wir haben gezeigt , R_p ist ganzabgeschlossen.

Sei jetzt J ein von Null verschiedenes Primideal von R_p. Dann ist $J \cap R$ ein Primideal von R, welches nach 1.2.2 von Null verschieden ist. Da jedes Element von $R_p - pR_p$ eine Einheit ist, gilt $J \subseteq pR_p$, also nach 1.2.2

$$J \cap R \subseteq pR_p \cap R = p$$

Da R nach Voraussetzung 1-dimensional ist, folgt $J \cap R = p$, also nach 1.2.2

$$J = (J \cap R)R_p = pR_p.$$

Wir haben gezeigt, pR_p ist das einzige von Null verschiedene Primideal von R_p Insbesondere ist R_p 1-dimensional und lokal, also ein diskreter Bewertungsring.

(ii) $\Rightarrow$ (iii). Sei I ein gebrochenes Ideal von R mit den Erzeugenden Elementen $a_1,...,a_n$. Für jedes von Null verschiedene Primideal p von R bezeiche v_p die Bewertung zum Bewertungsring R_p. Wir wählen ein i mit

$$v_p(a_i) = \inf \{v_p(x) \mid x \in I\}$$

Ein solches i existiert, da I von den a_i erzeugt wird. Der Einfachheit halber nehmen wir an, es sei i = 1. Dann gilt

$$IR_p = a_1 R_p.$$

Insbesondere ist

$$\frac{a_i}{a_1} = \frac{x_i}{y_i}, \; x_i, y_i \in R, \; y_i \notin p.$$

Wir setzen

$$y := \prod_i y_i .$$

Dann gilt $ya_1^{-1}a_i \in R$ für alle i, also $ya_1^{-1} \in I^{-1}$, also $y \in a_1 I^{-1} \subseteq I \cdot I^{-1}$. Nach Konstruktion liegt aber y nicht in p, d.h. $I \cdot I^{-1}$ liegt nicht in p. Da dies für alle maximalen Ideal p gilt, folgt $I \cdot I^{-1} = R$.

(iii) $\Rightarrow$ (i). Sei I eine gebrochenes Ideal von R. Dann existieren Elemente $a_1,...,a_n \in I$ und $b_1,...,b_n \in I^{-1}$ mit $\sum_i a_i b_i = 1$. Für jedes $x \in I$ ergibt sich

$$x = \sum_i a_i(xb_i) \text{ wobei } xb_i \in R$$

gilt. Also erzeugen die Elemente $a_1,...,a_n$ das Ideal I. Wir haben gezeigt, I ist noethersch.

Sei jetzt $x \in K := Q(R)$ ganz über R. Dann ist nach 1.1.5 die Menge S := R[x] ein gebrochenes Ideal. Außerdem ist R[x] ein Ring, d.h. es gilt SS = S. Damit ist aber auch

$$S = SR = SSS^{-1} = SS^{-1} = R.$$

Insbesondere liegt x in R. Wir haben gezeigt, R ist ganz abgeschlossen.

Seien jetzt I ein von Null verschiedenes Primideal und p ein maximales Ideal, welches I enthält. Dann ist Ip^{-1} ein Ideal von R und $(Ip^{-1})p = I$. Da I ein Primideal sein soll, folgt

(*) $$(Ip^{-1}) \subseteq I \text{ oder } p \subseteq I.$$

Aus der ersten Inklusion würde folgen,

$$p^{-1} = I^{-1}Ip^{-1} \subseteq I^{-1}I = R,$$

d.h. $p^{-1} = R$, also $p = pR = pp^{-1} = R$ im Widerspruch zur Wahl von R. Wir haben gezeigt, in (*) kann die ersten Inklusion nicht gelten. Also gilt die zweite, d.h. es ist $I = p$.
QED.

1.2.4 Bezeichnung

Für jedes von Null verschiedene Primideal p eines Dedekind-Ringes R bezeichne v_p die zum Ring R_p gehörige Bewertung von **Q**(R).

1.2.5 Die multiplikativen Bewertungen eines Dedekind-Rings

Seien R ein Dedekind-Ring mit dem Quotientenkörper K und |?| eine nicht-triviale multiplikative Bewertung von K mit

$$|r| \le 1 \text{ für alle } r \in R.$$

Dann gibt es eine reelle Zahl ρ mit $0 < \rho < 1$ und ein von Null verschiedenes Primideal p von R mit

$$|x| = \rho^{v_p(x)} \text{ für alle } x \in K.$$

Beweis. Wir können annehmen, die Dreieckungleichung gilt für die Bewertung. Die Voraussetzung $|r| \le 1$ für alle $r \in R$ impliziert, daß insbesondere

$$|n \cdot 1_K| \le 1$$

gilt für n=1,2,3,..., d.h. die Bewertung ist nicht-archimedisch[12]. Insbesondere gilt

$$|x+y| \le \max\{|x|,|y|\}$$

für beliebige $x,y \in K$. Die Menge

$$p := \{x \in R \mid |x| < 1\}$$

ist deshalb ein Primideal von R. Weil die Bewertung nicht-trivial ist, gibt es ein von Null verschiedenes $x = \frac{a}{b} \in K$ mit $a,b \in R$, $|x| < 1$. Dann gilt aber auch $|a| < |ax| = |b| \le 1$, d.h. a ist ein von Null verschiedenes Element von p. Insbesondere ist p vom Nullideal verschieden.

Nach (1.2.3)(ii) ist der lokale Ring

$$R_p$$

ein diskreter Bewertungsring. Nach Konstruktion gilt

$$R_p \subseteq \{x \in K \mid |x| \le 1\}.$$

Zeigen wir, es gilt sogar das Gleichheitszeichen. Sei umgekehrt $x \in K$ ein Element mit

$$|x| \le 1.$$

Da R_p ein diskreter Bewertungsring mit dem Quotientenkörper K ist, gilt $x \in R_p$ oder $x^{-1} \in R_p$. Im zweiten Fall wäre $|x^{-1}| \le 1$, also $|x| = 1$. Schreiben wir x in der Gestalt

$$x^{-1} = \frac{a}{b},\ a \in R,\ b \in R\text{-}p.$$

Wegen $|x| = 1$ und $b \notin p$ gilt $|a| = |b| = 1$, also $a \notin p$. Damit ist aber auch $x = \frac{b}{a}$ ein Element von R_p. Damit ist gezeigt,

---

[12] Es reicht zu zeigen, $|1+x| \le 1$ für jedes $x \in K$ mit $|x| \le 1$. Auf jeden Fall gilt

$$|1+x|^n = \left|\sum_{j=0}^{n} \binom{n}{j} x^j\right| = \sum_{j=0}^{n} \left|\binom{n}{j} \cdot 1_K\right| \cdot |x^j| = \sum_{j=0}^{n} |x^j| \le n+1$$

Wir ziehen die n-te Wurzel und lassen n gegen Null gehen und erhalten $|1+x| \le 1$, d.h. wir haben eine Bewertung mit C=1 vorliegen.

$$R_p = \{x \in K \mid |x| \leq 1\}.$$

Nach Definition von p gilt weiter

$$pR_p \subseteq \{x \in K \mid |x| < 1\}.$$

Zeigen wir, es gilt sogar das Gleichheitszeichen. Sei $x \in K$ ein Element mit $|x|<1$. Dann liegt x^{-1} nicht in R_p, d.h. x ist keine Einheit von R_p. Dann ist aber $x \in R_p$. Damit ist gezeigt,

$$pR_p = \{x \in K \mid |x| < 1\}.$$

Sei jetzt π ein Uniformisierende von R_p. Wir setzten

$$\rho = |\pi|.$$

Jedes Element $x \in K$ hat die Gestalt $x = u \cdot \pi^{v(x)}$, wobei $v = v_p$ die Bewertung zum Ring R_p bezeichne. Damit gilt

$$|x| = |u| \cdot |\pi|^{v(x)} = 1 \cdot \rho^{v(x)}.$$

QED.

1.2.6 Zerlegung in Primfaktoren

Sei R ein Dedekind-Ring. Dann gilt:

(i) Die gebrochenen Ideale von R bilden eine abelschen Gruppe Div(R) bezüglich der Multiplikation.

(ii) Die maximalen Ideale von R bilden ein freies Erzeugendensystem von Div(R).

(iii) Jedes gebrochene Ideal I von R hat die folgende Darstellung als Linearkombination von maximalen Idealen.

$$I = \prod_p p^{v_p(I)}$$

(iv) Es gilt

$$IR_p = (pR_p)^{v_p(I)}$$

für jedes gebrochene Ideal I und jedes Primideal p von R.

(v) Die Abbildung

$$\mathrm{Div}(R) \longrightarrow \oplus_p \mathrm{Div}(R_p)\,,\ I \mapsto (IR_p)_p\,,$$

wobei auf der rechten Seite die direkte Summe über alle maximalen Ideal von R erstreckt wird, ist ein Isomorphismus von abelschen Gruppen.

Zur Erinnerung, wir hatten definiert,

$$v_p(I) := \inf \{v_p(x) \mid x \in I\}.$$

Beweis. Zu (i). Nach (1.1.4) ist das Produkt von gebrochenen Idealen und das Inverse eines gebrochenen Ideals wieder ein gebrochenes Ideal. Nach (1.1.3) ist das Produkt kommutativ und assoziativ. Nach (1.2.3)(iii) ist das Inverse eines gebrochenen Ideals auch das Inverse im Sinne der Gruppentheorie.

Zu (ii). Wir zeigen zunächst, die maximalen Ideale erzeugen Div(R). Dazu genügt es zu zeigen, jedes gebrochene Ideal I ist Produkt von ganzzahligen Potenzen von maximalen Idealen. Wegen $aI \subseteq R$ für ein von Null verschiedenes $a \in R$ genügt es zu zeigen, die Ideale aI und aR sind Produkte von maximalen Idealen. OBdA können wir also annehmen, $I \subseteq R$ ist ein Ideal. Dann gibt es ein maximales Ideal p von R mit

$$I \subseteq p.$$

Insbesondere gilt

$$I = p(Ip^{-1}) \text{ und } I \subset Ip^{-1} \subseteq R.$$

Man beachte die Inklusion $I \subset Ip^{-1}$ ist echt, denn aus $I=Ip^{-1}$ folgte $p = I \cdot I^{-1} = R$. Falls Ip^{-1} ein echtes Ideal von R ist, können wir den eben durchgeführten Schluß mit Ip^{-1} anstelle von I wiederholen. Da R noethersch ist, ergibt daraus die Darstellbarkeit jedes Ideals als Produkt von maximalen Idealen.
Beweisen wir, die maximalen Ideale bilden ein freies Erzeugendensystem. Für beliebige gebrochene Ideal I,J von R und beliebige Primideale p gilt

$$(IR_p)\cdot(JR_p) = (IJ)R_p.$$

Mit anderen Worten, die Abbildung

$$f_p : \mathrm{Div}(R) \to \mathrm{Div}(R_p),\ I \mapsto IR_p,$$

ist ein Homomorphismus abelscher Gruppen.
Seien jetzt p und p' zwei verschiedene maximale Ideale von R. Dann gilt

$$p'R_p = R_p.$$

Mit anderen Worten, jedes von p verschiedene maximale Ideal liegt im Kern von f_p. Sei jetzt I ein gebrochenes Ideal von R und

$$I = \prod_p p^{r_p}$$

eine Darstellung von I als Linearkombination von maximalen Idealen. Wir wenden f_p an und erhalten

$$IR_p = p^{r_p} R_p$$

also $r_p = v_p(IR_p) = v_p(I) + v_p(R_p) = v_p(I)$. Insbesondere ist die Darstellung von I als Linearkombination von maximalen Idealen eindeutig.
Zu (iii),(iv) und (v). siehe Beweis von (ii).
QED.

1.2.7 Verschwinden des Wertes eines Elements an fast allen Stellen

Seien R ein Dedekind-Ring und $a \in K^*$ beliebig. Dann gilt

$$v_p(a) = 0$$

für fast alle Primideale p von R, d.h. für alle mit Ausnahme von endlich vielen.
Beweis. Nach (1.2.6) ist aR Produkt von endlich vielen Primidealen. Also ist

$$v_p(a) = v_p(aR)$$

nur für endlich viele p ungleich Null.
QED.

1.2.8 Bewertungen als Funktionen auf der Menge der gebrochenen Ideale

Seien R ein Dedekind-Ring und $p \subseteq R$ ein maximales Ideal von R. Dann gilt für gebrochene Ideale I,J von R:

(i) $v_p(I\cdot J) = v_p(I)v_p(J)$.

(ii) $v_p(I^{-1}) = -v_p(I)$.

(iii) $v_p(I+J) = \inf\{v_p(I), v_p(J)\}$.

(iv) $v_p(I \cap J) = \sup\{v_p(I), v_p(J)\}$.

Beweis. einfach.
QED.

1.3 Moduln und Bilinearformen

1.3.0 Gegenstand des Abschnitts

In diesem Abschnitt führen wir einige Begriffe ein, die wir später bei der Definition der Ideal-Norm und der Diskriminante einer Erweiterung von Dedekind-Ringen benötigen.

1.3.1 Bezeichnungen

R	ein Dedekind-Ring
K	Quotientenkörper von R
U	endlich-dimensionaler Vektorraum über K
n	$:= \dim_K U$ (>0)
T	R-Teilmodul von U, welcher eine K-Basis von U enthält.
L,M,N	endlich erzeugte R-Teilmoduln von U, welche eine K-Basis von U enthalten (Gitter).
T_p	$:= TR_p$ für maximale Ideale $p \subseteq R$.
$\Omega(R)$	Menge der maximalen Ideale von R.
$B: U \times U \to K$	eine nicht-entartete symmetrische Bilinearform (ab 1.3.8)

1.3.2 Durchschnittsatz von Krull

$$\bigcap_{p \in \Omega(R)} T_p = T$$

Beweis. Trivialerweise gilt $\supseteq$. Beweisen wir die umgekehrte Inklusion. Sei

$$u \in \bigcap_{p \in \Omega(R)} T_p$$

Wir betrachten das Ideal

$$J_u := \{x \in R \mid xu \in T\}.$$

Es genügt zu zeigen, $J_u = R$, d.h. J_u ist in keinem maximalen Ideal p von R enthalten. Um das einzusehen, schreiben wir

$$u = \frac{w}{x} \text{ mit } w \in T,\ x \in R-p.$$

Dann gilt $xu = w \in T$, also $x \in J_u$, also liegt J_u nicht in p.

QED.

1.3.3 Relationen zwischen Gittern von U

Für je zwei Gitter M und N von U gibt es ein $a \in K^*$ mit $aM \subseteq N$.

Beweis. Seien $\{u_i\}$ eine Basis des K-Vektorraums U, welche ganz im R-Modul N liegt, und $\{w_j\}$ ein (endliches) Erzeugendensystem von M. Wir schreiben

$$w_j = \sum_k c_{jk} u_k\ ,\ c_{jk} \in K.$$

Wir wählen ein $a \in R-\{0\}$ mit $a \cdot c_{jk} \in R$. Dann gilt $a \cdot w_j \in N$ für alle j, also $aM \subseteq N$.

QED.

1.3.4 Gleichheit fast aller Lokalisierungen von Gittern

Seien M und N zwei Gitter von U. Dann gilt

$$M_p = N_p$$

für fast alle maximalen Ideale p von R.

Beweis. Wir wählen Elemente $a,b \in K^*$ mit

$$aM \subseteq N \subseteq bM.$$

Die Elemente a, b sind genau dann Einheiten des Ringes R_p, wenn $v_p(a) = v_p(b) = 0$ gilt. Das ist nach 1.2.6 für fast alle p der Fall. Für fast alle p gilt deshalb

$$MR_p = aMR_p \subseteq NR_p \subseteq bMR_p = MR_p$$

QED.

1.3.5 Der (relative) Index zweier Gitter

Seien M und N zwei Gitter von U.

1. Fall. M und N sind freie R-Moduln.

Da M und N über K denselben endlich-dimensionalen Vektorraum U erzeugen, haben sie als freie R-Moduln denselben Rang. Es gibt also einen K-linearen Automorphismus

$$A: U \to U$$

mit

$$A(M) = N.$$

Je zwei solche Automorphismen unterscheiden sich um einen Automorphismus von N. Die Determinante von A ist deshalb bis auf eine Einheit von R eindeutig bestimmt. Das von der Determinante von A erzeugte Ideal,

$$(M:N) := \det(A)R,$$

deshalb eindeutig bestimmt und hängt nur von M und N ab.

2. Fall. M und N beliebige Gitter.

Für jedes maximale Ideal p von R sind M_p und N_p freie R_p-Moduln[13], also ist

$$(M_p:N_p)$$

wohldefiniert. Im Fall $M_p = N_p$ ist insbesonder $(M_p:N_p) = R_p$. Nach 1.2.6 gibt es genau ein gebrochenes Ideal (M:N) mit

$$(M:N)R_p = (M_p:N_p)$$

für alle $p \in R$.

Bemerkung

Im Fall $R=\mathbb{Z}$ und $M \supseteq N$ ist (M:N) der gewöhnliche Index ineinander liegender Gitter. Das ergibt sich zum Beispiel aus der nachfolgenden Eigenschaften des Index.

1.3.6 Eigenschaften des Index

(i) $(M:N)(N:L) = (M:L)$
(ii) $(M:M) = R$
(iii) $M \supseteq N \Rightarrow (M:N) \subseteq R$
(iv) $M \supseteq N$ und $(M:N) = R \Rightarrow M=N$

Beweis. Im Fall diskreter Bewertungsringe sind die Aussagen trivial. Im allgemeinen Fall ergeben sie sich mit Hilfe von 1.2.6 aus diesem Spezialfall.
QED.

1.3.7 Invarianz bei Automorphismen

Seien $A:U \to U$ ein Automorphismus des K-Vektorraumes U und $M,N \subseteq U$ zwei Gitter. Dann gilt

$$(A(M):A(N)) = (M:N).$$

Beweis. Es reicht, die Aussage im lokalen Fall zu beweisen. Wir wählen einen Automorphismus $L:U \to U$ mit $L(M) = N$. Dann gilt nach Definition

$$(M:N) = \det(L)R.$$

Weiter ist $ALA^{-1}(AM) = AN$, also

$$(A(M):A(N)) = \det(A)\det(L)\det(A)^{-1}R = \det(L)R.$$

---

[13] Man wähle ein minimales Erzeugendensystem des betrachteten Moduls. Gäbe es eine lineare Abhängigkeit zwischen den Erzeugenden, so könnte man die Koeffizienten so durch eine gemeinsame Potenz eines Parameters teilen, daß ein Koeffizient eine Einheit würde. Dann wäre aber das Erzeugendensystem nicht minimal.

QED.

1.3.8 Das Dual eines Gitters

Im folgenden sei U ein K-Vektorraum mit Skalarprodukt,

$$B: U\times U \to K,$$

d.h. B sei eine nicht-entartete symmetrische Bilinearform. Wir werden, wenn wir betonen wollen,daß U mit einem Skalarprodukt versehen ist, auch von einem euklidischen Vektorraum U sprechen. Zu jeder Basis $\{u_i\}$ von U gibt es dann eine eindeutig bestimmte duale Basis, d.h. eine Basis $\{\check{u}_i\}$ von U mit

$$B(u_i,\check{u}_j) = \delta_{ij}$$

für alle i und j. Für jeden R-Teilmodul von $T\subseteq U$, welcher U über K erzeugt, definieren wir den zu T dualen Modul,

$$D(T) := D_R(T) := \{u\in U \mid B(u,T)\subseteq R\}.$$

1.3.9 Das Dual eines freien Gitters

Sei M ein freies Gitter mit der (freien) Basis $\{u_i\}$. Dann gilt:

(i) D(M) ist ein freies Gitter mit der (freien) Basis $\{\check{u}_i\}$.

(ii) D(D(M)) = M.

Beweis. Es genügt, (i) zu beweisen. Wir schreiben $u\in U$ als Linearkombination der $\check{u}_i$,

$$u = \sum_i c_i\check{u}_i .$$

Dann gilt

$$\begin{aligned} u\in D(M) &\Leftrightarrow B(u,M)\subseteq R \\ &\Leftrightarrow B(u,u_j)\in R \text{ für alle } j \\ &\Leftrightarrow \sum_i c_i B(\check{u}_i,u_j)\in R \text{ für alle } j \\ &\Leftrightarrow c_j\in R \text{ für alle } j \end{aligned}$$

QED.

1.3.10 Eigenschaften des Duals

Seien M,N R-Gitter des euklidischen K-Vektorraums U und p ein maximales Ideal von R. Dann gilt:

(i) D(M) ist ein Gitter von U.

(ii) $D(M)R_p = D_{R_p}(M_p)$.

(iii) $D(M) = \cap_{q\in\Omega(R)} D(M_q)$

(iv) D(D(M)) = M.

(v) (D(M):D(N)) = (N:M).

Beweis. Zu (i). Wir haben zu zeigen, D(M) ist wieder endlich erzeugt über R und erzeugt über K den Vektorraum U. Zu Beweis wählen wir ein freies Gitter

$$F \subseteq M.$$

Ein solches existiert, weil M über K den Vektorraum U erzeugt, also eine Basis von U enthält. Nach Definition des Duals gilt

$$D(F) \supseteq D(M).$$

Da D(F) nach 1.3.8 endliche erzeugt ist, gilt dasselbe für den Teilmodul D(M). Nach 1.3.3 gibt es ein $a\in K^*$ mit $aM\subseteq F$, d.h. es ist

$$M \subseteq \frac{1}{a} F,$$

also $D(M) \supseteq D(\frac{1}{a} F)$. Nun ist $\frac{1}{a} F$ ein freies Gitter, so daß nach 1.3.8 auch $D(\frac{1}{a} F)$ ein freies Gitter ist, also eine Basis von U enthält. Dann enthält der größere Modul D(M) auch eine Basis von U. Wir haben gezeigt, D(M) ist ein Gitter.
Zu (ii). Nach Definition von $D(M_p)$ und auf Grund der Bilinearität von B gilt

$$B(D(M)R_p, M_p) \subseteq B(D(M),M)R_p \subseteq R_p .$$

Also besteht die Inklusion

$$D(M)R_p \subseteq D_{R_p}(M_p).$$

Zu Beweis der umgekehrten Inklusion wählen wir ein endliches Erzeugendensystem $\{w_i\}$ von M. Für jedes $v \in D_{R_p}(M_p)$ gilt $B(v, w_i) \in R_p$, d.h.

$$B(v, w_i) = \frac{a_i}{b} \text{ mit } a_i \in R, b \in R\text{-}p.$$

Dann gilt aber $B(bv,w_i) \in R$, also $B(bv, M) \subseteq R$, also $bv \in D(M)$, also

$$v \in D(M)R_p.$$

Zu (iii). Folgt aus (ii) und 1.2.6.
Zu (iv). Folgt aus 1.3.9 und 1.2.6.
Zu (v). Auf Grund von 1.2.6 und (ii) können wir annehmen, R ist ein diskreter Bewertungsring und M und N sind frei. Wir wählen einen linearen Automoprhismus

$$A: U \to U \text{ mit } A(N) = M.$$

Dann gilt

$$[N:M] = \det(A)R.$$

Wir wählen freie Basen $\{u_i\}$ und $\{v_i\}$ von M und N und bezeichnen mit $\{\check{u}_i\}$ bzw. $\{\check{v}_i\}$ die zugehörigen dualen Basen von D(M) und D(N). Wegen A(N) = M können wir annehmen

$$A(v_i) = u_i \text{ für jedes } i.$$

Sei $A^*: U \to U$ der zu A adjungierte Operator, d.h. die lineare Abbildung mit

$$(*) \qquad B(A^*u,u') = B(u,Au')$$

für alle $u,u' \in U$. Dann gilt

$$B(A^*(\check{u}_i), v_j) = B(\check{u}_i, A(v_j)) = B(\check{u}_i, u_j) = \delta_{ij}$$

also $A^*(\check{u}_i) = \check{v}_i$, also $A^*(D(M)) = D(N)$, also

$$(D(M):D(N)) = \det(A^*)R.$$

Es reicht also, wenn wir zeigen, $\det(A) = \det(A^*)$. Wir bestimmen dazu die Matrizen von A und A^* bezüglich der Basis $\{u_i\}$ bzw. $\{\check{u}_i\}$. Es wir schreiben

$$Au_i = \sum_j c_{ij} u_j \text{ und } A^*\check{u}_i = \sum_j d_{ij} \check{u}_j \text{ mit } c_{ij}, d_{ij} \in K.$$

Dann gilt

$$c_{ij} = B(Au_i, \check{u}_j) = B(u_i, A^*\check{u}_j) = B(A^*\check{u}_j, u_i) = d_{ji} .$$

Mit anderen Worten, die Matrix von A bzgl. der Basis $\{u_i\}$ ist transponiert zur Matrix von A^* bzgl. der Basis $\{\check{u}_i\}$. Da die Determinante nicht von der Wahl der Basis abhängt, folgt $\det(A) = \det(A^*)$.
QED.

1.3.11 Die Diskriminante eines Gitters

Sei M ein R-Gitter des euklidischen K-Vektorraum U. Dann heißt

$$\delta(M) := \mathrm{discr}(M) := (D(M):M)$$

Diskriminante von M über R.

1.3.12 Eigenschaften der Diskriminante

Seien M und N R-Gitter des euklidischen K-Vektorraum U und p ein maximales Ideal von R. Dann gilt

(i) $\mathrm{discr}(N) = \mathrm{discr}(M)\cdot(M:N)^2$.

(ii) $\mathrm{discr}_{R_p}(MR_p) = \mathrm{discr}_R(M)R_p$.

(iii) Klassische Definition über $\mathbb{Z}$. Ist M ein freies Gitter mit der Basis $\{u_i\}$, so ist discr(M) das von der Determinante

$$\det(B(u_i,u_j))$$

der Skalarprodukte $B(u_i,u_j)$ erzeugte gebrochene Ideal.

(iv) Im Fall $M \supseteq N$ gilt $\mathrm{discr}(M) \supseteq \mathrm{discr}(N)$ und die Gleichheit rechts ist äquivalent zur Gleichheit links.

Beweis. Zu (i). Es gilt

$$\begin{aligned} \mathrm{discr}(N) &= (D(N):N) && \text{(Definition 1.3.11)}\\ &= (D(N):D(M))\cdot(D(M):M)\cdot(M:N) && \text{(nach 1.3.6)}\\ &= (M:N)^2\cdot\mathrm{discr}(M) && \text{(nach 1.3.10)} \end{aligned}$$

Zu (ii). Gilt nach Definition 1.3.5 und 1.3.10(ii).

Zu (iii). Sei $\{v_i\}$ die zu $\{u_i\}$ duale Basis. Wir betrachten die lineare Abbildung

$$A: U \to U,\ v_i \mapsto u_i .$$

Nach Konstruktion gilt A(D(M)) = M, also

$$\mathrm{discr}(M) = \det(A)R.$$

Berechnen wir die Determinante von A bezüglich der Basis $\{v_i\}$. Sei

$$Av_i = u_i = \sum_{j=1}^{n} a_{ij}v_j$$

Dann ist

$$a_{ij} = B(\sum_{j=1}^{n} a_{ij}v_j\ ,\ u_j) = B(u_i\ ,\ u_j)$$

also $\det A = \det(B(u_i\ ,\ u_j))$ wie behauptet.

Zu (iv). Im Fall $M \supseteq N$ gilt $(M:N)\subseteq R$, d.h. der erste Teil der Behauptung folgt aus (i). Die Gleichheit discr(M)= discr(N) ist nach (i) äquivalent zu $(M:N)^2=R$, d.h. zu (M:N)=R. Nach 1.3.6(iv) ist letzteres aber äquivalent zu M =N:
QED.

1.3.13 Verhalten bei direkten Summen

Sei $U = U'\oplus U''$ eine orthogonale direkte Summe der Unterräume U',U''. Dann gilt für Gitter M',N' von U' und M'', N'' von U'':

(i) $(M'\oplus M'':N'\oplus N'') = (M':N')\cdot(M'':N'')$.

(ii) $D(M'\oplus M'') = D(M')+D(M'')$.

(iii) $\mathrm{discr}(M'\oplus M'') = \mathrm{discr}(M')\cdot\mathrm{discr}(M'')$.

Beweis. Es genügt, die Identitäten lokal zu beweisen, d.h. für freie Gitter.

Zu (i). Für freie Gitter folgt die Identität dem Produktsatz für Determinanten,

$$\det\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} = \det\left(\begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}\cdot\begin{pmatrix} 1 & 0 \\ 0 & B \end{pmatrix}\right) = \det\begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}\cdot\det\begin{pmatrix} 1 & 0 \\ 0 & B \end{pmatrix} = \det(A)\cdot\det(B).$$

Zu (ii). Sind $\{e'_i\}$ und $\{e''_i\}$ Basen der freien Gitter M' und M'' und sind $\{f'_i\}$ und $\{f''_i\}$ die zugehörigen dualen Basen. Dann ist $\{f'_i\}\cup\{f''_i\}$ duale Basis zu $\{e'_i\}\cup\{e''_i\}$.

Zu (iii). Es gilt

$$\begin{aligned} \mathrm{discr}(M'\oplus M'') &= (D(M'\oplus M''):M'\oplus M'') \quad \text{(nach Definition)} \\ &= (D(M')\oplus D(M''):M'\oplus M'') \quad \text{(nach (ii))} \\ &= (D(M'):M')\cdot(D(M''):M'') \quad \text{(nach (i))} \\ &= \mathrm{discr}(M')\cdot\mathrm{discr}(M'') \quad \text{(nach Definition).} \end{aligned}$$

QED.

1.3.14 Verhalten bei Erweiterungen

Sei $R\subseteq\bar{R}$ eine Erweiterung von Dedekind-Ringen. Wir setzten

$$\bar{K} := Q(\bar{R})$$

$$\bar{U} := U\otimes_K\bar{K}$$

und denken uns B: $U\times U \to K$ bilinear auf $\bar{U}$ fortgesetzt. Dann gilt für Gitter M,N von U:

(i) $(M\bar{R}:N\bar{R}) = (M:N)\bar{R}$.

(ii) $D(M\bar{R}) = D(M)\bar{R}$.

(iii) $\mathrm{discr}(M\bar{R}) = \mathrm{discr}(M)\bar{R}$.

Beweis. Es genügt, die Identitäten lokal in den maximalen Idealen $\bar{p}$ von $\bar{R}$ zu überprüfen. Ist $\bar{p}\cap R$ maximal in R, so reduziert dies die Behauptung auf den Fall, daß R und $\bar{R}$ Dedekind-Ringe und M,N freie R-Moduln sind. Ist $p = \bar{p}\cap R$ nicht maximal, so ist R_p ein Körper, also $MR_p = NR_p = U$ und die zu beweisenden lokalen Identitäten sind trivial. Damit genügt es, die Behauptung für freie Moduln M und N zu beweisen. In diesem Fall ergeben sich aber die Identitäten aus der jeweiligen expliziten Beschreibung der beteiligten Moduln.
QED.

1.4 Erweiterungen

1.4.1 Die Situation

R	ein Dedekind-Ring
K	:= Q(R), Quotientenkörper von R
L	ein endlicher separabler Erweiterungskörper von K
S	die ganze Abschließung von R in L (d.h. der Ring der Elemente von L, welche ganz über R sind).
$\mathrm{Tr}_{L/K}: L \to K$	Spurabbildung.

$B: L\times L \to K, (u,v) \mapsto Tr_{L/K}(uv)$, Die im folgenden verwendete Bilinearform. Da L/K separabel sein soll, ist B nicht entartet.

Bemerkungen

(i) S ist tatsächlich ein Ring.
(ii) Der Ring S ist ganz abgeschlossen in L.
(iii) Für jedes Primideal p von R ist SR_p die ganze Abschließung von R_p in L.
(iv) Sind $p\subseteq R$ und $P\subseteq S$ Primideale, so sagen wir, P liegt über p, falls gilt
$$p = R\cap P.$$
(v) Die Separabilität der Erweiterung $K \subseteq L$ wird nicht für alle Aussagen dieses Abschnitts gebraucht. Wir werden uns jedoch nicht mit dem inseparablen Fall befassen.

Beweis von (i)-(iii).

Zu (i). Für $x,y\in S$ sind R[x] und R[y] endlich erzeugte R-Moduln. Also ist R[x,y] endlich erzeugter Modul über R[x], also über R. Dann sich aber die Element $x+y$, $x\cdot y\in R[x,y]$ ganz über R, also Elemente von S.

Zu(ii). Ist $x\in L$ ganz über S, so gibt es ein normierte Polynom $g\in S[T]$ mit $g(x) = 0$. Sind $s_1,...,s_n\in S$ die Koeffizienten des Polynoms g, so ist x auch ganz über $S':=R[s_1,...,s_n]$, d.h. $S'':=R[x, s_1,...,s_n]$ ist ein endlich erzeugter S'-Modul. Da S' eine endlich erzeugter R-Modul ist, ist auch S" ein solcher, d.h. x ist ganz über R, d.h. $x\in S$.

Zu (iii). Offensichtlich ist SR_p ganz über R_p. Sei jetzt $x\in L$ ganz über R_p. Dann gibt es ein $s\in R-p$ mit der Eigenschaft xs ganz ist über R, d.h. es gilt $sx\in S$ also $x\in S_p$.

QED.

1.4.2 Proposition 4.2: Die Dedekind-Eigenschaft von S

(i) Der Ring S ist ein endlich erzeugter R-Modul, welcher den K-Vektorraum L erzeugt.
(ii) S ist ein Dedekind-Ring.
(iii) Jedes maximale Ideal von S liegt über einem maximalen Ideal von R.
(iv) Über jedem maximalen Ideal von R liegt ein maximales Ideal von S.

Beweis. Zu (i). Da R ein Integritätsbereich ist, ist das Nullideal p=(0) prim in R. Nach 1.4.1(iii) ist somit SR_p die ganze Abschließung von $R_p=K$ in L, d.h. es ist
$$L = SK.$$
Mit anderen Worten, S erzeugt den K-Vektorraum L und enthält damit einen freien R-Modul
$$N \subseteq S,$$
welcher von einer Basis des K-Vektorraums L erzeugt wird. Insbesondere ist auch D(N) ein freier R-Modul, welcher über K den Raum L erzeugt. Es gilt
$$D(N) \supseteq D(S).$$
Die Spuren ganzer Elemente liegen in R, d.h. es gilt nach Definition[14] des dualen Moduls
$$D(S) \supseteq S.$$
Zusammen ergibt sich $D(N)\supseteq S$, d.h. S ist endlich erzeugt.

Zu (ii) und (iii). Nach 1.4.1 ist S ganz abgeschlossen und nach (i) noethersch. Wir haben noch zu zeigen, dim S = 1. Seien P ein von Null verschiedenes Primideal von S und
$$b\in P - \{0\}.$$
Da S ganz ist über R, gilt
$$b^n + a_{n-1}b^{n-1}+...+a_1 = 0$$

[14] Mit Hilfe der Spurabbildung $B: L\times L \to K, (u,v)$ a $Tr_{L/K}(uv)$.

mit geeigneten $a_i \in R$. Da S ein Integritätbereich ist, können wir durch Kürzen mit einer b-Potenz erreichen, daß $a_1 \neq 0$ gilt. Dann ist aber

$$a_1 \in P \cap R,$$

d.h. p:= P∩R ist ein von Null verschiedenes Primideal von R und als solches maximal. Die natürliche Einbettung R⊆S induziert nach dem Homomorphiesatz eine injektive Abbildung

$$R/p \rightarrow S/P,$$

d.h. S/P ist eine nullteilerfreie Algebra über dem Körper R/p, welche als Vektorraum endlich erzeugt ist. Dann muß aber S/P ein Körper sein. Damit ist gezeigt P ist maximal, d.h. dim S = 1.

Zu (iv). Sei p ein maximales Ideal von R. Es reicht zu zeigen $pS \neq S$, denn dann liegt jedes maximale Primoberideal von pS automatisch über p. Angenommen es ist pS = S. Dann ist

$p^{-1}S = p^{-1}pS = RS = S$, also

$$p^{-1} \subseteq S \cap K = R.$$

Das Gleichheitszeichen rechts ergibt sich aus der Tatsache, daß R als Dedekind-Ring ganz-abgeschlossen in K ist. Andererseits ist $R \subseteq p^{-1}$, d.h. es gilt $p^{-1}=R$, also p=R im Widerspruch zur Wahl von p.

QED.

Wir geben jetzt zwei Folgerungen der obigen Aussagen an.

1.4.3 Folgerung 1:Fortsetzbarkeit multiplikativer Bewertungen

Sei |.| eine nicht-triviale multiplikative Bewertung von K mit

$$|r| \leq 1 \text{ für alle } r \in R$$

(d.h. eine diskrete nicht-archimedische Bewertung von K- vlg. Kapitel II).Dann gibt es eine Fortsetzung von |.| zu einer multiplikativen Bewertung von L.

Beweis. Nach 1.2.5 gibt es eine reelle Zahl ρ mit $0 < \rho < 1$ und ein von Null verschiedenes Primideal p von R mit

$$|x| = \rho^{v_p(x)} \text{ für alle } x \in K.$$

Sei P ein nach 1.4.2 existierendes über p liegendes Primideal von S. Wir fixieren ein Element $\pi \in R$ mit $v_p(\pi) = 1$ und setzen

$$e := v_P(\pi).$$

Für jedes $x \in K-\{0\}$ gilt dann[15]

$$v_P(x) = e \cdot v_p(x).$$

Mit $\sigma := \sqrt[e]{\rho}$ ist dann durch

$$\|y\| := \sigma^{v_P(y)}, \quad y \in L-\{0\},$$

eine multiplikative Bewertung von L definiert. Es reicht zu zeigen, diese stimmt auf K mit der vorgegeben Bewertung überein. Für $x \in K-\{0\}$ gilt

$$\|x\| = \sigma^{v_P(x)} = (\sigma^e)^{v_p(x)} = \rho^{v_p(x)} = |x|.$$

QED.

1.4.4 Folgerung 2: Vergleich der Divisorgruppen

Die Abbildung

---

[15] Man denke sich x in der Gestalt $x = u \cdot \pi^n$ geschrieben mit $n \in \mathbb{Z}$ und einer Einheit u von R.

$$\mathrm{Div}(R) \to \mathrm{Div}(S),\ I \mapsto IS,$$

ist ein injektiver Homomorphismus.
Beweis. Die Relationstreue der Abbildung ist offensichtlich. Zeigen wir die Injektivität. Seien I' und I" zwei gebrochene Ideale mit I'S = I"S. Durch Multiplikation mit $(I')^{-1}$ ergibt sich

$$S = (I')^{-1}I"S,$$

also $1 \in (I')^{-1}I"S$ und

$$(I')^{-1}I" \subseteq S \cap K = R.$$

Wäre $(I')^{-1}I"$ ein echtes Ideal von R, so müßte $(I')^{-1}I"S$ nach 1.4.2(iv) ein echtes Ideal von S sein. Also gilt $(I')^{-1}I"=R$, also I' = I".
QED.

1.4.5 Proposition 4.2: Vollständigkeit und endliche Erweiterungen

Seien R ein diskreter Bewertungsring und K=Q(R) vollständig. Dann ist auch S ein diskreter Bewertungsring und L=Q(S) ist vollständig.
Beweis. Nach 1.4.3 können wir die zur Bewertung von R gehörige multiplikative Bewertung von K fortsetzen zu einer Bewertung von von L. Da die Bewertung von K diskret ist, gilt

$$|n \cdot 1_K| \leq 1$$

für alle n=1,2,... (vgl. 1.1.7(vii)) und umgekehrt ergibt sich aus diesen Ungleichungen die Diskretheit der auf L fortgesetzten Bewertung. Sei

$$S' := \{x \in L \mid |x| \leq 1\}$$

der Bewertungsring der fortgesetzten Bewertung. Dann gilt $R \subseteq S'$ und, da S ganz ist über R und S' ganz abgeschlossen,

$$S \subseteq S'.$$

Wir wissen, S ist ein Dedekind-Ring mit demselben Quotientenkörper L wie S'. Um zu beweisen, S ist ein diskreter Bewertungsring, brauchen wir nur zu zeigen, S hat nur ein maximales Ideal. Hätte S außer der Einschränkung

$$P := \{x \in S \mid |x| < 1\}$$

des Bewertungsideals von S' auf S noch ein weiteres maximales Ideal P', so würde dieses Ideal eine additive, also multiplikative, Bewertung und damit eine weitere Topologie auf L definieren. Diese wäre verschieden von der durch P definierten Topologie[16], würde aber auf K dieselbe Topologie induzieren. Der erste Teil der Behauptung folgt deshalb aus dem ersten Teil des nachfolgenden Lemmas. Die Vollständigkeit von L ergibt sich aus dem zweiten Teil des Lemmas.
QED.

Lemma
Seien k ein vollständiger bewerteter Körper und K eine endliche Körpererweiterung von k. Dann gilt:
(i) Je zwei Bewertungen von K, die die von k fortsetzen, induzieren dieselbe Topologie auf K.
(ii) Eine Folge von Elementen aus K ist genau dann eine Cauchy-Folge, wenn die zugehörigen Koordinaten (bzgl. einer fixierten Basis) Cauchy-Folgen in k bilden.
Beweis: Zu (i): Wird in (2.8.3) in allgemeinerer Form bewiesen.
Zu (ii): Wird in (2.10.3) bewiesen.
QED.

---

[16] P besteht aus den Elementen x, für welche die Folge $\{x^n\}_{n=1,2,...}$ in der zugehörigen Topologie gegen Null geht, und analog für P'. Wenn also die Topolgien zusammenfallen, so auch die Primideale P und P' im Widerspruch zur Wahl von P'.

1.4.6 Die Idealnorm

Sei J ein gebrochenes Ideal des Rings S. Als R-Modul ist dann J endlich-erzeugt (da J über S und S über R endlich erzeugt sind). Für $a \in J-\{0\}$ ist außerdem

$$J \supseteq aS,$$

also erzeugt J über K den Vektorraum L. Deshalb ist das folgende gebrochene Ideal von R wohldefiniert.

$$N_{L/K}(J) := (S:J)_R$$

Es heißt Norm von J über K. Seine Beziehung zur Norm eines Elementes wird in der nachfolgenden Aussage beschrieben.

1.4.7 Proposition 4.3: Idealnorm und gewöhnliche Norm

Für $a \in L^*$ gilt

$$N_{L/K}(aS) = N_{L/K}(a)R.$$

Beweis. Das Element $N_{L/K}(a)$ ist nach Definition die Determinante der Abbildung

$$L \to L,\ x \mapsto ax,$$

also nach Definition des Quotienten (M:N) ein erzeugendes Element von $(S:aS)_R$.

QED.

Bemerkungen

(i) Im Fall $R = \mathbb{Z}$ wird $N_{L/K}(J)$ für jedes nicht-triviale Ideal $J \subseteq S$ von der Zahl der Restklassen von S/J erzeugt.

(ii) Wir werden sehen, daß die Idealnorm im noch zu präzisierendem Sinne mit dem Isomorphismus

$$Div(R) = \oplus_p Div(R_p)$$

von 1.2.5 kommutiert.

Beweis von (i). Nach der Bemerkung von 1.3.5 wird

$$N_{L/K}(J) := (S:J)_R$$

vom gewöhnlichen Index der Untergruppe J in der Gruppe S erzeugt, d.h. von Zahl der Elemente von S/J.

QED.

1.4.8 Die Vervollständigungen von L/K

Seien

R	ein diskreter Bewertungsring,
$p \subseteq R$	ein maximales Ideal,
$K = \mathbf{Q}(R)$	der Quotientenkörper von R
$\bar{K}$	die Vervollständigung von K bezüglich der durch p definierten Bewertung v_p von K.
$\{P_i\}_{i=1}^r$	die Familie der über p liegenden Primideale von S
$\bar{L}_i$	die Vervollständigung von $L=\mathbf{Q}(S)$ bzgl. der Bewertung v_{P_i}

Dann kann man $L \otimes_K \bar{K}$ und $\oplus_{i=1}^r \bar{L}_i$ als $\bar{K}$-Algebren und als topologische Vektorräume identifizieren,

$$L \otimes_K \bar{K} = \oplus_{i=1}^r \bar{L}_i .$$

Die direkte Summe rechts werde dabei mit der koordinatenweisen Multiplikation versehen.

Beweis. Da die Erweiterung L/K endlich und separabel ist, ist sie einfach,

$$L = K(\alpha) = K[x]/(f)$$

mit einem über K irreduziblen Polynom. Wir können annehmen, die Koeffizienten von f liegen in R und haben den ggT Eins,

$$f \in R[x] \text{ , } \mathrm{content}(f) = 1.$$

Als diskreter Bewertungsring ist R ein ZPE-Ring, also ist f nicht nur über K sondern auch über R irreduzibel. Sei

$$(1) \qquad f = f_1 \cdot ... \cdot f_r \text{ , } f_i \in \bar{K}[x]$$

die Zerlegung von f in irreduzible Faktoren über $\bar{K}$. Wegen der Separabilität von L/K hat f keine mehrfachen Nullstellen, d.h. die f_i sind paarweise teilerfremd. Deshalb gilt

$$L \otimes_K \bar{K} = K[x]/(f) \otimes \bar{K} \qquad (\otimes \text{ ist rechtsexakt und kommutiert mit } \oplus)$$

$$= \bar{K}[x]/(f_1 \cdot ... \cdot f_r) \qquad (\text{nach (1)})$$

$$= \bar{K}[x]/(f_1) \oplus ... \oplus \bar{K}[x]/(f_r) \qquad (\text{Chinesischer Restesatz})$$

Zum Beweis der Behauptung reicht es zu zeigen, es gibt genau r Primideale über $p \subseteq R$ und die Vervollständigungen bezüglich dieser Primideale sind isomorph zu

$$(2) \qquad \bar{L}_i := \bar{K}[x]/(f_i).$$

Jedenfalls sind die Körper (2) endliche algebraische Erweitungen von $\bar{K}$ also insbesondere endlich-dimensionale Vektorräume über $\bar{K}$ und als solche vollständig. Mit (2) schreibt sich die oben gewonnene direkte Summenzerlegung von $L \otimes_K \bar{K}$ als

$$(3) \qquad L \otimes_K \bar{K} = \bar{L}_1 \oplus ... \oplus \bar{L}_r$$

Jedes Tupel $(x_1,...,x_r)$ der direkten Summe rechts läßt sich als Element der linken Seite in der folgenden Gestalt schreiben.

$$(x_1,...,x_r) = \sum_j \ell_j \cdot \bar{k}_j \text{ mit } \ell_j \in L, \bar{k}_j \in \bar{K}.$$

Die Operation "$\cdot$" links kann man dabei mit dem Tensorprodukt identifizieren oder mit der Multiplikation der beiden Algebren (3). Wir wählen Folgen von Elementen $k_j^{(n)}$ aus K mit

$$k_j^{(n)} \to \bar{k}_j \text{ , } k_j^{(n)} \in K.$$

Dann gilt

$$L \ni \sum_j \ell_j \cdot k_j^{(n)} \to \sum_j \ell_j \cdot \bar{k}_j.$$

Mit anderen Worten, der Körper L liegt dicht in (3). Da es eine Surjektion von (3) auf jeden der Körper $\bar{L}_i$ gibt, ist L in jedem dieser Körper dicht. Mit anderen Worten,

(4) $\bar{L}_i$ ist eine Vervollständigung von L bezüglich einer Topologie, die auf $\bar{K}$ und damit auf K die gegebene Topologie induziert.

Die Topologie auf K ist aber gerade die gegebene p-adische also eine nicht-archimedische Topologie. Dann ist aber die Topologie auf jedem $\bar{L}_i$ ebenfalls eine nicht-archimedische Topologie und induziert auf L eine ebensolche, d.h. eine Topologie zu einem Bewertungsring (R_v,m_v) von L. Da eine Folge von Elementen aus R in der (R_v,m_v)-Topologie genau dann konvergiert, wenn sie in der p-adischen Topologie konvergiert, bestehen die folgenden Implikationen für ein $x\in R$:

$$x\in m_v \Leftrightarrow x^n\to 0\ m_v\text{-adisch} \Leftrightarrow x^n\to 0\ \text{p-adisch} \Leftrightarrow x\in p.$$

Damit gilt

$$m_v\cap R = p.$$

Diese Identität läßt sich auch so ausdrücken:

$$v_{m_v}(x) >0 \Leftrightarrow v_p(x)>0.$$

Analog sieht man, daß auch die umgekehrten Ungleichungen äquivalent sind. Damit gilt aber auch

$$v_{m_v}(x) =0 \Leftrightarrow v_p(x)=0.$$

Insbesondere gilt $R\subseteq R_v$. Da R_v ganz abgeschlossen in L ist, folgt

$$S\subseteq R_v.$$

Damit ist $S\cap m_v$ ein über p liegendes Primideal von S, d.h. eines der P_i und die betrachtete Topologie von L ist gerade die P_i-adische. Wir haben gezeigt, jedes der $\bar{L}_i$ in der Zerlegung (3) ist die Vervollständigung bezüglich der P_i-adischen Topologie von L, wobei P_i ein über p liegendes Primideal ist. Die zu verschiedenen $\bar{L}_i$ gehörigen Primideale P_i müssen verschieden sein, weil andernfalls L nicht dicht in der direkten Summe (3) sein könnte[17]. Zu Beweis der Behauptung fehlt jetzt nur noch die Aussage, daß unter den zu den $\bar{L}_i$ gehörigen Primidealen P_i sämtliche Primideale von S, die über p liegen, wirklich vorkommen. Sei also $P\subseteq S$ ein Primideal mit $P\cap R = p$. Wir versehen L mit der P-adischen Topologie und bezeichnen mit $\bar{L}$ die Vervollständigung. Wir betrachten die Abbildung

$$L\times K \to \bar{L},\ (x, y) \mapsto xy.$$

Ist $\{y_n\}$ eine Cauchy-Folge bezüglich der p-adischen Topologie von K, so ist $\{x\cdot y_n\}$ eine Cauchy-Folge bezüglich der P-adischen Topolgie[18]. Die Abbildung läßt sich also fortsetzen zu einer Abbildung

$$L\times\bar{K} \to \bar{L}\ ,\ (x,y) \mapsto xy.$$

---

[17] Eine Folge kann nicht in ein und derselben (separierten) Topologie gegen mehrere verschiedene Elemente konvergieren.

[18] wegen $p\subseteq P$

Diese Abbildung ist K-bilinear. Sie induziert also einen (stetigen) Homomorphismus von K-Algebren

$$\varphi: L \otimes_K \bar{K} \to \bar{L}\ ,\ x \otimes y \mapsto xy.$$

Nach (3) können wir diesen in der Gestalt

$$\varphi: \bar{L}_1 \oplus \ldots \oplus \bar{L}_r \to \bar{L}$$

schreiben. Wir wählen ein i mit der Eigenschaft, daß es ein $x \in \bar{L}_i$ gibt mit

$$\varphi(0,\ldots,x,\ldots,0) \neq 0.$$

Ein solches i existiert, da φ nicht identisch Null ist (zum Beispiel ist $\varphi(1) = 1$). Ist $y \in \bar{L}_j$ und $j \neq i$, so gilt $0 = (0,\ldots,y,\ldots,0) \cdot (0,\ldots,x,\ldots,0)$, also

$$0 = \varphi(0,\ldots,y,\ldots,0) \cdot \varphi(0,\ldots,x,\ldots,0).$$

Da der zweite Faktor rechts ungleich Null und $\bar{L}$ eine Körper ist, muß der erste Faktor Null sein. Wir haben gezeigt, es gibt genau einen direkten Summanden in (3) auf dem φ nicht identisch Null ist. Durch Einschränken auf diesen Summanden erhalten wir einen nicht-trivialen stetigen Homomorphismus von K-Algebren

$$\bar{L}_i \to \bar{L}.$$

Da $\bar{L}_i$ ein Körper ist, ist dieser injektiv,

$$\bar{L}_i \subseteq \bar{L}.$$

Eine Folge von Elementen aus L, die in der $\bar{L}_i$-Topologie konvergiert, konvergiert wegen der Stetigkeit dieser Abbildung auch in der $\bar{L}$-Topologie. Mit anderen Worten, jede P_i-adisch konvergente Folge ist P-adisch konvergent. Es gilt also $P_i \subseteq P$. Da beide Ideale maximal sind, folgt $P_i = P$.

QED.

1.4.9 Die Bewertungsringe der Vervollständigungen

Bezeichne in der Situation von 1.4.8 $\bar{R}$ den Bewertungsring von $\bar{K}$ und $\bar{S}_i$ den Bewertungsring von $\bar{L}_i$. Dann induziert der Isomorphismus von 1.4.8 einen Isomorphismus

$$\bar{R}S = \bar{S}_1 \oplus \ldots \oplus \bar{S}_r.$$

Beweis. Nach 1.4.5 ist $\bar{S}_i$ die ganze Abschließung von $\bar{R}$ in $\bar{L}_i$. Auf Grund der koordinatenweisen Multiplikation in $\bar{L}_1 \oplus \ldots \oplus \bar{L}_r$ ist damit

$$\bar{S}_1 \oplus \ldots \oplus \bar{S}_r$$

die ganze Abschließung von $\bar{R}$ in $\bar{L}_1 \oplus ... \oplus \bar{L}_r$. Da die $\bar{S}_i$ Moduln über S sind, folgt

(1) $$\bar{R}S \subseteq \bar{S}_1 \oplus ... \oplus \bar{S}_r.$$

Der Ring $\bar{R}S$ (=Im $(\bar{R} \otimes S)$) ist als endlicher $\bar{R}$-Modul vollständig und damit abgeschlossen in $\bar{L}_1 \oplus ... \oplus \bar{L}_r$. Es genügt deshalb zu zeigen der Teilring S von $\bar{R}S$ liegt dicht in der rechten Seite von (1).

Auf Grund des Beweises von 1.4.8 wissen wir, L liegt dicht in $\bar{L}_1 \oplus ... \oplus \bar{L}_r$. Weil $\bar{S}_i$ offen ist in $\bar{L}_i$ ist die rechte Seite von (1) offen in $\bar{L}_1 \oplus ... \oplus \bar{L}_r$. Zusammen erhalten wir, daß

$$(\bar{S}_1 \oplus ... \oplus \bar{S}_r) \cap L$$

liegt dicht in der rechten Seite von (1). Um zu zeigen, daß auch S dicht liegt, genügt es die Inklusion

$$(\bar{S}_1 \oplus ... \oplus \bar{S}_r) \cap L \subseteq S$$

zu beweisen. Sei x ein Element der Menge links. Das Minimalpolynom von x über $\bar{K}$ hat seine Koeffizienten in $\bar{R}$ (weil x und alle seine Konjugierten ganz sind über $\bar{R}$). Die Konjugierten von x über K =[19] $\bar{K} \cap L$ sind wegen $x \in L$ auch konjugiert über[20] $\bar{K}$. Das Minimalpolynom von x über $\bar{K}$ stimmt also mit dem Minimalpolynom von x über K überein[21]. Seine Koeffizienten liegen in $\bar{R} \cap K = R$. Mit anderen Worten, $x \in L$ ist ganz über R, und liegt damit in S.
QED.

1.4.10 Proposition 4.4:Die Zerlegung der Idealnorm

Seien R ein Dedekind-Ring und p ein maximales Ideal von R. Wir führen folgende Bezeichnungen ein.

K_p p-adische Vervollständigung des Quotientenkorpers K=Q(R).

$\bar{R}_p$ Bewertungsring von K_p bezüglich der p-adischen Bewertung.

Für die maximalen Ideale P der ganzen Abschließung S in der endlichen separablen Erweiterung L von K führen wir analog Bezeichnungen ein.

L_P P-adische Vervollständigung von L.

---

[19] Die Elemente von $\bar{K} \cap L$ können approximiert werden durch Elemente aus K, d.h. durch solche Elemente, die nur eine von Null verschiedene Koordinate (bzgl. einer Basis von L über K) haben. Die Limites solcher Folgen haben deshalb auch nur eine von Null verschiedene Koordinate, d.h. sie liegen in K.

[20] Jede K-lineare Abbildung auf L induziert eine $\bar{K}$-lineare Abbildung auf $L \otimes_K \bar{K}$.

[21] Zunächst ist das über $\bar{K}$ nur ein Teiler des Minimalpolynoms über K.

$\bar{S}_P$ Bewertungsring von L_P bezüglich der P-adischen Bewertung.

Mit diesen Bezeichnungen gilt für jedes gebrochene Ideal J von S:

$$\mathbf{N}_{L/K}(J)\bar{R}_p = \prod_{P|p} \mathbf{N}_{L_P/K_p}(J\bar{S}_P)$$

Das Produkt rechts wird dabei über die endlich vielen über p liegenden maximalen Ideale P von S erstreckt.

Beweis. Nach der Definition der Idealnorm in 1.4.6 gilt

$$\mathbf{N}_{L/K}(J) = (S:J)_R$$

Unter Verwendung der in 1.3 bewiesenen Eigenschaften des Index erhalten wir:

$$\mathbf{N}_{L/K}(J)\bar{R}_p = (S\bar{R}_p : J\bar{R}_p)_{\bar{R}_p} \qquad \text{(vgl. 1.3.14)}$$

$$= (\bar{S}_1 \oplus \ldots \oplus \bar{S}_r : J\bar{S}_1 \oplus \ldots \oplus J\bar{S}_r) \quad \text{(vgl.1.4.0)}$$

$$= \prod_{i=1}^{r} (\bar{S}_i : J\bar{S}_i) \qquad \text{(vgl. 1.3.13)}$$

Bei der zweiten Identität benutzen wir die Tatsache, daß nach 1.4.9 gilt

$$J\bar{R}_p = JS\bar{R}_p = J(\bar{S}_1 \oplus \ldots \oplus \bar{S}_r) = J\bar{S}_1 \oplus \ldots \oplus J\bar{S}_r .$$

Die Behauptung folgt jetzt aus

$$\mathbf{N}_{L_P/K_p}(J\bar{S}_P) = (\bar{S}_P : J\bar{S}_P)$$

und der Tatsache, daß jedes über p liegende Primideal in der Zerlegung von 1.4.9 genau einmal vorkommt.

QED.

1.4.11 Folgerung 1:Die Idealnorm als Gruppenhomomorphismus

Seien R ein Dedekind-Ring und S die ganze Abschließung in einer endlichen separablen Erweiterung L von K=Q(R). Dann definiert die Idealnorm einen Gruppen-Homomorphismus

$$\varphi:\mathbf{N}_{L/K}: \mathrm{Div}(S) \to \mathrm{Div}(R)$$

der Gruppe der gebrochenen Ideale von S in die der gebrochenen Ideale von S.

Beweis. Nach 1.2.6 haben wir einen injektiven Gruppen-Homomorphismus

$$\mathrm{Div}(R) \to \prod_{p \text{ maximal in } R} \mathrm{Div}(R_p),\ I \mapsto (IR_p)_{p \text{ maximal}} .$$

Es reicht daher, die Relationstreue der Komposition von φ mit diesem letzterem Homomorphismus zu beweisen, d.h. es reicht zu zeigen, die Abbildung

$$\mathrm{Div}(S) \to \mathrm{Div}(R_p),\ J \mapsto \mathbf{N}_{L/K}(J)R_p,$$

ist multiplikativ. Weiter ist die Abbildung

$$\mathrm{Div}(R_p) \to \mathrm{Div}(\bar{R}_p),\ I \mapsto I\bar{R}_p,$$

ein Gruppen-Isomorphismus (beide Gruppen sind isomorph zu $\mathbb{Z}$). Daher genügt es, die Relationstreue der folgenden Abbildung nachzuweisen.

$$\mathrm{Div}(S) \to \mathrm{Div}(R_p),\ J \mapsto \mathbf{N}_{L/K}(J)\bar{R}_p .$$

Nach 1.4.10 gilt

$$\mathbf{N}_{L/K}(J)\bar{R}_p = \prod_{P|p} \mathbf{N}_{L_P/K_p}(J\bar{S}_P),$$

so daß es genügt, die Multiplikativität von

$$\mathbf{N}_{L_P/K_p} : \mathrm{Div}(\bar{S}_P) \to \mathrm{Div}(\bar{R}_p)$$

zu beweisen. Die gebrochenen Ideale J von $\bar{S}_P$ sind aber Hauptideale,

$$J = a\bar{S}_P \text{ mit } a \in L_P.$$

Nach (1.4.7) gilt deshalb

$$\mathbf{N}_{L_P/K_p}(J) = \mathbf{N}_{L_P/K_p}(a)\bar{R}_p.$$

Die Multiplikativität der Idealnorm ist damit eine Folge der Multiplikativität der elementweisen Norm.
QED.

1.4.12 Folgerung 2:Die Idealnorm der Erweitung eines Ideals des Grundrings

Seien R ein Dedekind-Ring und S die ganze Abschließung in einer endlichen separablen Erweiterung L von K=Q(R). Dann gilt für jedes gebrochene Ideal I von R,

$$\mathbf{N}_{L/K}(IS) = I^n$$

Dabei bezeichne n := [L:K] den Grad der Erweiterung L/K.
Beweis. Wie beim Beweis von 1.4.11 reduziert man die Aussage auf den Fall, daß I ein Hauptideal ist. Wie dort folgt dann die Behauptung aus der entsprechenden Aussage über die die elementweise Norm.
QED.

1.4.13 Folgerung 3: Die Komposition von Idealnormen

Seien K⊂F⊂L endliche separable Körpererweiterungen. Dann gilt für die zugehörigen Idealnormen

$$\mathbf{N}_{L/K} = \mathbf{N}_{L/F} \circ \mathbf{N}_{F/K}$$

Beweis. Wir haben zu zeigen,

$$\mathbf{N}_{L/K}(J) = \mathbf{N}_{L/F}(\mathbf{N}_{F/K}(J))$$

für gebrochene Ideal J. Wie beim Beweis von 1.4.12 reduziert man die Aussage auf den Fall, daß J ein Hauptideal ist. Wie dort folgt dann die Behauptung aus der entsprechenden Aussage über die die elementweise Norm.
QED.

1.4.14 Die Differente der Erweiterung S/R

Sei R ein Dedekind-Ring. Dann ist der zu S duale R-Modul

$$D_R(S) = \{x \in L \mid \mathrm{Tr}_{L/K}(xs) \subseteq R \text{ für jedes } s \in S\}$$

endlich erzeugt über R (nach 1.3.10(i)). Direkt aus der Beschreibung folgt, daß $D_R(S)$ sogar ein S-Modul ist (und als solcher dann natürlich erst recht endlich erzeugt ist). Weiter sieht man unmittelbar aus der Definition, daß

$$D_R(S) \supseteq S$$

gilt. Also ist

$$\mathfrak{D} := \mathfrak{D}(S/R) := D_R(S)^{-1} \ (\subset S)$$

ein Ideal von S. Dieses Ideal heißt Differente der Erweiterung S/R. Man beachte es gilt,

$$\delta(S/R) = \mathbf{N}_{L/K}(\mathcal{D}(S/R)).$$

Nach Definition ist die Diskriminante nämlich gleich

$$\delta(S/R) = (D_R(S):S) = (S:D_R(S))^{-1} = (S:\mathcal{D}^{-1})^{-1} = \mathbf{N}_{L/K}(\mathcal{D}^{-1})^{-1} = \mathbf{N}_{L/K}(\mathcal{D}).$$

Die letzte Identität ist eine Folge der Multiplikativität der Idealnorm.

1.4.15 Proposition 4.5: Verhalten der Differente beim Komplettieren

Sei R ein Dedekind-Ring. Dann gilt mit den Bezeichnungen von 1.4.10:

(i) $\mathcal{D}(S/R)\bar{S}_P = \mathcal{D}(\bar{S}_P/\bar{R}_p)$ für jedes maximale Ideal p von R und jedes über p liegende maximale Ideal P von S.

(ii) $\delta(S/R)\bar{R}_p = \prod_{P|p} \delta(\bar{S}_P/\bar{R}_p)$.

Beweis. Die erste Aussage ergibt sich aus den in 1.3 bewiesenen allgemeinen Eigenschaften des Duals:

$$\begin{aligned}
\mathcal{D}(S/R)\bar{S}_P &= D_R(S)^{-1}\bar{S}_P \\
&= (D_R(S)\bar{S}_P)^{-1} \\
&= (D_{\bar{R}_p}(\bar{S}_P))^{-1} \qquad \text{(vgl. 1.3.14)} \\
&= \mathcal{D}(\bar{S}_P/\bar{R}_p)
\end{aligned}$$

Die zweite Aussage ergibt sich aus der in 1.4.14 gegebenen Beschreibung der Diskriminante als Norm der Differente $\mathcal{D}(S/R) = \mathcal{D}$ und aus 1.4.11:

$$\begin{aligned}
\delta(S/R)\bar{R}_p &= \delta(\mathbf{N}_{L/K}(\mathcal{D}))\bar{R}_p \\
&= \prod_{P|p} \mathbf{N}_{L_P/K_p}(\mathcal{D}\bar{S}_P) \qquad \text{(vgl. 1.4.11)} \\
&= \prod_{P|p} \mathbf{N}_{L_P/K_p}(\mathcal{D}(\bar{S}_P/\bar{R}_p)) \qquad \text{(vgl. (i))} \\
&= \prod_{P|p} \delta(\bar{S}_P/\bar{R}_p)
\end{aligned}$$

QED.

Zum Beweis unseres nächsten Ergebnisses benötigen wir das

Lemma

Seien $x_1,...,x_n$ und x Unbestimmte und g das ganzzahlige Polynome $g(x) := (x-x_1)...(x-x_n)$. Dann ist der Ausdruck

$$S := \sum_{i=1}^{n} \frac{x_i^k}{g'(x_i)} \in \mathbb{Z}$$

für $k=1,...,n-1$ eine von den x_i unabhängige ganze Zahl.

Beweis. Nach der Produktregel gilt

$$g'(x_i) = (x_i-x_1)...(x_i-x_{i-1})(x_i-x_{i+1})...(x_i-x_n).$$

Wir setzen

$$D := \prod_{a<b} (x_a-x_b)$$

$$D_i := \prod_{a<b,\, a,b\neq i} (x_a-x_b) = (-1)^{i-1}\cdot\frac{D}{g'(x_i)}.$$

Man beachte, in $g'(x_i)$ haben gerade die ersten i-1 Faktoren ein anderes Vorzeichen als die entsprechenden Faktoren von D.
Es gilt

$$S = \frac{P}{D}$$

mit

(1) $$P := \sum_{i=1}^{n} x_i^k\cdot\frac{D}{g'(x_i)} = \sum_{i=1}^{n} x_i^k\cdot(-1)^{i-1}\cdot D_i.$$

Dabei ist P ein ganzzahliges und symmetrisches Polynom in den $x_1,...,x_n$. Wegen $k \leq n-1 \leq \deg g'$ gilt

$$\deg P \leq \deg D.$$

Zum Beweis der Behauptung genügt es zu zeigen,

(2) $$(x_1-x_2) \mid P,$$

denn weil P symmetrisch ist, muß dann P auch durch die übrigen Differenzen teilbar sein, d.h. es muß $D \mid P$ gelten. Aus Gradgründen muß dann aber

$$S = \frac{P}{D}$$

eine Konstante sein (und zwar eine ganze Zahl, da der höchste Koeffizient von D Eins ist). Zeigen wir also, es gilt (2). Die einzigen eventuell nicht durch x_1-x_2 teilbaren Summanden in (1) sind die Summanden mit i=1 und i=2. Es reicht also zu zeigen,

$$x_1-x_2 \mid x_1^k\cdot D_1 - x_2^k\cdot D_2 .$$

Dazu genügt es zu zeigen, das Polynom rechts wird Null, wenn man $x_2 = x_1$ setzt, d.h.

$$D_1 = D_2 \text{ für } x_2 = x_1.$$

Die Faktoren von D_1, in denen x_2 vorkommt, sind gerade die folgenden[22].

$$x_2 - x_3 , ..., x_2-x_n .$$

Die Faktoren von D_2, in denen x_1 vorkommt, sind die folgenden[23].

$$x_1 - x_3 , ..., x_1-x_n .$$

In allen übrigen Faktoren stimmen D_1 und D_2 überein. Wenn wir also $x_2 = x_1$ setzen, erhalten wir also tatsächlich $D_1 = D_2$.

QED.

1.4.16 Proposition 4.6: Diskriminante und Ableitungen von Minimalpolynomen

Sei $\alpha \in S$ ein primitives Element der endlichen separablen Erweiterung

$$L = K(\alpha)$$

---

[22] Man beachte, x_1 kommt in D_1 überhaupt nicht vor.

[23] Man beachte, x_2 kommt in D_2 überhaupt nicht vor.

und sei $g(T)\in K[T]$ das Minimalpolynom von α über K. Weiter sei

$$M = R[\alpha]$$

die von α über R erzeugte Algebra. Man beachte, weil der höchste Koeffizient von g gleich 1 ist, ist M als Modul über R endlich erzeugt (und erzeugt den Körper L über K). Es gilt

(i) $D(R[\alpha]) = \frac{1}{g'(\alpha)} R[\alpha]$.

(ii) $\delta(R[\alpha]/R) = N_{L/K}(g'(\alpha))R$.

(iii) $R[\alpha] = S \Leftrightarrow \mathcal{D}(S/R) = g'(\alpha)S$.

Beweis. Zu (i) und (ii). Man beachte, $R[\alpha]$ ist ein freier R-Modul vom Rang n:=[L:K] über R, denn die Potenzen

$$1, \alpha, ..., \alpha^{n-1}$$

sind sogar linear unabhängig über K. Nach dem obigen Lemma ist

$$Tr_{L/K}(\frac{\alpha^k}{g'(\alpha)}) \in R$$

für k=0,...,n-1. Für $a\in\frac{1}{g'(\alpha)} R[\alpha]$ und $b\in R[\alpha]$ gilt $ab\in\frac{1}{g'(\alpha)}R[\alpha]$, also $Tr_{L/K}(ab)\in R$. Nach Definition des dualen Moduls folgt

(1) $$\frac{1}{g'(\alpha)} R[\alpha] \subseteq D_R(R[\alpha]).$$

Da $R[\alpha]$ ein freier R-Modul ist, können wir nach 1.3.12 die Diskriminante von $R[\alpha]$ besonders leicht ausrechnen:

$$\delta(R[\alpha]/R) = \det Tr_{L/K}(\alpha^{i+j})_{i,j=0,...,n-1}R$$

Seien

$$s_1,...,s_n: L \to \bar{K}$$

Die K-Einbettungen von L in eine algebraische Abschließung von K. Dann gilt

$$Tr_{L/K}(\alpha^{i+j}) = \sum_{k=1}^{n} s_k(\alpha^{i+j}) = \sum_{k=1}^{n} s_k(\alpha^i)\cdot s_k(\alpha^j),$$

also

$$\begin{aligned} \det Tr_{L/K}(\alpha^{i+j}) &= \det (s_i(\alpha^j))^2 \\ &= (\prod_{i<j} (s_i(\alpha)-s_j(\alpha)))^2 \quad \text{(Vandermonde)} \\ &= \pm \prod_{i=1}^{n} g'(s_i(\alpha)) \\ &= \pm N_{L/K}(g'(\alpha)) \end{aligned}$$

Damit ist

$$\delta(R[\alpha]/R) = N_{L/K}(g'(\alpha))R =^{24} (R[\alpha]:g'(\alpha)R[\alpha]) = (\frac{1}{g'(\alpha)}R[\alpha]:R[\alpha])$$

d.h. es gilt (ii). Damit ergibt sich weiter

$$(D_R(R[\alpha]):R[\alpha]) = \delta(R[\alpha]/R) = (\frac{1}{g'(\alpha)}R[\alpha]:R[\alpha]).$$

---

[24] Nach Definition der Norm 1.4.6.

Wir haben gezeigt, die beiden Moduln $\frac{1}{g'(\alpha)}R[\alpha]$ und $D_R(R[\alpha])$ sind ineinander enthalten (vgl. (1)) und haben denselben Index bezüglich $R[\alpha]$. Nach 1.3.6 müssen die Moduln gleich sein, d.h. es gilt (i).
Zu (iii). Im Fall $S= R[\alpha]$ gilt nach (i)

$$\mathcal{D}(S/R) = D_R(S)^{-1} = D_R(R[\alpha])^{-1} = g'(\alpha)S.$$

Sei umgekehrt

$$\mathcal{D}(S/R) = g'(\alpha)S.$$

Nach Definition der Differente bedeutet das,

$$D_R(S) = \frac{1}{g'(\alpha)} S \ . \tag{2}$$

Wegen $R[\alpha] \subseteq S$ gilt dann

$$\begin{aligned} D_R(R[\alpha]) &\supseteq D_R(S) \\ &= \frac{1}{g'(\alpha)} S && \text{(nach (2))} \\ &\supseteq \frac{1}{g'(\alpha)} R[\alpha] \\ &= D_R(R[\alpha]) && \text{(nach (i))} \end{aligned}$$

Damit gilt überall in dieser Abschätzung der Gleichheitszeichen. Insbesondere ist

$$D_R(R[\alpha]) = D_R(S)$$

Nach 1.3.10 ist das doppelte Dual gleich dem ursprüngliche Modul. Aus der letzten Identität folgt also

$$R[\alpha] = S.$$

QED.

1.4.17 Proposition 4.7: Diskriminante und Differente von Körpertürmen

Seien $L \supseteq F \supseteq K$ endliche separable Körpererweiterungen und
$S \supseteq T \supseteq R$
die zugehörigen Ring der ganzen Zahlen (d.h. T sei die ganze Abschließung von R in F).

(i) $\mathcal{D}(S/R) = \mathcal{D}(S/T)\cdot\mathcal{D}(T/R)$.

(ii) $\delta(S/R) = \delta(T/R)^m \cdot N_{F/K}\delta(S/T)$ mit $m:= [L:F]$

Beweis. Aussage (ii) folgt aus (i) und der Tatsache, daß die Norm der Differente gerade die Diskriminante ist.

$$\begin{aligned} \delta(S/R) &= N_{L/K}(\mathcal{D}(S/R)) \\ &= N_{L/K}(\mathcal{D}(S/T))\cdot N_{L/K}(\mathcal{D}(T/R)) && \text{(nach (i))} \\ &= N_{F/K}N_{L/F}(\mathcal{D}(S/T))\cdot N_{F/K}N_{L/F}(\mathcal{D}(T/R)) && \text{(nach 1.4.13)} \\ &= N_{F/K}\delta(S/T)\cdot N_{F/K}(\mathcal{D}(T/R)^m) && \text{(nach 1.4.12)} \\ &= N_{F/K}\delta(S/T)\cdot \delta(T/R)^m \end{aligned}$$

Damit reicht es, Aussage (i) zu beweisen. Statt dieser Aussage genügt es die analoge Aussage für die inversen Ideal zu beweisen:

$$D_R(S) = D_T(S)\cdot D_R(T).$$

Wegen der Transitivität der Spur gilt

$$Tr_{L/K}(Sx) = Tr_{F/K}(Tr_{L/F}(Sx)T).$$

Damit erhalten wir

$$x \in D_R(S) \Leftrightarrow Tr_{L/K}(Sx) \subseteq R$$

$$\Leftrightarrow \mathrm{Tr}_{F/K}(\mathrm{Tr}_{L/F}(Sx)T) \subseteq R$$
$$\Leftrightarrow \mathrm{Tr}_{L/F}(Sx)T \subseteq D_R(T) =: \mathcal{D}^{-1}$$
$$\Leftrightarrow \mathrm{Tr}_{L/F}(Sx\mathcal{D}) \subseteq T \qquad (\mathrm{Tr}_{L/F} \text{ ist F-linear und } \mathcal{D}\subset T)$$
$$\Leftrightarrow Sx\mathcal{D} \subseteq D_T(S)$$
$$\Leftrightarrow Sx \subseteq D_T(S)\cdot\mathcal{D}^{-1} = D_T(S)\cdot D_R(T)$$

QED.

1.5 Verzweigung

1.5.1 Relativgrad und Verzweigungsindex

Seien R_1 und R_2 zwei Dedekind-Ringe mit

$$R_1 \subseteq R_2$$

und p_1 und p_2 zwei maximale Ideale von R_1 bzw. R_2 mit

$$p_1 = p_2 \cap R_1$$

In dieser Situation sind die Restklassenkörper $k_i := R_i/p_i$ ineinander enthalten und der Grad der entsprechenden Körpererweiterung

$$f(p_2|p_1) := [k_2:k_1]$$

heißt Relativgrad von p_2 über p_1 (und kann im allgemeinen endlich sein). Der Verzweigungsindex von p_2 über p_1 ist die positive ganze Zahl

$$e(p_2|p_1) := v_{p_2}(p_1R_2)$$

Nach Definition hat der Verweigungsindex die Eigenschaft, daß für Elemente $x\in\mathbf{Q}(R_1)$

$$v_{p_2}(x) = e(p_2|p_1)\cdot v_{p_1}(x)$$

gilt.

1.5.2 Proposition 5.1:Multiplikativität von Relativgrad und Verzweigungsindex

Seien $R_1 \subseteq R_2 \subseteq R_3$ ineinanderliegende Dedekind-Ringe und $p_i \subseteq R_i$ (i=1,2,3) übereinanderliegende maximale Ideale. Dann gilt

(i) $f(p_3|p_1) = f(p_3|p_2)\cdot f(p_2|p_1)$

(ii) $e(p_3|p_1) = e(p_3|p_2)\cdot e(p_2|p_1)$

Beweis. trivial.
QED.

1.5.3 Proposition 5.2: Verhalten beim Vervollständigen

Seien R ein Dedekind-Ring und $p\subseteq R$ ein maximales Ideal. Weiter sei $\bar{p}$ das Bewertungs-ideal der p-adischen Vervollständigung von R. Dann gilt

$$f(\bar{p}|p) = e(\bar{p}|p) = 1.$$

Beweis. Nach 1.2.6(iii) gilt

$$e(pR_p|p) = 1.$$

Es reicht also zu zeigen,

$$e(\bar{p}|pR_p) = 1,$$

d.h. wir können annehmen, R ist ein diskreter Bewertungsring. Angenommen,

$$e = e(\bar{p}|p) > 1.$$

Sei π ein erzeugendes Element von p,

$$p = \pi R.$$

Nach Definition von e gibt es ein Element $\bar{\pi}$ in der Vervollständigung $\bar{R}$ mit

$$\pi = u \cdot \bar{\pi}^e.$$

Wir wählen Folgen von Elementen in R mit

$$u_i \to u,\ \pi_i \to \bar{\pi}$$

Dann gilt $v_{\bar{p}}(\bar{\pi}-\pi_i) \to \infty$ und $v_{\bar{p}}(u-u_i) \to \infty$, also $v_{\bar{p}}(u\cdot\bar{\pi}^e - u_i\cdot\pi_i^e) \to \infty$, also

$$v_p(\pi - u_i\cdot\pi_i^e) \to \infty.$$

Damit gilt für große i

$$v_p(\pi) = \min(v_p(\pi - u_i\cdot\pi_i^e), v_p(u_i\cdot\pi_i^e)) = v_p(u_i\cdot\pi_i^e) = e\cdot v_p(\pi_i) + v_p(u_i).$$

Analog folgert man aus $u_i \to u$, daß für große i gilt $v_{\bar{p}}(u_i) = v_{\bar{p}}(u) = 0$, also auch $v_p(u_i) = 0$.

Damit folgt

$$v_p(\pi) = e\cdot v_p(\pi_i),$$

im Widerspruch zu $v_p(\pi) = 1$.

Damit is die Aussage über den Verzweigungsindex bewiesen. Beweisen wir die Aussage über die Relativgrade. Zunächst gilt

$$f(pR_p|p) = [R_p/pR_p : R/p] = 1,$$

denn jedes Element $\alpha \in R_p/pR_p$ wird repräsentiert durch ein Element der Gestalt

$$xy^{-1} \text{ mit } x,y \in R,\ y \notin p.$$

Wegen $y \notin p$ repräsentiert y eine Einheit von R/p, d.h. das Element α hat auch einen Repräsentanten in R/p. Damit haben wir den Beweis auf den Fall, daß R ein diskreter Bewertungsring ist, reduziert.

Nach Konstruktion enthält die Vervollständigung $\bar{R}$ den Ring R als dichte Teilmenge. Damit liegt aber auch R/p dicht in $\bar{R}/\bar{p}$. Die Topologie von $\bar{R}/\bar{p}$ ist aber die diskrete Topologie (da $\bar{p}$ offen in $\bar{R}$ ist). Deshalb gilt $R/p = \bar{R}/\bar{p}$, also

$$f(\bar{p}|p) = [\bar{R}/\bar{p} : R/p] = 1.$$

QED.

1.5.4 Verhalten beim Vervollständigen II

Seien $R_1 \subseteq R_2$ ineinanderliegende Dedekind-Ringe und $p_i \subseteq R_i$ (i=1,2) übereinanderliegende maximale Ideale. Weiter sei $\bar{p}_i$ das Bewertungsideal der p_i-adischen Vervollständigung von R_i. Dann gilt

$$f(p_2|p_1) = f(\bar{p}_2|\bar{p}_1)$$

$$e(p_2|p_1) = e(\bar{p}_2|\bar{p}_1)$$

Beweis. folgt unmittelbar aus 1.5.3.
QED.

1.5.5 Vereinbarungen und Bezeichnungen

Die Ergebnisse von 1.4 zusammen mit den unmittelbar vorangehenden Ergebnissen zeigen, daß man

Differente,
Diskriminante,
Relativgrad,
Verzweigungsindex
Idealnorm

lokal mit Hilfe der Vervollständigungen beschreiben kann.

Beginnend mit dieser Stelle bis zum Ende des Kapitels werden wir deshalb annehmen,

R ist ein diskreter Bewertungsring mit dem Bewertungsideal p
K = Q(R) ist vollständig bezüglich der p-adischen Bewertung

Diese Situation bleibt nach 1.4.5 erhalten, wenn man zu einer endlichen separablen Erweiterung übergeht. Wir haben deshalb als Konsequenz unserer Annahmen:

S ist ein diskreter Bewertungsring mit dem Bewertungsideal P
L = Q(S) ist vollständig bezüglich der P-adischen Bewertung.

Die Umformulierung der Ergebnisse für den globalen Fall werden wir weitgend dem Leser überlassen.
Wir werden jetzt unsere Bezeichnungen etwas der Situation des lokalen Falles anpassen und schreiben

$$\mathcal{D}(L/K) := \mathcal{D}(S/R)$$
$$\delta(L/K) := \delta(S/R)$$
$$f(L/K) := f(S/R)$$
$$e(L/K) := e(S/R)$$

Weitere Bezeichnungen:

v_L P-adische Bewertung des Körpers L
k_L := S/P, Restklassenkörper des Körpers L.
U_L Gruppe der Einheiten des Rings S
k := k_K, Restklassenkörper zum Grundkörper.

Wir werden im folgenden nicht voraussetzen, daß die Körpererweiterung L/K separabel ist (außer in 1.9).

1.5.6 Proposition 5.3: Das Produkt von Verzweigungsindex und Relativgrad

$$e(L/K)\cdot f(L/K) = [L:K]$$

Beweis. Der k-Vektorraum S/pS besitzt eine Kette von Unterräumen mit den folgenden Faktoren

$$S/P,\ P/P^2,\ P^2/P^3,\ \ldots,\ P^{e-1}/P^e \text{ mit } e = e(S/R).$$

Man beachte, es gilt $P^e = pS$. Nach 1.1.17 sich alle diese Faktoren isomorph, d.h. es gilt

$$\dim_k S/pS = e\cdot\dim_k S/P = e(L/K)\cdot f(L/K).$$

Als Modul über dem diskreten Bewertungsring R ist S⊆L ein freier Modul. Da S ein Erzeugendensystem von L über K enthält, gilt

$$\mathrm{rk}_R\, S = [L:K]$$

Damit hat aber auch S/pS als k-Modul den Rang [L:K],

$$\dim_k S/pS = [L:K].$$

QED.

1.5.7 Ein kommutatives Diagramm zur Einbettung K*⊆L*

Die natürliche Einbettung j:K*⊆L* definiert ein kommutatives Diagramm mit exakten Zeilen

$$\begin{array}{ccccccccc} 0 & \to & U_K & \to & K^* & \xrightarrow{v_K} & \mathbb{Z} & \to & 0 \\ & & \downarrow & & \downarrow j & & \downarrow e & & \\ 0 & \to & U_L & \to & L^* & \xrightarrow{v_L} & \mathbb{Z} & \to & 0 \end{array}$$

Dabei seien U_K und U_L die Einheitengruppen von K bzw. L und die Abbildung rechts sei die Multiplikation mit dem Verzweigungsindex e = e(L/K).

Beweis. Die Kommutativität des linken Vierecks ist trivial und die des rechten folgt aus der Definition des Verzweigungsindex. Die Exaktheit der Zeilen folgt aus der Definition der Einheitengruppen.

QED.

1.5.8 Ein kommutatives Diagramm zur Normabbildung N:L*⊆K*

Die elementweise Norm $N:= N_{L/K}:L\to K$ definiert ein kommutativen Diagramm (mit exakten Zeilen)

$$\begin{array}{ccccccccc} 0 & \to & U_L & \to & L^* & \xrightarrow{v_L} & \mathbb{Z} & \to & 0 \\ & & \downarrow & & \downarrow N & & \downarrow f & & \\ 0 & \to & U_K & \to & K^* & \xrightarrow{v_K} & \mathbb{Z} & \to & 0 \end{array}$$

Dabei sei die vertikale Abbildung rechts die Multiplikation mit dem Relativgrad f = f(L/K). Mit anderen Worten, es gilt

$$f\cdot v_L(x) = v_K(N_{L/K}(x)) \text{ für } x\in L^*$$

und insbesondere ist

$$N_{L/K}(P)R = p^f.$$

Beweis. Wegen der Multiplikativität der Norm

$$N(ab) = N(a)N(b)$$

gilt

$$N(U_L) \subseteq U_K,$$

d.h. es gibt ein kommutatives Diagramm der behaupteten Art, wobei jedoch zunächst anstelle der f-Multiplikation irgend ein Gruppenhomomorphismus steht. Dieser ist die Multiplikation mit einer Zahl, sagen wir f', d.h. es ist

$$f'\cdot v_L(x) = v_K(N_{L/K}(x)) \text{ für } x\in L^*$$

Wir haben nur noch zu zeigen, f' = f. Dazu setzen wir für x ein Element von K ein. Nach Definition es Verzweigungsindex gilt

$$\begin{aligned} e\cdot f'\cdot v_K(x) &= f'\cdot v_L(x) \\ f'\cdot v_L(x) &= v_K(N_{L/K}(x)) \end{aligned}$$

$$= v_K(x^{[L:K]})$$
$$= v_K(x^{e\cdot f}) \qquad (1.5.6)$$
$$= e\cdot f\cdot v_K(x)$$

Also gilt f'=f.
Zum letzten Teil der Behauptung. Offensichtlich gilt wegen der Kommutativität des Diagramm

$$N_{L/K}(P) \subseteq p^f$$

(ein Element im Bild von N hat einen durch f teilbaren Wert, liegt also in p^f). Sei π ein erzeugendes Element von P. Dann gilt $v_L(\pi) = 1$, also

$$v_K(N(\pi)) = f,$$

d.h. $N(\pi)$ erzeugt p^f.
QED.

