3. Lokale Körper

3.1 Vorbemerkungen

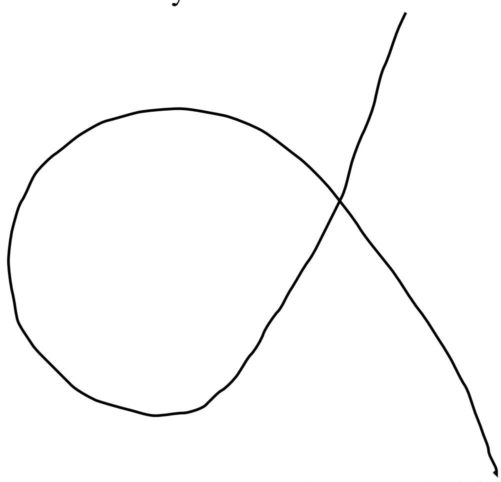
3.1.1. Lokale und globale Fragen in der Mathematik

Wie in anderen Gebieten der Mathematik kann man in der algebraischen Zahlentheorie viele Problemen unter zweierlei Gesichtspunkten untersuchen: einem lokalen und einem globalen.

Beispiel

Die Frage, ob die Kurve

$$y^2 = x^2 + x^3$$



in der Umgebung eines vorgegebenen Punktes eine Mannigfaltigkeit ist (d.h. wie ein Stück einer Geraden aussieht) ist eine lokale Frage. Zur Beantwortung genügt es, eine beliebig kleine Umgebung des gegebenen Punktes zu kennen. Genauer, es genügt die beiden partiellen Ableitungen des Polynoms $y^2 - x^2 - x^3$ in diesem Punkt zu kennen. (Antwort: die Kurve ist keine Mannigfaltigkeit im Ursprung, in allen anderen Punkten ist sie es).

Beispiel

Die Frage, ob es auf der Kugeloberfläche ein stetiges Tangentialvektorfeld ohne Nullstelle gibt, ist eine globale Frage. Selbst wenn man die Kugeloberfläche in jedem Punkt noch so genau kennt, reicht diese Kenntnis nicht aus um diese Frage zu beantworten. Man muß Eigenschaften der Kugeloberfläche untersuchen, die sich auf diese Kugeloberfläche also Ganzes beziehen. (Nach dem Satz vom Igel gibt es kein solches Vektorfeld, jedes stetige Vektorfeld auf der Kugeloberfläche besitzt Wirbel, und im Zentrum dieser Wirbel ist der Vektor gleich Null).

Die lokalen Fragen der algebraischen Zahlentheorie sind Fragen, die sich mit einer einzelnen Bewertung beschäftigen. Globale Fragen beziehen sich auf die Gesamtheit aller Bewertungen eines Körpers. Entsprechend diesen beiden Gesichtpunkten gibt es in der algebraischen Zahlentheorie die Begriffe des lokalen und des globalen Körpers.

Beispiele für globale Körper sind:

- die algebraischen Zahlenkörper, d.h. die endlichen Erweiterungen von $\mathbb{Q}$
- die rationalen Funktionenkörper k(x) in einer Unbestimmten über einem endlichen Körper k.

Man beachte, beides sind Quotientenkörper von Dedekind-Ringen mit unendlich vielen maximalen Idealen.

In der Regel muß man, um globale Fragen behandeln zu können, die lokalen Fragen hinreichend genau beantwortet haben. Deshalb wenden wir uns jetzt zunächst erst einman der Untersuchung der lokalen Körper zu.

3.1.2. Begriff des lokalen Körpers

Ein lokaler Körper ist ein diskret bewerteter Körper, welcher bezüglich dieser diskreten Bewertung vollständig ist und einen endlichen Restklassenkörper besitzt.

3.1.3 Beispiel: die p-adischen Zahlen

Seien p eine Primzahl und $\mathbb{Q}_p$ die Vervollständigung des Körpers $\mathbb{Q}$ der rationalen Zahlen bezüglich der multiplikativen p-adischen Bewertung

$$|\,?\,|_p : \mathbb{Q} \longrightarrow \mathbb{R},$$

oder, was dasselbe ist, bezüglich der p-adischen additiven Bewertung

$$v_p : \mathbb{Q}^* \longrightarrow \mathbb{Z}.$$

Man beachte, es gilt

$$|x|_p = p^{-v_p(x)}$$

$v_p(x) = n$, falls p in der Faktorzerlegung von x in der Potenz n vorkommt.

Der Körper $\mathbb{Q}_p$ heißt Körper der p-adischen Zahlen Als Vervollständigung eines bewerteten Körpers ist $\mathbb{Q}_p$ ein bewerteter Körper. Wir bezeichnen die Bewertung von $\mathbb{Q}_p$, welche die gegebene Bewertung von $\mathbb{Q}$ fortsetzt ebenfalls mit $|\,?\,|_p$ und sprechen von dieser Fortsetzung auch als von der p-adischen Bewertung,

$$|\,?\,|_p : \mathbb{Q}_p \longrightarrow \mathbb{R},$$

Der zugehörige Bewertungsring wird mit

$$\mathbb{Z}_p := \{x \in \mathbb{Q}_p : |x|_p \le 1\} = \{x \in \mathbb{Q}_p : v_p(x) \ge 0\}$$

bezeichnet und heißt Ring der ganzen p-adischen Zahlen. Wie wir wissen ist $\mathbb{Z}_p$ ein diskreter Bewertungsring und wegen $v_p(p) = 1$ ist p ein Parameter. Insbesondere ist

$$p\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p < 1\} = \{x \in \mathbb{Q}_p : v_p(x) > 0\}$$

das Bewertungsideal. Die natürliche Einbettung

$$\mathbb{Z} \hookrightarrow \mathbb{Z}_p$$

induziert einen Homomorphismus von Ringen mit 1,

$$\mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}_p/p\,\mathbb{Z}_p = \kappa(\mathbb{Q}_p) \qquad (1)$$

Weil links ein Körper steht, ist dieser Homomorphismus injektiv, d.h. (1) beschreibt eine Körpererweiterung. Es ist nicht schwer, zu zeigen, dies ist sogar ein Isomorphismus.[1] Insbesondere ist der Restklassenkörper $\kappa(\mathbb{Q}_p)$ endlich, d.h. $\mathbb{Q}_p$ ist ein lokaler Körper.

[1] Es reicht zu zeigen, die Abbildung (1) ist surjektiv. Sei

$$\alpha \in \mathbb{Z}_p - p\mathbb{Z}_p$$

Aus der Bijektivität der Abbildung (1) ergibt sich, daß die Elemente von $\mathbb{Z}_p$ gerade die Potenzreihen in p mit Koeffizienten zwischen 0 und p sind,

$$\mathbb{Z}_p = \{ \sum_{n=0}^{\infty} a_n p^n \mid 0 \le a_n < p, a_n \in \mathbb{Z}\} \qquad (2)$$

(vgl. den ersten Schritt im Beweis von 2.4.1)

Bemerkungen

(i) $\mathbb{Z}_p$ ist gerade die Vervollständigung von $\mathbb{Z}$ bezüglich der p-adischen Bewertung.[2]

(ii) $\mathbb{Z}_p$ ist gerade die Vervolltändigung des Quotientenrings $\mathbb{Z}_{(p)}$ von $\mathbb{Z}$ bezüglich des von p erzeugten Primideals (in der Metrik zur p-adischen Bewertung).[3]

(iii) $\mathbb{Z}_p$ ist gerade die topologische Abschließung von $\mathbb{Z}$ in $\mathbb{Q}_p$.[4]

---

eine ganze p-adische Zahl, die ein von Null verschiedenes Element von $\kappa(\mathbb{Q}_p)$ repräsentiert. Diese Zahl ist Limes einer Folge von rationalen Zahlen $\alpha_n \in \mathbb{Q}$.[1] Insbesondere gilt

$$|\alpha - \alpha_n| \longrightarrow 0,$$

also für große n

$$|\alpha_n| = \max\{|\alpha_n - \alpha|, |\alpha|\} = |\alpha| \le 1.$$

Man beachte, wegen $\alpha \neq 0$ gilt $|\alpha| > 0$, d.h. für große n wird $|\alpha - \alpha_n|$ echt kleiner als $|\alpha|$. Insbesondere sehen wir, für n groß ist α_n ein Element von $\mathbb{Z}_p$ und $\alpha - \alpha_n$ eines von $p\mathbb{Z}_p$,

$$\alpha \equiv \alpha_n \bmod p\mathbb{Z}_p \text{ und } \alpha_n \in \mathbb{Q} \cap \mathbb{Z}_p.$$

Wir können deshalb annehment,

$$\alpha \in \mathbb{Q} \text{ und } v_p(\alpha) \ge 0.$$

Insbesondere können wir α in der Gestalt

$$\alpha = a/b \text{ mit } a, b \in \mathbb{Z}, b \text{ teilerfremd zu } p$$

schreiben. Weil b teilerfremd ist zu p, gibt es ganze Zahlen b', p' mit

$$bb' + pp' = 1.$$

Es folgt

$$ab' = \alpha bb' = \alpha(1 - pp') \equiv \alpha \bmod p\mathbb{Z}_p$$

Mit anderen Worten, die Restklasse von α in $\kappa(\mathbb{Q}_p)$ enthält eine ganze Zahl ab'.

[2] Wegen (2) liegt $\mathbb{Z}$ dicht in $\mathbb{Z}_p$ und nach 2.4.1 ist $\mathbb{Z}_p$ kompakt und damit vollständig.

[3] Wegen Bemerkung (i) reicht es zu zeigen,

$$\mathbb{Z} \subseteq \mathbb{Z}_{(p)} \subseteq \mathbb{Z}_p.$$

Die linke Inklusion besteht trivialerweise. Es reicht also, zu zeigen, jedes Element von $\mathbb{Z}$-(p) ist eine Einheit in $\mathbb{Z}_p$. Sei a ein solches Element, d.h. sei a eine zu p teilerfremde ganze Zahl. Dann gibt es ganze Zahlen a', p' mit aa' + pp' = 1,also aa' $\equiv$ 1 mod $p\mathbb{Z}$, also erst recht aa' $\equiv$ 1 mod $p\mathbb{Z}_p$. Dann kann aber a nicht in $p\mathbb{Z}_p$ liegen, d.h. a ist Einheit in $\mathbb{Z}_p$.

3.1.4 Beispiel: der Funktionenkörper-Fall

Seien F ein endlicher Körper, t eine Unbestimmte und

$$\mathcal{O} := F[[t]]$$

der Ring der formalen Potenzreihen in t. Der Ring $\mathcal{O}$ ist ein diskreter Bewertungsring mit dem Bewertungsideal

$$p := t\bullet\mathcal{O}.$$

Bezeichne

$$k := Q(\mathcal{O})$$

den Quotientenkörper von $\mathcal{O}$ und

$$v_p: k^* \longrightarrow \mathbb{Z}$$

die p-adische Bewertung. Der Körper k besteht gerade aus den formalen Laurent-Reihen

$$\sum_{i=-n}^{\infty} c_i t^i$$

in t mit Koeffizienten aus F,

$$k = F((t)).$$

Eine Cauchy-Folge in k ist eine Folge $\{f_n\}_{n=1,2,...}$ von formalen Laurent-Reihen mit der Eigenschaft, daß es für jedes $m \in \mathbb{N}$ ein $N(m) \in \mathbb{N}$ gibt mit

$$v_p(f_{n'} - f_{n''}) \geq m \text{ für alle } n', n'' \text{ mit } n' \geq N(m) \text{ und } n'' \geq N(m),$$

d.h. es gilt

$$f_{n'} - f_{n''} \in t^m\bullet k[[t]]$$

für die angegebenen n', n''. Mit anderen Worten, die Koeffizienten von t^n der Laurent-Reihen

$$f_{N(m)}, f_{N(m)+1}, f_{N(m)+2}, ...$$

stimmen überein für alle $n \leq m$. Der Koeffizient von t^m in f_n bleibt von einen gewissen n ab unverändert. Es gibt also eine Laurent-Reihe f mit der Eigenschaft, daß jeder Koeffizient von f für jedes hinreichende große n mit dem entsprechenden Koeffizenten von f_n übereinstimmt. Es gilt deshalb

$$f_n \longrightarrow f.$$

Wir haben gezeigt, f ist vollständig. Außerdem ist der Restklassenkörper von k gerade

$$\kappa(k) = \mathcal{O}/p = F[[t]]/t\bullet F[[t]] \cong F,$$

d.h. dieser Restklassenkörper ist endlich. Insbesondere ist k ein lokaler Körper.

Bemerkung

Es ist möglich, sich eine vollständige Übersicht über alle lokalen Körper zu verschafffen. Entsprechend den oben angeführten Beispielen treten dabei zwei Typen von lokalen Körpern auf, solche der Charakteristik 0 und solche von Primzahl-Charakteristik.

Um die lokalen Körper von Primzahl-Charakteristik zu klassifizieren, braucht man einen Satz, der an dieser Stelle nicht bewiesen werden kann, den Cohen-Struktur-Satz, welcher einer der zentralen Sätze der kommutativen Algebra ist. Genauer benötigt man den foldenden Spezialfall des Cohen-Struktur-Satzes.

Cohen-Struktur-Satz

---

[4] Nach (i) liegt $\mathbb{Z}$ dicht in $\mathbb{Z}_p$ und nach 2.4.1 ist $\mathbb{Z}_p$ kompakt, also abgeschlossen.

Sei (A, m) ein noetherscher lokaler Ring, welcher vollständig ist bezüglich der m-adischen Topologie und welcher einen Körper enthält.[5] Dann ist A isomorph zu einem formalen Potenzreihen-Ring über einem Körper,

$$A \cong L[[t_1, ... , t_r]]$$

mit einem Körper L und Unbestimmten $t_1, ... , t_r$.

Zur Beschreibugn der lokalen Körper der Charakteristik Null benötigt man einen Satz, den wir in dieser Vorlesung beweisen werden. Genauer, dieser Satz ist eines der Hauptergebnisse dieses Kapitels und beschreibt eine Beziehung zwischen dem Körpergrad einer Erweiterung, dem Verzweigungsindex und dem sogenannten ´Relativgrad. Wir geben nachfolgend eine Formulierung an.

3.1.5 Der Körpergrad einer endlichen Erweiterung eines vollständigen Körpers

Sei k ein Körper, welcher vollständig ist bezüglich der diskreten Bewertung

$$|?|: k^* \twoheadrightarrow \mathbb{R}$$

und bezeichne

$\mathcal{O} := \{x \in k : |x| \le 1\}$

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

$\kappa := \mathcal{O}/p$

π

den zugehörigen Bewertungsring, das Bewertungsideal, den Restklassenkörper bzw. einen Parameter.
Weiter sei

$$K/k$$

eine endliche separable Körpererweiterung und

$$|?|_K: K \longrightarrow \mathbb{R}$$

die eindeutig bestimmte Fortsetzung von |?| auf K. Wir bezeichnen mit

$\mathcal{O}_K := \{x \in K : |x| \le 1\}$

$p_K := \{x \in K : |x| < 1\}$

$\kappa_K := \mathcal{O}/p$

π_K

den zugehörigen Bewertungsring, das Bewertungsideal, den Restklassenkörper bzw. einen Parameter. Weiter sei

$f := f(K/k) = [\kappa_K:\kappa]$

der Relativgrad (d.h. der Grad der zugehörigen Erweiterung der Restklassenkörper) und

$e := e(K/k)$

der Verzweigungsindex, d.h. $\pi = u\bullet\pi_K^e$ mit einer Einheit u von $\mathcal{O}_K$. Dann gilt

$[K:k] \quad = e\bullet f.$

[5] Im allgemeinen Cohen-Struktur-Satz kommt man ohne die Voraussetzung aus, daß A einen Körper enthält. Die Rolle des Körpers L nimmt dann ein sogenannter Cohen-Ring ein, das sind spezielle vollständige diskrete Bewertungsringe.

3.1.6 Klassifikation der lokalen Körper

Jeder lokale Körper ist isomorph zu einer endlichen Erweiterung des Körpers $\mathbb{Q}_p$ der p-adische Zahlen für ein p oder zu einem der rationalen Funktionenkörper F((t)) von 3.1.4.

Beweis. Sei k ein lokaler Körper.

1. Fall: char(k) = 0.

Weil die Charakteristik von k gleich Null ist, können wir $\mathbb{Z}$ mit einem einem Teilring von k identifizieren,

$$\mathbb{Z} \subseteq k.$$

Weil k ein Körper ist, gilt dann aber auch

$$\mathbb{Q} \subseteq k.$$

Die Bewertung von k ist diskret, also nicht-archimedisch. Ihre Einschränkung auf $\mathbb{Q}$ also eine p-adische Bewertung mit einer Primzahl p,

$$|?|_p: \mathbb{Q} \longrightarrow \mathbb{R}.$$

Weil k vollständig ist, liegt sogar die Vervollständigung von $\mathbb{Q}$ bezüglich der p-adischen Bewertung in k, d.h.

$$\mathbb{Q}_p \subseteq k, \qquad (1)$$

wobei die Einschränkung der Bewertung von k gerade die p-adische ist,

$$|?|_p: \mathbb{Q}_p \longrightarrow \mathbb{R}.$$

Für jede endliche Teilerweiterung k'/ $\mathbb{Q}_p$ von (1) gilt nach 3.1.5

$$[k': \mathbb{Q}_p] = e(k'/ \mathbb{Q}_p)\bullet f(k'/ \mathbb{Q}_p)$$

und

$$e(k'/ \mathbb{Q}_p) \le e(k/ \mathbb{Q}_p),\ f(k'/ \mathbb{Q}_p) \le f(k/ \mathbb{Q}_p).$$

Dabei ist e(k/ $\mathbb{Q}_p$) eine von k' unabhängige natürliche Zahl, und weil der Restklassenkörper von k nach Voraussetzung endlich ist, gilt dasselbe auch für den Relativindex f(k/ $\mathbb{Q}_p$). Deshalb bleibt der Körpergrad [k': $\mathbb{Q}_p$] beschränkt, wenn k' allle Teilerweiterungen von (1) durchläuft. Dann muß aber (1) selbst schon eine endliche Erweiterung sein.

2. Fall: char(k) = p > 0.

Seien P $\subseteq$ k der Primkörper von k, $\mathcal{O}$ der Bewertungsring von k, $\wp$ das Bewertungsideal und π ein Parameter.

Weil die Charakteristik von k von Null verschieden ist, besteht P aus den Vielfachen des Einselements von k. Insbesondere gilt

$$P \subseteq \mathcal{O},$$

Nach dem Cohen-Struktur-Satz ist der vollständige lokale Ring $\mathcal{O}$, der einen Körper (nämlich P) enthält isomorph zu einem Potenzreihenring

$$\mathcal{O} = k'[[t_1, \dots , t_r]]$$

über einem Körper k'. Das Bewertungsideal ist das einzig maximale Ideal $\wp$ von $\mathcal{O}$, d.h.

$$\wp = (t_1, \dots , t_r).$$

Außerdem ist $\wp$ ein Hauptideal, d.h. es gilt

$$r = 1.$$

Der Restklassenkörper κ ist nach Voraussetzung endlich,

$$\kappa = \mathcal{O}/\wp = k'[[t_1]]/(t_1) = k',$$

d.h. k' = F ist ein endlicher Körper.

QED.

Wiederholung

Ganze Abschließungen,

Verträglichkeit mit Lokalisierungen 1.9.2

Ganze Abschließung von Dedekind-Ringen in endlichen Körpererweiterungen 1.9.3

Vergleich der Gruppen der gebrochenden Ideale, $F(R) \hookrightarrow F(S)$, 1.9.4.

Fortsetzbarkeit von diskreten Bewertungen auf endliche separable Erweiterungen, 2.3.12

Der vollständige Fall: die Fortsetzung ist eindeutig 2.3.8

Insbesondere ist die Abschließung eines vollständigen Bewertungsrings in einer endlichen separablen Erweiterung des Quotientenkörpers nicht nur ein Dedekindring, sondern sogar wieder ein diskreter Bewertungsring, vgl. 2.3.13.

Das Tensorprodukt von Körpererweiterungen, vgl, 2.3.11

Seien K/k eine endliche separable und L/k eine beliebige Körpererweiterung. Dann ist das Tensorprodukt

$$K\otimes_k L$$

ein kommutativer Ring mit 1, welcher in ein direktes Produkt von endlichen Körpererweiterungen von L zerfällt, sagen wir[6]

$$K\otimes_k L \cong L_1\times\ldots\times L_r .$$

Als Körper über k und L sind die L_i paarweise isomorph und gleich dem Kompositum von K und L ,

$$L_i \cong K\cdot L.$$

Für $\alpha\in K$ bezeichne

$$\chi_\alpha \in k[x]\ ,\ \chi_{i,\alpha} \in L_i[x]$$

das Charakteristische Polynom[7] von α bezüglich K/k bzw. L_i/L. Dann gilt

$$\chi_\alpha = \chi_{1,\alpha}\cdot\ldots\cdot \chi_{r,\alpha}.$$

Insbesondere gilt für Norm und Spur

$$N_{K/k}(\alpha) = \prod_{i=1}^{r} N_{L_i/L}(\alpha)$$

und

$$Tr_{K/k}(\alpha) = \sum_{i=1}^{r} Tr_{L_i/L}(\alpha)$$

Spezialfall, vgl. 2.3.12

---

[6] Auf der rechten Seite stehe die direkte Summe der L-Moduln L_i , welche mit der koordinatenweisen Multiplikation versehen sei. Die Anzahl der direkten Summanden muß endlich sein, weil auf der linken Seite ein endlich-dimensionaler L-Vektorraum steht.

[7] d.h. das charakteristische Polynom der Multiplikation mit α bezüglich der Vektorräume K bzw. L_i über k bzw. L.

Ist in der obigen Situation k ein bewerter Körper und $L = \overline{k}$ die Vervollständigung von k, so sind die L_i gerade die Vervollständigungen von K bezüglich der Fortsetzungen auf K der Bewertung von k. Insbesondere gibt des gerade r verschiedene solcher Fortsetzungen.

3.2 Die Differente einer endlichen separablen Erweiterung eines diskret bewerteten Körpers

3.2.1 Die Norm eines gebrochenen Ideals

Seien R ein Dedekindring mit dem Quotientenkörper K,

L/K

eine endliche separable Körpererweiterung,

$$\begin{array}{ccc} K & \subseteq & L \\ \cup & & \cup \\ R & \subseteq & S \end{array}$$

S

die ganze Abschließung von R in L und

J

ein gebrochenes Ideal von S.

Dann ist J als S-Modul endlich erzeugt (nach 1.4.2) und S ist als R-Modul endlich erzeugt (nach 1.9.3), also sind S und J endlich erzeugte R-Teilmoduln des endlich-dimensionalen K-Vektorraums L, und diese enthalten eine Basis von L über K[8]. Mit anderen Worten S und J sind Gitter von L über R (vgl. 1.6.2). Insbesonder ist der Index dieser R-Gitter definiert (vgl. 1.6.5). Wir setzen

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

und nennen dieses gebrochene Ideal von R auch <u>Norm</u> von J über R.