1.5.9 Eine Eigenschaft der Spur (Lemma)

Seien k ein Körper, A eine k-Algebra und N das Radikal von A,

$$N := \bigcap_{m\subseteq A \text{ maximal}} m .$$

Es gelte

1. $\dim_k A < \infty$ (Vektorraumdimension).
2. $\bar{A} := A/N$ ist ein Körper.
3. $N^e = 0$, $N^{e-1} \neq 0$.
4. $N^i/N^{i+1} \cong A/N$.

Dann gilt für jedes Element $a\in A$

$$\mathbf{Tr}_{A/k}(a) = e\cdot\mathbf{Tr}_{\bar{A}/k}(\bar{a}) \text{ und } \mathbf{N}_{A/k}(a) = \mathbf{N}_{\bar{A}/k}(\bar{a})^e$$

Dabei bezeichne $\bar{a}$ die Restklasse von a in $\bar{A}$.
Beweis. Das Element $Tr_{A/k}(a)$ ist definiert als die Spur der k-linearen Abbildung

$$A \xrightarrow{a} A,\ x \mapsto ax.$$

Analog ist $N_{A/k}(a)$ definiert als die Determinante dieser Abbildung. Für i=0, ..., e-1 haben wir das folgende kommutative Diagram von k-Vektorräumen mit exakten Zeilen.

$$\begin{array}{ccccccccc} 0 & \to & N^{i+1} & \to & N^i & \to & N^i/N^{i+1} & \to & 0 \\ & & a_{i+1}\downarrow & & a_i\downarrow & & \bar{a}_i\downarrow & & \\ 0 & \to & N^{i+1} & \to & N^i & \to & N^i/N^{i+1} & \to & 0 \end{array}$$

Die vertikalen Pfeile sollen dabei ebenfalls die Multiplikation mit a bezeichnen. Bezüglich einer Basis von N^i, welche die Inklusion $N^{i+1} \subseteq N^i$ respektiert, hat die Matrix der mittleren vertikalen Abbildung eine Blockgestalt, aus der man die Relation

$$\mathbf{Tr}(a_i) = \mathbf{Tr}(a_{i+1})+\mathbf{Tr}(\bar{a}_i) \text{ und } \mathbf{N}(a_i) = \mathbf{N}(a_{i+1})\cdot\mathbf{N}(\bar{a}_i)$$

abliest. Wegen $A = N^0$ und $N^e = 0$ erhalten wir

$$\mathrm{Tr}_{A/k}(a) = \mathrm{Tr}(a_0) = \sum_{i=0}^{e-1} \mathrm{Tr}(\bar{a}_i).$$

Dabei bezeichnet $\bar{a}_i$ die Multiplikation mit a auf dem A-Modul N^i/N^{i+1}. Benutzen wir den Isomorphismus

$$N^i/N^{i+1} = A/N = \bar{A}$$

um N^i/N^{i+1} mit $\bar{A}$ zu identifizieren,so wird $\bar{a}_i$ zur Multiplikation mit a auf dem A-Modul $\bar{A}$, d.h. es gilt $\mathrm{Tr}(\bar{a}_i) = \mathrm{Tr}_{\bar{A}/k}(\bar{a})$, also $\mathrm{Tr}_{A/k}(a) = e \cdot \mathrm{Tr}_{\bar{A}/k}(\bar{a})$ wie behauptet. Die Formel für die Normen ergibt sich analog.
QED.

1.5.10 Die Spur der Restklasse eines Elements von S

Seien $a \in S$ ein Element und $\bar{a} \in k_L = S/P$ dessen Restklasse in k_L. Dann ist die Restklasse von $\mathrm{Tr}_{L/K}(a)$ in k_L gleich

$$\overline{\mathbf{Tr}_{L/K}(a)} = e(L/K) \cdot \mathbf{Tr}_{k_L/k_K}(\bar{a})$$

und analog erhält man für die Restklasse der Norm

$$\overline{\mathbf{N}_{L/K}(a)} = \mathbf{N}_{k_L/k_K}(\bar{a})^{e(L/K)}$$

Beweis. Es reicht zu zeigen, die Algebra $A = S/pS$ über dem Körper $k = k_K$ genügt den Bedingungen von 1.5.9 (mit e=e(L/K)). Die erste Bedingung ist erfüllt, da nach 1.4.2(i) S als R-Modul endlich erzeugt ist. Die zweite Bedingung gilt wegen

$$A/N = (S/pS)/(P/pS) = S/P.$$

Man beachte, mit S ist auch S/pS ein lokaler Ring (mit dem einzigen maximalen Ideal P/pS). Die dritte Bedingung ergibt sich aus der Definition des Verzweigungsindex. Die vierte Bedingung ist gerade die Aussage von 1.1.17(i).
QED.

1.5.11 Propostion 5.4: Eine Abschätzung für den Wert der Differente

Bezeichne

$$\mathcal{D} := \mathcal{D}(L/K)$$

die Differente der Erweiterung $K \subseteq L$. Dann gilt

$$v_L(\mathcal{D}) \geq e(L/K) - 1.$$

Beweis. Nach Definition des Relativ-Index f = f(L/K) ist

$$\bar{A} := S/pS$$

ein f-dimensionaler k-Vektorraum. Auf Grund der exakten Sequenzen

$$0 \to N^{i+1} \to N^i \to \bar{A} \to 0, \; N := P/pS,$$

kann man eine Basis von N^i gewinnen indem man zu einer Basis von N^{i+1} die Repräsentanten einer Basis von

$$N^i/N^{i+1} \cong \bar{A}$$

hinzufügt. Indem wir dieses Vorgehen wiederholen erhalten wir eine Basis

$$\{\bar{a}_i\}$$

des k-Vektorraums $\bar{A} := S/pS$, welche aus e·f Elementen, wobei die ersten (e-1)·f Elemente eine Basis des Unterraums $N = P/pS$ bilden. Bezeichne $a_i \in S$ einen Repräsentanten von $\bar{a}_i \in \bar{A}$ in S. Dann bilden die $a_i \in S$ eine Basis[25] von S über R. Nach 1.3.12(iii) können wir die Diskriminante von S/R mit Hilfe dieser Basis berechnen:

$$\delta(S/R) = \det\,(\mathrm{Tr}_{L/K}(a_i \cdot a_j)).$$

Nach Konstruktion gilt

$$a_i \in P \text{ für } 1 \le i \le (e-1)f\,.$$

Da P ein Ideal ist, haben wir damit

$$a_i \cdot a_j \in P \text{ für } 1 \le i \le (e-1)f \text{ und } j \text{ beliebig.}$$

Nach 1.5.10 erhalten wir

$$\overline{\mathbf{Tr}_{L/K}(a_i a_j)} = e(L/K)\cdot\mathbf{Tr}_{k_L/k_K}(\overline{a_i a_j}) = e(L/K)\cdot\mathbf{Tr}_{k_L/k_K}(0) = 0$$

Also

$$\mathrm{Tr}_{L/K}(a_i \cdot a_j) \in p \text{ für } 1 \le i \le (e-1)f \text{ und } j \text{ beliebig.}$$

Mit anderen Worten, die ersten (e-1)f Zeilen der Matrix

$$(\mathrm{Tr}_{L/K}(a_i \cdot a_j))$$

liegen im Ideal p. Wir entwickeln die Determinante dieser Matrix nach diesen ersten Zeilen und erhalten

$$\delta := \delta(S/R) \in p^{(e-1)f},$$

d.h.

$$v_K(\delta(S/R)) \ge (e-1)f.$$

Nach 1.5.8 folgt damit

$$v_L(\mathcal{D}) = \frac{1}{f}\cdot v_K(N_{L/K}(\mathcal{D})) = \frac{1}{f}\cdot v_K(\delta) \ge e-1.$$

---

[25] Die a_i sind linear unabhängig über R: wäre $\sum_i a_i r_i = 0$ eine nicht-triviale Relation über R, so könne man die Koeffizienten $r_i \in R$ durch eine geeignete Potenz eines Parameters von R teilen und erreichen, daß mindestens einer dieser Koeffizienten eine Einheit ist. Durch Übergang zu den Restklassen modulo pS erhalten wir dann aber eine nicht-triviale Relation zwischen den $\bar{a}_i$, was nach Konstruktion nicht möglich ist. Nach Konstruktion ist $S = \sum_i a_i R + pS$. Iterieren dieser Relation liefert $S = \sum_i a_i R + p^s S$ mit beliebig hohem s. Mit anderen Worten, jedes Element von S läßt sich durch Elemente aus $\sum_i a_i R$ beliebig gut approximieren. Da R vollständig ist, folgt $S = \sum_i a_i R$. Man beachte, die Topologie von L (⊇S) ist gerade die Vektorraum-Topologie über K(⊇R).

Man beachte, das Ideal $\mathcal{D}$ von S ist wie alle Ideale von S ein Hauptideal. Die Idealnorm von $\mathcal{D}$ kann man also mit Hilfe der elementweisen Norm berechnen.
QED.

1.5.12 Unverzweigte Erweiterungen

Die Erweiterung L/K heißt unverzweigt, wenn die folgenden Bedingungen erfüllt sind.
1. $e(L/K) = 1$.
2. Die Erweiterung der Restklassenkörper k_L/k ist separabel.

Bemerkung
Im nicht-lokalen Fall sagen wir, S/R ist unverzweigt im maximalen Ideal P von S, wenn die zugehörige Erweiterung der vervollständigten Quotientenkörper P bzw. $p:=S\cap P$ unverzweigt ist.

1.5.13 Theorem 5.1: Diskrimantenkriterium für unverzweigte Erweiterungen

Folgende Aussagen sind äquivalent.
(i) L/K ist unverzweigt.
(ii) $\delta(L/K) = R$.

Beweis. Im Fall $\delta=R$ gilt nach 1.3.6(iv) für die Differente $\mathcal{D} = \mathcal{D}(S/R)$ die analoge Identität[26]

$$\mathcal{D} = S.$$

Nach 1.5.11 ist damit aber

$$e(L/K) - 1 \le v_L(\mathcal{D}) = v_L(S) = 0,$$

d.h. $e(L/K) \le 1$, d.h. $e(L/K) = 1$. Wir nehmen jetzt an, der Verzweigungsindex

$$e(L/K) = 1$$

ist Eins. Wir haben dann nur noch zu zeigen,

$$k_L/k \text{ separabel} \Leftrightarrow \delta(L/K) = R.$$

Wir wählen ein freies Erzeugendensystem $\{x_i\}$ von S über R. Ein solches existiert, weil R nach Voraussetzung ein diskreter Bewertungsring ist. Die Diskriminante $\delta=\delta(S/R)$ wird dann nach 1.3.12(iii) erzeugt von der Determinante

$$d := \det(\mathbf{Tr}_{L/K}(x_i x_j))$$

Bezeichne $\bar{x}_i$ die Restklasse von x_i in S/pS. Dann ist $\{\bar{x}_i\}$ eine Vektorraumbasis von S/pS über $k = R/p$. Weil der Verzweigungsindex gleich 1 ist, gilt

$$S/pS = S/P = k_L.$$

Nach 1.5.10 ist

$$\bar{d} := \det(\mathbf{Tr}_{L/K}(\bar{x}_i \bar{x}_j)) = d \bmod p$$

gerade die Restklasse von d in $k = R/p$. Die Erweiterung k_L/k ist genau dann separabel, wenn die durch die Spur definierte Bilinearform $k_L \times k_L \to k$, $(u,v) \mapsto \mathrm{Tr}(uv)$, nicht entartet ist, d.h. es gilt

$$k_L/k \text{ separabel} \Leftrightarrow \bar{d} \neq 0 \Leftrightarrow d\cdot R \text{ enthält eine Einheit} \Leftrightarrow \delta = d\cdot R \text{ ist gleich } R.$$

QED.

---

[26] Nach Definition der Differente gilt $\mathcal{D}\subseteq S$. Nach 1.3.6(iv) genügt es zu zeigen, $[S:\mathcal{D}] = R$. Es gilt

$$[S:\mathcal{D}] = N_{L/K}(\mathcal{D}) = \delta = R.$$

1.5.14 Zahm verzweigte Erweiterungen

Bezeichne χ die Charakteristik des Restklassenkörpers k = R/p. Die Erweiterung L/K heißt zahm verzweigt, wenn die folgenden Bedingungen erfüllt sind.
1. χ ist kein Teiler von e(L/K).
2. k_L/k ist separabel.

1.5.15 Theorem 5.2: Kriterium für zahm verzweigte Erweiterungen

Folgende Bedingungen sind äquivalent.
(i) L/K ist zahm verzweigt.
(ii) $\mathrm{Tr}_{L/K}(S) = R$.
(iii) $v_L(\mathcal{D}) = e(L/K) - 1$.

Beweis. Man beachte, $\mathrm{Tr}_{L/K}(S) \subseteq R$ ist stets ein (ganzes) Ideal von R.
(i) $\Rightarrow$ (ii). Sei $a \in S$ eine Einheit. Für die Restklasse von $\mathbf{Tr}_{L/K}(a) \in R$ in k = R/p gilt nach 1.5.10,

$$\overline{\mathbf{Tr}_{L/K}(a)} = e(L/K) \cdot \mathbf{Tr}_{k_L/k_K}(\bar{a}),$$

wobei $\bar{a}$ die Restklasse von a in k_L = S/P bezeichne. Weil L/K nach Voraussetzung zahm verzweigt ist, ist die Charakteristik von k kein Teiler von e(L/K), d.h. e(L/K) repräsentiert eine Einheit von k. Da a eine Einheit von S sein soll, ist $\bar{a}$ von Null verschieden, also auch

$$\mathbf{Tr}_{k_L/k_K}(\bar{a}) \neq 0$$

(denn andernfalls wäre die Spur identisch Null, also die Erweiterung k_L über k inseparabel und damit L/K nicht zahm verzweigt). Zusammen erhalten wir,

$$\overline{\mathbf{Tr}_{L/K}(a)} \neq 0.$$

Mit anderen Worten, das Ideal $\mathbf{Tr}_{L/K}(S)$ von R enthält eine Einheit $\mathbf{Tr}_{L/K}(a)$. Also gilt

$$\mathbf{Tr}_{L/K}(S) = R,$$

wie behauptet.
(ii) $\Rightarrow$ (i). Für jedes $a \in S$ gilt nach 1.5.10,

$$\overline{\mathbf{Tr}_{L/K}(a)} = e(L/K) \cdot \mathbf{Tr}_{k_L/k_K}(\bar{a}).$$

Wäre die Erweiterung k_L über k inseparabel, so wäre die Spur auf der rechte Seite für alle a Null. Falls die Charakteristik von k den Verzweigungsindex e(L/K) teilt, so wäre die rechte Seite ebenfalls Null. Zusammen ergibt sich

$$\overline{\mathbf{Tr}_{L/K}(a)} = 0 \tag{1}$$

für jedes $a \in S$, falls die Erweiterung L/K nicht zahm verzweigt ist. Nun hat aber (1) zur Folge, daß $\mathbf{Tr}_{L/K}(S) \subseteq p$ gelten muß, was im Widerspruch zu unserer Annahme $\mathbf{Tr}_{L/K}(S) = R$ steht. Also muß L/K zahm verzweigt sein.
(ii) $\Leftrightarrow$ (iii). Für $a \in K$ gilt wegen der K-Linearität der Spur $\mathbf{Tr}_{L/K}$

$$\mathbf{Tr}_{L/K}(Sa) = \mathbf{Tr}_{L/K}(S) \cdot a. \tag{2}$$

Bezeichnet $\mathcal{D} = \mathcal{D}(S/R)$ die Differente, so gilt

$$\mathcal{D}^{-1} = D_R(S) \qquad \text{(Definition 1.4.14)}$$
$$= \{a \in L \mid \mathbf{Tr}_{L/K}(Sa) \subseteq R\} \qquad \text{(Definition 1.3.8)}$$

also wegen (2),

$$\mathcal{D}^{-1} \cap K = \{a \in K \mid \mathbf{Tr}_{L/K}(S) \cdot a \subseteq R\}$$

d.h.

$$\text{(3)} \qquad \mathcal{D}^{-1} \cap K = \mathbf{Tr}_{L/K}(S)^{-1},$$

Wir setzen

$$r := v_K(\mathbf{Tr}_{L/K}(S))$$
$$v := v_L(\mathcal{D})$$

und wählen lokale Parameter π und ρ von R bzw. S,

$$p = \pi R$$
$$P = \rho S$$

Wir können annehmen, es gilt

$$\pi = \rho^e \text{ mit } e = e(L/K).$$

Dann gilt

$$\mathcal{D} = \rho^v S$$
$$\mathbf{Tr}_{L/K}(S) = \pi^r R$$

und Relation (3) bekommt die Gestalt

$$\text{(4)} \qquad (\rho^{-v} S) \cap K = \pi^{-r} R.$$

Aus (4) folgt insbesondere $\rho^{-re} S = \pi^{-r} S \subseteq \rho^{-v} S$, also $-re \geq -v$, d.h.

$$\text{(5)} \qquad r \leq \frac{v}{e}.$$

Außer (5) benötigen wir noch die Abschätzung

$$\text{(6)} \qquad \frac{v}{e} < r+1.$$

Angenommen, es wäre $\frac{v}{e} \geq r+1$, so wäre $-v \leq -e(r+1)$ also

$$\pi^{-r-1} = \rho^{-e(r+1)} \in (\rho^{-v} S) \cap K = \pi^{-r} R \text{ (nach (4))}$$

Durch Multiplikation mit π^{r+1} ergibt sich daraus $1 \in \pi R$, was nicht möglich ist. Damit ist auch die Abschätzung (6) bewiesen. Zusammen gilt also

$$\text{(7)} \qquad r \leq \frac{v}{e} < r+1.$$

Ist Bedingung (ii) erfüllt, so gilt $r = 0$, also $0 \leq v < e$, also $v \leq e-1$. Nach 1.5.11 muß dann aber sogar

$$v = e-1$$

gelten, d.h. Bedingung (iii) ist erfüllt. Ist umgekehrt Bedingung (iii) erfüllt, so erhalten wir aus $v=e-1$ und (7), daß $r = 0$ sein muß. Nach Definition von r bedeutet dies,

$$\mathbf{Tr}_{L/K}(S) = R,$$

d.h. es gilt (ii).
QED.

Bemerkung

Falls die Erweiterung L/K normal ist, kann man zum eben bewiesenen Kriterium eine weitere Bedingung hinzufügen.

1.5.16 Kriterium für zahm verzweigte Erweiterungen im normalen Fall

Sei L/K eine normale Erweiterung mit der Galois-Gruppe G und bezeichne

$R[G]$

den Gruppenring von G mit Koeffizienten aus R. Dann sind folgende Aussagen äquivalent.

(i) L/K ist zahm verzweigt.

(ii) S ist als R[G]-Modul isomorph zu R[G].

Beweis. (ii) $\Rightarrow$ (i). Sei φ: $R[G] \to S$ ein R[G]-linearer Isomorphismus und $x \in S$ das Bild des Einselements $e \in R[G]$ bei φ. Dann gilt

$$S = \sum_{g \in G} Rg(x),$$

wobei die Summe sogar eine direkte Summe ist. Insbesondere gibt es eindeutig bestimmte Elemente $r_g \in R$ mit

$$1 = \sum_{g \in G} r_g \cdot g(x).$$

Da 1 invariant unter der Operation von G ist, sind die Koeffizienten r_g ebenfalls unabhängig von g, $r_g = r \in R$. Damit gilt

$$1 = r \cdot \sum_{g \in G} g(x) = \sum_{g \in G} g(r \cdot x) = Tr_{L/K}(rx),$$

Es gibt ein Element in S mit der Spur 1. Nach 1.5.15 ist die Erweiterung L/K zahm verzweigt.

(i) $\Rightarrow$ (ii). Das ist eine Konsequenz des folgenden Satzes von Swan [4, Th. 6.1] bzw. eines Korollar dieses Satzes [Corollar 6.4].

Theorem von Swan

Seien G eine endliche Gruppe, A ein vollständiger lokaler Integritätsbereich und $j: A \to K$ die Einbettung in dessen Quotientenkörper. Dann ist der Homomorphismus

$$\mathbf{K}(A\text{-Proj}) \to \mathbf{K}(K\text{-Proj}),\ M \mapsto K \otimes_A M,$$

ein Monomorphismus. Dabei bezeichne A-Proj die Kategorie der endlich erzeugten A-Moduln und $\mathbf{K}(\mathcal{C})$ die Grothendieckgruppe der Kategorie.

Folgerung

Seien G eine endliche Gruppe, A ein vollständiger lokaler Integritätsbereich, K dessen Quotientenkörper und P,P' endlich erzeugte projektive A[G]-Moduln. Mit $K \otimes P \cong K \otimes P'$ gilt dann sogar $P \cong P'$.

Nach der Folgerung genügt es zu zeigen, S ist über R im zahm verzweigten Fall ein projektiver R-Modul.

QED.

Bemerkung

Nachfolgend geben wir eine Formulierung des Diskriminantenkriteriums 1.5.13 für unverzweigte Erweiterungen im globalen Fal an.

1.5.17 Unverzweigte Erweiterungen im globalen Fall

Seien (vorübergehend) R ein beliebiger Dedekindring mit dem Quotientenkörper K, L eine endliche separable Erweiterung von K und S die ganze Abschließung von R in L.

$$\begin{array}{ccc} K & \subseteq & L \\ \cup & & \cup \\ R & \subseteq & S \end{array}$$

Ein maximales Ideal $P \subset S$ heißt <u>unverzweigt</u> über K, wenn folgenden beiden Bedingungen erfüllt sind.

1. $e(P|R \cap P) = 1$.

2. S/P ist separabel über R/R∩P.

Ein maximales Ideal p⊂R heißt unverzweigt in L, wenn alle Primideale von S über p unverzweigt sind über K. Für maximale Ideale p⊂R sind folgende Aussagen äquivalent.

(i) p ist unverzweigt in L.

(ii) p ist kein Teiler der Diskriminante von S/R.

Beweis. Bezeichnungen:

L_P := Vervollständigung von L bezüglich der P-adischen Bewertung

K_p := Vervollständigung bezüglich der p-adischen Bewertung

Beim Übergang zu den Vervollständigungen bleiben Verzweigungsindex und Restklassenkörper unverändert. Die Diskriminante im vollständigen Fall ist gerade die Erweiterung der Ausgangsdiskriminante in den vervollständigten lokalen Ring, bzw. das Produkt der zu den einzelnen über p liegenden Primidealen P gehörigen Diskriminanten (vergleiche 1.4.15). Da die Diskriminante nach Konstruktion ein ganzes Ideal ist, folgt damit die Behauptung aus der analogen Aussage im lokalen Fall (d.h. aus 1.5.13).

QED.

1.5.18 Die Anzahl der Verzweigungsstellen

Seien (vorübergehend) R ein beliebiger Dedekindring mit dem Quotientenkörper K, L eine endliche separable Erweiterung von K und S die ganze Abschließung von R in L.

$$\begin{array}{ccc} K & \subseteq & L \\ \cup & & \cup \\ R & \subseteq & S \end{array}$$

Dann ist S/R in fast allen maximalen Idealen p ⊂ R unverzweigt (d.h. in allen mit Ausnahme von endlich vielen.

Beweis. In der Zerlegung der Diskriminante in ein Produkt von maximalen Idealen kommen nur endlich viele Faktoren vor.

QED.

1.6 Total verzweigte Erweiterungen

1.6.0 Bezeichnungen

R sein ein vollständiger diskreter Bewertungsring mit dem Quotientenkörper K, L eine endliche separable Erweiterung von L und S die ganze Abschließung in L. S sei ebenfalls ein vollständiger diskreter Bewertungsring.

$$\begin{array}{ccc} K & \subseteq & L \\ \cup & & \cup \\ R & \subseteq & S \end{array}$$

v_K bezeichne die Bewertung zum Bewertungsring R.

v_L bezeichne die Bewertung zum Bewertungsring S.

1.6.1 Eisenstein-Polynome

Ein Polynom g(X)∈K[X] separabel, wenn gilt

$$ggT(g(X), g'(X)) = 1,$$

d.h. wenn es in keiner Erweiterung von K mehrfache Nullstellen besitzt. Ein Eisenstein-Polynom ist ein separables Polynom

$$g(X) = X^m + c_{m-1}X^{m-1} + ... + c_1X + c_0 \in K[X],$$

dessen Koeffizienten den folgenden Bedingungen genügen.

$$\begin{aligned} v_K(c_i) &\geq 1 \text{ für } i=1,...,m-1 \\ v_K(c_0) &= 1 \end{aligned}$$

Bemerkung

Die Separabilitätsbedingung ist für die nachfolgenden Sätze nicht wesentlich. Nur weil wir uns generell auf die Betrachtung von separablen Erweiterungen beschränken, müssen wir die Separabilitätsbedingung auch hier stellen.

1.6.2 Total verzweigte Erweiterungen

Die Erweiterung L/K heißt total verzweigt wenn gilt

$$e(L/K) = [L:K], \text{ d.h. } f(L/K) = 1.$$

Bemerkung

Unser nächstes Ziel ist die Charakterisierung der total verzweigten Erweiterungen mit Hilfe der Eisenstein-Polynome. Dazu benötigen wir zunächst folgende Beschreibung der Elemente eines vollständigen bewerteten Körpers.

1.6.3 Die Elemente eines vollständig bewerteten Körpers

Seien Abbildungen

$$\prod: \mathbb{Z} \to K^*,\ n \mapsto \prod_n$$

$$r: k = R/p \to R$$

gegeben mit r(0) = 0 und derart, daß die Zusammensetzungen

$$\mathbb{Z} \xrightarrow{\prod} K^* \xrightarrow{v_K} \mathbb{Z}$$

$$k \xrightarrow{r} R \xrightarrow{\text{nat. Abb.}} k$$

gerade die identischen Abbildungen sind. Dann läßt sich jedes Element $a \in K$ auf genau eine Weise in der folgenden Gestalt

$$a = \sum_{n>>-\infty} a_n \prod_n \text{ mit } a_n \in \mathrm{Im}(r)$$

schreiben, wobei auch umgekehrt jede solche Reihe ein Element von K definiert. Der Wert des durch die Reihe definierten Elements a ist gleich

$$v(a) = \inf \{n \mid a_n \neq 0\}$$

Die Summationsvorschrift soll dabei bedeuten, daß die Koeffizienten a_n für kleine n Null sind.

Beweis. Nach Voraussetzung ist

$$v(\prod_n) = n,$$

die Folge der Werte der $\prod_n$ geht gegen unendlich. Deshalb konvergiert die Reihe

$$\sum_{n>>-\infty} a_n \prod_n$$

(nach dem Kriterium für Cauchy-Folgen). Weiter ist

$$a_k \prod_k = a - \sum_{-\infty<<n<k} a_n \prod_n \bmod p^{k+1} \tag{1}$$

Wegen $v(\prod_k) = k$ ist deshalb die Restklasse modulo p des Elements a_k durch a und alle vorangehenden Koeffizienten a_n festgelegt. Nach Voraussetzung gibt es aber in jeder Restklasse mod p genau ein Element, welches im Bild von r liegt. Bedingung (1) definiert also a_k mit Hilfe von a und den vorherigen Koeffizienten. Das beweist die Existenz- und Eindeutigkeitsaussage. Die Aussage über den Wert von a ist einfach zu beweisen.

QED.

1.6.4 Totale Verzweigung und Eisenstein-Polynome

(i) Eisenstein-Polynome sind irreduzibel. Ist Π die Nullstelle eines Eisenstein-Polynoms $g(X)\in K[X]$, so ist die Erweiterung $L = K[\Pi]$ total verzweigt und es gilt

(1) $$v_L(\Pi) = 1.$$

(ii) Ist umgekehrt L/K eine total verzweigte Erweiterung und $\Pi\in L$ ein Element welches der Bedingung (1) genügt, so ist das Minimalpolynom von Π über K ein Eisenstein-Polynom und es gilt

$$S = R[\Pi] \text{ und } L = K(\Pi).$$

Beweis. Zu (i).Sei

$$g(X) = X^m + c_{m-1}X^{m-1} + ... + c_1X + c_0 \in K[X],$$

ein Eisenstein-Polynom, Π ein Nullstelle von g und $L = K(\Pi)$. Wir setzen

$$n := [L:K] \text{ und } e := e(L/K).$$

Wegen $g(\Pi) = 0$ kann nicht $v(\Pi)<0$ gelten, denn sonst wäre

$$v_L(\Pi^m) = \min\{v_L(\Pi^m), v_L(c_{m-1}\Pi^{m-1}),...,v_L(c_0)\} = v_L(g(\Pi)) = v_L(0) = \infty.$$

Also gilt $\Pi^m\in P$, also $v_L(\Pi)\geq 1$. Sei s die ganze Zahl mit

(2) $$s \geq \frac{e}{v_L(\Pi)} > s-1.$$

Dann gilt

(3) $$m \geq n \geq e \geq s.$$

Wäre $m>s$, so wäre $v(\Pi^m)>e$ (nach (2)[27]). Außerdem gilt

$$v_L(c_i) = e\cdot v_K(c_i) \geq e$$

also

$$v_L(c_{m-1}\Pi^{m-1}+...+c_1\Pi) > e.$$

Zusammen ergibt sich damit $v_L(b_0) > e$, also $v_K(b_0) > 1$ im Widerspruch zur Voraussetzung, daß g ein Eisenstein-Polynom sein soll. Wir haben gezeigt, $m\leq s$, d.h. in (3) gilt überall das Gleichheitszeichen,

(4) $$m = n = e = s.$$

Insbesondere ist damit g irreduzibel und $f = \frac{n}{e} = 1$, d.h. die Erweiterung ist total verzweigt. Nach (2) ist weiter

$$v_L(\Pi) = 1.$$

Damit ist (i) bewiesen.

Zu (ii). Wir wenden 1.6.3 auf den Körper L an. Wegen $f(L/K) = 1$ können wir annehmen, das Repräsentantensystem Im(r) von S/P in S liegt sogar in R. Wir fixieren ein Element $c\in K$ mit $v_K(c) = 1$ und setzten

$$\Pi_{qe+r} := c^q\cdot\Pi^r.$$

Durch Umordnen der Glieder der Summe $\sum_n a_n\Pi_n$ sehen wir, es gilt

$$L = K[\Pi] \text{ und } S = R[\Pi].$$

Sei jetzt

$$g(X) = X^m + c_{m-1}X^{m-1} + ... + c_1X + c_0 \in K[X],$$

---

[27] Nach (2) ist $v_L(\Pi) \geq \frac{e}{s}$, also $v_L(\Pi^m) \geq m\cdot\frac{e}{s} > e$.

das Minimalpolynom von $\prod$ über K. Wegen L = K[$\prod$] ist dann g auch das charakteristische Polynom der K-linearen Abbildung, welche in der Multiplikation mit $\prod$ besteht[28]. Insbesondere ist

$$c_0 = \pm N_{L/K}(\prod).$$

Nach 1.5.8 ist

$$f = f \cdot v_L(\prod) = v_K(N_{L/K}(\prod)) = v_K(c_0),$$

wobei hier f = f(L/K) = 1 ist,

$$v_K(c_0) = v_L(\prod) = 1.$$

Das Polynom g mod p ist das charakteristische Polynom der Multiplikation mit $\prod$ der Elemente des k-Vektorraums S/pS. Diese Multiplikation ist wegen $\prod \in P$ nilpotent, d.h. es gilt

$$g(X) \equiv X^m \bmod p,$$

d.h. es ist $v_K(c_i) \geq 1$ für alle i. Mit anderen Worten, g ist ein Eisenstein-Polynom.

QED.

1.6.5 Total verzweigte Erweiterungen zu vorgegebenen Grad

Zu jeder vorgegebenen positiven ganzen Zahl n gibt es eine total verzweigte Erweiterung des Grades n von K.

Beweis. Wir wählen ein Element $c \in K$ mit dem Wert $v_K(c) = 1$. Dann ist

$$g(X) := X^n - cX - c$$

ein Eisenstein-Polynom und definiert damit eine total verzweigte Erweiterung vom Grad n.

QED.

Bemerkungen

Zum Abschluß dieses Abschnittes weisen wir auf einige Folgerungen des Satzes 1.6.4 hin, die wir hier nicht beweisen werden (siehe [3], Kapitel II).

(i) Sei

$$K := Q(F[[t]]) = \{ \sum_{n>>-\infty} a_n t^n \mid a_n \in F \}$$

der Körper der formalen Laurent-Reihen über einem Körper F. Dann kann man

$$\prod_n := t^n \text{ und } Im(r) = F$$

setzen (d.h. es ist $F \cong k$). In diesem Fall fallen die Charakteristiken der Körper K und k zusammen. Umgekehrt kann man in diesem charakeristik-gleichem Fall allgemein zeigen, daß K isomorph zum Körper der formalen Laurentreihen über k ist.

---

[28] Die Multiplikation mit $\prod$ hat die Matrix

$$A := \begin{pmatrix} 0 & 0 & \dots & -c_0 \\ 1 & 0 & \dots & -c_1 \\ 0 & 1 & \dots & -c_2 \\ \dots & \dots & \dots & \dots \\ 0 & \dots & 1 & -c_{m-1} \end{pmatrix}$$

Entwickeln von X·Id - A nach der ersten Zeile liefert (zusammen mit einem induktiven Argument) die Behauptung.

(ii) Ein typisches Beispiel für den charakeristik-ungleichen Fall ist der Körper der p-adischen Zahlen $\mathbb{Q}_p$.

(iii) Sei K von der Charakteristik 0 und k von der Charakteristik p>0, d.h. es liege der charakteristik-ungleiche Fall vor. Ist k perfekt, so kann man das Repräsentantensystem Im(r) derart wählen, daß es multiplikativ abgeschlossen ist, und zwar auf genau eine Weise.

(iv) Ist k ein beliebiger perfekter Körper positiver Charakeristik p, so gibt es bis auf Isomorphie genau einen diskret bewerteten Körper der Charakteristik 0 (und auf diesem Körper genau eine diskrete Bewertung) derart, daß der zugehörige Restklassenkörper isomorph zu k und der Wert der Primzahl p gerade gleich 1 ist,

$$v_K(p) = 1.$$

1.7 Unverzweigte Erweiterungen

1.7.0 Vorbemerkung

Die separable Erweiterung L von K induziert, wie wir wissen, eine algebraische Erweiterung des Restekörpers k. Wenn L/K unverzweigt ist, so ist nach Definition die zugehörige Erweiterung der Restekörper separabel. Eines der Ziele dieses Abschnitts besteht darin, in gewissem Sinne eine Umkehrung dieser Aussage zu beweisen: jede separable Erweiterung des Körpers k läßt sich auf genau eine (funktorielle) Weise zu einer unverzweigten Erweiterung des Körpers K anheben.

Situation:

$$\begin{array}{ccc} K & \subseteq & L \\ \cup & & \cup \\ R & \subseteq & S \\ \downarrow & & \downarrow \\ R/p & \hookrightarrow & S/P \\ || & & || \\ k & & k_L \end{array}$$

L/K endlich und separabel, K vollständing
R,S die diskreten Bewertungsring von K bzw. L

Wir beginnen damit, die unverzweigten Erweiterungen in einer ähnlichen Weise zu charakterisieren, wie wir im letzten Abschnitt die total verzweigten Erweiterungen charakterisiert haben.

Bezeichnungen

Für $a \in S$ bezeichne $\bar{a}$ die Restklasse von a in $k_L = S/P$. Für $g(X) \in S[X]$ bezeichne

$$\bar{g}(X) \in k_L[X],$$

das Polynom, welches man aus g erhält, indem man jeden Koeffizienten durch seine Restklasse in k_L ersetzt.

1.7.1 Unverzweigte Erweiterungen und über k irreduzible Polynome

(i) Sei L/K eine unverzweigte Erweiterung. Dann gibt es ein Element $x \in S$ mit

$$k_L = k[\bar{x}].$$

Für jedes solche Element $x \in S$ gilt

$$S = R[x] \text{ und } L = K[x]$$

und das Minimalpolynom g(X) von x über K hat die Eigenschaft, daß $\overline{g}(X) \in k[X]$ wohldefiniert[29], irreduzibel und separabel über k ist.

(ii) Sei $g(X) \in R[X]$ ein normiertes Polynom mit der Eigenschaft, daß $\overline{g}(X) \in k[X]$ irreduzibel und separabel über k ist. Dann ist für jede Nullstelle x von g die Erweiterung

$$L := K[x]$$

unverzweigt über K und es gilt $k_L = k[\overline{x}]$.

Bemerkung

Im nachfolgenden Beweis wird sogar gezeigt, daß in (i) für jedes $x \in S$ mit $k_L = k[\overline{x}]$ die übrigen Bedingungen von (i) automatisch erfüllt sind.

Beweis. Zu (i). Da k_L/k separabel und endlich erzeugt ist, gilt

$$k_L = k[\overline{x}]$$

für ein geeignetes Element $x \in S$. Für jedes solche x ist das Minimalpolynom G(X) von $\overline{x}$ separabel über k. Außerdem gilt, wenn man g wie in (i) wählt[30],

$$[L:K] \geq \deg g(X) \geq^{31} \overline{g}(X) \geq G(X) = [k_L:k] = f = e \cdot f = [L:K].$$

Damit gilt überall das Gleichheitszeichen. Insbesondere ist $\overline{g}(X) = G(X)$, d.h. $\overline{g}(X)$ ist irreduzibel und es ist L = K[x]. Es bleibt noch zu zeigen,

$$S = R[x].$$

Nach 1.4.16 (Beschreibung der Differente durch die Ableitung eines Polynoms) genügt es zu zeigen,

$$\mathcal{D}(S/R) = g'(x)S.$$

Weil K/R unverzweigt, also zahm verzweigt ist, gilt nach 1.5.15

$$v_L(\mathcal{D}(S/R)) = e-1 = 0,$$

also $\mathcal{D}(S/R) = S$. Es reicht zu zeigen,

$$g'(x)S = S.$$

Da $\overline{g}$ separabel ist, gilt $ggT(\overline{g}, \overline{g}') = 1$, d.h.

$$1 = \overline{a}(X)\,\overline{g}(X) + \overline{b}(X)\,\overline{g}'(X)$$

für geeignete Polynome $a,b \in R[X]$. Wir setzen $X = \overline{x}$ und erhalten

$$1 = \overline{b}(\overline{x})\,\overline{g}'(\overline{x}) = b(x)g'(x) \bmod P.$$

Mit anderen Worten g'(x) ist eine Einheit von S, d.h. es ist g'(x)S = S.

Zu (ii). Es gilt

$$[L:K] = \deg g \;=^{32} \deg \overline{g} = [k[\overline{x}]:k] \leq [k_L:k] \leq [L:K].$$

In der Abschätzung gilt somit überall das Gleichheitszeichen. Insbesondere ist

$$k_L = k[\overline{x}]$$

---

[29] d.h. $g \in R[X]$

[30] Das Polynom $\overline{g}$ ist dann wohldefiniert, d.h. die Koeffizienten von g liegen dann in R: wegen $x \in S$ ist x ganz über R. Dasselbe gilt auch für die Konjugierten von x über K, d.h. für die anderen Nullstellen von g. Damit sind auch die elementarsymmetrischen Funktionen in diesen Konjugierten ganz über R. Die Koeffizienten von g liegen also in K und sind ganz über R. Weil R ein Dedekindring ist, liegen diese Koeffizienten sogar in R.

Man beachte weiter, wegen g(x) = 0 ist auch $\overline{g}(\overline{x})=0$.

[31] Es gilt sogar "=", da der höchste Koeffizient eines Minimalpolynoms gleich 1 ist.

[32] g ist normiert

separabel und $e(L/K) = \frac{[L:K]}{[k_L:k]} = 1$, d.h. L/K ist unverzweigt.

QED.

1.7.2 Eine Familie von algebraischen Erweiterungen

Sei $\underline{E} := \{E\}$ eine Familie von algebraischen Erweiterungen eines festen Körpers F. Unter einem Homomorphismus

$$\sigma: E \to E'$$

über F von zwei Elementen der Familie wollen wir wie üblich einen Homomorphismus von Ringen verstehen, bei dem jedes Element von F in sich abgebildet wird. Es gilt:

1. Die identische Abbildung ist ein Beispiel für einen solchen Homomorphismus.
2. Die Komposition zweier Homomorphismen ist dann wieder ein Homomorphismus.

Mit anderen Worten, diese Homomorphismen bilden die Morphismen einer Kategorie, deren Objekte die Elemente von $\underline{E}$ sind.

Ist E/F eine endliche normale (separable) Erweiterung, so ist Hom(E,E) gerade die Galoisgruppe von E über F.
Ist E/F allgemein und bezeichnet

$$E^S$$

die separable Abschließung von F in E, d.h. die größte separable Teilerweiterung von E/F, so erhält man durch Einschränken eine Abbildung

$$\text{(1)} \qquad \mathrm{Hom}(E,E') \to \mathrm{Hom}(E^S,E'^S),$$

welche die Komposition und die identischen Morphismen erhält. Mit andern Worten, die Abbildung

$$E \mapsto E^S$$

definiert einen Funktor. Es gilt

3. Die Abbildung (1) ist injektiv (da die Fortsetzung auf rein inseparable Erweiterungen eindeutig ist, falls sie existiert).
4. Die Abbildung ist bijektiv im Fall $E=E^S$ (da das Bild einer separablen Erweiterung separabel ist).

Bemerkung
Wir wenden jetzt die obigen (trivialen) Beobachtungen auf die Familie aller endlichen separablen algebraischen Erweiterungen L des Körpers K an. Für die verschiedenen L werden wir die zugehörigen diskreten Bewertungsringe mit R_L bezeichnen und die zugehörigen Bewertungsideale mit p_L.

1.7.3 Verhalten der Bewertungen bei Homomorphismen

Sei $\sigma: L \to L'$ ein Homomorphismus von endlichen separablen Erweiterungen über K. Dann gilt für jedes $x \in L$

$$v_{L'}(\sigma x) = e(L'/\sigma L)\cdot v_L(x).$$

Beweis. Betrachten wir die Funktion

$$v: L \to \mathbb{Q},\ x \mapsto \frac{v_{L'}(\sigma x)}{e(L'/\sigma L)}.$$

Dies ist eine diskrete Bewertung des Körpers L, welche auf K mit v_L übereinstimmt,

$$\frac{v_{L'}(\sigma x)}{e(L'/\sigma L)} = e(L'|K)\cdot\frac{v_K(x)}{e(L'/\sigma L)} = e(\sigma L|K)\cdot v_K(x) = e(L|K)\cdot v_K(x) = v_L(x)$$

für $x \in K$. Wegen der Eindeutigkeit der Fortsetzung erhalten wir, daß sie mit v_L übereinstimmen muß.
QED.

Folgerungen

(i) Für normale (separable) Erweiterungen L/K ist die Bewertung von L invariant unter der Galoisgruppe G(L/K),

$$v_L(\sigma x) = v_L(x)$$

für $x \in L$, $\sigma \in G(L/K)$.

(ii) Jeder Homomorphismus $\sigma: L \to L'$ induziert einen lokalen Homomorphismus

$$R_L \to R_L',$$

der zugehörigen Bewertungsring und damit einen Homomorphismus

$$k_L \to k_L',$$

(iii) Die in (ii) definierte Abbildung

$$\mathrm{Hom}_K(L, L') \to \mathrm{Hom}_k(k_L, k_L',)$$

erhält die Komposition von Homomorphismen und die identischen Homomorphismen.

Bemerkungen

(i) Wir haben gezeigt, die Abbildung $L \mapsto k_L$ läßt sich zu einem Funktor fortsetzten von der Kategorie der endlichen separablen Körpererweiterungen von K mit Werten in der Kategorie der endlichen separablen Körpererweiterungen von k.

(ii) Die analoge Aussage gilt auch für die separable Abschließung, $L \mapsto k_L^s$.

(iii) Wir wenden uns jetzt der Frage zu, ob man die Nullstelle modulo eines Primideals von einem Polynom so abändern kann, daß sie zu einer Nullstelle wird. Dazu benötigen wir das nachfolgende Lemma.

1.7.4 Henselsches Lemma

Sei k ein vollständig bewerteter Körper bezüglich der nicht-archimedischen Bewertung[33] $|?|$ und sei

(1) $$f(X) \in \mathcal{O}[X]$$

ein Polynom, wobei $\mathcal{O}$ den Ring der ganzen Elemente bezüglich $|?|$ bezeichne[34]. Weiter gelte

(2) $$|f(\alpha_0)| < |f'(\alpha_0)|^2$$

für ein $\alpha_0 \in \mathcal{O}$. Dann gibt es ein $\alpha \in \mathcal{O}$ mit $f(\alpha)=0$ und

(3) $$|\alpha - \alpha_0| \le |f(\alpha_0)|/|f'(\alpha_0)|$$

Beweis. Wir betrachten die Taylor-Entwicklung

(4) $$f(X+Y) = f(X) + f_1(X)Y + \ldots + f_j(X)Y^j$$

von f an der Stelle X. Man beachte es gilt $f_1(X) = f'(X)$. Das Element $\beta_0 \in \mathcal{O}$ sei so gewählt, daß gilt[35]

(5) $$f(\alpha_0) + f_1(\alpha_0)\cdot\beta_0 = 0.$$

Es reicht zu zeigen, es gilt

(6) $$|f(\alpha_0 + \beta_0)| < |f(\alpha_0)|$$

---

[33] d.h. die Bewertung sei von der Gestalt $|?| = \rho^{v(?)}$ mit einer diskreten Bewertung v.

[34] d.h. den Bewertungsring zur diskreten Bewertung v.

[35] Wegen (2) ist $f'(\alpha_0) \neq 0$, d.h. Gleichung (5) besitzt eine Lösung β_0. Wegen

$$|\beta_0| = |f(\alpha_0)/f_1(\alpha_0)| \le |f_1(\alpha_0)| \le 1$$

liegt diese automatisch in $\mathcal{O}$. Man beachte, die erste Abschätzung besteht wegen (2), die zweite, weil α_0, also auch $f_1(\alpha_0)$, in $\mathcal{O}$ liegt.

(7) $|f_1(\alpha_0 + \beta_0)| = |f_1(\alpha_0)|$

(8) $|\beta_0| \leq |f(\alpha_0)/f_1(\alpha_0)|$

Wegen (6) und (7) ist dann nämlich Bedingung (2) auch mit $\alpha_1 := \alpha_0 + \beta_0$ anstelle von α_0 erfüllt. Man kann deshalb die eben durchgeführte Konstruktion mit α_1 anstelle von α_0 wiederholen und erhält eine Folge

$$\{\alpha_i\}$$

von Elementen aus $\mathcal{O}$ mit[36]

(9) $|\alpha_{i+1} - \alpha_i| \leq |f(\alpha_i)/f_1(\alpha_i)| < |f(\alpha_{i-1})/f_1(\alpha_{i-1})| < \ldots < |f(\alpha_0)/f_1(\alpha_0)|.$

Insbesondere ist diese Folge konvergent[37],

$$\alpha_i \longrightarrow \alpha \text{ in } k.$$

Weil die α_i in $\mathcal{O}$ liegen, gilt dasselbe für α.[38] Wegen (6) ist die Folge der $f(\alpha_i)$ eine Nullfolge, d.h. es gilt

$$f(\alpha) = 0.$$

Die Abschätzung (3) ergibt sich aus (9) (und der verschärften Variante der Dreiecksungleichung).

Beweis von (8). Folgt aus der Definition von β_0 (vgl. (5)). Es gilt sogar das Gleichheitszeichen.

Beweis von (6). Wir setzen in der Taylor-Entwicklung (4) die Werte $X = \alpha_0$ und $Y = \beta_0$ ein. Wegen (5) wird dann die Summe der ersten beiden Glieder rechts gleich Null. Es folgt

$$\begin{aligned} |f(\alpha_0+\beta_0)| &\leq \max \{|f_j(\alpha_0)\beta_0^j| : j\geq 2\} \\ &\leq \max \{|\beta_0^j| : j\geq 2\} \end{aligned}$$

(wegen $f_j(\alpha_0) \in \mathcal{O}$). Die Norm von β_0 ist kleiner als 1,

$$|\beta_0| = |f(\alpha_0)/f_1(\alpha_0)| < |f_1(\alpha_0)| \leq^{39} 1.$$

Deshalb ist das Maximum rechts gleich der Norm der niedrigsten Potenz,

$$\begin{aligned} |f(\alpha_0+\beta_0)| \leq |\beta_0|^2 &= \frac{|f(\alpha_0)|^2}{|f_1(\alpha_0)|^2} \\ &< |f(\alpha_0)| \qquad \text{(nach (2)).} \end{aligned}$$

Beweis von (7).
Wir verwenden die Tayler-Entwicklung von $f_1 = f'$,

---

[36] Wegen (8).

[37] Die zugehörige Folge der additiven Bewerturngen $\log |\alpha_{i+1} - \alpha_i|$ geht gegen ∞, d.h. die Folge der $|\alpha_{i+1} - \alpha_i|$ geht gegen Null. Dann ist aber $\{\alpha_i\}$ eine Cauchy-Folge (wegen der verschärften Variante der der Dreiecksungleichung):

$$|\alpha_{i+n} - \alpha_i| \leq \max (|\alpha_{i+1} - \alpha_i|, \ldots, |\alpha_{i+n} - \alpha_{i+n-1}|)$$

[38] $\mathcal{O} = \{x \in k \mid |x| \leq 1\}$ ist abgeschlossen in k.

[39] weil α_0, also auch $f_1(\alpha_0)$ in $\mathcal{O}$ liegt.

$$f_1(X+Y) = f_1(X) + f'_1(X)Y+...+f'_j(X)Y^j$$

anstelle der von f. Wie oben setzen wir $X = \alpha_0$ und $Y = \beta_0$ und erhalten

$$f_1(\alpha_0+\beta_0) - f_1(\alpha_0) = f'_1(\alpha_0)\beta_0+...+f'_j(\alpha_0)(\beta_0)^j$$

also wie oben

$$\begin{aligned} |f_1(\alpha_0+\beta_0) - f_1(\alpha_0)| &\leq \max\{|f'_j(\alpha_0)\beta_0^j| : j\geq 1\} \\ &= |\beta_0| \\ &= |f(\alpha_0)/f_1(\alpha_0)| \\ &< |f_1(\alpha_0)| \qquad \text{(nach (2)).} \end{aligned}$$

Damit ist aber

$$|f_1(\alpha_0 + \beta_0)| = \max\{|f_1(\alpha_0+\beta_0) - f_1(\alpha_0)|, |f_1(\alpha_0)|\} = |f_1(\alpha_0)|.$$

QED.

Folgerung

Seien $g(X)\in R[X]$ ein normiertes Polynom mit der Eigenschaft, daß $\bar{g}(X)$ separabel ist, und sei $\alpha_0\in k$ eine Nullstelle von $\bar{g}$. Dann gibt es in R genau ein Element α mit

$$g(\alpha) = 0 \text{ und } \bar{\alpha} = \alpha_0.$$

Beweis. Wir wenden das Henselsche Lemma mit k = K, $\mathcal{O}$ = R und f = g an. Bedingung (2) ist erfüllt wegen

$$f(\alpha_0) \in p \text{ (:= maximales Ideal von R)}$$

und

$$f'(\alpha_0) \notin p.$$

Die Existenz von α folgt damit aus dem Henselschen Lemma. Gäbe es mehr als eine Lösung α der Gleichung g(X) = 0 mit $\bar{\alpha} = \alpha_0$, so wäre die Restklasse von α eine mehrfache Nullstelle von $\bar{g}$ im Widerspruch zur Annahme, daß $\bar{g}$ separabel ist.

QED.

1.7.5 Anhebung separabler zu unverzweigten Erweiterungen

Sei k' eine endliche separable algebraische Erweiterung von k. Dann gibt es eine endliche separable algebraische Erweiterung

$$L = L(k')$$

von K mit folgenden Eigenschaften.

(i) $k' \cong k_L$ (über k).

(ii) L/K ist unverzweigt.

(iii) Die Abbildung $\mathrm{Hom}_K(L,L') \rightarrow \mathrm{Hom}_k(k_L,k_{L'})$ ist bijektiv für jede endliche separable algebraische Erweiterung L' von K.

Durch die Bedingungen (i)und (ii) bzw. (i) und (iii) ist die Erweiterung L/K bis auf Isomorphie eindeutig charakterisiert.

Bemerkung

In Bedingung (iii) kann man die Körper k_L und $k_{L'}$ durch die separablen Abschließungen k_L^s bzw. $k_{L'}^s$, ersetzen.

Beweis. Nach Voraussetzung ist k'/k endliche separable Körpererweiterung. Es gibt also ein Element $\alpha\in k'$ mit

$$k' = k[\alpha].$$

Bezeichne $G(X) \in k[X]$ das Minimalpolynom von α über k. Wir wählen ein normiertes Polynom

$$g(X) \in R[X] \text{ mit } \bar{g}(X) = G(X)$$

und setzen

$$L := K[x],$$

wobei x eine Nullstelle von g sei. Wir können dann annehmen $\bar{x} = \alpha$ [40], sodaß

$$k_L = k[\bar{x}] = k'$$

gilt, d.h. Bedingung (i) ist erfüllt. Nach Konstruktion ist α separabel über k, d.h. das Polynom $\bar{g}$ ist separabel. Nach 1.7.1(ii) ist L/K unverzweigt, d.h. Bedingung (ii) ist erfüllt. Zum Nachweis von Bedingung (iii) betrachten wir einen beliebigen Homomorphismus

$$w: k_L \to k_L, \text{ über } k.$$

Nach der Folgerung des Henselschen Lemmas 1.7.4 existiert genau eine Element $y \in S$ mit $g(y) = 0$ und $\bar{y} = w(\bar{x})$. Damit gibt es aber auch einen Homomorphismus

$$\sigma: L = K[x] \to L', \; x \mapsto y,$$

über dem Körper K mit $\bar{\sigma} = w$.[41] Ist τ ein zweiter solcher Homomorphismus, so gilt

$$g(\tau(x)) = \tau(g(x)) = 0 \text{ und } \overline{\tau(x)} = w(\bar{x}) = \bar{y}.$$

Weil $\bar{g}$ separabel ist[42], folgt $\tau(x) = y$, also $\tau = \sigma$. Damit sind die Aussagen (i) - (iii) bewiesen.

Wir haben noch zu zeigen, die Körpererweiterung L/K ist durch (i) und (ii) bzw. (i) und (iii) bis auf Isomorphie festgelegt.

Sei L' ein Körper, welcher den Bedingungen (i) und (ii) genügt, d.h. L'/K sei unverzweigt und $k_{L'}$ sei k-isomorph zu k_L. Wir fixieren einen k-Isomorphismus

$$w: k_L \to k_{L'},$$

Wie wir gezeigt haben, läßt sich w zu einen Homomorphismus

$$\sigma: L \to L'$$

anheben.Weil L'/K und L/K unverzweigt sind, gilt

$$[L':K] = [k_{L'}:k] = [k_L:k] = [L:K],$$

d.h. σ ist ein Isomorphismus. Die Eigenschaften (i) und (ii) legen den Körper L folglich bis auf Isomorphie fest.
Betrachten wir den Funktor

$$\left\{ \begin{matrix} \text{endliche unverzweigte} \\ \text{Erweiterungen von K} \end{matrix} \right\} \to \text{Ens}, \; L' \mapsto \text{Hom}_k(\bar{k}, k_{L'})$$

Bedingungen (i) und (iii) besagen gerade, daß dieser Funktor darstellbar und L ein darstellendes Objekt ist.[43] Als solches ist L bis auf Isomorphie eindeutig bestimmt.[44]

---

[40] Die Restklassen der Nullstellen von g sind Nullstellen von $\bar{g}$. Verschiedene Nullstellen von g liefern verschiedene von $\bar{g}$ (da $\bar{g}$ separabel ist). Beide Polynome haben denselben Grad, also dieselbe Nullstellenzahl. Also kommt jede Nullstelle von $\bar{g}$ von einer Nullstelle von g.

[41] $\bar{\sigma}$ und w haben im Erzeuger $\bar{x}$ denselben Wert.

[42] d.h. die Restklassen in $k_{L'}$ von verschiedenen Nullstellen von g sind verschieden.

[43] d.h. bis auf Isomorphie ist dies gerade der Funktor

$$L' \mapsto \text{Hom}_K(L, L').$$

[44] L läßt sich durch eine Universalitätseigenschaft beschreiben: L ist eine unverzweigte Erweiterung mit $k' \hookrightarrow k_L$, und für jede unverzweigte Erweiterung L' mit

QED.

1.7.6 Anhebung normaler Erweiterungen

Die Erweiterung L(k') von 1.7.5 ist genau dann normal über K, wenn k' normal über k ist. Die Galois-Gruppen der beiden Erweiterung sind in diesem Fall isomorph,

$$G(L(k')/K) \cong G(k'/k).$$

Beweis. Betrachten wir den Funktor

$$\left(\begin{array}{c}\text{endliche unverzweigte}\\ \text{Erweiterungen von K}\end{array}\right) \to \left(\begin{array}{c}\text{endliche separable}\\ \text{Erweiterungen von k}\end{array}\right), \; L \mapsto k_L$$

Die Aussage von 1.7.5 bedeutet, dieser Funktor ist eine Äquivalenz von Kategorien. Nun läßt sich die Normalität einer Körpererweiterung L/K in der Sprache der Kategorien formulieren: für jedes Objekt L', welches L als Teilobjekt enthält und für jedes kommutative Diagramm

$$\begin{array}{ccc} L & \xrightarrow{\;f\;} & L' \\ \uparrow & & \uparrow \\ K & = & K \end{array}$$

faktorisiert sich f über das Teilobjekt L von L'. Die Eigenschaft, normale Erweiterung zu sein, bleibt daher beim Anwenden einer Äquivalenz von Kategorien erhalten.
QED.

1.7.7 Vereinbarung zum Begriff 'Teilkörper'

Ein Teilkörper der Erweiterung L von K sei im folgenden stets ein Teilkörper von L, welcher den Körper K enthält.

1.7.8 Die maximale unverzweigte Erweiterung, Trägheitsgruppe

(i) Es gibt einen Zwischenkörper L_0,

$$K \subseteq L_0 \subseteq L$$

mit der Eigenschaft, daß jede unverzweigte Erweiterung L' von K mit L'⊆L ganz in L_0 liegt und umgekehrt jede ganz in L_0 liegende Erweiterung von K unverzweigt ist.

(ii) Es gilt $k_{L_0} = k_L^s$.

(iii) Ist L/K eine normale Erweiterung mit der Galois-Gruppe G=G(L/K), so ist die Erweiterung L_0/K ebensfalls normal und fällt mit dem Fixkörper der folgenden Gruppe zusammen.

$$G_0 := \{g \in G \mid v_L(g(x)-x) > 0^{45} \text{ für alle } x \in R_L\}.$$

Diese Gruppe G_0 heißt Trägheitsgruppe der Erweiterung L/K.

Definition
Die Vereinigung K_{nr} aller unverzweigten Erweiterungen von L von K, welche in einer gegebenen separablen Abschließung von K liegen, heißt maximale unverzweigte Abschließung von K.

(*) $$k' \hookrightarrow k_{L'}$$

gibt es genau einen K-Homomorphismus f: L ⟶ L' derart, daß (*) gerade die Einschränkung auf k' der durch f induzierten Abbildung $k_L \longrightarrow k_{L'}$ ist.

[45] d.h. g(x) ≡ x mod P, wenn P das maximale Ideal von R_L bezeichnet (d.h. das Bewertungsideal).

Beweis. Zu (i) und (ii). Sei k' die separable Abschließung von k in k_L. Nach 1.7.5 gibt es dann einen Zwischenkörper L_0,

$$K \subseteq L_0 \subseteq L,$$

mit $k_{L_0} = k'$, welcher über K unverzweigt ist. Sämtliche Zwischenkörper L',

$$K \subseteq L' \subseteq L_0,$$

sind dann ebenfalls unverzweigt über K (nach Definition des Begriffs der unverzweigten Erweiterung).
Sei jetzt umgekehrt L' eine Erweiterung von K ganz in L, welche über K unverzweigt ist. Dann gilt

$$k_{L'} \subseteq k_L^s = k_{L_0}.$$

Nach 1.7.5 läßt sich die Inklusion $k_{L'} \to k_{L_0}$ anheben zu einem K-Homomorphismus

$$\sigma: L' \to L_0.$$

Wir wählen ein Element $x \in L'$ mit $k_{L'} = k[\bar{x}]$. Dann sind x und $\sigma(x)$ Elemente von L mit derselben Restklasse in k_L (da $\bar{\sigma}$ die natürliche Einbettung ist). Nach der Folgerung aus dem Henselschen Lemma 1.7.4 ergibt sich $x=\sigma(x)$ und nach 1.7.1(i) ist $L'=K[x]$, also σ die identische Abbildung und damit $L' \subseteq L_0$.

Zu (iii). Sei jetzt L/K eine normale Erweiterung. Alle konjugierten von L_0 über K sind dann unverzweigte Erweiterungen von K, die wieder in L liegen und nach Konstruktion von L_0 damit sogar in L_0. Aus Gradgründen sind diese Konjugierten sogar gleich L_0, d.h. L_0 ist normal über K. Wir haben noch die Galois-Gruppe von L/L_0 mit der Trägheitsgruppe zu vergleichen. Nach Definition ist die Trägheitsgruppe von L/K gerade der Kern des Homomorphismus

$$G(L/K) = \mathrm{Hom}_K(L,L) \to \mathrm{Hom}_k(k_L, k_L) = G(k_L/k).$$

Wie schon früher bemerkt ist der Einschränkungshomomorphismus

$$\mathrm{Hom}_k(k_L, k_L) \to \mathrm{Hom}_k(k_L^s, k_L^s)$$

injektiv. Die Trägheitsgruppe ist deshalb auch der Kern der Abbildung,

$$G(L/K) \to G(k_L^s/k).$$

Nach 1.7.5(iii) ist $G(L_0/K) = G(k_L^s/k)$, also

$$G_0 = \mathrm{Ker}(G(L/K) \to G(L_0/K)) = G(L/L_0).$$

Insbesondere ist L_0 der Fixkörper dieser Gruppe.

QED.

1.7.9 Komposition unverzweigter Erweiterungen

Die Komposition LL'/K von zwei unverzweigten Erweiterungen L/K und L'/K innerhalb einer gegebenen separablen Abschließung von K ist unverzweigt.
Beweis. Sei E/K eine separable Erweiterung von K, welche die beiden Körper L und L' enthält. Nach 1.7.8 liegen dann L und L' ganz in der maximalen unverzweigten Erweiterung E_0 von K in E. Dann gilt aber auch $LL' \subseteq E_0$, d.h. LL' ist unverzweigt über K.
QED.

1.7.10 Die Galois-Gruppe von K_{nr}/K

(i) Jede endliche Erweiterung L des Körpers K, welche ganz in K_{nr} liegt, ist unverzweigt über K.

(ii) Die Galois-Gruppe von K_{nr} über K ist (als topologische Gruppe) isomorph zur Galois-Gruppe der separablen Abschließung $\overline{k}^s$ des Körpers k,

$$G(K_{nr}/K) \cong G(\overline{k}^s/k)$$

Beweis. Zu (i). Jedes Element von L liegt nach Voraussetzung in K_{nr}, also in einer unverzweigten Erweiterung von K, erzeugt also selbst eine unverzweigte Erweiterung von K. Da die Komposition unverzweigter Erweiterungen nach 1.7.9 unverzweigt ist, erzeugen auch jeweils endlich viele Elemente von L eine unverzweigte Erweiterung. Also ist L selbst auch unverzweigt über K.
Zu (ii). Es gilt

$$G(K_{nr}/K) = \varprojlim_L G(L/K)$$
$$G(\overline{k}^s/k) = \varprojlim_L G(k_L/k)$$

wobei die inversen Limites über alle endlich erzeugten Teilerweiterungen L von K_{nr} zu nehmen sind. Da diese Teilerweiterungen L nach (i) unverzweigt sind, sind die endlichen Gruppen unter dem Limeszeichen rechts in natürlicher Weise isomorph. Also gilt dasselbe für die inversen Limites.
QED.

1.7.11 Die Erweiterung K_{nr}/K im Fall $\#k = p^n$ endlich

Sei k ein endlicher Körper mit $q = p^n$ Elementen,

$$k = \mathbb{F}_q,\ q = p^n.$$

Fakt aus der Theorie der endlichen Körpererweiterungen:
Jede endliche Körpererweiterung k'/k ist eine Galoiserweiterung mit einer zyklischen Galoisgruppe (der Ordnung [k':k]). Ein erzeugendes Element ist der Frobenius-Automorphismus

$$F^q: k' \to k',\ \alpha \mapsto \alpha^q.$$

Folgerung 1
Für die Körpererweiterung k'/k vom Grad n hat man deshalb einen Isomorphismus

$$\mathbb{Z}/n\mathbb{Z} \to G(k'/k),\ (i \bmod n) \mapsto (F^q)^i.$$

Die Gruppen auf der linken Seite bilden genauso wie die Gruppen rechts ein inverses System. Durch Übergang zum inversen Limes erhalten wir

$$\hat{\mathbb{Z}} := \varprojlim_n \mathbb{Z}/n\mathbb{Z} = G(\overline{k}^s/k) = G(K_{nr}/K).$$

Die Gruppe links ist die Vervollständigung der diskreten Gruppe $\mathbb{Z}$ bezüglich der Topologie, welche als Umgebungsbasis der 0 alle Untergruppen

$$n\mathbb{Z} \subseteq \mathbb{Z}$$

mit endlichem Index hat.
Folgerung 2
Es gibt genau ein Element $\sigma_q \in G(K_{nr}/K)$ mit folgender Eigenschaft. Ist L/K eine endliche Teilerweiterung von K_{nr}/K, gilt

$$\sigma_q(a) \equiv a^q \bmod p_L$$

für jedes $a \in R_L$. Dieses Element σ_q heißt Frobenius-Substitution.

Folgerung 3
Für jede ganze Zahl n>0 gibt es bis auf Isomorphie über K genau eine unverzweigte Erweiterung L/K des Grades n. Diese Erweiterung ist normal und hat eine zyklische Galois-Gruppe.
Beweis. Nach 1.7.5 ist der Funktor

$$L \mapsto k_L$$

eine Äquivalenz von Kategorien und erhält insbesondere die (die Hom-Mengen also auch die) Galois-Gruppen und die Eigenschaft normale Erweiterung zu sein. Die Behauptung ergibt sich damit aus der Tatsache, daß Erweiterungen von endlichen Körpern stets normal sind und eine zyklische Galoisgruppe besitzen.
QED.

Folgerung 4
Die maximale unverzweigte Erweiterung K_{nr}/K wird erzeugt von der Menge aller m-ten Einheitswurzeln, wobei m alle zu p teilerfremden Zahlen durchläuft.
Beweis. Jeder endliche Körper k' besteht neben der Null ausschließlich aus Einheitswurzeln: wenn die Elementzahl von k' gleich $q' = p^{n'}$ ist, so sind die Elemente von k' gerade die Nullstellen von

$$X^{q'}-X,$$

denn die multiplikative Gruppe von k' hat die Ordnung q'-1. Also wird $\overline{k}^s/k$ von den Einheitswurzeln erzeugt. Dabei kann man die p-ten Einheitswurzeln weglassen, da endliche Körper perfekt sind. Ist $\overline{g}$ das Minimalpolynom einer endlichen Körpererweiterung k_L/k und g ein Repräsentant von $\overline{g}$ mit Koeffizienten aus R, so ist L/K nach 1.7.1 gerade die durch g definierte Körpererweiterung. Mit anderen Worten die Erweiterung L/K wird durch m-te Einheitswurzeln erzeugt, wobei man annehmen kann, daß m teilerfremd zu p ist.
QED.

1.7.12 Verhalten der Einheiten bei der Normabbildung einer unverzweigten Erweiterung

Analog zu den Bezeichnungen am Ende von 1.1 benutzen wir folgende Bezeichnungen für die Einheitengruppen.

$$U_{L,i} := 1 + \mathfrak{P}_L^i,$$

wobei $\mathfrak{P}_L$ das Bewertungsideal von L sei. Entsprechend sei auch

$$U_{K,i} := 1 + \mathfrak{P}_K^i.$$

Dann gilt, falls L/K unverzweigt ist,

$$N_{L/K}(U_{L,i}) = U_{K,i}.$$

Beweis. Wir wählen ein Element $\pi \in K$ mit $v_K(\pi) = 1$, also

$$v_L(\pi) = v_K(\pi) = 1.$$

Die Einheitengruppe $U_{L,i}$ besteht dann aus den Elementen der Gestalt

(1) $$u = 1 + \pi^i\alpha \text{ mit } \alpha \in R_L.$$

Sei

$$n := [L:K].$$

Das Charakteristische Polynom des Elementes $\pi^i\alpha$ kann man dann in der folgenden Gestalt schreiben.

$$\begin{aligned} h(X) &:= \chi_{\pi^i\alpha}(X) \\ &= \det(X\cdot Id - mult(\pi^i\alpha)) \\ &= X^n - \pi^i\cdot Tr_{L/K}(\alpha)\cdot X^{n-1} + \pi^{i+1}\cdot h_1(X). \end{aligned}$$

Man beachte, multipliziert man die Unbestimmte X und das Element $\pi^i\alpha$ mit demselben Faktor $\lambda\in K$, so multipliziert sich h(X) mit dem Faktor λ^n. Das bedeutet, der Koeffizient von X^{n-j} in h(X) spaltet den Faktor λ^j ab, wenn man das Element $\pi^i\alpha$ mit λ multipliziert. Für das charakteristische Polynom von (1) erhalten wir,

$$\chi_u(X) = \det(X\cdot Id - mult(u)) = \det((X-1)\cdot Id - mult(\pi^i\alpha)) = h(X-1).$$

Damit gilt

$$N_{L/K}(u) = (-1)^n\cdot\chi_u(0) = (-1)^n\cdot h(-1)$$

$$(2) \qquad \equiv 1 - \pi^i\cdot Tr_{L/K}(\alpha) \pmod{\mathfrak{P}_K^{i+1}}$$

Aus dieser Kongruenz folgt zunächst einmal die Inklusion

$$(3) \qquad N_{L/K}(U_{L,i}) \subseteq U_{K,i}.$$

Da unverzweigte Erweiterungen auch zahm verzweigt sind, gilt auf Grund der Charakterisierung 1.5.15 zahm verzweigter Erweiterungen

$$Tr_{L/K}(R_L) = R_K.$$

Für jedes Element

$$v = 1 - \pi^i\beta \in U_{K,i}$$

gibt es also ein $\alpha\in R_L$ mit $Tr_{L/K}(\alpha) = \beta$. Nach (2) folgt mit $u := 1 + \pi^i\alpha$,

$$N_{L/K}(u) \equiv 1 - \pi^i\cdot Tr_{L/K}(\alpha) = 1 - \pi^i\beta = v \pmod{\mathfrak{P}_K^{i+1}}$$

also

$$N_{L/K}(u)^{-1}\cdot v \equiv 1 \pmod{\mathfrak{P}_K^{i+1}}$$

also

$$N_{L/K}(u)^{-1}\cdot v \in U_{K,i+1}.$$
$$v \in N_{L/K}(u)\cdot U_{K,i+1}$$

Wir haben gezeigt[46],

$$N_{L/K}(U_{K,i})\cdot U_{K,i+1} = U_{K,i}.$$

Da die beteiligten Körper und Gruppen vollständig sind, folgt durch Iteration und Grenzübergang

$$N_{L/K}(U_{K,i}) = U_{K,i}.$$

QED.

1.7.13 Das Bild der Normabbildung

Sei L unverzweigt über K. Dann liegt eine Einheit $\alpha\in U_K$ von K genau dann im Bild der Normabbildung

$$N_{L/K}: U_L \to U_K,$$

wenn die Restklasse

$$\alpha \pmod{\mathfrak{P}_K} \in k$$

---

[46] "$\subseteq$" gilt trivialerweise.

dieser Einheit im Bild der Normabbildung

$$N_{k_L/k}: k_L \to k$$

liegt. Insbesondere gilt, wenn k endlich ist,

$$N_{L/K}(U_L) = U_K .$$

Beweis. In 1.5.10 haben wir gesehen, die Normabbildung kommutiert mit dem Übergang zu den Restklassen (bis auf einen Exponenten, der im unverzweigten Fall gleich 1 ist). Aus der entsprechenden Formel und der Tatsache, daß alle beteiligten Körper vollständig sind, folgt der erste Teil der Behauptung.

Im Fall k endlich von der Ordnung $q=p^m$, besteht k aus den Nullstellen des Polynoms X^q-X,

$$k = \{\alpha \in \overline{k} \mid \alpha^q-\alpha = 0\}.$$

Analog ist dann k_L endlich von der Ordnung q^n und

$$k_L := \{\alpha \in \overline{k} \mid \alpha^{q^n}-\alpha = 0\}$$

Die Galoisgruppe $G(k_L/k)$ wird von der m-ten Potenz der Frobeniusabbildung F erzeugt und hat die Ordnung n. Also gilt

$$N_{k_L/k}(u) = \prod_{i=0}^{n-1} F^{im}(u) = \prod_{i=0}^{n-1} u^{p^{im}} = \prod_{i=0}^{n-1} u^{q^i} = u^s \text{ mit } s:= \sum_{i=0}^{n} q^i$$

Die Fasern der Abbildung

(1) $$N_{k_L/k}: k_L^* \to k^*$$

bestehen daher aus $s:= \sum_{i=0}^{n} q^i = \frac{q^n-1}{q-1}$ Elementen[47]. Das Bild der Normabbildung (1) besteht also aus

$$\frac{\#k_L}{s} = \frac{q^n-1}{s} = q-1$$

Elementen. Mit anderen Worten, die Normabbildung (1) ist surjektiv.

QED.

1.8 Zahm verzweigte Erweiterungen

1.8.1 Bezeichnungen

Die Voraussetzungen und Bezeichnungen seien dieselben wie in 1.6 und 1.7. Genauer:

R sei ein vollständiger diskreter Bewertungsring mit dem Quotientenkörper K, L eine endliche separable Erweiterung von L und S die ganze Abschließung in L. S sei ebenfalls ein vollständiger diskreter Bewertungsring.

$$\begin{array}{ccc} K & \subseteq & L \\ \cup & & \cup \\ R & \subseteq & S \end{array}$$

v_K bezeichne die Bewertung zum Bewertungsring R.

v_L bezeichne die Bewertung zum Bewertungsring S.

---

[47] Je zwei Elemente aus derselben Faser haben einen Quotienten, der eine s-te Einheitswurzel ist. Man beachte, s ist teilerfremd zur Charakteristik p, d.h. das Polynom X^s-1 ist separabel.

Für $a \in S$ bezeichne $\bar{a}$ die Restklasse von a in $k_L = S/P$. Für $g(X) \in S[X]$ bezeichne

$$\bar{g}(X) \in k_L[X],$$

das Polynom, welches man aus g erhält, indem man jeden Koeffizienten durch seine Restklasse in k_L ersetzt.

Die Charakteristik von des Restklassenkörpers k werde mit χ bezeichnet.

$$\chi := \mathrm{char}(k).$$

Unter einem Teilkörper von L wollen wir einen Körper zwischen K und L verstehen. Die Trägheitsgruppe werde mit G_0 bezeichnet (im Fall, daß L/K normal ist).

$$G_0(L/K) := \{g \in G(L/K) \mid v_L(g(x)-x) > 0 \text{ für alle } x \in R_L\}$$

L_0 bezeichne die maximale unverzweigte Erweiterung von K in L.

1.8.2 Die maximale zahm verzweigte Erweiterung in L

(i) Es gibt einen Körper L_1 zwischen K und L mit der Eigenschaft, daß ein Teilkörper $L' \subseteq L$ genau dann zahm verzweigt ist, wenn er in L_1 liegt. Ist die Charakteristik $p = \mathrm{char}(k) \neq 0$, so ist $[L:L_1]$ eine Potenz von p.

(ii) Sei L/K eine normale Erweiterung mit der Gruppe G = G(L/K). Dann ist auch L_1/K eine normale Erweiterung und fällt mit dem Fixkörper der folgenden Gruppe zusammen.

$$G_1(L/K) := \{g \in G \mid v_L(g(x)-x) \geq v_L(x)+1 \text{ für alle } x \in R_L\}$$

(iii) Sei $\prod \in L$ ein Element mit $v_L(\prod) = 1$. Dann ist die Abbildung

$$\theta_0 : G_0(L/K) \to k_{L_0}^*, \; g \mapsto \text{Restklasse von } \frac{g(\prod)}{\prod},$$

ein wohldefinierter und von $\prod$ unabhängiger Gruppenhomomorphismus mit dem Kern $G_1(L/K)$,

$$\mathrm{Ker}(\theta_0) = G_1(L/K).$$

(iv) Sei L/K weiterhin normal. Dann ist $G_0(L/K)/G_1(L/K)$ zyklisch. Im Fall positiver Charakteristik ist $G_1(L/K)$ eine (eindeutig bestimmte) p-Sylow-Untergruppe von $G_0(L/K)$.

Bemerkung

Ist die Charakteristik char(k) = 0, so ist die Erweiterung L/K stets zahm verzweigt. Die Behauptung der obigen Aussage reduziert sich dann auf Existenz des Homomorphismus θ_0 und die Zyklizität der Gruppe G_0.

Beweis. Wir betrachten zunächst den Fall, daß die Erweiterung

L/K normal

ist.

1. Schritt. $G_1 = G_1(L/K)$ ist ein Normalteiler in der Trägheitsgruppe.

Offensichtlich ist $G_1 = G_1(L/K)$ in der Trägheitsgruppe (vgl. 1.7.8) enthalten,

$$G_1 \subseteq G_0 := \{g \in G \mid v_L(g(x)-x) \geq 1 \text{ für alle } x \in R_L\}.$$

Für $g', g'' \in G_1$ ud $x \in R_L$ gilt

$$\begin{aligned} v_L(g'g''(x)-x) &= v_L(g'g''(x)-g''(x)+g''(x)-x) \\ &\geq \min\{ v_L(g'g''(x)-g''(x)), v_L(g''(x)-x) \} \end{aligned}$$

$$\geq v_L(x)+1,$$

also $g'g'' \in G_1$. Für $g \in G_1$ gilt weiter

$$\begin{aligned} v_L(g^{-1}(x)-x) &= v_L(-g^{-1}(g(x)-x)) \\ &= v_L(g^{-1}(g(x)-x)) \\ &= v_L(g(x)-x) \qquad \text{(vgl. 1.7.3)} \\ &\geq v_L(x)+1, \end{aligned}$$

d.h. es ist $g^{-1} \in G_1$. Wir haben damit gezeigt, G_1 ist eine Untergruppe von G_0. Seien jetzt g' und g Elemente von G_1 bzw. G_0. Dann gilt

$$\begin{aligned} v_L(gg'g^{-1}(x) - x) &= v_L(gg'g^{-1}(x) - gg^{-1}(x)) \\ &= v_L(g(g'g^{-1}(x) - g^{-1}(x))) \\ &= v_L(g'g^{-1}(x) - g^{-1}(x)) \qquad \text{(nach 1.7.3)} \\ &\geq v_L(g^{-1}(x)))+1 \qquad \text{(wegen } g' \in G_1\text{)} \\ &= v_L(x) + 1 \qquad \text{(nach 1.7.3)} \end{aligned}$$

Damit ist gezeigt, daß G_1 Normalteiler in G_0 ist.

2. Schritt. $\theta_0 : G_0(L/K) \to k_L^*$ ist ein wohldefinierter Gruppenhomomorphismus und hängt nicht von der Wahl von $\prod$ ab.

Sei $\prod' \in L$ ein weiteres Element mit $v_L(\prod') = 1$. Dann gilt

$$\prod' = u \cdot \prod$$

mit einer Einheit $u \in R_L$. Für $g \in G_0$ gilt nach Definition der Trägheitsgruppe

$g(u) = u + x \cdot \prod$ mit $x \in R_L$,

also

$$\frac{g(u)}{u} \equiv 1 \bmod \mathcal{P}_L$$

also

$$\frac{g(\prod')}{\prod'} = \frac{g(\prod)}{\prod}\cdot\frac{g(u)}{u} \equiv \frac{g(\prod)}{\prod} \bmod \mathcal{P}_L.$$

Wir haben gezeigt, die Definition von

$$\theta_0(g) := \frac{g(\prod)}{\prod} \bmod \mathcal{P}_L$$

hängt nicht von der speziellen Wahl von $\prod$ ab. Für $g', g'' \in G_0$ gilt weiter

$$\frac{g'g''(\prod)}{\prod} = \frac{g'g''(\prod)}{g''(\prod)}\cdot\frac{g''(\prod)}{\prod}.$$

Wegen $v_L(g''(\prod)) = v_L(\prod)$ (nach 1.7.3) ist $g''(\prod)$ ein zur Definition von $\theta_0(g')$ geeignetes Element von L, d.h. es ist

$$\theta_0(g'g'') = \theta_0(g')\,\theta_0(g'').$$

Da die Gruppe G_0 als Untergruppe der Galoisgruppe von L/K endlich ist, ist für jedes $g \in G_0$ das Element $\theta_0(g) \in k_L^*$ eine Einheitswurzel, also insbesondere separabel über k,

$$\theta_0(g) \in (k_L^s)^* = (k_{L_0})^*.$$

Die Abbildung θ_0 ist somit wohldefiniert.

3. Schritt. Berechnung des Kerns von θ_0 (d.h. Beweis von (iii)).

Sei $a \in L^*$. Wir schreiben a in der Gestalt

$$a = u \cdot \prod^v \text{ mit } v = v_L(a).$$

Für $g \in G_0$ gilt dann

$$\frac{g(a)}{a} = \left(\frac{g(\prod)}{\prod}\right)^v \cdot \frac{g(u)}{u}$$

Wie wir im vorigen Schritt gesehen haben, gilt $\frac{g(u)}{u} \equiv 1 \bmod \mathcal{P}_L$, also

$$\theta_0(g)^{v_L(a)} = \left(\frac{g(a)}{a} \bmod \mathcal{P}_L\right),$$

Wegen

$$v_L(g(a)-a) = v_L\left(\frac{g(a)}{a} - 1\right) + v(a)$$

erhalten wir damit

$$\begin{aligned} g \in G_1 &\Leftrightarrow v_L\left(\frac{g(a)}{a} - 1\right) \geq 1 \text{ für alle } a \in R_L \\ &\Leftrightarrow \frac{g(a)}{a} \equiv 1 \bmod \mathcal{P}_L \text{ für alle } a \in R_L \\ &\Leftrightarrow \theta_0(g)^{v_L(a)} = 1 \text{ für alle } a \in R_L \\ &\Leftrightarrow \theta_0(g) = 1 \\ &\Leftrightarrow g \in \mathrm{Ker}(\theta_0) \end{aligned}$$

4. Schritt. Die Gruppe G_0/G_1 ist zyklisch und im Fall $p:=\mathrm{char}(k)>0$ ist die Ordnung von G_0/G_1 teilerfremd to p.

Wie wir im 2. Schritt gesehen haben, besteht die Gruppe

$$\mathrm{Im}\,\theta_0 \cong G_0/\mathrm{Ker}(\theta_0) = G_0/G_1$$

aus endlich vielen Einheitswurzeln, ist damit Untergruppe einer zyklischen Gruppe und damit selbst zyklisch. Ist $p>0$ die Charakteristik von k, so liegen die p-ten Einheitswurzeln bereits im Primkörper[48] $\mathbb{F}_p$ sind also als Elemente von $\mathbb{F}_p^*$ auch (p-1)-te Einheitswurzeln. Die zyklische Gruppe $\mathrm{Im}\,\theta_0$ wird also von einer r-ten Einheitswurzel erzeugt, wobei r teilerfremd zur Charakteristik p von k ist (falls die Charakteristik positiv ist). Insbesondere ist die Ordnung von $\mathrm{Im}\,\theta_0$ kein Vielfaches der Charakteristik char(k).

5. Schritt. Konstruktion von L_1. Zahme Verzweigtheit von L_1/L_0.

Sei

$$L_1 := L^{G_1}$$

der Fixkörper der Gruppe G_1. Wegen $G_1 \subseteq G_0 \subseteq G$ bestehen die folgenden Inklusionen.

---

[48] Das Erheben in die p-te Potenz ist ein Automorphismus von $\mathbb{F}_p$.

$$K \subseteq L_0 \subseteq L_1 \subseteq L \text{ und } k \subseteq k_{L_0} \subseteq k_{L_1} \subseteq k_L.$$

Nach 1.7.8 ist k_{L_0} der separable Abschluß von k in k_L, d.h.

(1) $[k_L : k_{L_0}]$ ist eine p-Potenz.

Da G_1 normal ist in G_0, ist die Erweiterung L_1/L_0 normal. Insbesondere operiert G_0 auf L_1 und es gilt

(2) $$[L_1:L_0] = \#G_0/G_1.$$

Diese Zahl ist nach dem 4.Schritt teilerfremd zu p. Insbesondere ist

$$e(L_1/L_0) \text{ teilerfremd zu p.}$$

Wegen (1) ist der Relativgrad von L_1/L_0 aber ein Teiler von p. Also gilt

$$k_{L_1} = k_{L_0} \text{ und } f(L_1/L_0) = 1.$$

Da k_{L_0} die separable Abschließung von k in k_L ist, ist k_{L_1} separabel über k. Zusammen sehen wir, daß L_1 zahm verzweigt ist über L.

6. Schritt. L_1 ist zahm verzweigt über K.

Wir benutzen die Tatsache, daß die Zusammensetzung zahm verzweigter Erweiterungen wieder zahm ist (was sich unmittelbar aus der Definition von zahm ergibt). Da L über K unverzweigt, also zahm verzweigt, ist, ergibt sich zusammen mit dem 5. Schritt die zahme Verzweigtheit von L_1 über K.

7. Schritt. Sei $L' \subseteq L$ eine zahm verzweigte Erweiterung von K. Dann ist $E := L'L_0$ zahm verzweigt über L_0

Wir setzen

$$F := L' \cap L_0$$

und betrachten das kommutative Diagramm von Körpererweiterungen.

$$\begin{array}{ccc} L' & \subset & E = L'L_0 \\ \cup & & \cup \\ F & \subset & L_0 \end{array}$$

Der Körper L' ist nicht nur über K sondern auch über F zahm verzweigt. Nach 1.5.15 gibt es ein $a \in R_L$, mit

(1) $$Tr_{L'/F}(a) = 1.$$

Ebenfalls nach 1.5.15 genügt es zum Beweis der zahmen Verzweigtheit von E/L_0 zu zeigen, daß dann auch

(2) $$Tr_{E/L_o}(a) = 1$$

gilt. Zur Berechnung der letzten Spur wählen wir L_0-Einbettungen von E in eine algebraische Abschließung von K. Da E in L liegt und L/K nach Annahme normal ist, liegen die Bilder dieser Einbettungen sogar in L. Seien also

$$\tau_1,...,\tau_u : E \to L \text{ sämtliche } L_0\text{-Einbettungen von E}$$

in eine algebraischen Abschließung von K. Ihre Anzahl ist

$$u = [E:L_0].$$

Die Spur auf der linken Seite von (2) ist gerade

(3) $$\mathrm{Tr}_{E/L_o}(a) = \sum_{i=1}^{u} \tau_i(a).$$

Durch Einschränken der Einbettungen τ_i auf L' erhalten wir $L' \cap L_0$-Einbettungen von L',

(4) $$\sigma_i := \tau_i \mid_{L'} : L' \to L \text{ ist F-Einbettung von L' für } i=1,...,u.$$

Man beachte, sind zwei σ_i gleich, so stimmen die zugehörigen τ_i auf L' (und trivialerweise auf L_0) also auf $L'L_0 = E$ überein. Die Einbettungen (4) sind also paarweise verschieden. Zum Beweis der Behauptung dieses Schrittes genügt es zu zeigen, sämtliche F-Einbettungen von L' sind von der Gestalt (4). Dann berechnet sich nämlich die Spur auf der linken Seite von (1) nach derselben Formel (3) wie die auf der linken Seite von (2) und mit (1) gilt auch (2).
Die Zahl der F-Einbettungen von L' ist gerade [L':F]. Es genügt deshalb,

(5) $$[E:L_0] = [L':F]$$

zu beweisen.
Alle hier betrachteten Körpererweiterungen (von K) sind separabel. Es gibt also ein Element $\alpha \in L$ mit

$$L' = F(\alpha).$$

Sei f das Minimalpolynom von α über F und g das von α über L_0,

$$f \in F[x],\ g \in L_0[x],\ f(\alpha) = 0,\ g(\alpha) = 0,\ g \mid f.$$

Wir haben zu zeigen, f und g haben denselben Grad. Sei

$$f = g_1 \cdot ... \cdot g_r$$

die Zerlegung von f in irreduzible Faktoren über L_0. Wir haben zu zeigen, r=1. Dazu beachten wir, wegen $L' = F(\alpha) \subseteq L$ operiert die Galoisgruppe G(L/F) transitive auf den Nullstellen des Minimalpolynoms f. Diese Operation induziert eine Operation auf der Menge der g_i,

(6) $$G(L/F) \times \{g_1,...,g_r\} \to \{g_1,...,g_r\},\ (\sigma, g_i) \mapsto \sigma g_i.$$

Dabei sei $\sigma g_i = g_j$, wenn σ eine (und damit alle) Nullstellen von g_i in solche von g_j abbildet. Man beachte, diese Definition der Operation ist korrekt. Sind nämlich β und γ zwei Nullstellen von g_i, so gilt, da g_i irreduzibel über L_0 ist,

$$\gamma = \tau\beta \text{ für ein } \tau \in G(L/L_0).$$

Damit ist aber

$$\sigma\gamma = \sigma\tau\beta = \sigma\tau\sigma^{-1}\sigma\beta.$$

Da mit L/F auch die Körpererweiterung L_0/F normal ist (vgl. 1.7.8), ist $G(L/L_0)$ Normalteiler in G(L/F), also

$$\sigma\tau\sigma^{-1} \in G(L/L_0).$$

Die Elemente $\sigma\gamma$ und $\sigma\beta$ sind somit $G(L/L_0)$-konjugiert und deshalb Nullstellen desselben g_j. Die Operation (6) ist also korrekt definiert. O.B.d.A. sei $g_1 = g$. Betrachten wir den Stabilisator $G(L/F)_g$ von g bei der Operation (6). Es gilt

$$\begin{aligned} \sigma \in G(L/F)_g &\Leftrightarrow \sigma(\alpha) \text{ ist Nullstelle von } g \\ &\Leftrightarrow \sigma(\alpha) \text{ ist } G(L/L_0)\text{-konjugiert zu } \alpha \\ &\Leftrightarrow \sigma(\alpha) = \tau(\alpha) \text{ für ein } \tau \in G(L/L_0) \end{aligned}$$

$\Leftrightarrow (\tau^{-1}\sigma)(\alpha) = \alpha$ für ein $\tau \in G(L/L_0)$

$\Leftrightarrow \tau^{-1}\sigma$ läßt $F(\alpha) = L'$ fest für ein $\tau \in G(L/L_0)$

$\Leftrightarrow \tau^{-1}\sigma \in G(L/L')$ für ein $\tau \in G(L/L_0)$

$\Leftrightarrow \sigma \in G(L/L') \cdot G(L/L_0) = G(L/L' \cap L_0) = G(L/F)$.

Der Stabilisator von g fällt also mit der gesamten Gruppe G(L/F) zusammen. Da die Gruppe aber nach Konstruktion transitiv operiert, kann die Menge der g_i aus nur einem Element bestehen, d.h. es gilt r = 1.

8. Schritt. Jede zahm verzweigte Teilerweiterung von L liegt ganz in L_1

Sei L'/K eine zahm verzweigte Teilerweiterung von L/K. Wie oben setzen wir

$$F := L' \cap L_0 \text{ und } E := L'L_0.$$

Im vorangehenden Schritt haben wir gesehen, daß E/L_0 zahm verzweigt ist. Da L_0/K unverzweigt (also auch zahm verzweigt) ist, ist damit auch

$$E/K \text{ zahm verzweigt.}$$

Insbesondere ist die zu E/K gehörige Erweiterung der Restklassenkörper separabel,

$$k_E \subseteq k_L^s = k_{L_0}, \text{ d.h. } k_E = k_{L_0}.$$

Damit ist E/L_0 total verzweigt, d.h.

(7) $$f(E/L_0) = 1 \text{ und } e(E/L_0) = [E:L_0]$$

Nach 1.6.4(ii) gilt

$$S_E = S_{L_0}[c] \text{ und } E = L_0(c)$$

wenn $c \in L$ ein beliebig gewähltes Element mit $v_E(c) = 1$ ist. Nach 1.4.16(iii) folgt

$$\mathcal{D}(E/L_0) = g'(c)S_E,$$

wobei $g \in S_{L_0}[x]$ das Minimalpolynom von c über L_0 bezeichne. Das Kriterium für zahm verzweigte Erweiterungen (vgl. 1.5.15) liefert

$$e(E/L_0) - 1 = v_E(\mathcal{D}(E/L_0)) = v_E(g'(c)).$$

Wir multiplizieren diese Identität mit dem Verzweigungsindex $v_L(c)$ von L/E und erhalten

(8) $$v_L(g'(c)) = (e(E/L_0) - 1)v_L(c).$$

Sei jetzt $\Delta = G(L/E)$, d.h. $\Delta \subseteq G_0 = G(L/L_0)$ und

$$E = L^{\Delta}.$$

Durch Einschränken der Elemente von $G_0 = G(L/L_0)$ auf E erhalten wir gerade die L_0-Einbettungen von E. Der Kern dieser Einschränkungsabbildung ist gerade Δ. Die Faktormenge G_0/Δ läßt sich also identifizieren mit der Menge der L_0-Einbettungen von E. In jeder Restklasse $G_0 = G(L/L_0) \bmod \Delta$ wählen wir ein Element γ. Das Element $\gamma(c)$ durchläuft dann gerade die Konjugierten von c über L_0. Deshalb gilt

$$g'(c) = \prod_{\gamma} (c - \gamma(c)),$$

wobei rechts das Produkt über alle Restklassen von G_0/Δ, die von der trivialen Restklasse Δ verschieden sind, zu erstrecken ist. Für jeden der Faktoren in diesem Produkt erhalten wir, da c und $\gamma(c)$ denselben Wert haben (vgl. 1.7.3),

$$v_L(c\text{-}\gamma(c)) \geq v_L(c).$$

Die Anzahl der Faktoren ist $\#G_0/\Delta - 1 = [G_0:\Delta] - 1 = e(E/L_0) - 1$. Wegen (8) gilt also in allen diesen Ungleichungen das Gleichheitszeichen,

$$v_L(c\text{-}\gamma(c)) = v_L(c),$$

d.h. $\gamma \notin G_1$. Damit muß gelten $G_1 \subseteq \Delta$, also $L_1 \supseteq E$, also $L_1 \supseteq L'$.

9. Schritt. Die p-Sylow-Gruppen-Eigenschaft von G_1, p = char(k).

Die Aussage ist nur sinnvoll, wenn die Charakteristik von $p > 0$ ist. Nach dem 4. Schritt ist die Ordnung von G_0/G_1 teilerfremd zu p. Es reicht deshalb zu zeigen, jede Untergruppe von G_1 hat einen durch p teilbaren Index[49]. Sei $G'' \subseteq G_1$ eine echte Untergruppe und sei

$$L'' := L^{G''} \ (\supseteq L_1)$$

deren Fixkörper. Es reicht zu zeigen,

$$p \mid [L'':L_1] \ (= [L:L_1]/[L:L''] = [G_1:G'']\ ).$$

Nach dem 8. Schritt ist die Erweiterung L''/L_1 nicht zahm, d.h. es gilt

$$p \mid e(L''|L_1) \text{ oder } k_{L''}/k_{L_1} \text{ ist nicht separabel.}$$

Im zweiten Fall gilt $p \mid [k_{L''}:k_{L_1}] = f(L''|L_1)$. In jedem der beiden Fälle ist daher

$$p \mid e(L''|L_1) \cdot f(L''|L_1) = [L'':L_1].$$

10. Schritt. Der Fall nicht-normaler Erweiterungen L/K.
Wird behandelt, indem man L/K in eine normale Erweiterung einbettet.
QED.

1.8.3 Auflösbarkeit der Trägheitsgruppe

Die Trägheitsgruppe der normalen Erweiterung L/K ist auflösbar. Genauer:

(i) Ist die Charakteristik der Restklassenkörper $\chi = 0$, so ist $G_0(L/K)$ zylisch.

(ii) Ist $\chi \neq 0$, so ist $G_0(L/K)$ Erweiterung einer zyklischen Gruppe mit einer p-Gruppe.

Ist der Restklassenkörper $k=R/\mathcal{P}$ endlich, so ist die Galoisgruppe jeder normalen Erweiterung von K auflösbar.

Beweis. Die Aussagen (i) und (ii) folgen unmittelbar aus 1.8.2. Zum Beweis der verbleibenden Aussage im Fall, daß k endlich ist, betrachten wir die ineinander liegenden Gruppen

$$G \supseteq G_0 \supseteq G_1.$$

Auf Grund von 1.8.2 wissen wir, G_1 ist eine p-Gruppe, also auflösbar. Ebensfalls auf Grund von 1.8.2 ist G_0/G_1 eine zyklische Gruppe, also auflösbar. Wir haben also nur noch die Auflösbarkeit von

$$G/G_0 = G(L/K)/G(L/L_0) = G(L_0/K)$$

---

[49] Das gilt dann insbesondere für die p-Sylow-Untergruppe von G_1, deren Index aber gleichzeitig zu p teilerfremd also gleich 1 sein muß, d.h. die Gruppe G_1 ist gleich ihrer p-Sylow-Gruppe.

zu zeigen. Da L_0/K unverzweigt ist, folgt $G(L_0/K) = G(k_{L_0}/k)$. Die Galoisgruppe einer Erweiterung endlicher Körper ist aber zyklisch, also auflösbar.
QED.

1.8.4 Komposition zahm verzweigter Erweiterungen

Die Komposition von zwei zahm verzweigten Erweiterungen L', L" in der separablen Abschließung von K ist zahm.
Beweis. Wir wählen eine Erweiterung L, welche die Komposition L'L" von L' und L" enthält. Sei $L_1 \subseteq L$ die maximale in L enthaltene zahm verzweigte Teilerweiterung. Dann gilt

$$L' \subseteq L_1 \text{ und } L'' \subseteq L_1,$$

also

$$L'L'' \subseteq L_1.$$

Also ist L'L" zahm verzweigt.
QED.

1.8.5 Die maximale zahm verzweigte Erweiterung K_{tr}

Die Vereinigung aller zahm verzweigten Erweiterungen des Körpers K innerhalb der separablen Abschließung von K wird mit

$$K_{tr}$$

bezeichnet und heißt maximale zahm verzweigte Erweiterung von K.

1.8.6 Die Galoisgruppe von K_{tr}/K_{nr}

Jede endliche Teilerweiterung von K_{tr}/K ist zahm verzweigt. Die Erweiterung K_{tr}/K enthält K_{nr}/K als Teilerweiterung.Es gilt[50]

$$G(K_{tr}/K_{nr}) = \begin{cases} \overline{Z} & \text{falls char(k)=0} \\ \prod_{q \neq p} \overline{\mathbb{Z}}_q & \text{falls char(k)=p} \end{cases}$$

Beweis. Der erste Teil der Aussage wird in derselben Weise bewiesen wie die analoge Aussage über unverzweigte Erweiterungen. Der zweite Teil der Aussage folgt aus der Definition von K_{nr} und K_{tr} und der Tatsache, daß unverzweigte Erweiterungen zahm verzweigt sind. Bestimmen wir die Galois-Gruppe von K_{tr}/K. Da K_{tr} die Vereinigung aller zahm verzweigten Teilerweiterungen von K_{tr}/K ist, gilt

$$G(K_{tr}/K_{nr}) = \varprojlim_{L} G(L_1/L_0)$$

wobei der inverse Limes über alle normalen endlichen Erweiterungen L/K zu erstrecken ist, L_0 bzw. L_1 die zu L/K gehörige maximale unverzweigte bzw. zahm verzweigte Teilerweiterung bezeichne. Weiter gilt

$$\begin{aligned} G(L_1/L_0) &= G(L/L_0)/G(L/L_1) && \text{(da alle Erweiterungen normal sind)} \\ &= G_0(L/K)/G_1(L/K) && \text{(nach Definition von } G_0 \text{ und } G_1) \end{aligned}$$

---

[50] Es ist nicht klar, wieso das in voller Allgemeinheit gelten soll, zum Beispiel auch dann, wenn es mehrere separable Erweiterungen deselben Grades von k gibt. Die Aussage ist aber richtig falls k endlicher Körper ist (der erste Fall in der Formel für die Galois-Gruppe tritt dann nicht ein).

Nun gibt es zu jedem Grad n, welcher teilfremd zur Charakteristik von k ist, mindestens eine unverzweigte Erweiterung L/K vom Grad n: man nehme zum Beispiel eine Eisenstein-Erweiterung des Grades n. Nach 1.8.2 ist dann $G_0(L/K)/G_1(L/K)$ zyklisch und $G_1(L/K)$ ist die (einzige) p-Sylow-Untergruppe von G_0, d.h. es ist

$$G_0(L/K)/G_1(L/K) = G_0(L/K) = \mathbb{Z}/n\mathbb{Z} .$$

Hat n die Primfaktorzerlegung

$$n = p_1^{a_1} \cdot \ldots \cdot p_r^{a_r},$$

so gilt

$$G_0(L/K)/G_1(L/K) = \mathbb{Z}/(p_1^{a_1}) \times \ldots \times \mathbb{Z}/(p_r^{a_r}),$$

Durch Übergang zu den inversen Limites ergibt sich die obige Formel für die Galois-Gruppe von K_{tr}/K_{nr}. Man beachte, daß die Eisenstein-Erweiterungen zwar kein kofinales System von Teilerweiterungen bilden, die zu den übrigen Erweiterungen gehörigen Gruppen aber nur weitere zyklische Gruppe liefern (deren Ordnung zu p teilerfremd ist und) die den inversen Limes nicht verändern. Man verwendet dabei die Tatsache, daß eine zyklische Gruppe zu jede Ordnung, die die Gruppenordnung teilt, genau eine Untergruppe besitzt.
QED.

Bemerkungen

(0) (weglassen?) Die Gruppe G_1 besitzt eine interessante Beschreibung im Rahmen der Theorie der R-Moduln. Der Ring $S = R_L$ hat die Struktur eines Moduls über dem Gruppenring

$$R[G],\ G := G(L/K).$$

Für die Untergruppen $H \subseteq G$ kann man zeigen, daß S genau dann zahm projektiv ist über R[H], wenn $H \supseteq G_1$

(ii) Aus der Aussage von 1.8.2 ergibt sich, daß man, um die zahm verzweigten Erweiterungen zu bekommen, zwei Schritte durchführen muß. Im ersten Schritt muß man eine unverzweigte Erweiterunge konstruieren (vgl. Abschnitt 1.7) und im zweiten eine total verzweigte und zahm verzweigte normale Erweiterung. Den zweiten Schritt dieser Konstruktion kann man ebenfalls explizit beschreiben.

(iii) Erinnern wir an einige Tatsachen aus der Theorie von Kummer (siehe Kapitel III). Sei $e = e(L/K)$. Wir nehmen an, die Körper K enthält eine e-te Einheitswurzel und es gibt ein $c \in K^*$, welches modulo K^{*e} genau die Ordnung e besitzt. Dann ist der Körper

$$L := K(\prod) \text{ mit } \prod^e = c$$

normal über K vom Grad

$$[L:K] = e.$$

Die Abbildung

$$\psi_c : G(L/K) \to K^*,\ \gamma \mapsto \frac{\gamma\prod}{\prod},$$

ist dann ein wohldefinierter und injektiver Homomorphismus. Wir werden im folgenden

$$\overline{\psi}_c(\gamma) := \overline{\psi_c(\gamma)}$$

schreiben.

1.8.7 Die total und zahm verzweigten normalen Erweiterungen

(i) Sei L/K ein normale total und zahm verzweigte Erweiterung des Grades $e = e(L/K)$. Dann erhält der Körper eine primitive e-te Einheitswurzel und es gibt ein

Element $c \in K^*$ mit $v_K(c) = 1$ und $L = K(\sqrt[e]{c})$. Außerdem fällt der oben beschriebene Homomorphismus $\overline{\psi}_c$ mit dem Homomorphismus θ_0 von 1.8.2 zusammen. Weiter sind die beiden folgenden Bedingungen äquivalent:

1. $L = K(\sqrt[e]{b})$ und $v_K(b) = 1$.
2. $\overline{bc^{-1}} \in k^{*e}$.

(ii) Sei char(k) kein Teiler von e. Der Körper K enthalte eine primitive e-te Einheitwurzel und es gelt $v_K(c) = 1$. Dann ist der Körper

$$L := K(\sqrt[e]{c})$$

normal, total verzweigt und zahm verzweigt über K und hat den Grad $[L:K] = e$.

Beweis. Zu (i). Die Erweiterung soll total verzweigt sein, d.h.

$$f = f(L/K) = 1.$$

Der unverzweigte Teil der Erweiterung ist deshalb trivial,

$$L_0 = K,\ k_{L_0} = k.$$

Außerdem ist die Erweiterung zahm, d.h.

$$L_1 = L.$$

Insbesondere ist damit

$$G_0(L/K) = G(L/L_0) = G(L/K)$$

und

$$G_1(L/K) = G(L/L_1) = \{e\}.$$

Nach 1.8.2 besteht das Bild
Der Homomorphismus

$$\theta_0 : G(L/K) = G_0(L/K) \to k^*_{L_0} = k^*$$

von 1.8.2 ist gerade die Einbettung der Galoisgruppe von L/K in die multiplikative Gruppe von k. Sein Bild ist nach 1.8.2 zyklisch, d.h. G(L/K) ist zyklisch von der Ordnung $e \cdot f = e(L/K)$, d.h. das Bild des Homomorphismus besteht gerade aus den e-ten Einheitswurzeln. Die Nullstellen des Polynoms $X^e - 1$ liegen also sämtlich in k. Dies ist ein separables Polynom. Nach der Folgerung von 1.7.4 (Henselsches Lemma), lassen sich diese Nullstellen sämtlich anheben zu Nullstellen von $X^e - 1$ in R. Mit anderen Worten, $R \subseteq K$ enthält eine primitive e-te Einheitswurzeln und die verschiedenen e-ten Einheitswurzeln reduzieren sich zu verschiedenen Einheitswurzeln von k.

QED.

1.8.8 Die Erweiterung K_{tr}/K_{nt}

Sei $c \in K$ ein Element mit $v_K(c) = 1$. Dann gilt

$$K_{tr} = \cup\, K_{nr}(\sqrt[e]{c}),$$

wobei e die Menge der zu char(k) teilerfremden Zahlen durchläuft.

Beweis.

QED.

1.8.9 Die Normabbildung

Ist die Erweiterung L/K zahm verzweigt, so gilt

$$N_{L/K}(U_{L,1}) = U_{K,1}\ .$$

Beweis.

QED.

1.9 Verzweigungsgruppen

1.10 Zerlegungen

Literatur zu Kapitel 1

[1] Zariski, O., Samuel,P.: Commutative algebra, London, 1958

[2] Noether, E.: Normalbasis bei Körpern ohne höhere Verzweigung, J. reine angew. Math. 167(1932)147-152

[3] Serre, J.-P.: Corps loceaux, Paris, Hermann 1962

[4] Swan, R.S.: Induced representations and projective modules, Ann. Math. 71(1960), 552-578 (Übersetzung ins Russische: Математика, 8:1 (1964),3-29)

2 Globale Körper (J.W.S. Cassels)

2.1 Multiplikative Bewertungen (Wdhlg)

Sei K ein Körper. Eine multiplikative Bewertung von K ist eine Abbildung

$$K \to \mathbb{R}_{\geq 0} := \{x \in \mathbb{R} \mid x \geq 0\},\ x \mapsto |x|,$$

mit folgenden Eigenschaften.

1. $|x| = 0 \Leftrightarrow x = 0$.
2. $|xy| = |x| \cdot |y|$.
3. Es gibt eine Konstante C mit $|1+x| \leq C$ für alle $x \leq 1$.

Zwei Bewertungen $|\ |_1$ und $|\ |_2$ des Körpers K heißen äquivalent, wenn es ein $c>0$ gibt mit $|x|_2 = |x|_1^c$ für alle $x \in K$. Auf diese Weise ist eine Äquivalenzrelation für multiplikative Bewertungen definiert.

Jede multiplikative Bewertung ist äquivalent zu einer Bewertung mit $C \leq 2$. Für letztere gilt die Dreiecksungleichung

$$|x+y| \leq |x| + |y|.$$

Eine multiplikative Bewertung, welche äquivalent zu einer Bewertung mit C=1 ist heißt nicht-archimedisch. Für Bewertungen mit C=1 gilt die folgende verschärfte Variante der Dreiecksungleichung.

$$|x+y| \leq \max\{|x|,|y|\}$$

Eine multiplikative Bewertung des Körpers K ist genau nicht-archimedisch, wenn gilt

$$|n \cdot 1_K| \leq 1 \text{ für } n=1,2,3,...$$

Für diskrete Bewertungen $|.|: K-\{0\} \to \mathbb{R}_{\geq 0}$ ist die Menge

$$R_{|.|} := \{x \in K \mid |x| \leq 1\}$$

ein Ring, welcher Bewertungsring von |.| heißt. Die Menge

$$p_{|.|} := \{x \in K \mid |x| < 1\}$$

ist ein maximales Ideal des Bewertungsrings (und zwar das einzige). Es heißt Bewertungsideal von |.|.

Bemerkung

Der Ring $R=R_{|.|}$ ist im allgemeinen nicht noethersch. Wenn er es jedoch ist, so wird $p=p_{|.|}$ automatisch von nur einem Element erzeugt und R ist ein diskreter Bewertungsring. In I(1.2.5) haben wir gesehen, daß dann die Bewertung die Gestalt

$$|x| = \rho^{v_p(x)}, \quad x \in K$$

hat mit $0 < \rho < 1$, wobei $v_p: K-\{0\} \to \mathbb{Z}$ die zu p gehörige (additive) diskrete Bewertung bezeichnet. Im nachfolgenden Abschnitt beschäftigen wir uns mit einem Fall, in welchem R tatsächlich noethersch ist.

2.2 Diskrete multiplikative Bewertungen

Eine multiplikative Bewertung $|.|: K-\{0\} \to \mathbb{R}_{\geq 0}$ heißt diskret, wenn es ein $\delta>0$ gibt mit der Eigenschaft, daß aus $1-\delta < |x| < 1+\delta$ stets $|x| = 1$ folgt. Mit anderen Worten, es gilt eine Umgebung von $1 \in \mathbb{R}_{\geq 0}$, in welcher nur ein einziger Wert von |.| liegt. Das bedeutet, die Menge der reellen Zahlen

$$\log |x| \text{ mit } x \in K-\{0\}$$

ist eine diskrete additive Untergruppe von $\mathbb{R}$. Insbesondere unterschreitet der Abstand zwischen je zwei Elementen dieser Untergruppe nicht einen bestimmten positiven Wert. Sei c der minimale Abstand zwischen den Elementen der Untergruppe. Dann wird die Unterguppe gerade von c erzeugt. Wir haben gezeigt, für jede diskrete Bewertung gilt es ein positives c mit

$$|K-\{0\}| = \{c^n \mid n \in \mathbb{Z})\}.$$

O.B.d.A. können wir annehmen

$$0 < c < 1$$

(die Bewertung sei nicht-tivial). Durch diese Zusatzbedingung ist die Zahl c durch die Bewertung eindeutig bestimmt. Die Ordnung eines Elements $x \in K-\{0\}$ bezüglich der diskreten Bewertung |.| ist definiert als die eindeutig bestimmte ganze Zahl

$$\text{ord}(x) \in \mathbb{Z}$$

mit

$$|x| = c^{\text{ord}(x)}.$$

Für x=0 definieren wir $\text{ord}(x) = \infty$. Nach Konstruktion gilt

$$\text{ord}(xy) = \text{ord}(x)+\text{ord}(y).$$

Diskrete nicht-archimedische Bewertungen

Sei $|.|: K \to \mathbb{R}_{\geq 0}$ eine nicht-archmedische Bewertung. Dann sind folgende Aussagen äquivalent.

(i) |.| ist diskret.

(ii) Das Bewertungsideal von |.| ist ein Hauptideal des Bewertungsrings.

Beweis. (i) ⇒ (ii). Seien R der Bewertungsring von |.| und $p \subseteq R$ das Bewertungideal. Nach Voraussetzung hat die Bewertung die Gestalt

$$|x| = c^{\text{ord}(x)} \text{ mit } 0< c < 1,$$

wobei jede Potenz von c auch ein Wert ist. Sei $\pi \in R$ ein Element mit $|\pi|=c$. Dann gilt $\pi \in p$ also

$$\pi R \subseteq p.$$

Beweisen wir die umgekehrte Inklusion. Für jedes $x \in K-\{0\}$ ist

$$|x| = c^{\text{ord}(x)} = |\pi|^{\text{ord}(x)} = |\pi^{\text{ord}(x)}|$$

also $|\frac{x}{\pi^{ord(x)}}| = 1$, also

$$x = u \cdot \pi^{ord(x)}$$

mit einer Einheit u von R. Für $x \in p$ gilt insbesondere $|x|<1$, also $ord(x)>0$, also $x \in \pi R$. Damit gilt $p \subseteq \pi R$, also $p = \pi R$, d.h. p ist ein Hauptideal.
(ii) $\Rightarrow$ (i). Nach (1.2.5) hat $|.|$ die Gestalt

$$|x| = \rho^{v_p(x)}, \quad x \in K$$

hat mit $0 < \rho < 1$, wobei $v_p: K-\{0\} \to \mathbb{Z}$ die zu p gehörige (additive) diskrete Bewertung bezeichnet. In der Umgebung (ρ, ρ^{-1}) von 1 liegt deshalb der einzige Wert $|1|=1$, d.h. die Bewertung ist diskret.
QED.

2.3 Beispiele multiplikativer Bewertungen

2.3.1 Die komplexen Zahlen mit der euklidischen Norm

Der Körper der komplexen Zahlen hat bezüglich des gewöhnlichen Absolutbetrags

$$|.|: \mathbb{C} \to \mathbb{R}_{\geq 0}$$

die Struktur eines (archimedisch) bewerteten Körpers. Dasselbe gilt für jeden Teilkörper von $\mathbb{C}$. Wir nehmen uns jetzt vor, zu zeigen, daß es keine weiteren archimedisch bewerteten Körper gibt.

2.3.2 Satz von Gelfand-Mazur

Sei A eine $\mathbb{R}$-Algebra mit folgenden Eigenschaften.

1. Es gibt ein $j \in \mathbb{R}$ mit $j^2=-1$.
2. Es gibt eine reelle Norm[51] $|.|: A \to \mathbb{R}$ auf A mit $|xy| \leq |x| \cdot |y|$.
3. A ist ein Schiefkörper.

Dann gilt $A = \mathbb{R} \cdot 1 + \mathbb{R} \cdot j$. Insbesondere ist A sogar ein Körper.

Beweis. Wir setzen $\mathbb{C} := \mathbb{R} \cdot 1 + \mathbb{R} \cdot j$. Die Ungleichung $|xy| \leq |x| \cdot |y|$ impliziert,daß die Multiplikation von A eine stetige Abbildung ist. Wir können die Algebra A durch ihre Vervollständigung bezüglich der gegebenen Norm |.| ersetzen und deshalb annehmen, daß A eine Banachalgebra ist.
Es ist nicht sehr schwer, einzusehen, daß dann auch die Umkehrung

$$A-\{0\} \to A-\{0\}, \; x \mapsto x^{-1},$$

eine stetige Abbildung ist (vgl. nachfolgendes Lemma). Angenommen, es gibt ein Element $c \in A-\mathbb{C}$. Dann ist die Abbildung

$$f: \mathbb{C} \to A, \; z \mapsto \frac{1}{c-z},$$

wohldefiniert und stetig. Für $z \neq 0$ gilt

$$f(z) = \frac{1}{z} \cdot \frac{1}{\frac{c}{z} - 1},$$

d.h. für $z \to \infty$ geht f gegen Null. Insbesondere ist

$$|f|: \mathbb{C} \to \mathbb{R}_{\geq 0}, \; z \mapsto |\frac{1}{c-z}|$$

---

[51] Es soll also gelten $|x| \geq 0$, $|x|=0 \Leftrightarrow x=0$, $|\lambda x| = |\lambda| \cdot |x|$, $|x+y| \leq |x|+|y|$ für $x,y \in A$ und $\lambda \in \mathbb{R}$

eine stetige Abbildung, welche außerhalb einer hinreichend großen Kreisscheibe sehr kleine Werte annimmt. Insbesondere nimmt |f| einen Maximalwert M an. Sei

$$D := \{x \in \mathbb{C} \mid |f|(x) = M\}$$

Die Menge D ist abgeschlossen, nicht-leer und beschränkt. Zum Nachweis des gewünschten Widerspruchs genügt es zu zeigen, daß D offen ist.
Sei $a \in D$. Durch Ausführen einer Verschiebung können wir erreichen, daß a=0 gilt. Zeigen wir, für r>0 klein, liegt die r-Umgebung von a ganz in D,

$$U_r(a) \subseteq D.$$

Dazu betrachten wir die Summe

$$S(n) := \frac{1}{n} \cdot \sum_{k=1}^{n} \frac{1}{c - w^k r},$$

wobei w eine primitive n-te Einheitswurzel bezeichne. Durch Bilden der logarithmischen Ableitung von $X^n - r^n = \prod_{k=1}^{n} (X - w^k r)$ sehen wir, es gilt

$$\frac{nX^{n-1}}{X^n - r^n} = \sum_{k=1}^{n} \frac{1}{X - w^k r}$$

also $S(n) = \frac{c^{n-1}}{c^n - r^n} = \frac{1}{c - r \cdot (\frac{r}{c})^{n-1}}$. Für r klein (z.B. für r<|c|) erhalten wir

$$\lim_{n \to \infty} |S(n)| = |\frac{1}{c}| = |f|(0) = M$$

Falls in jeder Umgebung von a=0 Elemente aus dem Komplement von D liegen, kann man ein r<|c| wählen und eine komplexe Zahl b vom Betrag 1 mit

$$M > |f(rb)| = |\frac{1}{c - rb}|$$

In der Nähe von b gibt es dann auf dem Einheitskreis ein Intervall I und ein ε>0 mit

$$M - \varepsilon > |\frac{1}{c - r\zeta}|$$

für alle Einheitswurzeln $\zeta \in I$. Sei b(n) die Anzahl der n-ten Einheitswurzeln, welche in I liegen. Dann ist $\frac{b(n)}{n}$ annähernd gleich die Länge des Intervalls I (mal 2π). Insbesondere strebt $\frac{b(n)}{n}$ für $n \to \infty$ gegen einen von Null verschiedenen Grenzwert. Wir schreiben jetzt |S(n)| in der Gestalt

$$S(n) = \frac{1}{n} \left(\Sigma_I \frac{1}{c - w^k r} + \Sigma_{II} \frac{1}{c - w^k r} \right),$$

wobei die erste Summe über alle n-ten Einheitswurzeln aus I und die zweite Summe über den Rest erstreckt wird. Die Summenden der ersten Summe haben einen Betrag ≤ M-ε und die der zweiten Summe einen Betrag ≤ M. Also gilt

$$|S(n)| \leq \frac{1}{n}(b(n)(M-\varepsilon) + (n-b(n))M) = M - \frac{b(n)}{n} \cdot \varepsilon.$$

Für $n \to \infty$ liefert dies den gewünschten Widerspruch.
QED.
Lemma
Seien A eine $\mathbb{C}$-Algebra,

$$|.|: A \to \mathbb{R}$$

eine reelle Norm des $\mathbb{C}$-Vektorraums A und G := A* die Gruppe der Einheiten der Algebra A. Es gelte

$$|xy| \leq |x| \cdot |y| \text{ für } x,y \in A$$

und die Algebra A sei vollständig bezüglich der Norm |.| .

Dann ist G eine topologische Gruppe, d.h. die Multiplikation und der Übergang zum Inversen definieren stetige Abbildungen

$$G\times G \to G,\ (x,y) \mapsto xy,$$

$$G \to G,\ x \mapsto x^{-1}.$$

Beweis. Die Stetigkeit der Multiplikation ergibt sich aus der folgenden Abschätzung.

$$|xy - ab| = |x(y-b)+(x-a)b| \le |x|\cdot|y-b| + |x-a|\cdot|b|.$$

Zum Beweis der Stetigkeit der zweiten Abbildung müssen wir den Ausdruck

$$|\frac{1}{x} - \frac{1}{a}|$$

(mit $x,a\in G$ und x nahe bei a) abschätzen. Dazu betrachten wir das Element $u := \frac{1}{a}(x-a)$. Es gilt

(1) $$|u| \le |\frac{1}{a}|\cdot|x-a| < 1$$

falls x in einer geeigneten Umgebung von a liegt (nämlich falls $|x-a| < |\frac{1}{a}|$ gilt). Dann ist aber die Reihe

(2) $$\sum_{n=0}^{\infty} (-u)^n$$

absolut konvergent gegen das Inverse von 1+u. Insbesondere ist 1+u eine Einheit von A und es gilt

(3) $$\frac{1}{x} = \frac{1}{a(1+u)} = \frac{1}{a}\cdot\sum_{n=0}^{\infty}(-u)^n = \frac{1}{a} + \frac{1}{a}\cdot\sum_{n=1}^{\infty}(-u)^n$$

Die Reihe (2) läßt sich wie folgt betragmäßig abschätzen.

$$|\sum_{n=0}^{\infty}(-u)^n| \le \sum_{n=0}^{\infty}|u|^n = \frac{1}{1-|u|}$$

(4) $$\le \frac{1}{1-|\frac{1}{a}|\cdot|x-a|} \qquad \text{(nach Definition von u).}$$

Insbesondere bleibt die Reihe beschränkt, wenn x gegen a konvergiert.
Es gilt

$$|\frac{1}{x} - \frac{1}{a}| = |\frac{1}{a}\cdot\sum_{n=1}^{\infty}(-u)^n| \qquad \text{(nach (3))}$$

$$\le |\frac{1}{a}|\cdot|u|\cdot|\sum_{n=0}^{\infty}(-u)^n|$$

$$\le |\frac{1}{a}|^2\cdot|x-a|\cdot|\sum_{n=0}^{\infty}(-u)^n| \qquad \text{(nach (1)).}$$

Der Beweis der Behauptung ist damit zurückgeführt auf die Beschränktheit (4) des letzten Faktors.
QED.

2.3.3 Die archimedisch bewerteten Erweiterungen von $\mathbb{R}$

Sei K eine archimedisch bewertete Körpererweiterung von $\mathbb{R}$. Dann gilt $K\cong\mathbb{R}$ oder $K\cong\mathbb{C}$ (Isomorphie von bewerteten Körpern).

Beweis. Falls $\mathbb{C} \subseteq K$ gilt, so ist nach 2.3.2 sogar[52] $\mathbb{C} = K$. Sei jetzt $\mathbb{C}$ nicht in K enthalten. Wir setzen

$$L := K(j) \text{ mit } j^2=-1.$$

Wir versehen den $\mathbb{R}$-Vektorraum L mit der Norm

$$|x+yj| := |x| + |y|.$$

Diese Norm hat die in 2.3.2 geforderte Eigenschaft: mit $z=x+yj$ und $z'= x'+y'j$ gilt nämlich

$$\begin{aligned} |zz'| &= |xx'-yy'| + |xy'+x'y| \\ &\le |x|\cdot|x'|+|y|\cdot|y'| + |x|\cdot|y'|+|x'|\cdot|y| \\ &= (|x|+|y|)\cdot(|x'|+|y'|) \\ &= |z|\cdot|z'| \end{aligned}$$

Nach 2.3.2 erhalten wir $L=\mathbb{C}$, also $K = \mathbb{R}$.
QED.

2.3.4 Satz von Ostrowskij

Jede nicht-triviale multiplikative Bewertung des Körpers $\mathbb{Q}$ der rationalen Zahlen ist äquivalent zu einer der p-adischen Bewertungen $|.|_p$ oder zum gewöhnlichen Absolutbetrag.

Beweis. Sei |.| eine nicht-triviale Bewertung von $K:=\mathbb{Q}$, für welche die Dreiecksungleichung gilt. Sei $a\in\mathbb{Z}$ und $a>1$. Dann kann man jedes $b\in\mathbb{Z}$ in der folgenden Gestalt darstellen.

$$b = b_m a^m + b_{m-1} a^{m-1} + ... + b_0$$

mit $0\le b_j < a$ für jedes j und[53] $m \le \log(b)/\log(a)$. Die Dreiecksungleichung liefert

$$|b| \le M\cdot\left(\frac{\log(b)}{\log(a)} + 1\right)\cdot\max(1,|a|^{\log(b)/\log(a)})$$

mit

$$M:= \max\{|d| : d=0,...,a-1\}$$

Speziell für $b=c^n$ und $n \to \infty$ erhalten wir

$$(*) \qquad |c| \le \max\{1,|a|^{\log(c)/\log(a)}\}$$

1.Fall: Es gibt ein $c\in\mathbb{Z}$ mit $c>1$ und $|c|>1$.
Dann gilt $|a|>1$ für jedes $a>1$ aus $\mathbb{Z}$ und Bedingung (*) bekommt die Gestalt

$$|c|^{1/\log(c)} \le |a|^{1/\log(a)}.$$

Aus Symmetriegründen muß sogar das Gleichheitszeichen gelten,

$$|c|^{1/\log(c)} = |a|^{1/\log(a)}.$$

Durch Auflösen nach |a| sehen wir, |a| ist der gewöhnliche Absolutbetrag:

$$|a| = |c|^{\log(a)/\log(c)}.$$

2. Fall: Es gilt $|c| \le 1$ für jedes $c\in\mathbb{Z}$.
Nach Bemerkung (vii) von 1.1.7 ist |.| eine nicht-archimedische Bewertung. Da sie nach Voraussetzung nicht-trivial ist, gibt es ganze Zahlen $a\in\mathbb{Z}$ mit $|a|<1$ und die Menge dieser ganzen Zahlen ist ein Ideal. Wegen $|ab| = |a|\cdot|b|$ ist dieses Ideal ein Primideal, welches von einer Primzahl p erzeugt wird. Nach 1.2.4 ist |.| gerade die zur p-adischen Bewertung gehörige multiplikative Bewertung.
QED.

---

[52] Gleichheit als bewertete Körper, wegen der Eindeutigkeit der Fortsetzung auf endliche Erweiterungen, falls die der Grundkörper vollständig ist.

[53] Die letzte Ungleichung gilt, weil m die größte ganze Zahl ist mit $a^m \le |b|$.

2.3.5 Satz von Gelfand-Tornheim

Jeder archimedisch bewertete Körper k ist isomorph (als bewerteter Körper) zu einem Teilkörper des Körpers der komplexen Zahlen (versehen mit dem gewöhnlichen Absolutbetrag).

Beweis. 1. Schritt. char(k) = 0.

Angenommen, die Charakteristik von k ist eine Primzahl p>0. Dann liegt jedes von Null verschiedene $z = n \cdot 1_k$ mit $n \in \mathbb{Z}$ im Primkörper von k, d.h. es gilt nach dem kleinen Fermatschen Satz

$$z^{p-1}=1,$$

also $|z|^{p-1} = 1$, also $|z| = 1$. Wir haben gezeigt, es gilt

$$|n \cdot 1_k| \leq 1 \text{ für } n=1,2,3,...$$

Nach Bemerkung (vii) von 1.1.7 ist |.| nicht-archimedisch im Widerspruch zu unseren Voraussetzungen.

2. Schritt. Abschluß des Beweises.

Wir wissen nach dem ersten Schritt, daß k die Charakteristik Null hat, d.h. es gilt

$$\mathbb{Q} \subseteq k.$$

Die Einschränkung der Bewertung von k auf $\mathbb{Q}$ ist eine archimedische Bewertung von $\mathbb{Q}$, also nach 2.3.4 äquivivalent zum gewöhnlichen Absolutbetrag. Wir können annehmen, |.| ist auf $\mathbb{Q}$ gleich dem gewöhnlichen Absolutbetrag. Wir können k durch seine Vervollständigung bezüglich |.| ersetzen und deshalb ohne Beschränkung der Allgemeinheit annehmen, k ist vollständig. Dann gilt aber mit $\mathbb{Q} \subseteq k$ sogar $\mathbb{R} \subseteq k$. Die Behauptung folgt jetzt aus 2.3.3.

QED.

2.3.6 Die Bewertungen eines rationalen Funktionenkörpers

Seien k ein Körper, t eine Unbestimmte über k, K:= k(t), $p(t) \in k[t]$ ein irreduzibles Polynom und c eine reelle Zahl mit

$$0 < c < 1.$$

Jedes Element $f(t) \in K^*$ läßt sich dann in der Gestalt

$$f(t) = p(t)^n \cdot \frac{u(t)}{v(t)}$$

mit zu p(t) teilerfremden Polynomen u und v. Wir setzen.

$$\left|p(t)^n \cdot \frac{u(t)}{v(t)}\right|_p := c^{-n}$$

Die so definierte Abbildung

$$|.|_p : k(t)^* \to \mathbb{R}$$

ist eine multiplikative Bewertung von k(t) und heißt p(t)-adische Bewertung oder auch Bewertung zur Stelle p(t).

Für beliebige von Null verschiedenen Polynome $u,v \in k[t]$ setzen wir weiter

$$\left|\frac{u(t)}{v(t)}\right|_\infty := c^{\deg(v)-\deg(u)}$$

Auf diese Weise ist ebenfalls eine Bewertung von k(t) definiert. Ersetzt man in der obigen Definition von K=k(t) die Unbestimmte t durch $s := t^{-1}$ so ist dies gerade die Bewertung zur Stelle s. Man nennt diese Bewertung auch die Bewertung zur Stelle $t=\infty$.

Bemerkung

Jede nicht-triviale Bewertung von k(t), welche auf k trivial ist, ist äquivalent zu einer p(t)-adischen Bewertung oder einer solchen zu Stelle $t=\infty$.

Beweis. Wegen der Trivialität auf k ist die Bewertung nicht-archimedisch. Wie in 2.3.4 wende man 1.2.4 an.

QED.

2.4 Topologie

2.4.1 Definition

Seien k ein Körper und |.| eine multiplikative Bewertung von k. Dann ist durch |.| eine Topologie auf k definiert, bezüglich welcher die Mengen

$$U_\varepsilon(x) := \{y \in k \mid |y-x| < \varepsilon\}$$

mit $x \in k$ und $\varepsilon > 0$ eine Topologiebasis bilden. Diese Topologie heißt die durch die Bewertung induzierte Topologie.

Bemerkungen

(i) Äquivalente Bewertungen induzieren dabei dieselbe Topologie.

(ii) Bewertungen, für welche die Dreiecksungleichung gilt definieren eine Metrik $d(x,y) := |x-y|$, welche ihrerseits die zugehörige Topologie induziert.

2.4.2 Topologische Körper

Seien k ein Körper und |.| eine multiplikative Bewertung von k. Dann ist k mit der durch |.| induzierten Topologie eine topologischer Körper, d.h. die Abbildungen

$$k \times k \to k,\ (a,b) \mapsto a+b,$$

$$k \times k \to k,\ (a,b) \mapsto ab,$$

$$k^* \to k^*,\ a \mapsto a^{-1}$$

sind stetig.

Beweis. Wir können annehmen, für |.| gilt die Dreiecksungleichung. Die Stetigkeit der Addition ergibt sich aus folgender Abschätzung.

$$|(a+b)-(a_0+b_0)| \le |a-a_0| + |b-b_0|.$$

Die Stetigkeit der Subtraktion ergibt sich aus folgender Abschätzung.

$$|ab - a_0b_0| = |(a-a_0)b + a_0(b-b_0)| \le |a-a_0|\cdot|b| + |a_0|\cdot|b-b_0|.$$

Die Stetigkeit der Inversenbildung ergibt sich aus folgender Abschätzung.

$$\left|\frac{1}{a} - \frac{1}{a_0}\right| = \frac{1}{|a|\cdot|a_0|} \cdot |a-a_0|$$

QED.

2.4.3 Bewertungen mit äquivalenten Topologien

Seien k ein Körper und $|.|_1$ und $|.|_2$ zwei Bewertungen von k, welche dieselbe Topologie auf k induzieren. Dann sind die beiden Bewertungen äquivalent.

Beweis. Die Bedingung $|x| < 1$ ist für eine Bewertung genau dann erfüllt, wenn in der durch |.| induzierten Topologie $x^n \to 0$ gilt für $n \to \infty$. Deshalb gilt

$$|x|_1 < 1 \Leftrightarrow |x|_2 < 1.$$

Indem wir x durch sein Inverses ersetzen, sehen wir, es gilt auch

$$|x|_1 > 1 \Leftrightarrow |x|_2 > 1$$

und

$$|x|_1 = 1 \Leftrightarrow |x|_2 = 1.$$

Seien jetzt $b,c \in k^*$. Wir wenden die obigen Bemerkung auf $a := b^m c^n$ an und erhalten,

$$m \log|b|_1 + n \log|c|_1 \ge 0 \Leftrightarrow m \log|b|_2 + n \log|c|_2 \ge 0.$$

Das ist aber nur möglich, wenn

$$\frac{\log|b|_1}{\log|b|_2} = \frac{\log|c|_1}{\log|c|_2}$$

gilt. Speziell für c=1 erhalten wir $\log|b|_1 = \log|b|_2$ also $|b|_1 = |b|_2$.

QED.

2.5 Vollständigkeit

2.5.1 Vereinbarung

Multiplikative Bewertungen seien im folgenden innerhalb ihrer Äquivalenzklasse so gewählt, daß die Dreiecksungleichung (bzw. im nicht-archimedischen Fall die verschärfte Dreiecksungleichung) gilt.

2.5.2 Definition

Sei k ein (multiplikativ) bewerteter Körper. Dann heißt k vollständig, wenn k als metrischer Raum mit der Abstandsfunktion

$$d(x,y) := |x-y|$$

vollständig ist. Mit anderen Worten, wir fordern, daß jede Cauchy-Folge konvergent sein soll: für jede Folge $\{x_n\}_{n=1,2,...}$ von Elementen aus k mit der Eigenschaft, daß es für jedes $\varepsilon>0$ ein $N=N(\varepsilon)$ gibt mit $|x_n-x_m| < \varepsilon$ für $n,m\geq N$, gibt es ein $x\in k$ mit $x_n \to x$.

2.5.3 Existenz der Vervollständigung

Jeder bewertet Körper k ist Teilkörper eines vollständigen bewerteten Körpers $\bar{k}$ mit folgenden Eigenschaften.

1. Die Bewertung von k ist die Einschränkung der Bewertung von $\bar{k}$.

2. k liegt dicht in $\bar{k}$.

Der Körper $\bar{k}$ ist bis auf natürliche Isomorphie durch die beiden obigen Eigenschaften festgelegt.

Beweis(Skitze). Sei $\bar{k}$ die Vervollständigung von k als metrischer Raum. Da Addition und Multiplikation stetige Abbildungen sind, setzen sie sich zu stetigen Abbildungen auf $\bar{k}$ fort und definieren auf $\bar{k}$ eine Ringstruktur. Wie im Beweis des Lemmas von 2.3.2 sieht man, daß der Übergang zum Inversen ebensfalls eine stetige Abbildung ist. Das hat zur Folge, daß aus der Körpereigenschaft von k diejenige von $\bar{k}$ folgt.
QED.

2.5.4 Die Menge der Werte der Vervollständigung

Seien k ein (multiplikativ) bewerteter Körper und $\bar{k}$ dessen Vervollständigung. Dann sind folgende Aussage äquivalent.
(i) Die Bewertung von k ist nicht-archimedisch.

(ii) Die Bewertung von $\bar{k}$ ist nicht-archimedisch.
Sind die Bedingungen erfüllt, so stimmen die Wertemengen für beide Körper überein,

$$|k| = |\bar{k}|.$$

Beweis. Die Äquivalenz der beiden Bedingungen ergibt sich aus der Charakterisierung der nicht-archimedischen Bewertungen durch die Bedingung

$$|n\cdot 1_k| < 1 \text{ für } n\in\mathbb{Z}$$

(vgl. 1.1.7(vii)). Seien die beiden Bedingungen jetzt erfüllt und sei $x \in \bar{k}$. Wir haben ein $y \in k$ zu finden mit $|x| = |y|$. Dabei können wir annehmen, daß $x \neq 0$, also $|x|>0$ ist. Nach Definition von $\bar{k}$ gibt es ein $y \in k$ mit

(1) $$|x-y| < |x|.$$

Außerdem kann man y so wählen, daß der Wert von x-y beliebig nahe bei Null und der von y beliebig nahe bei |x| liegt. Insbesondere kann man

(2) $$|x-y| < |y|.$$

erreichen.

Es reicht zu zeigen, aus (1) und (2) folgt $|x|=|y|$. Aus (1) ergibt sich, da die Bewertung nicht-archimedisch ist,

$$|y| = |(y-x)+x| \leq \max\{|x-y|, |x|\} = |x|.$$

Analog folgt aus (2)

$$|x| = |(x-y) + y| \leq \max\{|x-y|, |y|\} = |y|$$

QED.

2.5.5 Fortsetzung von Einbettungen in vollständige Körper

Seien k und K (multiplikativ) bewertete Körper und $i:k \to K$ eine die Bewertungen erhaltende Einbettung. Ist K vollständig, so läßt sich i zu einer die Bewertungen erhaltenden Einbettung $\bar{k} \to K$ fortsetzen.

Beweis. Nach Voraussetzung ist $i:k \to K$ stetig. Deshalb läßt sich i auf die Abschließung $\bar{k}$ von k fortsetzen.

QED.

2.6 Unabhängigkeit

Schwacher Approximationssatz

Seien k ein Körper und

$$|.|_n : k \to \mathbb{R}_{\geq 0}, \quad n=1,...,N,$$

paarweise nicht-äquivalente (und nicht-triviale) Bewertungen. Für jedes n bezeichne k_n den bewerteten Körper k mit der Bewertung $|.|_n$. Dann liegt das Bild der Abbildung

$$\Delta: k \to \prod_{n=1}^{N} k_n$$

dicht im direkten Produkt $\prod_{n=1}^{N} k_n$.

Bemerkungen

(i) Ist $k=\mathbb{Q}$ und sind die Bewertungen $|.|_n$ nicht-archimedische (also p-adische) Bewertungen, so ist diese Aussage gerade eine Variante des Chinesischen Restesatzes.

(ii) Unter Vermeidung von topologischen Begriffen kann man die Aussage des Satzes wie folgt formulieren. Für gegebene Elemente $\alpha_n \in k$ und gegebenes $\varepsilon>0$ gibt es ein $\alpha \in k$

$$\text{mit } |\alpha_n - \alpha| < \varepsilon.$$

Beweis. 1. Schritt. Die Aussage folgt aus der Exisitenz von Elementen $\theta_n \in k$ mit

$$|\theta_n|_n > 1 \text{ und } |\theta_n|_m < 1$$

für alle n, m mit $n \neq m$.

Es gilt

$$\lim_{r\to\infty} \frac{\theta_n^r}{1+\theta_n^r} = \lim_{r\to\infty} \frac{1}{1+\theta_n^{-r}} = \begin{cases} 1 & \text{bezüglich } |.|_n \\ 0 & \text{bezüglich } |.|_m \text{ mit } m\neq n \end{cases}$$

(wegen der Stetigkeit von $\frac{x}{1+x}$ bzw. $\frac{1}{1+x}$ und wegen $|\theta_n^{-r}|_n \to 0$ bzw. $|\theta_n^r|_m \to 0$). Mit

$$\alpha(r) := \sum_{n=1}^{N} \frac{\theta_n^r}{1+\theta_n^r} \cdot \alpha_n$$

gilt deshalb

$$\lim_{r\to\infty} \alpha(r) = \alpha_n \text{ bezüglich } |.|_n.$$

Für hinreichend großes r können wir deshalb $\alpha := \alpha(r)$ setzen.

2. Schritt. Konstruktion der θ_n.

Es genügt, wenn wir ein $\theta := \theta_1$ konstruieren mit

$$|\theta|_1 < 1 \text{ und } |\theta|_n > 1 \text{ für } n=2,...,N.$$

Die Konstruktion der übrigen θ_i erfolgt dann analog. Die Konstruktion von θ erfolgt induktiv (bezüglich N).

Sei N = 2. Da die Bewertungen $|.|_1$ und $|.|_2$ nicht-äquivalent sein sollen, gibt es ein $a\in k$ mit

$$|a|_1 < 1 \text{ und } |a|_2 \geq 1.$$

und ein $b\in k$ mit

$$|b|_1 \geq 1 \text{ und } |b|_2 < 1.$$

Das Element $\theta := \frac{b}{a}$ ist dann ein Element der gesuchten Art.

Sei N>2. Nach Induktionsvoraussetzung gibt es ein Elemente $c,d\in k$ mit

$$|c|_1 > 1 \text{ und } |c|_n < 1 \text{ für } n\neq 1,N$$

$$|d|_1 > 1 \text{ und } |d|_n < 1 \text{ für } n\neq 1,N-1$$

Wir können setzen

$$\theta := \begin{cases} c & \text{falls } |c|_N < 1 \\ d & \text{falls } |d|_{N-1} < 1 \\ cd & \text{falls } |c|_N = |d|_{N-1} = 1 \\ \frac{c^r d}{1+c^r} & \text{falls } |c|_N > 1 \text{ und } |d|_{N-1} \geq 1 \\ \frac{cd^r}{1+d^r} & \text{falls } |c|_N > 1 \text{ und } |c|_{N-1} \geq 1 \end{cases}$$

mit r groß. In den ersten drei Fälle ist offensichtlich θ von der gesuchten Art. Es ist damit also nur noch der Fälle

$$|c|_{N-1} \geq 1,\ |d|_N \geq 1 \text{ (nicht beide =1)}$$

zu behandeln. Mit den vierten und fünften Fall sind somit alle Fälle erfaßt. Im vierten Fall gilt

$$\frac{c^r}{1+c^r} = \frac{1}{1+\frac{1}{c^r}} \to 1 \text{ bezüglich der Normen } \|_1 \text{ und } \|_N.$$

Für große Werte von r domminiert in θ der Wert von d, d.h. θ in diesen Bewertungen einen Wert der geforderten Art. Weiter gilt

$$\frac{c^r}{1+c^r} \to 0 \text{ bezüglich aller anderen Bewertungen,}$$

d.h. hat auch in den anderen Bewertungen einen Wert der geforderten Art (d.h. <1). Der fünfte Fall ist symmetrisch zum vierten.
QED.

2.7 Der Fall endlicher Restklassenkörper

2.7.1 Voraussetzungen und Bezeichnungen

k	nicht-archimedisch bewerteter Körper
$\|.\|$	Bewertung von k
$\mathcal{O}$	$:= \{x \in k \mid \|x\| \leq 1\}$ Bewertungsring von k, Ring der ganzen Zahlen von k.
$\mathcal{O}^*$	$:= \{x \in k \mid \|x\| = 1\}$ Einheitengruppe von k.
$\mathcal{P}$	$:= \{x \in k \mid \|x\| < 1\}$ Bewertungsideal von k.
$\mathcal{O}/\mathcal{P}$	Restklassenkörper von k.
$\bar{k}$	Vervollständigung von k.
$\bar{\mathcal{O}}$	Bewertungsring von $\bar{k}$
$\bar{\mathfrak{p}}$	Bewertungsideal von $\bar{k}$.

Voraussetzungen dieses Abschnitts (2.7)
1. $\mathcal{O}/\mathcal{P}$ ist endlich.
2. $|.|: k \to \mathbb{R}_{\geq 0}$ ist diskret, d.h. $\mathcal{P} = \pi\mathcal{O}$ für ein $\pi \in \mathcal{O}$.

Bemerkung
Unter den angegebenen Voraussetzungen gilt

$$\bar{\mathcal{O}}/\bar{\mathfrak{p}} = \mathcal{O}/\mathcal{P} \text{ und } \bar{\mathfrak{p}} = \pi\bar{\mathcal{O}} .$$

(mit demselben π wie in Voraussetzung 2.)
Beweis. Nach Konstruktion gilt

(1) $k \subseteq \bar{k}$

(2) $\mathcal{O} = k \cap \bar{\mathcal{O}}$

(3) $\bar{\mathfrak{p}} = k \cap \bar{\mathfrak{p}}$

1. Schritt. Beweis der Identität $\bar{\mathfrak{p}} = \pi\bar{\mathcal{O}}$.

Wegen $\mathcal{P} = k \cap \bar{\mathfrak{p}}$ gilt $\pi \in \bar{\mathfrak{p}}$, also $\bar{\mathfrak{p}} \supseteq \pi\bar{\mathcal{O}}$. Sei umgekehrt $x \in \bar{\mathfrak{p}}$. Dann gibt es eine eine Folge von Elementen x_n mit $x_n \to x$ in $\bar{k}$. Wegen $x \in \bar{\mathfrak{p}}$ gilt $|x|<1$ also $|x_n|<1$ für n hinreichend groß. Wir können deshalb annehmen $x_n \in \mathcal{P}$ für alle n, also $y_n := \frac{x_n}{\pi} \in \mathcal{P}$.
Wegen $x_n \to x$ und

$$|y_n - y_m| \leq |\frac{1}{\pi}| \cdot |x_n - x_m|$$

bilden die y_n eine Cauchy-Folge, d.h. es gibt ein $y\in\bar{k}$ mit $y_n\to y$. Wegen $y_n\in\mathcal{P}$ gilt $|y_n|\le 1$ für alle n, also auch $|y|\le 1$, also $y\in\bar{\mathcal{O}}$. Wegen der Stetigkeit der Multiplikation gilt mit $y_n\to y$ auch

$$x_n = \pi y_n \to \pi y,$$

also $x = \pi y\in\pi\bar{\mathcal{O}}$. Damit ist die Aussage des ersten Schrittes bewiesen.

2. Schritt. Beweis von $\bar{\mathcal{O}}/\bar{\mathfrak{p}} = \mathcal{O}/\mathcal{P}$.

Mit (2) und (3) gilt auch $p = \mathcal{O}\cap\bar{\mathfrak{p}}$. Also induziert die Inklusion $\mathcal{O}\subseteq\bar{\mathcal{O}}$ eine injektive Abbildung

(4) $$\mathcal{O}/\mathcal{P} \to \bar{\mathcal{O}}/\bar{\mathfrak{p}},\ (x \bmod \mathcal{P}) \mapsto (x \bmod \bar{\mathfrak{p}}).$$

Wir haben zu zeigen, diese Abbildung ist auch surjektiv. Sei $y\in\bar{\mathcal{O}}$ beliebig, dann gibt es ein

$$x\in\mathcal{O}$$

beliebig nahe bei y, zum Beispiel mit $|y-x|<1$. Letzeres bedeutet, es gibt ein $z\in\bar{\mathfrak{p}}$ mit

$$y = x + z.$$

Dann haben aber y und x in $\bar{\mathcal{O}}/\bar{\mathfrak{p}}$ dieselbe Restklasse, d.h. y liegt im Bild der Abbildung (4).
QED.

2.7.2 Beschreibung der Elemente von $\mathcal{O}$ im vollständigen Fall

Sei k ein vollständiger (multiplikativ) bewerteter Körper und $S\subseteq\mathcal{O}$ ein Repräsentantensystem von $\mathcal{O}/\mathcal{P}$. Dann besteht der Ring $\mathcal{O}$ der ganzen Zahlen von k gerade aus den Elementen $a\in k$ welche sich in der Gestalt

$$a = \sum_{j=0}^{\infty} a_j\pi^j,\ a_j\in S,$$

schreiben lassen. Die Koeffizienten a_j sind durch a (bei vorgegebenen S) eindeutig bestimmt.
Beweis. Sei

$$s_n := \sum_{j=0}^{n} a_j\pi^j$$

Dann gilt $s_n - s_m\in\pi^{\min(n,m)}\mathcal{O}$ also

$$|s_n - s_m| \le |\pi|^{\min(n,m)}$$

Die s_n bilden also eine Cauchy-Folge in $\mathcal{O}$. Wegen $s_n\in\mathcal{O}$ für alle n gilt $|s_n|\le 1$, d.h. die x_n konvergieren gegen ein Element a von $\mathcal{O}$.
Sei jetzt umgekehrt $a\in\mathcal{O}$ beliebig. Wir haben a in eine Reihe der oben beschriebenen Gestalt zu entwickeln. Dazu können wir annehmen $a\neq 0$. Dann gibt es ein $n\ge 0$ mit

$$a\in\pi^n\mathcal{O},$$

d.h.

$$a = u \cdot \pi^n$$

mit einer Einheit u von $\mathcal{O}$. Nach Definition von S gibt es genau ein Element $a_n \in S$ mit

$$u - a_n \in \pi\mathcal{O}.$$

Es gilt

$$a - a_n \pi^n = (u - a_n)\pi^n \in \pi^{n+1}\mathcal{O}$$

d.h.

$$a = a_n \pi^n + b \text{ mit } b \in \pi^{n+1}\mathcal{O}.$$

Durch Widerholung des eben angegeben Arguments sehen wir, daß sich jedes Element $a \in \mathcal{O}$ in der Gestalt

$$a = \sum_{j=0}^{n} a_j \pi^j + b \text{ mit } b \in \pi^{n+1}\mathcal{O}$$

schreiben läßt, wobei man n beliebig vorgeben kann. Für $n \to \infty$ erhält man die gesucht konvergente Reihe.
QED.

2.7.3 Kompaktheit von $\mathcal{O}$ im vollständigen Fall

Sei k ein vollständiger bewerteter Körper (mit $\mathcal{O}/\mathcal{P}$ endlich). Dann ist der Ring $\mathcal{O}$ der ganzen Zahlen von k kompakt in der durch die Bewertung definierten Topologie.
Beweis. Sei $U := \{U_i\}_{i \in I}$ eine offenen Überdeckung von $\mathcal{O}$. Angenommen, keine endliche Teilfamilie dieser Überdeckung überdeckt $\mathcal{O}$. Wir fixieren ein Repräsentantensystem

$$S \subseteq \mathcal{O} \text{ von } \mathcal{O}/\mathcal{P}.$$

Dann läßt sich $\mathcal{O}$ wie folgt als Vereinigung von endlich vielen Teilmengen schreiben.

(1) $$\mathcal{O} = \cup\{s + \pi\mathcal{O} \mid s \in S\}$$

Wenigstens eine dieser Teilmengen kann nicht durch eine endliche Teilfamilie von U überdeckt werden, sagen wir $a_0 + \pi\mathcal{O}$. Nun liefert die Zerlegung (1) von $\mathcal{O}$ auch eine Zerlegung von $a_0 + \pi\mathcal{O}$ und durch Wiederholung des eben angegebenen Schlusses sehen wir, es gibt eine Menge der Gestalt

$$a_0 + a_1\pi + \pi^2\mathcal{O},$$

welche durch keine endliche Teilfamilie von U überdeck wird. Iteration liefert ein Element

$$a = \sum_{j=0}^{\infty} a_j \pi^j, \; a_j \in S,$$

von $\mathcal{O}$ mit der Eigenschaft, daß keine der Mengen

$$a + \pi^n O = \sum_{j=0}^{n-1} a_j \pi^j + \pi^n O$$

von einer endlichen Teilfamilie von U überdeckt wird. Wegen $a \in \mathcal{O}$ gibt es ein $i_0 \in I$ mit $a \in U_{i_0}$. Da die Menge U_{i_0} offen ist, gibt es ein N mit

$$a + \pi^N\mathcal{O} \subseteq U_{i_0}$$

im Widerspruch zur Konstruktion von a.
QED.

2.7.4 Lokale Kompaktheit vollständiger bewerteter Körper

Sei k ein vollständiger bewerteter Körper (mit $\mathcal{O}/\mathcal{P}$ endlich). Dann ist k lokal kompakt bezüglich der durch die Bewertung definierten Topologie.

Beweis. Für jedes $x \in k$ ist nach 2.7.3 die Meng $x+\mathcal{O}$ eine relativ kompakte Umgebung vonx.

QED.

Bemerkung

Die nachfolgende Aussage besagt, 2.7.4 läßt sich umkehren.

2.7.5 Lokal kompakte bewertete Körper

Sei k ein nicht-archimedisch bewerteter Körper, der in der Topologie, die durch die Bewertung definiert wird, lokal kompakt ist. Dann gilt auch umgekehrt:

(i) k ist vollständig.
(ii) Der Restklassenkörper $\mathcal{O}/\mathcal{P}$ ist endlich.
(iii) Die Bewertung |.| von k ist diskret.

Beweis. Zu (i). Sei $U \subseteq k$ eine Umgebung der $0 \in k$, deren Abschließung $\bar{U}$ kompakt ist. Dann gibt es ein $\pi \in p-\{0\}$ und ein $N \in \mathbb{Z}$ mit

$$\pi^N \mathcal{O} \subseteq \bar{U}.$$

Die Menge $\pi^N\mathcal{O}$ ist abgeschlossene Teilmenge der kompakten Menge $\bar{U}$ und als solche selbst kompakt. Nun wird aber $\mathcal{O}$ bei der Abbildung

$$k \to k,\ x \mapsto \pi^N x,$$

homöomorph auf $\pi^N\mathcal{O}$ abgebildet, d.h. $\mathcal{O}$ ist kompakt. Nun definiert die Bewertung |.| eine Metrik auf der kompakten Menge $\mathcal{O}$, d.h. jede Cauchy-Folge in $\mathcal{O}$ besitzt einen Limes in $\mathcal{O}$. Mit anderen Worten, $\mathcal{O}$ ist ein vollständiger metrischer Raum. Für jede Cauchy-Folge $\{x_n\}$ in k ist die Folge der Wert $|x_n|$ beschränkt, d.h. die x_n liegen in einer Menge der Gestalt

$$\pi^N\mathcal{O},\ N \in \mathbb{Z}.$$

Aus der Vollständigkeit von $\mathcal{O}$ folgt, die Cauchy-Folge ist konvergent. Damit ist Aussage (i) bewiesen.

Zu (ii). Sei $S \subseteq \mathcal{O}$ ein Repräsentantensystem von $\mathcal{O}/\mathcal{P}$ in $\mathcal{O}$. Dann bilden die Mengen

$$U_s := \{x \in k \mid |x-s| < 1\} = s + \mathcal{P}$$

mit $s \in S$ eine offene Überdeckung von $\mathcal{O}$. Für je zwei Elemente x,y aus verschiedenen Mengen U_s ist die Differenz eine Einheit (da sie verschiedene Elemente modulo $\mathcal{P}$ repräsentieren). Insbesondere gilt $|x-y| = 1$, d.h. die Mengen U_s sind paarweise disjunkt. Da $\mathcal{O}$ kompakt ist, überdecken bereits endlich viele der Mengen U_s die Menge $\mathcal{O}$. Das ist aber nur möglich, wenn S selbst schon endlich ist, d.h. $\mathcal{O}/\mathcal{P}$ ist endlich.

Zu (iii). Wir zeigen zunächst, die Menge $\mathcal{P}$ ist kompakt. Die Menge $\mathcal{O}$-$\mathcal{P}$ ist nach (ii) Vereinigung von endlich vielen paarweise disjunkten Restklassen der Gestalt $x + \mathcal{P}$. Da $\mathcal{P}$ offen ist, ist jede dieser Restklassen offen. Also ist $\mathcal{O}$-$\mathcal{P}$ offen, d.h. $\mathcal{P}$ ist abgeschlossen.

Als abgeschlossene Teilmenge der kompakten Menge $\mathcal{O}$ ist $\mathcal{P}$ kompakt.

Sei jetzt

$$U_n := \{x \in O \mid |x| < 1 - \frac{1}{n}\}$$

Die Folge der U_n, n=1,2,3,..., bildet eine offene Überdeckung von $\mathcal{P}$. Da $\mathcal{P}$ kompakt ist, gibt es eine endliche Teilüberdeckung, d.h. es gilt

$$\mathcal{P} = U_n$$

für ein n. Mit anderen Worten, es gilt (iii).
QED.

2.7.6 Haarsche Maße auf bewerteten Körperen

Sei k ein nicht-archimedisch bewerteter Körper, der in der durch die Bewertung induzierten Topologie lokal kompakt ist. Wir bezeichnen mit k^+ die kommutative topologische Gruppe deren Punkte die Elemente von k sind, deren Komposition die Addition des Körpers k ist und deren Topologie durch die Bewertung |?| von k definiert ist. Wie wir gesehen haben, ist k lokal kompakt. Aus der allgemeinen Integrationstheorie wissen wir, daß es auf k ein Maß gibt, welches gebenüber Transformationen der Gestalt

$$k^+ \to k^+,\ x \mapsto x+a,$$

mit $a \in k^+$ invariant ist, das sogenannte Haarsche Maß. Es ist sogar bis auf einen konstanten von Null verschiedenen Faktor eindeutig bestimmt. Sei wie bisher $\mathcal{O} = \mathcal{O}_k$ der Ring der ganzen Zahlen von k. Als kompakte Teilmenge von k^+ hat $\mathcal{O}$ ein endliches Maß. Durch die Normalisierungsbedingung

$$\mu(\mathcal{O}) = 1.$$

ist damit das Haarsche Maß eindeutig festgelegt. Sei $\mathcal{P} = \pi\mathcal{O}$ das Bewertungsideal. Da die Mengen der Gestalt $a+\pi^n\mathcal{O}$ eine Topolgie-Basis für die Topolgie von k^+ bilden, genügt es für die Bestimmung von μ das Maß dieser Mengen zu berechnen.
Behauptung:

$$\mu(a+\pi^n\mathcal{O}) = |\mathcal{O}/\mathcal{P}|^{-n}$$

Beweis. Sei r:= $|\mathcal{O}/\mathcal{P}|$.Der Wert

$$\mu_n := \mu(a+\pi^n\mathcal{O})$$

hängt wegen der Invarianz gegenüber Translationen nicht von $a \in k^+$ ab. Weiter haben wir disjunkte Zerlegungen

$$\mathcal{O} = (a_1+\pi\mathcal{O}) \cup (a_2+\pi\mathcal{O}) \cup \ldots \cup (a_r+\pi\mathcal{O})$$

und

$$a+\pi^n\mathcal{O} = \cup_{j=1}^{r} (a + \pi^n a_j + \pi^{n+1}\mathcal{O}).$$

Deshalb gilt

$$\mu_n = r \cdot \mu_{n+1}.$$

Nach Vereinbarung soll $\mu_0 = \mu(\mathcal{O}) = 1$ sein. Für beliebiges n ist deshalb $\mu_n = r^{-n}$.

QED.

Bemerkungen

(i) Man kann leicht ohne Bezugnahme auf die Theorie des Haarschen Maßes zeigen, daß durch die obige Formel ein translationsinvariantes Maß auf k^+ definiert ist.

(ii) Das Haarsche Maß bietet die Möglichkeit unter den verschiedenen Bewertungen einer Klasse äquivalenter Bewertungen eine auszuzeichnen. Das führt zum Begriff der normalisierten Bewertung.

2.7.7 DefinitionNormalisierte Bewertungen

Sei k ein nicht-archimedisch bewerteter lokal kompakter Körper. Die Bewertung |?| von k heißt dann normalisiert, wenn

$$|\pi| = P^{-1}$$

gilt. Dabei bezeichne P die (endliche) Anzahl der Elemente des Restklassenkörpers des Körpers k (vgl. 2.7.5).

2.7.8 Haarsches Maß und normalisierte Bewertung

Sei k ein vollständer Körper bezüglich der normalisierten Bewertung |?| mit dem Bewertungsring $\mathcal{O}$ (und endlichem Restklassenkörper). Dann gilt für das Haarsche Maß von k,

$$|a+b\mathcal{O}| = |b|.$$

Beweis. siehe 2.7.6
QED.
Bemerkungen

(i) Die Aussage dieses Satzes kann man auch wie folgt ausdrücken. Sei μ ein (nicht notwendig normalisiertes) Haarsches Maß auf k^+. Dann kann man auf k^+ ein neues Haarsches Maß definieren, indem man setzt

$$\mu_\beta(E) := \mu(\beta \cdot E)$$

für ein fest gewähltes $\beta \in k^+ - \{0\}$ und beliebige meßbare Mengen E. Nun ist das Haarsche Maß bis auf einen konstanten Faktor eindeutig bestimmt. Deshalb gilt

$$\mu(\beta \cdot E) = f \cdot \mu(E)$$

für alle meßbaren Mengen E. Der Faktor $f \in \mathbb{R}$ hängt dabei nur von β ab. Der Satz sagt aus bezüglich der normalisierten Bewertung gilt

$$f = |\beta| .$$

Das gibt uns eine weiter Möglichkeit in die Hand zur Definition des Begriffs der normalisierten Bewertung.

(ii) In der Theorie der lokal kompakten Gruppen betrachtet man die zu k^+ duale Gruppe, welche Charakter-Gruppe von k^+ heißt. Man kann zeigen, die Charaktergruppe von k^+ ist isomorph zu k^+. Für die Zwecke der Klassenkörpertheorie wird diese Tatsache nicht benötigt. Wir werden sie deshalb nicht beweisen. Einen Beweis und Anwendungen kann man in [10] finden. Verallgemeinerung finden sich in [6] und [8]. Die Definition der Charaktergruppe ist Gegenstand der lokalen Klassenkörpertheorie.

2.7.9 Die multiplikative Gruppe von k (im vollständigen Fall)

Sei k ein nicht-archimedisch bewerteter lokal kompakter Körper. Die Menge der von Null verschiedenen Elemente des Körpers k bilden eine Gruppe

$$k^*$$

bezüglich der Multiplikation. Wir versehen k* mit der Unterraumtopologie von k. Dann definieren Multiplikation und Übergang zum Inversen stetige Abbildungen, d.h. k* ist eine topologische Gruppe[54]. Es gilt

$$k^* \supseteq E \supseteq E_1,$$

wenn

$$E := \{x \in k \mid |x|=1\}$$

die Gruppe der Einheiten von k und

$$E_1 := \{x \in k \mid |1-x|<1\}$$

die Gruppe der Haupteinheiten bezeichnet. Die Untergruppen E und E_1 sind beide offen und abgeschlossen[55] in k*. Die Gruppe k*/E ist isomorph zu $\mathbb{Z}$, als Isomorphismus kann man die Abbildung

$$\mathbb{Z} \to k^*/E,\ n \mapsto \pi^n \bmod E,$$

---

[54] Später werden wir den Fall eines topologischen Ringes betrachten und die Gruppe R* der Einheiten mit einer Topologie versehen, die von der hier betrachteten Topologie verschieden ist.

[55] E ist offen, weil mit $x \in E$ sogar $x+E_1 \subseteq E$ gilt. Die Gruppe E_1 ist abgeschlossen, weil die Bewertung nach Voraussetzung diskret ist.

mit einem lokalen Parameter π nehmen. Die Gruppe E/E_1 ist isomorph zur multiplikativen Gruppe der von Null verschiedenen Elemente des Restklassenkörpers[56],

$$E/E_1 \to (O/p)^*, \; u \bmod E_1 \mapsto u \bmod p.$$

Da $E_1 = 1 + \pi O$ kompakt ist und $(O/p)^*$ endlich, ist auch E kompakt. Die Gruppe k^* ist lokal kompakt. Das additive Haarsche Maß ist auch invariant gegenüber der Multiplikation mit Elementen aus $E_1 = 1 + \pi O$ (auf Grund der Formel von 2.7.6). Damit erhalten wir ein Haarsches Maß auf E_1 und damit auf $k^* = \mathbb{Z}\times\mathbb{Z}/(P-1)\times E_1$.

2.7.10 Der Zusammenhang von k^+ und k^*

Sei k ein nicht-archimedisch bewerteter lokal kompakter Körper. Die Gruppen k^+ und k^* sind dann vollständig unzusammenhängend (d.h. die einzigen zusammenhängenden Teilmengen sind die einpunktigen Mengen).

Beweis. Es reicht, die Aussage für k^+ zu beweisen. Sei $A \subseteq k^+$ eine zusammenhängende Teilmenge. Angenommen, A enthält zwei verschiedene Punkte $a,b \in A$. Dann gibt es ein n mit

$$(a+\pi^n\mathcal{O}) \cap (b+\pi^n\mathcal{O}) = \varnothing.$$

Die Zerlegung von k^+ in Restklassen modulo der Untergruppe $\pi^n O$ ist eine Zerlegung in paarweise disjunkte offene Untergruppen. Durch Einschränken auf A erhält man eine entsprechende Zerlegung von A, wobei mindestens zwei Mengen der Zerlegung nicht-leer sind. Durch Zusammenfassen erhält eine Zerlegung von A in zwei disjunkte offene und nicht-leere Teilmengen. Das steht aber im Widerspruch dazu, daß A zusammenhängend sein soll.
QED.

2.7.11 Lokale Isomorphie von k^+ und k^* im Fall der Charakteristik Null

Sei k ein nicht-archimedisch bewerteter lokal kompakter Körper. Außerdem sei die Charakteristik von k gleich 0. Dann sind k^+ und k^* lokal isomorph.
Beweis. Die Exponentialabbildung

$$x \mapsto \exp(x) := \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

ist für kleine x definiert und die Umkehrung

$$x \mapsto \log(x) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}\cdot(x-1)^n}{n}$$

ist für x nahe bei 1 ebenfalls definiert.
QED.

---

[56] Man kann zeigen, $(O/p)^*$ ist eine zyklische Gruppe (der Ordnung P-1), d.h. k enthält stets eine primitive (P-1)-te Einheitswurzel ρ. Damit läßt sich jedes Element aus k^* eindeutig in der Gestalt

$$\pi^v\cdot\rho^u\cdot\varepsilon$$

schreiben mit $\varepsilon \in E_1$. Die Gruppe k^* zerfällt daher in ein direktes Produkt

$$k^* = \mathbb{Z}\times\mathbb{Z}/(P-1)\times E_1.$$

Um die Existenz von ρ einzusehen, setzen wir $f(X) := X^{P-1}-1$ und wählen ein Element $\alpha \in O$ derart, daß α mod p die multiplikative Gruppe $(O/p)^*$ erzeugt. Dann gilt $|f(\alpha)| < 1$ und $|f'(\alpha)| = 1$. Nach dem Henselschen Lemma gibt es ein $\rho \in k$ mit $f(\rho) = 0$ und $\rho \equiv \alpha \bmod p$.

2.8 Normierte Räume

2.8.1 Begriff des normierten Vektorraums

Seien k ein bewerteter Körper und V ein k-Vektorraum. Eine reellwertige Abbildung

$$||?||: V \to \mathbb{R}$$

heißt Norm, wenn folgende Bedingungen erfüllt sind.

1. $||v|| > 0$ für jedes $v \in V-0$.
2. $||v'+v''|| \leq ||v'|| + ||v''||$ für $v', v'' \in V$.
3. $||c \cdot v|| = |c| \cdot ||v||$ für $c \in k$, $v \in V$.

Ein mit einer Norm versehene k-Vektorraum heißt normierter k-Vektorraum.

2.8.2 Äquivalente Normen

Zwei Normen $||?||_1$ und $||?||_2$ auf dem k-Vektorraum V heißen äquivalent, wenn es reelle Konstanten c_1, c_2 gibt mit

$$||v||_1 \leq c_1 ||v||_2 \text{ und } ||v||_2 \leq c_2 ||v||_1$$

für alle $v \in V$.

Bemerkungen

(i) Auf diese Weise ist eine Äquivalenzrelation definiert.
(ii) Äquivalente Normen definieren dieselbe Topologie auf V.

2.8.3 Endlich-dimensionale Vektorräume über vollständigen Körpern

Seien k ein bewerteter Körper und V ein k-Vektorraum. Ist k vollständig und V endlich-dimensional über k, so sind je zwei Normen von V äquivalent.

Beweis.

QED.

2.9 Tensorprodukte

2.9.1 Konstruktion: Definition von des Tensorprodukts

Wir benötigen nur einen Spezialfall. Seien

$$A, B$$

kommutative Ringe, die einen Körper

$$k$$

enthalten. Außerdem sei B als k-Vektorraum von endlicher Dimension

$$N := \dim_k B < \infty.$$

Wir fixieren eine k-Vektorraumbasis von B über k,

$$1 = \omega_1, \omega_2, \ldots, \omega_N.$$

Der Ring B ist bis auf Isomorphie festgelegt durch die Multiplikationstabelle

$$\omega_\ell \omega_m = \sum_{n=1}^{N} c_{\ell mn} \omega_n, \; c_{\ell mn} \in k.$$

Wir können jetzt einen neuen Ring C definieren, welcher den Körper k enthält, dessen Elemente Ausdrücke der Gestalt

$$\sum_{m=1}^{N} a_m \overline{\omega}_m \text{ mit } a_m \in A$$

wobei die Multiplikation gegeben ist durch

$$\overline{\omega}_\ell \overline{\omega}_m = \sum_{n=1}^{N} c_{\ell mn} \overline{\omega}_n, \; c_{\ell mn} \in k.$$

d.h. die $\overline{\omega}_n$ multiplizieren sich in derselben Weise wie die ω_n. Es gibt Isomorphismen der Ringe A und B mit Teilringen des Rings C,

$$i: A \to C,\ a \mapsto a\overline{\omega}_1,$$

$$j: B \to C,\ \sum_{m=1}^{N} \lambda_m \omega_m \mapsto \sum_{m=1}^{N} \lambda_m \overline{\omega}_m .$$

Bemerkungen

(i) Es ist klar, daß C bis auf Isomorphie durch die Ringe A und B festgelegt ist und nicht von der Wahl der speziellen Basis $\{\omega_m\}$ abhängt: Der Leser überprüft ohne Schwierigkeiten, daß der Ring C zusammen mit den Abbildungen i und j einer Universalitätseigenschaft genügt. Wir nennen C Tensorprodukt von A und B über k und schreiben

$$C = A \otimes_k B.$$

(ii) Sei jetzt A ein topologischer Ring, d.h. A besitze eine Topologie bezüglich welcher Addition und Multplikation stetig sind. Die Abbildung

$$C \to A^N,\ \sum_{m=1}^{N} a_m \overline{\omega}_m \mapsto (a_1,...,a_m),$$

ist A-linear bijektiv. Wir führen auf C die Produkt-Topologie ein. Es ist nicht schwer zu zeigen:

1. Diese Topologie hängt nicht von der Wahl der Basis $\{\omega_m\}$ ab.

2. Multiplikation und Addition in C sind stetig bezüglich der eingeführten Topologie.

Wir nennen diese Topologie von C die Tensorprodukt-Topologie.

2.9.2 Das Tensorprodukt von Körpern

Seien A und B zwei Körper, welche den gemeinsamen Teilkörper k enthalten. Der Körper B sei eine separable Erweiterung des Grades

$$N = [B:k] < \infty$$

von k. Dann ist

$$C := A \otimes_k B$$

eine direkte Summe von Körpern K_ν, von denen jeder einen zu A und zu B isomorphen Teilkörper enthält. Genauer, die Zusammensetzungen

$$A \xrightarrow{i} C \to K_\nu$$

$$B \xrightarrow{j} C \to K_\nu$$

der oben definierten Abbildungen i und j mit der natürlichen Projektion auf den ν-ten Faktor sind für jedes ν Einbettungen von A bzw. B als Teilkörper in K_ν.

Beweis. Nach einem bekannten Satz (vgl. Anhang B) gilt

$$B = k(\beta) \text{ mit } f(\beta) = 0$$

ein separables Polynom $f(X) \in k[X]$ des Grades N, welches irreduzibel über k ist. Die Elemente

$$1, \beta, \ldots \beta^{N-1}$$

bilden dann eine Basis von B über k. Damit ist

$$A \otimes_k B = ($$

wobei die Elemente

$$1, \overline{\beta}, \ldots \overline{\beta}^{N-1}$$

linear unabhängig über A sind und der Relation

$$f(\overline{\beta}) = 0$$

genügen. Obwohl das Polynom f irreduzibel über k ist, braucht es nicht über A irreduzibel zu sein. Sei

$$f(X) = \prod_{j=1}^{J} g_j(X)$$

eine Zerlegung von f in irreduzible Faktoren

$$g_j(X) \in A[X].$$

Die g_j sind paarweise teilerfremd, denn f ist separabel. Sei

$$K_j := A(\beta_j) \text{ mit } g_j(\beta_j) = 0.$$

Nach Konstruktion enthält jedes K_j eine Kopie von A und von B als Teilkörper. Es reicht also zu zeigen, $A \otimes B$ ist eine direkte Summe der K_j.

Die folgende Abbildung ist ein Ring-Homomorphismus.[57]

$$A \otimes_k B \xrightarrow{\mu_j} K_j \text{ , } h(\overline{\beta}) \mapsto h(\beta_j), \; h(X) \in A[X].$$

Wir erhalten damit einen Homomorphismus von A-Algebren

$$(1) \qquad (\mu_1,...,\mu_J): A \otimes_k B \to \oplus_{j=1}^{J} K_j \text{ .}$$

Diese Abbildung ist injektiv: sei $h(X) \in A[X]$, daß $h(\overline{\beta})$ im Kern der Abbildung liegt. Dann ist $h(\beta_j) = 0$ für jedes j, d.h. g_j teilt h für jedes j , f teilt h, d.h. $h(\overline{\beta}) = 0$. Wir haben gezeigt, (1) ist eine Einbettung. Da beide Vektorräume in (1) über A dieselbe Dimension

$$N = \deg f = \sum_{j=1}^{J} \deg g_j$$

haben, ist diese Abbildung sogar ein Isomorphismus.
QED.