Bemerkungen

(i) Zur Erinnerung, ist R ein diskreter Bewerungsring, so sind je zwei R-Gitter M, N freie R-Moduln desselben Rangs über R. Insbesondere gibt es eine R-lineare Surjektion

$$f: M \longrightarrow N$$

(sogar einen Isomorphismus). Der Index ist dann definiert als das gebrochene Ideal

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

welches von der Determiante von f erzeugt wird. Im allgemeinen Fall ist (M:N) das Gebrochene Ideal von R, welches in den Lokalisierungen von R von diesen Determinanten er zeugt wird.

(ii) Ist R = Z und $J \subseteq S$ ein Ideal ($\neq 0$), ist

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

---

[8] S•K ist eine nullteilerfreie K-Algebra (weil in L enthalten), welche als K-Vektorraum endlich erzeugt ist (weil S über R endlich erzeugt ist), also ein Körper. Deshalb ist

$$S\bullet K = Q(S\bullet K) = Q(S) = L.$$

Weil J ein gebrochenes Ideal von S ist, gibt es Elemente $a, b \in S - \{0\}$ mit

$$aS \subseteq J \subseteq \frac{1}{b} S$$

(nach dem Vergleichslemma 1.6.4).Wegen $aSK = aL = L$ und $\frac{1}{b}SK = \frac{1}{b}L = L$ erhalten wir durch Multiplikation von K:

$$L \subseteq JK \subseteq L.$$

gerade der gewöhnlich Index von J in S, d.h. die Anzahl der Restklassen von S/J (genauer, $N_{L/K}(J)$ ist das Ideal von $\mathbb{Z}$, welches von diesem gewöhnlichen Index erzeugt wird).

(iii) Für jeden Dedekind-Ring R, besteht eine Isomorphismus (vgl. 1.5.5)

$$F(R) \xrightarrow{\cong} \prod_{p \text{ maximal}} F(R_p), \quad I \mapsto (IR_p)_{p \text{ maximal}}$$

der Gruppen gebrochener Ideale, wobei rechts das direkte Produkt über alle maximalen Ideale p von R zu nehmen ist. Die Norm ist mit diesem Isomorphismus verträglich, weil der Index diese Eigenschaft hat, d.h. $N_{L/K}(J)$ ist das eindeutig bestimmte gebrochene Ideal von R mit

$$N_{L/K}(J)\bullet R_p = N_{L/K}(J\bullet R_p)$$

für jedes maximale Ideal $p \subseteq R$.

(iv) Allgemeiner kommutiert die Norm mit dem Übergang zu den Lokalisierungen[9], d.h.

$$N_{L/K}(J)\bullet R_S = N_{L/K}(J\bullet R_S)$$

für jede multiplikativ abgeschlossene Menge $S \subseteq R$.[10]

3.2.2 Die Norm eines Hauptideals

Seien R ein Dedekindring mit dem Quotientenkörper K,

L/K

eine endliche separable Körpererweiterung,

$$\begin{array}{ccc} K & \subseteq & L \\ \cup & & \cup \\ R & \subseteq & S \end{array}$$

S

die ganze Abschließung von R in L und

$$J = aS, \ a \in L^*,$$

ein gebrochenes Hauptideal von S, d.h. ein gebrochenes Ideal, welches von nur einem Element erzeugt wird. Dann gilt

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

Dabei steht rechts die gewöhnliche Norm $N_{L/K}: L \longrightarrow K$ der Körpererweiterung L/K.

Beweis. Wir haben zu zeigen, für jedes maximale Ideal p von R gilt

$$N_{L/K}(aS)R_p = N_{L/K}(a)R_p,$$

d.h.

$$(S:aS)R_p = N_{L/K}(a)R_p,$$

d.h.

$$(S_p:aS_p) = N_{L/K}(a)R_p$$

(vgl. 1.6.15(i)). Zur Berechung der linken Seite benötigen wir eine R-lineare Surjektion $f:S_p \longrightarrow aS_p$. Als eine solche können wir die Multiplikation mit a verwenden,

$$f(x) = ax.$$

Dann gilt

$$(S_p:aS_p) = \det(f)R.$$

Die Determinante der Multiplikation mit a ist aber gerade die Körpernorm von a.

---

[9] wegen (iii).

[10] Das folgt aus der Charakterisierung (iii) der Norm.

QED.

Bemerkung

Unser nächstes Ziel besteht darin, zu zeigen, daß die Bildung der Norm mit dem Übergang zur Vervollständigung verträglich ist. Genauer:

3.2.3 Die Verträglichkeit der Norm mit dem Übergang zur Vervollständigung

Seien R ein Dedekindring mit dem Quotientenkörper K,

$$L/K$$

eine endliche separable Körpererweiterung,

$$S \qquad \begin{tikzcd} K_p \arrow[rr] & & L_P & \\ & K \arrow[ul] \arrow[rr, dashed] & & L \arrow[ul] \\ \bar{R}_p \arrow[uu] \arrow[rr] & & \bar{S}_P \arrow[uu] & \\ & R \arrow[ul] \arrow[uu] \arrow[rr, dashed] & & S \arrow[ul] \arrow[uu] \end{tikzcd}$$

die ganze Abschließung von R in L und

$$J$$

ein gebrochenes Ideal von S.
Weiter seien

$$p \subseteq R$$

ein maximales Ideal von R,

$$\bar{R}_p \text{ bzw. } K_p$$

die Vervollständigung von R bzw. K bezüglich der p-adischen Topologie[11] . Entsprechend bezeichne

$$\bar{S}_P \text{ bzw. } L_P$$

für jedes über p liegende maximale Ideal $P \subseteq$ die Vervollständigung von S bzw. L bezüglich der P-adischen Topologie. Dann gilt

$$N_{L/K}(J)\cdot \bar{R}_p = \prod_{P|p} N_{L_P/K_p}(J\cdot \bar{S}_P). \tag{1}$$

Beweis. Wir betrachten die Zerlegung des Tensorprodukts $L\otimes_K K_p$ von 2.3.11. Sie hat nach 2.3.12 die Gestalt

$$L\otimes_K K_p \cong L_{P_1} \times\ldots\times L_{P_r} \tag{2}$$

wenn P_1 , ... , P_r gerade die maximale Ideale von S sind, welche über p liegen.

<u>1.Schritt</u>: $\bar{R}_p\cdot S = \bar{S}_{P_1} \times\ldots\times \bar{S}_{P_r}$

Dabei seien die beiden Seiten vermittels der Isomorphie (2) mit Teilmoduln desselben Moduls identifiziert.

---

[11] Äquivalent: $\bar{R}_p$ ist der Bewertungsring der Vervollständigung von K bezüglich der p-adischen Topologie.

Auf Grund der koordinatenweisen Multiplikation auf der rechten Seite von (2) ist ein Element dieser rechten Seite genau dann ganz über $\overline{R}_p$ ($\subseteq L_{P_i}$), wenn jede Koordinate dieses Elements ganz ist über R. Mit anderen Worten,

$$\overline{S}_{P_1}\times\ldots\times\overline{S}_{P_r} \tag{3}$$

ist gerade die ganze Abschließung von $\overline{R}_p$ in der rechten Seite von (2). Insbesondere liegt $\overline{R}_p$ in (3) und dasselbe gilt für S (denn die Elemente von S ganz sind über R, also erst recht über $\overline{R}_p$. Wir haben gezeigt,

$$\overline{R}_p\bullet S \subseteq \overline{S}_{P_1}\times\ldots\times\overline{S}_{P_r}. \tag{4}$$

Wir müssen noch die umgekehrte Inklusion beweisen. Nach dem schwachen Approximationssatz 2.3.4 liegt L dicht in $L_{P_1}\times\ldots\times L_{P_r}$, d.h. für jedes Element,

$$(\alpha_1, \ldots, \alpha_r) \in \overline{S}_{P_1}\times\ldots\times\overline{S}_{P_r}$$

gibt es eine Folge $\{\xi_n\}$ von Elementen aus L, die gegen dieses Element konvergiert, d.h.

$$\xi_n \longrightarrow \alpha_i \text{ in } L_{P_i} \text{ bezüglich der } P_i\text{-adischen Topologie.}$$

Wegen $\alpha_i \in S_{P_i}$ gilt $v_{P_i}(\alpha_i) \geq 0$. Wegen $v_{P_i}(\alpha_i - \xi_n) \longrightarrow \infty$ folgt für großes n

$$v_{P_i}(\xi_n) = v_{P_i}(\alpha_i - (\alpha_i - \xi_n)) = \min(v_{P_i}(\alpha_i), v_{P_i}(\alpha_i - \xi_n)) = v_{P_i}(\alpha_i) \geq 0,$$

d.h. für große n ist

$$v_{P_i}(\xi_n) \geq 0 \text{ für } i = 1, \ldots, r.$$

Betrachten wir die ganze Abschließung $S\bullet R_p$ von R_p in L und das von ξ_n in dieser Abschließung erzeugte gebrochene Ideal

$$\xi_n S\bullet R_p.$$

Wie wir gerade gesehen haben, sind die Exponenten der Faktor-Zerlegung dieses Ideals für große n sämtlich ≥ 0, d.h. es gilt

$$\xi_n S\bullet R_p \subseteq S\bullet R_p \text{ für große n,}$$

d.h.

$$\xi_n \in S\bullet R_p \subseteq \overline{R}_p\bullet S.$$

Wir haben gezeigt, $\overline{R}_p\bullet S$ liegt dicht in der rechten Seite von (4). Zum Beweis der Gleichheit in (4) reicht es zu zeigen, $\overline{R}_p\bullet S$ ist abgeschlossen. Dazu wiederum reicht es zu zeigen, $\overline{R}_p\bullet S$ ist vollständig.

Zum Beweis der Vollständigkeit von $\overline{R}_p$•S beachten wir, $\overline{R}_p$•S ist ein endlich erzeugter Modul über $\overline{R}_p$ (weil S endlich erzeugt ist über R). Weil $\overline{R}_p$ ein diskreter Bewertungsring ist, ist $\overline{R}_p$•S sogar ein endlich erzeugter freier Modul über $\overline{R}_p$, also ein direkters Produkt von Exemplaren von $\overline{R}_p$. Mit $\overline{R}_p$ ist dann aber auch dieses direkte Produkt vollständig.

<u>2. Schritt</u>. Beweis der Behauptung.

Für jedes gebrochene Ideal J von S erhalten wir aus der Zerlegung des ersten Schritts durch Multiplikation mit J die Zerlegung

$$J\bullet\overline{R}_p = (J\overline{S}_{P_1})\times\ldots\times(J\overline{S}_{P_r})$$

(wegen der koodinatenweisen Multiplikation auf der rechten Seite). Auf Grund der allgemeinen Rechenregeln für den Index von Moduln erhalten wir

$$(S\bullet\overline{R}_p : J\bullet\overline{R}_p) = (\overline{S}_{P_1} : J\overline{S}_{P_1})\bullet\ldots\bullet(\overline{S}_{P_r} : J\overline{S}_{P_r}) \qquad (5)$$

(vgl. 1.6.14). Nach 1.6.15 (i) ergibt sich

$$\begin{aligned} N_{L/K}(J)\bullet\overline{R}_p &= (S{:}J)\bullet\overline{R}_p = (S\bullet\overline{R}_p : J\bullet\overline{R}_p) \\ &= (\overline{S}_{P_1} : J\overline{S}_{P_1})\bullet\ldots\bullet(\overline{S}_{P_r} : J\overline{S}_{P_r}) \qquad \text{(wegen (5))} \\ &= N_{L_{P_1}/K_p}(J\overline{S}_{P_1})\bullet\ldots\bullet N_{L_{P_r}/K_p}(J\overline{S}_{P_r}) \end{aligned}$$

QED.

3.2.4 Folgerung: die Norm von gebrochenen Idealen als Homomorphismus

Seien R ein Dedekindring mit dem Quotientenkörper K,

$$L/K$$

eine endliche separable Körpererweiterung,

$$S \qquad\qquad \begin{array}{ccc} K & \subseteq & L \\ \cup & & \cup \\ R & \subseteq & S \end{array}$$

die ganze Abschließung von R in L. Dann definiert die Norm gebrochener Ideale einen Gruppen-Homomorphismus

$$N_{L/K}: F(S) \longrightarrow F(R).$$

Beweis. Wir haben zu zeigen,

$$N_{L/K}(J'\bullet J'') = N_{L/K}(J')\bullet N_{L/K}(J'')$$

für je zwei gebrochene Ideale J',, J" von S. Nach Bemerkung 3.2.1 (iii) reicht es zu zeigen,

$$N_{L/K}(J'\bullet J'')R_p = N_{L/K}(J')\bullet N_{L/K}(J'')\, R_p$$

für jedes maximale Ideal p $\subseteq$ R. Zwei gebrochene Ideale von R_p sind genau dann gleich, wenn sie von derselben Potenz des Parameters erzeugt werden, d.h. genau dann wenn sie in der Vervollständigung $\overline{R}_p$ gleich sind. Es reicht also zu zeigen,

$$N_{L/K}(J'\bullet J'')\overline{R}_p = N_{L/K}(J')\bullet N_{L/K}(J'')\,\overline{R}_p$$

für jedes maximale Ideal von $p \subseteq R$. Auf Grund der gerade bewiesenen Formel (von 3.2.3) reicht es zu zeigen

$$N_{L_P/K_p}(J'J''\bullet \overline{S}_P) = N_{L_P/K_p}(J'\bullet \overline{S}_P)\bullet N_{L_P/K_p}(J''\bullet \overline{S}_P).$$

für jedes maximale Ideal $p \subseteq R$ und jedes über p liegende maximale Ideal $P \subseteq S$. Nun ist $\overline{S}_P$ ein diskreter Bewertungsring, d.h. die von J' und J'' erzeugten Ideale sind Hauptideale, sagen wir

$$J'\bullet \overline{S}_P = a'\overline{S}_P \text{ und } J''\bullet \overline{S}_P = a''\,\overline{S}_P.$$

Es reicht somit zu zeigen,

$$N_{L_P/K_p}(a'a''\overline{S}_P) = N_{L_P/K_p}(a'\,\overline{S}_P)\bullet N_{L_P/K_p}(a''\,\overline{S}_P).$$

Nach 3.2.2 bedeutet dies, es reicht zu zeigen

$$N_{L_P/K_p}(a'a'')\,\overline{S}_P = N_{L_P/K_p}(a')\bullet N_{L_P/K_p}(a'')\overline{S}_P$$

Für die gewöhliche Körpernorm gilt abe sogar

$$N_{L_P/K_p}(a'a'') = N_{L_P/K_p}(a')\bullet N_{L_P/K_p}(a'').$$

QED.

3.2.5 Folgerung: die Norm eines Ideals über dem Grundring

Seien R ein Dedekindring mit dem Quotientenkörper K,

$$L/K$$

eine endliche separable Körpererweiterung,

$$S \qquad \begin{array}{ccc} K & \subseteq & L \\ \cup & & \cup \\ R & \subseteq & S \end{array}$$

die ganze Abschließung von R in L. Dann gilt für jedes gebrochene Ideal I von R

$$N_{L/K}(I) = I^n \text{ mit } n := [L:K]$$

Beweis. Wie im Beweis von 3.2.4 reduziert man den Beweis auf den Fall, daß I ein Hauptideal ist und verwendet die Beschreibung 3.2.2 der Idealnorm mit Hilfe der Körpernorm.
QED.

3.2.6 Folgerung: Transitivität der Norm gebrochener Ideale

Seien R ein Dedekindring mit dem Quotientenkörper F,

$$F \subseteq K \subseteq L$$

eine Folge von endlichen separablen Körpererweiterungen und

$$S \qquad \begin{array}{ccccc} F & \subseteq & K & \subseteq & L \\ \cup & & \cup & & \cup \\ R & \subseteq & \mathcal{O}_K & \subseteq & S \end{array}$$

die ganze Abschließung von R in L. Dann gilt für jedes gebrochene Ideal J von S

$$N_{L/F}(J) = N_{K/F}(N_{L/K}(J)).$$

Beweis. Wie im Beweis von 3.2.4 reduziert man den Beweis auf den Fall, daß I ein Hauptideal ist und verwendet die Beschreibung 3.2.2 der Idealnorm mit Hilfe der Körpernorm.
QED.

3.2.7 Die Differente einer Erweiterung

Seien R ein Dedekindring mit dem Quotientenkörper K,

$$L/K$$

eine endliche separable Körpererweiterung und

$$S \qquad \begin{array}{ccc} K & \subseteq & L \\ \cup & & \cup \\ R & \subseteq & S \end{array}$$

die ganze Abschließung von R in L. In dieser Situation ist S ein R-Gitter in L, also dessen Dual

$$D_R(S) := \{ u \in L \mid Tr_{L/K}(uS) \subseteq S\}$$

ein wohldefiniertes R-Gitter in L (vgl. 1.6.11). Insbesondere ist dieses Dual ein endlich erzeugter R-Teilmodul von L (vgl. 1.6.2). Unmittelbar auf Grund der Definition ist dieses Dual ein S-Modul, also insbesondere ein endlich erzeugter (von Null verschiedener)[12] S-Modul, also auch ein gebrochenes Ideal von S (vgl. 1.4.5). Dieses Ideal besitzt ein wohldefiniertes Inverses. Dieses Inverse wird mit

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

bezeichnet und heißt <u>Differente</u> von S über R.
Da S ein R-Gitter in L ist, können wir entsprechend die Diskriminante

$$\delta := \delta(S/R) := (D_R(S) : S)$$

von S über R bilden (vgl. 1.6.12).

Bemerkungen

(i) Nach Definition ist die Differente $\mathcal{D}(S/R)$ ein gebrochenes Ideal von S. Wegen

$$S \subseteq D_R(S)$$

gilt aber

$$\mathcal{D} = D_R(S)^{-1} \subseteq S^{-1} = S,$$

d.h. die Different ist sogar ein gewöhliches (von Null verschiedenes Ideal von S.

(ii) Für jedes R-Gitter M haben wir in 1.6.12 die Diskriminante dieses Gitters definiert als

$$\delta(M) := \delta(M/R) := (D_R(M) : M).$$

---

[12] Es gilt $S \subseteq D_R(S)$.

Insbesondere können wir die Diskriminante des R-Gitters M = S bilden,

$$\delta := \delta(S/R) := (D_R(S) : S)$$

Eines unserer nächsten Ziele ist die Berechnung dieser Diskriminante von S über R und deren Vergleich mit der Differente.

3.2.8 Vergleich von Differente und Diskriminante

Seien R ein Dedekindring mit dem Quotientenkörper K,

$$L/K$$

eine endliche separable Körpererweiterung und

$$S \qquad \begin{array}{ccc} K & \subseteq & L \\ \cup & & \cup \\ R & \subseteq & S \end{array}$$

die ganze Abschließung von R in L. Dann gilt

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

Beweis. Es gilt

$$\begin{aligned} \delta(S/R) &= (D_R(S) : S) && \text{(nach Definition von } \delta\text{)} \\ &= (S : D_R(S))^{-1} && \text{(nach 1.6.6)[13]} \\ &= N_{L/K}(D_R(S))^{-1} && \text{(nach Definition der Norm in 3.2.1)} \\ &= N_{L/K}(D_R(S)^{-1}) && (N_{L/K} \text{ ist ein Homomorphismus nach 3.2.4)} \\ &= N_{L/K}(\mathcal{D}(S/R)) && \text{(nach Definition der Differente).} \end{aligned}$$

QED.

3.2.9 Verträglichkeit von Differente und Diskriminante mit Vervollständigungen

Seien R ein Dedekindring mit dem Quotientenkörper K,

$$L/K$$

eine endliche separable Körpererweiterung und

$$S \qquad \begin{array}{ccc} K & \subseteq & L \\ \cup & & \cup \\ R & \subseteq & S \end{array}$$

die ganze Abschließung von R in L. Weiter sei $p \subseteq R$ ein maximales Ideal. Dann gelten folgende Aussagen.

(i) $\mathcal{D}(S/R)\overline{S}_p = \mathcal{D}(\overline{S}_p/\overline{R}_p)$

---

[13] Nach 1.6.6 gilt

$$(S: D_R(S)) \cdot D_R(S) : S) = (S:S) = S.$$

Die Identität ganz rechts besteht, weil man zur Berechnung des Index (S:S) die identische Abbildung verwenden kann (d.h. (R:R) wird in jeder Lokalisierung von 1 = det(Id) erzeugt). Die behauptete Identität ergibt sich jetzt aus der Tatsache, daß der Index ein gebrochenes Ideal ist.

für jedes über p liegende maximale Ideal $P \subseteq S$.

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

Dabei werde das Produkt auf der rechten Seite über die maximalen Ideal $P \subseteq S$ erstreckt, welche über p liegen.

Dabei bezeichne $\overline{R}_p$ wie bisher die Vervollständigung von R in der p-adischen und $\overline{S}_P$ die Vervollständigung von S in P-adischen Topologie.

Beweis. Zu (i). Es gilt

$$
\begin{aligned}
\mathcal{D}(S/R)\overline{S}_P &= D_R(S)^{-1}\overline{S}_P && \text{(nach Definition der Differente)}\\
&=^{14} (D_R(S)\overline{S}_P)^{-1} &&\\
&= (D_R(S)\,\overline{R}_p\overline{S}_P)^{-1} && \text{(wegen } 1\in\overline{R}_p\subseteq\overline{S}_P)=\\
&= (D_{\overline{R}_p}(S\overline{R}_p)\overline{S}_P)^{-1} && \text{(nach 1.6.15(ii))}\\
&= (D_{\overline{R}_p}(\overline{S}_P)\overline{S}_P)^{-1} && \text{(wegen } S\overline{R}_p = \overline{S}_P)^{15}\\
&= D_{\overline{R}_p}(\overline{S}_P)^{-1} && (D_{\overline{R}_p}(\overline{S}_P) \text{ ist ein } \overline{S}_P\text{-Modul})\\
&= \mathcal{D}(\overline{S}_P/\overline{R}_p) && \text{(nach Definition der Differente).}
\end{aligned}
$$

Zu (ii). Es gilt

$$
\begin{aligned}
\delta(S/R)\overline{R}_p &= N_{L/K}(\mathcal{D}(S/R))\overline{R}_p && \text{(nach 3.2.8)}\\
&= \prod_{P|p} N_{L_P/K_p}(\mathcal{D}(S/R)\bullet\overline{S}_P) && \text{(nach 3.2.3)}\\
&= \prod_{P|p} N_{L_P/K_p}(\mathcal{D}(\overline{S}_P/\overline{R}_p)) && \text{(nach (i))}
\end{aligned}
$$

---

[14] Für jeden injektiven Homomorphismus von Dedekind-Ringen $f:A \longrightarrow B$ und gebrochende Ideale I', I'' gilt

$$f(I')B\bullet f(I'')B = f(I'\bullet I'')B \text{ und } f(A)B = B,$$

d.h. f induziert einen Homomorphismus

$$F(A) \longrightarrow F(B)$$

der Gruppen der gebrochenen Ideale. Das gilt insbesondere für das gebrochene Ideal $D_R(S)^{-1}$ von S ist und die Inklusion $S \subseteq S_P \subseteq \overline{S}_P$

[15] Es gilt

$S \subseteq S\overline{R}_p \subseteq \overline{S}_P$

und $\overline{S}_P$ ist die Vervollständigung von S. Es reicht also zu zeigen, $S\overline{R}_p$ ist vollständig. Weil S ein endlich erzeugter R-Modul ist, ist $S\overline{R}_p$ ein endlich erzeugter $\overline{R}_p$-Modul. Weil $\overline{R}_p$ ein diskreter Bewertungsring ist, ist $S\overline{R}_p$ damit frei über $\overline{R}_p$, d.h. $S\overline{R}_p$ ein direktes Produkt von endlich vielen Exemplaren des vollständigen Rings $\overline{R}_p$ und damit vollständig.

$$= \prod_{P|p} \delta(\overline{S}_P/\overline{R}_p)) \qquad \text{(nach (3.2.8))}$$

QED.

3.2.10 Die Diskriminante einfacher Erweiterungen von Dedekind-Ringen
Seien R ein Dedekindring mit dem Quotientenkörper K,

$$L/K$$

eine endliche separable Körpererweiterung und

$$S \qquad \begin{array}{ccc} K & \subseteq & L \\ \cup & & \cup \\ R & \subseteq & S \end{array}$$

die ganze Abschließung von R in L. Weiter seien

$$\alpha \in S$$

ein Element mit

$$L = K[\alpha]$$

und

$$g(X) \in K[X]$$

das Minimalpolynom von α über K. Dann ist $R[\alpha]$ ein R-Gitter in L, und es gilt:

(i) $D_R(R[\alpha]) \quad =$[16] $\dfrac{1}{g'(\alpha)} R[\alpha]$.

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

(iii) Folgende Aussagen sind äquivalent.

  (a) $R[\alpha] \quad = S$.

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

Zum Beweis benötigen wir das folgende

3.2.11 Lemma von Euler
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

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

[16] Man beachte, $g'(\alpha) \neq 0$, weil die Erweiterung L/K separabel ist.

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

Man beachte, in $g'(x_i)$ haben gerade die ersten i-1 Faktoren ein anderes Vorzeichen als die entsprechenden Faktoren von D.
Aus der Formel für S erhalten wir durch Erweitern mit dem Polynom D,

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

mit

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

Dabei ist P ein ganzzahliges und symmetrisches[17] Polynom in den $x_1,\ldots,x_n$. Wegen $k \le n-1 \le \deg g'$ gilt

$$\deg P \le \deg D.$$

Zum Beweis der Behauptung genügt es zu zeigen,

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

denn weil P symmetrisch ist, muß dann P auch durch die übrigen Differenzen teilbar sein, d.h. es muß $D \mid P$ gelten[18]. 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[19].

$$x_2 - x_3 , \ldots, x_2 - x_n .$$

Die Faktoren von D_2, in denen x_1 vorkommt, sind die folgenden[20].

$$x_1 - x_3 , \ldots, x_1 - x_n .$$

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.

---

[17] Genauer: das Quadrat von P ist symmetrisch, weil S symmetrisch und das Quadrat von D symmetrisch ist. Die symmetrische Gruppe S_n läßt das Quadrat von P unverändert (und operiert auf P durch Multiplikation mit dem Vorzeichen der Permutation).

[18] Genauer: mit $x_1 - x_2 \mid P$ gilt $x_1 - x_2 \mid P^2$, d.h. P^2 ist durch jede der Differenzen $x_i - x_j$ teilbar. Weil diese Differenzen Primpolynome sind, gilt dann aber auch $x_i - x_j \mid P$.

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

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

Beweis 3.2.10. Wegen $\alpha\in S$ ist α ein über R ganzes Element. Dasselbe gilt für die zu α über K konjugierten Elemente (der algebraischen Abschließung von L). Die Koeffizienten von g(X) sind elementarsymmetrische Polynome in diesen konjugierten Elementen, also ebenfalls ganz über R. Da sie außerdem in K liegen und R ganz abgeschlossen ist in K, folgt

$$g(X) \in R[X].$$

Weil g außerdem den höchsten Koeffizienten 1 hat, ist damit $R[\alpha]$ ein freier R-Modul vom Rang

$$rk_R\, R[\alpha] = \deg g = [L:K]$$

mit dem R-linear unabhängigen Erzeugendensystem

$$1, \alpha, ..., \alpha^{n-1},\ n := [L:K]$$

(welches gleichzeitig eine Vektorraumbasis von L über K ist).

Zu (i) und (ii). Nach dem Lemma von Euler 3.2.11 ist

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

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

$$\frac{1}{g'(\alpha)}R[\alpha] \subseteq D_R(R[\alpha]). \qquad (3)$$

Da $R[\alpha]$ ein freier R-Modul ist, können wir nach 1.6.13 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

$$\begin{aligned}
\det Tr_{L/K}(\alpha^{i+j}) &= \det (s_i(\alpha^j))^2 \\
&= (\prod_{i<j} (s_i(\alpha)-s_j(\alpha)))^2 \quad \text{(Vandermonde)} \\
&=^{21} \pm \prod_{i=1}^{n} g'(s_i(\alpha)) \\
&= \pm N_{L/K}(g'(\alpha))
\end{aligned}$$

Damit ist

[21] Die Differenz $s_i(\alpha)-s_j(\alpha)$ kommt in den Faktoren $g'(s_i(\alpha))$ und $g'(s_j(\alpha))$ jeweils einfach vor und sie kommt in keinem weiteren Faktor vor. Die behauptete Identität besteht also, wenn man vom Vorzeichen absieht.

$$\begin{aligned}
\delta(R[\alpha]/R) &= N_{L/K}(g'(\alpha))R \\
&= N_{L/K}(g'(\alpha)S) && \text{(Norm eines Hauptideals, 3.2.2)} \\
&= (S: g'(\alpha)S) && \text{(Definition der Norm, 3.2.1)} \\
&=^{22} \left(\frac{1}{g'(\alpha)}R[\alpha]:R[\alpha]\right)
\end{aligned}$$

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

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

Wir haben gezeigt, die beiden Moduln $\frac{1}{g'(\alpha)}R[\alpha]$ und $D_R(R[\alpha])$ sind ineinander enthalten (vgl. (3)) und haben denselben Index bezüglich $R[\alpha]$. Nach 1.6.6 (iii) 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,

$$D_R(S) = \frac{1}{g'(\alpha)} S . \qquad (4)$$

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

$$\begin{aligned}
D_R(R[\alpha]) &\supseteq D_R(S) \\
&= \frac{1}{g'(\alpha)} S && \text{(nach (4))} \\
&\supseteq \frac{1}{g'(\alpha)} R[\alpha] \\
&= D_R(R[\alpha]) && \text{(nach (i))}
\end{aligned}$$

Damit gilt überall in dieser Abschätzung der Gleichheitszeichen. Insbesondere ist

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

Nach 1.6.11 ist das doppelte Dual gleich dem ursprüngliche Modul. Aus der letzten Identität folgt also

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

QED.

3.2.11 Diskriminante und Differente von Körpertürmen

Seien R ein Dedekind-Ring mit dem Quotientenkörper K und

$$K \subseteq F \subseteq L$$

ein Turm von endlichen separablen Körpererweiterungen. Weiter seien

$$R \subseteq T \subseteq S$$

die zugehörigen Ringe der ganzen Zahlen (d.h. T bzw. S sind die ganzen Abschließungen von R in F bzw. L). Dann gelten folgende Aussagen.

---

[22] Die Multiplikation mit $g'(\alpha)$ definiert R-lineare Surjektionen

$$S \twoheadrightarrow g'(\alpha)S \text{ und } \frac{1}{g'(\alpha)}R[\alpha] \twoheadrightarrow R[\alpha].$$

Beide Indizes lassen sich also mit Hilfe derselben Determinanten berechnen.

(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:

$$
\begin{aligned}
\delta(S/R) &= N_{L/K}(\mathcal{D}(S/R)) \quad \text{(nach 3.2.8)}\\
&= N_{L/K}(\mathcal{D}(S/T))\cdot N_{L/K}(\mathcal{D}(T/R)) && \text{(nach (i))}\\
&= N_{F/K}N_{L/F}(\mathcal{D}(S/T))\cdot N_{F/K}N_{L/F}(\mathcal{D}(T/R)) && \text{(nach 3.2.6)}\\
&= N_{F/K}\delta(S/T)\cdot N_{F/K}(\mathcal{D}(T/R)^m) && \text{(nach 3.2.5)}\\
&= N_{F/K}\delta(S/T)\cdot \delta(T/R)^m
\end{aligned}
$$

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

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

Wegen der Transitivität der Spur (vgl. 1.7.7) gilt

$$Tr_{L/K}(Sx) \overset{23}{=} Tr_{F/K}(Tr_{L/F}(Sx)T). \qquad (5)$$

Damit erhalten wir

$$
\begin{aligned}
x \in D_R(S) &\Leftrightarrow Tr_{L/K}(Sx) \subseteq R && \text{(nach Definitiion des Duals)}\\
&\Leftrightarrow Tr_{F/K}(Tr_{L/F}(Sx)T) \subseteq R && \text{(wegen (5))}\\
&\Leftrightarrow Tr_{L/F}(Sx) \subseteq D_R(T) =: \mathcal{D}^{-1} && \text{(nach Definition des Duals)}\\
&\Leftrightarrow Tr_{L/F}(Sx\mathcal{D}) \subseteq T && (Tr_{L/F} \text{ ist F-linear und } \mathcal{D}\subset T\subset F)\\
&\Leftrightarrow Sx\mathcal{D}\subseteq D_T(S) && \text{(nach Definition des Duals)}\\
&\Leftrightarrow Sx \subseteq D_T(S)\cdot\mathcal{D}^{-1} = D_T(S)\cdot D_R(T)\\
&\Leftrightarrow x \in D_T(S)\cdot D_R(T)
\end{aligned}
$$

QED.

3.3. Verzweigung

Die Begriffe des Verzweigungsindex und des Relativgrad sind uns bereits in verschiedenen Zusammenhängen begegnet. Wir beschreiben sie jetzt in einem möglichst allgemeinen Kontext.

3.3.1 Verzweigungsindex und Relativgrad

Seien R' und R" zwei ineinander enthaltene Dedekind-Ringe,

$$R' \subseteq R''$$

(d.h. R' sei ein Teilring von R" mit demselben Einselement wie R") mit den Quotientenkörpern

$$K' := Q(R'),\ K'' := Q(R'').$$

Weiter sei

$$p'' \subset R''$$

ein maximales Ideal von R" mit der Eigenschaft, daß das Primideal

---

[23] $Tr_{L/F}$ ist F-linear und es gilt $T \subseteq F$ und $T \subseteq S$.

$$p' := R' \cap p''$$
ebenfalls maximal ist. Die Inklusion der Ringe induziert dann eine Inklusion der zugehörigen Reste-Körper
$$\kappa' := R'/p' \hookrightarrow \kappa'' := R''/p''.$$
Der Grad dieser Körpererweiterung (welcher unendlich sein kann) wird mit
$$f(p''/p') := [\kappa'': \kappa']$$
bezeichnet und heißt Relativgrad von p' in p''. Der Verzweigungsindex von p' in p'' ist definiert als die natürliche Zahl
$$e(p''/p') := v_{p''}(p'R'').$$
Dabei bezeichne $v_{p''}$ die p''-adische (additive) Bewertung von R''.

Bemerkungen

(i) Nach Definition ist der Verzweigungsindex e(p''/p') gerade der Exponent von p'' in der Primfaktorzerlegung des Erweiterungsideals p'R''.

(ii) Alternativ kann man den Verzweigungsindex e(p''/p') als die natürliche Zahl e beschreiben mit
$$v_{p''}(x) = e\cdot v_{p'}(x) \text{ für jedes } x \in K'^*,$$
d.h. die Einschränkung der p''-adischen Bewertung von K'' auf K' ist gerade das e-fache der p'-adischen Bewertung von K'.

3.3.2 Multiplikativität von Verzweigungsindex und Relativgrad

Seien R, S und T ineinander enthaltene Dedekind-Ringe und
$$p \subseteq q \subseteq r$$
ineinanderliegende maximale Ideale von R bzw. S bzw. T. Dann gilt:

(i) $f(r/p) = f(r/q)\cdot f(q/p)$

(ii) $e(r/p) = e(r/q)\cdot e(q/p)$

Beweis. Zu (i). Folgt aus der Multiplikativität des Körpergrades.

Zu (ii). Aus
$$v_q(x) = e\cdot v_p(x) \text{ für } x \in Q(R)$$
und
$$v_r(y) = e'\cdot v_q(y) \text{ für } y \in Q(S)$$
folgt für $x \in Q(R) \subseteq Q(S)$:
$$\begin{aligned} v_r(x) &= e'v_q(x) \\ &= e'e\cdot v_p(x). \end{aligned}$$
QED.

3.3.3 Verzweigungsindex und Relativitätsgrad beim Übergang zu Quotientenringen

Seien R ein Dedekind-Ring mit dem Quotientenkörper K, $S \subseteq R$ eine multiplikativ abgeschlossene Teilmenge und $p \subseteq R_S$ ein von 0 verschiedenes Primideal des Quotientenrings R_S bezüglich S. Dann ist $p \cap R$ ein von 0 verschiedenes Primideal von R mit
$$f(p/p\cap R) = e(p/p\cap R) = 1.$$
Beweis. Offensichtlich ist mit p auch $p \cap R$ ein Primideal. Wegen

$$(p \cap R)R_S =^{24} p \qquad (1)$$

ist mit p auch $p\cap R$ von 0 verschieden. Nach dem Homomorphiesatz induziert die natürliche Abbildung $R \longrightarrow R_S$ einen injektiven Homomorphismus

$$R/p\cap R \longrightarrow R_S/p. \qquad (2)$$

Da die Primideale p und $p\cap R$ von Null verschieden sind und es sich bei den Ringen um Dedekind-Ringe handelt (nach 1.5.1) sind p und $p\cap R$ maximale Ideale (ebenfalls nach 1.5.1). Insbesondere ist (2) eine Körpererweiterung. Nach Definition besteht der Körper rechts aus Quotienten des Körpers links, d.h. (2) ist ein Isomorphismus. Damit ist aber

$$f(p/p\cap R) = 1.$$

Wegen (1) ist der Exponent von p in der Primfaktorzerlegung des Erweiterungsideals

$$(p \cap R)R_S$$

gleich 1, d.h. es gilt

$$e(p/p\cap R) = 1.$$

QED.

3.3.4 Verzweigungsindex und Relativgrad beim Vervollständigen I

Seien R ein Dedekind-Ring mit dem Quotientenkörper K,

$$p \subseteq R$$

ein maximales Ideal von R und (wie bisher)

$$\overline{R}_p, K_p$$

die Vervollständigungen von R bzw. K bezüglich der p-adischen Topologie. Weiter bezeichne

$$\overline{p} \subseteq \overline{R}_p$$

das Bewertungsideal von K_p. Dann gilt

$$f(\overline{p}/p) = e(\overline{p}/p) = 1.$$

Beweis. Die p-adische Bewertung von K ist gerade die Einchränkung der $\overline{p}$-adischen Bewertung von K_p(vgl. 2.3.3 und 2.3.8). Insbesondere gilt

$$v_{\overline{p}}(\pi) = v_p(\pi) = 1,$$

wenn π einen Parameter der p-adischen Bewertung von K bezeichnet. Damit erzeugt π nicht nur das Bewertungsideal von K sondern auch das von K_p:

$$\begin{aligned} pR_p &= \pi R_p \\ \overline{p} &= \pi\overline{R}_p. \end{aligned}$$

Es folgt

$$\begin{aligned} \overline{p} &= \pi R_p\overline{R}_p \qquad (\text{wegen } R_p \subseteq \overline{R}_p) \\ &= p\overline{R}_p \end{aligned}$$

---

[24] Der Beweis von 1.4.18 (ii) ist für beliebige multiplikativ abgeschlossene Mengen S gültig und nicht nur für solche der Gestalt S = R - p mit p Primideal.

Der Exponent von $\overline{p}$ in der Primfaktorzerlegung von $p\overline{R}_p$ ist damit gleich 1, d.h.

$$e(\overline{p}/p) = 1.$$

Der Verzweigungsindex ist also tatsächlich gleich 1. Wir haben noch den Relativgrad zu berechnen. Weil $pR_p \subseteq \overline{p} \cap R_p$ ineinander liegende Primideale sind und pR_p maximal in R_p ist, gilt sogar

$$pR_p = \overline{p} \cap R_p.$$

Die Inklusin $R_p \hookrightarrow \overline{R}_p$ induziert einen injektiven Homomorphismus

$$R_p/pR_p \hookrightarrow \overline{R}_p/\overline{p} \qquad (1)$$

Jedes Element $\alpha \in \overline{R}_p$ ist Limes einer Folge $\{\alpha_n\}_{n=1,2,\ldots}$ von Elementen aus K. Weil α im Bewertungsring von K_p liegt gilt

$$v_p(\alpha) \geq 0.$$

Wegen $\alpha_n \longrightarrow \alpha$ gilt $v_p(\alpha - \alpha_n) \longrightarrow \infty$, also ist für große n

$$v_p(\alpha_n) = v_p(\alpha - (\alpha - \alpha_n)) = \min(v_p(\alpha), v_p(\alpha - \alpha_n)) = v_p(\alpha) \geq 0.$$

Wir können also annehmen,, die α_n liegen im Bewertugnsring R_p von K. Wegen

$$v_p(\alpha - \alpha_n) \longrightarrow \infty$$

liegt für große n die Differenz $\alpha - \alpha_n$ im Bewertungsideal von K_p,

$$\alpha - \alpha_n \in \overline{p}.$$

Wir haben gezeigt, jedes Element von $\overline{R}_p/\overline{p}$ besitzt einen Repräsentanten in R_p. Mit anderen Worten, die Injektion (1) ist ein Isomorphismus. Es fogt

$f(\overline{p}/pR_p) = 1$,

also

$$\begin{aligned} f(\overline{p}/p) &= f(\overline{p}/pR_p)\cdot f(pR_p/p) && \text{(nach 3.3.2)} \\ &= f(\overline{p}/pR_p)\cdot 1 && \text{(nach 3.3.3)} \\ &= f(\overline{p}/pR_p). \end{aligned}$$

QED.

3.3.5 Verzweigungsindex und Relativgrad beim Vervollständigen II

Seien R' und R" ineinanderliegende Dedekind-Ringe[25],

$$R' \subseteq R''$$

und $p' \subseteq R'$ und $p'' \subseteq R''$ ineinanderliegende maximale Ideale

$$p' \subseteq p''.$$

Weiter seien

$$\overline{p}' \subseteq \overline{p}''$$

---

[25] Genauer: R' sei als Ring mit 1 ein Teilring von R".

die Bewertungsideale der Vervollständigung von Q(R') und Q(R") bezüglich der p'-adischen bzw. p"-adischen Bewertungen. Dann gilt

$$f(p''/p') = f(\overline{p}''/\overline{p}')$$

$$e(p''/p') = e(\overline{p}''/\overline{p}')$$

Beweis. Bezeichnet x den Relativgrad f oder den Verzweigungsindex e, so gilt

$$x(\overline{p}''/p'')\cdot x(p''/p') = x(\overline{p}''/p') = x(\overline{p}''/\overline{p}')\cdot x(\overline{p}'/p).$$

Wegen

$$x(\overline{p}''/p'') = x(\overline{p}'/p)$$

nach 3.3.4 folgt

$$x(p''/p') = x(\overline{p}''/\overline{p}').$$

Es gilt also die Behauptung.
QED.

3.3.6 Vereinbarung: die Beschränkung auf den lokalen vollständigen Fall

Die obigen Ergebnisse zeigen zusammen mit den Ergebnissen von 3.2, daß sich Differente, Diskriminante, Relativgrad, Verzweigungsindex und Norm einer endlichen separablen Erweiterung lokal mit Hilfe der Vervollständigungen berechnen lassen.

Von jetzt an wollen wir bis zum Ende des Kapitels über lokale Körper annehmen, daß

$$R = \mathcal{O}_K$$

ein diskreter Bewertungsring ist, dessen Quotientenkörper

$$K = Q(R)$$

vollständig ist bezüglich der durch R definierten Bewertung von K.

Bemerkungen

(i) Die Situation bleibt erhalten beim Übergang zu endlichen separablen Erweiterungen (nach 2.3.13 und 2.3.10).

(ii) Die Übersetzung der im folgenden erzielten Resultate von der lokalen Situation in die globalen werden wir weitgehend den Leser überlassen.

(iii) Den Bewertungsring R von K werden wir im folgenden auch mit

$$\mathcal{O} = \mathcal{O}_K := R$$

bezeichnen, dessen maximales Ideal mit

$$\wp = \wp_K$$

dessen Restklassenkörper mit

$$\kappa = \kappa_K := \mathcal{O}/\wp$$

und dessen ganze Abschließung in einer endlichen separablen Erweiterungen L/K auch mit

$$\mathcal{O}_L := S.$$

Man beachte, dies ist ein diskreter Bewertungsring (nach 2.3.13). Analog bezeichnen wir mit

$$\wp_L$$

das maximale Ideal von $\mathcal{O}_L$ und mit

$$\kappa_L := \mathcal{O}_L/\wp_L$$

den Restkörper von $\mathcal{O}_L$.

(iv) Im folgenden werden wri oft eine an die lokale vollständige Situation angepasste Bezeichnungweise verweden. So schreiben wir

$e(L/K) := e(\wp_L/\wp)$

$f(L/K) := f(\wp_L/\wp)$

$\mathcal{D}(L/K) := \mathcal{D}(\mathcal{O}_L/\mathcal{O})$

$\delta(L/K) := \delta(\mathcal{O}_L/\mathcal{O})$

$v = v_K := v_\wp$ ($\wp$-adische Bewertung von K)

$v_L := v_{\wp_L}$ ($\wp_L$-adische Bewertung von L)

Wir werden in diesem Kontext auch vom Verzweigungsindex, Relativegrad, der Differente, der Diskriminante von L über K sprechen.

(v) Für die meisten im folgenden bewiesenen Ergebnisse werden wir nicht voraussetzen, daß die endliche Erweiterung L/K separabel ist.