2.9.3 Folgerung 1: Verhalten des charakteristischen Polynoms beim Tensorieren mit einer Erweiterung

Seien A und B zwei Körper, welche den gemeinsamen Teilkörper k enthalten. Der Körper B sei eine endliche separable Erweiterung des von k und

$$A \otimes_k B = \oplus_{j=1}^{J} K_j$$

sei die in 2.9.2 beschriebene Zerlegung in gemeinsame Körpererweiterungen von A und B. Weiter sei

$$\alpha \in B$$

ein Element mit dem charakteristischen Polynom

$$f(X) \in k[X]$$

über k. Bezeichne α_j das Bild von α bei der natürlichen Abbildung

$$B \to A \otimes_k B \to K_j$$

und

$$g_j(X) \in A[X]$$

---

[57] Genauer: es gilt

$$A \otimes_k B = A[\overline{\beta}] = A[X]/(f) \text{ und } K_j = A[\beta_j] = A[X]/(g_j)$$

wegen $g_j \mid f$ in A[X] induziert die identische Abbildung $A[X] \to A[X]$ eine Surjektion

$$A \otimes_k B = A[X]/(f) \to A[X]/(g_j) = K_j \text{ .}$$

das charakteristische Polynom von α_j über A.Dann gilt

$$f(X) = \prod_{j=1}^{J} g_j(X).$$

Beweis. Es reicht zu zeigen, beide Seiten der zu beweisenden Identität sind gleich dem charakteristischen Polynom

$$\chi_{1\otimes\alpha}(X) = \det(\mathrm{mult}(1\otimes\alpha - X\cdot Id)$$

des Bildes von α in $A\otimes_k B$ über A. Dazu schreiben wir mit Hilfe einer k-Vektorraumbasis $\omega_1, \omega_2, \ldots, \omega_N$ von B über k,

$$\alpha\cdot\omega_i = \sum_{i=1}^{N} c_{ij}\omega_j \text{ mit } c_{ij} \in k.$$

Anwenden des B-Algebra-Homomorphismus $B \to A\otimes_k B$, $b \mapsto 1\otimes b$, liefert

$$(1\otimes\alpha)\cdot\overline{\omega}_i = \sum_{i=1}^{N} (1\otimes c_{ij})\overline{\omega}_j = \sum_{i=1}^{N} c_{ij}\overline{\omega}_j \text{ mit } \overline{\omega}_j = 1\otimes\omega_j.$$

Die $\overline{\omega}_j$ bilden eine Basis von $A\otimes_k B$ über A, d.h. es gilt

$$\chi_{1\otimes\alpha}(X) = \det(c_{ij} - X\cdot\delta_{ij}) = \chi_\alpha(X) = f(X).$$

Wählen wir für jedes K_j eine A-Vektorraumbasis über A, so bilden alle Basiselemente zusammen eine A-Vektorraumbasis von

$$\oplus K_j = A\otimes_k B$$

Die Multiplikation mit $1\otimes\alpha$ induziert auf dem j-ten direkten Summanden K_j die Multiplikation mit α_j. Die zugehörige Matrix bezüglich der gewählten Basis zerfällt in Blöcke, die entlang der Hauptdiagonalen angeordnet sind. Es folgt

$$\chi_{1\otimes\alpha}(X) = \prod_{j=1}^{J} \chi_{\alpha_j}(X) = \prod_{j=1}^{J} g_j(X).$$

Zusammen erhalten wir die Behauptung.
QED.

2.9.4 Folgerung 2: Verhalten von Norm und Spur beim Tensorieren mit einer Erweiterung

Seien A und B zwei Körper, welche den gemeinsamen Teilkörper k enthalten. Der Körper B sei eine endliche separable Erweiterung von k und

$$A\otimes_k B = \oplus_{j=1}^{J} K_j$$

sei die in 2.9.2 beschriebene Zerlegung in gemeinsame Körpererweiterungen von A und B. Dann gelten für Norm und Spur die Identitäten

$$N_{B/k}(\beta) = \prod_{j=1}^{J} N_{K_j/A}(\beta)$$

$$Tr_{B/k}(\beta) = \sum_{j=1}^{J} Tr_{K_j/A}(\beta)$$

für jedes Element $\beta\in B$.
Beweis. Spur und Norm sind gleich dem zweiten bzw. letzten Koeffizienten des charakteristischen Polynoms. Die Behauptung folgt damit aus der Formel vn 2.9.3.
QED.

2.10 Fortsetzung von Bewertungen

2.10.1 Definition

Seien K/k eine Körpererweiterung, |?| und ||?|| Bewertungen von k bzw. von K. Wir sagen, ||?|| ist eine Fortsetzung von |?|, wenn

$$||x|| = |x|$$

gilt für jedes $x \in k$.

2.10.2 Theorem 10.1: Existenz von Fortsetzungen

Seien K/k eine Körpererweiterung und |?| eine Bewertung von k. Wir nehmen an,

1. k ist vollständig bzgl. |?|.
2. $N:=[K:k]<\infty$.

Dann existiert genau eine Fortsetzung von |?| zu einer Bewertung von K. Diese ist durch folgende Formel gegeben.

(1) $$||x|| = |N_{K/k}(x)|^{1/N}$$

Beweis. Eindeutigkeit. Den Körper K kann man als Vektorraum über k ansehen. Dann ist die Bewertung || ? || von K eine Norm im Sinne von Definition 2.8.1. Also sind je zwei Fortsetzungen $||?||_1$ und $||?||_2$ von |?| auf K äquivalent als Normen (vgl. 2.8.3), d.h. sie induzieren dieselbe Topologie auf K. Wir haben jedoch gesehen (vgl. 2.4.3), daß zwei Bewertungen von K, die dieselbe Topologie induzieren, äquivalent sind, d.h. es gilt

$$||?||_1 = ||?||_2^c$$

für ein $c \neq 0$. Weil die beiden Bewertungen aber auf k übereinstimmen, muß sogar $c = 1$ gelten.

Existenz. Den Existenzbeweis im allgemeinen Fall findet man in [2]; für den Fall separabler Körper K und nicht-archimedischer diskreter Bewertungen, siehe Kapitel I, Folgerung 1 aus Proposition 4.1 (vgl. 1.4.3). Wir geben hier den von Dr. Geyer auf der Konferenz vorgeschlagenen Beweis für den Fall eines lokal kompakten Körpers k, welches der einzige uns interessierende Fall ist. Auf jeden Fall ist leicht zu sehen, daß die durch Formel (1) gegebene Funktion die Bedingungen 1 und 2 in der Definition einer Bewertung (siehe 2.1) erfüllt:

1. $||\alpha|| \geq 0$ und $||\alpha|| = 0 \Leftrightarrow \alpha = 0$.
2. $||\alpha\beta|| = ||\alpha|| \cdot ||\beta||$.

Das Problem besteht im Beweis der dritten Bedingung:

3. Es gibt eine Konstante C mit $|1+x| \leq C$ für alle $x \leq 1$.

Zum Beweis fixieren wir eine beliebige Norm

$$||?||_0 : K \to \mathbb{R}$$

auf dem k-Vektorraum K.[58] Dann ist die durch Formel (1) definierte Funktion

$$||?|| : K \to \mathbb{R}$$

eine stetige Funktion ohne Nullstellen auf der kompakten Menge[59]

$$\{ \alpha \in K : ||\alpha||_0 = 1 \}.$$

Also gibt es reelle Konstanten Δ und δ mit

$$\Delta > ||\alpha|| > \delta > 0$$

für beliebige α aus dieser Menge. Weil ||?|| und $||?||_0$ homogen sind, folgt

---

[58] Zum Beispiel das Maximum der Koordinaten bezüglich einer fest gewählten Vektorraum-Basis von K über k.

[59] die Menge ist kompakt, weil K nach Voraussetzung ein lokal kompakter Körper ist.

$$\Delta > \frac{||\alpha||}{||\alpha||_0} > \delta > 0 \text{ für jedes } \alpha \in K-\{0\}.$$

Sei jetzt $||\alpha|| \leq 1$. Dann gilt $||\alpha||_0 < \delta^{-1}$, also

$$||1+\alpha|| \leq \Delta \cdot ||1+\alpha||_0 \leq \Delta \cdot (||1||_0 + ||\alpha||_0) \leq \Delta \cdot (||1||_0 + \delta^{-1}).$$

Mit anderen Worten, Bedinung 3 ist erfüllt für ||?|| mit $C := \Delta \cdot (||1||_0 + \delta^{-1})$.

QED.

Bemerkung

Der Existenzbeweis von Geyer impliziert insbesondere, daß Formel (1) gilt. Es ist jedoch interessant, daß sich Formel (1) aus der reinen Existenz- und Eindeutigkeitsaussage des Satzes auf folgende Weise ergibt.

Sei $L \supseteq K$ eine endliche normale Erweiterung des Körpers k. Dann gibt es genau eine Fortsetzung der Bewertung |?| von k zu einer Bewertung von L. Bezeichnen wir diese Fortsetzung mit ||?||. Ist σ ein Automorphismus von L über k, so ist durch

$$||\alpha||_\sigma := ||\sigma\alpha||$$

eine weitere Fortsetzung von |?| definiert. Wegen der Eindeutigkeitsaussage gilt

$$||?||_\sigma = ||?||,$$

d.h. es ist

$$||\sigma\alpha|| = ||\alpha||$$

für jeden Automorphismus von L über K. Nun ist aber

$$N_{K/k}(\alpha) = \sigma_1(\alpha) \cdot \sigma_n(\alpha) \cdot \ldots \cdot \sigma_N(\alpha),$$

wenn die σ_i die Fortsetzungen der k-Einbettungen von K in L bezeichnen. Damit ist

$$|N_{K/k}(\alpha)| = ||N_{K/k}(\alpha)|| = ||\sigma_1(\alpha)|| \cdot ||\sigma_n(\alpha)|| \cdot \ldots \cdot ||\sigma_N(\alpha)|| = ||\alpha||^N.$$

Damit gilt Formel (1).

2.10.3 Folgerung 1:Der Wert eines Elements und von dessen Koordinaten

Seien k ein Körper, der vollständig ist bezüglich einer Bewertung l?l und K/k eine Körpererweiterung des Grades N. Weiter sei

$$\omega_1, \ldots, \omega_N$$

eine k-Vektorraumbasis von K. Dann gibt es positive reelle Konstanten c', c" mit

$$c' \leq |\sum_n b_n \omega_n| / \max |b_n| \leq c"$$

für beliebige Elemente $b_n \in k$, die nicht alle gleich Null sind.

Beweis. Durch $|\sum_n b_n \omega_n|$ und $\max |b_n|$ sind zwei Normen des k-Vektorraums K definiert. Diese sind nach 2.8.3 äquivalent.

QED.

2.10.4 Folgerung 2: Erhaltung der Vollständigkeit beim Erweitern

Jede endliche Erweiterung eines vollständigen bewerteten Körpers ist vollständig bezüglich der fortgesetzen Bewertung.

Beweis. Auf Grund der Folgerung 2.10.3 besitzt die Erweiterung die Topologie eine endlich-dimensionalen Vektorraums über dem Grundkörper.

QED.

2.10.4 Theorem 10.2: Zerlegung einer Erweiterung über der Vervollständigung des Grundkörpers

Seien K/k eine separable Körpererweiterung des Grades

$$N := [K:k]$$

und |?| eine Bewertung von k. Dann gibt es höchstens N Fortsetzungen von |?| auf K. Werden diese Fortsetzungen mit

$$||?||_j \text{ , } j = 1,...,J,$$

bezeichnet und ist $\overline{k}$ die Vervollständigung von k bezüglich |?|, so gilt

$$(2) \qquad \overline{k}\otimes_k K = \oplus_{j=1}^{J} K_j \text{ ,}$$

wobei K_j die Vervollständigung von K bezüglich $||?||_j$ ist. Dies gilt sowohl im algebraischen Sinne als auch im topologischen, wenn man die rechte Seite mit der Produkt-Topologie versieht.

Beweis. Als endliche separable Erweiterung von k hat K die Gestalt

$$K = k[T]/f\cdot k[T]$$

mit einem irreduziblen Polynom $f\in k[T]$. Sei

$$f = f_1\cdot...\cdot f_J$$

die Zerlegung von f in irreduzible Faktoren über $\overline{k}$. Man beachte, die f_j sind paarweise teilerfremd, f als separables Polynom keine mehrfachen Nullstellen besitzt. Deshalb gilt

$$\overline{k}\otimes_k K = \overline{k}[T]/f\cdot\overline{k}[T] = \oplus_{j=1}^{J} \overline{k}[T]/f_j\cdot\overline{k}[T] = \oplus_{j=1}^{J} K_j$$

mit endlichen separablen Körpererweiterungen

$$K_j = \overline{k}[T]/f_j\cdot\overline{k}[T]$$

von $\overline{k}$. Die Ring-Homomorphismen

$$\lambda_j: K \to \overline{k}\otimes_k K \to K_j$$

überführen das Einselement von K ins Einselement von K_j und sind deshalb von der Nullabbildung verschieden, also injektiv: wir können K als Teilkörper von K_j auffassen.

Wir bezeichnen die Forsetzung der Bewertung |?| von k auf die Vervollständigung $\overline{k}$ ebenfalls mit |?|. Als endlich Erweiterung von $\overline{k}$ besitzt K_j genau eine Fortsetzung $||?||_j^*$ von |?|. Mit Hilfe von λ_j erhalten wir eine Fortsetzung $||?||_j$ von |?| auf K, indem wir

$$||\beta||_j := |\lambda_j(\beta)| \text{ für } \beta\in K$$

setzen. Das Bild von K bei λ_j liegt dicht in K_j : jedes Element von K_j ist Bild eines Elements

$$\sum_i c_i\otimes\beta_i \in \overline{k}\otimes_k K \text{ mit } c_i\in\overline{k} \text{ , } \beta_i\in K$$

und jedes der c_i ist Limes einer Folge aus $k \subseteq K$. Damit ist K_j die Vervollständigung von K bezüglich der Fortsetzung $||?||_j$ von |?| auf K.

Es bleibt noch zu zeigen, die Bewertungen $||?||_j$ sind verschieden, und es sind die einzigen Fortsetzungen von |?|.

Sei ||?|| eine Bewertung von K, welche die Bewertung |?| von k fortsetzt. Dann läßt sich ||?|| zu einer stetigen Funktion auf $\overline{k}\otimes_k K$ fortsetzen, wie wir ebenfalls mit ||?|| bezeichnen. Aus Stetigkeitsgründen gilt insbesondere

$$||\alpha+\beta|| \le ||\alpha|| + ||\beta|| \text{ für } \alpha,\beta\in\overline{k}\otimes_k K$$

$$||\alpha\cdot\beta|| = ||\alpha||\cdot||\beta|| \text{ für } \alpha,\beta\in\overline{k}\otimes_k K$$

Betrachten wir die Einschränkung von ||?|| auf einen der Körper K_j. Falls

$$||\alpha|| \neq 0$$

gilt für ein $\alpha\in K_j$, so ist

$$||\alpha|| = ||\beta||\cdot||\beta\alpha^{-1}||$$

für jedes von Null verschiedene $\beta\in K_j$, also auch $||\beta|| \neq 0$. Also ist ||?|| entweder identisch Null auf K_j oder definiert dort eine Bewertung.

Außerdem kann ||?|| nicht auf zwei verschiedenen K_j eine Bewertung induzieren: wenn

$$\alpha\delta_j \in \oplus_{j=1}^{J} K_j$$

das Tupel mit der j-ten Koordinate α bezeichnet, dessen übrige Koordinaten 0 sind, so ist für j'≠j"

$$(\alpha' d_j,)\cdot(\alpha" d_{j"}) = 0$$

also

$$||\alpha'||\cdot||\alpha"|| = 0 \text{ für } \alpha'\in K_j, \text{ und } \alpha"\in K_{j"}.$$

Damit induziert ||?|| auf genau einem der K_j eine Bewertung, wobei diese Bewertung die Bewertung |?| von $\overline{k}$ fortsetzt. Damit gilt $||?|| = ||?||_j$ für genau ein j.

Wir haben noch zu zeigen, (2) gilt auch als Gleichheit topologischer Räume. Wir setzen

$$||(\beta_1,...,\beta_J)||_0 := \max\{||\beta_j||_j : j = 1,...,J\}$$

für jedes $(\beta_1,...,\beta_J)\in\oplus_{j=1}^{J} K_j$. Dann definiert $||?||_0$ eine Norm auf der rechten Seite von (2), aufgefaßt als Vektorraum über $\overline{k}$. Diese Norm induziert dort die Produkt-Topologie. Weil $\overline{k}$ vollständig ist, sind aber je zwei Normen äquivalent, d.h. $||?||_0$ induziert auf der linken Seite von (2) die Topologie des Tensorprodukts.
QED.

2.10.5 Folgerung

Sei mit den Bezeichnungen von 2.10.4

$$K = k(\beta)$$

und sei f∈k[T] das Minimal-Polynom von β über k. Weiter sei

$$f = f_1\cdot...\cdot f_J$$

die Zerlegung von f in irreduzible Faktoren über der Vervollständigung $\overline{k}$. Dann gilt (bis auf eine Permutation der K_j)

$$K_j = \overline{k}(\beta_j) \text{ mit } f_j(\beta_j) = 0.$$

2.11 Fortsetzung normalisierte Bewertungen

2.11.1 Die Situation

Sei k ein bewerteter Körper mit der Bewertung

$$|?|.$$

Wir betrachten drei Fälle.

1. Die Bewertung |?| ist diskret und nicht-archimedisch. Der Restekörper ist endlich.

2. Die Vervollständigung von k bezüglich |?| ist $\mathbb{R}$.
3. Die Vervollständigung von k bezüglich |?| ist $\mathbb{C}$.

Bemerkungen

(i) Auf Grund von 2.7.5 kann man diese drei Fälle zu der Bedingung zusammefassen, daß die Vervollständigung $\overline{k}$ von k bezüglich |?| lokal kompakt ist.[60]

(ii) Im Fall 1 haben wir bereits den Begriff der normalisierten Bewertung definiert (vgl. 2.7.7 und 2.7.8 Bemerkung (i)). Im zweiten Fall werden wir die Bewertung normalisiert nennen, wenn sie gleich dem gewöhnlichen Absolutbetrag ist und im dritten Fall, wenn sie gleich dem Quadrat des gewöhnlichen Absolutbetrags ist.

(iii) In allen drei Fällen ist die Bewertung genau dann normalisiert, wenn die Abbildung

$$\overline{k}^+ \to \overline{k}^+,\ x \mapsto \alpha x,$$

für jedes $\alpha \in \overline{k}^+$ der additiven Gruppe von $\overline{k}$ das Haarsche Maß von $\overline{k}^+$ mit dem Faktor

$$|\alpha|$$

multipliziert (vgl. 2.7.8 Bemerkung (i)). Dies charakterisiert die normalisierte Bewertung unter allen zu ihr äquivalenten Bewertungen.

2.11.2 Lemma 11.1: Normalisierte Fortsetzung einer Bewertung

Seien k ein bewerteter lokal kompakter vollständiger Körper, |?| dessen normalisierte Bewertung und K ein Erweiterung des Grades

$$N := [K:k] < \infty.$$

Dann ist die normalisierte Bewertung ||?|| von K, die äquivalent ist zur eindeutig bestimmten Fortsetzung von |?| auf K durch die folgende Formel gegeben.

$$||\alpha|| = |N_{K/k}(\alpha)| \text{ für } \alpha \in K.$$

Beweis. Nach 2.10.2 gilt

(1) $$||\alpha|| = |N_{K/k}(\alpha)|^c,\ \alpha \in K,$$

mit einer reellen Zahl

$$c > 0.$$

Es reicht zu zeigen,

$$c = 1.$$

Das ist trivial in den Fällen 2 und 2 von 2.11.1 und folgt aus den Struktursätzen des ersten Kapitels im Fall 1. Man argumentiert wie folgt. Sei

$$\omega_1,...,\omega_N \in K$$

eine Vektorraumbasis von K über k. Dann ist die Abbildung

$$K^+ \to (k^+)^N,\ \sum_{i=1}^{N} \xi_i\omega_i \mapsto (\xi_1,...,\xi_N),$$

ein Isomorphismus von additiven Gruppen. Wenn man im Raum rechts die Topologie des direkten Produktes einführt, ist diese Abbildung außerdem ein Homöomorphismus[61]. Insbesondere stimmen die Haarschen Maße von K^+ und $(k^+)^N$ bis auf eine multiplikative Konstante überein. Für $b \in k$ entspricht die Abbildung

$$K \to K,\ x \mapsto bx,$$

beim obigen Isomorphismus gerade der Abbildung

---

[60] Nach 2.3.5 ist jede archimedisch bewertete Körper k ein Teilkörper von $\mathbb{C}$. Wegen $\mathbb{Q} \subseteq k \subseteq \mathbb{C}$ folgt $\mathbb{R} \subseteq \overline{k} \subseteq \mathbb{C}$.

[61] Wegen 2.8.3.

$$(k^+)^N \to (k^+)^N, (\xi_1,...,\xi_N) \mapsto (b\xi_1,...,b\xi_N).$$

Da die Bewertung |?| von k normalisiert sein soll, multipliziert diese Abbildung das Haarsche Maß von $(k^+)^N$ mit dem Faktor $|b|^N$. Dasselbe muß damit auch für das Haaresche Maß von K^+ gelten. Also gilt

$$||b|| = |b|^N \text{ für jedes } b \in k.$$

Wegen $N_{K/k}(b) = b^N$ erhalten wir damit durch Einsetzen in (1)

$$|b|^N = ||b|| = |N_{K/k}(b)|^c = |b^N|^c \text{ für jedes } b \in k.$$

Damit ist aber c = 1.
QED.
Die nachfolgende Aussage ist ohne die Voraussetzung der Vollständigkeit richtig.

2.11.3 Theorem 11.1: Relative Produktformel für endliche Erweiterungen

Seien k ein bewerteter Körper mit lokal kompakter Vervollständigung, |?| dessen normalisierte Bewertung und K eine endliche separable[62] Erweiterung von k. Dann gilt

$$\prod_{j=1}^{J} ||\alpha||_j = |N_{K/k}(\alpha)| \text{ für jedes } \alpha \in K.$$

Dabei seien $||?||_j$ die normalisierten Bewertungen, die äquivalent sind zu den Fortsetzungen von |?| auf K.
Beweis. Sei $\overline{k}$ die Vervollständigung von k und

$$\overline{k} \otimes_k K = \oplus_{j=1}^{J} K_j$$

die Zerlegung von 2.10.4, d.h. die K_j seien die Vervollständigungen von K bezüglich der Bewertungen $||?||_j$. Nach 2.9.4 ist dann

$$N_{K/k}(\alpha) = \prod_{j=1}^{J} N_{K_j/\overline{k}}(\alpha)$$

für jedes $\alpha \in K$. Nach 2.11.2 ist dann aber

$$|N_{K/k}(\alpha)| = \prod_{j=1}^{J} |N_{K_j/\overline{k}}(\alpha)| = \prod_{j=1}^{J} ||\alpha||_j .$$

Wir haben dabei die stetigen Fortsetzungen der Bewertungen $||?||_j$ auf die Vervollständigungen K_j ebenfalls mit $||?||_j$ bezeichnet.
QED.

2.12 Globale Körper

2.12.1 Definition: globaler Körper

Ein globaler Körper ist ein Körper k, welcher entweder eine endliche Erweiterung des Körpers $\mathbb{Q}$ ist oder eine endliche separable Erweiterung eines Körpers der Gestalt $\mathbb{F}(t)$ mit einem endlichen Körper $\mathbb{F}$ und einem Element t, welches transzendent ist über $\mathbb{F}$.
Bemerkung

---

[62] "separabel" fehlt im Original. Die Verwendung der Zerlegung $\overline{k} \otimes_k K = \oplus_{j=1}^{J} K_j$, wobei die K_j Körper sind, weist jedoch darauf hin, daß die Separabilität der Erweiterung angenommen wird.

In unserer Darlegung konzentrieren wir uns auf den Fall der Erweiterungen von $\mathbb{Q}$ (des Falls der algebraischen Zahlkörper) und überlassen den Fall der Erweiterungen des Körpers $\mathbb{F}(t)$ (den Funktionenkörperfall) dem Leser.

2.12.2 Lemma 12.1

Seien k ein globaler Körper und

$$\alpha \in k-\{0\}$$

ein Element. Dann gibt es nur endlich viele paarweise nicht-äquivalente Bewertungen |?| von k mit

$$|\alpha| > 1.$$

Beweis. Wir wissen dies bereits in den Fällen

$$k = \mathbb{Q} \text{ und } k = \mathbb{F}_q(t)^{63}$$

gilt die Behauptung. Sei jetzt k ein endliche Erweiterung von $\mathbb{Q}$. Dann gibt es rationale Zahlen $a_1, \ldots, a_n$ mit

$$\alpha^n + a_1\alpha^{n-1} + \ldots + a_n = 0.$$

Ist die Bewertung |?| nicht-archimedisch, so folgt

$$|\alpha^n| = |- a_1\alpha^{n-1} - \ldots - a_n| \leq \max\{1, |\alpha|^{n-1}\} \cdot \max\{|a_1|, \ldots, |a_n|\},$$

also

$$|\alpha| \leq \max\{1, |a_1|, \ldots, |a_n|\}.$$

Die rechte Seite dieser Ungleichung ist nur für endlich viele Bewertungen |?| von $\mathbb{Q}$ größer als 1. Da es nur endlich viele archimedische Bewertungen von k gibt (Satz von Gelfand-Tornheim, 2.3.5) und nur endlich viele Fortsetzungen einer nicht-archimedischen Bewertung von $\mathbb{Q}$ auf k, folgt damit die Behauptung für den Körper k aus der Behauptung für $\mathbb{Q}$.
QED.

2.12.3 Die Bewertungen eines globalen Körpers

Alle Bewertungen eines globalen Körpers k besitzen die in 2.11 beschriebene Gestalt (da dies für $\mathbb{Q}$ und $\mathbb{F}_q((t))$ der Fall ist). Man kann also von normalisierten Bewertungen von k sprechen.

2.12.4 Theorem 12.1: die Produkt-Formel für globale Körper

Seien k ein globaler Körper,

$$\alpha \in k - \{0\}$$

ein Element und durchlaufe

$$|?|_v$$

die normalisierten Bewertungen des Körpers k. Dann gilt

$$|\alpha|_v = 1$$

für fast alle v (d.h. für alle mit eventuell endlich vielen Ausnahmen) und

---

[63] Im Fall $k = \mathbb{Q}$ folgt dies aus dem Satz von Ostrowskij 2.3.4 und der Tatsache, daß in der rationale Primfaktor-Zerlegung von α nur endlich viele Primzahlen vorkommen. Im Fall $k = \mathbb{F}_q(t)$ beachte man zunächst, daß die Einschränkung der Bewertung auf den endlichen Körper $\mathbb{F}_q$ trivial ist (vgl. 1.1.7 Bemerkung (iii)). Nach der Bemerkung von 2.3.6 sind dann die einzigen Bewertungen von k die zu den irreduziblen Polynomen über $\mathbb{F}_q$ und die an der unendlichen Primstelle. Die Behauptung folgt jetzt aus der Tatsache, daß in der Primfaktor-Zerleung von α nur endlich viele Primpolynome vorkommen.

$$\prod_v |\alpha|_v = 1.$$

Bemerkung
Später geben wir einen weniger verwickelten Beweis dieser Aussage.
Beweis. Nach 2.12.2 gilt

$$|\alpha|_v \leq 1$$

für fast alle v und analog

$$|\alpha^{-1}|_v \leq 1.$$

Zusammen ist also $|\alpha|_v = 1$ für fast alle v.

Durchlaufe V alle normalisierten Bewertungen des Teilkörpers $F = \mathbb{Q}$ bzw. $\mathbb{F}_q(t)$ von k. Wir schreiben

$$v \mid V,$$

wenn die Einschränkung der Bewertung v äquivalent ist zu V. Dann gilt

$$\prod_v |\alpha|_v = \prod_V (\prod_{v|V} |\alpha|_v) = \prod_V |N_{k/F}|_V$$

(wegen des letzten Gleichheitszeichen, siehe 2.11.3). Damit ist der Beweis des Theorem auf den Fall k = F reduziert. Sei

$$\alpha = e \cdot \prod_p p^{\alpha_p} \in F$$

die Primfaktor-Zerlegung von $\alpha \in F$ mit einer Einheit $e \in F$ (d.h. $e = \pm 1$ im Fall $F = \mathbb{Q}$ und $e \in \mathbb{F}_q$ im Fall $F = \mathbb{F}_q(t)$). Dabei durchläuft p die Primzahlen im Fall $F = \mathbb{Q}$ und die irrreduziblen Polynome über $\mathbb{F}_q$ im Fall $F = \mathbb{F}_q(t)$. Es gilt

$$|\alpha|_p = p^{-\alpha_p} \text{ bzw. } |\alpha|_p = c^{-\alpha_p \deg p}$$

und

$$|\alpha|_\infty = \prod_p p^{\alpha_p} \text{ bzw. } |\alpha|_\infty = c^{\deg \alpha} = c^{\sum_p \alpha_p \deg p}$$

(vgl. 2.3.6 für den Fall $F = \mathbb{F}_q(t)$, $c = 1/\#\mathbb{F}_q$, $c^{\deg p} = 1/\#\mathbb{F}_q[T]/(p)$). Zusammen erhalten wir die Behauptung.
QED.

2.12.5 Bezeichnungen
Seien k ein globaler Körper und K/k eine endliche separable Erweiterung. Dann gilt für jede Bewertung v von k,

$$k_v \otimes_k K = K_1 \oplus \ldots \oplus K_J .$$

Dabei bezeichne

$$k_v$$

die Vervollständigung von k bezüglich der Bewertung v und

$$K_1, \ldots, K_J$$

seien die Vervollständigungen von K bezüglich der Fortsetzungen

$$V_1, \ldots, V_J$$

von v auf K (vgl. 2.10). Die Anzahl

$$J = J(v)$$

dieser Fortsetzungen hängt von v ab. Wir werden später das nachfolgende Lemma benötigen.

2.12.6 Lemma 12.2:
Mit den Bezeichnungen von 2.12.5 sei

$$\omega_1,...,\omega_N$$

eine k-Vektorraumbasis von K. Dann gilt

(1) $$\omega_1\mathcal{O}\oplus...\oplus\omega_N\mathcal{O} = \mathcal{O}_1\oplus...\oplus\mathcal{O}_J$$

für fast alle normalisierten Bewertungen v des Körpers k. Dabei sei

$$N = [K:k],$$

und

$$\mathcal{O} = \mathcal{O}_v$$

der Ring der ganzen Elemente von k bezüglich der Bewertung v und

$$\mathcal{O}_j = \mathcal{O}_{V_j}$$

der Ring der ganzen Elemente von K bezüglich der Bewertung V_j. Wir identifizieren hier jedes Element $\alpha\in K$ mit dessen natürlichem Bild in $k_v\otimes_k K$.

Beweis. Die linke Seite von (1) ist in der rechten enthalten, vorausgesetzt es gilt

(2) $$|\omega_n|_{V_j} \le 1 \text{ für } n = 1,...,N \text{ und } j = 1,...,J.$$[64]

Die Bedingung $|\alpha|_V$ ist für fast alle V erfüllt (nach 2.12.2). Da über jedem v nur endlich viele Bewertungen V von K liegen, gilt damit (2) für fast alle v und in (1) gilt zumindest "$\subseteq$" für fast alle v.

Wir haben die umgekehrt Inklusion für fast alle v zu beweisen. Dazu betrachten wir die Diskriminante

$$D(\gamma_1,...,\gamma_N) := \det\left(\mathrm{Tr}_{K/k}(\gamma_i\gamma_j)\right)_{i,j=1,...,N} \text{ für } \gamma_1,...,\gamma_N\in K.$$

Nach 2.9.4 ist

$$\mathrm{Tr}_{K/k}(\gamma_i\gamma_j) = \sum_{j=1}^{J} \mathrm{Tr}_{K_j/k_v}(\gamma_i\gamma_j).$$

Falls die γ_i in der rechten Seite von (1) liegen, gilt

$$\mathrm{Tr}_{K_j/k_v}(\gamma_i\gamma_j) \in k_v\cap K\cap\mathcal{O}_j =^{65} k\cap\mathcal{O}_j =^{66} \mathcal{O}_v,$$

---

[64] Jedenfalls hat man natürliche Abbildungen

$$\sum_{n=1}^{N}\omega_n\mathcal{O} \hookrightarrow \sum_{n=1}^{N}\omega_n k = K \hookrightarrow k_v\otimes_k K \to K_j$$

wobei die Zusammensetzung der letzten beiden ebenfalls injektiv ist. Den Ring $\mathcal{O}_j$ kann man wahlweise als Teilring von K und von K_j ansehen. Er besteht aus den Elementen von K mit $|?|_{V_j} \le 1$.

[65] Die ω_j bilden auch eine Basis der Vervollständigung $k_v\otimes K$ des k-Vektorraumes K bezüglich einer durch v definierten Norm. Also ist (wegen $\omega_1 = 1$)

$$k_v\cap K = \omega_1 k_v \cap \sum_{j=1}^{N}\omega_j k = \omega_1 k_v\cap k = \omega_1 k = k$$

Zusammen ergibt sich also

(3) $D(\gamma_1,...,\gamma_N) \in \mathcal{O}_v$ für γ_j aus der rechten Seite von (1).

Sei jetzt α aus der rechten Seite von (1). Wir schreiben α in der Gestalt

$$\alpha = \sum_{n=1}^{N} a_n \omega_n \text{ mit } a_n \in k_v.$$

Wir haben zu zeigen

$$a_n \in \mathcal{O}_v$$

für fast alle v. Für jedes n gilt

$$D(\omega_1,...,\omega_{n-1},\alpha,\omega_{n+1},...,\omega_N) = a_n^2 \cdot d$$

mit

$$d := D(\omega_1,...,\omega_N).$$

Wie wir im ersten Teil des Beweises gesehen haben, liegen die ω_j für fast alle v in der rechten Setie von (1). Nach (3) gilt deshalb

(4) $d \cdot a_n^2 \in \mathcal{O}_v$ für fast alle v.

Weil die Erweiterung K/k separabel ist, gilt $d \neq 0$ (vgl. B9). Deshalb ist

$$|d|_v = 1$$

für fast alle v. Da $\mathcal{O}_v$ ein Bewertungsring ist, folgt mit (4) also auch $a_n \in \mathcal{O}_v$ für fast alle v.
QED.

2.12.7 Folgerung: Unverzweigtheit in fast allen Stellen

Seien k ein globaler Körper und K/k eine endliche separable Körpererweiterung. Dann ist fast jede Bewertung v von k unverzweigt in K.
Beweis. Nach 1.5.13 ist K/k in einer Stelle V über v unverzweigt, genau dann wenn die Diskriminante an dieser Stelle von einer Einheit erzeugt wird. Nach 1.3.12 wird die Diskriminante von

$$\det (Tr(\omega_i \omega_j))$$

erzeugt, wenn der Ganzheitsring von K an der betrachteteten Stelle über dem Ganzheitsring von k von der freien Basis $\{\omega_i\}$ erzeugt wird. Letzteres ist aber für jede Basis $\{\omega_i\}$ von K/k und fast alle Bewertungen v von k der Fall (nach 2.12.6). Die Bedingung für Unverzweigtheit über v lautet dann

$$|\det (Tr(\omega_i \omega_j))|_v = 1.$$

Diese Bedingung ist für fast alle v erfüllt (nach 2.12.4), weil $\det (Tr(\omega_i \omega_j)) \neq 0$ gilt für separable Erweiterungen K/k (nach B9).
QED.

2.13 Das eingeschränkte topologische Produkt

Wir beschreiben jetzt einen topologischen Mechanismus, den wir später brauchen werden.

2.13.1 Definition: eingeschränktes topologisches Produkt

Seien

$$(\Omega_\lambda)_{\lambda \in \Lambda}$$

---

[66] die V_j sind Fortsetzungen von v.

eine Familie von topologischen Räumen und

$$\Theta_\lambda \subseteq \Omega_\lambda$$

für fast jedes $\lambda\in\Lambda$ eine offene Teilmenge. Wir setzen

$$\Omega := \{(\alpha_\lambda)_{\lambda\in\Lambda} \mid \alpha_\lambda\in\Omega_\lambda \text{ für jedes } \lambda\in\Lambda \text{ und } \alpha_\lambda\in\Theta_\lambda \text{ für fast jedes } \lambda\}$$

Wir führen auf Ω eine Topologie ein, indem wir als Topologie-Basis die Mengen der folgenden Gestalt verwenden.

$$\prod_{\lambda\in\Lambda} \Gamma_\lambda$$

mit $\Gamma_\lambda \subseteq \Omega_\lambda$ offen für jedes $\lambda\in\Lambda$ und $\Theta_\lambda \subseteq \Gamma_\lambda$ für fast jedes λ. Der Raum Ω mit der so definierten Topologie heißt eingeschränktes topologisches Produkt der Ω_λ bezüglich der offenen Teilmengen $\Theta_\lambda \subseteq \Omega_\lambda$.

2.13.2 Folgerung: eine offene Überdeckung durch Mengen mit der Produkt-Topologie

Sei Ω das eingeschränkte topologische Produkt der Räume

$$\Omega_\lambda\ ,\ \lambda\in\Lambda,$$

bezüglich der offenen Teilmengen $\Theta_\lambda \subseteq \Omega_\lambda$ und sei

$$S \subseteq \Lambda$$

eine endliche Teilmenge. Wir setzen

$$\Omega_S := \{(\alpha_\lambda)_{\lambda\in\Lambda}\in\Omega \mid \alpha_\lambda\in\Theta_\lambda \text{ für } \lambda\notin S\} = \prod_{\lambda\in S} \Omega_\lambda \prod_{\lambda\notin S} \Theta_\lambda .$$

Dann ist Ω_S eine offene Teilmenge von Ω und die induzierte Topologie des Unterraums Ω_S von Ω ist gleich der Produkt-Topologie.

Beweis: trivial.
QED.

2.13.3 Lemma 13.1: Unabhängigkeit von den offenen Unterräumen

Sei

$$(\Omega_\lambda)_{\lambda\in\Lambda}$$

eine Familie von topologischen Räumen. Für fast jedes $\lambda\in\Lambda$ sei ein offener Unterraum

$$\Theta_\lambda \subseteq \Omega_\lambda$$

gegeben und ebenfalls für fast jedes λ ein weiterer offener Unterraum

$$\Theta'_\lambda \subseteq \Omega_\lambda .$$

Außerdem gelte für fast jedes $\lambda\in\Lambda$

$$\Theta_\lambda = \Theta'_\lambda .$$

Dann ist das eingeschränkte topologische Produkt der Ω_λ bezüglich der Θ_λ gleich dem eingeschränkten topologischen Produkt der Ω_λ bezüglich der Θ'_λ.

Beweis. trivial.
QED.

2.13.4 Lemma 13.2: Kriterium für lokale Kompaktheit
Sei Ω das eingeschränkte topologische Produkt der Räume Ω_λ, $\lambda\in\Lambda$, bezüglich der offenen Unterräume $\Theta_\lambda \subseteq \Omega_\lambda$. Falls die Räume Ω_λ lokal kompakt und die Unterräume Θ_λ kompakt sind, so ist Ω lokal kompakt.
Beweis. Die Mengen Ω_S von Folgerung 3.13.2 sind offen in Ω und trivialerweise lokal kompakt. Weil Ω die Vereinigung aller dieser Ω_S ist, folgt die Behauptung.
QED.

2.13.5 Definition: ein Maß auf dem eingeschränkten topologischen Produkt
Sei Ω das eingeschränkte topologische Produkt der Räume Ω_λ, $\lambda\in\Lambda$, bezüglich der offenen Unterräume $\Theta_\lambda \subseteq \Omega_\lambda$. Für jedes $\lambda\in\Lambda$ sei auf Ω_λ ein Maß μ_λ definiert und es gelte

$$\mu_\lambda(\Theta_\lambda) = 1,$$

für jedes $\lambda\in\Lambda$, für welches Θ_λ definiert ist. Wir definieren das zugehörige Produktmaß auf Ω , indem wir als Basis meßbarer Mengen die Produkte

$$\prod_{\lambda\in\Lambda} M_\lambda$$

verwenden mit $M_\lambda \subseteq \Theta_\lambda$ von endlichem μ_λ-Maß für jedes $\lambda\in\Lambda$ und $M_\lambda = \Theta_\lambda$ für fast jedes λ, wobei

$$\mu\left(\prod_{\lambda\in\Lambda} M_\lambda\right) := \prod_{\lambda\in\Lambda} \mu_\lambda(M_\lambda)$$

sei.

2.13.6 Folgerung
Die Einschränkung des Maßes μ von Definition 2.13.5 auf eine Menge Ω_S von Folgerung 2.13.2 ist gleich dem gewöhnlichen Produkt-Maß.

2.14 Der Ring der Adele (oder der Ring der Bewertungsvektoren)

2.14.1 Definition: Adele-Ring eines globalen Körpers
Sei

$$k$$

ein globaler Körper. Für jede normalisierte Bewertung

$$|?|_v$$

von k bezeichnen wir mit

$$k_v$$

die Vervollständigung von k bezüglich dieser Bewertung. Ist diese Bewertung nicht-archimedisch, so bezeichne

$$\mathcal{O}_v := \{x\in k_v : |x|_v \le 1\}$$

den Ring der ganzen Elemente von k_v. Der Adele-Ring des Körpers k wird mit

$$V_k$$

bezeichnet und ist definiert als das eingeschränkte topologische Produkt der Ringe k_v bezüglich der Teilringe $\mathcal{O}_v$ mit der koordinatenweise definierten Ringstruktur, d.h. Summe und Produkt von zwei Elementen des Adele-Rings sind wie folgt definiert.

$$(\alpha_v) + (\beta_v) := (\alpha_v + \beta_v)$$
$$(\alpha_v)\cdot(\beta_v) := (\alpha_v \beta_v).$$

Die Elemente von V_k heißt Adele von k.

Bemerkungen

(i) Die obigen Definitionen von Addition und Multiplikation in V_k sind korrekt, d.h. Produkt und Summe von zwei Adelen sind wieder Adele.

(ii) Addition und Multiplikation in V_k sind stetig in der V_k-Topologie, d.h. V_k ist ein topologischer Ring.

(iii) V_k ist lokal kompakt, da die $\mathcal{O}_v$ kompakt sind und die k_v lokal kompakt (vgl. 2.13.4 und 2.7.3).

(iv) Es gibt eine natürliche Abbildung

$$k \to V_k$$

des Körpers k in den Adele-Ring, welche jedem Element $\alpha \in k$ das Adel zuordnet, dessen sämtliche Koordinaten gleich α sind. Letzteres ist tatsächlich ein Adel, weil

$$\alpha \in \mathcal{O}_v$$

gilt für fast alle v (vgl. 2.14.4). Diese Abbildung ist eine Einbettung, da die natürliche Abbildung

$$k \to k_v$$

des Körpers k in dessen v-adische Vervollständigung für jedes v eine Einbettung ist.

2.14.2 Definition: Hauptadele

Seien k ein globaler Körper und

$$k \to V_k$$

die natürliche Einbettung von k in den Adele-Ring (vgl. Bemerkung 2.14.1(iv)). Das Bild von k bei dieser Einbettung heißt Ring der Hauptadele. Die Elemente des letzteren heißen Hauptadele von k.

Vereinbarung

Wir werden im folgenden bei Bedarf die Elemente von k mit den zugehörigen Hauptadelen identifizieren und k als Teilring von V_k ansehen.

2.14.3 Lemma 14.1: Verhalten des Adele-Rings bei separablen Erweiterungen

Seien k ein globaler Körper und K/k eine endliche separable Erweiterung. Dann gibt es eine natürliche Abbildung

$$V_k \otimes_k K \to V_K$$

welche im algebraischen und im topologischen Sinne ein Isomorphismus ist. Dabei wird

$$K = k \otimes_k K \subseteq V_k \otimes_k K$$

identisch auf $K \subseteq V_K$ abgebildet.

Beweis.
QED.

2.15 Der starke Approximationssatz

2.16 Die Gruppe der Idele

2.17 Idele und Divisoren

2.18 Einheiten

2.19 Einbettung und Normabbildungen für Adele, Idele und Ideale

A Anhang:Normen und Spuren

A.1 Der Endomorphismenring

Seien R ein kommutativer Ring mit Eins und M ein freier R-Modul mit dem linear unabhängigen Erzeugendensystem $\omega_1,...,\omega_n$. Die Menge der R-linearen Endomorphismen von M, d.h. der R-linearen Abbildungen M→M bezeichnen wir mit

$$\mathrm{End}_R(M).$$

Dies ist ein im allgemeinen nicht mehr kommutativer Ring, welcher isomorph ist zum Ring der n×n-Matrizen

$$R^{n\times n}$$

mit Einträgen aus R, und zwar gehört zu jeder Basis von M über R ein Isomorphismus.

$$R^{n\times n} \to \mathrm{End}_R(M),\ (r_{ij}) \mapsto (\omega_i \mapsto \sum_{j=1}^{n} r_{ij}\omega_j).$$

Der Ring R läßt sich als Teilring von $\mathrm{End}_R(M)$ auffassen vermittels der Abbildung

$$R \to \mathrm{End}_R(M),\ r \mapsto (m \mapsto rm).$$

A.2 Definition von Spur und Norm

Für jedes $A\in\mathrm{End}_R(M)$ betrachten wir das charakteristische Polynom von A,

$$\chi(A, x) := \det(A - x\cdot Id).$$

Wir schreiben

$$\chi(A, -x) = x^n + \mathrm{Tr}(A)\cdot x^{n-1} + ... + N(A).$$

Die Koeffizienten Tr(A) und N(A) heißen Spur bzw. von Norm von A.

A.3 Eigenschaften von Spur und Norm

(i) $N(AB) = N(A)N(B)$ für $A,B\in\mathrm{End}_R(M)$.

(ii) $\mathrm{Tr}(A+B) = \mathrm{Tr}(A) + \mathrm{Tr}(B)$ für $A,B\in\mathrm{End}_R(M)$.

(iii) $N(r) = r^n$ für $r\in R$.

(iv) $\mathrm{Tr}(r) = n\cdot r$ für $r\in R$.

(v) $\mathrm{Tr}(rA) = r\cdot\mathrm{Tr}(A)$ für $r\in R$ und $A\in\mathrm{End}_R(M)$.

Beweis. Zu (i). $N(AB) = \det(A\circ B) = \det(A)\cdot\det(B) = N(A)\cdot N(B)$.
Zu (ii) und (v). Sei (a_{ij}) die Matrix von A bezüglich der Basis $\omega_1, ..., \omega_n$. Dann gilt

$$\mathrm{Tr}(A) = a_{11}+...+a_{nn}.$$

Dieser Ausdruck ist offensichtlich R-linear in A.
Zu (iii) und (iv). Mit den Bezeichnungen von (ii) erhalten wir im Fall $A=r\in R$ für die zugehörigen Matrix

$$a_{ij} = r \cdot \delta_{ij},$$

also $Tr(r) = n \cdot r$ und $N(r) = r^n$.
QED.

A.4 Satz von Hamilton-Cayley
$\chi(A,A) = 0$ für jedes $A \in End_R(M)$.

Beweis. Sei (a_{ij}) die Matrix von A bezüglich der Basis $\omega_1, ..., \omega_n$. Dann gilt

$$A\omega_i = \sum_{j=1}^{n} a_{ij}\omega_j$$

also

$$(*) \qquad 0 = \sum_{j=1}^{n} (\delta_{ij}A - a_{ij})\omega_j$$

Dabei fassen wir die Ausdrücke $\delta_{ij}A - a_{ij}$ als Elemente des Rings $End_R(M)$ auf.
Genauer liegen diese Ausdrücke sogar in dem kommutativen Teilring

$$R[A] \subseteq End_R(M).$$

Wir betrachten die Matrix der $b_{ij} = \delta_{ij}A - a_{ij}$ im Ring der n×n-Matrizen über R[A]. Bezeichne B_{ij} die adjungierte Unterdeterminante von (b_{ij}) zur Position (i,j). Wir multiplizieren die i-te Gleichung von (*) mit B_{ij_0} und bilden die Summe der entstehenden Gleichungen. Wegen

$$\sum_{i=1}^{n} B_{ij_0} b_{ij} = \begin{cases} \det(b_{ij}) \text{ für } j=j_0 \\ 0 \quad \text{sonst} \end{cases}$$

erhalten wir aus (*):

$$0 = \det(\delta_{ij}A - a_{ij})\omega_{j_0}.$$

Da j_0 beliebig war, ist die Multplikation mit $\det(\delta_{ij}A - a_{ij})$ die Nullabbildung von $End_R(M)$, mit anderen Worten, es gilt $0 = \det(\delta_{ij}A - a_{ij}) = \chi(A,A)$.

QED.

A.5 Lemma
Sei t ein über dem Ring R transzendentes Element. Dann definieren die n×n-Matrizen mit Einträgen aus R[t] lineare Endomorphismen von $M \otimes_R R[t]$, so daß die für solche Endomorphismen die Norm definiert ist. Es gilt

$$(-1)^n \cdot N(t-A) = \chi(A,t)$$

für jedes $A \in End_R(M)$.

Beweis. Die Elemente $\omega_1, ..., \omega_n$ bilden eine Basis von $M \otimes_R R[t]$ über R[t]. Es gilt

$$A\omega_i = \sum_{j=1}^{n} a_{ij}\omega_j$$

also

$$(t-A)\omega_i = \sum_{j=1}^{n} (\delta_{ij}t - a_{ij})\omega_j$$

also

$$N(t\text{-}A) = \det(\delta_{ij}t\text{-}a_{ij}) = (\text{-}1)^n\chi(A,t).$$

QED.

Bemerkung

Die eben bewiesene Identität bleibt gültig, wenn man für t ein Element von R einsetzt.

A.6 Lemma

Seien $A_1,...,A_\ell \in \mathrm{End}_R(M)$ und t ein über R transzendentes Element. Dann gilt

$$N(t^\ell + A_1 t^\ell + ... + A_\ell) = t^{n\ell} + r_1 \cdot t^{n\ell-1} + ... + r_{n\ell}$$

mit gewissen Elementen $r_i \in R$. Insbesondere ist

$$r_1 \in \mathrm{Tr}(A_1) \text{ und } r_{n\ell} = N(A_\ell).$$

Beweis. Die Beweisidee ist dieselbe wie im vorangehenden Lemma. Für $\nu=1,...,\ell$ haben wir Identitäten

$$A_\nu \omega_i = \sum_{j=1}^{n} a_{\nu ij}\omega_j .$$

Also ist

$$(t^\ell + A_1 t^\ell + ... + A_\ell)\omega_i = \sum_{j=1}^{n} (\delta_{ij}t^\ell + a_{1ij}t^\ell + ... + a_{\ell ij})\omega_j ,$$

also

$$N(t^\ell + A_1 t^\ell + ... + A_\ell) = \det(\delta_{ij}t^\ell + a_{1ij}t^\ell + ... + a_{\ell ij}).$$

Aus der letzten Identität ergibt sich die Behauptung.

QED.

A.7 Komposition von Spuren und von Normen

Seien R und S kommutative Ringe mit Eins und M ein freier S-Modul endlichen Rangs. Weiter sei $R \subseteq S$ und S sei als R-Modul ebenfalls frei und vom endlichem Rang. Für jedes $A \in \mathrm{End}_S(M) \subseteq \mathrm{End}_R(M)$ gilt dann

$$\mathrm{Tr}_{M/R}(A) = \mathrm{Tr}_{S/R}(\mathrm{Tr}_{M/S}(A))$$
$$N_{M/R}(A) = N_{S/R}(N_{M/S}(A))$$

Außerdem ist

$$\chi_R(A, t) = N_{S/R}(\chi_S(A, t))$$

wobei $\chi_R(A, t)$ und $\chi_S(A, t)$ die charakteristischen Polynome von A bezeichnen sollen, wobei man einmal A als Element von $\mathrm{End}_R(M)$ und einmal als Element von $\mathrm{End}_S(M)$ auffaßt.

Bemerkung

Die ersten beiden Identitäten besagen, daß folgende Diagramme kommutativ sind.

$$\begin{array}{ccc} \mathrm{End}_S(M) & \xrightarrow{\mathrm{Tr}_{M/S}} & S \\ || & & \downarrow \mathrm{Tr}_{S/R} \\ \mathrm{End}_S(M) & \xrightarrow{\mathrm{Tr}_{M/R}} & R \end{array} \qquad \begin{array}{ccc} \mathrm{End}_S(M) & \xrightarrow{N_{M/S}} & S \\ || & & \downarrow N_{S/R} \\ \mathrm{End}_S(M) & \xrightarrow{N_{M/R}} & R \end{array}$$

Beweis von A.7. 1. Schritt. Beweis der Formel für die Norm.

Wir führen den Beweis durch Induktion nach der Anzahl der linear unabhängigen Erzeugenden des freien S-Moduls M. Im Fall eines Erzeugendensystems der Länge 1

gilt $M \cong S$, $Tr_{M/S} = N_{M/S} = Id$ und die Behauptung ist trivial. Sei jetzt $n>1$ und $\omega_1,...,\omega_n$ ein linear unabhängiges Erzeugendensystem von M über S. Für vorgegebenes $A \in End_S(M)$ schreiben wir

$$A\omega_i = \sum_{j=1}^{n} a_{ij}\omega_j \text{ mit } a_{ij} \in S.$$

Wir betrachten das Element $B \in End_S(M)$ mit

(1)
$$B\omega_1 := \omega_1 - \sum_{j=2}^{n} a_{1j}\omega_j$$
$$B\omega_i := a_{11}\omega_i \quad (\text{für } i>1)$$

Bei der Zusammensetzung C := BA werden die Basiselemente von M wie folgt abgebildet.

$$\omega_1 \mapsto \sum_{j=1}^{n} a_{1j}\omega_j \mapsto a_{11}(\omega_1 - \sum_{j=2}^{n} a_{1j}\omega_j) + \sum_{j=2}^{n} a_{1j}\, a_{11}\omega_j = a_{11}\omega_1$$

$$\omega_i \mapsto \sum_{j=1}^{n} a_{ij}\omega_j \mapsto a_{i1}(\omega_1 - \sum_{j=2}^{n} a_{1j}\omega_j) + \sum_{j=2}^{n} a_{ij}\, a_{11}\omega_j = a_{i1}\omega_1 + \sum_{j=2}^{n} c_{ij}\,\omega_j$$

mit $c_{ij} = a_{ij}\, a_{11} - a_{i1}\, a_{1j}$. Mit anderen Worten, es gilt

(2)
$$C\omega_1 := a_{11}\omega_1$$
$$C\omega_i := a_{i1}\omega_1 + \sum_{j=2}^{n} c_{ij}\,\omega_j \quad (\text{für } i>1)$$

Die Matrix dieser Abbildung hat in der ersten Zeile als einzigen eventuell von Null verschiedenen Eintrag das Element a_{11} in der ersten Position. Deshalb gilt nach dem Entwicklungssatz

$$N_{M/S}(C) = a_{11} N_{M'/S}(C').$$

Dabei sei $M' := S\omega_2 + ... S\omega_n$ und C' bezeichne die S-lineare Abbildung

$$C': M' \to M',\ \omega_i \mapsto \sum_{j=2}^{n} c_{ij}\,\omega_j .$$

Damit gilt

$$N_{S/R}(N_{M/S}(C)) = N_{S/R}(a_{11}) \cdot N_{S/R}(N_{M'/S}(C')).$$

Den Ausdruck ganz rechts können wir jetzt nach Induktionsvoraussetzung berechnen. Es folgt

(3)
$$N_{S/R}(N_{M/S}(C)) = N_{S/R}(a_{11}) \cdot N_{M'/R}(C').$$

Sei jetzt $s_1,...,s_m$ ein R-linearer unabhängiges Erzeugendensystem des R-Moduls S. Dann bilden die Produkte $s_i\omega_j$ ein lineare unabhängiges Erzeugendensystem des R-Moduls M und die Matrizen der Abbildungen B und C bezüglich der $s_i\omega_j$ lassen sich aus (1) und (2) gewinnen, indem man diese Identitäten auf alle möglichen Weisen mit einem s_i multipliziert. Da die Matrix von C über R nach (2) in der linken oberen Ecke die Matrix von $mult_{a_{11}}$ stehen hat und rechts von dieser Matrix lauter Nullen stehen, folgt nach dem Entwicklungssatz

$$N_{M/R}(C) = N_{S/R}(a_{11}) \cdot N_{M'/R}(C')$$

(4) $$N_{M/R}(C) = N_{S/R}(N_{M/S}(C)) \quad \text{(nach (3))}$$

Dies ist die gesuchte Formel für die Norm nur mit C = BA anstelle von A. Auf Grund der sehr speziellen Gestalt der Matrizen von B über R bzw. S (vgl. Formel (1)) erhalten wir ohne weiteres die entsprechende Formel für B,

$$N_{M/R}(B) = N_{S/R}(a_{11})^{n-1} = N_{S/R}(a_{11}^{n-1}) = N_{S/R}(N_{M/S}(B))$$

Da die Norm multiplikativ ist, ergibt sich daraus die Behauptung zumindest in dem Fall, daß $N_{S/R}(a_{11})$ eine Einheit ist. Im allgemeinen müssen wir einen etwas künstlich wirkenden Trick anwenden.

Sei t ein über S transzendentes Element (eine Unbestimmte). Wir bezeichnen mit A_t die Matrix, welche man aus A erhält, indem man das Element a_{11} durch $a_{11}+t$ ersetzt. Die obigen Betrachtungen sind dann natürlich auch für A_t anstelle von A gültig (mit S[t] anstelle von S). Identität (4) kann man dann in der folgenden Gestalt schreiben.

$$N_{S/R}(a_{11}+t)^{n-1}\, N_{M/R}(A_t) = N_{S/R}(a_{11}+t)^{n-1} \cdot N_{S/R}(N_{M/S}(A_t))$$

Dies ist eine Identität von Polynomen aus R[t]. Der höchst Koeffizient des Polynoms $N_{S/R}(a_{11}+t)$ ist Eins (z.B. nach Lemma A.5). Deshalb ist dieses Polynom in R[t] kein Nullteiler, d.h. es gilt

$$N_{M/R}(A_t) = N_{S/R}(N_{M/S}(A_t))$$

Wir setzen t=0 und erhalten die Behauptung des ersten Schritts.

2. Schritt. Beweis der beiden anderen Formeln.

Nach Lemma A.5 gilt

$$\chi_{M/S}(A,t) = (-1)^n \cdot N_{M/S}(t-A) \text{ mit } n := rk_S(M)$$

und analog

$$\chi_{M/R}(A,t) = (-1)^{nm} \cdot N_{M/R}(t-A) \text{ mit } m := rk_R(S).$$

Aus der eben bewiesenen Formel für die Norm ergibt sich damit

$$\chi_{M/R}(A,t) = (-1)^{nm} \cdot N_{M/R}(t-A)$$
$$= N_{M/R}(A-t)$$
$$= N_{S/R}(N_{M/S}(A-t)).$$

Die noch verbleibende Formel für die Spur ergibt sich jetzt aus Lemma A.6.

QED.

A.8 Der Fall einer endlichen Körpererweiterung

Seien K/k eine endliche Körpererweiterung und $\alpha \in K$ ein Element mit dem Minimalpolynom f(x) über k. Dann gilt

(i) $\deg f(x) \mid [K:k]$

(ii) $\chi(\alpha, x) = (-1)^n \cdot f(x)^{\ell}$ mit $\ell := \dfrac{[K:k]}{\deg f(x)}$.

(iii) $Tr_{K/k}(\alpha) = \ell \cdot (\alpha_1 + \ldots + \alpha_m)$

(iv) $N_{K/k}(\alpha) = (\alpha_1 \cdot \ldots \cdot \alpha_m)^{\ell}$

Dabei seien n = [K:k], m= deg f und $\alpha_1, \ldots, \alpha_m$ die (mit ihren Vielfachheiten gezählten) Nullstellen von f in irgendeiner Erweiterung von K.

Beweis. Betrachten wir zunächst den Fall K=k(α). Wegen $\chi(\alpha, \alpha)=0$ gilt $f|\chi$ und wegen [K:k] = deg f muß dann sogar $\chi(\alpha, x) = (-1)^n \cdot f(x)$, also

$$\chi(\alpha, -x) = (-1)^n \cdot f(-x) = (x+\alpha_1)\cdot\ldots\cdot(x+\alpha_m),$$

gelten. Daraus ergeben sich unmittelbar die Aussage des Satzes im Fall K=k(α) (d.h ℓ=1). Im allgemeinen Fall betrachten wie den Körperturm

$$k \subseteq k(\alpha) \subseteq K$$

und wenden A.7 an.
QED.

B Anhang:Separabilität

B.1 Die Zahl der Einbettungen eines Erweiterungskörpers

Seien K/k und L/k endliche Körpererweiterungen. Dann gibt es höchstens [K:k] Einbettungen

$$K \rightarrow L,$$

welche den Körper k elementsweise festlassen.
Beweis. Im Fall K=k(α) ist das trivial, da Nullstellen des Minimalpolynoms von α in Nullstellen des Minimalpolynoms übergehen müssen. Im allgemeinen Fall betrachtet man einen Körperturm

$$k=K_0 \subset K_1 \subset \ldots \subset K_j = K$$

aus einfachen Erweiterungen $K_i = K_{i-1}(\alpha_i)$ und führt den Beweis durch Induktion nach j.
QED.

B.2 Definition der Separabilität

Eine endliche Körpererweiterung K/k heißt separabel, wenn es eine endliche Erweiterung L/k gibt mit der Eigenschaft, daß die Zahl der verschiedenen Einbettungen

$$K \rightarrow L,$$

welche k elementeweise festlassen, gleich [K:k] ist.

B.3 Separabilität von Teilerweiterungen

Seien K/k und L/k endliche Körpererweiterungen. Dann besteht folgende Implikation.

$$L/k \text{ separabel} \Rightarrow K/k \text{ und } L/k \text{ separabel.}$$

Beweis. Nach B.1 gibt es höchstens [K:k] verschiedene Einbettungen

$$K \rightarrow M$$

in irgendeine endiche Erweiterung M/k. Nach demselben Lemma läßt sich jede von diesen Einbettungen auf höchstens [L:K] verschiedene Weisen fortsetzen zu einer Einbettung

$$L \rightarrow M.$$

Wenn man also insgesamt [L:k] = [L:K]·[K:k] Einbettungen L→M erhält, so muß in jedem Teilschritt bereits die maximal erreichbare Anzahl von Einbettungen möglich sein.
QED.

B.4 Separabilität und das Fehlen mehrfacher Nullstellen

Seien K/k eine endliche separable Erweiterung vom Grad n und

$$\sigma_i: K \rightarrow M$$

die n verschiedenen k-Einbettungen in einer (hinreichend großen) endlichen Erweiterung M/k. Weiter seien $\alpha \in K$ ein Element und $\alpha_1,\ldots,\alpha_m \in M$ die paarweise verschiedenen Nullstellen des Minimalpolynoms f(x) von α über k in M. Dann gilt

(i) $f(x) = (x-\alpha_1)\cdot\ldots\cdot(x-\alpha_m)$

(ii) $\{\alpha_1,...,\alpha_m\}=\{\sigma_1(\alpha),...,\sigma_m(\alpha)\}$, wobei in der Folge $\sigma_i(\alpha)$ jedes der α_j genau $\frac{n}{m}$ mal angenommen wird.

Beweis. Jede der Nullstellen α_j definiert eine k-Einbettung

$$k(\alpha) \to M.$$

Die Zahl dieser Einbettungen ist nach B.3 gleich $m = [k(\alpha):k] = \deg(f)$, d.h. es gilt (i). Jede dieser Einbettungen läßt sich auf $[K:k(\alpha)] = \frac{n}{m}$ verschiedene Weisen fortsetzen zu einem der σ_i. Also kommt jedes der α_j in $\frac{n}{m}$ - facher Weise in der Gestalt $\sigma_i(\alpha)$ vor.

QED.

B.5 Die Spurabbildung

Seien K/k eine endliche separable Erweiterung vom Grad n und

$$\sigma_i: K \to M$$

die n verschiedenen k-Einbettungen in eine endliche Erweiterung M/k. Dann gilt

$$Tr_{K/k}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$$

für jedes $\alpha \in K$.

Beweis. Dies folgt aus B.4 und A.8.

QED.

B.6 Transitivität

Seien K/k und L/K endliche separable Körpererweiterungen. Dann ist auch L/k separabel.

Beweis. Nach Voraussetzung gibt es paarweise verschiedene k-Einbettungen

$$\sigma_i:K \to U,\ i=1,...,[K:k]$$

und paarweise verschiedene K-Einbettungen

$$\tau_i:L \to V,\ i=1,...,[L:K].$$

Durch geeignetes Vergrößern von U können wir erreichen, daß die σ_i sich zu k-Einbettungen

$$\sigma_i:L \to U$$

fortsetzen lassen. Ohne Beschränkung der Allgemeinheit können wir annehmen $L \subseteq V$ (man identifiziere L mit seinem Bild bei einem der τ_i). Wir setzen die σ_i zu k-Einbettungen

$$\sigma_i:V \to U$$

fort (bei eventueller Vergrößerung von U). Nach Konstruktion sind die Einschränkungen der $\sigma_i\tau_j$ auf L paarweise verschieden:

$$\begin{aligned} \sigma_i\tau_j = \sigma_{i'}\tau_{j'} \text{ auf } L \quad &\Rightarrow \sigma_i = \sigma_{i'} \text{ auf K (da die } \tau \text{ K-Einbettungen sind)} \\ &\Rightarrow i=i' \\ &\Rightarrow \tau_j = \tau_{j'} \text{ auf L (da die } \sigma \text{ injektiv sind)} \\ &\Rightarrow j=j'. \end{aligned}$$

Die Anzahl der $\sigma_i\tau_j|_L$ ist gleich $[L:K]\cdot[K:k] = [L:k]$

QED.

B.7 Separabilität in der Charakteristik Null

Jede endliche Erweiterung K/k eines Körpers der Charakteristik Null ist separabel.

Beweis. Auf Grund von B.6 genügt es, den Fall einer einfachen Körpererweiterung zu betrachten,

$$K = k(\alpha).$$

Sei

$$f(x) = (x-\alpha_1)\cdot\ldots\cdot(x-\alpha_m)$$

das Minimalpolynom von α, wobei die α_i einer geeigneten endlichen Erweiterung M von K entnommen seien. Es reicht zu zeigen, daß es m verschiedene k-Einbettungen $K\to M$ gibt. Dazu wiederum genügt es zu zeigen, die Nullstellen von f sind paarweise verschieden. Hätte f eine mehrfache Nullstelle, so hätte der größte gemeinsame Teiler $g = GCD(f, f')$ von f und der Ableitung von f einen positiven Grad. Mit anderen Worten f hätte einen echten Teiler, im Widerspruch zur Wahl von f.
QED.

Bemerkungen

(i) Wir benutzen beim Beweis den Tatsache, daß in der Charakteristik Null die Ableitung eines von Null verschiedenen Polynoms ungleich Null ist.
(ii) Die obige Argumentation zeigt, ein irreduzibles Polynom f(x) hat genau dann mehrfache Nullstellen, wenn $f'(x)=0$ gilt.
(iii) Wir zeigen jetzt, daß jede endliche separable Erweitungen einfach ist. Die umgekehrte Aussage gilt natürlich nicht.

B.8 Satz vom primitiven Element

Jede endliche separable Erweiterung K/k ist einfach.
Beweisskitze. 1. Fall: k ist endlich.
Dann ist auch K endlich, d.h. die Einheitengruppe K* ist zyklisch. Sei ξ ein erzeugendes Element dieser Einheitengruppe. Dann enthält $k(\zeta)$ alle von Null verschiedenen Elemente von K, d.h. es ist $K=k(\zeta)$.
2. Fall: k ist unendlich und $K=k(\alpha,\beta)$.
Seien

$$\sigma_i: K \to M,\ i=1,\ldots,n := [K,k]$$

die paarweise verschiedenen k-Einbettungen von K in eine geeignete endliche Körpererweiterung M von k. Dann gilt für je zwei $i,j\in\{1,\ldots,n\}$ jeweils eine der beiden Ungleichungen

$$\sigma_i(\alpha) \neq \sigma_j(\alpha) \text{ oder } \sigma_i(\beta) \neq \sigma_j(\beta).$$

Weil k unendlich ist, gibt es Elemente $a,b\in k$ mit

$$a\cdot(\sigma_i(\alpha) - \sigma_j(\alpha)) + b\cdot(\sigma_i(\beta) - \sigma_j(\beta)) \neq 0$$

für beliebige $i,j\in\{1,\ldots,n\}$ mit $i\neq j$. Wir setzen $\gamma := a\cdot\alpha + b\cdot\beta$. Dann gilt

$$\sigma_i(\gamma) - \sigma_j(\gamma) \neq 0.$$

Insbesondere sind die k-Einbettungen $\sigma_i|_{k(\gamma)}: k(\gamma) \to M$ paarweise verschieden. Nach B.1 gilt deshalb

$$[k(\gamma):k] \geq n = [K:k].$$

Wegen $k(\gamma)\subseteq K$ muß dann aber $K=k(\gamma)$ gelten, d.h. K/k ist einfach.
3. Fall: k ist unendlich und K/k beliebig.

$$\text{Es gilt } K=k(\alpha_1,\ldots,\alpha_n).$$

Nach dem zweiten Fall kann man n solangen verkleinern bis n=1 gilt.
QED.

B.9 Separabilität und das Nichtentarten der Killingform

Sei K/k eine endliche separable Erweiterung. Dann ist die Abbildung

$$Tr: K\times K \to k,\ (a,b) \mapsto Tr(a,b) := Tr_{K/k}(ab).$$

eine nicht-entartete symmetrische Bilinearform über k.

Beweis. Lediglich die Aussage, daß die Form nicht-entartet ist, bedarf eines Beweises. Wir wählen ein primitiven Element $\gamma \in K$, d.h. ein Element mit

$$K = k(\gamma).$$

Wir betrachten die Vektorraumbasis

$$\omega_1 = 1, \omega_2 = \gamma, ..., \omega_n = \gamma^{n-1}$$

von K über k und die Determinante

$$D := \det(\mathrm{Tr}(\omega_i \omega_j)).$$

Wir haben zu zeigen $D \neq 0$. Dazu wir n paarweise verschiedene Einbettungen

$\sigma_\ell : K \to M$, $\ell = 1,...,n$,

in einen geeigneten Oberkörper M von K und betrachten wir die Determinante

$$\Delta := \det(\sigma_\ell \omega_i) = \det(\sigma_\ell \gamma^{i-1}) = \prod_{i<j} (\sigma_j \gamma - \sigma_i \gamma) \; (\neq 0).$$

Es gilt

$$\begin{aligned} 0 \neq \Delta^2 &= \det(\sigma_\ell \omega_i) \cdot \det(\sigma_\ell \omega_j)^T \\ &= \det\Big(\sum_{\ell=1}^{n} \sigma_\ell \omega_i \sigma_\ell \omega_j \Big) \\ &= \det\Big(\sum_{\ell=1}^{n} \sigma_\ell (\omega_i \omega_j) \Big) \\ &= \det(\mathrm{Tr}(\omega_i \omega_j)) \qquad \text{(vgl. B.5)} \\ &= D. \end{aligned}$$

QED.

B.10 Separabilität und mehrfache Nullstellen

Eine eine einfache algebraischen Erweiterung $K = k(\alpha)$ ist genau dann separabel, wenn das Minimalpolynom $f \in k(x)$ von α keine mehrfachen Nullstellen besitzt (d.h. wenn f separabel ist bzw. wenn α über k separabel ist).

Beweis. Besitze f keine mehrfache Nullstellen. Jede Nullstelle von f liefert dann eine andere Einbettung von K in eine hinreichend große Erweiterung von k, d.h. die Erweiterung K/k ist separabel. Die umgekehrte Implikation ergibt sich aus B.4.

QED.

B.11 Erhaltung der Separabilität bei Basiswechsel

Seien K/k eine beliebige und $k(\alpha)/k$ eine endliche separable Körpererweiterung. Dann ist $K(\alpha)/K$ separabel.

Beweis. Nach Voraussetzung hat das Minimalpolynom f von α über k keine mehrfachen Nullstellen. Das Minimalpolynom F von α über K ist aber ein Teiler von f.

QED.

B.12 Separabilität von Erweiterungen und von Elementen

Sei K/k eine endliche Körpererweiterung. Dann sind folgende Aussagen äquivalent.

(i) K/k ist separabel.

(ii) Jedes Element $\alpha \in K$ ist separabel über k (d.h. sein Minimalpolynom über k hat keine mehrfachen Nullstellen).

Beweis. (i) $\Rightarrow$ (ii). Nach B.3 ist $k(\alpha)/k$ für jedes $\alpha \in K$ separabel, also ist α nach B.10 separabel über k.

(ii) $\Rightarrow$ (i). Wir zerlegen die Erweiterung K/k in eine endliche Folge einfacher Erweiterungen

$$k=K_0 \subset K_1 \subset ... \subseteq K_t = K.$$

Nach B.6 reicht es zu zeigen, jede der Erweiterungen K_i/K_{i-1} ist separabel. Jedes $\alpha \in K_i$ ist nach Voraussetzung separabel über k, also erst recht über K_{i-1}. Da die Erweiterung

$$K_i/K_{i-1}$$

einfach ist, ist sie damit nach B.10 separabel.
QED.

B.13 Das Entarten der Killingform im inseparablen Fall
Sei K/k eine endliche inseparable Körpererweitung. Dann gilt

$$Tr_{K/k}(\alpha) = 0$$

für jedes $\alpha \in K$.

Beweis. 1. Fall: $K=k(\alpha)$ mit $\alpha \notin k$, $\alpha^p \in k$, p:= char(k)>0.
Wir betrachten die folgende Vektorraumbasis von K über k.

$$\omega_1 = 1, \omega_2 = \alpha, \omega_3 = \alpha^2, ..., \omega_p = \alpha^{p-1}$$

Für $\beta = b_1 + b_2\alpha + ... + b_p\alpha^{p-1}$ mit $b_i \in k$ schreiben wir

$$\beta \cdot \omega_i = \sum_{j=1}^{p} b_{ij}\omega_j \text{ mit } b_{ij} \in k.$$

Mit $b:= \alpha^p \in k$ erhalten wir

$$\begin{aligned} \beta = \beta\cdot\omega_1 &= b_1 + b_2\alpha + ... + b_p\alpha^{p-1} \\ \beta\cdot\omega_2 &= b\cdot b_p + b_1\alpha + ... + b_{p-1}\alpha^{p-1} \\ &... \end{aligned}$$

Koeffizientenvergleich für i=1,...,p liefert

$$b_{ii} = b_1,$$

d.h. es gilt $Tr_{K/k}(\beta) = p\cdot b_1 = 0$.

2.Fall: K/k beliebig.
Bezeichne p die Charakteristik von k. Nach B.7 gilt p>0. Nach B.12 gibt es ein Element $\beta \in K$, welches nicht separabel über k ist. Sei

$$f(x) = a_0 + a_1x + a_2x^2 + ... + a_{n-1}x^{n-1} + x^n \in k[x]$$

das Minimalpolynom von β über k. Dann gilt nach Bemerkung (ii) von B.7

$$0 = f'(x) = a_1 + 2a_2x + ... + (n-1)a_{n-1}x^{n-2} + nx^{n-1},$$

d.h. $i\cdot a_i = 0$ für alle i, d.h. p|i oder $a_i=0$. Mit anderen Worten, man kann f in der Gestalt

$$f(x) = g(x^{p^s}) \text{ mit } g \in k[x] \text{ und } s \geq 1$$

schreiben. Indem man s so groß wie mögliche wählt, erreicht man, daß das Polynom g eine von Null verschiedene Ableitung besitzt. Die Erweiterung $k \subset k(\beta)$ zerfällt damit in eine Folge

$$k \subseteq k' := k(\beta^{p^s}) \subseteq k(\beta)$$

von Erweiterungen. Das Minimalpolynom h von β^{p^s} über k ist ein Teiler von g. Wegen

$$[k(\beta):k] = \deg f = \deg g\cdot p^s \geq \deg h \cdot p^s \geq [k':k]\cdot[k(\beta):k']$$

muß sogar h=g gelten. Die Erweiterung links ist somit separabel. Also ist die Erweiterung rechts echt (und inseparabel). Insbesondere gilt

$$\beta^p \notin k'.$$

Sei t die kleinste natürliche Zahl mit $(\beta^{p^t})^p = \beta^{p^{t+1}} \in k'$. Wir setzen $\alpha := \beta^{p^t}$. Dann ist die Erweiterung $k''=k'(\alpha)$ von k' von der im 1.Fall betrachteten Gestalt, d.h. es gilt $Tr_{k''/k'} = 0$. Aus dem Körperturm

$$k \subseteq k' \subset k'' \subset K$$

und den Formeln von A.7 ergibt sich $Tr_{K/k} = 0$.

QED.

C Anhang: Henselsches Lemma

Literatur zu Kapitel 2

[1] Adamson: Introduction to field theory, Oliver and Boyd
[2] Artin, E.: Theory of algebraic numbers, Striker, Göttingen 1956
[3] Artin, E.: Representatives of the connected component of the idele class group, Proc. Int. Symp. Algebraic Numer Theory, Tokio-Nikko 1955
[4] Artin, E.: Galois Theory, Notre Dame, Paris 1946
[5] Arting, E., Tate, J.: Class field theory, Harvard 1951
[6] Weil, A.: Adeles and algebraic groups, Inst. Adv. Studies, Princeton 1961
[7] Weil, A.: On a certain type of the idele class group of an algebraic number field, Proc. Int. Symp. Algebraic Number Theory, Tokio - Nikko (1955), 9-22.
[8] Godement, R.: Bourbaki seminars, exp. 171, 176
[9] Iwasawa, K.: On the rings of valuation vectors, Ann. Math. 57 (1953),331-356
[10] Lang, S.: Algebraic numbers, Addison Wesley 1964
[11] Mahler, K.: Inequalities for ideal bases, J. Austr. Math. Soc. 4 (1964), 425-448

3 Kreisteilungskörper und Kummererweiterungen (B. J. *Birch)*

3.1 Kreisteilungserweiterungen

3.1.1 Der Körper $K(\sqrt[m]{1})$

Sei K ein beliebiger Körper der Charakteristik Null und m>1 eine natürliche Zahl. Dann gibt es eine minimale Erweiterung

(1) L/K

mit der Eigenschaft, daß das Polynom

(2) x^m-1

über L in ein Produkt von Linearfaktoren zerfällt. Die Nullstellen dieses Polynoms bilden eine Untergruppe der multiplikativen Gruppe von L. Dies ist eine zyklische Gruppe (da jede endliche Untergruppe der multiplikativen Gruppe eines Körpers zyklisch ist)[67]. Die Erzeugenden dieser Gruppe heißen primitive m-te Einheitswurzeln. Ist

---

[67] Seien K ein Körper und $H \subseteq K^*$ eine Untergruppe der multiplikativen Gruppe der Ordnun

$$\# H = m.$$

$\zeta \in L$

eine primitive m-te Einheitswurzel, so ist jede Nullstelle des Polynoms (2) eine Potenz von ζ., d.h. es gilt

$$L = K(\zeta).$$

Als Zerfällungskörper von (2) ist L eine über K normale Erweiterung. Wir werden schreiben

$$L = K(\sqrt[m]{1}).$$

3.1.2 Der Grad der Erweiterung $K(\sqrt[m]{1})/K$

Seien K ein Körper der Charatkeristik 0 und $m > 1$ eine natürliche Zahl. Dann gilt

$$[K(\sqrt[m]{1}):K] \leq \phi(m),$$

dabei sei ϕ die Euler-Funktion, d.h. $\phi(m)$ die Zahl der primen Restklassen modulo m.

Beweis. Sei ζ eine primitive m-te Einheitswurzel, $L := K(\zeta)$ und bezeichne

$$G(m) := (\mathbb{Z}/m\mathbb{Z})^*$$

die multiplikative Gruppe der primen Restklassen modulo m (d.h. die Einheitengruppe des Rings $\mathbb{Z}/m\mathbb{Z}$). Für jedes $\sigma \in G(L/k)$ ist $\sigma(\zeta)$ eine primitive m-te Einheitswurzel, d.h. es gilt

(3) $$\sigma(\zeta) = \zeta^k \text{ mit } (k,m) = 1.$$

Dabei ist k modulo m eindeutig bestimmt. Betrachten wir die Abbildung

(4) $$i: G(L/K) \to G(m) = (\mathbb{Z}/m\mathbb{Z})^*, \sigma \mapsto k \bmod m.$$

Dies ist ein Gruppenhomomorphismus: mit

$$\sigma(\zeta) = \zeta^k \text{ und } \tau(\zeta) = \zeta^{\ell}$$

Bezeichne H_d die Elemente der Ordnung d von H. Da die Ordnung jedes Elements von H die Ordnung m teilt, gilt

$$H = \bigcup_{d|m} H_d,$$

wobei dies eine disjunkte Vereinging ist, also

$$m = \# H = \sum_{d|m} \# H_d$$

Die Elemente von H_d sind primitive d-te Einheitswurzeln von K, ihre Anzahl ist also höchstens $\varphi(d)$,

$$\# H_d \leq \varphi(d) \qquad \text{(Euler-Zahl)}.$$

Für $K = \mathbb{C}$ gilt das Gleichheitszeichen. Es folgt

$$m = \# H = \sum_{d|m} \# H_d \leq \sum_{d|m} \varphi(d),$$

wobei für $K = \mathbb{C}$ das Gleichheitszeichen gilt. Nun hängt der Ausdruck rechts nicht von der speziellen Wahl des Körper ab, d.h. es ist stets

$$m = \# H = \sum_{d|m} \# H_d \leq \sum_{d|m} \varphi(d) = m.$$

Es gilt also für jeden Körper K in der gesamten obigen Rechnung das Gleichheitshzeichen. Insbesonderen gilt

$$\# H_m = \varphi(m),$$

d.h. H enthält ein Element der Ordnung m, ist also zyklisch.

gilt nämlich

$$(\sigma\tau)(\zeta) = \sigma(\tau(\zeta)) = \sigma(\zeta^{\ell}) = \sigma(\zeta)^{\ell} = \zeta^{k\ell},$$

also $i(\sigma\tau) = k\ell = i(\sigma)\cdot i(\tau)$. Der Automorphismus σ von (3) ist durch die Restklasse von k modulo m ein deutig bestimmt (da ζ die Erweiterung L/K erzeugt), d.h. die Abbildung (4) ist injektiv. Aus der Injektivität von (4) folgt aber die Behauptung.
QED.

3.1.3 Eine Zerlegung in Teilerweiterungen

Seien K ein Körper der Charatkeristik 0, $m > 1$ eine natürliche Zahl, ζ eine primitive m-te Einheitswurzeln und

$$L = K(\zeta).$$

Die natürliche Zahl m gestatte eine Produktzerlegung

$$m = r \bullet s \text{ mit } (r,s) = 1.$$

Dann existieren ganze Zahlen $a,b \in \mathbb{Z}$ mit

$$1 = ar + bs.$$

Insbesondere gilt $\zeta = (\zeta^r)^a \cdot (\zeta^s)^b$, also

$$L = K(\zeta) = K(\zeta^r, \zeta^s).$$

Die Erweiterung zerfällt in eine Komposition von zwei Erweiterungen desselben Typs. Dies gestattet es, sich auf die Untersuchung von Erweiterungen der Gestalt

$$L = K(\sqrt[m]{1}) \text{ mit } m = p^n, \text{ p Primzahl,}$$

zu beschränken.

3.1.4 Die Galoisgruppe der Erweiterung $K(\sqrt[m]{1})$ für Primzahlpotenzen $m = p^n$

Seien K ein Körper der Charatkeristik 0, $m > 1$ eine natürliche Zahl und

$$L := K(\zeta)$$

mit einer primitiven m-ten Einheitswurzel.

(i) Im Fall $m = p^n$ mit einer ungeraden Primzahl p ist die Gruppe

$$G(p^n)$$

der primen Restklassen modulo p^n zyklisch. Also ist auch die Untergruppe

$$G(L/K) \subseteq G(p^n)$$

zyklisch (vgl. Beweis von 3.1.2).

(ii) Im Fall $m = 2^n$ wird die Gruppe $G(2^n)$ von -1 und 5 erzeugt. Mit

$$\eta := \zeta + \zeta^{-1},$$

wobei ζ eine primitive 2^n-te Einheitswurzel bezeichne, erhalten wir

$$L = K(i, \eta).$$

Die Galoisgruppe

$$G(K(\eta)/K)$$

der Teilerweiterung $K(\eta)/K$ ist wieder zyklisch.

Beweis. <u>1. Schritt</u>. $\sum_{d|n} \phi(d) = n$.

Für jeden Teiler von d von n bezeichne $C_d \subseteq \mathbb{Z}/n\mathbb{Z}$ die einzige Untergruppe der Ordnung d. Weiter sei Φ_d die Menge der Erzeugenden von C_d. Da jedes Element von $\mathbb{Z}/n\mathbb{Z}$ eine der Untergruppen C_d erzeugt, ist $\mathbb{Z}/n\mathbb{Z}$ Vereinigung der paarweise disjunkten Mengen Φ_d. Deshalb gilt

$$n = \#\mathbb{Z}/n\mathbb{Z} = \sum_{d|n} \#\Phi_d$$

Es reicht also, zu zeigen

$$\#\Phi_d = \phi(d).$$

Sei η ein Erzeugendes von C_d. Dann hat η die Ordnung d und η^i die Ordnung $\frac{d}{(i,d)}$, d.h. η^i ist genau dann ein Erzeugendes von C_d, wenn i teilerfremd zu d ist. Es gibt also genau $\phi(d)$ Erzeugende.

2. Schritt. Sei H eine Gruppe der Ordnung n ($<\infty$). Für jeden Teiler d von n möge die Bestimmungsgleichung $x^d = 1$ höchstens d Lösungen haben. Dann ist H eine zyklische Gruppe.

Sei d ein Teiler von n. Wenn es ein Element $a \in H$ der Ordnung d gibt, so ist die von a erzeugte Untergruppe

$$<a> = \{1,a,...,a^{d-1}\}$$

gerade die zyklische Gruppe der Ordnung d. Nach Voraussetzung liegt deshalb jede Lösung von

$$x^d = 1$$

in dieser Untergruppe. Insbesondere sind die Elemente der Ordnung d von H (und nur diese) die Erzeugenden von <a>. Die Zahl dieser Elemente ist daher gleich $\phi(d)$. Wir haben gezeigt: die Zahl der Elemente der Ordnung d von H ist Null oder gleich $\phi(d)$. Auf jeden Fall ist die Zahl $\leq \phi(d)$. Da jedes Element von H irgendeine Ordnung hat (die n teilt), erhalten wir für die Zahl der Elemente von H die Abschätzung

$$\leq \sum_{d|n} \phi(d) = n \quad \text{(vgl. 1.Schritt).}$$

Wäre für irgendeinen Teiler d von n die Zahl der Elemente der Ordnung d gleich Null, so wäre diese Ungleichung echt, d.h. H hätte weniger als n Elemente im Widerspruch zur Definition von n. Also gibt es für jeden Teiler d von n ein Element der Ordnung d in H. Das gilt insbesondere für d=n, d.h. es gibt ein Element der Ordnung n in H. Mit anderen Worten, H ist zyklisch.