3.3.7 Das Produkt aus Verzweigungsindex und Relativgrad

Seien K ein vollständig bewerteter Körper mit dem Bewertungsring $(\mathcal{O}, \wp)$ und L/K eine endliche separable[26] Körpererweiterung. Dann gilt

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

(d.h. es gilt 3.1.5).

Beweis. Seien π ein Paramter von $\mathcal{O}_L$, d.h.

$$\wp_L = \pi\, \mathcal{O}_L$$

und

$$e := e(L/K),$$

d.h.

$$\wp\mathcal{O}_L = \wp_L^e = \pi^e\mathcal{O}_L.$$

Betrachen wir die exakten Sequenzen

$$0 \longrightarrow \pi^i\mathcal{O}_L/\pi^{i+1}\mathcal{O}_L \longrightarrow \mathcal{O}_L/\pi^{i+1}\mathcal{O}_L \longrightarrow \mathcal{O}_L/\pi^i\mathcal{O}_L \longrightarrow 0.$$

von Moduln über $\mathcal{O} = \mathcal{O}_K$. Diese Moduln werden für $i < e$ annulliert von

$$\pi^e\, \mathcal{O}_L = \wp\mathcal{O}_L,$$

also von $\wp$. Es sind also Vektorräume über $\mathcal{O}/\wp = \kappa$. Wir erhalten damit für deren Dimensionen

$$\dim_\kappa \mathcal{O}_L/\pi^{i+1}\mathcal{O}_L = \dim_\kappa \mathcal{O}_L/\pi^i\mathcal{O}_L + \dim_\kappa \pi^i\mathcal{O}_L/\pi^{i+1}\mathcal{O}_L \text{ für } i = 0, ..., e\text{-}1.$$

Die Multiplikation mit π^i definiert Isomorphismen

$$\mathcal{O}_L \longrightarrow \pi^i\mathcal{O}_L \text{ und } \pi\mathcal{O}_L \longrightarrow \pi^{i+1}\mathcal{O}_L$$

von Moduln über $\mathcal{O}_L$, also einen Isomorphismus

$$\kappa_L = \mathcal{O}_L/\wp\, \mathcal{O}_L = \mathcal{O}_L/\pi\mathcal{O}_L \xrightarrow{\cong} \pi^i\mathcal{O}_L/\pi^{i+1}\mathcal{O}_L$$

Damit bekommt die obige Dimensionsformel die Gestalt

$$\dim_\kappa \mathcal{O}_L/\pi^{i+1}\mathcal{O}_L = \dim_\kappa \mathcal{O}_L/\pi^i\mathcal{O}_L + [\kappa_L : \kappa] \text{ für } i = 0, ..., e\text{-}1.$$

Insbesondere gilt

$$\begin{aligned}\dim_\kappa \mathcal{O}_L\otimes_\mathcal{O}\mathcal{O}/\wp &= \dim_\kappa \mathcal{O}_L/\wp\mathcal{O}_L \\ &= \dim_\kappa \mathcal{O}_L/\pi^e\mathcal{O}_L\end{aligned}$$

---

[26] Die Aussage ist auch ohne die Voraussetzung der Separabilität richtig.

$$= (e-1)\cdot [\kappa_L : \kappa] + \dim_\kappa \mathcal{O}_L/\pi\mathcal{O}_L$$
$$= (e-1)\cdot [\kappa_L : \kappa] + \dim_\kappa \mathcal{O}_L/\wp_L$$
$$= e\cdot [\kappa_L : \kappa]$$
$$= e(L/K)\cdot f(L/K)$$

Nun ist $\mathcal{O}_L$ ein endlich erzeugter Modul über dem diskreten Bewertungsring $\mathcal{O}$ (nach 1.9.3), also eine freier $\mathcal{O}$-Modul. Die Dimension

$$\dim_\kappa \mathcal{O}_L \otimes_{\mathcal{O}} \mathcal{O}/\wp = \mathrm{rk}_{\mathcal{O}}\, \mathcal{O}_L$$

ist somit gerade die maximale Anzahl $\mathcal{O}$-linear Unabhängiger Elemente von $\mathcal{O}_L$. Wegen

$$\mathcal{O}_L\cdot K = S\cdot K = L$$

(vgl. zum Beispiel die Anmerkungen zu 3.2.1) folgt

$$\dim_\kappa \mathcal{O}_L \otimes_{\mathcal{O}} \mathcal{O}/\wp = \dim_K L = [L:K]$$

QED.

3.3.8 Vergleich der Einheitengruppen I

Seien K ein vollständig bewerteter Körper mit dem Bewertungsring $(\mathcal{O}, \wp)$ und L/K eine endliche Körpererweiterung. Dann ist das folgende Diagramm kommutativ und besitzt exakte Zeilen.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathcal{O}_K^* & \hookrightarrow & K^* & \overset{v_K}{\twoheadrightarrow} & \mathbb{Z} & \longrightarrow & 0 \\
 & & \cap & & \cap & & \downarrow e & & \\
0 & \longrightarrow & \mathcal{O}_L^* & \hookrightarrow & L^* & \overset{v_L}{\twoheadrightarrow} & \mathbb{Z} & \longrightarrow & 0
\end{array}$$

Dabei seien e = e(L/K) der Verweigungsindex und v_K und v_L die additiven Bewertungen von K bzw. L.

Beweis. Die Zeilen des Diagramms sind exakt nach Definition des Begriffs Bewertungsring einer additiven Bewertung (vgl. 1.4.8). Das linke Quadrat ist trivialerweise kommutativ, und das rechte auf Grund der Definition des Begriffs Verzweigungsindex.

QED.

3.3.9 Vergleich der Einheitengruppen II

Seien K ein vollständig bewerteter Körper mit dem Bewertungsring $(\mathcal{O}, \wp)$ und L/K eine endliche separable Körpererweiterung. Dann ist das folgende Diagramm kommutativ und besitzt exakte Zeilen.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathcal{O}_L^* & \hookrightarrow & L^* & \overset{v_L}{\twoheadrightarrow} & \mathbb{Z} & \longrightarrow & 0 \\
 & & N_{L/K}\downarrow & & \downarrow N_{L/K} & & \downarrow f & & \\
0 & \longrightarrow & \mathcal{O}_K^* & \hookrightarrow & K^* & \overset{v_K}{\twoheadrightarrow} & \mathbb{Z} & \longrightarrow & 0
\end{array}$$

d.h. es gilt

$$f\cdot v_L(x) = v_K(N_{L/K}(x))$$

für jedes $x \in L$, d.h.

$$N_{L/K}(\wp_L) = \wp_K^f.$$

Dabei seien $f = f(L/K)$ der Relativgrad und v_K und v_L die additiven Bewertungen von K bzw. L und $\wp_L$ und $\wp_K$ die zugehörigen Bewertungsideale.
Beweis. Für die gewöhnliche Norm $N_{L/K}$ der Körpererweiterung L/K gilt[27]

$$N_{L/K}(\mathcal{O}_L^*) \subseteq \mathcal{O}^*. \tag{2}$$

Die Abbildungen des Diagramms sind damit wohldefiniert, und das linke Viereck ist kommutativ. Weiter gilt, wenn e den Verzweigungsindex $e := e(\wp_L \mid \wp_K)$ bezeichnet,

$$\begin{aligned} e\cdot v_K(N_{L/K}(x)) &= v_L(N_{L/K}(x)) && \text{(Definition von e)} \\ &=^{28} [L:K]\cdot v_L(x) && \\ &= e\cdot f\cdot v_L(x) && \text{(nach 3.3.7)} \end{aligned}$$

Division durch e ($\neq 0$) liefert

$$v_K(N_{L/K}(x)) = f\cdot v_L(x),$$

d.h. das rechte Viereck ist ebenfalls kommutativ. Setzt man für x einen Parameter π_L von $\mathcal{O}_L$, so erhält man aus der letzten Identität

$$v_K(N_{L/K}(\pi_L)) = f\cdot v_L(\pi_L) = f,$$

d.h.. $N_{L/K}(\pi_L)$ ist die f-te Potenz eines Parameters von $\mathcal{O}$. Es folgt

$$\begin{aligned} \wp_K^f &= N_{L/K}(\pi_L)\mathcal{O} && \\ &= N_{L/K}(\pi_L \mathcal{O}_L) && \text{(Norm eines Hauptideals, 3.2.2).} \\ &= N_{L/K}(\wp_L). && \text{(Definition von } \pi_L\text{)} \end{aligned}$$

Damit besteht auch die letzte der behaupteten Identitäten.
QED.

3.3.10 Vergleich der Spuren auf K und κ

Seien K ein vollständig bewerteter Körper mit dem Bewertungsring $(\mathcal{O}, \wp)$ und dem Restekörper $\kappa = \mathcal{O}/\wp$ und L/K eine endliche separable Körpererweiterung. Dann ist das folgende Diagramm kommutativ.[29]

$$\begin{array}{ccc} \mathcal{O}_L & \longrightarrow & \kappa_L \\ {\scriptstyle Tr_{L/K}}\downarrow & & \downarrow{\scriptstyle e\cdot Tr_{\kappa_L/\kappa}} \\ \mathcal{O} & \longrightarrow & \kappa \end{array}$$

---

[27] Jedes Element von $\mathcal{O}_L^*$ ist ganz über $\mathcal{O}^*$ und ungleich Null. Dasselbe gilt auch für die Konjugierten dieses Elements, und damit auch für deren Produkt, d.h. für die Norm des Elements. Die Norm des Elements liegt aber auch in K, und $\mathcal{O}$ ist ganz abgeschlossen in K.

[28] Alle Konjugierten von x haben denselben Wert bezüglich einer Fortsetzung von v_L auf eine Galois-Erweiterung von K, welche L enthält (vgl. 2.3.8).

[29] Man beachte die Spur bildet Elemente aus $\mathcal{O}_L$ in $\mathcal{O}$ ab (weil die Konjugierten eines über $\mathcal{O}$ ganzen Elements ganz sind über $\mathcal{O}$ und $\mathcal{O}$ ganz abgeschlossen ist in K).

Dabei bezeichne

$$e = e(\wp_L | \wp)$$

den Verzweigungsindex von L über K, und die waagerechten Pfeile seien die natürlichen Abbildungen auf den Faktorring. Mit anderen Worten, es gilt

$$\overline{\mathrm{Tr}_{L/K}(\alpha)} = e\bullet \mathrm{Tr}_{\kappa_L/\kappa}(\overline{\alpha})$$

für jedes $\alpha \in \mathcal{O}_L$, wenn man den Übergang zu den Restklassen modulo $\wp_L$ bzw. modulo $\wp$ mit einem Querstrich bezeichnet.

Beweis. Wir betrachten zunächst eine etwas allgemeinere Situation.Seien k ein Körper und A eine kommutative k-Algebra, welche als k-Vektorraum endlich-dimensional ist und folgende Eigenschaften besitzt.

1. A ist ein lokaler Ring mit dem maximalen Ideal N und dem Restekörper B = A/N.
2. Es gibt eine natürliche Zahl mit $N^e = 0$ und $N^{e-1} = 0$.
3. Für $i < e$ gilt $N^i/N^{i+1} \cong B$.

Wir zeigen in dieser Situation, daß

$$\mathrm{Tr}_{A/k}(a) = e\bullet \mathrm{Tr}_{B/k}(a \bmod N)$$

gilt für jedes $a \in A$.

Betrachten wir die exakte Sequenz von A-Moduln (welche gleichzeitig eine exakte Sequenz von endlich-dimensionalen k-Vektorräumen ist).

$$0 \longrightarrow N^i/N^{i+1} \longrightarrow A/N^{i+1} \longrightarrow A/N^i \longrightarrow 0.$$

Die Multiplikation mit a definiert auf diesen k-Vektorräumen jeweils eine k-lineare Abbildung, die wir mit φ_i, ψ_{i+1} und ψ_i bezeichnen wollen. Diese Abbildungen setzen sich zu einem kommutativen Diagramm

$$\begin{tikzcd}
0 \arrow[r] & N^i/N^{i+1} \arrow[r] \arrow[d, "\varphi_i"] & A/N^{i+1} \arrow[r] \arrow[d, "\psi_{i+1}"] & A/N^i \arrow[r] \arrow[d, "\psi_i"] & 0 \\
0 \arrow[r] & N^i/N^{i+1} \arrow[r] & A/N^{i+1} \arrow[r] & A/N^i \arrow[r] & 0
\end{tikzcd}$$

mit exakten Zeilen zusammen. Die Kommutivität des linken Vierecks bedeutet, daß die mittlere vertikale Abbildung ψ_{i+1} den Unterraum N^i/N^{i+1} in sich abbildet. Wählt man eine Basis von A/N^{i+1}, welche eine Basis dieses Unterraums fortsetzt, so bedeutet dies, die Matrix von ψ_{i+1} zerfällt in vier Blöcke, wobei die beiden diagonalen Blöcke gerade die Matrizen von φ_i und ψ_i sind und einer der beiden anderen Blöcke die Nullmatrix ist. Es gilt deshalb

$$\mathrm{Tr}\,\psi_{i+1} = \mathrm{Tr}\,\varphi_i + \mathrm{Tr}\,\psi_i \text{ (und } \det \psi_{i+1} = \det \varphi_i \bullet \det \psi_i\text{)} \tag{1}$$

Wegen Eigenschaft 3 ist φ_i isomorph zu Multiplikation mit a auf B, d.h. es ist Tr φ_i gleich $\mathrm{Tr}_{B/k}(a \bmod N)$, also

$$\mathrm{Tr}\,\psi_{i+1} = \mathrm{Tr}_{B/k}(a \bmod N) + \mathrm{Tr}\,\psi_i$$

also

$$\mathrm{Tr}\,\psi_e = e\bullet \mathrm{Tr}_{B/k}(a \bmod N) + \mathrm{Tr}\,\psi_0$$

Weil ψ_0 die lineare Abbildung des 0-Vektorraums ist, folgt

$$\mathrm{Tr}\,\psi_e = e\bullet \mathrm{Tr}_{B/k}(a \bmod N).$$

Wegen $N^e = 0$ ist ψ_e die Multiplikation mit a auf A, d.h. es gilt wie behauptet

$$\mathrm{Tr}_{A/k}(a) = e\bullet \mathrm{Tr}_{B/k}(a \bmod N).$$

Betrachten wir jetzt den Spezialfall

$$A := \mathcal{O}_L/\wp\mathcal{O}_L.$$

Bedingung 1 ist erfüllt mit

$$N = \wp_L/\wp \text{ und } B = \mathcal{O}_L/\wp_L = \kappa_L.$$

Bedingung 2 ist erfüllt mit

$$e = e(\wp_L|\wp)$$

(mit diesem e gilt $\wp\mathcal{O}_L = \wp_L^e$ nach Definition des Verzweigungsindex). Bedingung 3 ist erfüllt weil $\mathcal{O}_L$ ein Integritätsbereich ist und $\wp_L$ ein Hauptideal.[30] Die bewiesene Identität bekommt für den betrachteten Spezialfall die Gestalt

$$\mathrm{Tr}_{A/k}(a) = e\bullet \mathrm{Tr}_{\kappa_L/\kappa}(a \bmod \wp_L) \text{ für } a \in \mathcal{O}_L$$

Nun ist der endlich erzeugte $\mathcal{O}$-Modul $\mathcal{O}_L$ dem diskreten Bewertungsring $\mathcal{O}$ frei. Die Matrix der Multiplikation mit a auf $A = \mathcal{O}_L/\wp\mathcal{O}_L$ entsteht aus der der Multiplikation mit a auf $\mathcal{O}_L$ durch Übergang zu den Restklassen modulo $\wp$, d.h.

$$\mathrm{Tr}_{A/k}(a) = \mathrm{Tr}_{\mathcal{O}_L/\mathcal{O}}(a) \bmod \wp = \mathrm{Tr}_{L/K}(a) \bmod \wp.$$

Unsere Identität bekommt die Gestalt

$$\mathrm{Tr}_{L/K}(a) \bmod \wp = e\bullet \mathrm{Tr}_{\kappa_L/\kappa}(a \bmod \wp_L) \text{ für } a \in \mathcal{O}_L.$$

Das ist aber gerade die Behauptung.
QED.

3.3.11 Vergleich der Normen auf K und κ

Seien K ein vollständig bewerteter Körper mit dem Bewertungsring $(\mathcal{O}, \wp)$ und dem Restekörper $\kappa = \mathcal{O}/\wp$ und L/K eine endliche separable Körpererweiterung. Dann ist das folgende Diagramm kommutativ.[31]

---

[30] Multiplikation mit der i-ten Potenz des Erzeugers π von $\wp_L$ definiert Isomorphismen

$$\mathcal{O}_L \longrightarrow \wp_L^i \text{ und } \wp_L \longrightarrow \wp_L^{i+1},$$

also einen Isomorphismus

$$\kappa_L = \mathcal{O}_L/\wp_L \longrightarrow \wp_L^i/\wp_L^{i+1} \cong N^i/N^{i+1}$$

(für jedes $i < e$).

[31] Man beachte die Spur bildet Elemente aus $\mathcal{O}_L$ in $\mathcal{O}$ ab (weil die Konjugierten eines über $\mathcal{O}$ ganzen Elements ganz sind über $\mathcal{O}$ und $\mathcal{O}$ ganz abgeschlossen ist in K).

$$\begin{array}{ccc} \mathcal{O}_L & \longrightarrow & \kappa_L \\ N_{L/K}\downarrow & & \downarrow N_{\kappa_L^e/\kappa} \\ \mathcal{O} & \longrightarrow & \kappa \end{array}$$

Dabei bezeichne

$$e = e(\wp_L|\wp)$$

den Verzweigungsindex von L über K, und die waagerechten Pfeile seien die natürlichen Abbildungen auf den Faktorring. Mit anderen Worten, es gilt

$$\overline{N_{L/K}(\alpha)} = N_{\kappa_L/\kappa}(\bar{\alpha})^e$$

für jedes $\alpha \in \mathcal{O}_L$, wenn man den Übergang zu den Restklassen modulo $\wp_L$ bzw. modulo $\wp$ mit einem Querstrich bezeichnet.

Beweis. Der Beweis ergibt sich aus dem Beweis von 3.3.10 indem man an allen Stellen die Betrachtung der Spur durch die der Norm bzw. der Determinante ersetzt. So erhält man anstelle von Formel (1) im Beweis von 3.3.10 die analoge Formel

$$\det \psi_{i+1} = \det \varphi_i \cdot \det \psi_i.$$

Daraus und aus der Determinanten-Definition der Norm ergibt sich die Behauptung.
QED.

3.3.12 Der Wert der Differente und der Verzweigungsindex

Seien K ein vollständig bewerteter Körper mit dem Bewertungsring $(\mathcal{O}, \wp)$ und dem Restekörper $\kappa = \mathcal{O}/\wp$ und L/K eine endliche separable Körpererweiterung. Dann gilt

$$v_L(\mathcal{D}(\mathcal{O}_L/\mathcal{O})) \ge e(L/K) - 1.$$

Beweis. Wir betrachten die exakten Sequenzen

$$0 \longrightarrow N^i/N^{i+1} \longrightarrow N/N^{i+1} \longrightarrow N/N^i \longrightarrow 0.$$

mit $A = \mathcal{O}_L/\wp\mathcal{O}_L$ und $N := \wp_L/\wp\mathcal{O}_L$ und beachten, daß wie in 3.3.10 gezeigt,

$$N^i/N^{i+1} \cong B/N \cong \mathcal{O}_L/\wp_L = \kappa_L.$$

gilt. Wir betrachten die $\mathcal{O}_L$-Moduln der Sequenz als $\mathcal{O}$-Moduln. Weil sie von $\wp$ annulliert werden, sind es Moduln über $\mathcal{O}/\wp = \kappa$, d.h. κ-Vektorräume. Für ihre Dimensionen erhalten wir

$$\begin{aligned} \dim_\kappa N/N^{i+1} &= \dim_\kappa N^i/N^{i+1} + \dim_\kappa N/N^i \\ &= \dim_\kappa \kappa_L + \dim_\kappa N/N^i \\ &= f(L/K) + \dim_\kappa N/N^i \end{aligned}$$

Wegen $N^e = 0$ folgt

$$\begin{aligned} \dim_\kappa N &= \dim_\kappa N/N^e \\ &= f\cdot(e-1) + \dim_\kappa N/N \\ &= f\cdot(e-1) \end{aligned}$$

mit

$$e = e(L/K)$$

$f \qquad = f(L/K).$

Wir können daher eine Basis des κ-Vektorraums $A = \mathcal{O}_L/\wp\mathcal{O}_L$ wählen, deren $f\bullet(e-1)$ erste Elemente den Unterraum $N = \wp_L/\wp\mathcal{O}_L$ erzeugen. Wir fixieren Repräsentanten α_i dieser Basis in $\mathcal{O}_L$, und zwar derart, daß die ersten $f\bullet(e-1)$ der α_i in $\wp_L$ liegen,

$$\alpha_i \in \wp_L \text{ für } i = 1, \dots, f\bullet(e-1).$$

Nach Konstruktion bilden die α_i modulo $\wp\mathcal{O}_L$ ein Erzeugendensystem des $\mathcal{O}$-Moduls $\mathcal{O}_L$, d.h.

$$\mathcal{O}_L = \sum_i \mathcal{O}\alpha_i + \wp\mathcal{O}_L$$

Indem wir diesen Ausdruck wiederholt in sich einsetzen, erhalten wir

$$\mathcal{O}_L = \sum_i \mathcal{O}\alpha_i + \wp^\ell\mathcal{O}_L \text{ für } \ell = 1, 2, 3, \dots$$

Für jedes Elemente $\alpha \in \mathcal{O}_L$ gibt es ein $\alpha' \in \sum_i \mathcal{O}\alpha_i$ mit $\alpha-\alpha' \in \wp^\ell\mathcal{O}_L$ mit ℓ beliebig groß, d.h. mit $v_L(\alpha-\alpha')$ beliebig groß, d.h. mit $|\alpha-\alpha'|_L$ beliebig klein. Der Teilmodul $\sum_i \mathcal{O}\alpha_i$ liegt dicht im $\mathcal{O}$-Modul $\mathcal{O}_L$. Nun ist dieser Teilmodul endlich erzeugt über dem diskreten Bewertungsring $\mathcal{O}$, also frei über $\mathcal{O}$, also vollständig, also abgeschlossen. Deshalb gilt

$$\mathcal{O}_L = \sum_i \mathcal{O}\alpha_i .$$

Wir haben ein $\mathcal{O}$-linear unabhängiges[32] Erzeugendensystem von $\mathcal{O}_L$ über $\mathcal{O}$ konstruiert, dessen $f\bullet(e-1)$ erste Elemente in $\wp_L$ liegen. Dieses Erzeugendensystem können wir zur Berechnung der Diskriminante verwenden (vgl. 1.6.13 (iii)):

$$\delta(L/K) = \delta(\mathcal{O}_L/\mathcal{O}) = \det(Tr_{L/K}(\alpha_i\alpha_j))\mathcal{O}$$

Für $i \le f\bullet(e-1)$ gilt nach Konstruktion $\alpha_i\alpha_j \in \wp_L$. Nach 3.3.10 folgt

$$Tr_{L/K}(\alpha_i\alpha_j) \bmod \wp = e\bullet Tr_{\kappa_L/\kappa}(\alpha_i\alpha_j \bmod \wp_L) = e\bullet Tr_{\kappa_L/\kappa}(0) = 0,$$

d.h. $Tr_{L/K}(\alpha_i\alpha_j) \in \wp$, d.h. die ersten $f\bullet(e-1)$ Zeilen der Matrix $(Tr_{L/K}(\alpha_i\alpha_j))$ liegen also in $\wp$. Die Determinante dieser Matrix liegt somit in $\wp^{f\bullet(e-1)}$, d.h.

$$v_K(\delta(L/K)) \ge f\bullet(e-1).$$

Es folgt

$$v_L(\mathcal{D}(L/K)) = \frac{1}{f} v_K(N_{L/K}(\mathcal{D}(L/K))) \qquad \text{(nach 3.3.9)}$$

---

[32] Die Koeffizienten einer nicht-trivialen linearen Relation der α_i könnte man so mit einer Potenz des Parameters multiplizieren, daß man daraus eine nicht-triviale Relatioin der Restklassen der α_i über κ erhielte.

$= \frac{1}{f} v_K(\delta(L/K))$ (nach 3.2.8)

$\geq \frac{1}{f} \cdot f \cdot (e-1)$ (wie gerade bewiesen)

$= e - 1.$

QED.

3.3.13 Definition: Unverzweigte Erweiterungen

Seien K ein vollständig bewerteter Körper mit dem Bewertungsring ($\mathcal{O}$, $\wp$) und dem Restekörper $\kappa = \mathcal{O}/\wp$ und L/K eine endliche separable Körpererweiterung. Dann heißt L unverzweigt über K, wenn die beiden folgenden Bedingungen erfüllt sind.

(i) $e(L/K) = 1$.

(ii) κ_L ist separabel über κ.

Im nicht-lokalen Fall (d.h. für nicht notwending vollständige Körper) bekommt diese Defintion die folgende Gestalt.

Seien K ein diskret bewerteter Körper mit dem Bewertungsideal p, L/K eine endliche separable Körpererweiterung und P ein über p liegenden maximales Ideal (der ganzen Abschließung des Bewertungsrings von p in L). Dann heißt p unverzweigt in P, wenn die Vervollständigung L_P unverzweigt ist über der Vervollständigung K_p, d.h. wenn folgende beiden Bedingungen erfüllt sind.

(i) $e(P/p) = 1$

(ii) κ_P ist separabel über κ_p.

3.3.14 Charakterisierung der unverzweigen Erweiterungen

Seien K ein vollständig bewerteter Körper mit dem Bewertungsring ($\mathcal{O}$, $\wp$) und dem Restekörper $\kappa = \mathcal{O}/\wp$ und L/K eine endliche separable Körpererweiterung.Dann sind folgende Aussagen äquivalent.

(i) L/K ist unverzweigt.

(ii) $\delta(L/K) = \mathcal{O}$.

Im allgemeinen ist die Diskriminante ein ganzes Ideal, d.h.

$$\delta(L/K) \subseteq \mathcal{O}.$$

Beweis. 1. Schritt. Dikriminante und Differente einer Körpererweiterung sind ganze Ideale.

Nach Definition 1.6.12 ist

$$\delta(L/K) = \delta(\mathcal{O}_L/\mathcal{O}) = (D(\mathcal{O}_L):\mathcal{O})$$

und

$$D(\mathcal{O}_L) = \{x \in L \mid Tr_{L/K}(x\mathcal{O}_L) \subseteq \mathcal{O}\}$$

enthält $\mathcal{O}_L$ (wegen $Tr(\mathcal{O}_L) \subseteq \mathcal{O}$), d.h. es ist

$$\delta(L/K) \subseteq \mathcal{O}_L.$$

Die Diskriminante ist also ein ganzes Ideal. Man beachte, die Differente ist nach Bemerkung 3.2.7 (i) ebenfalls ein ganzes Ideal.

$$\mathcal{D}(L/K) \subseteq \mathcal{O}.$$

2. Schritt. $\delta(L/K) = \mathcal{O} \Leftrightarrow \mathcal{D}(L/K) = \mathcal{O}_L$

Nach 3.2.8 ist die Diskriminante gerade die Norm der Differente,

$$\delta(L/K) = N_{L/K}(\mathcal{D}(L/K)),$$

und als Ideal des diskreten Bewertungsrings $\mathcal{O}_L$ ist die Diskriminaten ein Hauptideal, sagen wir

$$\mathcal{D}(L/K) = x\mathcal{O}_L.$$

Auf Grund der Formel 3.2.2 für die Norm eines Hauptideals folgt

$$\delta(L/K) = N_{L/K}(x)\mathcal{O}.$$

Zum Beweis der Behauptung des zweiten Schritts reicht es zu zeigen, x ist genau dann eine Einheit in $\mathcal{O}_L$, wenn $N_{L/K}(x)$ eine Einheit in $\mathcal{O}$ ist, d.h. es reicht zu zeigen

$$v_L(x) = 0 \Leftrightarrow v_K(N_{L/K}(x)) = 0.$$

Das folgt aber aus der Formel

$$v_K(N_{L/K}(x)) = f\bullet v_L(x),$$

von 3.3.9.

<u>3. Schritt</u>. Im Fall $\delta(L/K) = \mathcal{O}$ gilt $e(L/K) = 1$.

Nach dem zweiten Schritt gilt mit $\delta(L/K) = \mathcal{O}$ auch $\mathcal{D}(L/K) = \mathcal{O}_L$, also

$$0 = v_L(\mathcal{D}(L/K)) \geq e(L/K) - 1$$

(nach 3.3.12), also

$$e(L/K) = 1.$$

<u>4. Schritt</u>. Im Fall $e(L/K) = 1$ gilt $\delta(L/K) = \mathcal{O} \Leftrightarrow \kappa_L/\kappa$ separabel.

Weil $\mathcal{O}$ ein diskreter Bewertungsring ist und L/K eine endliche separable Erweiterung, so ist $\mathcal{O}_L$ ein endlich erzeugter freier $\mathcal{O}$-Modul. Sei

$$\{\alpha_1,...,\alpha_n\} \subseteq \mathcal{O}_L$$

ein linear unabhängiges Erzeugendensystem von $\mathcal{O}_L$ über $\mathcal{O}$. Dann gilt

$$\begin{aligned} n &= [L:K] \\ &= e(L/K)\bullet f(L/K) && \text{(nach 3.3.7)} \\ &= f(L/K) && \text{(nach Voraussetzung)} \\ &= [\kappa_L:\kappa] && \text{(nach Definition von f)} \end{aligned}$$

Das freie Erzeugendensystem kann man zur Berechnung der Diskriminante verwenden (nach 1.6.13 (iii)):

$$\delta(L/K) = \det \mathrm{Tr}_{L/K}(\alpha_i\alpha_j)\mathcal{O}.$$

Damit gilt

$$\begin{aligned} \delta(L/K) = \mathcal{O} &\Leftrightarrow \det \mathrm{Tr}_{L/K}(\alpha_i\alpha_j) \text{ ist Einheit von } \mathcal{O} \\ &\Leftrightarrow 0 \neq \det (\mathrm{Tr}_{L/K}(\alpha_i\alpha_j)) \bmod \wp \\ &\Leftrightarrow^{33}\ 0 \neq \det (\mathrm{Tr}_{L/K}(\alpha_i\alpha_j) \bmod \wp) \\ &\Leftrightarrow 0 \neq \det (\mathrm{Tr}_{\kappa_L/\kappa}(\alpha_i\alpha_j \bmod \wp_L) \end{aligned}$$

---

[33] Die Determinante ist ein Polynom und die natürliche Abbildung $\mathcal{O} \longrightarrow \mathcal{O}/\wp$ ein Ringhomomorphismus.

$$\Leftrightarrow 0 \neq \det(\mathrm{Tr}_{\kappa_L/\kappa}(\bar\alpha_i\bar\alpha_j))$$

mit

$$\bar\alpha_i = \alpha_i \bmod \wp_L \in \kappa_L.$$

Die Bedingung

$$\det(\mathrm{Tr}_{\kappa_L/\kappa}(\bar\alpha_i\bar\alpha_j)) \neq 0$$

bedeutet, daß die $\bar\alpha_i$ linear unabhängig über κ sein müssen: eine lineare Abhängigkeit der $\bar\alpha_i$ hätte eine lineare Abhängigkeit der Zeilen der Matrix der $\mathrm{Tr}_{\kappa_L/\kappa}(\bar\alpha_i\bar\alpha_j)$ zur Folge[34], d.h. die Determinante wäre Null. Damit ist die Determinante der $\mathrm{Tr}_{\kappa_L/\kappa}(\bar\alpha_i\bar\alpha_j)$ aber gerade die Determinanter der durch die Spur definieren Bilinearform. Wir haben damit gezeigt,

$$\delta(L/K) = \mathcal{O} \quad \Leftrightarrow \mathrm{Tr}_{\kappa_L/\kappa} \text{ definiert eine nicht-entartete Bilinearform } \kappa_L\times\kappa_L \longrightarrow \kappa.$$

Nach 1.8.10 und 1.8.13 ist die Bedingung rechts aber gerade gleichbedeutend mit der Separablität der Körpererweiterungen κ_L/κ.

Die Behauptung folgt jetzt aus dem 3. und 4. Schritt.

QED.

Bemerkung

Die nachfolgende Aussage übersetzt den gerade bewiesenen Satz aus der lokalen in die globale Situation.

3.3.15 Charakterisierung der Unverzweigtheit (globaler Fall)

Seien R ein Dedekind-Ring mit dem Quotientenkörper K, L/K eine endliche separable Körpererweiterung und S die ganze Abschließung von R in L.

$$\begin{array}{ccc} K & \subseteq & L \\ \cup & & \cup \\ R & \subseteq & S \end{array}$$

Weiter sei $p \subseteq R$ eine von Null verschiedenes Primideal von R. Dann sind folgende Aussagen äquivalent.

(i) p ist <u>unverzweigt</u> in L, d.h. für jedes über p liegende Primideal $P \subseteq S$ ist p unverweigt in P.

(ii) p ist kein Teiler der Diskriminante von $\delta(S/R)$, d.h. kommt nicht in der Primfaktoerzerlegung von $\delta(S/R)$ vor, d.h. $\delta(S/R) \not\subseteq p$.

Beweis. Sei $P \subseteq S$ ein über p liegendes Primideal von S. Wie bisher bezeichen wir mit

$$\bar R_p, K_p, \bar S_P, L_P$$

die Vervollständigungen von R, K, S, L bezüglich der p-adischen bzw. P-adischen Topologie. Dann gilt

$$\text{(ii)} \quad \Leftrightarrow \quad \delta(S/R) \not\subseteq p$$

[34] Weil die Spur κ-linear ist.

$\Leftrightarrow \quad \delta(S/R)\overline{R}_p \not\subseteq p\overline{R}_p$ (weil $p\overline{R}_p$ über p liegt)

$\Leftrightarrow \quad \prod_{P|p} \delta(\overline{S}_P/\overline{R}_p) \not\subseteq p\overline{R}_p$ (nach 3.2.9(ii))

$\Leftrightarrow$[35] $\quad \prod_{P|p} \delta(\overline{S}_P/\overline{R}_p) = \overline{R}_p$

$\Leftrightarrow$[36] $\quad \delta(\overline{S}_P/\overline{R}_p) = \overline{R}_p$ für jedes $P\subseteq S$ über p

$\Leftrightarrow$ p ist unverzweigt in P für jedes $P\subseteq S$ über p.

Die letzte Äquivalenz ergibt isch aus 3.3.14 und der Definition der Unverzweigtheit im globalen Fall.
QED.

3.3.16 Folgerung: fast alle Stellen sind unverzweigt (globaler Fall)

Seien R ein Dedekind-Ring mit dem Quotientenkörper K, L/K eine endliche separable Körpererweiterung und S die ganze Abschließung von R in L.

$$\begin{array}{ccc} K & \subseteq & L \\ \cup & & \cup \\ R & \subseteq & S \end{array}$$

Dann ist fast jedes von Null verschiedene Primideal $p \subseteq R$, d.h. jedes mit eventualler Ausnahme von endlich vielen, unverzweigt in L.
Beweis. Das folgt aus 3.3.15 und der Tatsache, daß in der Primfaktorzerlegung der Diskriminante $\delta(S/R)$ nur endlich viele Primideale vorkommen.
QED.

3.3.17 Definition: zahm verzweigte Erweiterungen

Seien K ein vollständig bewerteter Körper mit dem Bewertungsring $(\mathcal{O}, \wp)$ und dem Restekörper $\kappa = \mathcal{O}/\wp$ und L/K eine endliche separable Körpererweiterung. Dann heißt L zahm verzweigt über K, wenn die beiden folgenden Bedingungen erfüllt sind.

(i) Die Charakteristik von κ ist kein Teiler des Verzweigungsindex e(L/K).

(ii) κ_L ist separabel über κ.

Andernfalls heißt K/L wild verzweigt .

Im nicht-lokalen Fall (d.h. für nicht notwending vollständige Körper) bekommt diese Defintion die folgende Gestalt.

Seien K ein diskret bewerteter Körper mit dem Bewertungsideal p, L/K eine endliche separable Körpererweiterung und P ein über p liegenden maximales Ideal (der ganzen Abschließung des Bewertungsrings von p in L). Dann heißt p unverzweigt in P, wenn die Vervollständigung L_P unverzweigt ist über der Vervollständigung K_p, d.h. wenn folgende beiden Bedingungen erfüllt sind.

(i) Die Charakteristik von κ_p ist kein Teiler von e(P/p)

---

[35] $\overline{R}_p$ ist ein lokaler Ring mit dem maximalen Ideal $p\overline{R}_p$

[36] Für jedes P gilt $\delta(\overline{S}_P/\overline{R}_p) \subseteq \overline{R}_p$. Wäre einer der Faktoren echt, so auch deren Produkt.

(ii) κ_P ist separabel über κ_p.

3.3.18 Charakterisierung der zahm verzweigten Erweiterungen

Seien K ein vollständig bewerteter Körper mit dem Bewertungsring $(\mathcal{O}, \wp)$ und dem Restekörper $\kappa = \mathcal{O}/\wp$ und L/K eine endliche separable Körpererweiterung. Dann sind folgende Bedingungen äquivalent.

(i) L/K ist zahm verzweigt.

(ii) $Tr_{L/K}(\mathcal{O}_L) = \mathcal{O}$.

(iii) $v_L(\mathcal{D}(K/L)) = e-1$.

Beweis. 1. Schritt. (i) $\Rightarrow$ (ii).

Nach 3.2.10 gilt

$$\overline{Tr_{L/K}(\alpha)} = e\bullet Tr_{\kappa_L/\kappa}(\bar{\alpha}) \tag{1}$$

für jedes $\alpha\in\mathcal{O}_L$ mit e := e(L/K). Nach Voraussetzung ist κ_L/κ eine separable Erweiterung, d.h. die durch $Tr_{\kappa_L/\kappa}$ ist nicht entartet (vgl. 1.8.10). Weil e außerdem teilerfremd zur Charakteristik von κ ist, gibt es somit ein $\alpha \in \mathcal{O}_L$ derart, daß die rechte Seite von (1) ungleich Null ist, d.h.

$$Tr_{L/K}(\alpha) \in \mathcal{O}$$

ist eine Einheit von $\mathcal{O}$. Weil die Spur $Tr_{L/K}$ eine K-lineare, also auch $\mathcal{O}$-lineare, Abbildung, ist $Tr_{L/K}(\mathcal{O}_L)$ ein Ideal von $\mathcal{O}$, welches eine Einheit enthält, d.h. es gilt (ii).

2. Schritt. (ii) $\Rightarrow$ (i).

Wir betrachten weiterhin die Formel (1). Nach Voraussetzung gibt es ein $\alpha\in\mathcal{O}_L$ derart, daß die linke Seite von (1) ungleich Null wird. Deshalb gilt dasselbe für die rechte Seite. Insbesondere ist

$$e = e(L/K)$$

teilerfremd zur Charakteristik von κ und es ist

$$Tr_{\kappa_L/\kappa}(\bar{\alpha}) \neq 0.$$

Die Spur $Tr_{\kappa_L/\kappa}$ ist somit nicht identisch Null. Nach 1.8.13 ist dies nur möglich, wenn κ_L über κ separabel ist. Zusammen erhalten wir, die Erweiterung L/K ist zahm verwzeigt.

3. Schritt. (ii) $\Leftrightarrow$ (iii).

Die Spur $Tr_{L/K}$ ist K-linear, d.h. es gilt

$$Tr_{L/K}(\mathcal{O}_L\bullet\alpha) = Tr_{L/K}(\mathcal{O}_L)\bullet\alpha$$

für jeds $\alpha\in K$. Die Elemente der linken Seite liegen genau dann in $\mathcal{O}$, wenn α im Dual von $\mathcal{O}_L$ liegt. Die Elemente der rechten Seiten liegen genau dann in $\mathcal{O}$, wenn α im Inversen von $Tr_{L/K}(\mathcal{O}_L)$ liegt. Es ist also

$$\mathrm{Tr}_{L/K}(\mathcal{O}_L)^{-1} = D_{\mathcal{O}}(\mathcal{O}_L) \cap K = \mathcal{D}(L/K)^{-1} \cap K \qquad (2)$$

Wir setzen

$$r := v_K(\mathrm{Tr}_{L/K}(\mathcal{O}_L))$$

$$v := v_L(\mathcal{D}) \text{ mit } \mathcal{D} := \mathcal{D}(L/K).$$

Unser Ziel ist es, geeignete Relationen zwischen r und v zu finden. Dazu wählen wir lokale Parameter π und ρ von R bzw. S,

$$p = \pi\mathcal{O}$$

$$P = \rho\mathcal{O}_L$$

Wir schreiben

$$\pi = u\bullet\rho^e \text{ mit } e = e(L/K) \text{ und } u \in \mathcal{O}_L^*.$$

Dann gilt

$$\mathcal{D} = \rho^v\mathcal{O}_L$$

$$\mathrm{Tr}_{L/K}(\mathcal{O}_L) = \pi^r R$$

und Relation (2) bekommt die Gestalt

$$(\rho^{-v}\mathcal{O}_L)\cap K = \pi^{-r}\mathcal{O}. \qquad (3)$$

Wir gehen zu den Erweiterungsidealen in $\mathcal{O}_L$ über und erhalten

$$\rho^{-re}\mathcal{O}_L = \pi^{-r}\mathcal{O}_L \subseteq \rho^{-v}\mathcal{O}_L,$$

also $-re \ge -v$, d.h.

$$r \le \frac{v}{e}. \qquad (4)$$

Außer (4) benötigen wir noch die Abschätzung

$$\frac{v}{e} < r+1. \qquad (5)$$

Angenommen, es wäre $\frac{v}{e} \ge r+1$, so wäre $-v \le -e(r+1)$ also

$$\pi^{-r-1} = u^{-r-1}\bullet \rho^{-e(r+1)} \in (\rho^{-v}\mathcal{O}_L)\cap K = \pi^{-r}\mathcal{O} \qquad \text{(nach (3))}$$

Durch Multiplikation mit π^{r+1} ergibt sich daraus $1 \in \pi\mathcal{O}$, was nicht möglich ist. Damit ist auch die Abschätzung (5) bewiesen. Zusammen gilt also

$$r \le \frac{v}{e} < r+1. \qquad (6)$$

Ist Bedingung (ii) erfüllt, so gilt $r = 0$, also $0 \le v < e$, also $v \le e-1$. Nach 3.3.12 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 (6), daß $r = 0$ sein muß. Nach Definition von r bedeutet dies,

$$\mathrm{Tr}_{L/K}(\mathcal{O}_L) = \mathcal{O},$$

d.h. es gilt (ii).

QED.

Bemerkung

Falls die Erweiterung L/K normal ist, kann man zum eben bewiesenen Kriterium eine weitere Bedingung hinzufügen.

3.3.19 Satz von der Normalbasis

Seien K ein vollständig bewerteter Körper mit dem Bewertungsring $(\mathcal{O}, \wp)$ und dem Restekörper $\kappa = \mathcal{O}/\wp$ und L/K eine endliche Galoissche Körpererweiterung mit der Galois-Gruppe

$$G = G(L/K).$$

Weiter bezeichne

$$\mathcal{O}[G]$$

den Gruppenring von G mit Koeffizienten aus $\mathcal{O}$. Dann sind folgende Aussagen äquivalent.

(i) L/K ist zahm verzweigt.

(ii) $\mathcal{O}_L$ ist als $\mathcal{O}[G]$-Modul isomorph zu $\mathcal{O}[G]$.

Beweis. (ii) $\Rightarrow$ (i). Sei $\varphi: \mathcal{O}[G] \to \mathcal{O}_L$ ein $\mathcal{O}[G]$-linearer Isomorphismus und $x \in \mathcal{O}_L$ das Bild des Einselements $e \in R[G]$ bei φ. Dann gilt

$$\mathcal{O}_L = \sum_{g\in G} \mathcal{O} g(x),$$

wobei die Summe sogar eine direkte Summe ist. Insbesondere gibt es eindeutig bestimmte Elemente $r_g \in \mathcal{O}$ 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, $r_g = r \in \mathcal{O}$. 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 $\mathcal{O}_L$ mit der Spur 1. Nach 3.3.18(ii) 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

$$\mathbf{K}(A[G]\text{-Proj}) \to \mathbf{K}(K[G]\text{-Proj}),\ M \mapsto K\otimes_A M,$$

ein Monomorphismus.

Dabei bezeichne R-Proj für jeden (nicht-notwendig kommutativen) Ring R mit 1 die Kategorie der endlich erzeugten projektiven R-Moduln und $\mathbf{K}(\mathcal{C})$ die Grothendieckgruppe der Kategorie $\mathcal{C}$.

Folgerung

Seien G eine endliche Gruppe, A ein vollständiger lokaler Integritätsbereich, K dessen Quotientenkörper und P,P' endlich erzeugte projektive A[G]-Moduln. Mit $K\otimes P \cong K\otimes P'$ über K[G] gilt dann sogar $P \cong P'$ über A[G].

Zum Beweis von (i) $\Rightarrow$ (ii). Nach dem Satz von der Normalbasis gibt es ein Element $b \in L$ mit der Eigenschaft, daß

$$K[G] \longrightarrow L, \quad \sum_{g\in G} c_g \cdot g \mapsto c_g \cdot g(b),$$

ein K-linearer Isomorphismus von K-Vektorräumen mit G-Operation ist. Wäre

$$Tr_{L/K}(b) = 0,$$

so würde dasselbe für die Konjugierten von g(b) von b gelten, und damit auch für alle K-Linearkombinationen der g(b). Die Spur wäre dann identisch Null.