3. Schritt. Zu jeder ungeraden Primzahl p gibt es eine primitive Einheitswurzel[68] a modulo p mit

$$a^{p-1} \not\equiv 1 \pmod{p^2}$$

Die Restklassen modulo p, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, bilden einen Körper. Deshalb erfüllt die Gruppe der primen Restklassen modulo p,

$$\mathbb{F}_p^*$$

die Voraussetzungen des 2. Schrittes, d.h. sie ist zyklisch. Es gibt also eine primitve Einheitswurzel modulo p. Sei a' eine solche primitve Einheitswurzel und sei

(1) $a'' := a' + p.$

Mit a' ist auch a" eine primitve Einheitswurzel modulo p. Es gilt

(2) $$(a'')^p = \sum_{j=0}^{p} \binom{p}{j} (a')^j p^{p-j} \equiv (a')^p \pmod{p^2}.$$

Nach dem kleinen Fermatschen Satz gilt

$$(a')^p = a' + p \cdot b'$$

$$(a'')^p = a'' + p \cdot b''$$

mit ganzen Zahlen b', b"$\in\mathbb{Z}$. Wir setzen dies in (2) ein und erhalten

---

[68] d.h. die Gruppe G(p) der primen Restklassen modulo p ist zyklisch.

$$a' + p\cdot b' \equiv a'' + p\cdot b'' \pmod{p^2}$$

Wegen (1) folgt

$$b' \equiv b'' + 1 \pmod{p}.$$

Von den beiden Zahlen b', b'' ist also höchstens eine durch p teilbar. Von den Differenzen

$$(a')^p - a' = a'\cdot(a'^{p-1}-1)$$

$$(a'')^p - a'' = a''(a''^{p-1}-1)$$

ist daher höchstens eine durch p^2 teilbar. Dasselbe gilt dann aber auch für

$$a'^{p-1}-1 \text{ und } a''^{p-1}-1.$$

4. Schritt. Zu jeder ungeraden Primzahl p und jeder natürlichen Zahl k gibt es eine primitve Einheitswurzel[69] modulo p^k.

Wir wählen a wie im 3. Schritt. Wir zeigen zunächst, es reicht zu zeigen,

(3) $$a^{(p-1)p^{k-2}} \not\equiv 1 \pmod{p^k} \text{ für } k= 2, 3, \ldots$$

Da a eine primitve Einheitswurzel modulo p ist, ist a teilerfremd zu p. Bezeichne

$$\ell := \operatorname{ord}_{p^k}(a)$$

die Ordnung von a modulo p^k. Diese teilt die Gruppenordnung

$$\#G(p^k) = \phi(p^k) = p^k - p^{k-1} = (p-1)p^{k-1}.$$

Weiter gilt $a^\ell \equiv 1 \pmod{p^k}$ also $a^\ell \equiv 1 \pmod{p}$, also $p-1 \mid \ell$, also

$$\ell = (p-1)\cdot p^\alpha$$

für ein $\alpha\in\{0,1,\ldots,k-1\}$. Es ist also

$$a^\ell = a^{(p-1)\cdot p^\alpha} \equiv 1 \pmod{p^k}.$$

Nach (3) ist $k-2<\alpha$., also $\alpha=k-1$. Die Restklasse von a hat also modulo p^k die Ordnung

$$\ell = (p-1)\cdot p^{k-1} = \#G(p^k),$$

d.h. $G(p^k)$ ist zyklisch. Wir haben noch (3) zu beweisen. Für k=2 gilt dies nach Wahl von a (vgl. 3. Schritt). Gelte jetzt (3) für ein $k\geq 2$. Wir haben zu zeigen, (3) gilt dann auch mit k+1 anstelle von k. Es gilt

$$\phi(p^{k-1}) = p^{k-1}-p^{k-2} = (p-1)p^{k-2}$$

also nach dem kleinen Fermatschen (genauer, dem Eulerschen) Satz

$$a^{(p-1)p^{k-2}} = 1 + b\cdot p^{k-1} \text{ mit } b\in\mathbb{Z}.$$

Wegen (3) ist b nicht durch p teilbar. Wir erheben diesen Ausdruck in die p-te Potenz und erhalten

$$a^{(p-1)p^{k-1}} = (1 + b\cdot p^{k-1})^p = 1 + b\cdot p^k + c\cdot p^{2k-1} \text{ mit } c\in\mathbb{Z}.$$

Wir verwenden hier die Tatsache, daß $\binom{p}{2} = \frac{p(p-1)}{2}$ durch p teilbar ist. Nun ist

$$2k-1 \geq k+1$$

für $k\geq 2$ und b ist nicht durch p teilbar. Also gilt

$$a^{(p-1)p^{k-1}} \not\equiv 1 \pmod{p^{k+1}}$$

Dies ist gerade (3) mit k+1 anstelle von k.

5. Schritt. Sei $u\in\mathbb{Z}$ ungerade. Dann sind folgende Aussagen äquivalent.

(i) u repräsentiert für n=3,4,... ein Element von $G(2^n) := (\mathbb{Z}/2^n\mathbb{Z})^*$ der Ordnung 2^{n-2}.

---

[69] d.h. die Gruppe $G(p^k)$ der primen Restklassen modulo p^k ist zyklisch.

(ii) $u \equiv \pm 3 \pmod 8$

Die Gruppe $G(2^n)$ (der Ordnung $\varphi(2^n) = 2^n - 2^{n-1} = 2^{n-1}$) ist nicht zyklisch (für alle $n \geq 3$).

Die primen Restklassen modulo 8 haben die Menge

$$\{\pm 1, \pm 3\}$$

als vollständiges Repräsentantensystem. Sei zunächst

$$u \equiv \pm 1 \pmod 8).$$

Wir zeigen zunächst, daß dann

(4) $$u^{2^{n-3}} \equiv 1 \pmod{2^n} \text{ für } n = 4,5,...$$

gilt. Wegen $8 \mid (u \mp 1)$ gilt $8^2 \mid (u \mp 1)^2 = u^2 \mp 2u + 1$, also $u^2 \equiv \pm 2u - 1 \equiv 2 - 1 = 1 \pmod{16}$, d.h.

$$u^2 \equiv 1 \pmod{2^4}.$$

Die Kongruenz (4) besteht also wenigstens für $n=4$. Bestehe sie jetzt für n und zeigen wir, daß sie dann auch für $n+1$ besteht. Es gilt $2^n \mid u^{2^{n-3}} - 1$, also

$$2^{n+1} \mid (u^{2^{n-3}} - 1)^2 = u^{2^{n-2}} - 2u^{2^{n-3}} + 1$$

also

$$u^{2^{n-2}} \equiv 2u^{2^{n-3}} - 1 \equiv 2 - 1 = 1 \pmod{2^{n+1}}.$$

Damit ist (4) für alle $n \geq 4$ bewiesen. Insbesondere sehen wir, daß mit (i) notwendig (ii) gelten muß.

Sei jetzt $u \equiv \pm 3 \pmod 8$. Zeigen wir, daß dann für alle $k \in \mathbb{N}$ gilt

(5) $$u^{2^k} - 1 = 2^{k+2} \cdot v_k$$

mit ungeradem v_k. Für $k=1$ ist das klar:

$$u^{2^k} - 1 = u^2 - 1 = (u-1)(u+1) = (\pm 2 + 8\alpha)(\pm 4 + 8\alpha) = 8(\pm 1 + 4\alpha)(\pm 1 + 2\alpha).$$

Sei jetzt (5) für $k \geq 1$ bereits bewiesen. Dann gilt

$$u^{2^k} + 1 = 2^{k+2} \cdot v_k + 2 = 2w_k \text{ mit } w_k = 1 + 2^{k+1} \cdot v_k \text{ ungerade,}$$

also

$$u^{2^{k+1}} - 1 = (u^{2^k} - 1)(u^{2^k} + 1) = 2^{k+2} \cdot v_k \cdot 2w_k = 2^{k+3} \cdot v_k \cdot w_k$$

Damit ist (5) für alle k bewiesen.

Insbesondere sehen wir für $k=n-2$, das Element u hat modulo 2^n eine Ordnung, welche ein Teiler von 2^{n-2} ist,

$$\text{ord}\,(u \bmod 2^n) = 2^\ell \text{ mit } \ell \leq n-2.$$

Zu sammen mit (4) ergibt sich, daß die Gruppe $G(2^n)$ (welche die Ordnung 2^{n-1} hat) nicht zyklisch ist für $n \geq 4$ (für $n=3$ sieht man das unmittelbar).

Nach Definition von ℓ gilt

$$2^n \mid (u^{2^\ell} - 1) = 2^{\ell+2} v_\ell$$

(vgl. (5)), also $n \leq \ell + 2$, also $\ell = n-2$, also

$$\text{ord}\,(u \bmod 2^n) = 2^{n-2}$$

für alle $n = 3,4,...$ Damit ist die Aussage des 5. Schrittes bewiesen.

6.Schritt. $G(2^n)$ wird von den Restklassen von -1 und 5 erzeugt.

Für $n=1$ gilt $G(2^n) = \{1\}$ und die Aussage ist trivial.

Für n=2 gilt $G(2^n) = \{1, 3 = -1\}$ und die Aussage ist ebenfalls trivial.

Für $n \geq 3$ repräsentiert u=5 nach dem 5.Schritt ein Element der Ordnung 2^{n-2} der Gruppe $G(2^n)$, d.h. es gilt

$$[G(2^n):\langle u\rangle] = 2.$$

Zum Beweis der Behauptung reicht es zu zeigen, -1 repräsentiert ein Element von $G(2^n)$ welches nicht in der Untergruppe $\langle u\rangle$ liegt.
Wäre dies nicht so, so würde gelten

$$-1 \equiv u^k \pmod{2^n} \text{ mit } 0 < k < n-2,$$

also $2^n \mid u^k+1$, also $2^{n+1} \mid (u^k+1)^2 = u^{2k}+2u^k+1$, also

$$u^{2k} \equiv -2u^k-1 \equiv 1 \pmod{2^{n+1}}$$

Nach dem 5. Schritt hat u aber modulo 2^{n+1} die Ordnung 2^{n-1}, d.h. es muß gelten

$$2^{n-1} \mid 2k,$$

also

$$2^{n-2} \mid k,$$

Wegen $k \leq n-3 < 2^{n-2}$[70] folgt k = 0 im Widerspruch zur Wahl von k. Damit ist gezeigt, die Restklassen von 5 und -1 erzeugen $G(2^n)$.
7. Schritt. Abschluß des Beweises.
Wir haben noch zu zeigen,

1. $L = K(i,\eta)$ mit $\eta := \zeta+\zeta^{-1}$
2. Die Galoisgruppe von $K(\eta)/K$ ist zyklisch.

Zu 1. Da ζ eine primitive 2^n-te Einheitswurzel ist, ist $\zeta^{2^{n-2}}$ eine primitive 4-te Einheitwurzel, d.h.

$$\zeta^{2^{n-2}} = \pm i.$$

Mit anderen Worten, $i \in L$. Damit gilt $L \supseteq K(i,\eta)$. Zum Beweis der umgekehrten Inklusion genügt es zu zeigen,

$$\zeta \in K(i,\eta).$$

Nun hat K nach Voraussetzung die Charakteristik Null, d.h. es gilt $\mathbb{Q} \subseteq K$. Es reicht deshalb, wen wir zeigen,

$$\zeta \in \mathbb{Q}(i,\eta).$$

Mit anderen Worten, wir können annehmen, $K = \mathbb{Q}$. Nach Definition von η gilt

$$\zeta^2 - \eta\cdot\zeta + 1 = 0,$$

d.h. $L = \mathbb{Q}(\zeta)$ hat einen Grad ≤ 2 über $\mathbb{Q}(\eta)$,

$$[L:\mathbb{Q}(\eta)] \leq 2.$$

---

[70] Für n=3 ist die rechte Ungleichung trivial. Es reicht zu zeigen

$$\frac{d}{dx}(x-3) \leq \frac{d}{dx}(2^{x-2})$$

für alle x mit $3 \leq x$. Die linke Ableitung ist 1, die rechte ist

$$\frac{d}{dx}(2^{x-2}) = \frac{d}{dx}((e^{\log 2})^{x-2}) = \frac{d}{dx}\, e^{(\log 2)\bullet(x-2)} = e^{(\log 2)\bullet(x-2)}\bullet\log 2$$

$$= 2^{x-2}\bullet(\log 2)$$
$$\geq 2\bullet\log 2 \qquad \text{(wegen } x \geq 3\text{)}$$
$$\geq 2\bullet 0.693$$
$$> 1$$

Wegen $i \in L$ genügt es zu zeigen, i liegt nicht in $\mathbb{Q}(\eta)$. Das ist aber so, weil η eine rein reelle Zahl ist.

Zu 2. Wie wir oben gesehen haben, ist die Galoisgruppe von L/K eine Untergruppe von $G(2^n)$. Letztere Gruppe ist abelsch, d.h. jede Untergruppe ist ein Normalteiler. Nach dem Hauptsatz der Galoistheorie ist damit jede Teilerweiterung von L/K ebenfalls normal. Insbesondere ist

$$K(\eta)/K \text{ normal.}$$

Betrachten wir die Einschränkungsabbildung

$$G(L/K) \to G(\mathbb{Q}(\sqrt[n]{1})/\mathbb{Q}),\ \sigma \mapsto \sigma|_{\mathbb{Q}(\sqrt[n]{1})}.$$

Sie hat als Kern gerade diejenigen Automorphismen von L, welche die primitive Einheitswurzel $\zeta \in \mathbb{Q}(\sqrt[n]{1})$ in sich abbilden, d.h. der Kern ist trivial,

$$G(L/K) \subseteq G(\mathbb{Q}(\sqrt[n]{1})/\mathbb{Q}).$$

Weiter haben wir die Einschränkungsabbildungen

(7) $$G(L/K) \to G(K(\eta)/K)$$

(8) $$G(\mathbb{Q}(\sqrt[n]{1})/\mathbb{Q}) \to G(\mathbb{Q}(\eta)/\mathbb{Q})$$

Im Kern der zweiten liegt zum Beispiel die komplexe Konjugation, d.h. der Automorphismus

$$i: \zeta \mapsto \zeta^{-1}.$$

Dieser Automorphismus erzeugt eine Untergruppe der Ordnung 2. Wegen

$$\#\mathrm{Ker}\ (8) = \#G(\mathbb{Q}(\sqrt[n]{1})/\mathbb{Q}(\eta)) = [\mathbb{Q}(\sqrt[n]{1}):\mathbb{Q}(\eta)] = 2$$

besteht der Kern gerade aus zwei Elementen, d.h. es ist

$$\mathrm{Ker}\ (8) = \{i, Id\}.$$

Die beiden Homomorphismen (7) und (8) sind Bestandteile eines kommutativen Quadrats

$$\begin{array}{ccc} G(L/K) & \longrightarrow & G(K(\eta)/K) \\ \cap & & \cap \\ G(\mathbb{Q}(\sqrt[n]{1})/\mathbb{Q}) & \longrightarrow & G(\mathbb{Q}(\eta)/\mathbb{Q}) \end{array}$$

von Einschränkungsabbildungen. Deshalb gilt

$$\begin{aligned} G(K(\eta)/K) &= G(L/K)/\mathrm{Ker}(7) \\ &= G(L/K)/\{ i, Id \} \cap G(L/K) \\ &= G(L/K) \cdot \{ i, Id\}/\{ i, Id\} \\ &\subseteq G(2^n)/\{\pm 1\} \end{aligned}$$

Da $G(2^n)$ nach dem 6. Schritt von 5 und -1 erzeugt wird, ist die Gruppe $G(2^n)/\{\pm 1\}$ zyklisch. Dann ist aber auch die Untergruppe $G(K(\eta)/K)$ zyklisch.

QED.

Bemerkungen

(i) Uns werden hier in erster Linie die Erweiterungen $\mathbb{Q}(\sqrt[m]{1})$ und $\mathbb{Q}_p(\sqrt[m]{1})$ interessieren.

(ii) Wie wir im ersten Kapitel gesehen haben (Abschnitt 1.4 und der Anfang von 1.5) ist die Untersuchung der Zerlegung der Primzahl p im Körper $\mathbb{Q}(\sqrt[m]{1})$ äquivalent zur Untersuchung der Erweiterung $\mathbb{Q}_p(\sqrt[m]{1})$ von $\mathbb{Q}_p$.

(iii) Um einige abstrakte Sätze durchsichtiger zu gestalten, werden wir manchmal mehrere verschiedene Beweise ein und derselben Behauptung geben.
(iv) Einen guten Überblick zur Theorie der Kreisteilungskörper kann man in den Büchern von Weil[2] und Weiss[1], Kap. 7 finden.

3.1.5 Grad und Galois-Gruppe im Fall K = $\mathbb{Q}$

$$[\mathbb{Q}(\sqrt[m]{1}):\mathbb{Q}] = \Phi(m) \qquad \text{(Eulerfunktion)}$$

$$G(\mathbb{Q}(\sqrt[m]{1})/\mathbb{Q}) = G(m) \qquad \text{(prime Restklassen modulo m)}$$

Beweis (acording to Van der Waerden). Sei ζ eine primitive m-te Einheitswurzel. Wegen

$$G(\mathbb{Q}(\sqrt[m]{1})/\mathbb{Q}) \subseteq G(m) \text{ und } \#G(m) = \phi(m)$$

(vgl. Beweis von 3.1.2) genügt es zu zeigen, daß Minimalpolynom von ζ über $\mathbb{Q}$ hat über $\mathbb{Q}$ den Grad $\geq\phi(m)$. Mit anderen Worten, es genügt zu zeigen, ist

$$f(x) \in \mathbb{Z}[x]$$

ein Polynom mit $f(\zeta) = 0$ so gilt[71]

$$f(\zeta^a) = 0 \text{ für alle } a\in\mathbb{Z} \text{ mit } ggT(a,m) = 1.$$

O.B.d.A. können wir annehmen, daß

$$a=p$$

eine zu m teilerfremde Primzahl ist[72].

Bezeichne wie immer $\mathbb{F}_p$ den Körper mit p Elementen. Für jedes ganzzahlige Polynom $g\in\mathbb{Z}[x]$ bezeichne

$$g^*\in\mathbb{F}_p[x]$$

das Bild von g bei der natürlichen Abbildung $\mathbb{Z}[x] \to \mathbb{F}_p[x]$. Weiter sei

$$L^*/\mathbb{F}_p$$

eine endliche Körpererweiterung, über der das Polynom x^m-1 in Linearfaktoren zerfällt. Man beachte, die Linearfaktoren der Faktorzerlegung sind paarweise verschieden, denn das Polynom hat keine mehrfachen Nullstellen:

$$ggT(x^m-1, \frac{d}{dx}(x^m-1)) = ggT(x^m-1, mx^{m-1}) = 1.$$

Betrachten wir jetzt Zerlegung von x^m-1 in irreduzible Faktoren über $\mathbb{Z}$(oder $\mathbb{Q}$, was nach dem Gaußschen Lemma dasselben ist),

$$x^m-1 = f_1(x)\cdot f_2(x)\cdot\ldots\cdot f_r(x).$$

Über dem Körper $\mathbb{F}_p$ gilt dann

$$x^m-1 = f_1^*(x)\cdot f_2^*(x)\cdot\ldots\cdot f_r^*(x).$$

Im Körper L* sind die Nullstellen der Polynome $f_i^*(x)$ als Nullstellen von x^m-1 paarweise verschieden. Insbesondere haben die f_i^* keine gemeinsamen Nullstellen. Wir wählen die Indizes der Polynome f_i so, daß gilt

---

[71] Dann ist f Nullstelle aller primitiven m-ten Einheitswurzeln und davon gibt es $\Phi(m)$ Exemplare, d.h. f(x) hat mindestens $\Phi(m)$ Nullstellen, also mindestens den Grad $\Phi(m)$.
[72] Durch durch wiederholtes Anwenden der Aussage für den Spezialfall a=p erhält man die Aussage für beliebiges a (welches Produkt von solchen Primzahlen p ist).

$$\zeta \text{ ist Nullstelle von } f_1(x).$$

Ist ζ^p Nullstelle von $f_j(x)$, so ist ζ Nullstelle von $f_j(x^p)$, d.h.

$$f_1(x) \text{ teilt } f_j(x^p), \text{ d.h. } f_1^*(x) \text{ teilt } f_j^*(x^p).$$

Damit gilt für jede Nullstelle a von $f_1^*(x)$, daß a^p Nullstelle von $f_j^*(x)$ ist. Außerdem ist aber auch a^p Nullstelle von $f_1^*(x)$:

$$f_1^*(a^p) = f_1^*(a)^p = 0.$$

Da nach Konstruktion die f_i^* keine gemeinsamen Nullstellen besitzen, folgt $f_1^* = f_j^*$, also 1=j, also $f_1 = f_j$.. Wir haben gezeigt, ζ^p ist Nullstelle des irreduziblen Polynoms f_1 von ζ.
QED.

3.1.6 Der Frobenius-Automorphismus von $\mathbb{Q}(\sqrt[m]{1})$

Ist p eine zu m teilerfremde Primzahl, so gibt es genau ein Element

$$\sigma_p \in G(\mathbb{Q}(\sqrt[m]{1})/\mathbb{Q})$$

mit der Eigenschaft, daß für jedes (über $\mathbb{Z}$) ganze Element $\alpha \in \mathbb{Q}(\sqrt[m]{1})$ gilt

$$\sigma_p(\alpha) \equiv \alpha^p \pmod p.$$

Ist ζ eine primitive m-te Einheitswurzel, so gilt

$$\sigma_p(\sum_i a_i \zeta^i) = \sum_i a_i \zeta^{pi} \text{ für } a_i \in \mathbb{Q}.$$

Das Element σ_p heißt Frobenius-Automorphismus von $\mathbb{Q}(\sqrt[m]{1})$ zur Primzahl p.

Beweis. Da $\mathbb{Q}(\sqrt[m]{1})$ von ζ erzeugt wird, ist jeder Automorphismus von $\mathbb{Q}(\sqrt[m]{1})$ durch das Bild von ζ bei diesem Automorphismus eindeutig bestimmt. Da es $\Phi(m)$ primitive m-te Einheitswurzeln gibt, gibt es höchstens $\Phi(m)$ mögliche Bilder von ζ. Nach 3.1.5 sind damit je zwei primitive m-te Einheitswurzeln konjugiert, d.h. zu jedem a mit

$$ggT(a,m) = 1$$

gibt es einen Automorphismus σ mit

$$\sigma(\zeta) = \zeta^a.$$

Für einen solche Automorphismus gilt dann

$$\sigma(\sum_i a_i \zeta^i) = \sum_i a_i \zeta^{ai} \text{ für } a_i \in \mathbb{Q}.$$

Insbesondere ist durch diese Formel für jedes a mit ggT(a,m) = 1 ein Automorphismus von $\mathbb{Q}(\sqrt[m]{1})$ definiert und man erhält auf diese Weise alle Automorphismen.
Betrachten wir speziel den Fall
a = p.
Wir haben zu zeigen,

1. σ bildet den Ring[73] $\mathcal{O}$ der ganzen Zahlen von $\mathbb{Q}(\sqrt[m]{1})$ in sind ab.
2. Es gilt $\sigma(\alpha) \equiv \alpha^p \pmod p$ für alle $\alpha \in \mathcal{O}$.
3. σ ist durch Bedingung 2 eindeutig bestimmt.

Zu 1. Das ist trivial, weil $\mathbb{Z}$ elementweise festgelassen wird.
Zu 2.
1. Schritt. Reduktion auf die Aussage $\mathcal{O} \subseteq \mathbb{Z}_{(p)}[\zeta]$.
Diese Inklusion bedeutet, jedes Element $\alpha \in \mathcal{O}$ läßt sich in der Gestalt

$$\alpha = \sum_i \frac{a_i}{b} \zeta^i$$

schreiben mit $a_i, b \in \mathbb{Z}$ und b teilerfremd zu p. Insbesondere ist b eine Einheit modulo p. Das Inverse von b wird modulo p durch eine gewisse ganz Zahl, sagen wir b' repräsentiert. Es gilt daher modulo p,

$$\begin{aligned}
\sigma(\alpha) - \alpha^p &\equiv b' \sum_i a_i \cdot \zeta^{pi} - (b' \sum_i a_i \cdot \zeta^i)^p \\
&\equiv b' \sum_i a_i \cdot \zeta^{pi} - b'^p \sum_i a_i^p \cdot \zeta^{pi} \quad \text{(binom. Formeln in der Char. p)} \\
&\equiv b' \sum_i a_i \cdot \zeta^{pi} - b' \sum_i a_i \cdot \zeta^{pi} \quad \text{(kleiner Fermatscher Satz)} \\
&\equiv 0
\end{aligned}$$

Damit ist die Aussage von 2. auf den Beweis der angegebenen Inklusion reduziert. Zu deren Beweis betrachten wir die Vektorraumbasis[74]

(1) $$1, \zeta, \ldots, \zeta^{\Phi(m)-1}$$

von $\mathbb{Q}(\sqrt[m]{1})$ über $\mathbb{Q}$.

2. Schritt. Die Diskriminante des von den Potenzen (1) erzeugten (freien) $\mathbb{Z}$-Teilmoduls $M := \mathbb{Z}[\zeta]$ von $\mathcal{O}$ wird von einer zu p teilerfremden ganzen Zahl erzeugt.

Bezeichne f(x) das Mininimalpolynom von ζ über $\mathbb{Q}$ und N: $\mathbb{Q}(\sqrt[m]{1}) \to \mathbb{Q}$ die Normabbildung.

Dann gilt nach 1.4.16(ii)

$$\delta(M) = N(f'(\zeta))\mathbb{Z} \text{ mit } N(f'(\zeta)) \in \mathbb{Z}.$$

Man beachte, $f'(\zeta)$ ist ganz über $\mathbb{Z}$, d.h. die Norm von $f'(\zeta)$ liegt in $\mathbb{Z}$.

Weiter ist f ein Teiler von $x^m - 1$,

$$x^m - 1 = f(x)\, g(x)$$

mit einem ganz-zahligen Polynom g(x). Insbesondere ist das Absolutglied von f gleich ± 1, d.h. die Norm von ζ (= Produkt der Konjugierten von ζ) ist gleich ± 1,

$$N(\zeta) = \pm 1.$$

Wir differenzieren und erhalten

---

[73] d.h. die ganze Abschließung von $\mathbb{Z}$ in $\mathbb{Q}(\sqrt[m]{1})$.

[74] Dies ist tatsächlich eine Vektorraumbasis, denn $\mathbb{Q}(\sqrt[m]{1})$ besitzt über $\mathbb{Q}$ (nach 3.1.5) den Grad $\Phi(m)$

$$mx^{m-1} = f'(x)g(x) - f(x)g'(x),$$

also

$$m\zeta^{m-1} = f'(\zeta)g(\zeta),$$

also

$$\begin{aligned} N(f'(\zeta))N(g(\zeta)) &= N(m\,\zeta^{m-1}) \\ &= N(m)N(\zeta)^{m-1} \\ &= \pm m^{\Phi(m)} \end{aligned}$$

3. Schritt. $\mathcal{O} \subseteq \mathbb{Z}_{(p)}[\zeta]$.

Es reicht zu zeigen, $\mathcal{O}_{(p)} = \mathbb{Z}_{(p)}[\zeta]$. Wegen $\mathbb{Z}[\zeta] \subseteq \mathcal{O}$ besteht für die Lokalisierungen im Primideal (p) die Inklusion

(2) $$\mathbb{Z}_{(p)}[\zeta] \subseteq \mathcal{O}_{(p)}.$$

Damit ist (nach 1.3.6) der Index

$$[\mathcal{O}_{(p)} : \mathbb{Z}_{(p)}[\zeta]] \subseteq \mathbb{Z}_{(p)}$$

eine ganzes Ideal von $\mathbb{Z}_{(p)}$ und für die Diskriminanten gilt

$$\begin{aligned} \mathbb{Z}_{(p)} &= \delta(\mathbb{Z}[\zeta])\mathbb{Z}_{(p)} && \text{(nach dem 2. Schritt)} \\ &= \delta(\mathbb{Z}_{(p)}[\zeta]) && \text{(nach 1.3.12(ii))} \\ &= \delta(\mathcal{O}_{(p)}) \cdot ([\mathcal{O}_{(p)} : \mathbb{Z}_{(p)}[\zeta])^2 && \text{(nach 1.3.12(i))} \\ &\subseteq \delta(\mathcal{O}_{(p)}) \end{aligned}$$

Nun ist die Diskriminante von $\mathcal{O}_{(p)}$ ein ganzes Ideal von $\mathbb{Z}_{(p)}$, d.h. in der obigen Rechnung gilt überall das Gleichheitszeichen. Insbesondere ist

$$[\mathcal{O}_{(p)} : \mathbb{Z}_{(p)}[\zeta]] = \mathbb{Z}_{(p)},$$

also zusammen mit (2) (nach 1.3.6(iv)) sogar

$$\mathcal{O}_{(p)} = \mathbb{Z}_{(p)}[\zeta].$$

Zu 3. Wir haben noch zu zeigen, der Automorphismus σ wird durch die Bedingung 2 eindeutig festgelegt.

Zumindest ist σ durch seine Wirkung auf die m-te Einheitswurzel ζ vollständig festgelegt (da diese den Körper erzeugt $\mathbb{Q}(\sqrt[m]{1})$). Weiter bildet jeder Automorphismus des Körpers $\mathbb{Q}(\sqrt[m]{1})$ die m-te Einheitswurzel ζ wieder in eine primitive m-te Einheitswurzel

$$\zeta^a, \; ggT(a, m) = 1,$$

ab. Es reicht deshalb, die folgende Implikation zu beweisen.

$$\zeta^a \equiv \zeta^b \pmod{p} \Rightarrow \zeta^a = \zeta^b$$

Zum Beweis dieser Implikation genügt es die folgende zu beweisen.

(3) $$1 - \zeta^b \equiv 0 \pmod{p} \Rightarrow \zeta^b = 1.$$

Erster Beweis von (3). Angenommen, es gilt $\zeta^b \neq 1$. Es gilt

$$x^m - 1 = \prod_{i=1}^{m} (x - \zeta^i).$$

Wir differenzieren nach x und erhalten nach der Produktregel

$$mx^{m-1} = \sum_{j=1}^{m} \prod_{i \neq j} (x - \zeta^i).$$

Wir setzen im letzten Ausdruck x=1. Dadurch werden alle Summanden bis auf denjenigen mit j=m gleich Null und wir erhalten

$$m = \prod_{i=1}^{m-1} (1 - \zeta^i).$$

Unter den Faktoren dieser Produktzerlegung kommt $1-\zeta^b$ vor (wegen $\zeta^b \neq 1$), d.h. die Differenz $1-\zeta^b$ ist im Ring der ganzen Zahlen $\mathcal{O}$ von $\mathbb{Q}(\sqrt[m]{1})$ ein Teiler von . Da m zu p nach Voraussetzung teilerfremd ist (d.h. mit m gemeinsam das Einheitsideal erzeugt), erzeugen auch $1-\zeta^b$ und p gemeinsam das Einheitideal. Dann kann aber p kein Teiler von $1-\zeta^b$ sein (denn dann würden diese Element gemeinsam das Ideal $p\mathcal{O}$ erzeugen).

Zweiter Beweis von (3).

Betrachten wir die p-adische Vervollständigung $\mathbb{Q}_p$ von $\mathbb{Q}$ und bilden die Erweiterung

$$K := \mathbb{Q}_p(\sqrt[m]{1}).$$

Bezeichne L den Restklassenkörper dieses Körpers (genauer, den Restklassenkörper der ganzen Abschließung von $\mathbb{Z}_p$ in K, d.h. den Bewertungsring $\mathcal{O}_p$ der auf K fortgesetzen p-adischen Bewertung). Dann ist L eine endlich erzeugte algebraische Erweiterung von

$$k_p := \mathbb{Z}_p/(p) = \mathbb{Z}/(p)$$

(und damit ein endlicher Körper). Da Erweiterungen endlicher Körper normal sind, ist damit L gerade der Zerfällungskörper von

(4) $$x^m - 1$$

über k_p. Die Komposition

(5) $$\mathbb{Z}_p[\zeta] \subseteq \mathcal{O}_p \to L$$

bildet die Nullstellen von (4) in K ab in Nullstellen von (4) in L. Die Nullstellen von (4) in L sind paarweise verschieden. Nach dem Henselschen Lemma kommt jede dieser Nullstellen in L von einer Nullstelle von (4), die in $\mathcal{O}_p$ liegt. Die Abbildung (5) induziert also eine Bijektion der Nullstellen von (4) in K mit denen in L. Insbesondere ist diese Abbildung injektiv, d.h. es gilt die Implikation (3).

QED.

Bemerkung

Aus dem 2. und 3. Schritt ergibt sich, daß die Erweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[m]{1})$$

in den zu m teilerfremden Primzahlen p unverzweigt ist.

3.1.7 Totale Verzweigung im Primteiler von $m = p^f$

Seien $m = p^f$ eine Primzahlpotenz und ζ eine primitive q-te Einheitswurzel. Dann ist p total verzweigt in $\mathbb{Q}(\sqrt[m]{1})$. Genauer, im Ring $\mathcal{O}$ der ganzen Zahlen von $\mathbb{Q}(\sqrt[m]{1})$ gilt

$$p\mathcal{O} = (1-\zeta)^{\phi(q)}\mathcal{O}.$$

Beweis. Sei $\lambda := 1-\zeta$. Wegen $\zeta^q = 1$ und $\zeta^{q/p} \neq 1$ ist λ Nullstelle des Polynoms

$$F(x) := \frac{(1+x)^q-1}{(1+x)^{q/p}-1} = (1+x)^{q(p-1)/p} + (1+x)^{q(p-2)/p} + \ldots + 1.$$

Dieses Polynom hat den höchsten Koeffizienten 1 und das Absolutglied F(0) = p. Alle weiteren Koeffizienten sind durch p teilbar. Mit anderen Worten, F ist ein Eisensteinpolynom, d.h. die Erweiterung

$$\mathbb{Q}_p \subseteq \mathbb{Q}_p(\sqrt[q]{1})$$

ist eine total verzweigte Erweiterung (nach 1.6.4) des Grades $\Phi(q)$ und λ ist ein Element der Ordnung 1 in $\mathbb{Q}_p(\sqrt[q]{1})$. Insbesondere ist

$$p\mathcal{O}_p = (\lambda)^{\phi(q)}\mathcal{O}_p$$

im (lokalen) Ring $\mathcal{O}_p$ der ganzen Zahlen von $\mathbb{Q}_p(\sqrt[q]{1})$. Wir gehen zur Erweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[q]{1})$$

über und sehen, diese Erweiterung muß mindestens den Grad $\Phi(q)$ haben[75]. Da ihr Grad höchsten $\Phi(q)$ muß er gleich $\Phi(q)$ sein und über dem Primideal (p) von $\mathbb{Z}$ liegt nur ein einziges Primideal. Wir haben gezeigt, die gebrochenen Ideale

(1) $$p\mathcal{O} \text{ und } (\lambda)^{\phi(q)}\mathcal{O}$$

stimmen in der einzigen über (p) liegenden Primstelle überein. Wir haben noch zu zeigen, daß sie auch an allen übrigen Primstellen P von $\mathcal{O}$ übereinstimmen. Ein nicht über (p) liegendes Primideal liegt notwendig über einer von p verschiedenen Primzahl p'. An einer solchen Stelle ist das Ideal $p\mathcal{O}$ notwendig trivial[76],

$$p\mathcal{O}_P = \mathcal{O}_P.$$

Es reicht zu zeigen, daß dies auch für das zweite Ideal von (1) der Fall ist. Es gilt in $\mathcal{O}$

$$1 = (1-\lambda)^q = 1 + \binom{q}{1}\lambda + \binom{q}{2}\lambda^2 + \ldots = 1 + q\lambda + a\lambda^2$$

für ein $a \in \mathcal{O}$, also

$$\lambda(q-\lambda a) = 0$$

Weil $\mathcal{O}$ nullteilerfrei ist, folgt

$$\lambda a = q$$

Als p-Potenz ist q eine Einheit in $\mathcal{O}_P$, also ist auch λ eine Einheit in diesem Ring,

$$\lambda\mathcal{O}_P = \mathcal{O}_P.$$

QED.

Alternativer (direkterer) Beweis. Für ganze Zahlen a, b mit

$$ggT(a,p) = ggT(b,p) = 1$$

ist die Kongruenz

$$a \equiv bs \pmod q$$

lösbar. Also ist

---

[75] Wir verwenden hier die Formel

$$[L:K] = \sum_P e(P)f(P)$$

wobei über die Primideale P von L summiert wird, die über einem gegebenen Primideal p von K liegen.

[76] Es gibt ganze Zahlen a und b mit $ap + bp' = 1$, d.h. $ap - 1 \in (p') \subseteq P$. Also liegt ap nicht in P, also ist ap eine Einheit in $\mathcal{O}_P$, also ist auch p eine solche.

$$\frac{1-\zeta^a}{1-\zeta^b} = \frac{1-\zeta^{bs}}{1-\zeta^b} = 1 + \zeta^b + \zeta^{2b} + ... + \zeta^{b(s-1)}$$

ein Element von $\mathcal{O}$. Aus Symmetriegründen ist damit auch

$$\frac{1-\zeta^b}{1-\zeta^a}$$

ein Element von $\mathcal{O}$. Für je zwei zu p teilerfremde ganze rationale Zahlen ist also

$$\frac{1-\zeta^a}{1-\zeta^b}$$

eine Einheit von $\mathcal{O}$. Weiter gilt

$$p = \lim_{x\to 1} \frac{x^q-1}{x^{q/p}-1}$$

$$= \lim_{x\to 1} \prod_{a\in(\mathbb{Z}/(q))^*} (x-\zeta^a) \qquad \text{(genau die prim. q-ten EW sind Nullst.)}$$

$$= \prod_{a\in(\mathbb{Z}/(q))^*} (1-\zeta^a)$$

$$= (1-\zeta)^{\Phi(q)} \prod_{a\in(\mathbb{Z}/(q))^*} \frac{1-\zeta^a}{1-\zeta}$$

Da die Elemente unter dem Produktzeichen Einheiten in $\mathcal{O}$ sind, erzeugen die Elemente p und $(1-\zeta)^{\Phi(q)}$ in $\mathcal{O}$ dasselbe Ideal.
QED.

3.1.8 Unverzweigtheit von $\mathbb{Q}(\sqrt[m]{1})$ in den zu m teilerfremden Stellen, der Relativgrad

Seien ζ ein primitive m-te Einheitswurzel und p eine zu m teilerfremde Primzahl. Dann ist p im Körper $\mathbb{Q}(\sqrt[m]{1})$ unverzweigt und der Relativegrad f_p ist gleich der kleinsten ganzen Zahl $f\geq 1$ mit $p^f \equiv 1 \pmod m$.
Beweis (nach Serre, Corps locaux, Hermann Paris 1962). Betrachten wir die Erweiterung

$$\mathbb{Q}_p \subseteq \mathbb{Q}_p(\zeta).$$

Der Restklassenkörper $\mathbb{F}_p$ von $\mathbb{Q}_p$ besteht aus p Elementen. Das Polynonom x^m-1 zerfällt über dem endlichen Erweiterungskörper

$$\mathbb{F}_q \text{ mit } q:=p^f$$

genau dann in Linearfaktoren, wenn $\mathbb{F}_q^*$ die Untergruppe μ_m der m-ten Einheitswurzeln enthält, d.h. wenn

$$m = \#\mu_m \mid \#\mathbb{F}_q^* = p^f-1$$

gilt[77]. Sei f jetzt die kleinste natürliche Zahl mit

$$(q:=)\ p^f \equiv 1 \pmod m.$$

Dann gibt es nach 1.7.5 eine unverzweigte Erweiterung

$$\mathbb{Q}_p \subseteq L,$$

deren Restklassenkörper gerade $\mathbb{F}_q$ ist. Wie in der zweiten Variante des Beweises von 3.1.6 betrachten wir die Komposition natürlicher Abbildungen

$$(L \supseteq)\ \mathcal{O} \to \mathbb{F}_q$$

und beachten, daß diese Abbildung eine Bijektion[78] der Nullstellen von x^m-1 in $\mathcal{O}$ und $\mathbb{F}_q$ induziert. Da x^m-1 nach Konstruktion über $\mathbb{F}_q$ in Linearfaktoren zerfällt, gilt dasselbe über $\mathcal{O}$ und L. Da $\mathbb{F}_q$ kleinste Erweiterung von $\mathbb{F}_p$ ist, über welcher x^m-1 in Linearfaktoren zerfällt, ist L die kleinste Erweiterung von $\mathbb{Q}_p$ mit dieser Eigenschaft[79]. Mit anderen Worten, es gilt

$$L = \mathbb{Q}_p(\zeta).$$

Damit ist gezeigt, die Erweiterung $\mathbb{Q}(\zeta)$ ist in p über $\mathbb{Q}$ unverzweigt und der Grad der Restklassenerweiterung ist gleich der im Satz beschriebenen Zahl f_p.

QED.

3.1.9 Die in $\mathbb{Q}(\sqrt[m]{1})$ vollständig zerfallenden Primzahlen

Sei p eine zu m teilerfremde Primzahl. Dann sind folgende Aussagen äquivalent.

(i) p zerfällt in $\mathbb{Q}(\sqrt[m]{1})$ vollständig (in ein Produkt von $[\mathbb{Q}(\sqrt[m]{1}):\mathbb{Q}]$ teilerfremden Primidealen).
(ii) $p \equiv 1 \pmod m$.

Beweis. (ii) ⇒ (i). Nach 3.1.8 sind Verzweigungsindex und Relativgrad der Erweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[m]{1})$$

gleich 1. Auf Grund der Formel

$$[L:K] = \sum_{P|p} e(P)f(P) \tag{1}$$

liegen über p gerade $[\mathbb{Q}(\sqrt[m]{1}):\mathbb{Q}]$ Primideale P, d.h. es gilt (i).
(i) ⇒ (ii). Vollständiges Zerfallen von p ist auf Grund der Formel nur möglich, wenn für jedes über p liegende Primideal P gilt

$$e(P) = f(P) = 1.$$

---

[77] Die Bedingung ist auch hinreichend, denn $\mathbb{F}_q^*$ ist zyklisch und wird von einer (q-1)-ten primitiven Einheitswurzel erzeugt, enthält also, wenn die Teilbarkeitsbedingung erfüllt ist, auch eine primitive m-te Einheitswurzel.

[78] Nach dem Henselschen Lemma liegt über jeder Nullstelle in $\mathbb{F}_q$ eine Nullstelle in $\mathcal{O}$.

[79] Zunächst ist L erst einmal die kleinste unverzweigte Erweiterung, über welcher x^m-1 in Linearfaktoren zerfällt (wegen der in 1.7.5 beschriebenen Äquivalenz von Kategorien). Gäbe es eine noch kleinere Erweiterung, so läge diese ganz in L, wäre also auch unverzweigt und müßte damit gleich L sein.

Die Erweiterung muß also über p unverzweigt[80] sein und den Relativgrad 1 haben. Die Unverzweigtheit impliziert (nach 3.1.7), daß p teilerfremd zu m sein muß. Nach 3.1.8 muß dann aber (ii) gelten.
QED.

3.1.10 Die Diskriminante von $\mathbb{Q}(\sqrt[m]{1})$ im Fall $m = p^t$

Seien p eine Primzahl, $m = p^t$ eine Potenz von p und ζ eine primitive m-te Einheitswurzel. Dann ist die Diskriminante der Erweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[m]{1})$$

gleich $\frac{m^{\phi(m)}}{p^{m/p}}$. Der $\mathbb{Z}$-Modul der ganzen Elemente von $\mathbb{Q}(\sqrt[m]{1})$ hat die Basis

$$1, \zeta, \zeta^2, \ldots, \zeta^{\Phi(m)-1}.$$

Beweis. 1. Schritt. Der Fall t=1.
Offensichtlich gilt

(1) $$M := \mathbb{Z}[\zeta] \subseteq \mathcal{O},$$

wenn $\mathcal{O}$ den Ring der ganzen Zahlen von $\mathbb{Q}(\zeta)$ bezeichnet. Das Minimalpolynom ζ über $\mathbb{Q}$ ist

$$f(x) := \frac{x^p-1}{x-1} = x^{p-1}+x^{p-2}+\ldots+x+1,$$

d.h. M ist gerade der von $1, \zeta, \zeta^2, \ldots, \zeta^{\Phi(q)-1}$ erzeugte freie $\mathbb{Z}$-Modul und es reicht folgendes zu zeigen.

1. In (1) gilt das Gleichheitszeichen.
2. Die Diskriminante der Erweiterung ist p^{p-2}

Wegen der Inklusion (1) gilt nach 1.3.12(iv) die analoge Inklusion zwischen den Diskriminanten dieser Moduln und die Gleichheit in (1) ist äquivalent zur Gleichheit der Diskriminanten. Deshalb reicht es zu zeigen,

(2) $$\delta(\mathcal{O}) = \delta(M) = p^{p-2}\mathbb{Z}.$$

Es gilt nach 1.4.16

$$\delta(M) = N(f'(\zeta))\mathbb{Z}$$

und nach Definition von f ist $f(x) = \prod_a (x-\zeta^a)$, wobei a ein primes Restesystem modulo p durchlaufe. Wir differenzieren, wenden die Produktregel an und setzen $x=\xi$,

$$\begin{aligned} f'(\zeta) &= \prod_{1<a<p} (\zeta-\zeta^a) \\ &= \zeta^{p-2} \prod_{1<a<p} (1-\zeta^{a-1}) \\ &= (1-\zeta)^{p-2} \zeta^{p-2} \prod_{1<a<p} \frac{1-\zeta^{a-1}}{1-\zeta} \end{aligned}$$

Man beachte, die Argumente im zweiten Beweis von 3.1.7 zeigen, daß die Ausdrücke unter dem Produktzeichen Einheiten von $\mathcal{O}$ sind. Ihre Normen sind also Einheiten von $\mathbb{Z}$. Dasselbe gilt für ζ. Wir erhalten damit

---

[80] Die Separabilität der Restklassenkörpererweiterung ist gewährleistet, da die Restklassenkörper endlich sind.

$$N(f'(\zeta))\mathbb{Z} = N(1-\zeta)^{p-2}\mathbb{Z}.$$

also

$$\delta(M) = N(1-\zeta)^{p-2}\mathbb{Z}$$

Nach 3.1.7 ist nun $p\mathcal{O} = (1-\zeta)^{p-1}\mathcal{O}$, also

$$N(1-\zeta)^{p-1}\mathbb{Z} = N(p)\mathbb{Z} = p^{[\mathbb{Q}(\sqrt[p]{1}):\mathbb{Q}]}\mathbb{Z} = p^{\Phi(p)}\mathbb{Z} = p^{p-1}\mathbb{Z},$$

also $N(1-\zeta)\mathbb{Z} = p\mathbb{Z}$, also

$$\delta(M) = p^{p-2}\mathbb{Z}$$

Damit ist das rechte Gleichheitszeichen von (2) bewiesen. Wir haben noch zu zeigen,

(3) $$\delta(\mathcal{O}) = p^{p-2}\mathbb{Z}.$$

Zeigen wir diese Identität lokal. Nach 3.1.7 und 3.1.8 ist p die einzige Primzahl, in welcher $\mathbb{Q}(\zeta)$ verzweigt ist, d.h. (3) gilt in allen von p verschiedenen Primzahlen (auf beiden Seiten steht das Einsideal). Nach 3.1.7 ist der Verzweigungsindex von p in $\mathbb{Q}(\zeta)$ gerade $\Phi(p) = p-1$, d.h. an der Stelle p gilt

$$e := e(\mathbb{Q}(\zeta):\mathbb{Q}) = p-1 = [\mathbb{Q}(\zeta):\mathbb{Q}]$$
$$f := f(\mathbb{Q}(\zeta):\mathbb{Q}) = 1$$

Die Verzweigung an der Stelle p ist zahm und der Relativindex ist 1. Auf Grund des Kriteriums 1.5.15 für zahm verzweigte Erweiterungen hat die Differente an der Stelle p den Wert

$$v_L(\mathcal{O}) = e - 1 = p-2, \quad L := \mathbb{Q}_p(\zeta)$$

Für den Wert der Diskriminante[81] erhalten wir damit

$$v_{\mathbb{Q}_p}(\delta) = v_{\mathbb{Q}_p}(N(\mathcal{D})) = \frac{1}{e}\cdot v_L(N(\mathcal{D})) = \frac{ef}{e}\cdot v_L(\mathcal{D}) = f\cdot(p-2) = p-2,$$

d.h. (3) gilt auch an der Stelle p.

2. Schritt. $t \geq 2$.

Nach 3.1.8 ist die Erweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[m]{1})$$

wiederum unverzweigt in allen von p verschiedenen Primzahlen. Der Verzweigungsindex in p ist nach 3.1.7 gleich

$$e = \Phi(m) = \Phi(p^t) = (p-1)p^{t-1},$$

d.h. die Verzweigung ist wild (d.h.nicht zahm). Da p die einzige Stelle ist, in der die Erweiterung verzweigt ist, wird die Diskriminante von einer Potenz von p erzeugt, wobei der Exponent mindestens $\Phi(m)$ ist[82],

(4) $$\delta := \delta(\mathcal{O}) \subseteq p^{\Phi(m)}\mathbb{Z}.$$

Wir geben einen direkten Beweis, daß der Ring $\mathcal{O}$ der ganzen Zahlen von $\mathbb{Q}(\sqrt[m]{1})$ von den angegebenen Potenzen von ζ als $\mathbb{Z}$-Modul erzeugt wird. Da das Minimalpolynom

---

[81] Wir benutzen die Tatsache, daß die Diskriminante die Norm der Differente ist (vgl. 1.4.14).

[82] Da die Diskriminante $\delta = N(\mathcal{D})$ gleich der Norm der Differente ist, gilt

$$v_p(\delta) = \frac{1}{e}v_L(N(\mathcal{D})) \geq f\cdot v_L(\mathcal{D}) > f(e-1) \geq e-1.$$

Das line Größergleichzeichen ergibt sich aus der Formel $\sum e_i f_i$ = Körpergrad. Das Größerzeichen rechts davon gilt nach 1.5.11 und 1.5.15 (weil die Verzweigung nicht zahm ist). Der Körper L sei hier die Vervollständigung von $\mathbb{Q}(\sqrt[m]{1})$ in der p-adischen Topologie.

von ζ über $\mathbb{Q}$ den Grad $\Phi(m)$ hat (vgl. 3.1.5), ist das äquivalent zu der Identität $\mathcal{O}=\mathbb{Z}[\zeta]$. Trivialerweise gilt

(5) $$\mathbb{Z}[\zeta] \subseteq \mathcal{O}.$$

Für die Diskriminante von $\mathbb{Z}[\zeta]$ erhalten wir (nach einer längeren Rechnung)[83]

(6) $$\delta(\mathbb{Z}[\zeta]) = \frac{m^{\Phi(m)}}{p^{m/p}}.$$

---

[83] Wie im ersten Schritt erhalten wir (vgl. 1.4.16)

$$\delta(\mathbb{Z}[\zeta]) = N(f'(\zeta))\mathbb{Z},$$

wenn f das Minimalpolynom von ζ bezeichnet. Analog zum ersten Schritt ist

$$\begin{aligned} f'(\zeta) &= \prod_{1<a<p^t,(a,p)=1} (\zeta-\zeta^a) \\ &= \zeta^{\Phi(m)-1} \prod_{1<a<p^t,(a,p)=1} (1-\zeta^{a-1}) \\ &= (1-\zeta)^{\Phi(m)-1}\, \zeta^{\Phi(m)-1} \prod_{1<a<p} \frac{1-\zeta^{a-1}}{1-\zeta} \end{aligned}$$

Im Gegensatz zum ersten Schritt ist sind die Quotienten unter dem Summenzeichen nicht mehr notwendig Einheiten in $\mathcal{O}$, und zwar dann nicht, wenn a-1 nicht mehr teilerfremd zu p ist, d.h. für

$$a = p\cdot b + 1,\ b = 1,\ldots,p^{t-1}-1\ (=m/p - 1).$$

Wir erhalten damit immerhin noch

$$\begin{aligned} N(f'(\zeta))\mathbb{Z} &= N(1-\zeta)^{\Phi(m)-1}.\prod_{b=1}^{\frac{m}{p}-1} N\left(\frac{1-\zeta^{pb}}{1-\zeta}\right)\cdot\mathbb{Z} \\ &= N(1-\zeta)^{\Phi(m)-m/p}\cdot N\left(\prod_{b=1}^{\frac{m}{p}-1} 1-\zeta^{pb}\right)\cdot\mathbb{Z} \end{aligned}$$

Die ζ-Potenzen, die unter dem Produktzeiche vorkommen, sind gerade alle nicht-primitiven von 1 verschiedenen m-ten Einheitswurzeln, d.h. alle Nullstellen von

$$\frac{x^{m/p}-1}{x-1} = x^{m/p-1}+x^{m/p-2}+\ldots+1$$

An der Stelle 1 hat dieses Polynom den Wert m/p. Deshalb gilt

$$\begin{aligned} N(f'(\zeta))\mathbb{Z} &= N(1-\zeta)^{\Phi(m)-m/p}.N(m/p)\cdot\mathbb{Z} \\ &= N(1-\zeta)^{\Phi(m)-m/p}.\left(\frac{m}{p}\right)^{\Phi(m)}.\mathbb{Z} \end{aligned}$$

Nach 3.1.7 ist nun $p\mathcal{O} = (1-\zeta)^{\Phi(m)}\mathcal{O}$, also

$$N(1-\zeta)^{\Phi(m)}\mathbb{Z} = N(p)\mathbb{Z} = p^{[\mathbb{Q}(\sqrt[p]{1}):\mathbb{Q}]}\mathbb{Z} = p^{\Phi(p)}\mathbb{Z},$$

Also $N(1-\zeta)\mathbb{Z} = p\mathbb{Z}$, also

$$\begin{aligned} N(f'(\zeta))\mathbb{Z} &= p^{\Phi(m)-m/p}.\left(\frac{m}{p}\right)^{\Phi(m)}.\mathbb{Z} \\ &= m^{\Phi(m)}.p^{-m/p}.\mathbb{Z}, \end{aligned}$$

d.h. es gilt Formel (6).

Damit ist der Beweis der Behauptung auf den Nachweis des Gleichheitszeichens in (5) reduziert. Wäre die Inklusion (5) echt, so würde es eine Linearkombination der Potenzen

(7) $$1, \zeta, \zeta^2, \ldots, \zeta^{\Phi(m)-1}.$$

geben, welche in $\mathcal{O}$ liegt, jedoch nicht in $\mathbb{Z}[\zeta]$, d.h. die Linearkombination ist ganz über $\mathbb{Z}$, die Koeffizienten selbst sind aber nicht alle aus $\mathbb{Z}$. Da die Diskriminanten von $\mathbb{Z}[\zeta]$ und $\mathcal{O}$ von p-Potenzen erzeugt werden, gilt in (5) das Gleichheitszeichen in allen von p verschiedenen Primstellen. Der Hauptnenner der Koeffizienten der betrachteten Linearkombination ist also eine p-Potenz. Die Echtheit der Inklusion (5) ist deshalb äquivalent zu der folgenden Aussage.

(8) Es gibt eine ganzzahlige Linearkombination der Potenzen (7), welche in $\mathcal{O}$ ein p-Vielfaches ist, ohne daß die Koeffizienten der Linearkombination sämtlich p-Vielfache sind.

Wir haben zu zeigen, daß (8) nicht gilt. Mit den Potenzen (7) bilden auch die entsprechenden Potenzen von $1-\zeta$ eine Basis von $\mathbb{Z}[\zeta]$. Deshalb benügt es, die folgende Aussage zu beweisen.

(9) Ist $\sum_{i=0}^{\Phi(m)-1} a_i(1-\zeta)^i$ mit $a_i \in \mathbb{Z}$ in $\mathcal{O}$ ein p-Vielfaches, so sind sämtliche a_i in $\mathbb{Z}$ durch p teilbar.

Wir zeigen jetzt induktiv, daß sämtliche Koeffizienten a_i durch p teilbar sind.

Angenommen, wir wissen bereits, daß $a_1,\ldots,a_s$ ganzzahlige Vielfache von p sind. Dann gilt wegen $p\mathcal{O} = (1-\zeta)^{\Phi(m)}\mathcal{O}$ (vgl. 3.1.7) in $\mathcal{O}$,

$$(1-\zeta)^{\Phi(m)} \mid \sum_{i=s+1}^{\Phi(m)-1} a_i(1-\zeta)^i,$$

d.h. es gibt ein $a \in \mathcal{O}$ mit

$$a\cdot(1-\zeta)^{\Phi(m)} + \sum_{i=s+1}^{\Phi(m)-1} a_i(1-\zeta)^i = 0.$$

Wir können auf der linken Seite den Faktor $(1-\zeta)^{s+1}$ ausklammern und diesen Faktor kürzen und erhalten so

$$a\cdot(1-\zeta)^{\Phi(m)-s-1} + a_{s+1} + a_{s+2}\cdot(1-\zeta) + \ldots = 0.$$

Der Koeffizient a_{s+1} ist also in $\mathcal{O}$ durch $1-\zeta$ teilbar. Durch Übergang zu den Normen erhalten wir

$$p \mid N(a_{s+1}) = a_{s+1}^{\Phi(m)},$$

d.h. p teilt a_{s+1}. Damit ist (9) und mit (9) der Satz bewiesen.

QED.

3.1.11 Die Diskriminante von $\mathbb{Q}(\sqrt[m]{1})$ für beliebiges m

Seien m eine positive ganze Zahl und ζ eine primitive m-te Einheitswurzel. Dann gelten die folgenden Aussagen.

(i) Die Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[m]{1})$$

hat den Grad $\Phi(m)$ und die Diskriminante

$$\delta = \frac{m^{\Phi(m)}}{\prod_{p|m} p^{\Phi(m)/(p-1)}}.$$

(ii) Der Ring der ganzen Zahlen von $\mathbb{Q}(\sqrt[m]{1})$ ist gerade der freie $\mathbb{Z}$-Modul mit der Basis

$$1, \zeta, \zeta^2, \ldots, \zeta^{\Phi(m)-1}$$

(iii) Die Primzahl p ist genau dann verzweigt in $\mathbb{Q}(\sqrt[m]{1})$, wenn sie m teilt[84].

Vorbemerkung.
Der größte Teil der obigen Aussage wurde bereits bewiesen. Die Aussage über den Grad der Erweiterung findet sich in 3.1.5. Ist p kein Teiler von m, ist p nach 3.1.8 unverzweigt in $\mathbb{Q}(\sqrt[m]{1})$. Wird m dagegen von p geteilt, so ist p bereits in einer Teilerweiterung von $\mathbb{Q}(\sqrt[m]{1})$ verzweigt (siehe 3.1.7)[85]. Es bleiben also nur noch die Aussagen über die Diskriminante und über die $\mathbb{Z}$-Modulbasis von $\mathcal{O}$ zu beweisen. Wie die vorangehenden Betrachtungen nahelegen sind diese beiden Aussagen im wesentlichen äquivalent. Sie können auch direkt bewiesen werden (vgl. Chap. 7, §5 in Weiss, E.: Algebraic number theory, McGraw Hill, New York 1963).
Beweis.

QED.

3.2 Kummer-Erweiterungen

3.3. Anhang: Der Satz von Kummer

3.3.1 Die Situation

Innerhalb dieses Anhangs benutzen wir folgende Bezeichnungen.

K	ein algebraischer Zahlenkörper.
$\mathcal{O}$	der Ring der ganzen Zahlen von K.
θ	ein über K ganzes Element, dessen Minimalpolynom über K den Grad n hat.
$f \in \mathcal{O}[x]$	das Minimalpolynom von θ über K.
$L = K(\theta)$	die von θ erzeugte Erweiterung (des Grades n) von K.
$\mathcal{P}$	ein maximale Ideal von $\mathcal{O}$.
v	die durch $\mathcal{P}$ definierte Bewertung von K.
$K_{\mathcal{P}}$	die Vervollständigung von K bezüglich der Bewertung v.

---

[84] Man beachte die nachfolgende Fußnote zum Fall p=2, wobei p in m nicht quadratisch vorkommt.
[85] Ein Sonderfall, der von 3.1.7 ist der Fall p = 2, wobei p in m nicht quadratisch vorkommt. Nun ist die primitive zweite Einheitswurzel gleich -1. Die zugehörige Kreisteilungserweiterung ist trivial. Auf Grund von 3.1.3 ändert sich der $\mathbb{Q}(\sqrt[m]{1})$ nicht, wenn man m durch $\frac{m}{2}$ ersetzt. Da $\frac{m}{2}$ nicht mehr durch 2 teilbar ist, ist 2 in $\mathbb{Q}(\sqrt[m]{1})$ unverzweigt.

$k_{\mathfrak{p}}$ der Restklassenkörper von $K_{\mathfrak{p}}$.[86]

$\mathcal{P} = \prod_j \mathfrak{q}_j^{e_j}$ die Primfaktorzerlegung von $\mathcal{P}$ in L.

v_j die durch $\mathfrak{q}_j$ in L definierte Bewertung.

L_j die Vervollständigung von L bezüglich v_j.

$\mathcal{O}_j$ der Ring der ganzen Zahlen von L_j.

k_{L_j} der Restklassenring von L_j.[87]

$\bar{g}$ das Polynom über k_{L_j}, welches man aus $g \in \mathcal{O}[x]$ erhält, indem man die Koeffizienten durch deren Restklassen ersetzt.

3.3.2 Bemerkung zum Ziel des Abschnitts

...

3.3.3 Ein Lemma

3.3.4 Satz von Kummer

Wir verwenden die Bezeichnungen von 3.3.1. Seien das Ideal $\mathcal{P}$ und das Element θ so gewählt, daß das Element

$$\sum_{i=0}^{n-1} a_i \theta^i \in K[\theta]$$

genau dann ganz ist über K, wenn $v(a_i) \geq 0$ gilt für alle $i = 0,...,n-1$. Weiter sei

$$\bar{f}(x) = \prod_j \bar{G}_j(x)^{e_j}$$

die Zerlegung von $\bar{f}(x)$ in paarweise teilerfremde irreduzible Faktoren in $k_{\mathfrak{p}}[x]$ und

$$G_j(x) \in \mathcal{O}[x]$$

ein unitäres Polynom, welches das Polynom $\bar{G}_j(x)$ repräsentiert. Dann hat die Primfaktorzerlegung von $\mathcal{P}$ in L die folgende Gestalt.

$$\mathcal{P} = \prod_j \mathfrak{q}_j^{e_j} \text{ mi t } \mathfrak{q}_j = (\mathcal{P}, G_j(\theta)).$$

Literatur zu Kapitel 3

[1] Weiss, E.: Algebraic number theory, McGraw Hill, New York, 1963.
[2] Weyl, H.: Algebraic theory of numbers, Annals of Math. Studies, Princeton 1940
[3] Serre, J.-P.: Corps loceaux, Hermann, Paris 1962

---

[86] Im Original wird die Bezeichnung $K_{\mathfrak{p}}^*$ benutzt, im Gegensatz zur bisherigen Art, den Restklassenkörper zu bezeichnen.

[87] Im Original L_j^*

Bezeichnungen

G	eine Gruppe, im Zusammenhang mit den Tate-Gruppen stets endlich
M,M', N,...	G-Moduln

4. Gruppenkohomologie (M. Atiyah, K. Wall)

4.1. Definition der Kohomologie

4.1.1 G-Moduln

Seien G eine Gruppe, und $\Lambda := \mathbb{Z}[G]$ die ganzzahlige Gruppenalgebra von G.

Ein (linker) G-Modul soll im folgenden einfach ein (linker) Λ-Modul sein. Wir werden fast ausschließlich linke Moduln betrachten. Durch die Vorschrift

$$M \times G \to M,\ (m,g) \mapsto g^{-1}m,$$

ist aber auf jedem linken G-Modul auch eine rechte G-Modulstruktur definiert, so daß dies keine Einschränkung der Allgemeinheit bedeutet. Umgekehrt besitzt auch jeder rechte G-Modul M die Struktur eines linken G-Moduls bezüglich der Multiplikation

$$G \times M \to M\ (g, m) \mapsto mg^{-1}.$$

4.1.2 Morphismen von G-Moduln

Ein Morphismus $f: M \to N$ von G-Moduln ist einfach eine Λ-lineare Abbildung. Die Menge aller G-Modul-Homomorphismen $M \to N$ werde mit

$$\mathrm{Hom}_G(M,N)$$

bezeichnet. Sie ist eine Untergruppe in der Gruppe

$$\mathrm{Hom}(M,N)$$

aller Gruppenhomomorphismen $M \to N$. Für G-Moduln M und N hat Hom(M,N) die Struktur eines G-Moduls mit der Operation

$$G \times \mathrm{Hom}(M,N) \to \mathrm{Hom}(M,N),\ (g,f) \mapsto g \circ f \circ g^{-1}.$$

Wir habe hier das Gruppenelement g mit der Abbildung $N \to N$, $n \mapsto gn$ identifiziert.

Beispiel

$$\mathrm{Hom}(\mathbb{Z}, M) = M$$

wenn man $\mathbb{Z}$ als G-Modul mit der trialen Operation betrachtet.

4.1.3 Invariante Elemente

Seien G eine Gruppe und M eine Untergruppe. Dann bezeichne

$$M^G := \{m \in M \mid gm = m \text{ für alle } g \in G\}$$

die Untergruppe der G-invarianten Elemente von M. Die ist wieder ein G-Modul, auf dem G trivial operiert.

Beispiel

$$\mathrm{Hom}(M,N)^G = \mathrm{Hom}_G(M,N)$$

Beispiel

$$\mathrm{Hom}_G(\mathbb{Z},M) = \mathrm{Hom}(\mathbb{Z},M)^G = M^G$$

4.1.4 Linksexaktheit

Da der Hom-Funktor linksexakt ist, folgt aus der letzten Isomorphie, daß der Übergang zu den G-invarianten Elementen ein linksexakter Funktor

$$\text{G-Mod} \to \text{Ab},\ M \mapsto M^G$$

ist, d.h. für jede kurze exakte Sequenz von G-Moduln

$$0 \to M' \to M \to M'' \to 0$$

ist die zugehörige Sequenz

$$0 \to M'^G \to M^G \to M''^G$$

4.1.5 Koinduzierte Moduln

Seien G eine Gruppe und X ein beliebige abelsche Gruppe. Dann hat

$$\mathrm{Hom}(\Lambda, X)$$

in natürlicher Weise die Struktur eines G-Moduls.[88] Ein G-Modul dieser Gestalt heißt koinduziert.

4.1.6 Definition: kohomologische Erweitung des Funktors $M \mapsto M^G$

Unter einer kohomologischen Erweiterung der Funktors

$$\text{G-Mod} \to \text{Ab},\ M \mapsto M^G$$

versteht man eine Folge von Funktoren

$$\text{G-Mod} \to \text{Ab},\ M \mapsto H^q(G,M),$$

(q=0,1,2,3,...) zusammen mit einem sogenannten Zusammenhangshomomorphismus

$$\delta\colon H^q(G,M'') \to H^{q+1}(G,M')$$

für jede kurze exakte Sequenz von G-Moduln

(*) $$0 \to M' \to M \to M'' \to 0,$$

und jedes $q \in \mathbb{N}$, wobei folgenden Bedingungen erfüllt sind.

1. $H^0(G,M) = M^G$.
2. $H^q(G,M) = 0$ für $q>0$ und M koinduziert.
3. Für jede kurze exakte Sequenz (*) von G-Moduln ist die folgende zugehörige Sequenz exakt (und heißt lange Homologiesequenz von (*)).

$$\ldots \to H^q(G,M') \to H^q(G,M) \to H^q(G,M'') \xrightarrow{\delta} H^{q+1}(G,M') \to \ldots$$

4. Die lange Homologiesequenz ist funktoriel in (*).

4.1.7 Existenz und Eindeutigkeit der kohomologischen Erweiterung

Sei G eine Gruppe. Dann besitzt der Funktor

$$\text{G-Mod} \to \text{Ab},\ M \mapsto M^G,$$

eine kohomologische Erweiterung. Diese ist eindeutig bestimmt bis auf natürliche Isomoprhie.

Beweis. Existenz. Wir wählen für den G-Modul $\mathbb{Z}$ (versehen mit der trivialen Operation von G) eine Auflösung P durch freie G-Moduln:

$$\ldots \to P_1 \to P_0 \to \mathbb{Z} \to 0$$

und bilden den Komplex

$$K = \mathrm{Hom}_G(P, M),$$

d.h.

$$0 \to \mathrm{Hom}_G(P_0, M) \to \mathrm{Hom}_G(P_1, M) \to \ldots$$

Sei

$$H^q(K)$$

für $q \geq 0$ die q-Kohomologie-Gruppe des Komplexes K. Dann besitzen die Gruppen

$$H^q(G, M) := H^q(K)$$

---

[88] Man verwende 4.1.2 indem man G auf X in trivialer Weise operieren läßt.

die Eigenschaften einer kohomologischen Erweiterung des Funktors $M \mapsto M^G$. Auf Grund des Hauptsatzes der Homologischen Algebra[89] haben die so definierten Gruppen $H^q(G, M)$ die Eigenschaften 3 und 4. Außerdem gilt

$$H^0(G, M) = H^0(K) =^{90} \mathrm{Hom}_G(\mathbb{Z}, M) = M^G,$$

d.h. die $H^q(G, M)$ haben Eigenschaft 1. Wir haben noch Eigenschaft 2 nachzuweisen. Sei M ein koinduzierter G-Modul, d.h.

$$M = \mathrm{Hom}(\Lambda, X)$$

mit einer abelschen Gruppe X. Für jeden G-Modul N besteht dann ein Isomorphismus

$$\mathrm{Hom}_G(N, M) \cong \mathrm{Hom}(N, X),\ N \xrightarrow{\varphi} M \mapsto (n \mapsto \varphi(n)(1)).$$

Der Komplex K bekommt damit die Gestalt

$$0 \to \mathrm{Hom}(P_0, X) \to \mathrm{Hom}(P_1, X) \to \ldots$$

Dieser Komplex ist mit eventueller Ausnahme der 0-ten Stelle exakt, da die P_i freie abelsche Gruppen sind.[91] Also gilt $H^q(G, M) = 0$ für $q > 0$.

Eindeutigkeit. Für jeden G-Modul M sei

$$M^* := \mathrm{Hom}(\Lambda, M).$$

Wir betrachten die natürliche Einbettung

$$M \to M^*,\ m \mapsto \varphi_m \text{ mit } \varphi_m(g) = gm$$

für jedes $g \in G$ und erhalten eine kurze exakte Sequenz von G-Moduln

$$0 \to M \to M^* \to M' \to 0 \tag{4}$$

mit $M' := M^*/M$. Aus Eigenschaft 3 und der Tatsache, daß M^* koinduziert ist, ergibt sich, daß der Zusammenhangshomomorphismus

$$\delta: H^q(G, M') \to H^{q+1}(G, M)$$

ein Isomorphismus ist für jedes $q \geq 1$ und einen Isomorphismus

$$H^1(G, M) \cong \mathrm{Koker}(H^0(G, M^*) \to H^0(G, M')) \tag{5}$$

induziert. Deshalb kann man die $H^q(G, M)$ schrittweise aus den H^0 konstruieren, und deshalb sind diese Gruppen eindeutig bestimmt bis auf natürliche Isomorphie. Man kann diese Konstruktion für eine induktive Definition der Gruppen $H^q(G, M)$ verwenden.

QED.

4.1.8 Definition: Gruppen-Kohomologie

Seien G eine Gruppe und M ein G-Modul. Die nach 4.1.7 eindeutig festgelegten Gruppe

$$H^q(G, M)$$

heißt q-te Kohomologie-Gruppe des G-Moduls M.

4.1.9 Bemerkung: Unabhängigkeit von der Wahl der speziellen Resolvente

Aus der Eindeutigkeitsaussage von 4.1.7 folgt, daß die Gruppen $H^q(G, M)$ nicht von der Wahl der speziellen Resolvente P von $\mathbb{Z}$ abhängen, die zur Konstruktioin dieser Gruppen verwendet wurde.

---

[89] Auf Grund des Vergleichssatzes gibt es zur jeder kurzen exakten Seqenz von G-Moduln eine kurze exakte Sequenz der freien Auflösungen (die bis auf Homotopie eindeutig ist). Die zugehörige lange Homololgie-Sequenz liefert Eigenschaften 3 und 4.

[90] Gilt wegen der Linksexaktheit des Hom-Funktors.

[91] Die Kohomologie des Komplexes an der i-ten Stelle ist $\mathrm{Ext}^i_{\mathbb{Z}}(P_i, X)$.

4.2. Der Standardkomplex

4.2.1 Konstruktion der Standard-Resolvente

Zur Berechnung der Kohomologie einer Gruppe G mit Koeffizienten in einem G-Modul M kann man zum Beispiel die folgende Resolvente P von $\mathbb{Z}$ verwenden.

$$P_i := \mathbb{Z}[G^{i+1}]$$

Dies ist ein freier $\mathbb{Z}$-Modul. Die Gruppe G operiere wie folgt auf den Basis-Elementen $(g_0,...,g_i)\in G^{i+1}$ von P_i. Für $s\in G$ sei

$$s\cdot(g_0,...,g_i) = (sg_0,...,sg_i)$$

Die Operation von G auf P_i. Der Homomorphismus $d: P_i \to P_{i-1}$ sei der folgende.

(1) $$d: P_i \to P_{i-1}\ ,\ (g_0,...,g_i) \mapsto \sum_{j=0}^{i} (-1)^j (g_0,...,g_{j-1},g_{j+1},...g_i).$$

Der Homomorphismus $\varepsilon: P_0 \to \mathbb{Z}$ über führe jedes Basis-Element $g\in G$ von P_0 in die 1, d.h.

$$\varepsilon: P_0 \to \mathbb{Z}\ ,\ \sum_\nu n_\nu g_\nu \mapsto \sum_\nu n_\nu.$$

Der augmentierte Komplex

(2) $$P \xrightarrow{\ \varepsilon\ } \mathbb{Z}$$

heißt Standard-Resolvente von $\mathbb{Z}$ über der Gruppe G.

4.2.2 Exaktheit der Standard-Resolvente

Die Standard-Resolvente P von $\mathbb{Z}$ über der Gruppe G ist exakt (sie ist sogar kontrahierbar).

Beweis.

Idee: Für jedes fest gewählte $s\in G$ definieren die Abbildungen

$$h: P_i \to P_{i+1}\ ,\ (g_0,...,g_i) \mapsto (s, g_0,...,g_i),$$

eine Homotopie der identischen Abbildung zur Null-Abbildung.

QED.

4.2.3 Beschreibung des normalisierten Teilkomplexes von Hom(P, M)

Seien G eine Gruppe, M ein G-Modul und P die Standard-Resolvente von $\mathbb{Z}$ über G. Ein Element des Komplexes

$$K^i := \mathrm{Hom}(P_i, M)$$

ist dann gegeben durch eine Abbildung

$$f: G^{i+1} \to M$$

mit

$$f(sg_0,...,sg_i) = s\cdot f(g_0,...,g_i)$$

für jedes $s\in G$. Eine solche Abbildung ist bereits eindeutig festgelegt durch ihre Werte auf den Elementen der Gestalt $(1, g_1, g_1g_2,...,g_1\cdot...\cdot g_i)$ von G^{i+1}. Ist

$$\varphi(g_1,...,g_i) := f(1, g_1, g_1g_2,...,g_1\cdot...\cdot g_i)$$

so hat die zum Korand df von f gehörige Abbildung $d\varphi$ die Gestalt

$$d\varphi(g_1,...,g_{i+1}) = g_1\cdot\varphi(g_2,...,g_{i+1})$$

(3) $$+ \sum_{j=1}^{i} (-1)^j \varphi(g_1,...,g_j g_{j+1},...g_{i+1})$$
$$+ (-1)^{j+1} \varphi(g_1,...,g_i).$$

Wir können daher den Komplex
$$K = Hom(P, M)$$
identifizieren mit dem Komplex mit
$$K^i = Hom(G^i, M)$$
wobei der Korand-Operator durch die Formel (3) gegeben ist. Die Elemente von K^i der angegebenen speziellen Gestalt heißt normierte G-Koketten mit Werten in M. Die entsprechenden Kozyklen bzw. Koränder heißen normierte Kozyklen bzw. Koränder.

4.2.4 Beschreibung der normalisierten 1-Kozyklen und 1-Koränder

Ein (normalisierter) 1-.Kozyklus mit Werten im G-Modul M ist ein verdrehter Homomorphismus, d.h. eine Abbildung
$$\varphi: G \to M$$
mit
$$\varphi(gg') = g\cdot\varphi(g) + \varphi(g).$$
Und φ ist genau dann ein (normalisierter) 1-Korand, wenn es ein Element $m \in M$ gibt mit
$$\varphi(g) = gm - m \text{ für jedes } g \in G.$$
Insbesondere gilt

(4) $$H^1(G, M) = Hom(G, M)$$

falls G trivial auf M operiert.
Beweise: Folgt aus 4.2.3 Formel (3).
QED.

4.2.5 Beschreibung der normalisierten 2-Kozyklen, H^2 und Erweiterungen

Ein (normierter) 2-.Kozyklus mit Werten im G-Modul M ist eine Abbildung
$\varphi: G\times G \to M$
mit
$$g_1\cdot\varphi(g_2, g_3) - \varphi(g_1g_2, g_3) + \varphi(g_1, g_2g_3) - \varphi(g_2, g_2) = 0.$$
(vgl. 4.3.2 Formel (3)).

Bemerkungen

(i) Solche Funktionen (man nennt sie Faktor-Systeme) findet man in der Theorie der Erweiterungen von Gruppen. Dabei beschreibt
$$H^2(G, M)$$
alle möglichen Erweiterungen
$$0 \to M \to E \to G \to 0$$
der Gruppe G durch M. Dabei sei M ein abelscher Normalteiler in E und G operiert auf M durch innere Automorphismen von E.

(ii) Sei
$$\sigma: G \to E$$
ein Schnitt von $E \to G$ (ein Repräsentantensystem). Dann gilt
$$\sigma(g_1)\cdot\sigma(g_2) = \varphi(g_1, g_2)\sigma(g_1g_2)$$
mit $\varphi(g_1, g_2) \in M$. Die Funktion φ ist dann ein 2-Kozyklus auf G mit Werten in M. Wenn wir σ durch einen anderen Schnitt ersetzen, so ändert sich φ um einen 2-Korand ab, d.h. die Klasse von φ in $H^2(G, M)$ hängt nur von der Erweiterung ab.

(iii) Jedes Element von $H^2(G, M)$ erhält man in der in (ii) beschriebenen Art aus einer Erweiterung von G mit M.

4.2.6 Beschreibung des ersten Zusammenhangshomomorphismus

Seien G eine Gruppe und

$$0 \to M' \to M \to M'' \to 0$$

eine kurze exakte Sequenz von G-Moduln. Dann kann man den zugehörigen Homomorphismus

$$\delta\colon H^0(G, M'') \to H^1(G, M')$$

wie folgt beschreiben. Sei

$$x'' \in H^0(G, M'') = M''^G.$$

Wir wählen ein Element

$$x \in M$$

mit dem Bild x'' in M''. Dann genügt dx der Abbildungsvorschrift

$$dx\colon G \to M,\ s \mapsto sx - x.$$

Nach Wahl von x'' ist das Bild des Elements sx - x gleich Null in M'', d.h. es gilt

$$sx - x \in M'.$$

Das bedeutet, dx ist ein 1-Kozyklus auf G mit Werten in M'. Die Kohomologie-Klasse von dx ist gerade das Bild von x'' bei δ,

$$\delta(x'') = [dx].$$

Bemerkung

[dx] hängt nicht von der speziellen Wahl des Urbildes x von x'' ab: bei einer anderen Wahl ändert sich dx um einen 1-Kozyklus auf G mit Werten in M'.

4.3. Homologie

4.3.1 Tensorprodukt von G-Moduln

Seien G eine Gruppe und M und N zwei G-Moduln. Wir bezeichnen mit

$$M \otimes N \text{ bzw. } M \otimes_G N$$

deren Tensorprodukt über $\mathbb{Z}$ bzw. über $\Lambda = \mathbb{Z}[G]$.

Bemerkung

Das Tensorprodukt

$$M \otimes N$$

besitzt in natürlicher Weise die Struktur eines G-Moduls bezüglich der Operation

$$g \cdot (m \otimes n) =^{92} (gm) \otimes (g^{-1}n).$$

4.3.2 Das Augementations-Ideal

Seien G eine Gruppe und

$$I_G$$

der Kern des Augmentations-Homomorphismus

$$\varepsilon\colon \Lambda = \mathbb{Z}[G] \to \mathbb{Z},\ \sum_{g \in G} n_g \cdot g \mapsto \sum_{g \in G} n_g,$$

welcher jedes Element von G in die 1 abbildet,

$$I_G := \mathrm{Ker}(\varepsilon).$$

Dies ist ein Ideal von Λ, welches Augmentations-Ideal von G heißt.

Bemerkungen

(i) I_G wird als $\mathbb{Z}$-Modul erzeugt von den Elementen der Gestalt

$$g - e$$

mit $g \in G$.[93]

---

[92] Wir haben N als rechten G-Modul zu betrachten.

(ii) Aus der Exaktheit der Sequenz

$$0 \to I_G \to \Lambda \to \mathbb{Z} \to 0$$

und der Rechstexaktheit des Tensorprodukts ergibt sich für jeden G-Modul M,

$$\mathbb{Z}\otimes_G M \cong \mathbb{Z}/I_G \otimes_G M \cong M/I_G M.$$

4.3.3. Der Modul M_G

Für jeden G-Modul M setzen wir

$$M_G := M/I_G M.$$

Bemerkungen

(i) M_G ist der größte Faktormodul von M, auf welchem die Gruppe G trivial operiert.

(ii) Durch

$$\text{G-Mod} \to \text{Ab}, M \mapsto M_G,$$

ist ein rechtsexakter Funktor definiert.

(iii) Für je zwei G-Moduln M und N gilt[94]

$$M\otimes_G N \cong (M\otimes N)_G .$$

Beweis. Zu (i). Sei $N \subseteq M$ eine Teilmodul über G mit der Eigenschaft, daß G trivial auf M/N operiert. Wir haben zu zeigen,

$$I_G M \subseteq N.$$

Es reicht zu zeigen

$$(g - e)\cdot m \in N$$

für beliebige $g\in G$ und beliebige $m\in M$ (vgl. Bemerkung 4.3.2(i)). Nach Voraussetzung gilt

$$gm \equiv em \bmod N,$$

also $(g-e)\cdot m \in N$.

Zu (ii). Folgt aus den allgemeinen Eigenschaften des Tensorprodukts.

Zu (iii). Die natürliche Abbildung

$$b: M\times N \to (M\otimes N)_G , (m, n) \mapsto m\otimes n \bmod I_G\cdot(M\otimes N),$$

ist Λ-bilinear: für $m\in M$, $n\in N$ und $g\in G$ gilt

$$b(mg, n) = b(g^{-1}m,n) = [(g^{-1}m)\otimes n] =^{95} [g\cdot((g^{-1}m)\otimes n)] = [m\otimes(gn)] = b(m, gn).$$

---

[93] Sei $\sum_{g\in G} n_g\cdot g \in I_G$. Dann gilt $0 = \varepsilon(\sum_{g\in G} n_g\cdot g) = \sum_{g\in G} n_g$, also

$$\sum_{g\in G} n_g\cdot g = \sum_{g\in G} n_g\cdot(g-e).$$

[94] Die G-Modul-Struktur von $C\otimes M$ ist durch die Identifikation mit $\text{Hom}(C^*, M)$ eindeutig festgelegt:

$$C\otimes M \to \text{Hom}(C^*, M), c\otimes m \;a\; (f \;a\; f(c)\cdot m), C^* = \text{Hom}(C,\mathbb{Z})$$

(vgl. das Lemma von 4.6.8). Für $g\in G$ ist das g-fache der Abbildung

$$f \;a\; f(c)\cdot m$$

die Abbildung

$$f \;a\; g\cdot((g^{-1}f)(c)\cdot m) = g(f(gc)\cdot m) = f(gc)\cdot gm.$$

Letztere ist das Bild des Elements $(gc)\otimes(gm) \in C\otimes M$. Die Operation von G auf $C\otimes M$ ist damit die folgende:

$$G \times C\otimes M \to C\otimes M, (g, c\otimes m) \;a\; (gc)\otimes(gm).$$

Diese Konstruktion funktioniert nur für Gruppenringen, nicht für (einseitige) Moduln über einem beliebigen Ring.

Sei jetzt

$$b': M\times N \to P$$

eine Λ-bilineare Abbildung. Dann ist b' auch $\mathbb{Z}$-bilinear, induziete als eine $\mathbb{Z}$-lineare Abbildung

$$\tilde{b}': M\otimes N \to P,\ m\otimes n \mapsto b'(m,n).$$

Für $g\in G$ gilt

$$\begin{aligned}\tilde{b}'((g-e)\cdot(m\otimes n)) &= \tilde{b}'(gm\otimes g^{-1}n - m\otimes n) = \tilde{b}'(gm\otimes g^{-1}n) - \tilde{b}'(m\otimes n)\\ &= b'(gm,\ g^{-1}n) - b'(m,\ n)\\ &= 0 \qquad \text{(weil } b' \text{ } \Lambda\text{-bilinear ist)},\end{aligned}$$

d.h. $\tilde{b}'(I_G\cdot M\otimes N) = 0$ (vgl. Bemerkung 4.3.2(i)). Deshalb faktorisiert sich $\tilde{b}'$ über

$$M\otimes N/I_G(M\otimes N) = (M\otimes N)_G.$$

Es ist leicht zu sehen, diese Faktorisierung ist eindeutig. Wir haben gezeigt: $(M\otimes N)_G$ besitzt die Universalitätseigenschaft des Tensorprodukts $M\otimes_G N$.

QED.

4.3.4 Definition: induzierter G-Modul

Sei X eine beliebige abelsche Gruppe. Dann hat

$$\Lambda\otimes_{\mathbb{Z}} X$$

in natürlicher Weise die Struktur eines G-Moduls.[96] Ein G-Modul dieser Gestalt heißt induziert.

4.3.5 Definition: homologische Erweiterung des Funktors $M \mapsto M_G$

Unter einer homologischen Erweiterung der Funktors

$$G\text{-Mod} \to Ab,\ M \mapsto M_G$$

versteht man eine Folge von Funktoren

$$G\text{-Mod} \to Ab,\ M \mapsto H_q(G,M),$$

$(q=0,1,2,3,...)$ zusammen mit einem sogenannten Zusammenhangshomomorphismus

$$\delta: H_q(G,M") \to H_{q-1}(G,M')$$

für jede kurze exakte Sequenz von G-Moduln

(*) $$0\to M'\to M\to M"\to 0,$$

und jedes $q\in\mathbb{N}$, wobei folgenden Bedingungen erfüllt sind.

1. $H^0(G,M) = M_G$.
2. $H_q(G,M) = 0$ für $q>0$ und M induziert.
3. Für jede kurze exakte Sequenz (*) von G-Moduln ist die folgende zugehörige Sequenz exakt (und heißt lange Homologiesequenz von (*)).

$$...\to H_q(G,M')\to H_q(G,M)\to H_q(G,M")\xrightarrow{\delta} H_{q-1}(G,M')\to...$$

4. Die lange Homologiesequenz ist funktoriel in (*).

---

[95] G operiert trivial auf $(M\otimes N)_G$ (nach Definition von $(M\otimes N)_G$).

[96] Man verwende 4.3.1 indem man G auf X trivial operieren läßt.

4.3.6 Existenz und Eindeutigkeit der homologischen Erweiteung

Sei G eine Gruppe. Dann gibt es bis auf natürliche Isomorphie eindeutig bestimmte homologische Erweiterung des Funktors

$$G\text{-Mod} \to Ab,\ M \mapsto M_G$$

Beweis. Der Beweis ist analog zum Beweis von 4.1.7
QED.

4.3.7 Definition: Homologie

Seien G eine Gruppe und M ein G-Modul. Dann heßt die nach 4.3.6 eindeutig bestimmte Gruppe

$$H_q(G, M)$$

q-te Homologie von G mit Koeffizienten in M.

4.3.8 Berechnung der Homologie mit Hilfe der Standard-Resolvente

Seien G eine Gruppe, M ein G-Modul und

$$P \to \mathbb{Z} \to 0$$

die Standard-Resolvente von $\mathbb{Z}$ über G (vgl. 4.2.1). Dann gilt

$$H_q(G, M) \cong H_q(P \otimes_G M).$$

4.3.8 Beschreibung des ersten Zusammenhangshomomorphismus

Seien G eine Gruppe und

$$0 \to M' \to M \to M'' \to 0$$

eine kurze exakte Sequenz von G-Moduln. Dann läßt sich der zugehörige Zusammenhangshomomorphismus

$$\delta: H_1(G, M'') \to H_0(G, M')$$

wie folgt beschreiben.
Ein 1-Zyklus auf G mit Werten in M" ist eine Abbildung

$$f: G \to M''$$

mit $f(s) = 0$ für fast alle $s \in G$ und mit

$$df = \sum_{s \in G} (s^{-1}-1)f(s) = 0.$$

Für jedes $s \in G$ wählen wir eine Element

$$\overline{f}(s) \in M$$

mit dem Bild f(s) in M", wobei $\overline{f}(s)$ ebenfalls für fast alle s Null sei. Das Bild des Elements $d\overline{f}$ in M" ist dann Null, d.h. es gilt

$$d\overline{f} \in M'.$$

Es gilt dann

$$\delta[f] = [d\overline{f}],$$

d.h. das Bild der durch f repräsentierten Homologie-Klasse ist gerade die Homologie-Klasse von $d\overline{f}$.

4.3.9 Proposition 3.1: die erste Homologie mit Koeffizienten in $\mathbb{Z}$

Seien G eine Gruppe und G' die Kommutatorgruppe. Dann besteht eine natürliche Isomorphie

$$H_1(G, \mathbb{Z}) \cong G/G'.$$

Beweis. Wir betrachten die exakte Sequenz

$$0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

von 4.3.2(ii) und die zugehörige exakte Sequenz

$$H_1(G, \mathbb{Z}[G]) \to H_1(G, \mathbb{Z}) \to H_0(G, I_G) \to H_0(G, \mathbb{Z}[G]) \to H_0(G, \mathbb{Z}[G]) \to 0.$$

Da $\mathbb{Z}[G] = \mathbb{Z}[G] \otimes \mathbb{Z}$ ein induzierter G-Modul ist, hat diese Sequenz die Gestalt

$$0 \to H_1(G, \mathbb{Z}) \to I_G/I_G^2 \to \mathbb{Z}[G]/I_G\mathbb{Z}[G] \to \mathbb{Z}/I_G\mathbb{Z} \to 0.$$

Weil G trivial auf $\mathbb{Z}$ operiert, gilt $I_G Z = 0$. Die Sequenz nimmt damit die Gestalt

$$0 \to H_1(G, \mathbb{Z}) \to I_G/I_G^2 \to \mathbb{Z} \to \mathbb{Z} \to 0.$$

Der vorletzte Homomorphismus ist surjektiv, also bijektiv. Wir erhalten

$$H_1(G, \mathbb{Z}) \cong I_G/I_G^2.$$

Es reicht somit, zu zeigen, die Abbildung

$$G/G' \to I_G/I_G^2,\ g \bmod G' \mapsto g\text{-}1 \bmod I_G^2,$$

ist ein wohldefinierter Isomorphismus. Zunächst ist

$$\varphi: G \to I_G/I_G^2,\ g \mapsto g\text{-}1 \bmod I_G^2$$

eine wohldefinierte Abbildung. Es gilt

$$\begin{aligned} \varphi(gg') &= gg' - 1 \qquad \bmod I_G^2 \\ &= (g - 1) + (g' - 1) + (g - 1)(g'-1) \bmod I_G^2 \\ &= \varphi f(g) + \varphi(g'), \end{aligned}$$

d.h. φ ist ein Gruppen-Homomorphismus, dessen Bild ein Erzeugenden-System der Gruppe I_G/I_G^2 enthält[97]. Insbesondere ist φ surjektiv. Es gilt

$$\varphi(xyx^{-1}y^{-1}) = \varphi(x) + \varphi(y) - \varphi(x) - \varphi(y) = 0,$$

also

$$G' \subseteq \mathrm{Ker}(\varphi).$$

Wir haben damit einen wohldefinierten sujektiven Homomorphismus

$$\tilde{\varphi}: G/G' \to I_G/I_G^2,\ g \bmod G' \mapsto g\text{-}1 \bmod I_G^2,$$

Es reicht zu zeigen, dieser ist injektiv. Zum Beweis konstruieren wir eine Abbildung in umgekehrter Richtung. Dazu betrachten wir

$$I_G = \sum_{g \in G} \mathbb{Z} \cdot (g\text{-}1)$$

als freie abelsche Gruppe mit dem freien Erzeugendensystem

$$g\text{-}1 \text{ mit } g \in G.$$

Es gibt einen Gruppen-Homomorphismus

$$\psi: I_G \to G/G' \text{ mit } \psi(g\text{-}1) = g \bmod G' \text{ für jedes } g \in G.$$

Für ein Element der Gestalt

$$(g\text{-}1)(g'\text{-}1) = gg' - g - g' + 1 \text{ mit } g, g' \in G$$

gilt

$$\psi((g\text{-}1)(g'\text{-}1) = gg' \cdot g^{-1} \cdot g'^{-1} \bmod G' = 1.$$

---

[97] I_G wird als $\mathbb{Z}$-Modul von den Elementen der Gestalt g-1 mit $g \in G$ erzeugt.

Mit anderen Worten, die Erzeugenden der Untergruppe I_G^2 liegen im Kern von ψ. Der Homomorphismus induziert einen Gruppen-Homomorphismus

$$\tilde{\psi}: I_G/I_G^2 \to G/G' \text{ mit } \tilde{\psi}(g\text{-}1 \bmod I_G^2) = g \bmod G' \text{ für jedes } g \in G.$$

Für jedes $g \in G$ gilt damit

$$\tilde{\psi}(\tilde{\varphi}(g \bmod G')) = \tilde{\psi}(g - 1 \bmod I_G^2) = g \bmod G'.$$

Es ist also $\tilde{\psi} \circ \tilde{\varphi} = \mathrm{Id}$. Insbesondere ist $\tilde{\varphi}$ injektiv.
QED.

4.4. Wechsel der Gruppe

4.4.1 Koinduzierte Moduln

Seien G eine Gruppe, $G' \subseteq G$ eine Unter gruppe und M' ein G'-Modul. Dann hat

$$M := \mathrm{Hom}_{G'}(\mathbb{Z}[G], M')$$

die Struktur eines rechten G-Moduls. Wie in 4.1.1 beschrieben, versehen wir M mit der zugehörigen Struktur eines linken G-Moduls, d.h. wir betrachten M als linken G-Modul bezüglich der Multiplikation mit

$$(g \cdot \varphi)(g') :=^{98} \varphi(g'g)$$

für $g, g' \in G$ und $\varphi \in M$. Wir sagen in dieser Situation, M entsteht aus M' durch Kofortsetzung der Skalare von G' auf G oder auch der durch M' koinduzierte Modul über G.

4.4.2 Proposition 4.1: Lemma von Shapiro

Seien G eine Gruppe, $G' \subseteq G$ eine Untergruppe und M' ein G'-Modul. Dann besteht für jedes $q \geq 0$ eine natürliche Isomorphie

$$H^q(G, \mathrm{Hom}_{G'}(\mathbb{Z}[G], M')) \cong H^q(G', M').$$

Beweis. Seien

$$\Lambda := \mathbb{Z}[G]$$
$$\Lambda' := \mathbb{Z}[G']$$
$$M := \mathrm{Hom}_{G'}(\Lambda, M').$$

und P eine freie Resolvente von $\mathbb{Z}$ über G,

$$P \to \mathbb{Z} \to 0.$$

Dann ist P auch eine freie Resolvente von $\mathbb{Z}$ über G', und es gilt

$$\begin{aligned} \mathrm{Hom}_G(P, M) &= \mathrm{Hom}_G(P, \mathrm{Hom}_{G'}(\Lambda, M')) \\ &\cong \mathrm{Hom}_G(P \otimes_\Lambda \Lambda, M') \\ &\cong \mathrm{Hom}_{G'}(P, M'), \end{aligned}$$

d.h. es gilt die Behauptung.
QED.
Bemerkungen

(i) Ein Analoges Ergebnis gilt auch für die Homologie, wenn man Hom durch $\otimes$ ersetzt:[99]

---

[98] Diese Definition entspricht der Operation von G auf $M = \mathrm{Hom}_{G'}(\mathbb{Z}[G^\circ], M')$, wobei G° die zu G entgegengesetzte Gruppe bezeichnet (d.h. ab in G° ist gerade ba in G). Dies ist erforderlich, damit der letzte Isomorphismus im Beweis des Lemmas von Shapiro tatsächlich ein Isomorphismus ist.

[99] Mit

$$H_q(G, M'\otimes_{\Lambda',\Lambda}) \cong H_q(G', M')$$

für jede Untergruppe $G' \subseteq G$ der Gruppe G und jeden G'-Modul M'.

(ii) Die Aussage von 4.4.2 kann man als Verallgemeinerung von Eigenschaft 2 der Kohomologie-Gruppen (vgl. 4.1.6) auffassen. Für $G' = \{1\}$ ist nämlich $\Lambda' = \mathbb{Z}$, der Modul M ist koinduziert und die Gruppen $H^q(G, M)$ sind trivial für $q \geq 1$.

4.4.3 Funktorielle Abhängigkeit der Kohomologie von der Gruppe, die Restriktion

Sei

$$f: G' \to G$$

ein Gruppen-Homomorphismus. Dieser induziert einen Homomorphismus

$$P' \to P$$

der Standard-Resolventen und damit einen Homomorphismus

$$f^*: H^q(G, M) \to H^q(G', M)$$

für jeden G-Modul M, welcher inverses Bild entlang f heißt. Man beachte, vermittels f kann man M auch als G'-Modul auffassen.
Ist speziell $G' \subseteq G$ eine Untergruppe und

$$i: G' \hookrightarrow G$$

die natürliche Einbettung, so schreibt man

$$Res := i^*: H^q(G, M) \to H^q(G', M)$$

und nennt den Homomorphismus Res auch Einschränkungs-Homomorphismus oder auch einfach Einschränkung auf die Untergruppe G' oder Restriktion.

4.4.4 Die Inflation

Seien G eine Gruppe,

$$H \subseteq G$$

ein Normalteiler von G und M ein G-Modul. Dann hat

$$M^H$$

in natürlicher Weise die Struktur eines G/H-Moduls und der natürliche Homomorphismus

$$f: G \to G/H$$

induziert enen Homomorphismus

$$H^q(G/H, M^H) \to H^q(G, M^H).$$

Die Zusammensetzung

$$Inf: H^q(G/H, M^H) \to H^q(G, M^H) \to H^q(G, M)$$

mit dem durch die Einbettung $M^H \hookrightarrow M$ induzierten Homomorphismus heißt Inflation der Kohomologie von G mit Koeffizienten in M zur Untergruppe H.

4.4.5 Funktorielle Abhängigkeit der Homologie von der Gruppe, die Korestriktion

Sei

$$f: G' \to G$$

ein Gruppen-Homomorphismus. Dieser induziert wie in 4.4.3 einen Homomorphismus

$$P' \to P$$

$$M := M'\otimes_{\Lambda',\Lambda}$$

und P wie im obigen Beweis gilt

$$P\otimes_G M = P\otimes_{\Lambda}(M'\otimes_{\Lambda',\Lambda}) \cong P\otimes_{\Lambda',M'}$$

Übergang zur Homologie liefert die Behauptung.

der Standard-Resolventen und damit einen Homomorphismus

$$f_*: H_q(G', M) \to H_q(G, M)$$

für jeden G-Modul M, welcher direktes Bild entlang f heißt. Man beachte, vermittels f kann man M auch als G'-Modul auffassen.
Ist speziell $G' \subseteq G$ eine Untergruppe und

$$i: G' \hookrightarrow G$$

die natürliche Einbettung, so schreibt man

$$Cor := i_*: H_q(G', M) \to H_q(G, M)$$

und nennt den Homomorphismus Cor auch Korestriktion oder Koeinschränkung zur Untergruppe G' von G.

4.4.6 Modifikation der G-Modul-Struktur durch innere Automorphismen

Seien G eine Gruppe, M ein G-Modul und

$$t \in G$$

ein Elemnent. Der innere Automorphismus

$$G \to G,\ s \mapsto tst^{-1},$$

definiert auf M eine neue G-Modul-Struktur mit der Mutliplikation

$$s \cdot^t m := tst^{-1}m \text{ für } s \in G \text{ und } m \in M.$$

Den Modul M mit dieser abgeänderten G-Modulstruktur bezeichnen wir mit

$$M^t.$$

Bemerkungen

(i) Der innere Automorphismus

$$\sigma_t: G \to G,\ s \mapsto tst^{-1},$$

induziert nach 4.4.3 einen Homomorphismus

(1) $$(\sigma_t)^*: H^q(G, M) \to H^q(G, M^t)$$

(ii) Die Abbildung

$$\alpha: M^t \to M,\ m \mapsto t^{-1}m,$$

ist ein Homomorphismus von G-Moduln:

$$\alpha(s \cdot^t m) = \alpha(tst^{-1}m) = st^{-1}m = s \cdot \alpha(m).$$

Sie induziert also insbesondere einen Homorphismus

(2) $$H^q(G, M^t) \to H^q(G, M).$$

4.4.7 Proposition 4.2: die Homorphismen auf der Kohomologie zu einem inneren Automorphismus[100]

Seien G eine Gruppe, M ein G-Modul und

$$t \in G$$

ein Element. Dann sind die beiden Homomorphismen (1) und (2) von 4.4.6 invers zueinander.

Beweis. Der Beweis verwendet eine Standard-Methode, welche Dimensions-Verschiebung heißt: man beweist das Ergebnis zuerst für $q = 0$ und danach allgemein durch induktive Betrachtungen bezüglich q unter Verwendung des Isomorphismus (5) im Beweis von 4.1.7.
Der Fall $q = 0$. Die Links-Multiplikation mit t ist ein Isomorphismus von G-Moduln[101]

---

[100] vgl. auch die K-Theorie-Vorlesung vom Sommer-Semester 2011, Abschnitt 1.4.13, Bemerkung (iii).

[101] $L_t(s \cdot m) = tsm = tst^{-1} \cdot L_t(m) = s \cdot^t L_t(m)$. Die Tatsache, daß die Linksmultiplikation M mit M^t identifiziert, beweist die Behauptung eigentlich für alle q.

$$L_t: M \to M^t,\ m \mapsto tm,$$

d.h. wir können L_t benutzen, um M^t mit M zu identifizieren. Für die 0-ten Kohomologie-Gruppen von M bzw. M^t identifizieren sich dann ebenfalls vermittels der Linksmultiplikation mit t. Die Homomorphismus (1) von 4.4.6 ist also ebenfalls die Links-Multiplikation mit t:

$$L_t: M^G \to (M^t)^G,\ m \mapsto tm.$$

Man beachte, es gilt

$$\begin{aligned} H^0(G, M^t) = (M^t)^G &= \{m \in M \mid tst^{-1}m = m \text{ für } s \in G\} \\ &= \{m \in M \mid st^{-1}m = t^{-1}m \text{ für } s \in G\} \\ &= t\{m \in t^{-1}M \mid sm = m \text{ für } s \in G\} \\ &= t \cdot M^G \end{aligned}$$

Der Homomorphismus (2) von 4.4.6 ist aber die Links-Multiplikation mit t^{-1}. Die beiden Abbildungen sind somit invers zueinander.
Der Fall q > 0. Wir betrachten die exakte Sequenz

$$0 \to M \to M^* \to M' \to 0$$

mit dem koinduzierten G-Modul

$$M^* := \mathrm{Hom}(\Lambda, M)$$

(vgl. (4) im Beweis von 4.1.7). Diese Sequenz läßt sich auch als kurze exakte Sequenz

$$0 \to M^t \to M^{*t} \to M'^t \to 0$$

interpretieren. Der Modul M^{*t} ist isomorph zu M*, hat also triviale Kohomologie. Die lange Kohomologie-Sequenz liefert deshalb natürliche Isomorphien

$$H^q(G, M^t) \cong H^{q-1}(G, M'^t)$$

und

$$H^1(G, M^t) \cong \mathrm{Koker}(H^0(G, M^{*t}) \to H^0(G,, M'^t)).$$

Die Behauptung ergibt sich deshalb aus der Induktionsvoraussetzung.
QED.

4.5. Sequenzen welche Restriktion und Inflation verbinden

4.5.1 Proposition 5.1: der Fall q = 1

Seien G eine Gruppe, M ein G-Modul und

$$H \subseteq G$$

ein Normalteiler. Dann ist die folgende Sequenz exakt.

$$0 \to H^1(G/H, M^H) \xrightarrow{\mathrm{Inf}} H^1(G, M) \xrightarrow{\mathrm{Res}} H^1(H, M).$$

Beweis. 1. Schritt: Exaktheit an der Stelle $H^1(G/H, M^H)$.
Sei f: $G/H \to M^H$ ein 1-Kozyklus. Die Abbildung f definiert eine Abbildung

$$\overline{f}: G \to G/H \xrightarrow{f} M^H \to M,$$

welche ebenfalls ein 1-Kozyklus ist.

Wir nehmen an, $\overline{f}$ ist ein Korand und haben in dieser Situation zu zeigen, daß auch f ein Korand ist.
Auf Grund der Annahme gibt es ein Element

$$m \in M$$

mit

$$\overline{f}(s) = sm - m$$

für jedes $s \in G$. Nach Konstruktion ist $\overline{f}$ konstant auf den Restklassen modulo H. Deshalb gilt

$$sm - m = stm - m$$

für alle $t \in H$. Insbesondere ist

$$tm - m = 1 \cdot m - m = 0$$

für jedes $t \in H$, d.h. m ist invariant bezüglich der Operation von H,

$$m \in M^H.$$

Für $s \in G$ ist damit

$$f(sH) = \overline{f}(s) = sm - m \text{ und } m \in M^H.$$

Mit anderen Worten, f ist ein Korand.

2. Schritt. $\mathrm{Res} \circ \mathrm{Inf} = 0$.

Sei $\varphi: G \to M$ ein 1-Kozyklus auf G mit Werten in M, Dann die Einschränkung

$$\varphi|_H : H \to M$$

ein 1-Kozyklus auf H mit Werten in M und die Kohomologie-Klasse dieser Einschränkung ist gerade

$$[\varphi|_H] = \mathrm{Res}\,[\varphi].$$

Ist nun φ von der Gestalt

$$\varphi = \overline{f}$$

mit einem 1-Kozyklus $f: G/H \to M^H$ wie im ersten Schritt, so ist

$$\varphi|_H = \overline{f}|_H$$

konstant auf der Faser H von $G \to G/H$, d.h.

(*) $\varphi|_H$ = die konstante Abbildung mit dem Wert $\overline{f}(1)$.

Als 1-Kozyklus genügt $\overline{f}$ den Relationen

$$\overline{f}(gg') = g\overline{f}(g') + \overline{f}(g) \text{ für } g, g' \in G.$$

Da die Werte von $\overline{f}$ in M^H liegen, folgt

$$\overline{f}(hh') = \overline{f}(h) + \overline{f}(h') \text{ für } h, h' \in H,$$

d.h. auf H ist $\overline{f}$ ein Gruppen-Homomorphismus. Insbesondere gilt $\overline{f}(1) = 0$. Aus (*) ergibt sich damit

$$\varphi|_H = \text{die konstante Abbildung mit dem Wert } 0.$$

Wir haben gezeigt

$$\mathrm{Res}(\mathrm{Inf}\,[f]) = \mathrm{Res}\,[\overline{f}] = [\varphi|_H] = 0,$$

Das f beliebig war, folgt $\mathrm{Res} \circ \mathrm{Inf} = 0$.

3. Schritt: Exaktheit an der Stelle $H^1(G, M)$.

Sei

$$\varphi: G \to M$$

ein 1-Kozyklus, dessen Einschränkung auf H ein Korand ist. Wir haben zu zeigen, dann liegt die Kohomologie-Klasse von φ im Bild der Inflation. Nach Voraussetzung gibt es ein

$$m \in M$$

mit

$$\varphi(t) = tm - m \text{ für jedes } t \in H.$$

Wir ziehen von φ den Korand

$$G \to M,\ s \mapsto sm - m,$$

ab und können deshalb ohne Beschränkung der Allgemeinheit annehmen,

$$\varphi|_H = 0.$$

Da φ ein 1-Kozyklus ist, gilt

$(*)$ $$\varphi(st) = \varphi(s) + s\cdot\varphi(t) \text{ für } s, t\in G.$$

Lassen wir speziell t die Untergruppe H durchlaufen, so erhalten wir,

$$\varphi(st) = \varphi(s) \text{ für } s\in G \text{ und } t\in H,$$

d.h. φ ist konstant auf den Nebenklassen modulo H, d.h. φ ist die Zusammensetzung

$$\varphi: G \to G/H \xrightarrow{f} M$$

mit einem 1-Kozyklus f. Als nächstes betrachten wir (*) für den Fall $s\in H$ und $t\in G$:

$$\varphi(st) = s\cdot\varphi(t) \text{ für } s\in H \text{ und } t\in G.$$

Der Wert links ist aber gleich $\varphi(t)$, da φ auf den Nebenklassen modulo H constant ist,

$$\varphi(t) = s\cdot\varphi(t) \text{ für } s\in H \text{ und } t\in G.$$

Mit anderen Worten, die Werte von φ (und damit die von f) liegen in M^H, d.h. f ist ein 1-Kozyklus

$$f: G/H \to M^H.$$

Nach Konstruktion gilt

$$\text{Inf } [f] = [\varphi],$$

d.h. die Klasse von φ liegt im Bild der Inflation.
QED.

4.5.2 Proposition 5.2: der Fall q beliebig

Seien G eine Gruppe, M ein G-Modul und

$$H \subseteq G$$

ein Normalteiler mit

$$H^i(H, M) = 0 \text{ für } 1 \le i \le q-1.$$

Dann ist die folgende Sequenz exakt.

$$0 \to H^q(G/H, M^H) \xrightarrow{\text{Inf}} H^q(G, M) \xrightarrow{\text{Res}} H^q(H, M).$$

Beweis. Der Beweis dieser Aussage ist ein weiteres Beispiel für die Methode der Dimensionsverschiebung: wir reduzieren die Aussage auf den Fall q = 1, d.h. auf 4.5.1. Wir betrachten die exakte Sequenz

$$0 \to M \to M^* \to M' \to 0$$

mit dem koinduzierten G-Modul

$$M^* := \text{Hom}(\Lambda, M)$$

(vgl. (4) im Beweis von 4.1.7). Der Modul M^* ist auch koinduziert als Modul über der Untergruppe H, denn $\Lambda = \mathbb{Z}[G]$ ist ein freier Modul über $\Lambda' := \mathbb{Z}[H]$.[102] Insbesondere gilt

$$H^i(H, M') \cong H^{i+1}(H, M) = 0 \text{ für } 1 \le i \le q-2.$$

Wegen $H^1(H, M) = 0$ ist die Sequenz

$$0 \to M^H \to (M^*)^H \to (M')^H \to 0$$

exakt. Der G/H-Modul in der Mitte ist koinduziert:

$$(M^*)^H = \text{Hom}(\Lambda, M)^H = \text{Hom}_H(\Lambda, M) =^{103} \text{Hom}(\mathbb{Z}[G/H], M).$$

Die vertikalen Homomorphismen im folgenden Diagramm sind Isomorphismen.

$$\begin{array}{ccccccc} 0\to & H^{q-1}(G/H, (M')^H) & \to & H^{q-1}(G,M') & \to & H^{q-1}(H, M') \\ & \delta\downarrow & & \downarrow\delta & & \delta\downarrow \\ 0\to & H^q(G/H, M^H) & \to & H^q(G, M) & \to & H^q(G, M) \end{array}$$

---

[102] d.h. $\Lambda = \oplus_i \Lambda'$ und $\text{Hom}(\Lambda, M) = \text{Hom}(\oplus_i \Lambda' , M) = \times_i \text{Hom}(\Lambda' , M) = \text{Hom}(\Lambda' , \times_i M)$.

[103] Eine H-äquivariante Abbildung $\Lambda = \mathbb{Z}[G] \to M$ ist bereits festgelegt, wenn ihre Werte auf einem Repräsentanten-System von G modulo H feststehen.

Für die beiden äußeren vertikalen Abbildungen gilt dies, weil $(M^*)^H$ und M^* koninduziert sind über G/H bzw. über G. Für die vertikale Abbildung in der Mitte folgt dies auf Grund des Fünfer-Lemmas.
Nach Induktionsvoraussetzung ist die obere Zeile des Diagramms exakt. Also ist es auch die untere.
QED.

4.5.3 Folgerung

Seien G eine Gruppe, M ein G-Modul und

$$H \subseteq G$$

ein Normalteiler mit

$$H^i(H, M) = 0 \text{ für } 1 \leq i \leq q\text{-}1.$$

Dann gilt

$$H^i(G/H, M^H) \cong H^i(G, M) \text{ für } 1 \leq i \leq q\text{-}1.$$

Beweis. Man wende die exakten Sequenzen von 4.5.2 wiederholt an und verwende dabei die Voraussetzung $H^i(H, M) = 0$ für $1 \leq i \leq q\text{-}1$.
QED.

4.6 Die Tate-Kohomologie

4.6.1 Vereinbarungen und Bezeichnungen

Von jetzt ab nehem wir an, die Gruppe G ist endlich,

$$G \text{ endlich.}$$

Wir bezeichnen mit N das Element

$$N := N(G) := \sum_{s \in G} s \in \Lambda = \mathbb{Z}[G].$$

Für jeden G-Modul M definiert die Multiplikation mit N einen Endomorphismus, den wir ebenfalls mit N bezeichnen,

$$N = N(G): M \to M,\ m \mapsto N \cdot m.$$

Bemerkung
Nach Konstruktion gilt

$$I_G M \subseteq \operatorname{Ker} N \text{ und } \operatorname{Im}(N) \subseteq M^G.$$

4.6.2 Die Tate-Kohomologie im Grad 0

Seien G eine endliche Gruppe und M ein G-Modul. Der in 4.6.1 definierte Endomorphismus

$$N: M \to M$$

induziert einen Homomorphismus

$$N^* = N_G^*: H_0(G, M) = M/I_G M \to M^G = H^0(G, M).$$

Wir definieren

$$\hat{H}_0(G, M) := \operatorname{Ker}(N^*) \subseteq H_0(G, M)$$

$$\hat{H}^0(G, M) := \operatorname{Koker}(N^*) = H^0(G, M)/\operatorname{Im} N^*.$$

4.6.3 Induzierte und koinduzierte Moduln im Fall endlicher Gruppen

Für jede endliche Gruppe fallen die Begriffe induzierter G-Modul und koinduzierter G-Modul zusammen.

Zum Beweis reicht es zu zeigen, die Abbildung

$$\alpha:\mathrm{Hom}(\Lambda, X) \to \Lambda\otimes X,\ \varphi \mapsto \sum_{s\in G} s\otimes\varphi(s),$$

ist für jede abelsche Gruppe X ein Isomorphismus von G-Moduln.

Beweis. 1. Schritt: Bijektivität von α.
Beide Seiten kommutieren mit direkten Limiten und direkten Summen bezüglich X. Wir können deshalb annehmen

$$X = \mathbb{Z}/(p^m)$$

mit einer Primzahl p. Es reicht, die Aussage für einen beliebigen freien endlich erzeugten $\mathbb{Z}$-Modul anstelle vonΛ zu beweisen. Da beide Seiten mit endliche direkten Summen kommutieren, reicht es, die Aussage mit $\mathbb{Z}$ anstelle von Λ zu beweisen, d.h. zu zeigen ist, die Abbildung

$$\mathrm{Hom}(\mathbb{Z}, X) \to X,\ \varphi \mapsto \varphi(s),$$

ist bijektiv. Das ist aber trivial.
2. Schritt: α ist G-äquivariant.
Für $\lambda\in\Lambda$, $g\in G$ und $\varphi\in\mathrm{Hom}(\Lambda,X)$ gilt

$$\alpha(g\varphi) = \sum_{s\in G} s\otimes(g\varphi)(s) = \sum_{s\in G} s\otimes\varphi(g^{-1}s) = \sum_{s\in G} gs\otimes\varphi(s) = g\sum_{s\in G} s\otimes\varphi(s) = g\cdot\alpha(\varphi)$$

QED.

4.6.4 Die 0-te Tate-(Ko-)Homologie eines induzierten Moduls

Seien G eine endliche Gruppe und M ein induzierter G-Modul. Dann gilt

$$\hat{H}^0(G, M) = \hat{H}_0(G, M) = 0.$$

Beweis. Sei

$$M = \Lambda\otimes X$$

mit einer abelschen Gruppe X. Als Modul über $\mathbb{Z}$ ist Λ frei. Jedes Element von M läßt sich deshalb in der Gestalt

$$m = \sum_{s\in G} s\otimes x_s$$

schreiben mit eindeutig bestimmten Elementen $x_s\in X$. Das Element m ist genau dann G-invariant, wenn gilt

$$\sum_{s\in G} gs\otimes x_s = \sum_{s\in G} s\otimes x_s \text{ für jedes } g\in G,$$

d.h. genau dann, wenn alle x_s gleich sind. Dann hat aber m die Gestalt

$$m = N\cdot(1\otimes x) \text{ mit } x\in X,$$

d.h. m liegt im Bild von $N^*: M/I_GM \to M^G$. Wir haben gezeigt, der Kokern

$$\hat{H}^0(G, M)$$

dieser Abbildung N^* ist Null.
Liegt m im Kern der Multiplikation mit N,

$$0 = N\cdot m = \sum_{t\in G} t\cdot \sum_{s\in G} s\otimes x_s =$$

$$= \sum_{u\in G} u\otimes \sum_{t\in G} x_{t^{-1}u}$$

$$= \sum_{u\in G} u\otimes \sum_{v\in G} x_v,$$

so gilt $\sum_{v\in G} x_v = 0$, d.h. es ist

$$m = \sum_{s\in G} s\otimes x_s = \sum_{s\in G} (s-1)\otimes x_s = \sum_{s\in G} (s-1)\cdot(1\otimes x_s) \in I_G M.$$

Wir haben gezeigt, der Kern

$$\hat{H}_0(G, M)$$

der Abbildung N*: $M/I_G M \to M^G$ ist Null.

QED.

4.6.5 Defintion: die Tate-Kohomologie

Seien G eine endliche Gruppe und M ein G-Modul. Dann heißt

$$\hat{H}^q(G, M) := \begin{cases} H^q(G,M) & \text{falls } q \geq 1 \\ \text{Koker}(N^*: M/I_G M \to M^G) & \text{falls } q = 0 \\ \text{Ker}(N^*: M/I_G M \to M^G) & \text{falls } q = -1 \\ H_{|q|-1}(G, M) & \text{falls } q \leq -2 \end{cases}$$

q-te Tate-Kohomologie von G mit Koeffizienten in M.

Bemerkung

Nach 4.6.3 fallen die Begriffe induziert und koinduziert im Fall endlicher Gruppen zusammen, und nach 4.6.4 gilt für induzierte G-Moduln

$$\hat{H}^q(G, M) = 0$$

für $q= 0,-1$. Für alle anderen $q\in\mathbb{Z}$ ist dies aber ebenfalls der Fall, weil für solche q die Tate-Kohomologie mit der gewöhnlichen Kohomologie bzw. der gewöhnlichen Homologie zusammenfällt. Also ist für induzierte G-Moduln

$$\hat{H}^q(G, M) = 0 \text{ für jedes } q\in\mathbb{Z}.$$

4.6.6 Die lange Kohomologie-Sequenz

Seien G eine endliche Gruppe und

$$0 \to M' \to M \to M'' \to 0$$

eine kurze exakte Sequenz von G-Moduln. Diese induziert die folgende exakte Sequenz abelscher Gruppen.

$$\ldots \to \hat{H}^q(G, M') \to \hat{H}^q(G, M) \to \hat{H}^q(G, M'') \xrightarrow{\delta} \hat{H}^{q+1}(G, M') \to \ldots$$

Beweis. Wir verheften die langen exakten Sequenzen der Homologie und der Kohomologie. Dazu betrachten wir das folgenden Diagramm.

$$\begin{array}{ccccccccc} \ldots\to & H_1(G,M'') & \xrightarrow{\delta} & H_0(G,M') & \to & H_0(G,M) & \to & H_0(G,M'') & \to & 0 \\ & \downarrow & & \downarrow N^*_{M'} & & \downarrow N^*_{M} & & \downarrow N^*_{M''} & & \downarrow \\ & 0 & \to & H^0(G,M') & \to & H^0(G,M) & \to & H^0(G,M'') & \xrightarrow{\delta} & H^1(G,M') \to \ldots \end{array}$$

Dabei seien $N^*_{M'}$, N^*_{M} und $N^*_{M''}$ die Homomorphismen N* von 4.6.2 für die Moduln M', M bzw. M". Die beiden inneren Quadrate des Diagramms sind trivialerweise kommutativ. Für die beiden äußeren Quadrate folgt dies aus der Kommutativität der

inneren Quadrate und der Exaktheit der Zeilen des Diagramms. Die gesuchte exakte Sequenz erhält man nun aus diesem Diagramm auf Grund des Schlangen-Lemmas. Man beachte:

1. das Bild des Zusammenhangs-Homomorphismus δ links oben liegt ganz im Kern
$$\hat{H}^{-1}(G, M')$$
von N^*_M, (wegen der Kommutativität des linken Vierecks).
2. der Kern von $\hat{H}^{-1}(G, M') \to \hat{H}^{-1}(G, M)$ ist höchstens so groß wie der von
$$H_0(G, M') \to H_0(G, M)$$
und wegen 1. mindestens so groß wie das Bild des linken obereren δ. Insgesamt erhält man also die Gleichheit.

Die zu den obigen Argumenten dualen Argumente liefern die Existenz und Exaktheit der Sequenz rechts unten.
QED.

4.6.7 Volle Resolventen einer endlichen Gruppe G

Seien G eine endliche Gruppe und
$$P \xrightarrow{\varepsilon} \mathbb{Z} \to 0$$
eine Auflösung von $\mathbb{Z}$ durch endlich erzeugte freie Moduln über $\Lambda = \mathbb{Z}[G]$.[104] Wir wenden den Funktor Hom(? , $\mathbb{Z}$) an und erhalten einen Komplex
$$0 \to \mathbb{Z} \xrightarrow{\varepsilon^*} P^*$$
Dieser Komplex ist exakt, da die P_i freie $\mathbb{Z}$-Moduln sind. Wir setzen

$P_{-n} := P^*_{n-1}$ für $n = 1, 2, 3, ...$
und erhalten eine exakte Sequenz von freien Λ-Moduln
$$... \to P_1 \to P_0 \xrightarrow{\varepsilon^* \circ \varepsilon} P_{-1} \to P_{-2} \to ...$$
Eine exakte Sequenz dieser Gestalt heißt volle Resolvente der endlichen Gruppe G.

4.6.8 Die Tate-Kohomologie als Kohomologie zu einer vollen Resolvente

Seien G eine endliche Gruppe, M ein G-Modul und L eine volle Resolvente von G. Dann gilt
$$\hat{H}^q(G, M) = H^q(\mathrm{Hom}_G(L, M))$$
für jedes $q \in \mathbb{Z}$.
Beweis. Die Aussag ist trivial für $q \geq 1$. Zum Beweis der verbleibenden Aussagen unterscheiden wir die Fälle
$$q \leq -2,\ q = -1,\ q = 0.$$
1. Fall: $q \leq -2$.
Zum Beweis verwenden wir das folgende

Lemma

Seien C ein endlich erzeugter G-Modul, welcher als $\mathbb{Z}$-Modul frei ist, und
$$C^* := \mathrm{Hom}(C, \mathbb{Z})$$
der zugehörige duale G-Modul. Dann ist die folgende Abbildung für jeden G-Modul M ein Isomorphismus von G-Moduln[105].

---

[104] Zum Beispiel die Standard-Resolvente von 4.2.1.

[105] Die G-Modul-Struktur von $C \otimes M$ ist durch die von $\mathrm{Hom}(C^*, M)$ eindeutig festgelegt: für $g \in G$ ist das g-fache der Abbildung
$$f \;a\; f(c)\cdot m$$

$$C\otimes M \to \mathrm{Hom}(C^*, M),\ c\otimes m \mapsto (f \mapsto f(c)\cdot m).$$

Beweis des Lemmas. Die G-Modul-Struktur des Tensor-Produkts links ist so gewählt, daß die Abbildung ein G-Modul-Homomorphismus ist. Es reicht deshalb, deren Bijektivität zu beweisen.

Wir werden zeigen, die Abbildung ist bijektiv für jeden freien $\mathbb{Z}$-Modul C endlichen Rangs. Da beide Seiten mit direkten Summen kommutieren, können wir dazu annehmen,

$$C = \mathbb{Z}.$$

Die linke Seite ist dann isomorph zu M,

$$M \cong \mathbb{Z}\otimes M,\ m \mapsto 1\otimes m,$$

und die rechte Seite ebenfalls,

$$\mathrm{Hom}(\mathbb{Z}^*, M) \cong \mathrm{Hom}(\mathbb{Z}, M) \cong M,\ f \mapsto (g \mapsto f(g\cdot Id)) \mapsto f(Id).$$

Identifizieren wir so beide Seiten mit M, so bekommt die obige Abbildung die Gestalt

$$M \to \mathbb{Z}\otimes M \to \mathrm{Hom}(\mathbb{Z}^*, M) \to M,\ m \mapsto 1\otimes m \mapsto (f\mapsto f(1)\cdot m) \mapsto m,$$

d.h. wir erhalten die identischen Abbildung, welche in der Tat bijektiv ist.

QED (Lemma).

Aus dem Lemma ergibt sich, daß die folgende Komposition ein Isomorphismus ist.

$$(1)\qquad C\otimes_G M = (C\otimes M)_G \xrightarrow{N^*} (C\otimes M)^G \to \mathrm{Hom}(C^*, M)^G = \mathrm{Hom}_G(C^*, M).$$

$$[c\otimes m] \quad \mapsto N\cdot(c\otimes m) \mapsto \quad (f\mapsto \sum_{g\in G} f(gc)\cdot gm$$

Man beachte, N* ist ein Isomorphismus (nach 4.6.4), weil der Modul C⊗M induziert ist, d.h. seine Tate-Kohomologie ist Null, d.h. Kern und Kokern von N* sind trivial. Damit ist für $q \le -2$, wenn P die Standard-Resolvende bezeichnet,

$$\begin{aligned}
\check{H}^q(G, M) &= H_{-q-1}(G, M) && \text{(nach Definition von } \check{H}^q \text{ für } q \le -2)\\
&= H_{-q-1}(P\otimes_G M) && \text{(nach Definition der } H_i)\\
&= H_{-q-1}(\mathrm{Hom}_G(P^*, M)) && \text{(wegen (1))}\\
&= H^q(\mathrm{Hom}_G(L, M)) && (\text{wegen } L_q = P^*_{-q-1})
\end{aligned}$$

2. Fall: q = -1, 0:

Die Abbildung

$$(2)\qquad \mathrm{Hom}_G(P_{-1}, M) \to \mathrm{Hom}_G(P_0, M),\ f \mapsto f\circ\varepsilon^*\circ\varepsilon,$$

kommt von der Komposition

$$P_0 \xrightarrow{\varepsilon} \mathbb{Z} = \mathbb{Z}^* \xrightarrow{\varepsilon^*} P_{-1} = P_0^*,\ p \mapsto \varepsilon(p) = \varepsilon(p)\cdot Id \mapsto \varepsilon(p)\cdot Id\circ\varepsilon = \varepsilon(p)\cdot\varepsilon$$

Wir identifizieren den Modul

$$\mathrm{Hom}_G(P_{-1}, M) = \mathrm{Hom}_G(P_0^*, M)$$

mit Hilfe des Isomorphismus (1) mit dem Tensor-Produkt $P_0\otimes_G M$. Abbildung (2) bekommt dann die Gestalt

$$P_0\otimes_G M \to \mathrm{Hom}_G(P_0^*, M) \to \mathrm{Hom}_G(P_0, M),$$

---

die Abbildung

$$f\ a\ g\cdot((g^{-1}f)(c)\cdot m) = g(f(gc)\cdot m) = f(gc)\cdot gm.$$

Letztere ist das Bild des Elements $(gc)\otimes(gm) \in C\otimes M$. Die Operation von G auf C⊗M ist damit die folgende:

$$G \times C\otimes M \to C\otimes M,\ (g, c\otimes m)\ a\ (gc)\otimes(gm).$$

$$p\otimes m \quad \mapsto (f \mapsto \sum_{g\in G} f(gp)\cdot gm) \mapsto (\, p' \mapsto \varepsilon(p')\cdot\varepsilon \;\mapsto \varepsilon(p')\varepsilon(p) \sum_{g\in G} g\cdot m)$$

Diese Abbildung faktorisiert sich

$$P_0\otimes_G M \xrightarrow{\varepsilon\otimes 1} \mathbb{Z}\otimes_G M = M_G \xrightarrow{N^*} M^G = \mathrm{Hom}_G(\mathbb{Z}, M) \xrightarrow{\varepsilon^*} \mathrm{Hom}_G(P_0, M)$$

$$p\otimes m \quad \mapsto \varepsilon(p)\cdot m \bmod I_G M \quad \mapsto (\, z \mapsto z\cdot\varepsilon(p)N\cdot m\,) \mapsto (p' \mapsto \varepsilon(p')\varepsilon(p)Nm).$$

Weil ε^* injektiv ist, folgt

(3) $\quad \mathrm{Ker}\,(2) = \mathrm{Ker}(P_0\otimes_G M \xrightarrow{\varepsilon\otimes 1} \mathbb{Z}\otimes_G M = M_G \xrightarrow{N^*} M^G)$

Weil $\varepsilon\otimes 1$ surjektiv und ε^* injektiv ist, folgt

(4) $\quad \mathrm{Im}\,(2) = \mathrm{Im}(M_G \xrightarrow{N^*} M^G)\ (\subseteq \mathrm{Hom}_G(P_0, M))$

Es folgt

$$\begin{aligned} H^0(\mathrm{Hom}(L,M)) &= \mathrm{Ker}(\mathrm{Hom}_G(P_0, M) \to \mathrm{Hom}_G(P_1, M))/\mathrm{Im}\,(2) \\ &= \mathrm{Hom}_G(\mathbb{Z}, M)/\mathrm{Im}\,(2) && \text{(Linksexaktheit von Hom)} \\ &= M^G/\mathrm{Im}\,N^* && \text{(nach (4))} \\ &= \mathrm{Koker}\,N^* \\ &= \hat{H}^0(G, M) \end{aligned}$$

und

$$\begin{aligned} H^{-1}(\mathrm{Hom}(L,M)) &= \mathrm{Ker}\,(2)/\mathrm{Im}(P_1\otimes_G M \to P_0\otimes_G M) \\ &= \mathrm{Ker}(P_0\otimes_G M \xrightarrow{\varepsilon\otimes 1} \mathbb{Z}\otimes_G M = M_G \xrightarrow{N^*} M^G)/\mathrm{Im}(P_1\otimes_G M \to P_0\otimes_G M) \\ &=^{106} \mathrm{Ker}(P_0\otimes_G M \xrightarrow{\varepsilon\otimes 1} \mathbb{Z}\otimes_G M = M_G \xrightarrow{N^*} M^G)/\mathrm{Ker}(P_0\otimes_G M \to \mathbb{Z}\otimes_G M) \\ &= \mathrm{Ker}(N^*\colon M_G \to M^G) \\ &= \hat{H}_0(G, M) = \hat{H}^{-1}(G, M) \end{aligned}$$

QED.

4.6.9 Verschiebung des Kohomologischen Grades

Seien G eine endliche Gruppe und M ein G-Modul. Dann ist M ein Teilmodul eines koinduzierten Moduls, sagen wir M',

$$0 \to M \to M'$$

und Faktormodul eines induzierten Moduls, sagen wir M",

$$M'' \to M \to 0.$$

Wir haben damit kurze exakte Sequenzen von G-Moduln

$$0 \to M \to M' \to C \to 0$$
$$0 \to K \to M'' \to M \to 0$$

deren mittlere Moduln koinduziert bzw. induziert sind, also kohomologisch trivial bezüglich der Tate-Kohomologie,

$$\hat{H}^q(G, M') = \hat{H}^q(G, M'') = 0 \text{ für jedes } q\in\mathbb{Z}$$

(nach der Bemerkung von 4.6.5). Auf Grund der langen Kohomologie-Sequenz von 4.6.8 bestehen damit natürliche Isomorphismen

$$\hat{H}^q(G, M) \cong \hat{H}^{q-1}(G, C) \cong \hat{H}^{q+1}(G, K).$$

---

[106] weil $\otimes$ rechtsexakt ist.

Dies wird uns im folgenden oft in die Lage versetzen, Aussagen über die Tate-Kohomologie durch Induktion nach q zu beweisen und entsprechende induktive Konstruktionen durchzuführen.

4.6.10 Restriktion und Korestriktion für die Tate-Kohomologie

Sei H eine Untergruppe der endlichen Gruppe G. Dann ist die Restriktion

$$\text{Res: } H^q(G, M) \to H^q(H, M)$$

für jedes $q \geq 0$ definiert. Für die Tate-Kohomologie,

(1) $$\text{Res: } \hat{H}^q(G, M) \to \hat{H}^q(H, M)$$

ist sie damit für jedes $q \geq 1$ definiert. Da Res mit den Zusammenhangshomomorphismen zu kurzen exakten Sequenzen kommutiert, erhalten wir damit eine Definition von Res für beliebige

$$q \in \mathbb{Z},$$

(denn jedes $\hat{H}^q$ läßt sich nach 4.6.9 als ein $\hat{H}^{q+1}$ auffassen).
Analog ist die Korestriktion

$$\text{Cor: } H_q(H, M) \to H_q(G, M)$$

für jedes $q \geq 0$ definiert, also nach 4.6.5

$$\text{Cor: } \hat{H}^q(H, M) \to \hat{H}^q(G, M)$$

für jedes $q \leq -2$. Da Cor mit den Zusammenhangshomomorphismen zu kurzen exakten Sequenzen kommutiert, erhalten wir damit eine Definition von Cor für beliebige

$$q \in \mathbb{Z},$$

(denn jedes $\hat{H}^q$ läßt sich nach 4.6.9 als ein $\hat{H}^{q-1}$ auffassen).

4.6.11 Proposition 6.2

Seien G eine endliche Gruppe, $H \subseteq G$ eine Untergruppe, M ein G-Modul und

$$\{g_i\}_{i=1}^{\ell}$$

ein Repräsentantensystem von G modulo H,

$$G = g_1 H \cup \ldots \cup g_\ell \text{ (disjunkte Vereinigung)}$$

Dann gilt:

(i) $\text{Res: } \hat{H}_0(G, M) \to \hat{H}_0(H, M)$ wird durch die folgende Abbildung induziert.

$$N'_{G/H}: M_G \to M_H, [m] \mapsto [\sum_{i=1}^{\ell} g_i^{-1} m].$$

(ii) $\text{Cor: } \hat{H}^0(H, M) \to \hat{H}^0(G, M)$ wird durch die folgende Abbildung induziert.

$$N_{G/H}: M^H \to M^G, [m] \mapsto \sum_{i=1}^{\ell} g_i m.$$

Beweis. Wir beschränken uns auf den Beweis von (i). Der Beweis von (ii) ist analog zu dem von (i). Sei

$$0 \to M' \to M^* \to M \to 0$$

eine kurze exakte Sequenz von G-Moduln mit

M^* induziert über G (also auch über H).

Dann ist die Abbildung

$$\text{Res} = \text{Res}^{-1}: \hat{H}^{-1}(G,M) = \hat{H}_0(G, M) \to \hat{H}_0(H, M) = \hat{H}^{-1}(H,M)$$

definiert durch die Kommutativität des oberen Vierecks von

(1)
$$\begin{array}{ccc} \hat{H}^{-1}(G,M) & \xrightarrow{Res^{-1}} & \hat{H}^{-1}(H,M) \\ \delta_G \downarrow \cong & & \cong \downarrow \delta_H \\ \hat{H}^{0}(G,M') & \xrightarrow{Res^{0}} & \hat{H}^{0}(H,M') \\ \uparrow & & \uparrow \\ M',G & \subseteq & M',H \end{array}$$

Man beachte, die Zusammenhangshomomorphismen δ_G und δ_H sind Isomorphismen, weil M* induziert ist über G und H. Nach Definition ist $\hat{H}^{-1}(G,M)$ der Kern der Abbildung

$$N_G: M_G \to M^G,\ [m] \mapsto \Big(\sum_{g\in G} g\Big)m.$$

und analog $\hat{H}^{-1}(H,M)$ der Kern von

$$N_H: M_H \to M^H,\ [m] \mapsto \Big(\sum_{h\in H} h\Big)m.$$

Folgendes Diagramm ist kommutativ:

$$\begin{array}{ccc} M_G & \xrightarrow{N_G} & M^G \\ \downarrow N'_{G/H} & & \cap \\ M_H & \xrightarrow{N_H} & M^H \end{array}$$

denn für $m\in M$ gilt

$$N_H(N'_{G/H}[m]) = N_H\Big(\Big[\sum_{i=1}^{\ell} g_i^{-1}\cdot m\Big]\Big) = \sum_{h\in H}\sum_{i=1}^{\ell} h\, g_i^{-1}\cdot m = \sum_{g\in G} gm = N_G([m]).$$

Insbesondere wird der Kern von N_G wird durch $N'_{G/H}$ in den Kern von N_H abgebildet, d.h. $N'_{G/H}$ induziert eine Abbildung

$$v := N'_{G/H}\,|_{Ker(N_G)} : \hat{H}^{-1}(G,M) \to \hat{H}^{-1}(H,M).$$

Wir haben zu zeigen, das obere Viereck von (1) bleibt kommutativ, wenn man in diesem Diagramm Res^{-1} durch v ersetzt, d.h. wir haben zu zeigen,

(2) $$Res^0(\delta_G[m]) = \delta_H(v[m]) \text{ für jedes } [m] \in \operatorname{Ker} N_G = \hat{H}^{-1}(G,M).$$

Der Rest des Beweises besteht in der Berechung der beiden Seiten von (2).

Berechnung der linken Seite von (2).

Wir erinnern zunächst daran, daß sich der Zusammenhangshomomorphismus δ_G mit Hilfe des Schlangenlemmas aus dem nachfolgenden Diagramm ergibt (vgl. 4.6.6).

(3)
$$\begin{array}{ccccccccc} \ldots \to H_1(G,M) & \xrightarrow{\delta} & H_0(G,M') & \to & H_0(G,M^*) & \to & H_0(G,M) & \to & 0 \\ \downarrow & & \downarrow N'_G & & \downarrow N^*_G & & \downarrow N_G & & \downarrow \\ 0 & \to & H^0(G,M') & \to & H^0(G,M^*) & \to & H^0(G,M) & \xrightarrow{\delta} & H^1(G,M') \to \ldots \end{array}$$

Seien

$$[m] \in \hat{H}^{-1}(G,M) = \operatorname{Ker} N_G \subseteq H_0(G,M) = M_G = M/I_G M$$

ein vorgegebenes Element,

$$[m^*] \in \hat{H}^{-1}(G,M^*) = \operatorname{Ker} N_G^* \subseteq H_0(G,M^*) = M_G^* = M^*/I_G M^*$$

ein Urbild von [m] und $m^* \in M^*$ ein Repräsentant von $[m^*] \in M^*/I_G M^*$. Dann ist das Bild

$$\bigcup_{m \in M}$$

von m^* bei der Abbildung $M^* \to M$ ein Repräsentant von $[m] \in M/I_G M$, und das Element

$$N_G^* m^* = \sum_{g \in G} g m^*$$

repräsentiert ein Element von $H^0(G,M')$[107], dessen natürliches Bild in

$$\text{Koker } N_G' = \hat{H}^0(G,M')$$

gerade

$$\delta_G[m] = [\sum_{g \in G} g m^*]$$

ist. Wenden wir auf beide Seiten die Abbildung Res^0 von (1) an. Da Res^0 durch die natürliche Inklusion $M'^G \to M'^H$ induziert wird, erhalten wir durch Übergang zum natürlichen Bild in $\text{Koker } N'_H = \hat{H}^0(H,M')$,

$$\text{Res}^0(\delta_G[m]) = [\sum_{g \in G} g m^*].$$

Berechnung der rechten Seite von (2).

Wir haben δ_H auf $v[m] = [\sum_{i=1}^{\ell} g_i^{-1} m]$ anzuwenden. Dazu gehen wir analog zur Bestimmung des Bildes bei δ_G vor, wobei wir das zu Diagramm (3) analoge Diagramm verwenden mit H anstelle von G. Unter Verwendung des oben gewählten Elements m^* erhalten wir

$$\delta_H(v[m]) = [\sum_{h \in H} h \cdot \sum_{i=1}^{\ell} g_i^{-1} m^*] = [\sum_{i=1}^{\ell} \sum_{h \in H} h g_i^{-1} m^*].$$

Da die g_i ein Repräsentantensystem von G/H bilden,, bilden die g_i^{-1} eines für H\G, d.h. es gilt

$$\delta_H(v[m]) = [\sum_{g \in G} g m^*] = \text{Res}^0(\delta_G[m]).$$

QED.

---

[107] Zunächst ist $N_G^* m^* = \sum_{g \in G} g m^*$ ein Element in $H^0(G,M^*) = M^{*G}$, dessen Bild in $H^0(G,M) = M^G$ nach Konstruktion gleich Null ist. Wegen der Exaktheit der unteren Zeile des Diagramms können wir es aber als Element vn $H^0(G,M') = M'^G$ auffassen.

4.6.12 Beispiel

Wir betrachten den Fall q = -2 und A = $\mathbb{Z}$. Dann ist

$$\hat{H}^{-2}(G, \mathbb{Z}) = H_1(G, \mathbb{Z}) \cong G/G'$$

die Faktorkommutatorgruppe und die Restriktion ist eine Abbildung

$$\text{Res: } G/G' \to H/H',$$

welche sich wie folgt beschreiben läßt. Die abelsche Gruppe G/G' ist dual zu ihrer Charaktergruppe Hom(G, $\mathbb{C}^*$). Deshalb ist Res dual zu einem Homomorphismus

$$\text{Hom}(H, \mathbb{C}^*) \to \text{Hom}(G, \mathbb{C}^*).$$

Dieser genügt der folgenden Abbildungsvorschrift

$$\rho \mapsto \det(i_*\rho)/\det(i_*1).$$

Dabei bezeichnet

$$i_*\rho: G \to \text{Aut}(\mathbb{C} \otimes_{\mathbb{Z}[H]} \mathbb{Z}[G])$$

die durch die eindimensionale Darstellung ρ: H $\to$ $\mathbb{C}^*$ = Aut($\mathbb{C}$) induzierte Darstellung.[108]

4.6.13 Proposition

Seien G eine endliche Gruppe und H $\subseteq$ G eine Untergruppe vom Index

$$n = (G:H)$$

und M ein G-Modul.

Dann ist die Zusammensetzung

$$\hat{H}^q(G, M) \xrightarrow{\text{Res}} \hat{H}^q(H, M) \xrightarrow{\text{Cor}} \hat{H}^q(G, M)$$

für jedes q gerade die Multiplikation mit n,

$$\text{Cor} \circ \text{Res} = n.$$

Beweis. Der Fall q = 0. Nach Definition von n gibt es ein Repräsentantensystem

$$\{g_i\}_{i=1}^{n}$$

der Restklassen modulo H in G. Nach 4.6.11 (ii) ist die Korestriktion für q = 0 gerade die Abbildung, für welche das folgende Diagramm kommutativ ist.

$$\begin{array}{ccc} \hat{H}^0(H,M) & \xrightarrow{\text{Cor}} & \hat{H}^0(G,M) \\ \uparrow & & \uparrow \\ M^H & \to & M^G \\ m & \mapsto & \sum_{i=1}^{n} g_i m \end{array}$$

Die Restriktion dagegen ist induziert durch natürliche Einbettung $M^G \subseteq M^H$. Für $m \in M^G$ gilt aber

$$\sum_{i=1}^{n} g_i m = \sum_{i=1}^{n} m = n \cdot m,$$

d.h. Cor$\circ$Res: $\hat{H}^0(G, M) \to \hat{H}^0(G, M)$ ist die Multiplikation mit n.

---

[108] Sei $\{g_i\}_{i=1}^{l}$ ein Repräsentantensystem in G der Restklassen von G modulo H. Man verwende die Tatsache, daß dann die g_i ein freies Erzeugendensystem von $\mathbb{Z}[G]$ über $\mathbb{Z}[H]$ bilden, also die $1 \otimes g_i$ eines von $\mathbb{C} \otimes_{\mathbb{Z}[H]} \mathbb{Z}[G]$ über $\mathbb{C}$.

Der Fall $q \neq 0$. Für jedes q kann $Cor \circ Res: \hat{H}^q(G, M) \to \hat{H}^q(G, M)$ nach 4.6.9 mit einer Abbildung der Gestalt $Cor \circ Res: \hat{H}^0(G, M') \to \hat{H}^0(G, M')$ identifiziert werden (mit geeignet gewähltem M').
QED.

4.6.14 Folgerung 1
Seien G eine Gruppe der Ordnung n und M ein G-Modul. Dann gilt

$$n \cdot \hat{H}^q(G, M) = 0$$

für jedes $q \in \mathbb{Z}$.
Beweis. Nach 4.6.13 ist die Abbildung

$$\hat{H}^q(G, M) \xrightarrow{Res} \hat{H}^q(\{e\}, M) \xrightarrow{Cor} \hat{H}^q(G, M)$$

gerade die Multiplikation mit n. Als Modul über der trivialen Gruppe {e} ist aber M ein induzierter Modul,

$$\mathbb{Z}[\{e\}] \otimes M = \mathbb{Z} \otimes_{\mathbb{Z}} M = M.$$

Die Kohomologie-Gruppe in der Mitte ist somit trivial. Also ist die Multiplikation mit n gerade die Null-Abbildung.
QED.

4.6.15 Folgerung 2
Seien G eine endliche Gruppe und M ein eindlich erzeugter G-Modul. Dann ist die Gruppe

$$\hat{H}^q(G, M) \text{ für jedes } q \in \mathbb{Z}$$

endlich.
Beweis. Die Standard-Resolvente

$$P_*(G) \to \mathbb{Z} \to 0$$

besteht aus endlich erzeugten $\mathbb{Z}$-Moduln. Wenn M endlich erzeugt ist über $\mathbb{Z}[G]$, also auch über $\mathbb{Z}$, so gilt dasselbe auch für die Moduln von

$$\mathrm{Hom}(P_*(G), M)$$

also auch für die Moduln des Teilkomplexes

$$\mathrm{Hom}_G(P_*(G), M)$$

Dann sind aber auch die Kohomologie-Moduln

$$H^q(G, M) = H^q(\mathrm{Hom}_G(P_*(G), M))$$

endlich erzeugte $\mathbb{Z}$-Moduln. Analog ergibt sich, daß auch die

$$H_q(G, M)$$

endlich erzeugt sind. Zusammen erhalten wir, die $\mathbb{Z}$-Moduln

(1) $$\hat{H}^q(G,M) \text{ , } q \in \mathbb{Z},$$

sind endlich erzeugt. Nach 4.6.14 liegt aber die Gruppen-Ordunung n = #G im Annullator, d.h. die $\mathbb{Z}$-Moduln (1) sind Faktormoduln von freien $\mathbb{Z}/(n)$-Moduln endlichen Rangs, also endlich.
QED.

4.6.16 Folgerung 3
Seien G eine endliche Gruppe, $S \subseteq G$ eine p-Sylow-Untergruppe von G und M ein G-Modul. Dann ist die Abbildung

$$Res: \hat{H}^q(G, M) \to \hat{H}^q(S, M)$$

ein Monomorphismus auf dem p-Torsionsteil[109] von $\hat{H}^q(G, M)$.
Beweis. Sei G von der Ordnung

$$\# G = p^{\alpha}m,$$

mit m teilerfremd zu p. Weiter sei

$$x \in \hat{H}^q(G, M)$$

ein Element des p- Torsionsteils mit

$$\mathrm{Res}(x) = 0.$$

Dann gilt nach 4.6.13

$$mx = (G:S)x = \mathrm{Cor}(\mathrm{Res}(x)) = 0.$$

Nach Voraussetzung wird x von einer p-Potenz annulliert,

$$p^{\ell}x = 0$$

für ein $\ell \in \mathbb{N}$. Da m und p^{ℓ} teilerfremd sind, läßt sich 1 als $\mathbb{Z}$-Linearkombination von m und p^{ℓ} schreiben. Aus $mx = 0$ und $p^{\ell}x = 0$ folgt damit $x = 0$.
QED.

4.6.17 Folgerung 4
Seien G eine endliche Gruppe, M ein G-Modul und

$$x \in \hat{H}^q(G, M)$$

ein Element, dessen Bild bei

$$\mathrm{Res}: \hat{H}^q(G, M) \to \hat{H}^q(S, M)$$

für jede Sylow-Untergruppe $S \subseteq G$ Null ist. Dann gilt

$$x = 0.$$

Beweis. Da G endlich ist, liegen alle Werte eines jede Kozyklus bereits in einem endlich erzeugten Teilmodul von M. Ist I das induktive System der endlich erzeugten Teilmoduln von M, so gilt

$$\hat{H}^q(G, M) = \varinjlim_{M' \in I} \hat{H}^q(G, M')$$

und

$$\hat{H}^q(S, M) = \varinjlim_{M' \in I} \hat{H}^q(S, M').$$

Es reicht deshalb, die Behauptung für den Fall, daß

M endlich erzeugter G-Modul

ist, zu beweisen. Dann zerfallen aber

$$\hat{H}^q(G, M) \text{ und } \hat{H}^q(S, M)$$

als $\mathbb{Z}$-Moduln in direkte Summen von p-Torsionsmoduln, wobei p die Teiler der Gruppenordnung von G durchläüft (wegen 4.6.14). Bei Res werden diese p-Torsionsmoduln ineinander abgebildet (wie bei jeden beliebigen Gruppen-Homomorphsmus). Nun ist der p-Torsionsteil von

Res(x)

für jedes p gleich Null, d.h. der p-Torsionsteil von x ist nach 4.6.16 für jedes p gleich Null. Da dies für jedes p gilt, ist $x = 0$.
QED.

4.7 Das Cup-Produkt

4.7.1 Theorem 7.1
Sei G eine endliche Gruppe. Dann gibt es für beliebige

---

[109] d.h. auf der Menge der Elemente, die von einer Potenz von p annulliert weriden.

$$p,q \in \mathbb{Z}$$

und beliebige G-Moduln M und N eindeutig bestimmte Homomorphismen

$$\hat{H}^p(G, M) \otimes \hat{H}^q(G,N) \to \hat{H}^{p+q}(G, M \otimes N),\ m \otimes n \mapsto^{110} m \cdot n,$$

welche den folgenden Bedingungen genügen.

(i) Die Homomorphismen hängen in funktorieller Weise von M und N ab.

(ii) Für $p = q = 0$ sind die Homomorphismen durch die natürliche Abbildung

$$M^G \otimes N^G \to (M \otimes N)^G$$

induziert.

(iii) Ist

$$0 \to M' \to M \to M'' \to 0$$

eine exakte Sequenz von G-Moduln mit der Eigenschaft, daß die induzierte Sequenz

$$0 \to M' \otimes N \to M \otimes N \to M'' \otimes N \to 0$$

exakt ist, so gilt

$$\delta_N(m'' \cdot n) = (\delta m'') \cdot n \text{ für } m'' \in \hat{H}^p(G, M'') \text{ und } n \in \hat{H}^q(G,N).$$

Dabei sei

$$\delta: \hat{H}^p(G, M'') \to \hat{H}^{p+1}(G, M')$$

der Zusammenhangshomomorphismus zur ersten und

$$\delta_N: \hat{H}^{p+q}(G, M'' \otimes N) \to \hat{H}^{p+q+1}(G, M' \otimes N)$$

der Zusammenhangshomomorphismus zur zweiten kurzen exakten Sequenz.

(iv) Ist

$$0 \to N' \to N \to N'' \to 0$$

eine exakte Sequenz von G-Moduln mit der Eigenschaft, daß die induzierte Sequenz

$$0 \to M \otimes N' \to M \otimes N \to M \otimes N'' \to 0$$

exakt ist, so gilt

$$\delta_M(m \cdot n'') = (-1)^p m \cdot \delta(n'') \text{ für } m \in \hat{H}^p(G, M) \text{ und } n'' \in \hat{H}^q(G,N'').$$

Dabei sei

$$\delta: \hat{H}^p(G, N'') \to \hat{H}^{p+1}(G, N')$$

der Zusammenhangshomomorphismus zur ersten und

$$\delta_M: \hat{H}^{p+q}(G, M \otimes N'') \to \hat{H}^{p+q+1}(G, M \otimes N')$$

der Zusammenhangshomomorphismus zur zweiten kurzen exakten Sequenz.

Bemerkung

Das Bild $m \cdot n$ von $m \otimes n$ der oben beschriebenen Abbildung heißt dann Cup-Produkt der Kohomologie-Klassen m und n.

Beweis. Wir beginnen damit, den Existenzbeweis auf den Beweis der folgenden Aussage zu reduzieren.

Lemma

Sei

$$P: \ldots \xrightarrow{d} P_{n+1} \xrightarrow{d} P_n \xrightarrow{d} P_{n-1} \xrightarrow{d} \ldots$$

eine volle Resolvente (vgl. 4.6.7). Dann gibt es einen Homomorphismus von G-Moduln

$$\varphi_{p,q}: P_{p+q} \to P_p \otimes P_q$$

für je zwei ganze Zahlen $p, q \in \mathbb{Z}$, wobei die folgenden Bedingungen erfüllt sind.

(1) $\varphi_{p,q} \circ d = (d \otimes 1) \circ \varphi_{p+1,q} + (-1)^p (1 \otimes d) \circ \varphi_{p,q+1}$

(2) $(\varepsilon \otimes \varepsilon) \circ \varphi_{0,0} = \varepsilon.$

---

[110] Wir bezeichnen das Bild von $m \otimes n$ bei dieser Abbildung mit $m \cdot n$.

Dabei sei

$$\varepsilon: P_0 = \mathbb{Z}[G] \to \mathbb{Z}$$

der G-Modul-Homomorphismus mit $\varepsilon(g) = 1$ für jedes $g \in G$.

Nehmen wir also an, die Abbildungen $\varphi_{p,q}$ sind bereits konstruiert. Für je zwei G-Moduln M und N und je zwei Koketten

$$f \in \mathrm{Hom}(P_p, M) \text{ und } g \in \mathrm{Hom}(P_q, N)$$

setzen wir

$$f \cdot g := (f \otimes g) \circ \varphi_{p,q} : P_{p+q} \to M \otimes N.$$

Auf Grund von (1) gilt dann

$$d(f \cdot g) = (df) \cdot g + (-1)^p f \cdot dg \tag{3}$$

Insbesondere ist $f \cdot g$ ein Kozyklus, wenn f und g Kozyklen sind und die Kohomologie-Klasse von $f \cdot g$ hängt nur von den Kohomologie-Klassen von f und g ab.[111] Mit anderen Worten, die Abbildungen $\varphi_{p,q}$ induzieren für beliebige G-Moduln M und N Gruppen-Homomorphismen

$$\varphi_{p,q^*} : \hat{H}^p(G, M) \otimes \hat{H}^q(G, N) \to \hat{H}^{p+q}(G, M \otimes N),\ [f] \otimes [g] \mapsto [f \cdot g].$$

Diese Konstruktion ist offensichtlich funktoriell bezüglich M und N, d.h. sie hat die Eigenschaft (i) der Behauptung.

Zu Eigenschaft (ii).

Auf Grund von (2) ist das Diagramm

$$\begin{array}{ccccc} P_0 \otimes P_0 & \xrightarrow{\varepsilon \otimes \varepsilon} & \mathbb{Z} \otimes \mathbb{Z} & \varphi_{0,0}(z) & x \otimes y \mapsto \varepsilon(x) \otimes \varepsilon(y) \\ \varphi_{0,0} \uparrow & & \uparrow \cong & \uparrow & \uparrow \\ P_0 & \xrightarrow{\varepsilon} & \mathbb{Z} & z & 1 \otimes 1 \\ & & & z \mapsto \varepsilon(z) & 1 \end{array}$$

Anwenden von $\mathrm{Hom}_G(\,?\,, M \otimes N)$ liefert ein kommutatives Diagramm

$$\begin{array}{ccc} \mathrm{Hom}_G(P_0 \otimes P_0, M \otimes N) & \xleftarrow{(\varepsilon \otimes \varepsilon)^*} & \mathrm{Hom}_G(\mathbb{Z} \otimes \mathbb{Z}, M \otimes N) \\ \varphi_{0,0}^* \downarrow & & \downarrow \cong \\ \mathrm{Hom}_G(P_0, M \otimes N) & \xleftarrow{\varepsilon^*} & \mathrm{Hom}_G(\mathbb{Z}, M \otimes N) \\ \cup & & || \\ H^0(G, M \otimes N) & \xleftarrow{\cong} & (M \otimes N)^G \end{array} \tag{4}$$

Nun ist die Abbildung,

$$\mathrm{Hom}_G(P_0, M) \times \mathrm{Hom}_G(P_0, N) \to \mathrm{Hom}_G(P_0 \otimes P_0, M \otimes N),\ (f,g) \mapsto f \otimes g,,$$

bilinear, induziert also eine natürliche Abbildung

$$\mathrm{Hom}_G(P_0, M) \otimes \mathrm{Hom}_G(P_0, N) \to \mathrm{Hom}_G(P \otimes P, M \otimes N),\ (f,g) \mapsto f \otimes g,,$$

Analog erhält man eine Abbildung

---

[111] Aus (3) mit f = df' folgt

$$d(df' \cdot g) = (-1)^p f \cdot dg$$

und analog auf (3) mit g = dg':

$$d(f \cdot dg') = df \cdot g.$$

Mit anderen Worten das Produkt $f \cdot g$ ist ein Rand, wenn einer der Faktoren ein Rand ist. Also ändert sich $f \cdot g$ um einen Rand ab, wenn man einen der Faktoren um einen Rand abändert.

$$\mathrm{Hom}_G(\mathbb{Z}, M) \otimes \mathrm{Hom}_G(\mathbb{Z}, N) \to \mathrm{Hom}_G(\mathbb{Z} \otimes \mathbb{Z}, M \otimes N),\ (f,g) \mapsto f \otimes g,.$$

Die beiden letzten Abbildungen bilden die Spalten eines kommutativen Vierecks. Durch Zusammensetzen mit (4) erhalten wir ein kommutatives Diagramm

$$\begin{array}{ccc}
H^0(G, M)\otimes H^0(G, N) & \xleftarrow{\cong} & M^G \otimes N^G \\
\downarrow & & \| \\
\mathrm{Hom}_G(P_0, M)\otimes \mathrm{Hom}_G(P_0, N) & \xleftarrow{\varepsilon^*\otimes\varepsilon^*} & \mathrm{Hom}_G(\mathbb{Z}, M)\otimes \mathrm{Hom}_G(\mathbb{Z}, N) \\
\downarrow & & \downarrow \\
\mathrm{Hom}_G(P_0; M\otimes N) & \xleftarrow{\varepsilon^*} & \mathrm{Hom}_G(\mathbb{Z}, M\otimes N) \\
\cup & & \| \\
H^0(G, M\otimes N) & \xleftarrow{\cong} & (M\otimes N)^G
\end{array}$$

also ein kommutatives Diagramm

$$\begin{array}{ccc}
H^0(G, M)\otimes H^0(G, N) & \xleftarrow{\cong} & M^G \otimes N^G \\
\downarrow & & \downarrow \\
H^0(G, M\otimes N) & \leftarrow & (M\otimes N)^G
\end{array}$$

Wir faktorisieren nach den Bildern der Abbildung N_N^* (vgl. 4.6.2) und erhalten ein kommutatives Diagramm

$$\begin{array}{ccc}
\hat{H}^0(G,M)\otimes \hat{H}^0(G,N) & \xrightarrow{\varphi_{0,0}^*} & \hat{H}^0(G; M\otimes N) \\
\uparrow & & \uparrow \\
M^G \otimes N^G & \to & (M\otimes N)^G
\end{array}$$

Mit anderen Worten, die von uns konstruierten Abbildungen φ_{p,q^*} haben die Eigenschaft (ii).

Zu Eigenschaft (iii). Sei

$$0 \to M' \to M \to M'' \to 0$$

eine exakte Sequenz von G-Moduln mit der Eigenschaft, daß die induzierte Sequenz

$$0 \to M'\otimes N \to M\otimes N \to M''\otimes N \to 0$$

exakt ist. Wir wenden auf die erste Sequenz die Funktoren

$$\mathrm{Hom}_G(P_p, ?) \text{ und } \mathrm{Hom}_G(P_{p+1}, ?)$$

an und erhalten ein kommutatives Diagramm mit exakten Zeilen[112]:

$$\begin{array}{ccccccc}
0\to & \mathrm{Hom}_G(P_p, M') & \to & \mathrm{Hom}_G(P_p, M) & \to & \mathrm{Hom}_G(P_p, M'') & \to 0 \\
& d\downarrow & & d\downarrow & & d\downarrow & \\
0\to & \mathrm{Hom}_G(P_{p+1}, M') & \to & \mathrm{Hom}_G(P_{p+1}, M) & \to & \mathrm{Hom}_G(P_{p+1}, M'') & \to 0
\end{array}$$

Die Zeilen sind tatsächlich exakt, weil P_p und P_{p+1} freie $\mathbb{Z}[G]$-Moduln sind.

Sei

$$\alpha'' \in \mathrm{Hom}_G(P_p, M'')$$

ein Kozyklus, welcher die Kohomologie-Klasse

$$m'' = [\alpha''] \in \hat{H}^p(G, M'')$$

Repräsentiert. Wir wählen ein Urbild

---

[112] Genauer: wir wenden den Funktor $\mathrm{Hom}_G(P_*, ?)$ auf die exakte Sequenz an und erhalten eine kurze exakte Sequenz von Komplexen.

$$\alpha \in \mathrm{Hom}_G(P_p, M)$$

ein Urbild von α". Dann ist das Bild von $d\alpha$ in $\mathrm{Hom}_G(P_{p+1}, M")$ gleich Null, d.h. es gilt

$$d\alpha \in \mathrm{Hom}_G(P_{p+1}, M').$$

Die Kohomologie-Klasse dieses Elements ist gerade $\delta(m")$,

$$\delta(m") = [d\alpha].$$

Für jeden Repräsentanten

$$\beta \in \mathrm{Hom}_G(P_q, N)$$

eines Elements

$$n = [\beta] \in \hat{H}^q(G, N)$$

ist

$\alpha"\cdot\beta$ ein Repräsentant von $m"\cdot n$,
$d\alpha$ ein Repräsentant von $\delta m"$

also

$(d\alpha)\cdot\beta$ ein Repräsentant von $(\delta m")\cdot n$

Indem wir anstelle der ersten kurzen exakten Sequenz die mit N tensorierte (d.h. die zweite kurze exakte Sequenz betrachten, sehen wir:

$d(\alpha\cdot\beta)$ ein Repräsentant von $\delta(m"\cdot n)$.

Weil β ein Kozyklus ist, gilt nach (3)

$d(\alpha\cdot\beta) = (d\alpha)\cdot\beta$,

d.h. $\delta(m"\cdot n)$ und $(\delta m")\cdot n$ werden durch dasselbe Element repräsentiert. Also gilt

$\delta(m"\cdot n) = (\delta m")\cdot n$.

Damit ist Eigenschaft (iii) bewiesen.

Zu Eigenschaft (iv): der Beweis ist analog zu dem für Eigenschaft (iii).

Damit ist der Existenzbeweis für das Cup-Produkt auf den Beweis des Lemmas zurückgeführt, d.h. auf die Konstruktion der Abbildungen

$$\varphi_{p,q}: P_{p+q} \to P_p \otimes P_q$$

mit den Eigschaften (1) und (2).

Beweis des Lemmas. Es reicht, die Konstruktion der $\varphi_{p,q}$ mit den Eigenschaften (1) und (2) für den Fall der vollen Standard-Resolvente durchzuführen, d.h. für den Fall

$P_q = \mathbb{Z}[G^{q+1}]$ für $q \geq 0$ und

$P_{-q} = P^*_{q-1} := \mathrm{Hom}(P_{q-1}, \mathbb{Z})$ für $q \geq 1$.

(vgl. 4.6.7) durchzuführen.[113] Der G-Modul P_{-q} $(q\geq 1)$ besitzt als Basis die q-Tupel

$$g^* := (g_1^*, \ldots, g_q^*): \mathbb{Z}[G^q] \to \mathbb{Z}, \text{ mit } g_1,\ldots,g_q \in G$$

welche das Element $g := (g_1,\ldots,g_q)$ in die 1 und alle anderen Elemente aus G^q in die Null abbilden. Bezüglich dieser Basis ist der Randoperator

$$d: P_{-q} \to P_{-q-1}$$

durch die folgende Formel gegeben $(h= (h_0,\ldots,h_q) \in H^{q+1})$

---

[113] Obwohl das für den Existenzbeweis hier nicht gebraucht wird, wollen wir anmerken, daß sich daraus die Aussage für jede volle Resolvente ergibt, denn nach dem Vergleichssatz der homologischen Algebra sind je zwei freie Auflösungen von $\mathbb{Z}$ über $\mathbb{Z}[G]$ homotop.

$$dg^*(h) = g^*(dh) = g^*(\sum_{i=0}^{q} (-1)^i(h_0,...,h_{i-1},h_{i+1},...,h_q))$$

$$= \sum_{i=0}^{q} (-1)^i g^*(h_0,...,h_{i-1},h_{i+1},...,h_q)$$

$$= \sum_{i=0}^{q} (-1)^i \delta_{g_1 h_0} \cdot ... \cdot \delta_{g_i h_{i-1}} \delta_{g_{i+1} h_{i+1}} \cdot ... \cdot \delta_{g_q h_q}$$

$$=^{114} \sum_{s\in G} \sum_{i=0}^{q} (-1)^i \delta_{g_1 h_0} \cdot ... \cdot \delta_{g_i h_{i-1}} \delta_{s h_i} \delta_{g_{i+1} h_{i+1}} \cdot ... \cdot \delta_{g_q h_q}$$

$$= \sum_{s\in G} \sum_{i=0}^{q} (-1)^i (g_1^*, ... ,g_i^*,s^*,g_{i+1}^*,...,g_q^*)(h),$$

d.h. durch

$$d(g_1^*, ... ,g_q^*) = \sum_{s\in G} \sum_{i=0}^{q} (-1)^i (g_1^*, ... ,g_i^*,s^*,g_{i+1}^*,...,g_q^*).$$

Die Abbildung

$$d:P_0 \to P_{-1}$$

ist gegeben durch

$$dg_0 = \sum_{s\in G} (s^*).$$

Bei der Definition von $\varphi_{p,q}$ unterscheiden wir drei Fälle.

(a) Für $p\geq 0$ und $q\geq 0$ setzen wir

$$\varphi_{p.q}(g_0,...,g_{p+q}) := (g_0,...,g_p)\otimes(g_p,...,g_{p+q}).$$

(b) Für $p\geq 1$ und $q\geq 1$ setzen wir

$$\varphi_{-p.-q}(g_1^*,...,g_{p+q}^*) := (g_1^*,...,g_p^*)\otimes(g_p^*,...,g_{p+q}^*).$$

(c) Für $p\geq 0$ und $q\geq 1$ setzen wir[115]

$$\varphi_{p,-p-q}(g_1^*,...,g_q^*) = \sum_{s_1,...,s_p\in G} (g_1,s_1,...,s_p)\otimes(s_p^*,...,s_1^*,g_1^*,...,g_q^*)$$

$$\varphi_{-p-q,p}(g_1^*,...,g_q^*) = \sum_{s_1,...,s_p\in G} (g_1^*,...,g_q^*, s_1^*,..., s_p^*)\otimes(s_p,...,s_1,g_q)$$

$$\varphi_{p+q,-q}(g_0,...,g_p) = \sum_{s_1,...,s_p\in G} (g_0,...,g_p,s_1,...,s_q)\otimes(s_q^*,...,s_1^*)$$

$$\varphi_{-q,p+q}(g_0,...,g_p) = \sum_{s_1,...,s_p\in G} (s_1^*,...,s_q^*)\otimes(s_q,...,s_1, g_0,...,g_p)$$

---

[114] Die äußere Summe hat nur für $s = h_i$ einen von Null verschiedenen Summanden.

[115] Im letzten Fall haben die beiden Indizes verschiedene Vorzeichen. In den ersten beiden Fällen ist die Summe der beiden Indizes negativ, in den letzten beiden nicht-negativ. Die ungeraden unterscheiden sich von den geraden Fällen durch die Position des negativen bzw. positiven Vorzeichens.

Durch unmittelbare aber langwierige Rechnung zeigt man, die so definierten Abbildungen Eigenschaft (1) besitzen. Eigenschaft (2) liest man direkt and der Definitin von $\varphi_{0,0}$ in (a) ab.
Damit ist der Existenzbeweis abgeschlossen.

Eindeutigkeitsbeweis. Beim Beweis der Eindeutigkeit geht man von Eigenschaft (ii) aus und verwendet Dimensionsverschiebung und die Eigenschaften (iii) und (iv).
Um die Dimensionsverschiebung bezüglich des ersten Tensorfaktors M durchzuführen, verwendet man die exakte Sequenz
(5) $$0 \to M' \to M_* \to M \to 0$$

mit dem induzierten G-Modul

$$M_* = \mathbb{Z}[G] \otimes M.$$

Die kurze exakte Sequenz verfällt über $\mathbb{Z}$, denn die $\mathbb{Z}$-lineare Abbildung

$$M \to M_*,\ m \mapsto 1 \otimes m,$$

ist ein Schnitt der natürlichen Projektion $M_* \to M$, $g \otimes m \mapsto gm$. Weil die Sequenz verfällt, ist für jeden G-Modul N die induzierte Sequenz
(6) $$0 \to M' \otimes N \to M_* \otimes N \to M \otimes N \to 0$$

Außerdem ist der Modul

$$M_* \otimes N = \mathbb{Z}[G] \otimes M \otimes N$$

induziert. Die Zusammenhangshomomorphismen der Tate-Kohomologie-Sequenzen zu den kuzen exakten Sequenzen (5) und (6) sind deshalb Isomorphismen. Sie gestatten es, die Cup-Produkte zu den Moduln M und N mit den Cup-Produkten zu den Moduln M' und N zu identifizieren, wobei eine Dimensionsverschiebung um 1 auftritt. Induktiv ergibt sich so aus den Formeln von (iii) die Eindeutigkeit der Cup-Produkt-Abbildungen für alle p und ein festes q (wenn man sie für ein p bereits bewiesen hat).

Analog geht zeigt man unter Verwendung von (iv) die Eindeutigkeit für alle q und festes p (wenn man sie für ein q bereits bewiesen hat). Zusammen erhält man dann aus der Eindeutigkeit für $p = 0$ und $q = 0$ die Eindeutigkeit für alle p und alle q.
QED.

4.7.2 Proposition 7.1: Eigenschaften des Cup-Produkts

(i) $(m \cdot n) \cdot \ell = m \cdot (n \cdot \ell)$ (wenn man $(M \otimes N) \otimes L$ mit $M \otimes (N \otimes L)$ identifiziert.
(ii) $m \cdot n = (-1)^{\dim m \cdot \dim n}\ n \cdot m$ (wenn man $M \otimes N$ mit $N \otimes N$ identifiziert.
(iii) $\mathrm{Res}(a \cdot b) = \mathrm{Res}(a) \cdot \mathrm{Res}(b)$.
(iv) $\mathrm{Cor}(m \cdot \mathrm{Res}(n)) = \mathrm{Cor}(m) \cdot n$.
Beweis. Zu (i). Für $p = q = 0$ gilt diese Formel, weil dann das Cup-Produkt nach 4.71(i) durch die natürliche Abbildung

$$M^G \otimes N^G \to (M \otimes N)^G,\ m \otimes n \mapsto m \otimes n,$$

induziert wird. Alle anderen Fälle beweist man durch Dimensionsverschiebung.
Zu (ii). Im Fall $p = q = 0$ ist die Aussage trivialerweise richtig. In den anderen Fällen beweist man sie durch Dimensionsverschiebung mit Hilfe der Formeln von 4.7.1 (iii) und (iv).
Zu (iii). Sei $H \subseteq G$ eine Untergruppe. Für $p = q = 0$ sind dann die Restriktionen induziert durch die natürlichen Einbettungen

$$M^G \to M^H \text{ und } N^G \to N^H \text{ und } (M \otimes N)^G \to (M \otimes N)^H$$

Da das Cup-Produkt in diesen Graden ebenfalls durch die natürlichen Abbildungen

$$M^G \otimes N^G \to (M \otimes N)^G,\ M^H \otimes N^H \to (M \otimes N)^H,\ m \otimes n \mapsto m \otimes n,$$

induziert wird, kommutieren diese beiden Operation.