Weil L/K zahm verzweigt ist, gilt aber nach 3.3.18 (ii)

$$Tr_{L/K}(\mathcal{O}_L) = \mathcal{O}.$$

Insbesondere ist die Spur nicht identisch Null, und es gilt $Tr_{L/K}(b) \neq 0$. Wir können b durch ein Element aus K dividieren und erreichen so, daß o. B.d.A.

$$Tr_{L/K}(b) = 1$$

gilt.
QED.

3.4 Total verzweigte Erweiterungen

In diesem Abschnitt behandeln wir eine Art von Erweiterungen, die das andere Extrem gegenüber den unverzweigten Erweiterungen darstellen. Wir beginnen mit einigen Definitionen.

3.4.1 Eisenstein-Polynome

Ein Polynome $g(X) \in K[X]$ heißt separabel, wenn es teilerfremd zu seiner Ableitung ist,

$$ggT(g(X), g'(X)) = 1,$$

d.h. wenn es in keiner Körpererweiterung von K mehrfache Nullstellen besitzt.
Ein Eisenstein-Polynom über K ist ein separables Polynom

$$g(X) = X^m + g_{m-1}X^{m-1} + ... + g_0 \in K[X]$$

welchen den folgeden beiden Bedingungen genügt.
(i) $v_K(g_i) \geq 1$ für i = 1, ... , m-1
(ii) $v_K(b_0) = 1$
d.h. die Ideale (g_i) werden vom Bewertungsideal geteilt, das Ideal (g_0) zum Absolutglied jedoch nicht von dessen Quadrat.
Bemerkung
In der obigen Definition tritt die Bedingung der Separabilität nur auf, weil wir uns generell auf separable Körpererweiterungen L/K beschränkt haben.

3.4.2 Total verzweigte Erweiterungen

Seien K ein vollständig bewerteter Körper mit dem Bewertungsring $(\mathcal{O}, \wp)$ und dem Restekörper $\kappa = \mathcal{O}/\wp$ und L/K eine endliche separable Körpererweiterung. Dann heißt die Erweiterung

$$L/K$$

total verweigt, wenn

$$e(L/K) = [L:K]$$

gilt.

Im nicht-lokalen Fall (d.h. für nicht notwending vollständige Körper) bekommt diese Defintion die folgende Gestalt.

Seien K ein diskret bewerteter Körper mit dem Bewertungsideal p, L/K eine endliche separable Körpererweiterung und P ein über p liegenden maximales Ideal (der ganzen Abschließung des Bewertungsrings von p in L). Dann heißt p total verzweigt in P, wenn die Vervollständigung L_P von L in der P-adischen Topologie unverzweigt ist über der Vervollständigung K_p von K in der p-adischen Topologie, d.h. wenn gilt Bedingungen

$$f(P/p) = 1.$$

Bemerkungen

(i) Nach 3.3.7 ist im lokaken Fall, d.h. für separable Erweiterungen vollständig bewerteter Körper L/K, die Bedingung der totalen Verweigung äquivalent zur Bedingung

$$f(L/K) = 1.$$

(ii) Man beachte, beim Übergang zur Vervollständigung bleiben zwar Verzweigungsindex und Relativgrad erhalten, im allgmeinen jedoch nicht der Körpergrad. Wegen der Isomorphie

$$L\otimes_K K_p \cong L_{P_1}\times\ldots\times L_{P_r}$$

ist der Körpergrad

$$[L:K] = \dim_{K_p} L\otimes_K K_p = \sum_{i=1}^{r} [L_{P_i}:K_p]$$

gerade die Summe der Körpergrade der zugehörigen lokalen Körpererweiterungen.

3.4.3 Die Struktur der total verzweigten Körpererweiterungen

Die Eisenstein-Polynome sind gerade die Minimalpolynome der Parameter der unverzweigten Erweiterungen. Genauer gilt:

(i) Seien K ein vollständiger diskret bewerteter Körper,

$$E(X) \in K[X]$$

ein Eisenstein-Polynom und

$$\Pi$$

eine Nullstelle von E in einer Körpererweiterung von K. Dann ist

$$L := K[\Pi]$$

eine total verzweigte Körpererweiterung von K und Π ein Parameter von L, d.h.

$$v_L(\Pi) = 1.$$

Eisenstein-Polynome sind irreduzibel.

(ii) Seien L/K ein total verweigte Erweiterung des vollständigen diskret bewerteten Körper K und Π ein Parameter von L, d.h.

$$v_L(\Pi) = 1.$$

Dann ist das Minimalpolynom von Π ein Eisenstein-Polynom, und es gilt

$$L = K(\Pi) \text{ und } \mathcal{O}_L = \mathcal{O}[\Pi].$$

Bemerkung

Zum Beweis benötigen wir eine Aussage zur Darstellbarkeit der Elemente eines vollständignen diskret bewerteten Körpers K durch geeignete konvergente Reihen.

Die Reihe

$$\sum_{n \gg -\infty}^{\infty} a_n \Pi_n$$

für beliebige $a_n, \Pi_n \in K$ mit

$$v_K(\Pi_n) = n \text{ und } v_K(a_n) \ge \rho$$

und einer Konstanten ρ.[37] Dabei bedeute die Bedingung $n \gg -\infty$ daß die Koeffizienten a_n für alle n unterhalb eines festen Werts gleich Null sind.

3.4.4 Laurentreihen in vollständigen diskret bewerteten Körpern

Seien K ein vollständiger diskrete bewerteter Körper mit dem Bewertungsring $(\mathcal{O}, \wp)$ und dem Restekörper $\kappa = \mathcal{O}/\wp$. Seien Abbildungen

$$\Pi: \mathbb{Z} \longrightarrow K^*, n \mapsto \Pi_n,$$

$$r: \kappa \longrightarrow \mathcal{O}, r(0) = 0,$$

gegeben, für welche die beiden Diagramme

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\text{Id}} & \mathbb{Z} \\ & \Pi \searrow \nearrow v_K & \\ & K^* & \end{array} \qquad \begin{array}{ccc} \kappa & \xrightarrow{\text{Id}} & \kappa \\ & r \searrow \nearrow & \\ & \mathcal{O} & \end{array}$$

kommutativ sind. Dabei sei die Abbildung $\mathcal{O} \twoheadrightarrow \kappa$ des rechten Diagramm die natürliche Abbildung auf den Restklassenring.

Dann läßt sich jedes Element $\alpha \in K$ auf genau eine Weise in der Gestalt

$$a = \sum_{n \gg -\infty}^{\infty} a_n \Pi_n \text{ mit } a_n \in \text{Im}(r) \qquad (1)$$

schreiben. Aus dieser Darstellung läßt sich der Wert des Elements a ablesen:

$$v_K(a) = \inf \{n \mid a_n \neq 0\}. \qquad (2)$$

Bemerkungen

(i) Die Kommutativität des linken Dreiecks ist äquivalent zur Bedingung

$$v_K(\Pi_n) = n \text{ für jedes } n \in \mathbb{Z}.$$

(ii) Die Kommutativität des rechte Dreiecks bedeutet gerade, daß die Abbildung

$$r: \kappa \longrightarrow \mathcal{O},$$

jedem Element $c \in \kappa$ einen Repräsentanten von c in $\mathcal{O}$ zuordnet.

Beweis. <u>1. Schritt: Konvergenz der Reihen der Gestalt</u> (1).

Auf Grund der beiden obigen Bemerkungen genügen die Reihen der Gestalt (1) den Bedingungen der Bemerkung von 3.4.3. Man beachte, für die Koeffizienten gilt

$$a_n \in \text{im}(r) \subseteq \mathcal{O},$$

also $v_K(a_n) \ge 0$ für jedes n.

---

[37] Wegen $v_K(a_n \Pi_n) = v_K(a_n) + v_K(\Pi_n) \longrightarrow \infty$ und der verschärften Dreiecksungleichung für nicht-archimedische Bewertungen genügen die Partialsummen den Bedingungen an einer Cauchy-Folge.

2. <u>Schritt</u>: Eindeutigkeit der Koeffizienten der Reihe (1).
Nehmen wir an, mindestens ein Koeffizient der Reihe (1) ist ungleich Null. Sei

$$a_{n_0} \neq 0$$

derjenige mit dem kleinsten Index. Dann gilt

$$v_K(a_{n_0}\Pi_{n_0}) = n_0 .$$

Alle anderen Summanden von (1) haben dagegen einen echt größeren Wert. Deshalb haben alle endlichen ummen von (1) den Wert n_0, d.h. die Reihe (1) hat den Wert n_0. Es gilt also (2),

$$n_0 = v_K(a).$$

Außerdem ist der Limes der Reihe $\neq 0$.

Multipliziert man beide Seiten von (1) mit $\Pi_{n_0}^{-1}$, so erhält man Einheiten von $\mathcal{O}$ mit[38]

$$a\,\Pi_{n_0}^{-1} - a_{n_0} \in \wp,$$

d.h. die Restklasse von a_{n_0} in κ ist eindeutig durch a festgelegt. Weil a_{n_0} im Bild von r liegen soll, ist dann aber auch a_{n_0} selbst eindeutig festgelegt. Damit ist das Anfangsglied der Reihe (1) durch a eindeutig festgelegt.
Indem wir die eben durchgeführte Betrachtung mit $a - a_{n_0}\Pi_{n_0}$ anstelle von a wiederholen, sehen wir, auch das zweite Glied der Reihe ist durch a festgelegt. Durch weiteres Wiederholen sehen wir , alle Koeffizienten der Reihe sind durch a festgelegt.

3. <u>Schritt</u>: Existenz der Reihenentwicklung
Sei $a \in K - \{0\}$ vorgegeben und sei

$$n_0 := v_K(a).$$

Dann ist $a\,\Pi_{n_0}^{-1}$ eine Einheit von $\mathcal{O}$. Nach Bemerkkung (ii) gibt es ein (eindeutig bestimmtes) $a_{n_0} \in \mathrm{Im}(r)$ mit derselben Restklasse in κ wie $a\,\Pi_{n_0}^{-1}$, d.h. mit

$$a\,\Pi_{n_0}^{-1} - a_{n_0} \in \wp,$$

d.h.

$$(a - a_{n_0}\Pi_{n_0})\,\Pi_{n_0}^{-1} \in \wp.$$

d.h.

$$a - a_{n_0}\Pi_{n_0} \in \wp\,\Pi_{n_0} = .\wp^{n_0+1}$$

[38] Weil alle Glieder der multiplizierten Reihe außer dem ersten in $\wp$ liegen.

Insbesondere ist

$$n_1 := v_K(a - a_{n_0} \Pi_{n_0}) \geq n_0+1 > v_K(a) = n_0.$$

Wir wiederholen die Konstruktion mit $a - a_{n_0} \Pi_{n_0}$ anstelle von a und erhalten eine echt aufsteigende Folge ganzer Zahlen

$$n_0 < n_1 < n_2 < \dots$$

und eine Folge von Elementen

$$a_{n_i} \in \mathrm{Im}(r)$$

mit

$$n_i = v_K(a - \sum_{j=0}^{i-1} a_{n_j} \Pi_{n_j}).$$

Insbesonder konvergiert die Folge der Partialsummen $\sum_{j=0}^{i-1} a_{n_j} \Pi_{n_j}$ gegen a,

$$a = \sum_{j=0}^{\infty} a_{n_j} \Pi_{n_j} \text{ in } K,$$

d.h. a kann als konvergente Reihe der angegebenen Art geschrieben werden.

QED.

Beweis von 3.4.3. Zu (i). Seien

$$E(X) = X^m + E_{m-1}X^{m-1} + \dots + E_0 \in K[X]$$

ein Eisenstein-Polynom und

$$\Pi$$

eine Nullstelle von E in einem Erweiterungskörper von K. Wir setzen

$$L := K(\Pi).$$

Nach Definition des Begriffs Eisenstein-Polynom liegen die Koeffizienten von E in $\mathcal{O}$, d.h. Π ist ganz über $\mathcal{O}$,

$$\Pi \in \mathcal{O}_L,$$

und es gilt

$$v_L(\Pi) \geq 0.$$

Es folgt

$$m \cdot v_L(\Pi) = v_L(\Pi^m) =^{39} v_L(E_{m-1}\Pi^{m-1} + \dots + E_0) \geq^{40} 1,$$

also

$$v_L(\Pi) \geq 1.$$

Wir wählen die ganze Zahl s derart, daß gilt

$$s \geq \frac{e}{v_L(\Pi)} > s - 1 \text{ mit } e := e(L/K).$$

Dann ist

$$m \geq n \geq e \geq s \text{ mit } n := [L:K]. \tag{3}$$

---

[39] Π ist Nullstelle von E(X).

[40] Alle Koeffizienten E_i mit $i < m$ liegen im Bewertungsideal von K.

Die Ungleichung

- $m \ge n$ besteht, weil das Minimalpolynom μ von Π über K das Polynom E teilt, d.h. es ist $m = \deg E \ge \deg \mu = [L:K] = n$.
- $n \ge e$ besteht wege $n = [L:K] = e \cdot f$
- $e \ge s$ besteht nach Wahl von s, d.h. wegen $e \ge \frac{e}{v_L(\Pi)} \ge s$

Wir wollen zeigen, m = s. Angenommen es ist m > s. Dann gilt

$$v_L(\Pi^m) = \frac{m \cdot v_L(\Pi)}{e} \cdot e \ge^{41} \frac{m}{s} \cdot e > e. \tag{4}$$

Außerdem ist

$$v_L(E_i) = e \cdot v_K(E_i) \ge^{42} e \text{ für } i = 0, \ldots, m-1,$$

d.h. jedes $E_i \Pi^i$ liegt in[43] $\wp_L^{e+1}$ für i = 1, ... , m-1. Zusammen mit (4) ergibt sich

$$v_L(E_0) =^{44} v_L(\Pi^m + E_{m-1}\Pi^{m-1} + \ldots + E_1\Pi) > e$$

also

$$v_K(E_0) = \frac{1}{e} v_L(E_0) > 1.$$

Das steht im Widerspruch dazu, daß E(X) Eisenstein-Polynom sein soll. Die Annahme m > s ist falsch. Es gilt somit überall in (3) das Gleichheitszeichen. Insbesondere ist

L/K total verzweigt	(wegen e = n).
$v_L(\Pi) = 1$	(wegen s = e und Definition von s)
E irreduzibel	(wegen m = n).

Damit ist Aussage (i) bewiesen.

<u>Zu (ii)</u>. Sei L/K eine total verzweigte Erweiterung und Π ein Parameter von L. Dann gilt

$$f(L/K) = 1,$$

d.h.

$$\mathcal{O}/\wp = \kappa = \kappa_L \tag{5}$$

Sei π ein Parameter von K. Die Abbildung

$$\mathbb{Z} \longrightarrow L^*,\ ue + v \mapsto \Pi_{ue+v} := \pi^u \cdot \Pi^v,$$

fügt sich dann in das kommutative Diagramm

$$\begin{tikzcd} \mathbb{Z} \arrow[rr, "\mathrm{Id}"] \arrow[dr] & & \mathbb{Z} \\ & L^* \arrow[ur, "v_L"'] & \end{tikzcd}$$

ein: $v_L(\Pi_{ue+v}) = u \cdot v_L(\pi) + v \cdot v_L(\Pi) = u \cdot e$ Weiter fixieren wir eine Abbildung r mti r(0) = 0, welche sich in das folgende Diagramm kommutativ einfügt.

---

[41] nach Wahl von s ist $\frac{v_L(\Pi)}{e} \ge \frac{1}{s}$

[42] weil die Koeffizienten von E(X) in $\mathcal{O}$ liegen.

[43] wegen $v_L(\Pi) \ge 1$.

[44] Π ist Nullstelle von E(X).

$$\begin{array}{ccc} \kappa_L & \xrightarrow{\mathrm{Id}} & \kappa_L \\ & r \searrow \nearrow & \\ & \mathcal{O}_L & \end{array}$$

d.h. r ordnet jedem Element von κ_L einen Repräsentanten in $\mathcal{O}_L$ zu. Wegen (5) können wir r sogar so wählen, daß

$$\mathrm{Im}(r) \subseteq \mathcal{O}$$

gilt. Die beiden Abbildungen genügen den Bedingungen von 3.4.4 an (mit L anstelle von K). Jedes Element von L läßt sich somit in der Gestalt

$$\sum_{n>>-\infty}^{\infty} a_n \Pi_n \text{ mit } a_n \in \mathrm{Im}(r) \subseteq \mathcal{O}$$

schreiben Wegen

$$\sum_{n>>-\infty}^{\infty} a_n \Pi_n = \sum_{n>>-\infty}^{\infty} \sum_{n=qe+r} a_{qe+r} \pi^q \cdot \Pi^r$$

$$= \sum_{r=0}^{e-1} (\sum_{q>>-\infty}^{\infty} a_{qe+r} \pi^q) \cdot \Pi^r \in^{45} K(\Pi)$$

erhalten wir

$$L = K[\Pi] = K(\Pi).$$

Die gerade betrachtete Potenzreihe liegt genau dann in $\mathcal{O}_L$, wenn sie bezüglich v_L einen nicht-negativen Wert hat, d.h. wenn alle auftretenden Exponenten ≥ 0 sind. Es gilt deshalb

$$\mathcal{O}_L = \mathcal{O}[\Pi].$$

Sei jetzt

$$E(X) = X^m + E_{m-1}X^{m-1} + ... + E_0 \in K[X].$$

Wir haben noch zu zeigen, E ist ein Eisenstein-Polynom.

Nach Wahl von E ist E auch das charakteristische Polynom der Multiplikation mit Π auf $L = K(\Pi)$. Insbesondere ist

$$E_0 = \pm N_{L/K}(\Pi),$$

also

$$v_K(E_0) = v_K(N_{L/K}(\Pi) =^{46} f \cdot v_L(\Pi) = f =^{47} 1.$$

Ersetzt man die Koeffizienten von E durch deren Restklassen modulo $\wp$, so erhält man ein Polynom

$$\bar{E}(X) \in \mathcal{O}/\wp[X] = \kappa[X].$$

welches gerade das charakteristische Polynom für die Multiplikation mit Π auf dem κ-Vektorraum

---

[45] Links steht ein Quotient, wobei im Nenner eine Potenz von Π steht und im Zähler ein Polynom in Π, dessen Koeffizienten Potenzreihen mit Werten in K sind.

[46] nach 3.3.9.

[47] L/K ist total verzweigt.

$$\mathcal{O}_L/\wp\mathcal{O}_L$$

ist. Nun ist diese Multiplikation mit Π eine nilpotente lineare Abbildung.[48] Es gibt also eine Basis dieses Vektorraums (zu einer geeignete vollständigen Fahne), bezüglich welcher die Matrix dieser Abbildung Dreiecksgestalt hat, wobei auf der Hauptdiagonalen lauter Nullen stehen. Das charakteristische Polynom ist also gleich einer Potenz der Unbestimmten,

$$\overline{E}(X) = X^m.$$

Damit gilt

$$E_i \in \wp \text{ für } i = 0, \dots , m-1,$$

d.h. E(X) ist ein Eisenstein-Polynom.
QED.

3.4.5 Existenz total verzweigter Erweiterungen

Sei K ein vollständiger diskret bewerteter Körper. Dann gibt es zu jeder natürlichen Zahl e eine total verzweigte Erweiterung vom Grad e.

Beweis. Seien π ein Parameter von K und

$$E(X) = X^e - \pi X - \pi \in K[X].$$

Dann ist E(X) ein Eisenstein-Polynom von Grad e, definiert also eine Erweiterung der gesuchten Art.
QED.

3.4.6 Anmerkungen (überflüssig ?)

(i) Wir verweisen hier noch auf einige weitere Ergebnisse, die wir hier nicht beweisen werden (siehe Serre [1], Kapitel II).

(ii) Ist

$$K = F[[t]]$$

der Körper der formalen Laurent-Reihen

$$\sum_{n>>-\infty} a_n \cdot t^n$$

über dem Körper F, so kann man

$$\Pi_n = t^n \text{ und } Im(r) = F$$

setzen. In diesem Falls haben K und κ dieselbe Charakteristik.

(iii) Ein typisches Beispiel mit einem Restekörper der Charakteristik $p > 0$, wobei der Körper K selbst die Charakteristik 0 hat, ist der Körper der p-adischen Zahlen

$$K = \mathbb{Q}_p.$$

Setzt man noch voraus, daß κ perfekt ist (zum Beispiel, wenn κ endlich ist wie im Fall $K = \mathbb{Q}_p$), so kann man Im(r) multiplikativ abgeschlossen wählen, und zwar auf genau eine Weise.

(iv) Man kann zeigen, ist κ perfekt von der Charakteristik $p > 0$, so existiert bis auf Isomorphie genau ein diskret bewerteter Körper K der Charakteristik 0, welcher κ als Restekörper besitzt und für welchen $v(p) = 1$ ist.

---

48 Wegen $\Pi^e \in \wp\mathcal{O}$ ist die Multiplikation mit Π^e die Nullabbildung.

3.5 Unverzweigte Erweiterungen

3.5.1 Vorbemerkung

Nach Definition des Begriffs der unverzweigten Erweiterung (im lokalen Fall, vgl. 3.3.13) ist für jede unverzweige Erweiterungen

$$L/K$$

die zugehörige Ereweiterung

$$\kappa_L/\kappa$$

separabel. Ein Ziel dieses Abschnitts ist es zu zeigen, daß in einem gewissen Sinne auch die Umkehrung dieser Aussage richtig ist: für jede endliche separable Erweiterung κ'/κ des Restkörpers κ gibt es eine bis auf Isomorphie eindeutig bestimmte unverzweigte Erweiterung L/K mit $\kappa_L = \kappa'$. Wir werden sogar zeigen, daß die Zuordnung

$$\kappa_L \mapsto L$$

einen Funktor definiert.

Wir beginnen mit einer Beschreibung der Struktur unverzweigten Erweiterung im selben Stil, wie wir das gerade für die total verzweigten Erweiterungen getan haben.

3.5.2 Die Struktur der unverzweigten Erweiterungen

Sei K ein volltändiger diskret bewerteter Körper mit dem Bewertungsring ($\mathcal{O}$, $\wp$) und dem Restekörper $\kappa = \mathcal{O}/\wp$. Die unverzweigten Erweiterungen von K sind dann gerade die einfachen algebraischen Erweiterungen, für welche die Minimalpolynome über dem Restekörper irreduzibel und separabel bleiben. Genauer gilt:

(i) Sei L/K eine unverzweigte Erweiterung von K. Dann gibt es ein Element $x \in \mathcal{O}_L$ dessen Restklasse $\bar{x}$ in κ die Erweiterung der Restekörper erzeugt, d.h.

$$\kappa_L = \kappa(\bar{x}).$$

Ist $g(X) \in K[X]$ das Minimalpolynom eines solchen Elements x über K, so liegen die Koeffizienten von g in $\mathcal{O}$,

$$g(X) \in \mathcal{O}[X]$$

und das zugehörige Polynom[49]

$$\bar{g}(X) \in \kappa[X]$$

ist irreduzibel und separabel. Außerdem gilt

$$L = K(x) \text{ und } \mathcal{O}_L = \mathcal{O}[x].$$

(ii) Sei

$$g(X) \in \mathcal{O}[X]$$

ein normiertes Polynom, für welches das zugehörige Polynom

$$\bar{g}(X) \in \kappa[X]$$

irreduzibel und separabel ist. Für jede Nullstelle x von g(X) in einer Körpererweiterung von K ist dann

$$L = K(x)$$

eine unverweigte Körper-Erweiterung mit $x \in \mathcal{O}_L$ und die Restklasse $\bar{x}$ von x in κ erzeugt die zugehörige Erweiterung der Restekörper, d.h.

$$\kappa_L = \kappa(\bar{x}).$$

---

[49] $\bar{g}$ entstehe aus g, indem man die Koeffizienten von g durch deren Restklassen in κ ersetzt.

Beweis. Zu (i). Als endliche separable Erweiterung ist κ_L/κ einfach, d.h. sie hat die Gestalt

$$\kappa_L = \kappa[\bar{x}].$$

mit einem geeignet gewählten Element $x \in \mathcal{O}_L$. Seien jetzt

$$x \in \mathcal{O}_L$$

ein solches Element,

$$g(X) \in K[X]$$

dessen Minimalpolynom über K und

$$h(X) \in \kappa[X]$$

das Minmalpolynom von $\bar{x}$ über κ. Dann gilt

$$g(X) \in \mathcal{O}[X],$$

denn die Koeffizienten von g(X) sind die elementarsymmeterischen Funktionen in den Konjugierten von x, d.h. sie sind ganz über $\mathcal{O}$ und liegen in K, also liegen sie in $\mathcal{O}$. Weiter ist

$$[L:K] \ge [K(x):K] = \deg g \ge^{50} \deg h = [\kappa_L:\kappa] = f(L/K) =^{51} e(L/K)\cdot f(L/K) = [L:K].$$

In der Abschätzung gilt somit überall das Gleichheitszeichen. Insbesondere gilt deg g = deg h, d.h. das zu g(X) gehörige Polynom $\bar{g}(X) \in \kappa[X]$ ist gerade h(X),

$$\bar{g}(X) = h(X).$$

Insbesondere ist $\bar{g}$ irreduzibel und separabel. Weiter ergibt sich aus den Gleichheitszeichen in der obigen Abschätzung

$$L = K(x).$$

Wir haben noch zu zeigen, es gilt

$$\mathcal{O}_L = \mathcal{O}[x].$$

Nach Wahl von x gilt zumindest "$\supseteq$". Zum Beweis der Gleichheit wenden wir die Beschreibung der Diskriminante einfacher Erweiterungen von Dedekind-Ringen 3.2.10 an.[52] Nach 3.2.10 (iii) ist die zu beweisende Gleichheit äquivalent zur Bedingung

$$\mathcal{D}(\mathcal{O}_L/\mathcal{O}) = g'(x)\mathcal{O}_L.$$

Weil L/K nach Voraussetzung (i) unverzeigt ist, ist die Differente auf der linken Seite gleich $\mathcal{O}_L$ (nach 3.3.14 und den zweiten Schritt des Beweises von 3.3.14). Es reicht somit zu zeigen,

$$g'(x)\mathcal{O}_L = \mathcal{O}_L. \tag{1}$$

Wie wir gerade gesehen haben, ist $\bar{g}$ separabel, d.h. $\bar{g}$ und $\bar{g}'$ sind teilerfremd. Ein Linearkombination von $\bar{g}$ und $\bar{g}'$ mit Koeffizienten aus $\kappa[X]$ ist gleich 1. Wir gehen zu den Repräsentanten in $\mathcal{O}$ und und sehen, eine Linearkombination von g und g' mit Koeffizienten aus $\mathcal{O}$ ist eine Einheit in $\mathcal{O}$. Wir setzen X = x und erhalten, ein $\mathcal{O}_L$-Vielfaches von g'(x) ist eine Einheit in $\mathcal{O}$, d.h. es gilt (1).

---

[50] Das zu g(X) gehörige Polynom $\bar{g}(X) \in \kappa[X]$ ist ein normiertes Polynom mit der Nullstelle $\bar{x}$, wird also vom Minimalpolynom h(X) von $\bar{x}$ geteilt. Beim Übergang zu $\bar{g}$ bleibt der Grad unverändert, beimÜbergang zum Teiler h kann er höchstens kleiner werden.

[51] L/K ist nach Voraussetzung (i) unverzweigt.

[52] Man kann auch die Beschreibung 3.4.4 der Elemente von vollständigen bewerteten Körpern duch Laurent-Reihen verwenden.

<u>Zu (ii)</u>. Sei umgekehrt $g(X) \in \mathcal{O}[X]$ ein normiertes Polynom mit $\bar{g}(X) \in \kappa[X]$ irreduzibel und separabel, x eine Nullstelle von g in einer Körpererweiterung und

$$L = K(x).$$

Dann ist auch g irreduzibel[53]. Wegen $g(X) \in \mathcal{O}[X]$ ist x ganz über $\mathcal{O}$, d.h.

$$x \in \mathcal{O}_L$$

Weiter gilt

$$[L:K] = \deg g(X) = \deg \bar{g}(X) = [\kappa(\bar{x})/\kappa] \le [\kappa_L:\kappa] = f(L/K) \le e(L/K)\bullet f(L/K) = [L:K]$$

Wieder muß in der Abschätzung überall das Gleichheitzeichen gelten. Insbesonder ist

$$e(L/K) = 1 \text{ und } \kappa_L = \kappa[\bar{x}]$$

Weil das Minimalpolynom $\bar{g}$ von $\bar{x}$ über κ separabel ist, ist κ_L/κ eine separabel Körper-Erweiterung und damit L/K unverzweigt.
QED.

3.5.3 Kategorien von Körpererweiterungen

Seien F ein Körper und $\mathcal{E}$ eine Familie von Körper-Erweiterungen von F. Wir ordnen jetzt dieser Familie $\mathcal{E}$ eine Kategorie zu, die wir ebenfalls mit $\mathcal{E}$ bezeichnen.

Die Objekte der Kategorie $\mathcal{E}$ seien die Elemente der Familie von $\mathcal{E}$.
Für je zwei Elemente E', E" der Familie $\mathcal{E}$ sei

$$\mathrm{Hom}_{\mathcal{E}}(E', E'')$$

die Menge der Homomorphismen

$$h: E' \longrightarrow E''$$

von Ringen mit 1, welche den Teilkörper F elementweise festlassen,

$$h(x) = x \text{ für jedes } x \in F.$$

Damit sind die Morphismen der Kategorie $\mathcal{E}$ festgelegt. Die Morphismen-Komposition in $\mathcal{E}$ sei die gewöhnliche Zusammensetzung von von Abbildungen.

Bemerkungen

(i) Für jedes $E\in\mathcal{E}$ liegt die identische Abbildung in $\mathrm{Hom}_{\mathcal{E}}(E, E)$ und für je drei Körper $E,E',E'' \in \mathcal{E}$ definiert Morphismen-Kompostionen eine Abbildung

$$\mathrm{Hom}_{\mathcal{E}}(E, E') \times \mathrm{Hom}_{\mathcal{E}}(E', E'') \longrightarrow \mathrm{Hom}_{\mathcal{E}}(E,E''),\ (f, g) \mapsto g\circ f,$$

d.h. $\mathcal{E}$ ist tatsächlich eine Kategorie.j

(ii) Sei jetzt $\mathcal{E}$ eine Familie von algebraischen Körper-.Erweiterungen von F mit der Eigenschaft, daß für jedes

$$E \in \mathcal{E}$$

auch die <u>separable Abschließung</u>[54]

$$E^s \in \mathcal{E}$$

von F in E in $\mathcal{E}$ liegt. Dann definiert die Einschränkung eine Abbildung

$$\mathrm{Hom}(E', E'') \longrightarrow \mathrm{Hom}(E'^s, E''^s),\ \sigma \mapsto \sigma^s := \sigma|_{E'^s}, \qquad (1)$$

---

[53] Da $\mathcal{O}$ ein ZPE-Ring ist, kann man den Satz von Gauß anwenden: eine Zerlegung von g über K würde eine Zerlegung von g über $\mathcal{O}$ zur Folge haben und damit eine Zerlegung von $\bar{g}$.

[54] dies ist der größte Körper E' zwischen F und E, welcher separabel über F ist ist, d.h.

$$E^s = \{x \in E \mid x \text{ separabel über } F\}$$

die mit der Morphismen-Komposition verträglich ist. Mit anderen Worten, durch

$$? ^{S}:\mathcal{E} \longrightarrow \mathcal{E},\ E \mapsto E^{S},\ \sigma \mapsto \sigma^{S},$$

ist ein Funktor definiet.

(iii) Abbildung (1) ist injektiv[55] und im Fall E' = E'^{S} bijektiv.

3.5.4 Verhalten von Bewertungen bei Homomorphismen

Seien K ein vollständiger diskret bewerteter Körper, L/K und L'/K zwei endliche separable Körpererweiterungen und

$$\sigma: L \longrightarrow L'$$

ein Homomorphismus von Ringen mit 1, welcher K elementweise fest läßt. Dann gilt

$$v_{L'}(\sigma(x)) = e(L'/\sigma(L))\bullet v_L(x)$$

für jedes $x \in L$.

Beweis. Sei

$$v_{\sigma L}: \sigma L^* \longrightarrow \mathbb{Z}$$

die eindeutig bestimmte Bewertung des Körpers σL. Dann ist durch

$$v: L^* \longrightarrow \mathbb{Z},\ x \mapsto v_{\sigma L}(\sigma x),$$

eine Bewertung von L definiert. Wegen der Vollständigkeit von K ist aber die Bewertung von L durch die von K eindeutig bestimmt, d.h. es gilt für $x \in L$

$$\begin{aligned} v_L(x) &= v(x) \\ &= v_{\sigma L}(\sigma x) && \text{(Definition von v)} \\ &= \frac{v_{L'}(\sigma x)}{e(L'/\sigma(L))} && \text{(Definition des Verzweigungsindex),} \end{aligned}$$

also

$$e(L'/\sigma(L))\bullet v_L(x) = v_{L'}(\sigma x).$$

QED.

3.5.5 Invarianz der Bewertung gegenüber der Galois-Gruppe

Seien K ein vollständiger diskret bewerteter Körper und L/K eine endliche Galois-Erweiterung mit der Galois-Gruppe G = G(L/K). Dann gilt

$$v_L(\sigma x) = v_L(x)$$

für jededs $x \in L$ und jedes $\sigma \in G$.

Beweis. Folgt aus 3.5.4 mit L' = L.

QED.

3.5.6 Auf den Reste-Körpern induzierte Homomorphismen

Seien K ein vollständiger diskret bewerteter Körper, L/K und L'/K zwei endliche separable Körpererweiterungen und

$$\sigma: L \longrightarrow L'$$

---

[55] Die Elemente von E^{S} erhält man durch wiederholtes ziehen von p-ten Wurzeln, wobei p die Charakteristik von F bezeichne. Das Ziehen der p-ten Wurzel ist in der Charakteristik p eindeutig, d.h. alle Elemente von E sind über E^{S} nur zu sich selbst konjugiert. Das Bild einer p-ten Wurzel eines Elements x bei einem Homomorphismus ist deshalb, falls es existiert, bereits durch das Bild von x eindeutig festgelegt.

ein Homomorphismus von Ringen mit 1, welcher K elementweise fest läßt. Dann gilt

$$\sigma(\mathcal{O}_L) \subseteq \mathcal{O}_{L'}, \text{ und } \sigma(\wp_L) \subseteq \wp_{L'}, \tag{1}$$

d.h. σ induziert einen Homomorphismus

$$\kappa_\sigma: \kappa_L \longrightarrow \kappa_{L'},$$

von Ringen mit 1, welcher den Körper κ elementweise festläßt. Außerdem gilt

(i) $\kappa_{Id} = Id.$[56]

(ii) $\kappa_{\tau\sigma} = \kappa_\tau \circ \kappa_\sigma$ für K-Homomorphismen $\sigma: L \longrightarrow L'$ und $\tau: L' \longrightarrow L''$.

Auf diese Weise sind Funktoren

$$\left\{\begin{matrix}\text{Kategorie der endlichen}\\ \text{separabelen Körper-}\\ \text{erweiterungen von K}\end{matrix}\right\} \longrightarrow \left\{\begin{matrix}\text{Kategorie der endlichen}\\ \text{Körpererweiterung}\\ \text{von } \kappa\end{matrix}\right\}, L \mapsto \kappa_L, \sigma \mapsto \kappa_\sigma .$$

und

$$\left\{\begin{matrix}\text{Kategorie der endlichen}\\ \text{separabelen Körper-}\\ \text{erweiterungen von K}\end{matrix}\right\} \longrightarrow \left\{\begin{matrix}\text{Kategorie der endlichen}\\ \text{separablen Körper-}\\ \text{erweiterun von } \kappa\end{matrix}\right\}, L \mapsto \kappa_L^s, \sigma \mapsto \kappa_\sigma^s .$$

definiert. Dabei bezeichne κ_L^s die separable Abschließung von κ in κ_L und κ_σ^s die Einschränkung von κ_σ auf die separablen Abschließungen.

Beweis. Aus der Formel

$$v_{L'}(\sigma(x)) = e(L'/\sigma(L))\cdot v_L(x) \text{ für } x \in L$$

von 3.5.4 folgt

$$v_L(x) \ge 0 \Rightarrow v_{L'}(\sigma(x)) \ge 0$$

und

$$v_L(x) > 0 \Rightarrow v_{L'}(\sigma(x)) > 0$$

Deshalb bestehen die Inklusionen (1). Insbesondere induziert damit σ einen Homomorphismus

$$\kappa_\sigma: \kappa_L \longrightarrow \kappa_{L'},$$

der beschriebenen Art. Wir erhalten so für je zwei endliche separable Erweiterungen L/K und L'/K eine Abbildung

$$Hom_{\mathcal{E}}(L, L') \longrightarrow Hom_{\mathcal{E}'}(\kappa_L, \kappa_{L'}), \sigma \mapsto \kappa_\sigma,$$

wenn $\mathcal{E}$ die Kategorie der endlichen separabelen Körper-Erweiterungen von K und $\mathcal{E}'$ die der endlichen Körpererweiterungen von κ bezeichnet. Für $\sigma = Id: L \longrightarrow L$ ist κ_σ die identische Abbildung, und die Zuordung $\sigma \mapsto \kappa_\sigma$ ist mit der Komposition von Homomorphismen σ verträglich. Wir erhalten so den ersten der beiden beschriebenen F Durch die Zusammensetzung mit dem Übergang zu den separablen Abschließungen (vgl. Bemerkung 3.5.3 (ii)) erhält man den zweiten.

QED.

Bemerkung

---

[56] d.h. für L' = L und σ = Id ist κ_σ die identische Abbildung.

Das nachfolgende Ergebnis besagt in der Sprache der Kategorien im wesentlichen, daß der oben konstruierte Funktor

$$L \mapsto \kappa_L^s, \sigma \mapsto \kappa_\sigma^s,$$

einen adjungierte Funktor besitzt. Insbesondere ergibrt sich so quasi-inverse Äquivalenzen[57]

$$\kappa_?^s: \mathcal{E} \longrightarrow \mathcal{E}' \text{ und } L(?): \mathcal{E}' \longrightarrow \mathcal{E}$$

der Kategorie $\mathcal{E}$ der endlichen unverzweigten den Erweiterungen von K mit der Kategorie $\mathcal{E}$' der endlichen separablen Erweiterungen von κ.

3.5.7 Die unverzweigte Erweiterung L(κ') zu einer der Restekörper

Sei K ein vollständiger diskret bewerteter Körper mit dem Bewertungsring ($\mathcal{O}$, $\wp$) und dem Restkörper $\kappa = \mathcal{O}/\wp$. Sei weiter κ'/κ eine endliche separable Körper-Erweiterung. Dann existiert eine endliche separable Körper-Erweiterung

$$L = L(\kappa')$$

von K derart daß folgende Bedingungen erfüllt sind.

(i) $\kappa' \cong \kappa_L$ (Isomorphie über κ).

(ii) L/K ist eine unverzweigte Erweiterung.

(iii) Die Abbildung

$$\mathrm{Hom}_K(L, L') \longrightarrow \mathrm{Hom}_\kappa(\kappa_L, \kappa_{L'}), \sigma \mapsto \kappa_\sigma,$$

ist bijektiv für jede endliche separable Körper-Erweiterung L'/K.

Die Erweiterung L/K ist bis auf K-Isomorphie eindeutig bestimmt durch die Eigenschaften (i) und (ii) und auch durch die Eigenschaften (i) und (iii).

Bemerkungen

(i) In (iii) kann man κ_L, $\kappa_{L'}$, und κ_σ durch κ_L^s, $\kappa_{L'}^s$, und κ_σ^s ersetzen.

(ii) Im Beweis benötigen wir den in 2.4.5 beschriebenen zweiten Spezial des Henselschen Lemmas:

Seien K ein vollständiger bewerteter Körper mit dem Bewertungsring $\mathcal{O}$, und dem Restekörper κ, $g(X) \in \mathcal{O}[X]$ ein normiertes Polynom mit der Eigenschaft, daß das zugehörige Polynom

$$\bar{g}(X) \in \kappa[X]$$

separabel ist, und sei $\alpha_0 \in k$ eine Nullstelle von $\bar{g}$. Dann gibt es in $\mathcal{O}$ genau ein Element α mit

$$g(\alpha) = 0 \text{ und } \bar{\alpha} = \alpha_0.$$

Beweis von 3.5.7. 1. Schritt: Existenz von L.

Als endliche separable Erweiterung ist κ'/κ einfach, d.h.

$$\kappa' = \kappa(\alpha).$$

Bezeichne

$$h(X) \in \kappa[X]$$

das Minimalpolynom von α über κ.Wir ersetzen die Koeffizienten von h durch irgendwelche Repräsentanten in $\mathcal{O}$ und erhalten ein Polynom

---

[57] d.h. die beiden Zusammensetzungen der beiden nachfolgenden Funktoren sind isomorph zum identischen Funktor.

$$g(X) \in \mathcal{O}[X]$$
mit der Eigenschaft, daß das zugehörige Polynom über κ gerade h ist,
$$\bar{g}(X) = h(X).$$
Wir können dabei g so wählen, daß der höchste Koeffizient von g gleich 1 ist,
$$g(X) \text{ normiert.}$$
Seien x eine Nullstelle von g in einem Erweiterungskörper von K und
$$L := K(x).$$
Dann ist x ganz über L,
$$x \in \mathcal{O}_L$$
und die Restklasse $\bar{x}$ von x in κ_L ist eine Nullstelle des irreduziblen und separablen Polynoms $\bar{g} = h$, d.h. wir können κ_L mit κ' identifizieren,
$$\kappa_L = \kappa',$$
und zwar so, daß
$$\bar{x} = \alpha$$
wird.
Auf Grund des Struktursatzes für unverzweigte Erweiterungen (vgl. 3.5.2) ist
$$L/K \text{ unverzweigte Erweiterung.}$$
Insbesondere sind die Bedingungen (i) und (ii) erfüllt. Zeigen wir, daß auch Bedinung (iii) erfüllt ist, d.h. die Abbildung
$$\mathrm{Hom}_K(L, L') \longrightarrow \mathrm{Hom}_\kappa(\kappa_L, \kappa_{L'}), \sigma \mapsto \kappa_\sigma,$$
ist bijektiv. Sei ein κ-Homomorphismus
$$w: \kappa_L \longrightarrow \kappa_{L'},$$
vorgegeben. Mit $\bar{g}(\bar{x}) = 0$ gilt dann auch $\bar{g}(w(\bar{x})) = 0$. Nach dem Henselschen Lemma (d.h. nach der obigen Bemerkung (ii) mit L' anstelle von K) gibt es genau ein
$$x' \in \mathcal{O}_{L'} \text{, mit } g(x') = 0 \text{ und } \bar{x}' = w(\bar{x}),$$
wobei $\bar{x}'$ die Restklasse von x' in $\kappa_{L'}$ bezeichne. Da x und x' Nullstellen desselben irreduziblen Polynoms sind und die Erweiterung L von x über K erzeugt wird, gibt es genau einen K-Isomorphismus
$$\sigma: L \longrightarrow L' \text{ mit } \sigma(x) = x'.$$
Nach Konstruktion gilt $\kappa_\sigma(\bar{x}) = \bar{x}'$ und da $\bar{x}$ die Erweiterung κ_L über κ erzeugt,
$$\kappa_\sigma = w.$$
Die Abbildung von Bedingung (iii) ist somit surjektiv. Außerdem gilt für jeden K-Homomorphismus $\sigma: L \longrightarrow L'$ mit $\kappa_\sigma = w$ auch
$$\sigma(x) \bmod \wp = \kappa_\sigma(\bar{x}) = w(\bar{x}) = \bar{x}',$$
also
$$\bar{g}(\sigma(x) \bmod \wp) = \bar{g}(\kappa_\sigma(\bar{x})) = \bar{g}(\bar{x}') = 0.$$
Auf Grund der Eindeutigkeitsaussage des Henselschen Lemmas folgt $\sigma(x) = x' = w(x)$.
Weil x die Körperweiterung L über K erzeugt, folgt
$$\sigma = w.$$
Die Abbildung von Bedingung (iii) ist somit injektiv.
<u>2. Schritt</u>: L ist durch die Bedinungen (i) und (ii) bis auf Isomorphie festgelegt.

Sei L' neben L eine weitere endliche separable Körpererweiterung von K, welche den Bedingungen (i) und (ii) genügt, d.h. L' ist unverzweigt über K und hat einen zu κ' isomorphen Restekörper (über κ). Dann gibt es einen κ-Isomorphismus

$$w: \kappa_L \longrightarrow \kappa_{L'},$$

und dieser kommt von einem K-Homomorphimus

$$\sigma: L \longrightarrow L'$$

(auf Grund der gerade für L bewiesenen Aussage (iii)). Das L und L' unverzweigt sind über K, gilt außerdem

$$[L:K] =^{58} f(L/K) = [\kappa_L:\kappa] = [\kappa_{L'}:\kappa] = f(L'/K) = [L':K].$$

Deshalb ist σ ein K-Isomorphismus.