Zu (iv). Seien G eine endliche Gruppe und $H \subseteq G$ eine Untergruppe, M und N zwei G-Moduln,

$$m \in \hat{H}^p(H, M) \text{ und } n \in \hat{H}(G, N).$$

Dann liegen die beiden Seiten der Identität (iv) in

$$\hat{H}^{p+q}(G, M \otimes N).$$

Wir betrachten zuerst den Fall

$$p = q = 0.$$

Wir wählen Repräsentanten

$$\mu \in M^H \text{ und } \nu \in N^G$$

von m bzw. n:

$$m = [\mu] \text{ und } n = [\nu].$$

Nach 4.6.11 Proposition 6.2(ii) wird die Korestriktion von m repräsentiert durch

$$N_{G/H}(\mu) = \sum_i g_i\mu, \in M^G$$

wenn die $g_i \in G$ ein Repräsentantensystem von G/H bilden:

$$\text{Cor}(m) = [\sum_i g_i\mu] \text{ in } \hat{H}^p(G, M).$$

Das Element $\text{Cor}(m) \cdot n \in \hat{H}^{p+q}(G, M \otimes N)$ wird also repräsentiert durch

$$N_{G/H}(\mu) \otimes \nu = (\sum_i g_i\mu, \otimes \nu) =^{116} \sum_i g_i(\mu, \otimes \nu) = N_{G/H}(\mu, \otimes \nu) \in (M \otimes N)^G,$$

d.h. für die linke Seite der zu beweisenden Identität erhalten wir

(1) $\text{Cor}(m) \cdot n = [N_{G/H}(\mu, \otimes \nu)]$.

Auf der anderen Seite wird $m \cdot \text{Res}(n)$ repräsentiert durch $\mu \otimes \nu \in (M \otimes N)^H$. Wiederum nach 4.6.11 Proposition 6.2(ii) erhalten wir

$\text{Cor}(m \cdot \text{Res}(n)) = [N_{G/H}(\mu \otimes \nu)]$.

Vergleich mit (1) liefert die gesuchte Identität für $p = q = 0$.

Für die übrigen p und q wird die Aussage durch Dimensionsverschiebung bewiesen unter Verwendung der Eigenschaften 4.7.1(iii) und (iv) des Cup-Produkts und der Tatsache, daß Restriktion und Kostriktion mit den Zusammenhangshomomorphismen kommutieren.

QED.

4.7.3 Eine Verallgemeinerung: Cup-Produkt bezüglich einer Abbildung

Im folgenden haben wir das Cup-Produkt in einer etwas allgemeineren Situation zu betrachten. Seien

$$L, M, N$$

irgendwelche Moduln über der endliche Gruppe G und

$$\varphi: M \otimes N \to L$$

ein G-Modul-Homomorphismus. Durch Zusammensetzen des Cup-Produkts mit der durch φ auf der Kohomologie induzierten Abbildung erhalten wir eine Abbildung

$$\hat{H}^p(G, M) \otimes \hat{H}^q(G, N) \to \hat{H}^{p+q}(G, L),\ m \otimes n \mapsto \varphi^*(m \cdot n).$$

Das Element $\varphi^*(m \cdot n)$ heißt auch Cup-Produkt von m und n bezüglich φ.

---

[116] Wegen $\nu \in N^G$ gilt $\nu = g_i\nu$.

4.8 Zyklische Gruppen, Herbrand-Index

4.8.1 Bezeichnung

Sei

$$G$$

eine zyklische Gruppe der Ordnung

$$\# G = n < \infty$$

mit dem Erzeuger s,

$$G = < s >.$$

Wir setzen

$$T = s-1$$

und wie bisher

$$N = \sum_{g \in G} g.$$

Gleichzeitig sollen T und N auch die Multiplikation mit T bzw. N bezeichnen.

4.8.2 Kern und Kokern der Abbildung T

Mit den Bezeichnungen von 4.8.1 gilt

(i) $\quad \mathrm{Ker}\,(\mathbb{Z}[G] \xrightarrow{T} \mathbb{Z}[G]) = \mathbb{Z}[G]^G = N\cdot\mathbb{Z}[G] = \mathrm{Im}\,(\mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G])$

(ii) $\quad \mathrm{Im}\,(\mathbb{Z}[G] \xrightarrow{T} \mathbb{Z}[G]) = I_G = \mathrm{Ker}\,(\mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G])$

Beweis. Zu (i). Für $x = \sum_{g \in G} x_g \cdot g$ gilt

$$x \in \mathrm{Ker}(T) \Leftrightarrow 0 = \sum_{g \in G} x_g \cdot g \cdot (s-1) = \sum_{g \in G} x_{gs^{-1}} g - \sum_{g \in G} x_g g = \sum_{g \in G} (x_{gs^{-1}} - x_g) \cdot g$$

$$\Leftrightarrow x_{gs^{-1}} = x_g \text{ für jedes } g \in G$$

$$\Leftrightarrow x_g = x_e \text{ für jedes } g \in G$$

$$\Leftrightarrow x = x_e \cdot \sum_{g \in G} g = x_e \cdot N$$

$$\Leftrightarrow^{117} x \in N\cdot\mathbb{Z}[G].$$

Zu (ii). Für $x = \sum_{g \in G} x_g \cdot g$ gilt

$$x \in \mathrm{Ker}(N) \Leftrightarrow 0 = N\cdot x = \sum_{g \in G} x_g N \cdot g = \left(\sum_{g \in G} x_g\right) \cdot N$$

$$\Leftrightarrow \sum_{g \in G} x_g = 0$$

$$\Leftrightarrow x = \sum_{g \in G} x_g \cdot g = \sum_{g \in G} x_g \cdot (g-1)$$

$$\Leftrightarrow^{118} x \in I_G$$

---

[117] Die Multiplikation von N mit einem Element von G hat denselben Effekt wie die mit 1.

Weil I_G als Ideal von $\mathbb{Z}[G]$ von Elementen der Gestalt g-1 erzeugt wird, gilt

$$\mathrm{Im}(T) \subseteq I_G.$$

Sei umgekehrt, $x \in I_G$. Wir haben noch zu zeigen, dann gilt

$$x \in \mathrm{Im}(T).$$

Wie wir gerade gesehen haben, ist

$$x = \sum_{g \in G} x_g \cdot (g-1).$$

Da die Multiplikation mit T eine $\mathbb{Z}$-lineare Abbildung ist, reicht es zu zeigen,

$$g-1 \in \mathrm{Im}(T) \text{ für jedes } g \in G.$$

Weil G zyklisch ist, hat g die Gestalt

$$g = s^u, \; u = 0, \ldots, n.$$

O.B.d.A. sei $u > 1$. Dann gilt aber

$$g - 1 = (s-1)(s^{u-1} + s^{u-2} + \ldots + 1) \in I_G$$

QED.

4.8.3 Eine volle Resolvente

Seien G eine zyklische Gruppe der Ordnung n mit dem Erzeuger s. Dann ist

$$K_*: \ldots \xrightarrow{d} K_{i+1} \xrightarrow{d} K_i \xrightarrow{d} \ldots$$

mit

$$K_i = \mathbb{Z}[G] \text{ für jedes i,}$$

und

$$d: K_i \to K_{i-1}, \begin{array}{ll} x \mapsto Tx & \text{für i ungerade} \\ x \mapsto Nx & \text{für i gerade} \end{array},$$

eine volle Resolvente von G.

Dabei sei wie bisher $T = s-1$ und $N = \sum_{g \in G} g$

Beweis. Nach 4.8.3 liefert die linke"Hälfte" von K_* eine exakte Sequenz:

$$(1) \qquad \ldots \xrightarrow{d} K_{i+1} \xrightarrow{d} K_i \xrightarrow{d} \ldots \xrightarrow{d} K_1 \xrightarrow{d\,(=T)} K_0 \xrightarrow{\varepsilon} \mathbb{Z} \to 0,$$

d.h. ein Resolvente von $\mathbb{Z}$ über $\mathbb{Z}[G]$. Nun ist das Dual der Multiplikation mit einem Ring-Element wieder die Multiplikation mit diesem Ring-Element. Durch Dualisieren von (1) erhalten wir also bis auf Isomorphie die Sequenz

$$0 \to \mathbb{Z} \xrightarrow{\varepsilon^*} K_{-1} \xrightarrow{d\,(=T)} K_2 \xrightarrow{d} \ldots \xrightarrow{d} K_i \xrightarrow{d} K_{i-1} \xrightarrow{d} \ldots$$

Wir haben noch zu zeigen, die Komposition

$$K_0 \xrightarrow{\varepsilon} \mathbb{Z} \xrightarrow{\varepsilon^*} K_{-1}$$

ist gerade die Multiplikation mit N. Für jedes $g \in G$ gilt

$$\varepsilon^*(\varepsilon(g)) = \varepsilon^*(1) = \varepsilon^*(\mathrm{Id}_{\mathbb{Z}}) = \mathrm{Id} \circ \varepsilon \in \mathrm{Hom}(\mathbb{Z}[G], \mathbb{Z}),$$

also

---

[118] Liegt x in I_G, so ist x $\mathbb{Z}$-Linearkombination von Elementen der Gestalt g-1. Insbesondere ist die Summe der Koeffizienten x_g gleich Null.

$$\varepsilon^*(\varepsilon(g)) =^{119} \sum_{y\in G},\ y^* =^{120} \sum_{y\in G},\ y = N$$

QED.

4.8.4 Die Tategruppen der $\mathbb{Z}_n$

Bezeichne $G = \mathbb{Z}_n$ die zyklische Gruppe der Orndung n und M einen G-Modul. Dann gilt

$$\hat{H}^q(G, M) = \begin{cases} M^G/NM & \text{für q gerade} \\ {}_NM/I_GM & \text{für q ungerade} \end{cases}$$

Dabei bezeichne ${}_NM$ den Kern der Abbildung $N: M \to M$,

$${}_NM := \mathrm{Ker}(M \xrightarrow{N} M).$$

Beweis. Wir wenden auf die volle Resolvente von 4.8.3 den Funktor $\mathrm{Hom}_{\mathbb{Z}_n}(?, M)$ an und erhalten

$$\mathrm{Hom}_G(K_*, M): \ldots \xrightarrow{d^*} \mathrm{Hom}_G(K_i, M) \xrightarrow{d^*} \mathrm{Hom}_G(K_{i+1}, M) \xrightarrow{d^*} \ldots$$

Dabei ist d* die Multiplikation mit N für i ungerade und die Multiplikation mit T für i gerade. Wegen $\mathrm{Hom}_G(K_i, M) \cong M$ für alle i, folgt

$$\hat{H}^q(G, M) = H^q(\mathrm{Hom}_{\mathbb{Z}_n}(K_*, M)) = \begin{cases} \mathrm{Ker}(N)/\mathrm{Im}\ T & \text{für q ungerade} \\ \mathrm{Ker}(T)/\mathrm{Im}\ N & \text{für q gerade} \end{cases}$$

Wegen 4.8.2 erhalten wir damit für ungerades q

$$\hat{H}^q(G, M) = {}_NM/I_G \cdot M$$

Für gerades q ist

$$\begin{aligned} \hat{H}^q(G, M) = \hat{H}^0(G, M) &= \mathrm{Koke}\ H_0(G, M) \xrightarrow{N} H^0(G, M) \\ &= \mathrm{Koker}\ M_G \xrightarrow{N} M^G \\ &= M^G/N \cdot M \end{aligned}$$

QED.

Beispiel

$$H^2(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) = \mathbb{Z}^G/N\mathbb{Z} = \mathbb{Z}/n\mathbb{Z}.$$

4.8.5 Das Cup-Produkt mit einem Erzeuger von $H^2(\mathbb{Z}_n, \mathbb{Z})$

Sei $G = \mathbb{Z}_n$ die zyklische Gruppe der Ordnung n und $u \in H^2(G, \mathbb{Z})$ ein Erzeuger. Dann induziert das Cup-Produkt mit u Isomorphismen

---

[119] Für $y \in G$ sei y* die Abildung, die jedes Element $x = \sum_{g\in G} x_g \cdot g$ auf dessen y-ten Koeffizienten x_y abbildet, d.h. $\sum_{y\in G},\ y^*$ bildet jedes Element auf die Summe von dessen Koeffizienten ab, genau wie ε.

[120] Wir identifizieren $\mathrm{Hom}(\mathbb{Z}[G], \mathbb{Z})$ mit $\mathbb{Z}[G]$.

$$\hat{H}^q(G,M) \to \hat{H}^{q+2}(G,M),\ x \mapsto u\cdot x$$

für beliebige $q\in\mathbb{Z}$ und beliebige G-Moduln M.

Beweis. Die beiden exakten Sequenzen

$$0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0 \qquad (1)$$

und

$$0 \to \mathbb{Z} \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{T} I_G \to 0 \qquad (2)$$

(vgl. 2) induzieren bijektive Zusammenhangshomomorphismen

$$\hat{H}^q(G, \mathbb{Z}) \xrightarrow{\delta} \hat{H}^{q+1}(G, I_G) \xrightarrow{\delta} \hat{H}^{q+2}(G, \mathbb{Z})$$

(weil $\mathbb{Z}[G] = \mathbb{Z}[G]\otimes\mathbb{Z}$ ein induzierter Modul ist). Insbesondere hat der Erzeuger u die Gestalt

$$u = \delta(\delta(v) \text{ mit einem Erzeuger v von } \hat{H}^0(G, \mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}.$$

Die beiden Sequenzen (1) und (2) zerfallen über $\mathbb{Z}$. Sie bleiben also exakt, wenn man mit M tensoriert,

$$0 \to I_G\otimes M \to \mathbb{Z}[G]\otimes M \to M \to 0$$

$$0 \to M \xrightarrow{N} \mathbb{Z}[G]\otimes M \xrightarrow{T} I_G\otimes M \to 0,$$

und wir erhalten Bijektionen

$$\hat{H}^q(G, M) \xrightarrow{\delta_M} \hat{H}^{q+1}(G, I_G\otimes M) \xrightarrow{\delta_M} \hat{H}^{q+2}(G, M)$$

Für $x\in\hat{H}^q(G, M)$ gilt

$$u\cdot x = \delta(\delta(v)\cdot x = \delta_M(\delta_M(v\cdot x)).$$

Deshalb reicht es zu zeigen, das Cup-Produkt mit dem Erzeuger v induziert einen Isomorphismus

$$\hat{H}^q(G, M) \to \hat{H}^q(G, M),\ x \mapsto v\cdot x.$$

Da das Cup-Produkt mit den Zusammenhangshomomorphismen verträglich ist, kann man Dimensionsverschiebung anwenden, d.h. es reicht, die Aussage für den Fall

$$q = 0$$

zu beweisen. Wir wählen eine Repräsentanten

$$\tilde{v} \in \mathbb{Z}$$

des Erzeugers

$$v \in \hat{H}^0(G, \mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}.$$

Dann ist $\tilde{v}$ eine zu n teilerfremde ganze Zahl und das Cup-Produkt für q = 0 ist gerade die Multiplikation mit dieser ganzen Zahl (nach 4.7.1 (ii)). Weil $\tilde{v}$ teilerfremd ist zu n, gibt es eine ganze Zahl $w\in\mathbb{Z}$ mit

$$w\cdot\tilde{v} \equiv 1 \bmod n.$$

Nun wird $\hat{H}^q(G, M)$ von der Gruppen-Ordnung annulliert (vgl. 4.6.14). Also sind definieren die Multiplikationen mit w und $\tilde{v}$ zueinander inverse Abbildungen. Insbesondere ist die Multiplikation mit $\tilde{v}$ ein Isomorphismus.

QED.

4.8.6 Der Herbrand-Index

Seien $G = \mathbb{Z}_n$ die zyklische Gruppe der Ordnung n und M ein beliebiger G-Modul.
Weiter bezeichne

$$h_q(M) := \#\,\hat{H}^q(G,M) \text{ für } q=0,1.$$

die Elementzahl der Tategruppe $\hat{H}^q(G,M)$. Falls falls diese beiden Zahlen endlich sind, definieren wir den Herbrand -Index von M als

$$h(M) := \frac{h_0(M)}{h_1(M)}.$$

4.8.7 Verhalten des Herbrand-Index bei exakten Sequenzen

Seien $G = \mathbb{Z}_n$ die zyklische Gruppe der Ordnung n und

$$0 \to M' \to M \to M'' \to 0$$

eine kurze exakte Sequenz von G-Moduln. Wenn dann zwei der Zahlen

$$h(M'),\ h(M),\ h(M'')$$

definiert sind, so ist es auch die dritte, und es gilt

$$h(M) = h(M') \cdot h(M'').$$

Beweis. Wegen der Periodizität der langen Kohomologiesequenz zur gegebenen kurzen exakten Sequenz, kann man diese in der folgenden Gestalt schreiben.

$$\begin{array}{ccc} \hat{H}^0(M') & \to & \hat{H}^0(M) \\ \uparrow & & \downarrow \\ \hat{H}^1(M'') & & \hat{H}^0(M'') \\ \uparrow & & \downarrow \\ \hat{H}^1(M) & \leftarrow & \hat{H}^1(M') \end{array} \qquad (*)$$

Dabei stehe $\hat{H}^q(N)$ für $\hat{H}^q(G,N)$. Nehmen wir zum Beispiel an, die Gruppen

$$\hat{H}^0(M'),\ \hat{H}^1(M'),\ \hat{H}^0(M),\ \hat{H}^1(M)$$

sind endlich. Bezeichne

$$M_i \ (i=1,2,3,4,5,6)$$

die Folge der Bilder der Abbildungen in obigen Diagramm, und zwar in der Reihenfolge wie sie die Richtung der Pfeile angibt. Zum Beispiel sei

$$M_1 := \mathrm{Im}(\hat{H}^0(M') \to \hat{H}^0(M))$$

$$M_2 := \mathrm{Im}(\hat{H}^0(M) \to \hat{H}^0(M''))$$

$$M_3 := \mathrm{Im}(\hat{H}^0(M'') \to \hat{H}^1(M'))$$

...

Dann ist die Sequenz

$$0 \to M_2 \to \hat{H}^0(M'') \to M_3 \to 0$$

exakt (wegen der Exaktheit von (*)). Weiter ist M_2 endlich als Bild einer endlichen Menge, und M_3 ist endlich als Teilmenge einer endlichen Menge. Die kurze exakte Sequenz liefert damit die Endlichkeit von $H^0(M'')$. Analog ergibt sich die Endlichkeit von $H^1(M'')$ aus der Exaktheit der Sequenz

$$0 \to M_5 \to \hat{H}^1(M'') \to M_6 \to 0.$$

Aus kurzen exakten Sequenzen, die analog zu den oben angebenen sind erhalten wir weiter die folgenden Identitäten.

$$\begin{aligned} h_0(M) &= \#M_1 \cdot \#M_2 \\ h_0(M'') &= \#M_2 \cdot \#M_3 \\ h_1(M') &= \#M_3 \cdot \#M_4 \\ h_1(M) &= \#M_4 \cdot \#M_5 \\ h_1(M'') &= \#M_5 \cdot \#M_6 \\ h_0(M') &= \#M_1 \cdot \#M_6 \end{aligned}$$

Damit ist aber

$$\begin{aligned} h(M) &= h_0(M)/h_1(M) \\ &= (\#M_1 \cdot \#M_2)/(\#M_4 \cdot \#M_5) \\ &= (\#M_1 \cdot \#M_6 \cdot \#M_2 \cdot \#M_3)/(\#M_3 \cdot \#M_4 \cdot \#M_5 \cdot \#M_6) \\ &= h_0(M') \cdot h_0(M'')/(h_1(M') \cdot h_1(M'')) \\ &h(M') \cdot h(M''). \end{aligned}$$

QED.

4.8.8 Herbrand-Index eines endlichen Moduls

Seien $G = \mathbb{Z}_n$ die zyklische Gruppe der Ordnung n und M ein endlicher G-Modul. Dann gilt

$$h(M) = 1.$$

Beweis. Wir betrachten die folgenden exakten Sequenzen.[121]

$$0 \to M^G \to M \xrightarrow{T} M \to M_G \to 0$$

$$0 \to \hat{H}^1(M) \to M_G \xrightarrow{N} M^G \to \hat{H}^0(M) \to 0$$

Die erste dieser Sequenzen zeigt, daß M^G und M_G dieselbe Ordnung haben. Die zweite der Sequenzen zeigt dann aber, daß $\hat{H}^1(M)$ und $\hat{H}^0(M)$ dieselbe Ordnung haben.
QED.

4.8.9 G-Homomorphismen mit endlichem Kern und Kokern

Seien $G = \mathbb{Z}_n$ die zyklische Gruppe der Ordnung n und

$$f: M \to N$$

ein Homomorphismus von G-Moduln mit endlichem Kern und Kokern. Dann ist von den beiden Zahlen h(M) und h(N) die eine genau dann definiert, wenn die andere es ist. Sind sie definiert, so sind sie gleich,

$$h(M) = h(N).$$

---

[121] Sei s der Erzeuger von G, durch welchem T definiert ist. Der Kern von T besteht dann aus den Elementen $m \in M$ mit

$$0 = (s-1)m = sm - m,$$

d.h. den Elementen die bei s fest bleiben. Da s die Gruppe G erzeugt, bleiben diese m aber bei allen Elementen der Gruppe G fest. Zur Exaktheit der ersten Sequenz an der Stelle M, siehe 4.8.2. Die zweite Sequenz ist exakt mit $\hat{H}^{-1}(M)$ anstelle von $\hat{H}^1(M)$. Die Exaktheit mit $\hat{H}^1(M)$ ergibt sich aus der Periodiziät.

Beweis. Nehmen wir zum Beispiel an, h(M) ist definiert. Aus den exakten Sequenzen

$$0 \to \mathrm{Ker}(f) \to M \to \mathrm{Im}(f) \to 0$$
$$0 \to \mathrm{Im}(f) \to N \to \mathrm{Koker}(f) \to 0$$

lesen wir dann nacheinander ab, daß die folgenden Zahlen definiert sind.

$$h(\mathrm{Im}(f)),\ h(N).$$

Außerdem ist nach 4.8.8 $h(\mathrm{Ker}(f)) = h(\mathrm{Koker}(f)) = 1$, also

$$h(N) = h(\mathrm{Im}(f)) = h(M).$$

QED.

4.8.10 $\mathbb{Z}_n$-invariante Gitter eines Vektorraums

Seien $G = \mathbb{Z}_n$ die zyklische Gruppe der Ordnung n, E ein $\mathbb{R}$-Vektorraum der Dimension

$$\dim_{\mathbb{R}} E < \infty,$$

und

$$G \to \mathrm{Aut}_{\mathbb{R}}(E)$$

ein Gruppenhomomorphismus. Weiter seien $L, L' \subseteq E$ zwei Gitter (d.h. endlich erzeugte $\mathbb{Z}$-Moduln), welche E erzeugen und welche unter der Operation von G auf E stabil sind.

Wenn dann eine der Zahlen h(L), h(L') definiert ist, so ist es auch die andere, und die beiden Zahlen sind gleich.

Wir beweisen zunächst das folgende Lemma.

Lemma

Seien G eine endliche Gruppe, M und M' zwei endlich erzeugte $\mathbb{Q}[G]$-Moduln derart, daß

$$M_{\mathbb{R}} := M \otimes_{\mathbb{Q}} \mathbb{R} \text{ und } M'_{\mathbb{R}} := M' \otimes_{\mathbb{Q}} \mathbb{R}$$

isomorph sind als $\mathbb{R}[G]$-Moduln. Dann sind M und M' isomorph als $\mathbb{Q}[G]$-Moduln.

Beweis des Lemmas. Seien L/K eine beliebige Körpererweiterung, A eine K-Algebra und V ein K-Vektorraum. Wir bezeichnen dann mit V_L den L-Vektorraum

$$V_L := V \otimes_K L .$$

Seien die A-Moduln M und M' endlich-dimensional als K-Vektorräume. Jede A-lineare Abbildung $\varphi: M \to M'$ induziert dann eine A_L-lineare Abbildung $\varphi \otimes 1: M_L \to M'_L$. Dies definiert einen Isomorphismus von L-Vektorräumen

(1) $$\mathrm{Hom}_A(M,M')_L \to \mathrm{Hom}_{A_L}(M_L, M'_L).$$

Das ist zunächst richtig für den Fall A = K: denn dann kann man den L-Vektorraum links mit

$$K^{d \times d'} \otimes_K L$$

identifizieren ($d := \dim_K M$, $d' := \dim_K M'$) und den L-Vektorraum rechts mit

$$(K \otimes_K L)^{d \times d'},$$

und die betrachtete Abbildung (1) sorgt gerade dafür, daß das Tensorprodukt mit direkten Summen kommutiert. Im Fall A beliebig betrachten wir eine Basis $\{a_i\}_{i \in I}$ des K-Vektorraums A und die K-lineare Abbildung

$$\varphi:\mathrm{Hom}_K(M, M') \to \mathrm{Hom}_K(M,M')^I,\ \alpha \mapsto (\mathrm{mult}(a_i)\circ\alpha - \alpha\circ \mathrm{mult}(a_i))_{i\in I}.$$

Der Kern dieser Abbildung ist gerade $\mathrm{Hom}_A(M,M')$, d.h. es besteht eine exakte Sequenz

$$0 \to \mathrm{Hom}_A(M,M') \to \mathrm{Hom}_A(M,M') \xrightarrow{\varphi} \mathrm{Hom}_A(M,M')^I.$$

Durch Tensorieren mit L über K erhalten wir eine exakte Sequenz

$$0 \to \mathrm{Hom}_A(M,M')_L \to \mathrm{Hom}_K(M,M')_L \xrightarrow{\varphi\otimes 1} \mathrm{Hom}_K(M,M')^I{}_L.$$

Wir wenden den Isomorphismus (1) im Fall A = K an und erhalten eine exakte Sequenz

$$0 \to \mathrm{Hom}_A(M,M')_L \to \mathrm{Hom}_L(M_L,M'_L) \xrightarrow{\psi} \mathrm{Hom}_L(M_L,M'_L)^I.$$

Dabei ist ψ gerade die Abbildung

$$\mathrm{Hom}_L(M_L,M'_L) \xrightarrow{\psi} \mathrm{Hom}_L(M_L,M'_L)^I,\ \alpha \mapsto (\mathrm{mult}(a_i)\circ\alpha - \alpha\circ \mathrm{mult}(a_i))_{i\in I},$$

d.h. der Kern von ψ ist gerade die Menge der L-linearen Abbildungen, die mit der Multiplikation mit Elementen aus A kommutieren,

$$\mathrm{Hom}_A(M,M')_L = \mathrm{Ker}(\psi) = \mathrm{Hom}_{A_L}(M_L,M'_L).$$

Betrachten wir jetzt den Fall K=$\mathbb{Q}$, L=$\mathbb{R}$, A = $\mathbb{Q}$[G]. Dann ist A_L = $\mathbb{R}$[G]. Aus den Voraussetzungen des Lemmas folgt insbesondere, daß M und M' dieselbe Dimension als $\mathbb{Q}$-Vektorräume haben. Indem wir in M und M' Basen fixieren, können wir von der Determinante eines Elements von

(2) $$\mathrm{Hom}_{\mathbb{Q}[G]}(M,M') \text{ bzw. } \mathrm{Hom}_{\mathbb{R}[G]}(M_{\mathbb{R}},M'_{\mathbb{R}})$$

sprechen. Aus der Isomorphie (1) ergibt sich, daß eine $\mathbb{Q}$-Basis ξ_i des ersten Moduls von (2) auch eine $\mathbb{R}$-Basis des zweiten Moduls von (2) ist. Da die Moduln $M_{\mathbb{R}}$ und $M'_{\mathbb{R}}$ isomorph sind über $\mathbb{R}$[G], existieren Elemente $a_i\in\mathbb{R}$ mit $\det(\sum a_i\xi_i)\neq 0$. Deshalb ist das folgende Polynom nicht identisch Null.

$$F(t) = \det(\sum t_i\xi_i) \in \mathbb{Q}[t_1,...,t_m].$$

Da der Körper der rationalen Zahlen unendlich ist, gibt es rationale Zahlen $b_i\in\mathbb{Q}$ mit

$$\det(\sum b_i\xi_i)\neq 0.$$

Dann ist aber $\sum b_i\xi_i$ ein $\mathbb{Q}$[G]-Isomorphismus M→M'.

QED.

Beweis von 4.8.10. Zum Beweis setzen wir M = L⊗$\mathbb{Q}$ und M'=L'⊗$\mathbb{Q}$. Dann sind $M_{\mathbb{R}}$ und $M'_{\mathbb{R}}$ beide $\mathbb{R}$[G]-isomorph zu E. Nach dem Lemma existiert ein $\mathbb{Q}$[G]-Isomorphismus

$$\varphi:L\otimes\mathbb{Q} \to L'\otimes\mathbb{Q}.$$

Dieser Isomorphismus definiert eine Einbettung von L in ein Gitter der Gestalt $\frac{1}{N}\cdot L'$ für eine geeignete natürliche Zahl N. Die Zusammensetzung von φ mit der Multiplikation mit N definiert deshalb eine Einbettung

$$f: L \to L'.$$

Da L und L' abelsche Gruppen desselben Rangs sind, ist der Kokern dieser Abbildung endlich. Die Behauptung folgt damit aus 4.8.9.
QED.

4.9 Kohomologische Trivialität

4.9.1 Definition

Ein G-Modul M heißt kohomologisch trivial, wenn

$$\hat{H}^q(H,M) = 0$$

gilt für jede Untergruppe $H \subseteq G$ und jede ganze Zahl $q \in \mathbb{Z}$.

Beispiel. Die induzierten Moduln

$$X \otimes \mathbb{Z}[G] \qquad (X \text{ abelsche Gruppe})$$

sind kohomologisch trivial. Ist nämlich $H \subseteq G$ eine Untergruppe, so ist $\mathbb{Z}[G]$ ein freier Modul über $\mathbb{Z}[H]$,

$$\mathbb{Z}[G] = \bigoplus_{g \in I} \mathbb{Z}[H]g\ .$$

Das Element g durchlaufe hier ein volles Repräsentantensystem I von G/H. Über $\mathbb{Z}[H]$ hat man deshalb eine Isomorphie

$$X \otimes \mathbb{Z}[G] = X \otimes \left(\bigoplus_{g \in I} \mathbb{Z}[H]g\right) = \left(\bigoplus_{g \in I} Xg\right) \otimes \mathbb{Z}[H],$$

d.h. $X \otimes \mathbb{Z}[G]$ ist auch induziert über H.

4.9.2 Null-Moduln über p-Gruppen

Seien p eine Primzahl, G eine p-Gruppe und M ein G-Modul mit $p \cdot M = 0$. Dann sind folgende Bedingungen äquivalent.

(i) $M = 0$.
(ii) $H^0(G,M) = 0$.
(iii) $H_0(G,M) = 0$.

Beweis. Offensichtlich gilt (i) $\Rightarrow$ (ii) und (i) $\Rightarrow$ (iii).
(ii) $\Rightarrow$ (i). Angenommen, es gilt $M \neq 0$. Wir wählen ein von Null verschiedenes $x \in M$. Der von x erzeugte Teilmodul

$$N := x \cdot \mathbb{Z}[G] = x \cdot \mathbb{F}_p[G]$$

ist endlich und hat als Ordnung eine p-Potenz (nämlich einen Teiler von $\#\mathbb{F}_p[G] = p \cdot \#G$, - man beachte, wegen $p \cdot M = 0$ ist M ein $\mathbb{F}_p$-Modul). Betrachten wir die G-Orbits der Elemente aus N. Ihre Ordnungen sind sämtlich Potenzen von p (Teiler von #G). Außerdem gibt es in B ein Element, dessen G-Orbit die Ordnung 1 hat, nämlich das Nullelement. Dann gibt es aber mindestens p Elemente in B, die bei G stabil bleiben. Mit anderen Worten,

$$H^0(G,M) = M^G$$

enthält mindestens p Elemente, ist also $\neq 0$. Dieser Widerspruch beweist die Implikation.
(iii) $\Rightarrow$ (i). Sei

$$M' := \mathrm{Hom}(M,\mathbb{F}_p)$$

der zu M duale Modul (als $\mathbb{F}_p$-Vektorraum). Dann ist die Gruppe

$$H^0(G,M') = (M')^G = \mathrm{Hom}_G(M,\mathbb{F}_p) = \mathrm{Hom}(M_G,\mathbb{F}_p)$$

dual zu $H_0(G,M) = M_G := M/I_GM$. Mit $H_0(G,M) = 0$ gilt also auch $H^0(G,M') = 0$. Dann ist aber, wie wir bereits gezeigt haben, $M = 0$.
QED.

4.9.3 Kriterium für freie Moduln über p-Gruppen

Seien p eine Primzahl, G eine p-Gruppe und M ein G-Modul mit $p\cdot M = 0$. Außerdem gelte

$$H_1(G,M) = 0.$$

Dann ist M ein freier Modul über dem Ring $\mathbb{F}_p[G] = \mathbb{Z}[G]/p\mathbb{Z}[G]$.

Beweis. Es gilt $p\cdot M = 0$, also auch $p\cdot H_0(G,M) = 0$,[122] d.h. $H_0(G,M)$ läßt sich als Vektorraum über $\mathbb{F}_p$ auffassen. Fixieren wir eine Basis $\{h_\lambda\}$ dieses Vektorraums und wählen Repräsentanten $m_\lambda \in M$ der Basisvektoren. Sei

$$M'$$

der von den m_λ erzeugte G-Teilmodul von M und sei $M'':=M/M'$ der zugehörige Faktormodul. Dann besteht folgende exakte Sequenz.

$$H_0(G,M') \xrightarrow{\alpha} H_0(G,M) \to H_0(G,M'') \to 0.$$

Aus der Konstruktion des Moduls M' ergibt sich, daß α ein Isomorphismus ist. Folglich gilt $H_0(G,M'') = 0$, also $M'' = 0$ (nach 4.9.2). Das bedeutet aber, die m_λ erzeugen den G- Modul M und definieren damit einen Epimorphismus

$$\varphi: L \to M,$$

mit einem freien $\mathbb{F}_p[G]$ -Modul L. Nach Konstruktion induziert φ einen Isomorphismus

$$\beta: H_0(G,L) \to H_0(G,M).$$

Sei $R:= \mathrm{Ker}(\varphi)$. Wegen $H_1(G,M) = 0$ erhalten wir eine exakte Sequenz

$$0 \to H_0(G,R) \to H_0(G,L) \xrightarrow{\beta} H_0(G,M) \to 0.$$

Da β ein Isomorphismus ist, gilt $H_0(G,R) = 0$, also $R=0$ (nach 4.9.2). Also ist φ ein Isomorphismus und damit M ein freier $\mathbb{F}_p[G]$ -Modul.
QED.

4.9.4 Kohomologisch triviale Moduln über p-Gruppen

Seien p eine Primzahl, G ein p-Gruppe umd M ein G-Modul mit $p\cdot M = 0$. Dann sind folgende Bedingungen äquivalent.

(i) M ist ein freier $\mathbb{F}_p[G]$-Modul.
(ii) M ist ein induzierter Modul.
(iii) M ist kohomologisch trivial.

---

[122] denn $H_0(G,M) = M/I_GM$ ist ein Faktormodul von M.

(iv) $\hat{H}^q(G,M) = 0$ für irgendeine ganze Zahl q.

Beweis. Trivialerweise gilt (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv). Beweisen wir (iv) $\Rightarrow$ (i). Mit Hilfe einer Dimensionsverschiebung konstruieren wir einen G-Modul N mit

$$\hat{H}^r(G,N) = \hat{H}^{r+q+2}(G,M)$$

für alle $r \in \mathbb{Z}$. Dann gilt insbesondere $H_1(G,N) = \hat{H}^{-2}(G,N) = \hat{H}^q(G,M) = 0$, d.h, N ist frei über $\mathbb{F}_p[G]$ (nach 4.9.3). Dann ist aber

$$H_1(G,M) = \hat{H}^{-2}(G,M) = \hat{H}^{-q-4}(G,N) = 0.$$

Nach 4.9.3 ist M ein freier $\mathbb{F}_p[G]$-Modul.

QED.

4.9.5 Torsionsfreie Moduln über p-Gruppen

Seien p eine Primzahl, G eine p-Gruppe und M ein G-Modul ohne p-Torsion. Dann sind folgende Bedingungen äquivalent.

(i) M ist kohomologisch trivial.

(ii) $\hat{H}^q(G,M) = \hat{H}^{q+1}(G,M) = 0$ für eine ganze Zahl q.

(iii) M/pM ist ein freier $\mathbb{F}_p[G]$-Modul.

Beweis. (i) $\Rightarrow$ (ii). Trivial.

(ii) $\Rightarrow$ (iii). Da M keine p-Torsion besitzt, definiert die Multiplikation mit p eine kurze exakte Sequenz

(*) $$0 \to M \to M \to M/pM \to 0.$$

Die lange Kohomologiesequenz liefert die Exaktheit von

$$\hat{H}^q(G,M) \to \hat{H}^q(G,M/pM) \to \hat{H}^{q+1}(G,M).$$

Nach Voraussetzung (ii) folgt $\hat{H}^q(G,M/pM) = 0$. Nach 4.9.4 ist dann aber M/pM ein freier $\mathbb{F}_p[G]$-Modul.

(iii) $\Rightarrow$ (i). Sei also M/pM ein freier $\mathbb{F}_p[G]$-Modul (also auch ein freier $\mathbb{F}_p[H]$-Modul für jede Untergruppe H von G). Nach 4.9.3 gilt dann $\hat{H}^q(H,M/pM) = 0$. Aus der kurzen exakten Sequenz (*) ergibt sich damit, daß die Multiplikation mit p eine bijektive Abbildung

$$\hat{H}^q(H,M) \to \hat{H}^q(H,M)$$

definiert (für jedes q und jede Untergruppe H von G). Wir wissen aber bereits (4.6 Folgerung 1 zu Proposition 6.3), $\hat{H}^q(H,M)$ wird von der Gruppenordnung von H annulliert (d.h. von einer p-Potenz). Dann muß aber $\hat{H}^q(H,M) = 0$ gelten.

QED.

4.9.6 $\mathbb{Z}$-freie Moduln über p-Gruppen

Seien G eine p-Gruppe, M ein $\mathbb{Z}$-freier G-Modul und N ein G-Modul ohne p-Torsion. Genügt M einer der äquivalenten Bedingungen von 4.9.5, so ist der G-Modul

$$H := \mathrm{Hom}(M,N)$$

kohomologisch trivial.

Beweis. Da N keine p-Torsion besitzt, liefert die Multiplikation mit p eine exakte Sequenz

$$0 \to N \xrightarrow{p} N \to N/pN \to 0.$$

Da M nach Voraussetzung $\mathbb{Z}$-frei ist, d.h Hom(M,?) ist exakt, haben wir eine exakte Sequenz

$$0 \to \mathrm{Hom}(M,N) \xrightarrow{p} \mathrm{Hom}(M,N) \to \mathrm{Hom}(M,N/pN) \to 0.$$

Insbesondere besitzt H := Hom(M,N) also keine p-Torsion, und es gilt[123]

$$H/pH \cong \mathrm{Hom}(M/pM,\ N/pN).$$

Nun ist M/pM ein freier $\mathbb{F}_p[G]$-Modul[124], also direkte Summe von Untergruppen der Gestalt M'·g (g∈G) mit einer Untergruppe M' von M/pM. Dann ist aber H/pH direkte Summe der Untergruppen Hom(M', N/pN)·g, d.h . H/pH ist ein induzierter G-Modul. Nach 4.9.4 ist H/pH ein $\mathbb{F}_p[G]$-freier Modul und nach 4.9.5 ist H kohomologisch trivial.

QED.

4.9.7 Definition: projektive Moduln

Ein G-Modul P heißt projektiv, wenn der Funktor Hom(P,?) exakt ist. Das ist äquivalent zu der Forderung, daß P direkter Summand eines freien Moduls ist. Projektive Moduln sind kohomologisch trivial.

4.9.8 $\mathbb{Z}$-freie G-Moduln über beliebigen endlichen Gruppen

Seien G eine endliche Gruppe, M ein $\mathbb{Z}$-freier G-Modul und G_p eine p-Sylow-Untergruppe von G. Dann sind folgende Aussagen äquivalent.

(i) Für jede Primzahl p genügt der G_p-Modul M einer der äquivalenten Bedingungen von 4.9.5.

(ii) M ist ein projektiver Modul.

Beweis. (ii) ⇒ (i). Nach Voraussetzung ist M ein direkter Summand eines freien $\mathbb{Z}[G]$-Moduls F. Der Modul F ist auch als $\mathbb{Z}[G_p]$-Modul frei (für jedes p). Dann ist aber M/pM direkter Summand des freien $\mathbb{F}_p[G]$-Moduls F/pF. Nach 4.9.5 ist F kohomologisch trivial über G_p (für jedes p). Da die Tate-Kohomologie mit direkten Summen kommutiert, ist damit auch M kohomologisch trivial über G_p (für jedes p).

(i) ⇒ (ii). Seien F ein freier $\mathbb{Z}[G]$-Modul, der sich surjektiv auf M abbilden läßt und

$$0 \to Q \to F \to M \to 0$$

eine entsprechende exakte Sequenz von G-Moduln. Da M als $\mathbb{Z}$-Modul frei ist, erhält man durch Anwenden von Hom(M,?) eine exakte Sequenz

(*) $$0 \to \mathrm{Hom}(M,Q) \to \mathrm{Hom}(M,F) \to \mathrm{Hom}(M,M) \to 0.$$

---

[123] Jede $\mathbb{Z}$-lineare Abbildung M → N/pN faktorisiert sich auf genau eine Weise über M/pM, d.h. es ist Hom(M, N/pN) = Hom(M/pM, N/pN).

[124] Nach Voraussetzung ist Bedingung 4.9.5 (iii) erfüllt.

Da Q torsionsfrei ist, ist nach 4.9.6 der Modul Hom(M,Q) kohomologisch trivial über jeder p-Sylow-Untergruppe G_p.Nach 4.6.17 ist dann aber Hom(M,Q) auch über G selbst kohomologisch trivial. Insbesondere ist

$$H^1(G,\mathrm{Hom}(M,Q)) = 0.$$

Wir wenden auf die Sequenz (*) den Funktor

$$H^0(G,?) = (?)^G$$

an und erhalten die exakte Sequenz

$$0\to \mathrm{Hom}_G(M,Q)\to \mathrm{Hom}_G(M,F)\to \mathrm{Hom}_G(M,M)\to H^1(G,\mathrm{Hom}(M,Q)) \ (=0).$$

Insbesonder ist die natürliche Abbildung

$$\mathrm{Hom}_G(M,F)\to \mathrm{Hom}_G(M,M)$$

surjektiv, d.h. die identische Abbildung von M faktoriesiert sich über F, d.h. die Projektion F→M besitzt einen Schnitt, d.h. M ist direkter Summand von F. Mit anderen Worten, M ist projektiv.
QED.

4.9.9 Beliebige G-Moduln über endlichen Gruppen

Seien G eine endliche Gruppe und M ein beliebiger G-Modul. Dann sind folgende Aussagen äquivalent.

(i) Für jede Primzahl p gibt es eine ganze Zahl $q\in\mathbb{Z}$ mit

$$\hat{H}^q(G_p,M) = \hat{H}^{q+1}(G_p,M) = 0.$$

(ii) M ist kohomologisch trivial.

(iii) Es gibt eine exakte Sequenz der Gestalt

$$0\to P'\to P\to M\to 0$$

mit projektiven G-Moduln P und P'.

Beweis. (ii) ⇒ (i). Trivial.

(iii) ⇒ (ii). Folgt aus der kohomologischen Trivialität der projektiven G-Moduln.

(i) ⇒ (iii). Wir wählen einen freien $\mathbb{Z}[G]$-Modul P, der sich surjektiv auf M abbilden läßt und betrachten die zugehörige exakte Sequenz

$$0\to P'\to P\to M\to 0.$$

Es genügt zu zeigen, der G-Modul P' ist projektiv. Da P kohomologisch trivial ist, gilt

$$\hat{H}^q(G_p,P') \cong \hat{H}^{q-1}(G_p,M)$$

für jedes p und q. Dann gilt aber $\hat{H}^q(G_p,P')=0$ für jedes p und je zwei aufeinanderfolgende q. Nach 4.9.8 ist P' projektiv (man beachte, P' ist als Teilmodul des $\mathbb{Z}$-freien Moduls P selbst $\mathbb{Z}$-frei).
QED.

4.10 Der Satz von Tate

4.10.1 Kriterium für Quasi-Isomorphie

Seien G eine endliche Gruppe und f: M→N ein Homomophismus von G-Moduln. Für jede Primzahl bezeichne G_p eine p-Sylow-Untergruppe von G. Für jede Primzahl existiere eine ganze Zahl $n_p\in\mathbb{Z}$ derart, daß die von f induzierte Abbildung

$$f_q^*:\hat{H}^q(G_p,M)\to\hat{H}^q(G_p,N)$$

surjektiv für $q=n_p$, bijektiv für $q=n_p+1$ und injektiv für $q=n_p+2$ ist. Dann ist die Abbildung

$$f_q^*:\hat{H}^q(G_p,M)\to\hat{H}^q(G_p,N)$$

für jedes q und für jede Untergruppe $H\subseteq G$ ein Isomorphismus.

Beweis. Sei $M^* := \mathrm{Hom}(\mathbb{Z}[G],M)$ und bezeichne i die natürliche Abbildung

$$i: M \to M^*,\ m \mapsto i_m := (\lambda \mapsto \lambda\cdot m).$$

Diese Abbildung ist injektiv, also ist es auch die Abbildung

$$(f,i): M \to N\oplus M^*,\ m \mapsto (f(m), i_m).$$

Wir erhalten deshalb eine exakte Sequenz

$$(*)\qquad 0\to M\to N\oplus M^*\to D\to 0.$$

Da der Modul M^* koinduziert, also kohomogisch trivial ist. haben N und $N\oplus M^*$ dieselbe Kohomologie. Die lange Kohomologiesequenz zu (*) über der Untergruppe G_p hat also die Gestalt

$$\ldots\to \hat{H}^q(G_p,M)\to\hat{H}^q(G_p,N)\to\hat{H}^q(G_p,D)\to\ldots$$

Auf Grund unserer Voraussetzungen folgt

$$\hat{H}^q(G_p,D) = 0$$

für $q=n_p$ und $q=n_p+1$, d.h. nach 4.9.9 ist D kohomologisch trivial. Die Behauptung ergibt sich damit aus der langen Kohomologiesequenz zu (*) über der Untergruppe H. **QED**.

4.10.2 Isomorphie der Cup-Multiplikation mit einem Element

Seien G eine endliche Gruppe, M, N, P drei G-Moduln und $\varphi: M\otimes N\to P$ ein G-Homomorphismus. Weiter seien $q\in\mathbb{Z}$ und

$$a\in\hat{H}^q(G,M)$$

fest gewählte Elmente. Für jede Primzahl p existiere ein ganze Zahl n_p derart, daß die Cup-Multiplikation

$$\hat{H}^q(G_p,N)\to\hat{H}^{n+q}(G_p,P),\ x \mapsto \varphi^*_{n+q}(\mathbf{Res}_{G/G_p}(a)\cup x)$$

surjektiv für $q=n_p$, bijektiv für $q=n_p+1$ und injektiv für $q=n_p+2$ ist. Dann ist

$$\hat{H}^q(H,N)\to\hat{H}^{n+q}(H,P),\ x \mapsto j^*_{n+q}(\mathbf{Res}_{G/H}(a)\cup x)$$

für jedes q und jede Untergruppe H von G ein Isomorphismus.

Beweis. 1. Schritt. Der Fall q=0. Wir führen den Beweis in diesem Fall auf die Aussage von 4.10.1 zurück. Nach Voraussetzung gibt es ein Element

$$a\in\hat{H}^0(G,M) = M^G/\mathrm{Im}(N^*)$$

derart, daß die Cup-Multiplikation mit a wie oben Isomorphismen definiert. Sei

$$\alpha\in M^G$$

ein Repräsentant von a. Man beachte, dann ist α auch Repräsentant der Kohomologieklasse $\mathbf{Res}_{G/H}(a) \in \hat{H}^0(H,M)$ (für jede Untergruppen $H \subseteq G$). Betrachten wir die Abbildung

$$f: N \to P,\ m \mapsto \varphi(\alpha \otimes n).$$

Da α invariant ist, ist f ein Homorphismus von G-Moduln. Es reicht zu zeigen,

$$(1) \qquad \varphi^*(\mathbf{Res}_{G/H}(a) \cup x) = f^*(x) \text{ für jedes } x \in \hat{H}^n(H,N),$$

denn dann genügt die Abbildung f den Bedingungen von 4.10.1, und die Aussage von 4.10.1 fällt mit unserer Behauptung im Fall q=0 zusammen.
Für n=0 ist dies gerade die Aussage, daß das Cup-Produkt durch das Tensorprodukt induziert wird.
Sei jetzt n beliebig. Wir haben den Beweis der Identität (1) mit Hilfe von Dimensionsverschiebungen auf den Fall n=0 zurückführen. Um zum Beispiel den Schluß von n+1 auf n machen zu können, betrachten wir des kommutative Diagramm

$$(2) \qquad \begin{array}{ccccccc} 0 & \to & M' & \to & M_* & \to & M \to 0 \\ & & f'\downarrow & & \downarrow 1\otimes f & & \downarrow f \\ 0 & \to & P' & \to & P_* & \to & P \to 0 \end{array}$$

mit $N_* := \mathbb{Z}[G] \otimes N$, $P_* := \mathbb{Z}[G] \otimes P$ und N', P' derart, daß die Zeilen exakt sind. Die Moduln N_* und P_* sind induziert, also kohomologisch trivial. Die Zusammenhangshomomorphismen der Kohomologiesequenzen zu den Zeilen sind deshalb Isomorphismen, die sich in ein kommutatives Diagramm

$$\begin{array}{ccc} \hat{H}^n(H,N) & \xrightarrow{\delta} & \hat{H}^{n+1}(H,N') \\ f^*\downarrow & & \downarrow f'^* \\ \hat{H}^n(H,P) & \xrightarrow{\delta} & \hat{H}^{n+1}(H,P') \end{array}$$

einfügen. Außerdem zerfallen die Zeilen von (2) als Sequenzen von $\mathbb{Z}$-Moduln. Sie bleiben also exakt, wenn man sie mit M (über $\mathbb{Z}$) tensoriert.
Der G-Homomorphismus $\varphi: M \otimes N \to P$ induziert, wenn man mit $\mathbb{Z}[G]$ tensoriert und zu entsprechenden Teilmoduln übergeht einen G-Homomorphismus

$$\varphi': M \otimes N' \to P'.$$

Aus der induktiven Definition des Cup-Produkts ergibt sich dann

$$\begin{aligned} \delta \circ f^*(x) &= f'^* \circ \delta(x) && \text{(Funktorialität von } \delta) \\ &= \varphi'^*(\mathbf{Res}_{G/H}(a) \cup \delta x) && \text{(Induktion bezüglich n)} \\ &= \varphi'^* \circ \delta(\mathbf{Res}_{G/H}(a) \cup x) && \text{(Definition von } \cup) \\ &= \delta \circ f^*(\mathbf{Res}_{G/H}(a) \cup x) && \text{(Funktorialität von } \delta) \end{aligned}$$

Da δ ein Isomorphismus ist, folgt Formel für n+1.

2. Schritt. Beweis der Behauptung für $a \in \hat{H}^q(G,M)$ mit q beliebig.
Der allgemeine Fall ergibt sich aus dem Fall q=0 durch Dimensionsverschiebung. Um den Schluß von q+1 auf q zu machen, betrachten wir die exakte Sequenz von G-Moduln

$$0 \to M' \to M_* \to M \to 0$$

mit $M_* := \mathbb{Z}[G] \otimes M$. Sie liefert Isomorphismen $\delta: \hat{H}^q(H,M) \to \hat{H}^{q+1}(H,M')$. Mit

b := $\mathbf{Res}_{G/H}(a) \in \hat{H}^q(H,M)$

gilt

b' := $\delta(u) = \mathbf{Res}_{G/H}(\delta(a))$ (da Res funktoriell ist).

Weiter induziere $\varphi: M \otimes N \to P$ den G-Homomorphismus $\varphi'': M' \otimes N \to P''$. Zeigen wir, das folgende Diagramm ist kommutativ.

$$\begin{array}{ccccc} \hat{H}^n(H,N) & \xrightarrow{u} & \hat{H}^{n+q}(H,M\otimes N) & \xrightarrow{\varphi^*} & \hat{H}^{n+q}(H,P) \\ \| & & & & \downarrow\delta \\ \hat{H}^n(H,N) & \xrightarrow{u'} & \hat{H}^{n+q+1}(H,M'\otimes N) & \xrightarrow{\varphi'^*} & \hat{H}^{n+q+1}(H,P') \end{array}$$

Es gilt

$\delta \circ \varphi^*(u \cup x) = \varphi'^* \circ \delta(u \cup x)$ (Funktorialität von δ)

$= \varphi'^*(\delta(u) \cup x))$ (Definition von $\cup$)

$= \varphi'^*(u' \cup x))$.

Nach Induktionsvoraussetzung ist die untere Zeile ein Isomorphismus. Also gilt dasselbe für die obere Zeile (weil δ ein Isomorphismus ist).

QED.

4.10.3 Satz von Tate

Seien G eine endliche Gruppe, M ein G-Modul und $a \in H^2(G,M)$ ein Element. Für jede Primzahl p bezeichne G_p eine p-Sylow-Untergruppe von G mit

1. $H^1(G_p,M) = 0$
2. $H^2(G_p,M) = \mathbb{Z} \cdot \mathbf{Res}_{G/G_p}(a)$ ist zyklisch von der Ordnung $|G_p|$ und wird von $\mathbf{Res}_{G/G_p}(a)$ erzeugt.

Dann ist die Cup-Multiplikation

$$\hat{H}^n(H,\mathbb{Z}) \to \hat{H}^{n+2}(H,M),\ x \mapsto \mathbf{Res}_{G/H}(a) \cup x$$

mit für jede Untergruppe $H \subseteq G$ und für jede ganz Zahl $n \in \mathbb{Z}$ ein Isomorphimus.

Beweis. Wir setzen in 4.10.2 N:= $\mathbb{Z}$, P:=M, q=2, n_p:=-1. Wir haben zu zeigen,

$$\hat{H}^n(G_p,\mathbb{Z}) \to \hat{H}^{n+2}(G_p,M)$$

ist surjektiv für n=-1, bijektiv für n=0 und injektiv für n=1. Die Surjektivität im Fall n=-1 folgt aus Voraussetzung 1. Die Injektivität im Fall n=1 folgt aus

$\hat{H}^1(G_p,\mathbb{Z}) = H^1(G_p,\mathbb{Z})$

$= \mathrm{Hom}(G_p,\mathbb{Z})$ (weil G trivial auf $\mathbb{Z}$ operiert, vgl. 4.2)

$= 0.$ (weil $\mathbb{Z}$ keine p-Torsion hat)

Für n=0 beachten wir, $\hat{H}^0(G_p,\mathbb{Z}) = \mathbb{Z}/|G_p| \cdot \mathbb{Z}$ (nach 4.8.4 Kohomologie der zyklischen Gruppen). Die Bijektivität im Fall n=0 ergibt sich damit aus Voraussetzung 2.

QED.

5 Proendliche Gruppen (K. Grünberg)

5.1 Gruppen

5.1.1 Einführung

Eine proendliche Gruppe ist ein projektiver Limes von endlichen Gruppen. Proendliche Gruppen treten in in natürlicher Weise bei der Untersuchung von unendlichen Galois-Erweiterungen auf.

Wir beginnen mit der Klärung einiger Einzelheiten dieser Definition (Alle grundlegenden Fakten, welche sich auf projektive Limites, und ebenso auf induktive, beziehen, findet man in [5], Kapitel VIII).

Vereinbarungen

(i) Alle hier betrachteten topologischen Gruppen seien Hausdorff-Räume. Unter einem Morphismus von topologischen Gruppen werden wir einen stetigen Homomorphismus verstehen.

(ii) Insbesondere werden allen endlichen Gruppen werden als topologische Gruppen aufgefaßt, wobei nach (i) ihre Topologie die diskrete Topologie sein muß.

5.1.2 Projektive Systeme

5.1.2.1 Begriff des projektiven Systems

Eine gerichtete Menge ist eine Menge I zusammen mit einer Relation $\leq$ auf I, welche reflexiv und transitiv ist und außerdem die Eigenschaft hat, daß es zu je zwei $i,j \in I$ ein $k \in I$ gibt mit $i \leq k$ und $j \leq k$. Ein projektives System von topologischen Gruppen über I ist eine Familie

$$\{\pi_i^j : G_j \to G_i\}_{i,j \in I, i \leq j}$$

von stetigen Homomorphismen topologischer Gruppen derart, daß für je drei Elemente $i,j,k \in I$ mit $i \leq j \leq k$ gilt $\pi_i^k = \pi_i^j \circ \pi_j^k$. Mit anderen Worten, ein projektives System von topologischen Gruppen ist kontravarianter Funktor

$$\pi : I^0 \to (\text{topological groups})$$

auf I mit Werten in der Kategorie der topologischen Gruppen und stetigen Homomorphismen. Hier haben wir I mit der durch I definierten Kategorie identifieziert.

5.1.2.2 Morphismen von projektiven Systemen

Seien zwei projektive Systeme

$$\pi : I^0 \to (\text{topological groups})$$

$$\pi' : J^0 \to (\text{topological groups})$$

von topologischen Gruppen gegeben und eine ordnungserhaltende Abbildung

$$\phi : J \to I.$$

Ein ϕ-Morphismus $\varphi : \pi \to \pi'$ ist eine natürliche Transformation

$$\varphi : \pi \circ \phi \to \pi'.$$

Wir identifizieren hier ϕ mit dem von ϕ induzierten Funktor $J \to I$. Mit anderen Worten, ein ϕ-Morphismus $\varphi : \pi \to \pi'$ ist eine Familie von stetigen Homomorphimen

$$\{\varphi(j):\pi(\phi(j))\to\pi'(j)\}_{j\in J}$$

mit der Eigenschaft, daß für je zwei Elemente $j,j'\in J$ mit $j\leq j'$ das folgende Diagramm kommutativ ist.

$$\begin{array}{ccc} \pi(\phi(j)) & \to & \pi'(j) \\ {\scriptstyle \pi^{\phi j'}_{\phi j}}\uparrow & & \uparrow{\scriptstyle \pi^{j'}_{j}} \\ \pi(\phi(j')) & \to & \pi'(j') \end{array}$$

5.1.3 Projetive Limites

5.1.3.1 Konstruktion des projektiven Limes

Sei ein projektives System

$$\{\pi^j_i: G_j\to G_i\}_{i,j\in I, i\leq j}$$

von endlichen Gruppen gegeben. Wir setzen

$$G := \prod_{i\in I} G_i$$

und versehen G mit der Produkt-Topologie, d.h. mit der stärksten Topologie, bei der alle Projektionen

$$\pi_i: G\to G_i,\ (g_\alpha)_{\alpha\in J}\mapsto g_i$$

stetig sind. Mit anderen Worten, eine Teilmenge $U\subseteq G$ ist offen, wenn es zu jedem Element $g\in G$ einen endlichen Durchschnitt

$$D = \mathrm{Ker}(\pi_{i_1})\cap\ldots\cap\mathrm{Ker}(\pi_{i_r})$$

mit $g\cdot D\subseteq U$ gibt. Betrachten wir die Teilmenge

$$L := \{(g_\alpha)_{\alpha\in I}\in G \mid \text{für je zwei } i,j\in I \text{ mit } i\leq j \text{ gilt } \pi^j_i(g_j) = g_i\}$$

von G und versehen sie mit der Unterraumtopologie. Dies ist eine topologische Gruppe und heißt projektiver Limes (oder auch inverser Limes) des gegebenen projektiven Systems.

Bezeichnung

$$L := \varprojlim_{i\in I} G_i$$

Eine proendliche Gruppe ist eine Gruppe der oben beschriebenen Gestalt L.

5.1.3.2 Funktorialität des projektiven Limes

Seien zwei projektive Systeme

$$\pi: I^0\to(\text{topological groups}),\qquad i\mapsto G_i$$

$$\pi': J^0\to(\text{topological groups}),\qquad j\mapsto G'_j$$

eine ordnungserhaltende Abbildung $\phi: J\to I$ und ein ϕ-Morphismus $\varphi:\pi\circ\phi\to\pi'$ gegeben. Der Morphismus definiert einen stetigen Homomorphismus

$$\psi: G:=\prod_{i\in I} G_i\to G:=\prod_{j\in J} G'_j,\ (g_\alpha)_{\alpha\in I}\mapsto(\varphi g_{\phi\beta})_{\beta\in J}$$

Dies ist offensichtlich ein Gruppenhomomorphismus. Außerdem ist er stetig. Zum Beweis des letzteren genügt es zu zeigen, $\psi^{-1}(\mathrm{Ker}(\pi'_j))$ ist offen für jedes j, wobei

$$\pi'_j: G'\to G'_j$$

die Projektion auf den j-ten Faktor bezeichne. Nach Konstruktion von ψ gilt

$$\pi'_j \circ \psi = \varphi \circ \pi_{\phi j}$$

also

$$\psi^{-1}(\mathrm{Ker}(\pi'_j)) = \mathrm{Ker}(\pi'_j \circ \psi) = \mathrm{Ker}(\varphi \circ \pi_{\phi j}) = \pi_{\phi j}^{-1}(\varphi^{-1}(0)).$$

Die Menge rechts ist eine Vereinigung von Mengen der Gestalt $\mathrm{Ker}(\pi_{\phi j}) \cdot g$ mit $g \in G$, also eine offene Menge. Die Einschränkung auf den projektiven Limes L induziert einen stetigen Homomorphismus

$$\varprojlim_{i \in I} G_i \rightarrow \varprojlim_{j \in J} G'_j$$

(wegen der Kommutativität der Vierecke von 5.2.2).

5.1.4 Topologische Charakterisierung der proendlichen Gruppen

5.1.4.1 Vollständig unzusammenhängende Mengen

Ein topologischer Raum X heißt zusammenhängend, wenn er nicht in die Vereinigung von zwei disjunkten nicht-leeren offenen Teilmengen zerlegt werden kann. Sei $x \in X$ ein Punkt. Die Vereinigung aller zusammenhängenden Teilmengen von X, welche x enthalten, ist selbst zusammenhängend und heißt Zusammenhangskomponente von x in X. Ein topologischer Raum heißt vollständing unzusammenhängend oder auch total unzusammenhängend, wenn die Zusammenhangs-Komponente jedes Punktes nur aus dem Punkt selbst besteht.

Bemerkungen

1. Jede Menge ist mit der diskreten Topologie vollständig unzusammenhängend.
2. Die Menge der rationalen Zahlen ist mit der gewöhnlichen Topologie vollständig unzusammenhängend (weil zwischen je zwei rationalen Zahlen ein irrationale Zahl liegt). Ihre Topologie ist jedoch nicht diskret.
3. Die Vereinigung einer Familie von zusammenhängenden Mengen, von denen je zwei einen gemeinsamen Punkt haben, ist zusammenhängend. Insbesondere ist somit die obige Definition der Zusmmenhangskomponente korrekt.

Beweis von 3. Seien X ein topologischer Raum und $Y \subseteq X$ eine Vereinigung von zusammenhängenden Teilmengen der beschriebenen Art. Wir haben zu zeigen, Y ist zusammenhängend. Angenommen, es gibt eine disjunkte Zerlegung

(*) $$Y = (Y \cap U_1) \cup (Y \cap U_2)$$

in nicht-leere Teilmengen mit offenen Teilmengen $U_1, U_2 \subseteq X$. Wir wählen Punkte

$$x_i \in Y \cap U_i$$

(i=1,2). Nach Voraussetzung gibt es zusammenhängende Teilmengen $Z_i \subseteq X$ mit

$$x_i \in Z_i \subseteq Y \text{ für } i = 1,2 \text{ und } Z_1 \cap Z_2 \neq \emptyset.$$

Wegen (*) hat man disjunkte Zerlegungen

$$Z_i = (Z_i \cap U_1) \cup (Z_i \cap U_2).$$

Da Z_i zusammenhängend ist, ist eine der Mengen $Z_i \cap U_1$, $Z_i \cap U_2$ leer. Nun liegt x_i in der Menge $Z_i \cap U_i$, d.h. es gilt $Z_i = Z_i \cap U_i$ also

$$Z_i \subseteq Y \cap U_i.$$

Die Zerlegung (*) ist nach Voraussetzung disjunkt. Dann müssen aber die Z_i disjunkt sein, im Widerspruch zu ihrer Wahl.

QED.

5.1.4.2 Abgeschlossenheit der Zusammenhangskomponenten

Sei X ein topologischer Raum.

(i) Die Abschließung einer zusammenhängenden Teilmenge von X ist zusammenhängend.

(ii) Die Zusammenhangskomponenten eines topologischen Raums sind abgeschlossen.

Beweis. Die zweite Aussage folgt aus der ersten. Es genügt also, (i) zu beweisen. Sei $A \subseteq X$ eine zusammenhängende Teilmenge. Angenommen, ihr Abschluß $\bar{A}$ ist nicht zusammenhängend. Dann gibt es offene Teilmengen $U_1, U_2 \subseteq X$ mit

$$\bar{A} = (U_1 \cap \bar{A}) \cup (U_2 \cap \bar{A}),\ U_1 \cap \bar{A} \neq \emptyset,\ U_1 \cap U_2 \cap \bar{A} = \emptyset.$$

Aus der Identität ganz links folgt

$$A = (U_1 \cap A) \cup (U_2 \cap A)$$

und, da A zusammenhängend ist, $U_i \cap A = \emptyset$ für ein i. Da U_i offen ist, gilt dann aber auch $U_i \cap \bar{A} = \emptyset$ im Widerspruch zur Wahl der Mengen U_1, U_2.

QED.

5.1.4.3 Normalität der kompakten Hausdorff-Räume

Ein topologischer Raum X heißt normal, wenn es zu je zwei disjunkte abgeschlossenen Teilräumen

$$A_1, A_2 \subseteq X$$

disjunkte offene Teilmengen $U_1, U_2 \subseteq X$ gibt mit $A_i \subseteq U_i$ für $i = 1,2$.

Jeder kompakte Hausdorff-Raum X ist normal.

Beweis. Seien $A_1, A_2 \subseteq X$ disjunkt und abgeschlossen. Da X kompakt ist, gilt dasselbe für die Mengen A_i. Da X Hausdorff-Raum ist, gibt es zu je zwei Punkten $x_i \in A_i$ (i=1,2) disjunkte offene Mengen U_{x_i} mit $x_i \in U_{x_i}$. Halten wir x_1 fest und variieren x_2 innerhalb A_2 so erhalten wir eine offene Überdeckung von A_2 durch endlich viele Mengen U_{x_2}. Ihre Vereinigung ist disjunkt zu Durchschnitt der entsprechenden Mengen U_{x_1}. Mit anderen Worten, es gibt zu vorgegebenen $x \in A_1$ disjunkte offene Mengen U_x und V mit $x \in U_x$ und $A_2 \subseteq V$. Variieren wir jetzt x innerhalb von A_1, so erhalten wir eine Überdeckung von A_1 durch endlich viele U_x. Die Vereinigung dieser U_x ist disjunkt zum Durchschitt der entsprechenden Mengen V.

QED.

5.1.4.4 Die Komponenten als Durchschnitte kompakter offener Teilmengen

Seien X ein kompakter Hausdorff-Raum und $x \in X$ ein Punkt. Weiter sei

$$\mathbf{A} := \{A_i\}_{i \in I}$$

die Familie aller kompakten und gleichzeitig offenen Teilmengen von X, welche x enthalten. Dann ist

$$C := \cap_{i \in I} A_i$$

die Komponente des Punktes x.

Beweis. Für jede zusammenhängende Menge Teilmenge $Z \subseteq X$, die den Punkt x enthält, hat man Zerlegungen

$$Z = (Z \cap A_i) \cup (Z - A_i),\ i \in I,$$

von Z in disjunkte offene Teilmengen. Da Y zusammenhängend ist, muß dann aber $Z = Z \cap A_i$ also $Z \subseteq A_i$. Wir haben gezeigt, die Komponente K des Punktes x liegt ganz in C,

$$K \subseteq C.$$

Zum Beweis der umgekehrten Inklusion genügt es zu zeigen, C ist zusammenhängend. Nehmen wir an, es gibt eine disjunkte Zerlegung

$$C = Y' \cup Y''$$

von C in abgeschlossene Teilmengen Y', Y". Es reicht zu zeigen, eine der Mengen Y', Y" ist leer. Nach 5.4.3 ist der Raum X normal, d.h. es gibt disjunkte offene Mengen U', U" von X mit

$$Y' \subseteq U' \text{ und } Y'' \subseteq U''.$$

Insbesondere gilt

$$\emptyset = (X - (U' \cup U'')) \cap C = (X - U') \cap (X - U'') \cap (\cap_{i \in I} A_i).$$

Wir haben eine Familie von abgeschlossenen Teilmengen von X gefunden, deren Durchschnitt leer ist. Da X kompakt ist, gibt es bereits eine endliche Teilfamilie, deren Durchschnitt ebenfalls leer ist,

$$\emptyset = (X - U') \cap (X - U'') \cap B,\ B := (\cap_{i \in J} A_i)$$

wobei $J \subseteq I$ eine geeignete endliche Teilmenge von I ist. Die Identität besagt gerade, es gilt $B \subseteq U' \cup U''$. Wir haben also eine disjunkte Zerlegung

$$B = (B \cap U') \cup (B \cap U'').$$

Insbesondere sind $B \cap U'$ und $B \cap U''$ disjunkte kompakte offene Teilmengen von X. Nur eine dieser Mengen enthält den Punkt x, sagen wir $B \cap U'$. Dann ist $B \cap U'$ ein Mitglied der Familie der A_i, d.h. es gilt

$$C = \cap_{i \in I} A_i \subseteq B \cap U' \subseteq U'.$$

Da die Mengen U' und U" disjunkt sind, folgt

$$Y'' = Y'' \cap U'' \subseteq C \cap U'' = \emptyset,$$

d.h. $Y'' = \emptyset$. Wir haben gezeigt, C ist zusammenhängend.
QED.

5.1.4.5 Existenz kleiner offener Untergruppen in topologischen Gruppen

Seien G eine topologische Gruppe und $U \subseteq G$ eine offene und kompakte Umgebung des neutralen Elements $e \in G$. Dann gibt es eine kompakte offene Untergruppe H von G mit $H \subseteq U$.

Beweis. Betrachten wir die Multiplikationsabbildun

$$\mu: G \times G \to G,\ (x,y) \mapsto x \cdot y.$$

Für jedes $u \in U$ gilt $\mu(e,u) \in U$. Also gilbt es offene Mengen $V_u, W_u \subseteq U$ mit $e \in V_u$, $u \in W_u$ und $\mu(V_u \times W_u) \subseteq U$. Wenn wir u innerhalb von U variieren, erhalten wir eine Überdeckung von U durch endlich viele der Mengen W_u. Bezeichne W die Vereinigung dieser endlich vielen W_u und V den Durchschnitt der entsprechenden Mengen V_u. Dann ist V eine offene Umgebung von e mit $V \cdot U \subseteq U$. Durch Verkleinern von V können wir noch erreichen, daß V symmetrisch ist, d.h. daß gilt

$$V^{-1} = V$$

(man ersetze V durch $V \cap V^{-1}$). Bezeichne V^n die Menge aller Produkte von n Elementen aus V. Dann gilt mit $V \cdot U \subseteq U$ auch

$$V^n \cdot U \subseteq U$$

für alle n. Ersetzt man links den Faktor U noch durch die Menge $V \subseteq U$, so erhält man

$$V^n \subseteq U$$

für alle n. Also liegt die Gruppe

$$H := \cup_{n \in \mathbb{Z}} V^n$$

ganz in U. Die Mengen V^n sind Vereinigungen von Mengen der Gestalt $g \cdot V$ mit $g \in G$ also offene Menge. Damit ist H auch offen. Weiter ist G-H die Vereinigung aller von H verschiedenen Nebenklassen von H, also auch offen. Also ist H abgeschlossen. Wegen $H \subseteq U$ ist damit H sogar kompakt.
QED.

5.1.4.6 Existenz kleiner offener Normalteiler in total unzusammenhängenden Gruppen

Seien G eine kompakte total unzusammenhängende topologische Gruppe und U eine Umgebung des neutralen Elements $e \in G$. Dann gibt es einen offenen kompakten Normalteiler $N \subseteq U$ (mit endlichem Index).
Beweis. 1.Schritt. U enthält eine kompakte offene Umgebung von e.
Die Menge {e} ist die Zusammenhangskomponente von e und als solche Durchschnitt von offenen kompakten Umgebungen A_i von e (nach 5.4.4).Insbesondere haben die A_i mit dem Komplement G-U einen leeren Durchschnitt. Da G-U abgeschlossen also kompakt ist, ist bereits der Durchschnit mit endlich vielen der A_i leer. Der Durchschnitt dieser A_i liegt also ganz in U.

2. Schritt. Existenz des beschriebenen Normalteilers.
Nach dem ersten Schritt und 5.4.5 gibt es eine kompakte offene Untergruppe $H \subseteq U$. Es reicht zu zeigen, der Normalteiler

$$N := \cap_{g \in G} gHg^{-1}$$

ist kompakt und offen. Die Kompaktheitsaussage ist trivial. Zum Beweis der Offenheit genügt es zu zeigen, die Menge

$$M := \{gHg^{-1} \mid g \in G\}$$

der zu H konjugierten Untergruppen ist endlich. Betrachten wir die surjektive Abbildung

$$\varphi: G \to M,\ g \mapsto gHg^{-1}.$$

Für zwei Elemente $g,g' \in G$ aus derselben Nebenklasse modulo H gilt

$$g' = gh$$

mit $h \in H$, also

$$g'Hg'^{-1} = ghHh^{-1}g^{-1} = gHg^{-1}.$$

Die beiden Elemente haben also dasselbe Bild bei φ. Die Abbildung φ induziert deshalb eine surjektive Abbildung

$$G/H \to M.$$

Es genügt, wenn wir zeigen, G/H ist endlich (d.h. H hat in G einen endliche Index). Betrachten wir die natürliche Abbildung

$$\gamma: G \to G/H$$

und versehen G/H mit der Faktortopologie, d.h. der stärksten Topologie, bei der γ stetig ist. Eine Menge von G/H ist dann genau dann offen, wenn ihr Urbild in G offen ist. Die Urbilder in G sind aber Vereinigungen von Mengen der Gestalt gH, also stets offen. Mit anderen Worten, die Topologie von G/H ist diskret.
Andererseits ist G/H als stetiges Bild der kompakten Menge G selbst kompakt. Das ist aber nur möglich, wenn G/H endlich ist.
QED.

5.1.4.7 Charakterisierung der proendlichen Gruppen

Sei G eine (Hausdorffsche) topologische Gruppe. Dann sind die beiden folgenden Aussagen äquivalent.

(i) G ist eine proendliche Gruppe.

(ii) G ist kompakt und total unzusammenhängend.

Beweis.(i) $\Rightarrow$ (ii). Sei $\{\pi_i^j : G_j \to G_i\}_{i,j\in I, i\le j}$ ein projektives System endlicher Gruppen. Wir setzen

$$G := \prod_{i\in I} G_i \qquad \text{und} \qquad L := \varprojlim_{i\in I} G_i.$$

Nach dem Satz von Tichonov ist G als Produkt kompakter topologischer Räume selbst kompakt. Die Untergruppe L liegt für je zwei i,j∈I mit i≤j im Kern des stetigen Homomorphismus

$$G \to G_i \times G_j \to G_i \times G_i \to G_i,\ (g_\alpha) \mapsto (g_i, g_j) \mapsto (g_i, \pi_i^j(g_j)) \mapsto g_i - \pi_i^j(g_j),$$

(die beiden letzten Pfeile bezeichnen stetige Abbildungen, da die Topologe der endlichen Gruppen G_i diskret sein soll) und ist gleich dem Durchschnitt aller dieser Kerne. Insbesondere ist L abgeschlossen in G, also kompakt.

Wir haben noch zu zeigen, L ist total unzusammenhängend. Dazu genügt es nach 5.4.4 zu zeigen, die Einermenge {e} läßt sich als Durchschnitt von offenen kompakten Teilmengen schreiben. Die Topologie von L ist die Unterraum-Topologie von G. Es genügt deshalb, die letzte Aussage für G anstelle von L zu beweisen. Insbesonder wird sich also erweisen, daß auch G total unzusammenhängend ist.

Sei $(g_\alpha)\in G$ vorgegeben und vom neutralen Element $e=\{e_\alpha\}$ verschiedenen. Wir haben zu zeigen, es gibt eine kompakte und gleichzeitig offene Umgebung des neutralen Elements, welche (g_α) nicht enthält. Wegen $(g_\alpha)\neq e$ gibt es eine Koordinate g_i mit $g_i \neq e_i$.

Wir setzen

$$U_\alpha := \begin{cases} \{e_\alpha\} & \text{falls } \alpha = i \\ G_\alpha & \text{sonst} \end{cases}$$

Dann ist $U := \prod_{\alpha\in I} U_\alpha$ offen in G (als Kern der Projektion auf die i-te Komponente) und kompakt (als direktes Produkt kompakter topologischer Räume) und eine Untergruppe. Nach Konstruktion liegt (g_α) nicht in U.

(ii) $\Rightarrow$ (i). Sei eine kompakte total unzusammenhängende Gruppe G gegeben. Bezeichne

$$\mathbf{N} := \{N_i\}_{i\in I}$$

die Familie aller offenen kompakten Normalteiler von G. Nach 5.4.6 enthält jede offene Umgebung des neutralen Elements e einen der Normalteiler N_i. Deshalb bilden die N_i eine Umgebungsbasis von e (d.h.die offenen Mengen von G sind gerade die Vereinigungen der Mengen der Gestalt $g\cdot N_i$ mit g∈G). Ebensfalls nach 5.4.6 sind die Faktorgruppen

$$G_i := G/N_i$$

endlich. Sie bilden ein projektives System, denn der Durchschnitt $N_i \cap N_j$ von je zwei der betrachteten Normalteiler gehört wieder zur Familie **N**. Sei

$$L := \varprojlim_{i\in I} G/N_i$$

der zugehörige projektive Limes. Da die G/N_i endich sind, ist L eine proendliche Gruppe. Es reicht zu zeigen, G ist isomorph zu L. Betrachten wir die Abbildung

$$f: G \to L,\ g \mapsto (g \bmod N_i)_{i\in I}.$$

Für $N_i \subseteq N_j$ ist das natürliche Bild der Restklasse $gN_i = (g \bmod N_i)$ gerade die Restklasse $gN_j=(g \bmod N_j)$, d.h. die Familie $(g \bmod N_i)_{i\in I}$. liegt tatsächlich in L und die Abbildung f ist wohldefiniert. Sie ist offensichtlich ein Gruppenhomorphismus (da die natürlichen Abbildungen $G\to G/N_i$ Homomorphismen sind). Da die Zusammensetzungen von f mit den Projektionen auf die Faktoren G/N_i gerade die natürlichen Abbildungen $G \to G/N_i$ also stetig sind, ist f selbst auch stetig (nach Definition der Produkttopologie). Der Kern von f ist der Durchschnitt

$$\mathrm{Ker}(f) = \cap\mathbf{N} = \cap_{i\in I} N_i$$

aller N_i, also gleich der Zusammenhangskomponente {e} von e (nach 5.4.4). Mit anderen Worten, f ist injektiv. Zum Abschluß des Beweises genügt es zu zeigen, daß f surjektiv ist (denn eine stetige Bijektion eines kompakten Raumes in einen Hausdorff-Raum ist ein Homöomorphismus). Sei also $(g_iN_i)\in L$ vorgegeben. Zeigen wir zunächst, der Durchschnitt

$$\cap_{i\in I} g_iN_i$$

ist nicht leer. Andernfalls wäre schon der Durchschnitt von endlich vielen der g_iN_i leer (weil G kompakt ist), sagen wir

$$g_{i_1}N_{i_1} \cap \ldots \cap g_{i_n}N_{i_n} = \varnothing.$$

Nun ist aber $N_j := N_{i_1} \cap \ldots \cap N_{i_n}$ ein Element der Familie **N.** Wegen $(g_iN_i)\in L$ ist das natürliche Bild von g_jN_j in G/N_{i_ν} für jedes ν gerade $g_{i_\nu}N_{i_\nu}$, d.h g_j liegt für jedes ν in der Restklasse $g_{i_\nu}N_{i_\nu}$ also auch im Durchschnitt dieser Restklassen. Dieser Widerspruch zeigt, es gibt ein Element

$$g\in\cap_{i\in I} g_iN_i.$$

Dann ist aber $gN_i = g_iN_i$ für jedes i, also $f(g) = (g_iN_i)$. Die Abbildung f ist surjektiv.
QED.

5.1.4.8 Limesdarstellung proendlicher Gruppen

Für jede proendliche Gruppe G gilt

$$G \cong \varprojlim_{N} G/N$$

wobei der Limes über alle offenen Normalteiler von G genommen wird.

Beweis. Dies ein Nebenergebnis des Beweises von 5.4.7.
QED.

5.1.4.9 Limesdarstellung für abgeschlossene Untergruppen

Für jede abgeschlossene Untergruppe H einer proendlichen Gruppe G gilt

$$H \cong \varprojlim_{N} H/H\cap N$$

wobei der Limes über alle offenen Normalteiler von G genommen wird.

Beweis. Die Untergruppe H ist mit G ebenfalls kompakt und total unzusammenhängend, also proendlich. Nach 5.4.8 gilt

$$G \cong \varprojlim_{N'} G/N'$$

wobei N' alle offenen Normalteiler von H durchläuft. Jeder solche Normalteiler hat die Gestalt

$$N' = H \cap U$$

mit einer offenen Menge $U \subseteq G$. Da G proendlich ist, enthält U einen offenen Normalteiler N von G (nach 5.4.6). Insbesondere gilt $H \cap N \subseteq N'$, d.h. jeder offene Normalteiler von H enthält einen offenen Normalteiler der Gestalt $H \cap N$. Die Gruppen der Gestalt $H/H \cap N$ bilden ein kofinales Teilsystem des Systems aller G/N'. Ein solches Teilsystem hat denselben projektiven Limes.
QED.

5.1.4.10 Limesdarstellung des Faktors nach einem abgeschlossenen Normalteiler

Seien G eine proendliche Gruppe und $N \subseteq G$ ein abgeschlossener Normalteiler. Dann gilt

$$G/N \cong \varprojlim_{N'} G/N'N,$$

wobei der Limes über alle offenen Normalteiler N' von G zu nehmen ist.
Beweis. Schreibt man

$$G/N'N = (G/N)/(N'N/N)$$

so sieht man, daß in der zu beweisenden Isomorphie rechts der Limes über alle offenen Normalteiler von G/N steht. Nach 5.4.8 genügt es deshalb zu zeigen, daß G/N proendlich ist. Dazu benutzen wir die topologische Charakterisierung 5.4.7 der proendlichen Gruppen. Mit G ist natürlich auch G/N kompakt. Es reicht also zu zeigen, G/N ist total unzusammenhängend.

Sei $x \notin N$ ein beliebiger Punkt. Da G ein Hausdorff-Raum ist, gibt es zu jedem $y \in N$ disjunkte offene Umgebungen $U_y(x)$ von x und V_y von y. Da G total unzusammenhängend ist, können wir nach 5.4.6 sogar annehmen, $U_y(x)$ hat die Gestalt

$$U_y(x) = N'(y)x$$

mit einem offenen kompakten Normalteiler N'(y) (mit endlichem Index). Nun ist N als abgeschlossene Untergruppe von G kompakt, wird also von endlich vielen der Mengen V_y überdeckt. Der Durchschnitt von endlich vielen der Mengen $U_y(x)$ ist deshalb disjunkt zum Normalteiler N. Mit anderen Worten, es gibt einen offenen kompakten Normalteiler N' von G mit

$$N'x \cap N = \varnothing.$$

Dann gilt aber $x \notin N'N$, also $xN \cap N'N = \varnothing$. Das bedeutet, es gibt eine kompakte offene Umgebung N'N/N des neutralen Elements von G/N, welche ein vorgegebenes Element xN nicht enthält. Die Zusammenhangskomponente des neutralen Elements von G/N besteht nur aus einem Element, d.h. G/N ist total unzusammenhängend.
QED.

5.1.5 Die Konstruktion von proendlichen Gruppen aus abstrakten Gruppen

5.1.5.1 Die Vervollständigung einer abstrakten Gruppe

Seien G eine abstrakte Gruppe und $\{N_i\}_{i\in I}$ eine Familie von Normalteilern mit der Eigenschaft, daß es für je zwei Normalteiler N_{i_1} und N_{i_2} der Familie einen dritten N_i gibt mit

$$N_i \subseteq N_{i_1} \cap N_{i_2} .$$

Wir führen in I eine Halbordnung ein, indem wir setzen

$$i \leq j \Leftrightarrow N_i \supseteq N_j .$$

Dann wird I zu einer gerichteten Menge und die Faktorgruppen G/N_i bilden zusammen mit den natürlichen Abbildungen

$$G/N_j \to G/N_i \text{ , } x \bmod N_j \mapsto x \bmod N_i ,$$

für $i \leq j$ ein projektives System. Der projektive Limes

$$\varprojlim_{i\in I} G/N_i$$

heißt Vervollständigung der Gruppe G bezüglich der Familie $\{N_i\}_{i\in I}$.

5.1.5.2 Reduktion auf den Fall separierter Familien

Setzt man $G_0 = \cap_{i\in I} N_i$, $\bar{G} := G/G_0$, $\bar{N}_i := N_i/G_0$, so gilt

$$G/N_i \cong \bar{G}/\bar{N}_i$$

also

$$\varprojlim_{i\in I} G/N_i \cong \varprojlim_{i\in I} \bar{G}/\bar{N}_i$$

Die Gruppen G und $\bar{G}$ haben somit dieselbe Vervollständigung bezüglich der angegebenen Familien.

5.1.5.3 Normalteiler mit endlichen Index

Seien G eine Gruppe und $\{N_i\}_{i\in I}$ die Familie aller Normalteiler mit endlichem Index. Dann sind die Bedingungen von 5.5.1 erfüllt. Die zugehörige Vervollständigung von G wird mit

$$\hat{G} := \varprojlim_{i\in I} G/N_i$$

bezeichnet. Zum Beispiel ist $\hat{\mathbb{Z}}$ der projektive Limes aller endlichen zyklischen Gruppen.

5.1.5.3 Normalteiler von p-Potenz-Ordnung

Seien G eine Gruppe, p eine Primzahl und $\{N_i\}_{i\in I}$ die Familie aller Normalteiler deren Index in G eine Potenz von p ist. Dann sind die Bedingungen von 5.5.1 erfüllt. Die zugehörige Vervollständigung von G wird mit

$$\hat{G}_p := \varprojlim_{i\in I} G/N_i$$

bezeichnet. Zum Beispiel ist $\hat{\mathbb{Z}}_p$ der projektive Limes aller zyklischen p-Gruppen. Dies ist die Gruppe der p-adischen (ganzen) Zahlen.

5.1.5.4 Übungsaufgabe

Man beweise

$$\hat{\mathbb{Z}} = \prod_{p \text{ Primzahl}} \hat{\mathbb{Z}}_p$$

5.1.6 Proendliche Gruppen in der Körpertheorie

5.1.6.1 Wiederholung zur Körpertheorie

Algebraische Körpererweiterungen

Eine Körpererweiterung heißt algebraisch, wenn eine der folgenden äquivalenten Bedingungen erfüllt ist.

(i) Für jedes Element $a\in K$ gibt es ein Polynom $p\in k[x]-\{0\}$ mit $p(a)=0$.

(ii) Für jedes Element $a\in K$ ist $k\{a)$ als k-Vektoraum endlich-dimensional.

Fortsetzungsatz

Seien K/k eine algebraische Körpererweitung und $s:k\to L$ ein nicht trivialer Ringhomomorphismus (von Ringen mit 1) mit Werten in einem algebraisch abgeschlossenen Körper L. Dann läßt sich s zu einem Ringhomormorphismus $K\to L$ fortsetzen.

Endliche Körpererweiterungen

Eine Körpererweiterung K/k heißt endlich, wenn eine der folgenden äquivalenten Bedingungen erfüllt ist.

(i) K ist als k-Vektorraum endlich-dimensional.

(ii) K ist algebraisch über k und endlich erzeugt.

Endliche Normale Körpererweiterung

Eine endliche Körpererweiterung K/k heißt normal, falls eine der folgenden äquivalenten Bedingungen erfüllt ist.

(i) K/k ist Zerfällungskörper eines Polynoms $p\in k[x]$, d.h. es gilt $K=k(a_1,...,a_n)$ mit

$$p = (x-a_1)\cdot...\cdot(x-a_n).$$

(ii) Jedes über k irreduzible Polynom mit einer Nullstelle in K zerfällt über K in Linearfaktoren.

(iii) Jeder Isomorphismus $K\to\bar{K}$ mit Werten in der algebraischen Abschließung, welcher k elementweise festläßt, ist ein Automorphismus $K\to K$.

(iv) $K\subseteq\bar{K}$ enthält mit jedem Element auch alle seine k-Konjugierten.

Beispiel: $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ ist nicht normal.

Separable Körpererweiterungen

Eine algebraische Körpererweiterung K/k heißt separabel, wenn für jedes $a\in K$ das über k irreduzible Polynom von a keine mehrfachen Nullstellen besitzt. In den Fällen $\mathbb{Q}\subseteq k$ bzw. $\#K < \infty$ ist die Körpererweitung K/k stets separabel.

Beispiel. Für $k := \mathbb{F}_p(x)$, $K := k(\sqrt[p]{x})$ erhält man eine inseparable Körpererweiterung K/k.

Satz vom primitiven Element
Jede endliche separable Körpererweiterung K/k ist einfach, d.h. von der Gestalt K=k(a).
Endliche Galoiserweiterungen
Eine endliche algebraissche Körpererweiterung K/k heißt Galoiserweiterung, wenn eine der folgenden äquivalenten Bedingungen erfüllt ist.

(i) Es gibt eine Gruppe von G von k-Automorphismen von K, mit $k = K^G$.
(ii) K/k ist normal und separabel.

Die Gruppe

$$G(K/k)$$

der k-Automorphismen von K (d.h der Ringhomomorphismen K→K, welche k elementweise festlassen), heißt dann Galoisgruppe von K/k.
Haupsatz der endlichen Galoistheorie
Seien K/k eine (endliche) Galoiserweitung und G = G(K/k) die Galoisgruppe.

(i) Die Abbildung

$$\{\text{Untergruppen von } G\} \to \{\text{Körper zwischen k und K}\},\ H \mapsto K^H,$$

ist bijektiv (und kehrt die $\subseteq$-Relation um). Die zugehörige inverse Abbildung ist durch die folgende Zuordnungsvorschrift gegeben.

$$F \mapsto G(K/F)$$

(ii) Bei der Zuordnung (i) entsprechen die Normalteiler von G gerade den normalen Körpererweiterungen.
(iii) Die Ordnung der Galoisgruppe G(K/k) ist gleich dem Grad der Erweitungen K/k.

$$\#G(K/k) = [K:k].$$

Literatur

1. Artin, E.: Galoissche Theorie, Teubner, Leipzig 1964
2. Lang, S.: Algebra, Addison-Wesley, Reading, Mass., 1965
3. van der Waerden, B.L.: Algebra, Springer, Berlin 1967 (2 Bände)
4. Bourbaki, N.: Algèbre, Hermann, Paris 1950
5. Redei, L.: Algebra, Teil I, Geest & Portig, Leipzig 1959

5.1.6.2 Das projektive System zu einer unendlichen Galoiserweiterung

Sei E eine Galoiserweiterung des Körpers F. Das bedeutet, E ist algebraisch über F und die Gruppe

$$G := G(E/F)$$

aller F-Automorphismen des Körpers E läßt kein Element von E - F fest:

$$E^G = F.$$

Die einfachsten Phenomene der Körpertheorie einschließlich der endlichen Galoistheorie findet man in [1], Kapitel V.
Sei $\{K_i\}_{i\in I}$ die Familie aller endlichen Galoiserweiterungen des Körpers F, welche in E enthalten sind. Dann ist

$$E = \cup_{i\in I} K_i .$$

Weiter gelten die folgenden Aussagen.

(i) Für $K_i \subseteq K_j$ ist die Einschränkungsabbildung

$$G(K_j/F) \to G(K_i/F),\ s \mapsto s|_{K_i},$$

wohldefiniert und surjektiv.
(ii) Das Kompositium von zwei Körpern aus der Familie der K_i ist wieder ein Körper aus dieser Familie.

Mit anderen Worten, die Galoisgruppen $G(K_i/F)$ bilden ein projektives System.

5.1.6.3 Die Galoisgruppe als proendliche Gruppe

Seien E/F eine Galoiserweiterung und $\{K_i\}_{i\in I}$ die Familie aller endlichen Galoisschen Teilerweiterungen von F. Dann gilt

$$G(E/F) \cong \varprojlim_{i\in I} G(K_i/F).$$

Die Galoisgruppe G(E/F) hat folglich die Struktur einer proendlichen Gruppe und insbesondere einer topologischen Gruppe. Die Untergruppen $U_i:=G(E/K_i)$ bilden eine Umgebungsbasis des neutralen Elements.

Beweis. Für jedes $i\in I$ haben wir einen Einschränkungshomomorphismus

$$\varphi: G(E/F) \to G(K_i/F),\ s \mapsto s|_{K_i}.$$

Die Familie aller dieser Homomorphismen definierte einen Homomorphismus ins direkte Produkt

$$\varphi: G(E/F) \to \prod_{i\in I} G(K_i/F),\ s \mapsto (s|_{K_i})_{i\in I}.$$

Das Bild dieses Homomorphismus liegt nach Konstruktion im projektiven Limes

$$L := \varprojlim_{i\in I} G(K_i/F).$$

Wir haben zu zeigen, die Abbildung

$$\varphi: G(E/F) \to L$$

ist bijektiv. Sei $s\in G(E/F)$ ein nicht-trivialer F-Automorphismus $E\to E$. Dann gibt es ein $x\in K$ mit $s(x)\neq x$. Das Element x liegt bereits in einer endlichen Galoisschen Teilerweiterung, sagen wir $x\in K_i$. Trivialerweise gilt

$$s|_{K_i}(x) \neq x.$$

Mit anderen Worten, $\varphi(s)$ ist nicht die identische Abbildung. Wir haben gezeigt, der Homomorphismus φ ist injektiv. Sei jetzt $(s_i)_{i\in I}$ ein beliebiges Element von L. Das bedeutet, $s_i: K_i \to K_i$ ist für jedes i ein F-Automorphismus, und für jedes j mit $K_j \subseteq K_i$ ist die Einschränkung von s_i auf K_j gerade gleich s_j. Mit anderen Worten, die s_i setzen sich zu einer Abbildung $s: E\to E$ zusammen. Nach Konstruktion ist s ein F-Automorphismus, dessen Bild bei φ gerade das vorgegebene Element von L ist.

Der letzte Teil der Behauptung folgt aus der Tatsache, daß $U_i:=G(E/K_i)$ gerade der Kern der Einschränkungsabbildung

$$G(E/F) \to G(K_i/F)$$

ist.

QED.

5.1.6.4 Die Galoisgruppe der algebraischen Abschließung eines endlichen Körpers

Sei E die algebraische Abschließung des Körpers $\mathbb{F}_p$ mit p Elementen. Dann Gilt

$$G(E/\mathbb{F}_p) \cong \hat{\mathbb{Z}}$$

Beweis. Die endlichen Körpererweiterungen von $\mathbb{F}_p$ sind von der Gestalt

$$\mathbb{F}_{p^n}.$$

Letzterer Körper ist gerade der Zerfällungskörper der Polynoms $X^{p^n}-X \in \mathbb{F}_p[X]$ und stimmt mit der Menge aller Nullstellen dieses Polynoms überein. Insbesondere ist $\mathbb{F}_{p^n}$ eine Galois-Erweiterung von $\mathbb{F}_p$. Bestimmen wir die Galoisgruppe von $\mathbb{F}_{p^n}$. Auf allse Fälle ist die Abbildung

$$F: \mathbb{F}_{p^n} \to \mathbb{F}_{p^n},\ x \mapsto x^p,$$

ein Automorphismus von $\mathbb{F}_{p^n}$. Da alle Elemente von $\mathbb{F}_{p^n}$ Nullstellen von $X^{p^n}-X$ sind, gilt

$$F^n = id.$$

Wäre bereits eine niedrigere Potenz von F die identische Abbildung, so gäbe es ein Polynom von Grad $< p^n$, welches in allen Elementen von $\mathbb{F}_{p^n}$ Null wäre, was unmöglich ist. Also erzeugt F eine n-elementige Untergruppe der Galoisgruppe von $\mathbb{F}_{p^n}$, d.h. es gilt

$$G(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle F \rangle \cong \mathbb{Z}/n\mathbb{Z}.$$

Nach 5.6.3 und 5.5.3 ist damit

$$G(E/\mathbb{F}_p) \cong \varprojlim_n G(\mathbb{F}_{p^n}/\mathbb{F}_p) = \varprojlim_n \mathbb{Z}/n\mathbb{Z} \cong \hat{\mathbb{Z}}.$$

QED.

5.1.6.5 Hauptsatz der Galoistheorie

Sei E/F eine Galoiserweiterung mit der Galoisgruppe G = G(E/F). Wir führen folgende Bezeichnungen ein.

S := {H | H abgeschlossen Untergruppe von G}
F := {K | K Körper mit F⊆K⊆E}

Dann ist die folgende Abbildung bijektiv.

$$\varphi: \mathbf{F} \to \mathbf{S},\ K \mapsto G(E/K).$$

Die inverse Abbildung ist dabei gerade die Abbildung

$$\mathbf{S} \to \mathbf{F},\ H \mapsto E^H := \{e \in E \mid h(e) = e \text{ für alle } h \in H\}.$$

Beweis. 1.Schritt. $K \in \mathbf{F} \Rightarrow G(E/K) \in \mathbf{S}$ (d.h. die Abbildung φ ist wohldefiniert).
Sei $\{L_j\}_{j\in J}$ die Familie der endlichen Teilerweiterungen von F, die ganz in K liegen. Dann gilt $K = \cup L_j$, also $G(E/K) = \cap G(E/L_j)$. Jeder Körper $L_j \subseteq K_j$ liegt ganz in einer endlichen Galoiserweiterung K_j von F mit $K_j \subseteq E$. Insbesondere gilt $G(E/L_j) \supseteq G(E/K_j)$. Auf Grund der Limesdarstellung 5.6.3 für G(E/F) ist $G(E/K_j)$ offen in G(E/F). Dann ist aber auch $G(E/L_j)$ als Vereinigung von Nebenklassen modulo $G(E/K_j)$ offen in G(E/F). Insbesondere ist $G(E/L_j)$ abgeschlossen. Dann ist aber der Durchschnitt

$$G(E/K) = \cap G(E/L_j)$$

ebenfalls abgeschlossen.

2.Schritt. $K \in \mathbf{F} \Rightarrow K = E^{G(E/K)}$ (insbesondere ist die Abbildung φ ist injektiv).

Die Inklusion "$\subseteq$" ist trivial. Zum Beweis der umgekehrten Inklusion benutzen wir die Tatsache, daß die zu beweisende Identität richtig ist im Fall endlicher Körpererweiterungen E/K. Sei $x \in E^{G(E/K)}$. Falls x nicht in K liegt, gibt es eine endliche Galoiserweiterung $K' \subseteq E$ von K mit $x \in K'$ und einen Automorphismus $\sigma \in G(K'/K)$ mit $\sigma(x) \neq x$. Dieser Automorphismus σ besitzt eine Fortsetzung zu einem Automorphismus $\sigma: E \to E$. Da auch für die Fortsetzung $\sigma(x) \neq x$ gilt, folgt $x \notin E^{G(E/K)}$ im Widerspruch zur Wahl von x.
3. Schritt. Die Abbildung φ ist surjektiv.
Sei $H \in \mathbf{S}$ vorgegeben. Wir setzen

$$K := E^H \text{ und } H' := G(E/K).$$

Nach Konstruktion gilt dann $H \subseteq H'$ und nach dem zweiten Schritt ist

$$E^H = K = E^{G(E/K)} = E^{H'}.$$

Für jeden offenen Normalteiler V_i von H' gilt also

$$(L_i)^{H'/V_i} = K = L_i^{HV_i/V_i} \text{ mit } L_i := E^{V_i}.$$

Der Hauptsatz der Galoistheorie für endliche Erweiterungen liefert

$$H'/V_i = HV_i/V_i$$

für alle V_i, also $H' = HV_i$. Die Untergruppe H von H' liegt also dicht in H'. Da H abgeschlossen ist, folgt H = H'.
QED.

5.2 Kohomologietheorie

5.2.1 Vorbemerkung

Unser nächstes Ziel ist es, die für endliche Gruppen entwickelte Kohomologietheorie auf den Fall von proendlichen Gruppen zu erweitern. Dazu benötigen wir zunächst eine Vorbereitungen.

5.2.2 Induktive Systeme und induktive Limiten

5.2.2.1 Induktive Systeme

Wir beschränken uns hier auf die Kategorie der (additiv geschriebenen) diskreten abelschen Gruppen.
Seien I eine gerichtete Menge und $\{G_i\}_{i \in I}$ eine Familie von abelschen Gruppen. Für beliebige $i,j \in I$ mit $i \leq j$ sei ein Gruppenhomomorphismus $\tau_i^j: G_i \to G_j$ gegenben, wobei folgende Bedingungen erfüllt seien.

1. $\tau_i^i = \mathrm{id}$ für beliebige $i \in I$.
2. $\tau_j^k \circ \tau_i^j = \tau_i^k$ für beliebige $i,j,k \in I$ mit $i \leq j \leq k$.

Die Familie der Morphismen

$$\{\tau_i^j: G_i \to G_j\}_{i,j \in I, i \leq j}$$

heißt dann induktives System über der Indexmenge I. Häufig werden wir auch von der Familie $\{G_i\}_{i \in I}$ als von dem induktiven System sprechen und uns die Morphismen τ_i^j als gegeben denken.

5.2.2.2 Morphismen induktiver Systeme

Seien $\{\tau_i^j: G_i \to G_j\}_{i,j\in I, i\le j}$ und $\{\tau'^j_i: G'_i \to G'_j\}_{i,j\in J, i\le j}$ zwei induktive Systeme. Ein Morphismus

$$(f,\psi): \{\tau_i^j: G_i \to G_j\}_{i,j\in I, i\le j} \to \{\tau'^j_i: G'_i \to G'_j\}_{i,j\in J, i\le j}$$

von induktiven System besteht aus einer ordnungserhaltenden Abbildung

$$\psi: I \to I'$$

und aus einer Familie

$$f = \{f_i: G_i \to G'_{\psi i}\}_{i\in I}$$

Gruppenhomomorphismen, wobei für je zwei Indizes $i,j\in I$ mit $i\le j$ das folgende Diagramm kommutativ ist.

$$\begin{array}{ccc} G_i & \xrightarrow{f_i} & G'_{\psi i} \\ {\scriptstyle \tau_i^j}\downarrow & & \downarrow{\scriptstyle \tau'^{\psi j}_{\psi i}} \\ G_j & \xrightarrow{f_j} & G'_{\psi j} \end{array}$$

Die Familie f heißt in dieser Situation auch ψ-Morphismus.

5.2.2.3 Induktive Limites

Sei $\{\tau_i^j: G_i \to G_j\}_{i,j\in I, i\le j}$ ein induktives System. In der disjunkten Vereinigung

$$S := \cup_{i\in I} G_i$$

definieren wir eine Äquivalenzrelation $\sim$. Die Elemente $x\in G_i$ und $y\in G_j$ werden als äquivalent angesehen, wenn es ein $k\in I$ mit $i\le k$ und $j\le k$ gibt mit

$$\tau_i^k x = \tau_j^k y.$$

Es ist leicht zu sehen, daß die beschriebenen Relation tatsächlich eine Äquivalenzrelation ist. Die Menge der zugehörigen Äquivalenzklassen wird mit

$$G := \varinjlim_{i\in I} G_i$$

und heißt induktiver Limes. Der induktive Limes ist wie folgt mit der Struktur einer abelschen Gruppe versehen. Repräsentieren $x\in G_i$ und $y\in G_j$ zwei Elemente des induktiven Limes und ist $k\in I$ ein Index mit $i\le k$ und $j\le k$, so wird die Summe der beiden Elemente durch

$$\tau_i^k x + \tau_j^k y \in G_k$$

repräsentiert. Das Nagative des durch x repräsentierten Elementes von G wird durch -x repräsentiert.
Ein Morphismus von induktiven Systemen induziert einen Gruppenhomomorphismus der zugehörigen induktiven Limites. Der induktive Limes ist deshalb ein Funktor von der Kategorie der induktiven Systeme in die Kategorie der abelschen Gruppen.

5.2.3 Diskrete Moduln

5.2.3.1 Definition: diskreter Modul

Seien G eine proendliche Gruppe und M ein (linker) G-Modul. Ist $U\subseteq G$ eine offene Untergruppe von G, so bezeichnen wir wie üblich mit

$$M^U := \{m\in M \mid gm = m\}$$

den Teilmodul der U-invarianten Elemente von M. Der G-Modul M heißt diskret, wenn gilt

$$M = \cup_U M^U,$$

wobei die Vereinigung über alle offenen Normalteiler von G erstreckt werde. Wir werden im folgenden fast ausschließlich diskrete G-Moduln betrachten.

5.2.3.2 Kriterium für diskrete Moduln

Seien G eine proendliche Gruppe und M ein G-Modul. Dann sind folgenden Bedingungen äquivalent.

(i) M ist ein diskreter G-Modul.

(ii) Für jedes $m \in M$ ist der Stabilisator $G_m := \{g \in G \mid gm = m\}$ von m in G eine offene Untergruppe von G.

(iii) Die Abbildung $G \times M \to M$, $(g,m) \mapsto gm$, ist stetig, wenn man M als diskreten topologischen Raum betrachtet und G mit der üblichen Topologie einer proendlichen Gruppe versehen ist.

Beweis.(i) $\Rightarrow$ (ii). Nach Voraussetzung gibt es für jedes $m \in M$ einen offenen Normalteiler $U \subseteq G$ mit $m \in M^U$, d.h. mit $Um = \{m\}$. Mit anderen Worten, es gilt $U \subseteq G_m$. Dann ist aber G_m Vereinigung von Nebenklassen modulo U und als solche offen.

(ii) $\Rightarrow$ (iii). Da die Topologie von M diskret sein soll, genügt es zu zeigen, für jedes $m \in M$ ist die Faser $\mu^{-1}(m)$ der Multiplikationsabbildung

$$\mu: G \times M \to M,\ (g,m) \mapsto gm,$$

eine offene Teilmenge von $G \times M$. Der Stabilisator G_m von m operiert auf der Faser

$$\mu^{-1}(m) = \{(g,n) \in G \times M \mid gn = m\}$$

vermittels der Vorschrift

$$G_m \times \mu^{-1}(m) \to \mu^{-1}(m),\ (h, (g,n)) \mapsto (hg,n),$$

d.h. die Menge $\mu^{-1}(m)$ zerfällt in die Vereinigung von G_m-Orbits. Diese sind Menge der Gestalt $G_m g \times \{n\}$, also nach Voraussetzung (i) offene Mengen von $G \times M$. Dann ist aber auch $\mu^{-1}(m)$ offen in $G \times M$.

(iii) $\Rightarrow$ (i). Da die Mulitiplikation $\mu: G \times M \to M$, $(g,m) \mapsto gm$, stetig ist, ist

$$\mu^{-1}(m)$$

für jedes $m \in M$ eine offene Menge. Nach 5.4.6 gibt es deshalb einen offenen Normalteiler $U \subseteq \mu^{-1}(m)$, d.h. es ist $m \in M^U$. Da m beliebig war, sehen wir M ist ein diskreter G-Modul.

QED.

5.2.3.3 Diskrete G-Moduln als direkte Limites

Seien G eine proendliche Gruppe und M ein diskreter G-Modul. Weiter sei

$$\{U_i\}_{i \in I}$$

die Familie aller offenen Normalteiler von G. Dann gilt

$$G \cong \varprojlim_{i \in I} G/U_i$$

und

$$M = \varinjlim_{i\in I} M^{U_i}.$$

Beweis. Die erstere Isomorphie besteht nach 5.4.8 und die letztere, auf Grund von Definition 5.7.5 (diskreter G-Modul) und der Tatsache, daß die Vereinigung $\cup M^{U_i}$ zum entsprechenden direkten Limes isomorph ist. Für gegebene $i,j\in I$ mit $i\leq j$ (d.h. $U_j \subseteq U_i$) haben wir Gruppenhomomorphismen

$$G/U_j \to G/U_i \text{ und } M^{U_i} \to M^{U_j}$$

QED.

5.2.4 Kohomologie der proendlichen Gruppen

5.2.4.1 Definition: Kohomologie einer proendlichen Gruppe

Seien G eine proendliche Gruppe, M ein diskreter G-Modul und

$$\{U_i\}_{i\in I}$$

die Familie aller offenen Normalteiler von G. Dann heißt

$$H^q(G,M) := \varinjlim_{i\in I} H^q(G/U_i, M^{U_i})$$

q-te Kohomologie von G mit Koeffizienten in M.

5.2.4.1 Alternative Definition der Kohomologie proendlicher Gruppen

Seien G eine proendliche Gruppe und M ein diskreter G-Modul. Bezeichne

$$C^q = C^q(G,M)$$

die additive Gruppe aller stetigen Abbildungen

$$G^q = G\times\ldots\times G \to M.$$

Wir definieren einen Randoperator $d:G^q\to G^{q+1}$ durch

$$\begin{aligned}(df)(g_1,\ldots,g_{q+1}) &:= g_1\cdot f(g_2,\ldots,g_{q+1})\\ &+ \sum_{i=1}^{q}(-1)^i f(g_1,\ldots,g_ig_{i+1},\ldots,g_{q+1})\\ &+ (-1)^{n+1} f(g_1,\ldots,g_q)\end{aligned}$$

Zusammen mit diesen Randoperatoren bilden die Gruppen C^q einen Komplex, dessen Kohomologiegruppen gerade die in 5.7.7 definierten Kohomologiegruppen von G mit Koeffizienten in M sind.

Beweisskitze. Der vollständige Beweis ist nicht besonders schwer, aber etwas langwierig. Wir beschränken uns deshalb auf einige Bemerkungen.

1. Eine Abbildung

   $$\Phi: H \to S$$

   einer proendlichen Gruppe mit Werten in einem diskreten topologischen Raum S ist genau dann stetig, wenn es einen offenen Normalteiler $K\subseteq H$ gibt und eine solche Abbildung

   $$\Psi: H/K \to S$$

   der endlichen Gruppe H/K mit Werten in S, daß Φ die Zusammensetzung von Ψ mit dem natürliche Homomorphismus $H\to H/K$ ist.

Sei $\Phi: H \to S$ stetig.

Für jeden Punkt $s\in S$ und jedes $h\in H$ mit $\Phi(h) = s$ gibt es wegen der Stetigkeit von Φ einen offenen Normalteiler N_h mit $\Phi(hN_h) = s$. Endlich viele solcher Normalteiler

überdecken H (da H kompakt ist).Sei N der Durchschnitt einer solchen endlichen Familie von Normalteilern. Jedes N_h ist der gegebenen Familie dann Vereinigung von Nebenklassen modulo N (wegen $N \subseteq N_h$). Mit anderen Worten, H kann als Vereinigung von Nebenklassen modulo N geschreiben werden, wobei Φ auf jeder dieser Nebenklassen konstant ist. Dann existiert aber die oben beschriebene Faktorisierung von Φ. Die umkehrte Aussage, daß aus der Existenz einer Faktorisierung die Stetigkeit von Φ folgt, ist trivial.

2. Sei $f \in C^q(G,M)$. Dann existiert nach der ersten Bemerkung ein offener Normalteiler $U' \subseteq G$ derart, daß sich f über einer Abbildung $f':(G/U')^q \to M$ faktorisiert. Da f' nur endlich viele Werte annimmt, gibt es einen offenen Normalteilter[125] U" mit $Im(f') \subseteq M^{U"}$ Wir setzen U := U'∩U". Dann ist U eine offener Normalteiler und f faktorisiert sich über eine Abbildung

$$(G/U)^q \to M^U.$$

Mit anderen Worten, jedes Element von $C^q(G,M)$ kommt von einem Element der Gruppe $C^q(G/U,M^U)$ mit geeignet gewählten U. Es ist jetzt nicht sehr schwer, zu zeigen

$$C^q(G,M) := \varinjlim_{i \in I} C^q(G/U_i, M^{U_i})$$

Daraus ergibt sich die entsprechende Relation der Kohomologiegruppen.
QED.

5.2.5 Beispiel: Erzeugende von Pro-p-Gruppen

5.2.5.1 Das Beispiel

Seien G eine Pro-p-Gruppe (d.h. der inverse Limes von p-Gruppen) und $\mathbb{F}_p$ der Körper mit p Elementen. Wir betrachten $\mathbb{F}_p$ als diskreten G-Modul mit der trivialen Operation. Aus der Formel für den Randoperator in 5.7.8 ergibt sich unmittelbar

$$H^1(G,\mathbb{F}_p) = Hom(G,\mathbb{F}_p).$$

Da $\mathbb{F}_p$ kommutativ und die p-te Potenz jedes Elements gleich Eins ist, gilt

$$Hom(G,\mathbb{F}_p) = Hom(G/G^*,\mathbb{F}_p)$$

mit $G^* = G^p[G,G]$. Da G/[G,G] abelsch ist, ist G* ein Normalteiler. Die $\mathbb{Z}$-Modulstruktur von G/G* induziert auf G/G* die Struktur eines $\mathbb{F}_p$-Vektorraums. Wenn G endlich erzeugt ist, so ist es auch die Faktorgruppe G/G*, d.h. G/G* ist dann ein endlich-dimensionaler $\mathbb{F}_p$-Vektorraum (und als solcher endlich). Seien jetzt

$$x_1G^*, \ldots, x_dG^*, \qquad d := \dim_{\mathbb{F}_p} H^1(G,\mathbb{F}_p),$$

eine $\mathbb{F}_p$-Vektorraumbasis von G/G* und

---

[125] Im(f') ist ein G-Teilmodul von M mit nur endlich vielen Elementen. Insbesondere sind die G-Orbits der Elemente von M endlich. Die Stabilisatoren der Elemente von M in G haben also endlichen Index. Da G auf M stetig operiert, sind die Stabilisatoren offene Untergruppen von G. Wegen der Endlichkeit von Im(f') gibt es einen offenen Normalteiler U", der in jedem Stabilisator eines Elements von Im(f') liegt.

$$U \subseteq G^*$$

ein offener Normalteiler. Nach dem Satz von Bernside[126] (s.u.) wird dann G modulo U von den Elementen $x_1, \ldots, x_d$ erzeugt. Mit anderen Worten, die x_i erzeugen eine dichte Untergruppe von G. Man sagt in dieser Situation, die x_i sind topologische Generatoren. Wir haben gezeigt,

$$\dim_{\mathbb{F}_p} H^1(G,\mathbb{F}_p)$$

ist gerade die Minimalzahl topologischer Generatoren von G.

5.2.5.2 Satz von Bernside

Sei $f:G' \to G$ ein stetiger Homomorphismus von Pro-p-Gruppen. Dann sind die folgenden Aussagen äquivalent.

(i) f ist surjektiv.

(ii) Die durch f induzierte Abbildung $H^1(f): H^1(G,\mathbb{F}_p) \to H^1(G',\mathbb{F}_p)$ ist injektiv.

(iii) Die durch f induzierte Abbildung $G'/G'^* \to G/G^*$ ist surjektiv.

Beweis. Wie wir eben gesehen haben gilt

$$H^1(G,\mathbb{F}_p) = \mathrm{Hom}(G,\mathbb{F}_p) = \mathrm{Hom}(G/G^*,\mathbb{F}_p)$$

Aus der ersten Gleichheit ergibt sich daraus unmittelbar die Implikation

$$(i) \Rightarrow (ii).$$

Das zweite Gleichheitszeichen besagt, $H^1(G,\mathbb{F}_p)$ ist gerade der zu G/G^* duale Vektorraum. Man beachte, die Gruppe G/G^* hat die Struktur eines $\mathbb{F}_p$-Vektorraums und die Abbildung von (iii) ist eine $\mathbb{F}_p$-lineare Abbildung. Daraus ergibt sich die Äquivalenz

$$(ii) \Leftrightarrow (iii).$$

Es genügt also, die Implikation (ii) $\Rightarrow$ (i) zu beweisen. Nehmen wir an, f ist nicht surjektiv: $f(G') \neq G$. Wir haben zu zeigen, daß dann $H^1(f)$ nicht injektiv ist.Da G' kompakt ist, ist f(G') eine abgeschlossene Untergruppe. Insbesondere gilt nach 5.9.4

$$f(G') = \varprojlim_N f(G')/f(G') \cap N,$$

wobei N die offenen Normalteiler von G durchläuft. Wegen $f(G') \neq G$ gilt somit

$$(f(G')/f(G') \cap N =)\ f(G')N/N \neq G/N$$

für mindestens einen offenen Normalteiler $N \subseteq G$. Mit anderen Worten, es gibt einen surjektiven Homomorphismus

$$\pi: G \to \bar{G} \text{ mit } \bar{H} := \pi(\mathrm{Im}(f)) \neq \bar{G}\ (:= G/N).$$

Behauptung: $\bar{H}$ liegt im Kern eines nicht-tivialen Homomorphismus $\bar{G} \to G$". (*)

Wir führen den Beweis nach Induktion nach der Ordnung $n := \#\bar{G}$ der endlichen p-Gruppe $\bar{G}$. Da $\bar{G}$ eine echte Untergruppe hat, gilt $n \geq p$.

Im Fall $n=p$ ist $\bar{H}$ selbst schon die triviale Gruppe und wir können für $\bar{G} \to G" := \{e\}$ den trivialen Homomorphismus nehmen.

---

[126] Sei G' die von den Elementen x_i erzeugte Untergruppe und $f:G' \to G$ die natürliche Einbettung.

Sei jetzt n>p. Als endliche p-Gruppe hat $\bar{G}$ ein nicht-tiviales Zentrum[127] $Z(\bar{G})$. Ist der Durchschnitt $\bar{H}\cap Z(\bar{G})$ nicht-trivial, so können wir durch Faktorisieren nach dem Normalteiler $Z(\bar{G})$ von $\bar{G}$ das Problem auf den Fall einer Gruppe $\bar{G}$ mit weniger Elementen reduzieren.[128] Sei also

$$\bar{H}\cap Z(\bar{G}) = \{e\}.$$

Im Fall $\bar{H}\cdot Z(\bar{G}) \neq \bar{G}$ können wir nach $Z(\bar{G})$ faktorisieren und dann ebenfalls die Induktionsvoraussetzung anwenden. Sei also außerdem

$$\bar{H}\cdot Z(\bar{G}) = \bar{G}.$$

Dann ist aber $\bar{H}$ ein Normalteiler, sodaß wir für $\bar{G}\to G$" den natürlichen Homomorphismus $\bar{G}\to\bar{G}/\bar{H}$ nehmen können. Damit ist (*) bewiesen. Sei jetzt ein surjektiver Homomorphism $\bar{G}\to G$" wie in (*) gegeben. Dann können wir G" durch eine nicht-triviale Faktorgruppe ersetzen ersetzen und erhalten wieder einen solchen Homorphismus. Da G" eine p-Gruppe ist, also ein nicht-triviales Zentrum besitzt, können wir auf diese Weise erreichen, daß G"= $\mathbb{F}_p$ gilt. Mit anderen Worten, wir haben einen nicht-trivialen Homomorphismus

$$\varphi: G \to \mathbb{F}_p,$$

dessen Kern die Untergruppe f(G') enthält. Fassen wir φ als Element von

$$H^1(G,\mathbb{F}_p) = \mathrm{Hom}(G,\mathbb{F}_p),$$

so bedeutet die Bedingung $f(G')\subseteq \mathrm{Ker}(\varphi)$, daß φ im Kern von $H^1(f)$ liegt, d.h. $H^1(f)$ ist nicht injektiv.
QED.
Bemerkung. Der Satz von Bernside ist ein Analogon zum Lemma von Nakayama in der kommutativen Algebra.

5.2.6. Galois-Kohomologie I: die additive Theorie

5.2.6.1 Die Situation

Seien E/F eine Galoiserweiterung und G = Gal(E/F) deren Galoisgruppe. Weiter sei

$$\{K_i\}_{i\in I}$$

die Familie der endlichen Galoisschen Teilerweiterungen von E/F. Wir setzen

$$U_i := \mathrm{Gal}(E/K_i) = \mathrm{Ker}(\mathrm{Gal}(E/F) \to \mathrm{Gal}(K_i/F)).$$

Dann gilt nach 5.6.3

$$G = \varprojlim_{i\in I} U_i$$

---

[127] Man betrachte die Operation G×G→G von G auf sich durch Konjugation. Alle Orbits von G haben p-Potenzordung. Das Orbit von e hat die Ordnung 1. Also gibt es ein weiteres Orbit der Ordunung 1.

[128] Ist die Inklusion $\bar{H}\bullet Z(\bar{G})/Z(\bar{G}) \longrightarrow \bar{G}/Z(\bar{G})$ nicht mehr echt, d.h. gilt $\bar{H}\bullet Z(\bar{G}) = \bar{G}$, so ist $\bar{H}$ ein Normalteiler von $\bar{G}$ und $\bar{H}$ liegt im Kern des natürlichen Homomorphismus $\bar{G} \longrightarrow \bar{G}/\bar{H}$.

Die Operation von G auf E definiert auf E die Struktur eines G-Moduls mit

$$E^{U_i} = K_i \text{ und } E = \cup_{i\in I} K_i.$$

Mit anderen Worten, E ist ein diskreter G-Modul. Weiter ist K_i ein $Gal(K_i/F)$-Modul und es gilt $Gal(K_i/F) = G/U_i$. Damit ist aber

$$(1) \qquad H^q(G,E) = \varinjlim_{i\in I} H^q(G/U_i, E^{U_i}) \qquad \text{(Definition 5.7.7)}$$
$$= \varinjlim_{i\in I} H^q(Gal(K_i/F), K_i).$$

5.2.6.2 Proposition 2.1: die additive Variante von Hilberts Satz 90

Seien E/F eine Galoiserweiterung und G = Gal(E/F) deren Galoisgruppe. Dann gilt

$$H^q(G,E) = 0 \text{ für jedes } q\geq 1.$$

Dabei bezeichne $H^q(G,E)$ die proendliche Kohomologie im Sinne von 5.7.7.
Beweis. Auf Grund von Darstellung (*) von 5.8.1 der Kohomologie von G mit Werten in E genügt es das nachfolgende Lemma zu beweisen.
QED.

5.2.6.3 Lemma

Sei E/F eine endliche Galoiserweiterung mit der Galoisgruppe G = Gal(E/F). Dann gilt

$$H^q(G,E) = 0 \text{ für jedes } q\geq 1.$$

Beweis. Sei $w_1,...,w_n$ eine Normalbasis von E/F. Dann ist die F-lineare Abbildung

$$F[G] \to E,\ g \mapsto g(w_1),$$

sogar ein Homomorphismus von G-Moduln. Die Normalbasiseigenschaft impliziert, daß das Bild des Homomorphismus ein Erzeugendensystem von E enthält, also surjektiv ist. Da die F-Vektorraume F[G] und E dieselbe Dimension besitzen, ist der Homomorphismus sogar bijektiv. Wir haben gezeigt, E ist ein freier F[G]-Modul (von Rang 1), d.h.

$$E \cong F\otimes_{\mathbb{Z}}\mathbb{Z}[G]$$

ist ein induzierte G-Modul. Dann gilt aber $H^q(G,E) = 0$ für jedes $q\geq 1$.
QED.

5.2.6.4 Folgerung

Sei K/k eine endliche Galoiserweiterung. Dann ist die Tate-Kohomologie von E über der Galoisgruppe G = Gal(E/k) trivial:

$$\hat{H}^q(G, E) = 0 \text{ für alle } q\in\mathbb{Z}.$$

Beweis. Wegen $\hat{H}^q = H^q$ für $q\geq 1$ gitl die Aussage für alle $q\geq 1$. Nun ist E induziert, also kohomologisch trivial. Durch Dimensionsverschiebung entstehen aus kohomologisch trivialen Moduln aber wieder kohomologisch triviale Moduln. Also gilt die Aussage für alle q.
QED.

5.2.7 Galois-Kohomologie II: Hilberts Satz 90

5.2.7.1 Die Situation

Wie in 5.8.11.1 seien E/F eine Galoiserweiterung und G = Gal(E/F) deren Galoisgruppe. Weiter sei

$$\{K_i\}_{i\in I}$$

die Familie der endlichen Galoisschen Teilerweiterungen von E/F. Wir setzen

$$U_i := \mathrm{Gal}(E/K_i).$$

Wir haben gesehen, daß E als G-Modul aus kohomologischer Sicht uninteressant ist. Vollkommen anders ist die Situation, wenn man die multiplikative Gruppe E* als G-Modul betrachtet.

Wegen $(E^*)^{U_i} = K_i^*$ und $E^* = \cup K_i^*$ ist E* ebenfalls ein diskreter G-Modul, so daß gilt

(2) $$H^q(G, E^*) = \varinjlim_i H^q(G(K_i/F), K_i^*)$$

5.2.7.2 Proposition 2.2: Hilberts Satz 90

Seien E/F eine Galoiserweiterung und G = Gal(E/F) deren Galoisgruppe. Dann gilt

$$H^1(G,E^*) = 0.$$

Dabei bezeichne $H^q(G,E)$ die proendliche Kohomologie im Sinne von 5.7.7.
Beweis.
QED.

5.2.7.3 Folgerung: klassischen Formulierung

Seien E/F eine Galois-Erweiterung mit der Eigenschaft, daß

$$G = G(E/F)$$

eine endliche zyklische Gruppe ist mit dem Erzeuger

$$g\in G$$

und

$$a\in E^*$$

ein Element mit

$$N_{E/F}(a) = 1.$$

Dann gibt es ein Element $b\in E^*$ mit

$$a = b/g(b).$$

Beweis. Weil die Gruppe G zyklisch ist, gilt für jeden diskreten G-Modul (vgl. 4.8.4)

(1) $$H^1(G, A) = {}_NA/(1-g)A.$$

Dabei seien N die Summe der Elemente von G und ${}_NA$ der Kern der Multiplikation mit N. Sei jetzt

$$A = E^*.$$

Dann ist (1-g)A (in multiplikativer Schreibweise) gleich

(2) $$\{ \frac{b}{g(b)} \mid b \in E^*\}$$

und es gilt

(3) $${}_NA = \{ a\in E^* \mid 1 = N(a) = \prod_{x\in G} x(a) = N_{E/F}(a) \}.$$

Nach 5.2.7.2 ist die Gruppe (1) trivial für A = E*, d.h. jedes Element der Menge (3) liegt in der Menge (2).

QED.

5.2.8 Galois-Kohomologie III: Brauer-Gruppen

5.2.8.1 Konstruktion

Seien

$$E_1 \text{ und } E_2$$

zwei Galois-Erweiterungen des Körpers F und sei

$$G_i = G(E_i/F) \quad (i = 1,2)$$

deren Galois-Gruppe. Weiter sei

$$j: E_1 \to E_2$$

eine Einbettung über F.
Dann ist $j(E_1)$ eine Galois-Erweiterung von F und die Einschränkung auf $j(E_1)$ definiert einen Gruppen-Homomorphismus

$$G_2 \to G_1.$$

Sei

$$U := G(E_2/j(E_1))$$

und bezeichne j* die Komposition

$$H^q(G_1, E_1) \cong H^q(G_2/U, E_2^{*U}) \xrightarrow{\text{Inf}} H^q(G_2, E_2)$$

5.2.8.2 Unabhängigkeit von j von der Wahl der Einbettung j*

Der in 5.8.13.2 konstruierte Homomorphismus j* hängt nicht von der speziellen Wahl der Einbettung j ab.
Beweis. Sei $j': E_1 \to E_2$ eine zweite Einbettung über F. Weil E_1/F als Galois-Erweiterung normal ist, gilt

$$j(E_1) = j'(E_1),$$

d.h. es eine Element $g \in G_1$ mit

$$j' = j \circ g.$$

also

$$j'^* = j^* \circ g^*.$$

Der zum Isomorphismus $g: E_1 \to E_1$ gehörige Homomorphismus $\bar{g}$ ist gerade der innere Automorphismus

$$\bar{g}: G_1 \to G_1 , x \mapsto g^{-1}xg.$$

Nach 4.4.7 ist der zugehörige Isomorphismus

$$g^*: H^q(G_1, E_1) \to H^q(G_1, E_1)$$

die identische Abbildung.
QED.

5.2.8.3 Die Kohomologie mit Werten in der separablen Abschließung

Seien F ein Körper und E' und E" zwei separabel Abschließungen von F. Dann gibt es stets einen F-Isomorphismus

$$E' \to E"$$

und je zwei solche Isomorphismen liefern (nach 5.8.13.2) ein und denselben Isomorphismus

$$H^q(G(E'/F), E'^*) \to H^q(G(E''/F, E''^*).$$

Aus kohomologischer Sicht ist es deshalb gleichgültig, welche separable Abschließung des Körpers F man wählt. Wir werden deshalb schreiben

$$H^q(F) := H^q(G(E/F), E^*),$$

wobei E irgendeine separable Abschließung von F bezeichnet.

5.2.8.4 Definition: Brauer-Gruppe eines Körpers

Sei F ein Körper. Dann heißt

$$Br(F) := H^2(F)$$

Brauer-Gruppe von F.

5.2.8.5 Theorem 2.1: Eine kurze halb-exakte Sequenz

Sei

$$F \subseteq K \subseteq E$$

ein Körperturm mit

K/F und E/F Galois-Erweiterungen.

Dann besteht eine exakte Sequenz

$$0 \to H^2(G(K/F), K^*) \to H^2(G(E/F), E^*) \to H^2(G(E/K), E^*).$$

Wir stellen dem Beweis zwei Folgerungen voran.

5.2.8.6 Folgerung 1

Seien F ein Körper und K/F eine Galois-Erweiterung. Dann ist die Sequenz

$$0 \to H^2(G(K/F), K^*) \to H^2(F) \to H^2(K)$$

exakt.

Beweis.

QED.

5.2.8.7 Folgerung 2

Seien F ein Körper und $(K_i)_{i\in I}$ die Familie der Galois-Erweiterungen von F in einer festen separablen Abschließung von F. Dann gilt

$$H^2(F) = \cup_{i\in I} H^2(G(K_i/F), K_i^*).$$

Beweis.

QED.

Zum Beweis des obigen Theorems 5.2.8.5 benötigen wir die folgende Proposition:

5.2.8.8 Proposition 2.3

Seien G eine proendliche Gruppe,

$$H \subseteq G$$

ein abgeschlossener Normalteiler und

M

ein diskreter G-Modul mit

$$H^1(H, M) = 0.$$

Dann ist die folgende Sequenz exakt.

$$0 \to H^2(G/H, M^H) \xrightarrow{Inf} H^2(G, M) \xrightarrow{Res} H^2(H, M).$$

Dabei werden die Inflation und die Restriktion im Falle proendlicher Gruppen in derselben Weise definiert wie für abstrakte Gruppen.

Beweis. Sei $(U_i)_{i\in I}$ die Familie der offenen Normalteiler von G. Die Bedingung

$$H^1(H, M) = 0.$$

bedeutet dann, es gilt[129]

$$H^1(HU_i/U_i, M^{U_i}) = 0.$$

Deshalb ist für jedes i die folgende Sequenz exakt,

$$0 \to H^2(G/HU_i, M^{HU_i}) \xrightarrow{Inf} H^2(G/U_i, M^{U_i}) \xrightarrow{Res} H^2(HU_i/U_i, M^{U_i}).$$

(vgl. 4.5.2). Für verschiedene i, sagen wir i' und i", mit i' ≤ i" bilden diese Sequenzen kommutative Diagramme mit exakten Zeilen. Die Gesamtheit dieser Diagramme bildet ein induktives System von exakten Sequenzen. Die Behauptung ergibt sich damit durch Übergang zum direkten Limes zusammen mit den folgenden Tatsachen.

1. $\varinjlim$ ist ein exakter Funktor auf der Kategorie der induktiven Systeme über einer fixierten Index-Menge (vgl. [5]).
2. $\varprojlim_i H/H\cap U_i \cong H$ und $\varprojlim_i G/HU_i \cong G/H$

(vgl. die Folgerungen 5.1.4.8 und 5.1.4.8 aus Theorem 5.1.4.7).
Man kann die Behauptung der Proposition auch direkt beweisen fast auf dieselbe Weise wie man im abstrakten Fall.
QED.

5.2.8.9 Beweis von Theorem 5.2.8.5

Wir formulieren den Satz zunächst um und übersetzen ihn in die Sprache der abstrakten proendlichen Gruppen. Seien

G := G(E/F)
H := G(E/K)
M := E*.

Dann gilt nach dem Hauptsatz der Galois-Theorie

$$G/H = G(K/F) \text{ und } M^H = K^*.$$

Die Abbildung

$$H^2(G, M) \to H^2(H, M)$$

ist die Restriktion und die Abbildung

$$H^2(G/H, M^H) \to H^2(G, M)$$

die Inflation. Die Behauptung folgt damit aus der Proposition 5.2.8.8.

Literatur zu Kapitel 5

[1] Bourbaki, N.: Algèbre, Hermann, Paris 1950
[2] Montgomery, D., Zippin, L.: Topological transformation groups, Interscience, New York - London 1955
[3] Serre, J.-P.: Cohomologie Galoisienne, Springer-Verlag, Berlin 1965
[4] Serre, J.-P.: Corps locaux, Hermann, Paris 1962
[5] Steenrod, N., Eilenberg, S.: Foundations of algebraic topology, Princeton Univ. Press, Princeton 1952

[129] Die Inflation bildet diese Gruppen injektiv in $H^1(H, M)$ ab, vgl. 4.5.1.

6. Lokale Klassenkörper-Theorie (J.-P. *Serre)*

6.0 Einleitung

6.0.1 Vereinbarungen und Bezeichnungen

Einen Körper

$$K$$

wollen wir lokal nennen, wenn er vollständig ist bezüglich der Topologie einer diskreten Bewertung

$$v: K^* \to \mathbb{Z}$$

und sein Restklassenkörper endlich ist. Seien

$$k$$

der zugehörige Restklassenkörper und

$$q := p^f = \#(k)$$

die Anzahl der Elemente von k.
Im gesamten Kapitel werden wir die folgenden Bezeichnungen beibehalten.

$\mathcal{O}_K$ Ring der ganzen Zahlen des Körpers K
K^* multiplikative Gruppe des Körpers K
U_K Gruppe der Einheiten von $\mathcal{O}_K$

Die analogen Bezeichnungen verwenden wir auch für die Erweiterungskörper L von K. Ist L/K eine Galois-Erweiterung, so bezeichne

$$G_{L/K} = G(L/K)$$

die Galois-Gruppe der Erweiterung. Ist $s \in G(L/K)$ und $\alpha \in L$ so verwenden wir auch die Exponentialschreibweise

$$^s\alpha := s(\alpha).$$

Eine Beschreibung aller fehlenden Einzelheiten kann der Leser in den vorangehenden Kapiteln oder auch im Buch [8] finden.

Wir werden stets annehmen, alle diskreten Bewertungen

$$v: K^* \to \mathbb{Z}$$

sind normalisiert (d.h. surjektive Abbildungen).

Bemerkungen

(i) Ist K ein lokaler Körper der Charakteristik 0, so handelt es sich um eine endliche Erweiterung des Körpers

$$\mathbb{Q}_p$$

der p-adischen Zahlen, d.h. der Vervollständigung von $\mathbb{Q}$ der rationalen Zahlen bezüglich der p-adischen Bewertung. Ist

$$[K. \mathbb{Q}_p] = n,$$

so gilt

$$n = ef,$$

wobei

$$f = [k : \mathbb{F}_p]$$

der Grad des Restklassenkörpers von K ist und

$$e = v(p)$$

der Verzweigungsindex von K über $\mathbb{Q}_p$.

(ii) Ist der lokale Körper K von der Charakteristik $p > 0$ (Fall gleicher Charakteristik), so ist

$$K = k((T))$$

der Körper der formalen Laurent-Reihen, wobei T ein uniformisierender Parameter ist.

(iii) Der erste Fall ist genau derjenige, der beim Vervollständigen eines Zahlkörpers bezüglich einer Primzahl auftritt.

Beweise. Zu (ii). Sei $\mathcal{O}$ der Bewertungsring von K,

$$\mathcal{O} := \{x \in K \mid v(x) \geq 0\}.$$

Dabei bezeichne v die Bewertung von K. Mit K ist dann auch $\mathcal{O}$ vollständig, d.h. $\mathcal{O}$ ist ein vollständiger diskreter Bewertungsring und damit insbesondere ein regulärer Ring von der Dimension 1. Als vollständiger lokaler Ring ist $\mathcal{O}$ Faktorring eines Potenzreihenrings über einem Cohen-Ring C,

$$\mathcal{O} = C[[T_1, \ldots, T_r]]/I.$$

Nach Voraussetzung hat K die Charakteristik $p > 0$, d.h. es ist $p \cdot \mathcal{O} = 0$, d.h. $p \in I$. Wir können C durch C/pC ersetzen und erhalten

$$\mathcal{O} = k[[T_1, \ldots, T_r]]/I .$$

Dabei ist $k = C/pC$ der Restklassenkörper von K. Als diskreter Bewertungsring ist $\mathcal{O}$ von der Dimension 1, d.h. das maximale Ideal

$$m \subseteq \mathcal{O}$$

wird von einem Element erzeugt und damit von der Restklasse eines T_i, sagen wir von

$$T = T_1.$$

Wir bezeichnen die Restklasse von T bzw. T_i in $\mathcal{O}$ mit t bzw. t_i. Da t das maximale Ideal erzeugt, ist jedes t_i ein Vielfaches von t,

$$T_i - T \cdot F \in I \text{ mit } F \in k[[T_1, \ldots, T_r]].$$

Das bedeutet, T_r läßt sich (falls $r > 1$ ist) modulo I durch eine Potenzreihe in $T_1, \ldots, T_{r-1}$ ausdrücken, d.h. $\mathcal{O}$ ist Faktorring von $k[[T_1, \ldots, T_{r-1}]]$. Indem wir diesen Schluß wiederholen, sehen wir, $\mathcal{O}$ ist Faktorring von k[[T]]. Aus Dimensionsgründen folgt

$$\mathcal{O} = k[[T]].$$

Durch Übergang zum Quotientenkörper erhalten wir die Behauptung,

$$K = Q(\mathcal{O}) = Q(k[[T]]) = k((T)).$$

Zu (i). Dieselben Schlüsse wie oben liefern

$$\mathcal{O} = C[[T]]/I$$

mit einem Cohenring C und eine Unbestimmten T. Wird das maximale Ideal von $\mathcal{O}$ vom Erzeuger, sagen wir $p \in \mathbb{N}$, des Cohenrings erzeugt, so erhalten wir sogar

$$\mathcal{O} = C.$$

Andernfalls ist die Restklasse t von T Erzeuger des maximalen Ideals m von $\mathcal{O}$, und es gilt

$$p = u \cdot t^e$$

mit einer Einheit u von $\mathcal{O}$. Wir erhalten

$$\mathcal{O} =^{130} C[[T]]/(p - F \cdot T^e)$$

mit einer Potenzreihe F vom Anfangsgrad 0 von C[[T]]. Da F eine Einheit im Potenzreihenring C[[T]] ist, können wir damit $\mathcal{O}$ auch in der Gestalt

$$\mathcal{O} = C[T]/(T^e - G \cdot p)$$

schreiben mit einer Einheit mit $G \in C[T]$, d.h. $G \in C^*$. Wir haben gezeigt: K ist endliche algebraische Erweiterung des Quotientenkörpers Q(C) eines Cohenrings. Zum Beweis der Behauptung reicht es zu zeigen, Q(C) ist endliche algebraische Erweiterung von $\mathbb{Q}_p$. Weil C ein Cohenring ist, ist Q(C) unverzweigt. Insbesondere ist

---

[130] Zumindest ist $\mathcal{O}$ ein Faktorring eines Rings von der Gestalt des Rings rechts. Letzterer ist aber regulär von der Dimension 1. Aus Dimensionsgründen muß deshalb "=" gelten.

$$[Q(C): \mathbb{Q}_p] = [C/pC, \mathbb{F}_p] < \infty.$$

QED.

6.0.2 Gegenstand des Kapitels

Unser Ziel ist die Untersuchung der Galois-Gruppen der Erweiterungen des Körpers K. Natürlich wäre es wünschenswert, die Struktur der Galois-Gruppe

$$G(K_s/K)$$

der separablen Abschließung K_s von K zu beschreiben, da diese alle Informationen über diese Erweiterungen enthält (Im Fall der Charakteristik 0 ist $K_s = \overline{K}$ gleich der algebraischen Abschließung). Wir beschränken uns jedoch auf folgendes:

1. Beschreibung der kohomologischen Eigenschaften aller Galois-Erweiterungen, sowohl der abelschen als auch der nicht-abelschen.

2.Bestimmung der abelschen Erweiterungen des Körpers K, d.h. Bestimmung der Gruppe $G(K_s/K)$ modulo der Kommutator-Untergruppe.

6.1 Die Brauer-Gruppe eines lokalen Körpers

6.1.1 Formulierung der Sätze

In diesem Abschnitt formulieren wir die Hauptergebnisse von 6.1, die dann in 6.1.2-6.1.6 bewiesen werden. Wir beginnen mit der Defintion der Brauer-Gruppe (siehe auch 5.2.8)..

6.1.1.1 Definition: Brauer-Gruppe eines lokalen Körpers

Seien K ein lokaler Körper und

$$L/K$$

eine endliche Galois-Erweiterung von K mit der Gruppe G(L/K). Abkürzung:

$$H^2(L/K) := H^2(G_{L/K}, L^*).$$

Sei

$$(L_i)_{i\in I}$$

die Familie aller endlichen Galois-Erweiterungen des Körpers K. Dann heißt der induktive Limes

$$Br(K) := \varinjlim_{i\in I} H^2(L_i/K)$$

auch Brauer-Gruppe des lokalen Körpers K.

Bemerkungen

(i) Nach Defintion ist

$$Br(K) = H^2(K_s/K).$$

(ii) Zur Berechnung der Brauer-Gruppe zerlegen wir die Erweiterung K_s/K in Teilerweiterungen

$$K \subset K_{nr} \subset K_s .$$

Dabei bezeichne K_{nr} die maximale unverzweigte Erweiterung von K. Mit den Eigenschaften von K_{nr} kann sich der Leser in 1.7 bekannt machen. Wir erinnern hier nur daran, es gilt

$$G(K_{nr}/K) = G(\overline{k}/k).$$

(iii) Wir bezeichnen mit

$$F: K_{nr} \to K_{nr}$$

die Frobenius-Abbildung der Gruppe $G(K_{nr}/K)$. Die Operation von F auf $\overline{k}$ ist die folgende.[131]

$$F: \overline{k} \to \overline{k},\ x \mapsto x^q.$$

(iv) Die Abbildung

$$\hat{\mathbb{Z}} \to G(K_{nr}/K),\ n \mapsto F^n,$$

ist ein Isomorphismus topologischer Gruppen. Aus 5.2.5 wissen wir, die Gruppe

$$\hat{\mathbb{Z}} = \varprojlim_{n \in \mathbb{N}} \mathbb{Z}/n\mathbb{Z}$$

ist gerade der projektive Limes von zyklischen Gruppen.

(v) Da K_{nr} enthalten ist in K_s, liegt die Gruppe $H^2(K_{nr}/K)$ in $H^2(K_s/K)$.[132] Tatsächlich gilt sogar mehr:

6.1.1.2 Theorem 1.1: $H^2(K_{nr}/K)$ ist die Brauer-Gruppe

Sei K ein lokaler Körper. Dann besteht eine natürliche Isomorphie

$$H^2(K_{nr}/K) \cong Br(K).$$

6.1.1.3 Theorem 1.2: Berechnung von $H^2(K_{nr}/K)$

Seien K ein lokaler Körper und

$$v: K_{nr}^* \to \mathbb{Z}$$

die Bewertung der maximalen unverzweigten Erweiterung von K. Dann definiert v einen Isomorphismus

$$H^2(K_{nr}/K) \to H^2(\hat{\mathbb{Z}}, \mathbb{Z}).$$

6.1.1.4 Konstruktion: die Invariante eines Elements der Brauer-Gruppe

Sei G irgendeine proendliche Gruppe. Wir betrachten die exakte Sequenz

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

als Sequenz von G-Moduln, wobei die Gruppe G trivial operiere. Der Modul $\mathbb{Q}$ hat triviale Kohomologie, da er eindeutig teilbar ist (d.h. er ist $\mathbb{Z}$-injektiv)[133]. Deshalb ist der Zusammenhangshomomorphismus

---

[131] $q = p^f$ ist nach Vereinbarung die Anzahl der Elemente des Restklassen körpers k.

[132] Auf Grund der exakten Sequenz von 5.2.8.5.

[133] Da G proendlich ist, können wir die Aussage leicht auf den Fall endlicher Gruppen reduzieren. Sei also

G endlich.

Seien M' ein G-Modul, $M \subseteq M'$ ein G-Teilmodul und

$$\alpha: M \to \mathbb{Q}$$

eine G-invariante $\mathbb{Z}$-lineare Abbildung. Wir haben zu zeigen, α läßt sich fortsetzen zu einer $\mathbb{Z}$-linearen G-invarianten Abbildung

$$M' \to \mathbb{Q}.$$

Da $\mathbb{Q}$ als $\mathbb{Z}$-Modul injektiv ist, gibt es zumindest eine $\mathbb{Z}$-lineare Fortsetzung

$$\delta: H^1(G, \mathbb{Q}/\mathbb{Z}) \to H^2(G, \mathbb{Z})$$

ein Isomorphismus. Weil G trivial auf $\mathbb{Q}/\mathbb{Z}$ operiert, gilt

$$H^1(G, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$$

(vgl. 4.2.4), also

$$H^2(G, \mathbb{Z}) = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}).$$

Wenden wir uns jetzt der Gruppe $\mathrm{Hom}(\hat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z})$ zu. Die Abbildung[134]

$$\gamma: \mathrm{Hom}(\hat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) \to \mathbb{Q}/\mathbb{Z}, \ \phi \mapsto \phi(1),$$

ist ein Isomorphismus.[135] Nach Theorem 6.1.1.3 bestehen daher Isomorphien

$$\mathrm{inv}_K: H^2(K_{nr}/K) \xrightarrow[\cong]{v} H^2(\hat{\mathbb{Z}}, \mathbb{Z}) \xrightarrow[\cong]{\delta^{-1}} \mathrm{Hom}(\hat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) \xrightarrow[\cong]{\gamma} \mathbb{Q}/\mathbb{Z}.$$

Der Wert der Abbildung inv_K im Element $\alpha \in H^2(K_{nr}/K)$ heißt Invariante von α.

6.1.1.5 Folgerung: Bijektivität von inv_K

Für jeden lokalen Körper K ist die oben konstruierte Abbildung

$$\mathrm{inv}_K: H^2(K_{nr}/K) \to \mathbb{Q}/\mathbb{Z}$$

ein Isomorphismus von Gruppen.

Bemerkungen

(i) Nach 6.1.1.2 ist $H^2(K_{nr}/K)$ die Brauer-Gruppe von K, d.h. inv_K ist ein Isomorphismus

$$\mathrm{inv}_K: \mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}.$$

(ii) Für jede endliche Erweiterung L des Körpers K bezeichnen wir mit

$$\mathrm{inv}_L: \mathrm{Br}(L) \to \mathbb{Q}/\mathbb{Z}.$$

die analog definierte Abbildung.

$$\beta: M' \to \mathbb{Q}.$$

Wir setzen

$$\tilde{\alpha}(m') := \frac{1}{\#G} \sum_{g \in G} \beta(gm') \text{ für } m' \in M'.$$

Dann ist $\tilde{\alpha}$ eine G-invariante Fortsetzen von α auf M'.
Auf dieselbe Weise zeigt man, jeder über $\mathbb{Z}$ injektive Modul M, auf dem G trivial operiert und der eindeutig teilbar ist (d.h. Multiplikation mit $n \in \mathbb{N}$ induziert einen Isomorphismus $M \to M$ für jedes n), ist injektiv als G-Modul.

[134] $1 \in \hat{\mathbb{Z}}$ ist der natürliche Erzeuger, der von den natürlichen Bildern von $1 \in \mathbb{Z}$ in den $\mathbb{Z}/n\mathbb{Z}$ kommt.

[135] Die Abbildung ist injektiv: Jedes Element von $\mathbb{Q}/\mathbb{Z}$ hat eine endliche Ordnung. Deshalb ist jedes Element $\phi \in \mathrm{Hom}(\hat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z})$ automatisch stetig (bezüglich der diskreten Topologie von $\mathbb{Q}/\mathbb{Z}$). Deshalb ist ϕ durch den Wert $\phi(1)$ bereits eindeutig festgelegt (die Vielfachen von 1 liegen dicht in $\hat{\mathbb{Z}}$).
Die Abbildung ist surjektiv: Sei $r \in \mathbb{Q}/\mathbb{Z}$ vorgegeben. Dann gibt es eine natürliche Zahl mit $n \cdot r = 0$. Indem wir n minimal wählen, erreichen wir $\mathbb{Z} \cdot r \cong \mathbb{Z}/n\mathbb{Z}$. Die Zusammensetzung

$$\hat{\mathbb{Z}} \to \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z} \cdot r \subseteq \mathbb{Q}/\mathbb{Z}$$

ist ein Element $\phi \in \mathrm{Hom}(\hat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z})$ mit $\phi(1) = r$.

6.1.1.6 Theorem 1.3: Verhalten der Brauer-Gruppe bei Erweiterungen

Seien K ein lokaler Körper und L/K eine endliche Körpererweiterung des Grades n. Dann ist das folgende Diagramm kommutativ.

$$\begin{array}{ccc} Br(K) & \xrightarrow{Res_{L/K}} & Br(L) \\ inv_K\downarrow & & \downarrow inv_L \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{n} & \mathbb{Q}/\mathbb{Z} \end{array}$$

Dabei bezeichne der untere horizontale Pfeil die Multiplikation mit n. Die Abbildung $Res_{L/K}$ wurde in 4.4.3 und in 5.2.8.8 definiert.

6.1.1.7 Folgerung 1: der Kern der Restriktion auf der Brauer-Gruppe

Seien K ein lokaler Körper und L/K eine endliche Körpererweiterung des Grades n. Dann gilt

$$\text{Ker } (Res_{L/K}: Br(K) \to Br(L)) = \{ \alpha \in Br(K) \mid n \cdot \alpha = 0 \}$$

6.1.1.8 Folgerung 2: ein Erzeuger von $H^2(L/K)$

Seien K ein lokaler Körper und L/K eine endliche Körpererweiterung des Grades n. Dann ist die Gruppe $H^2(L/K)$ zyklisch von der Ordnung n. Genauer: die Gruppe

$$H^2(L/K)$$

wird erzeugt vom Element

$$u_{L/K} \in Br(K)$$

mit der Invarianten $\frac{1}{n} \in \mathbb{Q}/\mathbb{Z}$.

6.1.2 Berechnung der Gruppe $H^2(K_{nr}/K)$

6.1.2.1 Vorbemerkung

In diesem Abschnitt beweisen wir 6.1.1.3 Theorem 1.2, d.h. wir beweisen, daß der durch die Bewertung definierte Homomorphismus

$$H^2(K_{nr}/K) \to H^2(\hat{\mathbb{Z}}, \mathbb{Z}).$$

ein Isomorphismus ist.

6.1.2.2 Proposition 1.1:

Seien K ein lokaler Körper, K_n/K eine unverzweigte Erweiterung des Grades n und

$$G := G(K_n/K).$$

Dann gilt für jedes $q \in \mathbb{Z}$

(i) $H^q(G, U_n) = 0$ mit $U_n := \mathcal{O}^*_{K_n}$.

(ii) Die durch die Bewertung $v: K_n^* \to \mathbb{Z}$ induzierte Abbildung

$$H^q(G, K_n^*) \to H^q(G, \mathbb{Z})$$

induzierte Abbildung ist ein Isomorphismus.

Bemerkung

6.1.1.3 Theorem 1.2 ist eine offensichtliche Folgerung von Aussage (ii) dieser Proposition, denn $H^2(K_{nr}/K) = H^2(\hat{\mathbb{Z}}, K_{nr}^*)$.

Beweis. Betrachten wir die kurze exakte Sequenz von G_n-Moduln

$$0 \to U_n \to K_n^* \xrightarrow{v} \mathbb{Z} \to 0$$

und die zugehörige lange Kohomologie-Sequenz

$$H^q(G, U_n) \to H^q(G, K_n^*) \to H^q(G, \mathbb{Z}) \to H^{q+1}(G, U_n).$$

Wir lesen aus dieser Sequenz ab, daß Aussage (ii) aus (i) folgt. Es reicht also, (i) zu beweisen. Zum Beweis von (i) betrachten wir die folgende Kette von offenen Untergruppen:

$$U_n \supset U_n^1 \supset U_n^2 \supset ...$$

mit

$$U_n^i := \{x \in U_n \mid v(x-1) \geq i\}.$$

Sei

$$\pi \in K_n$$

ein uniformisierender Parameter. Dann gilt

$$U_n^i = 1 + \pi^i \mathcal{O}_n \text{ mit } \mathcal{O}_n := \mathcal{O}_{K_n}.$$

und

$$U_n = \varprojlim_i U_n/U_n^i.$$

Die Behauptung der Proposition folgt jetzt aus den nachfolgenden drei Lemmata.
QED.

6.1.2.3 Lemma 1.1

Sei k_n der Restklassenkörper von K_n. Dann gibt es mit der Operation der Galois-Gruppe verträgliche Isomorphismen

$$U_n/U_n^1 \cong k_n^* \text{ und } U_n^i/U_n^{i+1} \cong k_n^+ \ (i = 1, 2, 3, ...).$$

Bemerkung
Mit der Galois-Gruppen-Operation verträgliche Isomorphismen heißen auch Galois-Isomorphismen.
Beweis.
QED.

6.1.2.4 Lemma 1.2

Für jede ganze Zahl q und jedes ganze $i \geq 0$ gilt

$$H^q(G, U_n^i/U_n^{i+1}) = 0.$$

Beweis.
QED.

6.1.2.5 Lemma 1.3

Seien G eine endliche Gruppe und M ein G-Modul. Weiter sei

$$\{M^i\}_{i=0,2,...}$$

eine absteigende Folge von Teilmoduln von M mit $M^0 = M$ und

$$M \cong \varprojlim_i M/M^i$$

(genauer: die natürliche Abbildung von M in den inversen Limes sei bijektiv). Dann gilt (für ein fest vorgegebenes q)

$$H^q(G, M) = 0,$$

falls $H^q(G, M^i/M^{i+1}) = 0$ ist für jedes i.
Beweis.
QED.

6.1.3 Einige Diagramme

6.1.3.1 Proposition 1.2

Seien K ein lokaler Körper und

$$L/K$$

eine endliche Körpererweiterung vom Grad n und

$$L_{nr} \text{ und } K_{nr}$$

maximale Unverzweigte Erweiterungen von L bzw. K mit

$$K_{nr} \subseteq L_{nr}.$$

Dann ist das folgende Diagramm kommutativ.

$$\begin{array}{ccc} H^2(K_{nr}/K) & \xrightarrow{\text{Res}} & H^2(L_{nr}/L) \\ \text{inv}_K \downarrow & & \text{inv}_L \downarrow \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{n} & \mathbb{Q}/\mathbb{Z} \end{array}$$

Beweis. Sei

$$\Gamma_K := G(K_{nr}/K)$$

und bezeichne

$$F_K$$

das Frobenius-Element der Gruppe Γ_K. Analog definieren wir Γ_L und F_L. Es gilt

$$F_L = (F_K)^f,$$

wenn

$$f := [k_L : k_K]$$

der Grad der Erweiterung der Restklassenkörper zur Erweiterung L/K bezeichnet.[136] Sei

---

[136] Wenn der Körper k_K den Grad m über seinem Primkörper besitzt, also aus p^n Elementen Besteht, so besteht k_K aus den Nullstellen der Gleichung $X^{p^n} - X = 0$, d.h. aus den Elementen, die bei der Abbildung

(1) $$f_K : X \text{ a } X^{p^n}$$

invariant bleiben. Analog besteht k_L aus p^{nf} Element, d.h. k_L ist der Fixkörper von

(2) $$f_L : X \text{ a } X^{p^{nf}}.$$

Die Abbildungen (1) und (2) sind gerade topologische Erzeuger der Gruppen $G(\overline{k}/k_K)$ bzw. $G(\overline{k}/k_L)$, wenn $\overline{k}$ die gemeinsame algebraische Abschließung von k_K und k_L bezeichnet. Bei den Identifikationen

$$G(\overline{k}/k_K) = G(K_{nr}/K) \text{ und } G(\overline{k}/k_L) = G(L_{nr}/L)$$

entsprechen sie gerade den Frobenius-Elementen der Gruppen rechts. Wegen $f_L = (f_K)^f$ ist damit auch $F_L = (F_K)^f$.

$$e = e(L/K)$$

der Verzweigungsindex von L über K. Wir betrachten das folgende Diagramm.

$$\begin{array}{ccccccc} H^2(\Gamma_K, K_{nr}^*) & \xrightarrow{v_K} & H^2(\Gamma_K, \mathbb{Z}) & \xrightarrow{\delta^{-1}} & \mathrm{Hom}(\Gamma_K, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\gamma_K} & \mathbb{Q}/\mathbb{Z} \\ \mathrm{Res}\downarrow & (1) & e\cdot\mathrm{Res}\downarrow & (2) & e\cdot\mathrm{Res}\downarrow & (3) & n\downarrow \\ H^2(\Gamma_L, L_{nr}^*) & \xrightarrow{v_L} & H^2(\Gamma_L, \mathbb{Z}) & \xrightarrow{\delta^{-1}} & \mathrm{Hom}(\Gamma_L, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{v_L} & \mathbb{Q}/\mathbb{Z} \end{array}$$

Der Homomorphismus Res werde durch die natürliche Einbettung

$$\Gamma_L \hookrightarrow \Gamma_K$$

induziert.[137] Die Homomorphismen γ_K und γ_L seien durch die Abbildungsvorschriften

$$\varphi \mapsto \varphi(F_K) \text{ bzw. } \varphi \mapsto \varphi(F_L)$$

gegeben.[138] Die drei Quadrate (1), (2) und (3), in welche das Diagramm zerfällt, sind kommutativ: für das Quadrat (1) ergibt sich das aus der Tatsache, daß die Einschränkung von v_L auf K_{nr}^* gerade $e\cdot v_K$ ist,

$$\begin{array}{ccc} K_{nr}^* & \xrightarrow{v_K} & \mathbb{Z} \\ \cap & & e\downarrow \\ L_{nr}^* & \xrightarrow{v_L} & \mathbb{Z} \end{array}$$

(nach Definition des Verzweigungsindex e). Für das Quadrat (3) ergibt sich die Kommutativität aus den Relationen

$$F_L = (F_K)^f \text{ und } e\cdot f = n.$$

Die Kommutativität des Quadrats (2) ergibt sich aus der Funktorialistät des Zusammenhangshomomorphismus. Die beiden Zeilen des Diagramms sind aber gerade inv_K bzw. inv_L (vgl. Definition 6.1.1.4 - man identifiziert Γ_K und Γ_L mit $\hat{\mathbb{Z}}$ indem man den topologischen Erzeuger von $\hat{\mathbb{Z}}$ mit F_K bzw. F_L identifiziert). Das obige Diagramm ist also gerade das Diagramm der Behauptung.
QED.

6.1.3.2 Folgerung 1

Seien K ein lokaler Körper, L/K eine Körpererweiterung vom Grad n und bezeichne

$$H^2(L/K)_{nr} \subseteq H^2(K_{nr}/K)$$

die Untergruppe der über L zerfallenden Elemente, d.h. der Elemente aus dem Kern der Abbildung

$$H^2(K_{nr}/K) \xrightarrow{\mathrm{Res}} H^2(L_{nr}/L).$$

Dann ist

$$H^2(L/K)_{nr}$$

zyklisch von der Ordnung n und wird vom Element

$$u_{L/K} \in H^2(K_{nr}/K)$$

mit der Invarianten

---

[137] $\Gamma_L = G(L_{nr}/L) = G(\bar{k}/k_L) \subseteq G(\bar{k}/k_K) = G(K_{nr}/K) = \Gamma_K$

[138] F_K und F_L sind topologische Erzeuger der Gruppen Γ_K bzw. Γ_L.

$$\mathrm{inv}_k(u_{L/K}) = \frac{1}{n}$$

erzeugt.
Beweis. Wegen des kommutativen Diagramms

$$\begin{array}{ccc} H^2(K_{nr}/K) & \xrightarrow{\mathrm{Res}} & H^2(L_{nr}/L) \\ {\scriptstyle \mathrm{inv}_K}\downarrow & & {\scriptstyle \mathrm{inv}_L}\downarrow \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{n} & \mathbb{Q}/\mathbb{Z} \end{array}$$

von 6.1.3.1 , denn vertikale Abbildungen Isomorphismen sind (vgl. 6.1.1.5), wird der Kern von Res durch die linke vertikale Abbildung mit

$$\frac{1}{n}\mathbb{Z}/\mathbb{Z}$$

identifiziert.
QED.

6.1.3.3 Alternative Definition der zerfallenden Elemente

Seien K ein lokaler Körper und L/K eine endliche Körpererweiterung. Ist L/K eine Galois-Erweiterung, dann gilt für die in 6.1.3.2 definierte Gruppe der zerfallenden Elemente

$$H^2(L/K)_{nr} = H^2(K_{nr}/K) \cap H^2(L/K).$$

Beweis. Nach 5.2.8.6 sind die Zeilen und Spalten des folgenden kommutativen Diagramms exakt.

$$\begin{array}{ccccccc} & & & & 0 & & 0 \\ & & & & \downarrow & & \downarrow \\ & & & & H^2(L/K) & \to & H^2(L_{nr}/K_{nr}) \\ & & & & \downarrow & & \downarrow \\ 0 & \to & H^2(K_{nr}/K) & \to & H^2(K) & \xrightarrow{\mathrm{Res}} & H^2(K_{nr}) \\ & & \downarrow & & \downarrow \mathrm{Res} & & \downarrow \mathrm{Res} \\ 0 & \to & H^2(L_{nr}/L) & \to & H^2(L) & \xrightarrow{\mathrm{Res}} & H^2(L_{nr}) \end{array}$$

Die obere horizontale und die linke vertikale Abbildung existieren auf Grund des kommutativen Vierecks rechts unten. Man erkennt, der Kern der linken vertikalen Abbildung besteht aus den Elementen des Kerns der Abbildung rechts daneben, die im Definitionsbereich $H^2(K_{nr}/K)$ liegen. Das ist aber gerade die Behauptung.

QED.

6.1.3.4 Folgerung 2

Seien K ein lokaler Körper und L/K eine endliche Galois-Erweiterung des Grades n.

Dann ist die Ordnung von $H^2(L/K)$ ein Vielfaches von n.

Beweis. Nach 6.1.3.2 enthält $H^2(L/K)$ eine Untergruppe der Ordnung n.
QED.

6.1.4 Die Struktur der Untergruppen mit trivialer Kohomologie

Literatur

[8] Serre, J.-P.: Corps loceaux, Hermann, Paris 1962
[9] Serre, J.-P.: Introduction à la théorie de Brauer, Seminaire IHES, 1963-1966
[10] Serre, J.-P.: Sur la rationalité des representations d' Artin, Ann. Math. 72 (1960), 406-420

7. Globale Klassenkörper-Theorie (J. T. *Tate)*

8. Zeta- und L-Funktionen (H. Heilbronn)

Anhänge & Ergänzungen

Der Satz von der Normalbasis

1. Normalbasen

Sei K/k eine Galoiserweiterung. Eine k-Vektorraumbasis von K über k heißt Normalbasis von K/k, wenn je zwei Elemente dieser Basis zu einander konjugiert sind.

2. Lineare Unabhängigkeit der Automorphismen

Seien K/k eine endliche Galoiserweiterung des Grades n mit der Galoisgruppe G und

$$\sigma_1,...,\sigma_n \in G$$

paarweise verschiedenen Automorphismen. Dann sind die σ_i linear unabhängig über K.

Beweis. Angenommen, die σ_i sind K-linear abhängig. OBdA können wir annehmen, jede echte Teilmenge von $\{\sigma_1,...,\sigma_n\}$ ist k-linear unabhängig. Nach Annahme gibt es Elemente $c_1,...,c_n \in K$ mit

(1) $$c_1\sigma_1 + c_2\sigma_2 +... + c_n\sigma_n = 0,$$

wobei die c_i nicht sämtlich gleich Null sind. Da keine Teilmenge von $\{\sigma_1,...,\sigma_n\}$ linear abhängig ist, sind dann sämliche c_i ungleich Null. Aus (1) folgt

(2) $$0 = c_1\sigma_1(x)\sigma_1(y) + c_2\sigma_2(x)\sigma_2(y) + ... + c_n\sigma_n(x)\sigma_n(y).$$

Weiter erhalten wir durch Multiplikation mit $\sigma_1(x)$ aus (1),

(3) $$0 = c_1\sigma_1(x)\sigma_1(y) + c_2\sigma_1(x)\sigma_2(y) + ... + c_n\sigma_1(x)\sigma_n(y).$$

Vergleich von (2) und (3) liefert

$$0 = c_2(\sigma_1(x)-\sigma_2(x))\sigma_2(y) + ... + c_n(\sigma_1(x)-\sigma_n(x))\sigma_n(y)$$

Da σ_1 und σ_2 verschieden sind, kann man ein $x \in K$ wählen mit

$\sigma_1(x)-\sigma_2(x) \neq 0$.

Da y beliebig ist, folgt, die Teilmenge $\{\sigma_2,...,\sigma_n\}$ ist ebenfalls linear abhängig, im Widerspruch zu unserer Annahme.
QED.

3. Nichttrivialität der Spur

Sei K/k eine endliche Galoiserweiterung des Grades n mit der Galoisgruppe

$$G = \{\sigma_1,...,\sigma_n\}.$$

Dann gibt es eine Element $c \in K-\{0\}$ mit

$$Tr(c) := \sigma_1(c)+...+\sigma_n(c) \neq 0$$

Beweis. Andernfalls wären die $\sigma_1,...,\sigma_n$ K-linear abhängig im Widerspruch zur 2. Aussage.
QED.

4. Eine von Null verschiedenen Determinante

Sei K/k eine endliche Galoiserweiterung des Grades n mit der Galoisgruppe

$$G = \{\sigma_1,...,\sigma_n\}.$$

und der k-Vektorraumbasis $\omega_1,...,\omega_n$. Dann gilt $\det(\sigma_i(\omega_j)) \neq 0$.

Beweis. Nach Aussage 2 sind die $\sigma_1,...,\sigma_n$ linear unabhängig über K. Mit anderen Worten, die Menge der Vektoren

$$s(c) := (\sigma_1(c),...,\sigma_n(c)) \in K^n$$

liegt in keinem echten linearen Unterraum von K^n. Wir können deshalb eine Folge von Elementen $c_1,...,c_n \in K$ derart wählen, daß $s(c_{i+1})$ nicht in dem von $s(c_1),...,s(c_1)$ erzeugten Teilraum liegt. Dann gilt

$$\det(\sigma_i(c_j)) \neq 0.$$

Da die ω_j den k-Vektorraum K erzeugen, können wir die c_j in der Gestalt

$$c_j = \sum_{\alpha=1}^{n} a_{j\alpha}\omega_\alpha \text{ mit } a_{j\alpha} \in k$$

schreiben. Dann gilt aber

$$\sigma_i(c_j) = \sum_{\alpha=1}^{n} a_{j\alpha}\sigma_i(\omega_\alpha)$$

also

$$0 \neq \det(\sigma_i(c_j)) = \det(a_{ij})\cdot\det(\sigma_i(\omega_j))$$

also $\det(\sigma_i(\omega_j)) \neq 0$.

QED.

5. Algebraische Unabhängigkeit der Automorphismen

Seien K/k eine endliche Galoiserweiterung des Grades n mit der Galoisgruppe

$$G = \{\sigma_1,...,\sigma_n\}$$

und $f(X_1,...,X_n) \in \Omega[X_1,...,X_n]$ ein nicht-triviales Polynom mit Koeffizienten aus einer Erweiterung von K. Ist k unendlich, so gibt es ein $c \in K$ mit $f(\sigma_1(c),...,\sigma_n(c)) \neq 0$.

Beweis. Angenommen, es gilt

(*) $$f(\sigma_1(c),...,\sigma_n(c)) = 0$$

für jedes $c \in K$. Wir wählen eine k-Vektorraumbasis $\omega_1,...,\omega_n$ von K über k. Die Elemente $c \in K$ lassen sich dann schreiben als

$$c = a_1\omega_1 + ... + a_n\omega_n \text{ mit } a_i \in k.$$

Ihre Konjugierte haben die Gestalt

$$\sigma_i(c) = a_1\sigma_i(\omega_1) + ... + a_n\sigma_i(\omega_n).$$

Betrachte wir das Polynom

$$g(Y_1,...,Y_n) := f(\sum_{j=1}^{n} \sigma_1(\omega_j)Y_j,..., \sum_{j=1}^{n} \sigma_n(\omega_j)Y_j).$$

Die Annahme (*) läßt sich dann schreiben als

$$g(a_1,...,a_n) = 0 \text{ für beliebige } (a_1,...,a_n) \in k^n.$$

Da k unendlich ist, folgt g = 0. Nach Aussage 4 ist die lineare Transformation

$$X_i = \sum_{j=1}^{n} \sigma_i(\omega_j)Y_j$$

umkehrbar. Mit g ist deshalb auch f identisch Null.

QED.

6. Normalbasenkriterium

Seien K/k eine endliche Galoiserweiterung des Grades n mit der Galoisgruppe

$$G = \{\sigma_1,...,\sigma_n\}$$

und $c \in K$ ein Element. Dann sind folgende Aussage äquivalent.

(i) $\sigma_1(c),...,\sigma_n(c)$ ist eine Normalbasis.

(ii) $\det(\sigma_i(\sigma_j(c))) \neq 0$.

Beweis. (i) $\Rightarrow$ (ii). Angenommen die Determinante ist Null. Dann sind ihre Spalten K-linear abhängig, d.h. es gibe ein $(a_1,...,a_n) \in K^n - \{o\}$ mit

(1) $$a_1\sigma_i(\sigma_1(c))+...+a_n\sigma_i(\sigma_n(c)) = 0$$

für alle i. OBdA sei $a_1 \neq 0$. Durch Multiplikation mit einem Element aus K können wir dann erreichen, daß sogar

(2) $$Tr(a_1) \neq 0$$

gilt (nach Aussage 3). Aus (1) erhalten wir durch Anwenden des Inversen von σ_i

$$\sigma_i^{-1}(a_1)\cdot\sigma_1(c)+...+\sigma_i^{-1}(a_n)\cdot\sigma_n(c) = 0.$$

Summation über alle i liefert

$$Tr(a_1)\cdot\sigma_1(c)+...+Tr(a_n)\cdot\sigma_n(c) = 0.$$

Mit anderen Worten, die $\sigma_i(c)$ sind linear abhängig über k. Sie können deshalb nicht den ganzen (n-dimensionalen) k-Vektorraum K erzeugen. Das steht aber im Widerspruch zu (i).

(ii) $\Rightarrow$ (i). Es reicht zu zeigen, die Elemente $\sigma_1(c),...,\sigma_n(c)$ sind k-linear unabhängig. Seien $a,...,a \in k$ Elemente mit

$$a_1\sigma_1(c)+...+a_n\sigma_n(c) = 0.$$

Anwenden von σ_i liefert

$$a\sigma_i(\sigma_1(c))+...+a_n\sigma_i(\sigma_n(c)) = 0.$$

Aus der Voraussetzung (ii) folgt damit aber, daß alle a_i Null sein müssen.

QED.

7. Existenz von Normalbasen über unendlichen Körpern

Seien k ein unendlicher Körper und K/k eine endliche Galoiserweiterung. Dann besitzt K/k eine Normalbasis.

Beweis. Bezeichne $p(i,j) \in \{1,...,n\}$ die Zahl mit $\sigma_i\sigma_j = \sigma_{p(i,j)}$ und sei f das Polynom

$$f(X_1,...,X_n) := \det(X_{p(i,j)}).$$

Weil $G = \{\sigma_1,...,\sigma_n\}$ eine Gruppe ist, kommt jede Unbestimmte in jeder Zeile und jeder Spalte der Determinante genau einmal vor:

$$p(i,j) = p(i,j') \Rightarrow \sigma_i\sigma_j = \sigma_i\sigma_{j'}, \Rightarrow \sigma_j = \sigma_{j'},$$
$$p(i,j) = p(i',j) \Rightarrow \sigma_i\sigma_j = \sigma_{i'}\sigma_j \Rightarrow \sigma_i = \sigma_{i'},$$

Insbesonder ist f(1,0,...,0) die Determinante einer Matrix, die aus der Einheitmatrix durch Permutieren der Spalten entsteht, d.h. $f(1,0,...,0) = \pm 1$. Das Polynom f ist deshalb nicht identisch Null. Nach Aussage 5 gibt es folglich ein $c \in K$ mit

$$\det(\sigma_i(\sigma_j(c))) = \det(\sigma_{p(i,j)}(c)) = f(\sigma_1(c),...,\sigma_n(c)) \neq 0.$$

Nach Aussage 6 bilden dann aber die Elemente $\sigma_1(c),...,\sigma_n(c)$ von K eine Normalbasis von K/k.
QED.

Index

—H—

—I—

—K—

—L—

—M—

—N—

—P—

Inhalt

4. GRUPPENKOHOMOLOGIE (M. ATIYAH, K. WALL) 147