3. Schritt: L ist durch die Bedingungen (i) und (iii) bis auf Isomorphie festgelegt.

Sei L' neben L eine weitere endliche separable Körpererweiterung von K, welche den Bedingungen (i) und (iii) genügt. Dann gibt es einen κ-Isomorphismus

$$w: \kappa_L \longrightarrow \kappa_{L'},$$

und die Abbildungen

$$\mathrm{Hom}_K(L, L') \longrightarrow \mathrm{Hom}_\kappa(\kappa_L , \kappa_{L'}) , \sigma \mapsto \kappa_\sigma,$$

und

$$\mathrm{Hom}_K(L', L) \longrightarrow \mathrm{Hom}_\kappa(\kappa_{L'} , \kappa_L) , \tau \mapsto \kappa_\tau,$$

sind bijektiv. Insbesondere gibt es K-Homomorphismen

$$\sigma: L \longrightarrow L' \text{ und } \tau: L' \longrightarrow L \text{ mit } \kappa_\sigma = w \text{ und } \kappa_\tau = w^{-1}.$$

Diese insbesondere auch K-lineare Injektionen von Vektorräumen, sodaß L und L' über K dieselbe Dimension besitzen. Dann sind aber σ und τ Isomorphismen über K.

QED.

3.5.8 Der Körper L(κ') im normalen Fall

Sei K ein vollständiger diskret bewerteter Körper mit dem Bewertungsring $(\mathcal{O}, \wp)$ und dem Restkörper $\kappa = \mathcal{O}/\wp$. Sei weiter κ'/κ eine endliche separable Körper-Erweiterung. Dann sind folgende Aussagen äquivalent.

(i) L(κ') ist normal über K.

(ii) κ' ist nomal über κ.

Sind die beiden Bedingungen erfüllt so sind die Galois-Gruppen der Körpererweiterungen L(κ')/K und κ'/κ isomorph,

$$G(L(\kappa')/K) \xrightarrow{\cong} G(\kappa'/\kappa), \sigma \mapsto \kappa_\sigma.$$

Beweis. 1. Schritt. Für jede endliche separable Erweiterung E/F gilt

$$\#(\mathrm{Aut}_F E) \le [E:F].$$

Das Gleichheitszeichen besteht genau dann, wenn die Erweiterung normal ist.

Sei $\overline{F}$ die algebraische Abschließung von F und

$$X := \{\sigma_1 , ... , \sigma_\ell\}$$

---

[58] nach 3.3.7.

die Menge der F-Einbettungen

$$\sigma_i: E \longrightarrow \overline{F}$$

von E in $\overline{F}$. Weil E separabel über F ist, gilt

$$\ell = [E:F].$$

Die Zusammensetzung eines Elements von

$$\mathrm{Aut}_F(E) := \mathrm{Hom}_F(E, E)$$

mit einer Einbetung σ_i ist wieder eine solche Einbettung. Wir erhalten so eine Abbildung

$$\mathrm{Aut}_F(E) \longrightarrow X, \sigma \mapsto \sigma_1 \circ \sigma. \tag{1}$$

Weil die Einbettung σ_1 injektiv sind, gilt mit $\sigma_1 \circ \sigma = \sigma_1 \circ \tau$ stets $\sigma = \tau$, d.h. (1) ist injektiv. Insbesondere gilt

$$\#(\mathrm{Aut}_F(E)) \le \# X = \ell = [E:F]. \tag{2}$$

Identifizieren wir jetzt E vermittels σ_1 mit seinem Bild in $\overline{F}$. Die Abbildung σ_1 wird dadurch zur identischen Abbildung und $\mathrm{Aut}_F(E)$ wird durch (1) zu einer Teilmenge X.

Ist die Erweiterung L/K normal, so sind alle Konjugierten von L über K (in $\overline{F}$) gleich L, d.h. die Bilder der σ_i sind gleich L und die σ_i sind K-Automorphismen von L. Abbildung (1) ist surjektiv und in (2) gilt das Gleichheitszeichen.
Gilt umgekehrt in (2) das Gleichheitszeichen, so ist die injektive Abbildung (1) auch surjektiv. Jede K-Einbettung von E in $\overline{F}$ ist ein Automorphismus von L. Insbesondere sind die Bilder der σ_i sämlich gleich L. Die Konjugierten von L über K in $\overline{F}$ sind sämtlich gleich L, d.h. L/K ist eine normale Erweiterung.
<u>2. Schritt</u>: Bedingungen (i) und (ii) sind äquivalent.
Weil $L(\kappa')$ unverzweigt ist über κ gilt

$$[L(\kappa'):K] = f(L(\kappa'):K) = [\kappa':\kappa].$$

Außerdem gilt nach 3.5.7(iii)

$$\begin{aligned} \mathrm{Aut}_K L(\kappa') &= \mathrm{Hom}_K(L(\kappa'), L(\kappa')) \\ &\cong \mathrm{Hom}_K(\kappa', \kappa') \\ &= \mathrm{Aut}_\kappa \kappa' \end{aligned}$$

Damit ist

$$\# \mathrm{Aut}_K L(\kappa') = [L(\kappa'):K] \Leftrightarrow \# \mathrm{Aut}_\kappa \kappa' = [\kappa':\kappa].$$

Nach dem ersten Schritt bedeutet dies gerade (i) $\Leftrightarrow$ (ii).

Sind die Erweiterungen normal, so stimmen die Galois-Gruppen aber gerade mit den Automorphismen-Gruppen überein, d.h. es ist dann

$$G(L(\kappa')/K) \cong G(\kappa'/\kappa).$$

QED.

3.5.9 Maximale unverzweigte Teilerweiterungen und die Trägheitsgruppe

Sei K ein vollständiger diskret bewerteter Körper mit dem Bewertungsring $(\mathcal{O}, \wp)$ und dem Restkörper $\kappa = \mathcal{O}/\wp$. Sei weiter L/K eine endliche separable Körper-Erweiterung. Dann gibt es einen Zwischenkörper L_0

$$K \subseteq L_0 \subseteq L$$

mit der Eigenschaft, daß für jeden Zwischenkörper L',

$$K \subseteq L' \subseteq L,$$

die beiden folgenden Aussagen äquivalent sind.

(i) L'/K ist unverzweigt.

(ii) $L' \subseteq L_0$.

Außerdem gilt

$$\kappa_{L_0} = \kappa_L^s.$$

Der Zwischenkörper L_0 heißt auch <u>maximale unverzweigte Teilerweiterung</u> von L/K. Ist L/K eine Galois-Erweiterung, so ist auch L_0/K Galoissch und gleich

$$L_0 = L^{G_0}$$

dem Fixkörper der Gruppe

$$G_0 = G_0(L/K) := \{ \sigma \in G(L/K) \mid v_L(\sigma(x) - x) > 0 \text{ für jedes } x \in \mathcal{O}_L \}.$$

Die Gruppe G_0(L/K) heißt <u>Trägheitsgruppe</u> der Erweiterung L/K.

Bemerkung

Nach Definition besteht die Trägheitsgruppe aus denjenigen Elementen

$$\sigma: L \longrightarrow L$$

der Galoisgruppe, welche auf dem Restkörper die identische Abbildung

$$\kappa_\sigma = \mathrm{Id}: \kappa_L \longrightarrow \kappa_L$$

induzieren.

Beweis. Nach 3.5.7 gibt es eine (bis auf K-Isomorphie eindeutig bestimmte) unverzweigte Erweiterung L_0 von K mit

$$\kappa_{L_0} = \kappa_L^s.$$

Ebenfalls nach 3.5.7 kommt die natürlichen Einbettung

$$\kappa_{L_0} = \kappa_L^s \hookrightarrow \kappa_L$$

von einer K-Einbettung $\sigma: L_0 \hookrightarrow L$. Wir können L_0 durch sein Bild bei σ ersetzen, und erreichen so, daß L_0 ein Körper zwischen K und L wird,

$$K \subseteq L_0 \subseteq L.$$

Alle Körper L' zwischen K und L_0 sind dann unverzweigt.[59]

---

[59] Weil $\kappa_{L'}$, als Teilerweiterung von κ_{L_0} separabel ist über κ und weil e(L'/K) ein Teiler von $e(L_0/K)$ = 1 ist.

Sei jetzt L'ein Körper zwischen K und L, welcher unverzweigt ist über K,

$$K \subseteq L' \subseteq K,\ L'/K \text{ unverzweigt.}$$

Dann gilt $\kappa_{L'} \subseteq \kappa_L$ und $\kappa_{L'}$ ist separabel über κ, d.h.

$$\kappa_{L'} \subseteq \kappa_L^s = \kappa_{L_0}.$$

Nach 3.5.7 kommt diese κ-Einbettung von einer K-Einbettung

$$\sigma: L' \hookrightarrow L_0.$$

Wir wählen ein Element

$$x \in \mathcal{O}_{L'} \subseteq L',$$

dessen Restklasse die Erweiterung $\kappa_{L'}/\kappa$ erzeugt,

$$\kappa_{L'} = \kappa[\bar{x}]. \tag{1}$$

Dann sind x und $\sigma(x)$ Elemente von $\mathcal{O}_L$ mit derselben Restklasse $\bar{x}$ in $\kappa_{L'}$,[60] wobei letztere separabel über κ ist. Nach dem Henselschen Lemma (vgl. Bemerkung 3.5.7 (ii))[61] ist deshalb

$$\sigma(x) = x.$$

Nach dem Struktursatz für unverzweigte Erweiterungen (3.5.2) gilt mit (1) auch L' = K(x), d.h. σ ist die identische Abbildung und es gilt

$$L' \subseteq L_0.$$

Wir haben gezeigt, für Körper L' zwischen K und L sind die beiden Bedingungen (i) und (ii) äquivalent, d.h. der konstruierte Körper L_0 ist ein Körper mit der behaupteten Eigenschaft. Nach Konstruktion von L_0 ist

$$\kappa_{L_0} = \kappa_L^s.$$

Wir haben noch den Spezialfall, daß L/K eine Galois-Erweiterung ist, zu betrachten. Dann sind alle zu L_0 über K konjugierten Körper zwischen K und L unverzweigt, liegen also in L_0, und sind damit (aus Gradgründen) gleich L_0. Der Körper L_0 ist somit normal über K, d.h.

$$L_0/K \text{ ist eine Galois-Erweiterung.}$$

Die Trägheitsgruppe G_0 ist nach Definition gerade der Kern der Abbildung

$$G(L/K) \longrightarrow \mathrm{Aut}_\kappa(\kappa_L),\ \sigma \mapsto \kappa_\sigma.$$

Nun ist nach Bemerkung 3.5.3(iii) die Einschränkungs-Abbildung

$$\mathrm{Aut}_\kappa(\kappa_L) \longrightarrow \mathrm{Aut}_\kappa(\kappa_L^s) = G_\kappa(\kappa_L^s),\ f \mapsto f|_{\kappa_L^s}$$

injektiv. Deshalb ist G_0 auch der Kern der Abbildung

---

[60] weil σ die natürliche Einbettung $\kappa_{L'} \hookrightarrow \kappa_L^s$ induziert.

[61] Weil L'/K unverzweigt ist, ist das zum Minimalpolynom von x bzw. σx gehörige Polynom über κ gerade das Minimalpolynom von $\bar{x}$ über κ, also irreduzibel und separabel (nach dem Struktursatz für unverzweigte Erweiterungen, vgl. 3.5.2 (i)).

$$G(L/K) \longrightarrow G_\kappa(\kappa_L^s) = G_\kappa(\kappa_{L_0}), \sigma \mapsto \kappa_\sigma^s .$$

Weil L_0 unverzweigt ist über K, können wir die Galois-Gruppe rechts mit der von L_0/K identifizieren (nach 3.5.8). Wir sehen so, G_0 ist der Kern der Einschränkungsabbildung

$$G(L/K) \longrightarrow G(L_0/K), \sigma \mapsto \sigma|_{L_0} ,$$

d.h.

$$G_0 = G(L/L_0).$$

Nach dem Hauptsatz der Galois-Theorie ist L_0 der Fixkörper von G_0.

QED.

3.5.10 Das Kompositum unverzweigter Erweiterungen

Sei K ein vollständiger diskret bewerteter Körper mit dem Bewertungsring $(\mathcal{O}, \wp)$, dem Restkörper $\kappa = \mathcal{O}/\wp$ und der separablen Abschließung $\bar{K}^s$.

Für je zwei Zwischenkörper

$$K \subseteq L_i \subseteq \bar{K}^s \quad (i = 1,2)$$

welche endlich und unverzweigt über K sind, ist dann auch das Kompositum

$$L_1L_2$$

unverzweigt über K.

Beweis. Seien

$$L := L_1L_2$$

und L_0 die maximale unverzweigte Teilerweiterung von L/K. Nach Definition (vgl. 3.5.9) gilt dann $L_1 \subseteq L_0$ und $L_2 \subseteq L_0$, also

$$L_1L_2 \subseteq L_0 \subseteq L = L_1L_2 ,$$

d.h. $L = L_0$ ist unverzweigt über K.

QED.

3.5.11 Maximale unverzweigte Erweiterungen K_{nr}

Sei K ein vollständiger diskret bewerteter Körper mit dem Bewertungsring $(\mathcal{O}, \wp)$, dem Restkörper $\kappa = \mathcal{O}/\wp$ und der separablen Abschließung $\bar{K}^s$.

Dann wird die Vereinigung aller endlichen Zwischenkörper L,

$$K \subseteq L \subseteq \bar{K}^s$$

mit

$$L/K \text{ unverzweigt}$$

mit[62]

$$K_{nr}$$

bezeichnet und heißt <u>maximale unverzweigte Erweiterung</u> von K.

Bemerkung

Die Menge K_{nr} ist auch die Vereinigung aller Zwischenkörper L,

$$K \subseteq L \subseteq \bar{K}^s$$

[62] nr steht für “none-ramified”.

mit

L/K unverzweigt und normal,

d.h.

$$K_{nr} = \bigcup X \text{ mit } X := \{ L \mid K \subseteq L \subseteq K_{nr}, L/K \text{ unverzweigt und normal} \} \quad (1)$$

Beweis. Die in der Bemerkung definierte Menge ist als Vereinigung von weniger Mengen in K_{nr}. Wir haben die umgekehrte Inklusion zu beweisen. Dazu reicht es zu zeigen, zu jedem Zwischenkörper L,

$$K \subseteq L \subseteq \bar{K}^s$$

mit L/K unverzweigt gibt es einen Zwischenkörper L',

$$K \subseteq L' \subseteq \bar{K}^s$$

mit L'/K unverzweigt und normal, wobei gilt

$$L \subseteq L'.$$

Zur Konstruktion von L' wählen wir ein Element $\alpha \in L$, welches L über K erzeugt,

$$L = K(\alpha),$$

und betrachten den Zerfällungskörper L" des Minimalpolynoms von α über K. Es gilt[63]

$$K \subseteq L \subseteq L'' \subseteq \bar{K}^s \text{ und } L''/K \text{ normal.}$$

Sei L' die maximale unverzweigte Teilerweiterung von L"/K. Weil L/K unverzweigt ist, gilt $L \subseteq L'$, zusammen also

$$K \subseteq L \subseteq L' \subseteq L'' \subseteq \bar{K}^s.$$

Nach 3.5.9 ist mit L"/K auch L'/K eine unverzweigte Galois-Erweiterung,

L'/K unverzweigt und Galoissch.

Mit anderen Worten, L' ist ein Körper der gesuchten Art.

QED.

3.5.12 Eigenschaften von K_{nr}

Sei K ein vollständiger diskret bewerteter Körper mit dem Bewertungsring $(\mathcal{O}, \wp)$, dem Restkörper $\kappa = \mathcal{O}/\wp$ und der separablen Abschließung $\bar{K}^s$. Dann gilt:

(i) K_{nr}/K ist eine <u>unendliche Galois-Erweiterung</u>, d.h.

1. K_{nr} ist ein Körper
2. Jedes Element von K_{nr} ist algebraisch separabel über K.
3. Liegt ein Element $\alpha \in \bar{K}^s$ in K_{nr}, so gilt dasselbe für alle zu α konjugierten Elemente von $\bar{K}^s$.

(ii) Jede endliche Teilerweiterung von K_{nr}/K ist unverzweigt über K.

(iii) Die Galois-Gruppe $G(K_{nr}/K)$ ist als topologische Gruppe isomorph zur Galois-Gruppe $G(\bar{\kappa}^s/\kappa)$ der separablen Abschließung $\bar{\kappa}^s$ von κ.

---

[63] Die Inklusion links besteht trivialerweise. Der Körper L" wird von α und den Konjugierten von α erzeugt. Also gilt

$$L \subseteq L''.$$

Mit α sind auch alle Konjugierten von α separabel über K, also gilt

$$L'' \subseteq \bar{K}^s.$$

Beweis. Zu (i). Zeigen wir, die Menge K_{nr} genügt den drei angegebenen Bedingungen.

Bedingung 1. Seien α, $\beta \in K_{nr}$. Es reicht zu zeigen, es gibt einen ganz in K_{nr} enthaltenen Körper, welcher die Elemente α und β enthält. Zum Beispiel reicht es zu zeigen,

$$K(\alpha, \beta) \subseteq K_{nr}.$$

Dazu reicht es zu zeigen,

$$K(\alpha, \beta)/K \text{ ist unverzweigt.}$$

Nun ist

$$K(\alpha, \beta) = K(\alpha)K(\beta)$$

gerade das Kompositum von $K(\alpha)$ und $K(\beta)$. Nach 3.5.10 reicht es zu zeigen,

$$K(\alpha) \text{ und } K(\beta) \text{ sind unverzweigt über } K.$$

Nach Wahl von α und β gibt es Körperweiterungen L_α und L_β von K mit

$$\alpha \in L_\alpha \text{ und } \beta \in L_\beta \text{ und mit } L_\alpha \text{ und } L_\beta \text{ unverzweigte über } K.$$

Als Teilkörper von L_α bzw. L_β sind dann aber auch $K(\alpha)$ und $K(\beta)$ unverzweigt über K.

Bedingung 2. Jedes Element $\alpha \in K_{nr}$ liegt nach Definition von K_{nr} in einer endliche separablen und unverzweigten Körper-Erweiterung von K, ist also insbesondere algebraisch und separabel über K.

Bedingung 3. Nach der Bemerkung von 3.5.11 gibt es für jedes $\alpha \in K_{nr}$ einen Zwischenkörper L,

$$K \subseteq L \subseteq K_{nr}$$

mit $\alpha \in L$ und L/K normal (und unverzweigt). Dann liegen aber alle Konjugierten von α über K ebenfalls in L, also erst recht in K_{nr}.

Zu (ii). Sei L/K eine endliche Teilerweiterung von K_{nr}/K. Als endliche separable Erweiterung ist dann L/K einfach, sagen wir

$$L = K(\alpha).$$

Nach Definition von K_{nr} gibt es eine endliche unverzweigte Teilerweiterung L'/K von K_{nr}/(K, welche das Element α enthält. Dann gilt aber

$$K \subseteq L \subseteq L',$$

und mit L'/K ist auch L/K unverzweigt.

Zu (iii). 1. Schritt: Beschreibung von $G(K_{nr}/K)$.

Wie in der Bemerkung von 2.5.11 schreiben wir K_{nr} in der Gestalt

$$K_{nr} = \bigcup X \text{ mit } X := \{ L \mid K \subseteq L \subseteq K_{nr}, L/K \text{ unverzweigt und normal } \} \quad (1)$$

Jeder K-Automorphismus σ von K_{nr}/K induziert auf jedem $L \in X$ einen K-Automorphismus und die Einschränkung auf L definiert einen surjektiven Gruppen-Homomorphismus

$$\varphi_L : G(K_{nr}/K) \twoheadrightarrow G(L/K),\ \sigma \mapsto \sigma|_L\ ,\ (L \in X).$$

Da jedes $x \in K_{nr}$ in einem $L \in X$ liegt, ist ein Automorphismus $\sigma \in G(K_{nr}/K)$ durch seine Einschränkunken auf die Körper $L \in X$ bereits eindeutig festgelegt, d.h. die Abbildung

$$\varphi : G(K_{nr}/K) \longrightarrow \prod_{L \in X} G(L/K),\ \sigma \mapsto (\varphi_L(\sigma))_{L \in X}\ , \tag{2}$$

ist ein injektiver Gruppen-Homomorphismus.

Für je zwei Elemente L', L" $\in$ X mit L' $\subseteq$ L" definiert die Einschränkungsabbildung einen Gruppen-Homomorphismus

$$\varphi_{L'',L'} : G(L''/K) \longrightarrow G(L'/K),\ \sigma \mapsto \sigma|_{L'}\ ,$$

Auf Grund der bekannten Fortsetzungssätze der Theorie der algebraischen Körper-Erweiterungen ist dieser Homomorphismus surjektiv. Trivialerweise ist das Diagramm

$$\begin{tikzcd}
G(K_{nr}) \arrow[r, "\varphi_{L''}"] \arrow[d, "\varphi_{L},L"'] & G(L''/K) \arrow[dl, "\varphi_{L'',L'}"] \\
G(L'/L) &
\end{tikzcd} \tag{3}$$

kommutativ für beliebige L', L" $\in$ X mit L'$\subseteq$L". Mit anderen Worten, für jedes Element

$$\sigma := (\sigma_L)_{L \in X} \tag{4}$$

aus dem Bild von φ gilt

$$0 = \varphi_{L'',L'}(\sigma_{L''}) - \sigma_{L'} = (\varphi_{L'',L'} \circ pr_{L''} - pr_{L'})(\sigma) \tag{5}$$

für L' $\subseteq$ L", wenn pr_L die Projektion auf die L-te Koordinate bezeichbnet. Sei umgekehrt (4) ein Element aus dem direkten Produkt der G(L/K) welches, der Bedinung (5) genügt. Dann ist

$$\sigma_L : L \longrightarrow L$$

ein K-Automorphismus und für L' $\subseteq$ L" ist $\sigma_{L'}$ gerade die Einschränkung von $\varphi_{L''}$ auf L'. Für jedes $x \in K_{nr}$ ist

$$\sigma_L(x)$$

für jedes L mit $x \in L$ wohldefiniert und unabhängig[64] von der Wahl des speziellen L. Indem wir $\sigma(x) = \sigma_L(x)$ für $x \in L$ setzen, erhalten wir einen wohldefinierten K-Automorphismus von K_{nr}/K, dessen Bild bei φ gerade das vorgegebene Element σ ist. Wir haben gezeigt,

---

[64] Der Durchschnitt L' aller L mit $x \in L$ ist eine endliche Galois-Erweiterung von K, liegt in X, und es gilt

$$\sigma_{L'}(x) = \sigma_L(x) \text{ für jedes L mit } x \in L.$$

$$G(K_{nr}/K) \cong \{ (\sigma_L) \in \prod_{L\in X} G(L/K) \mid \varphi_{L'',L'}(\sigma_{L''}) = \sigma_{L'} , \text{ für } L' \subseteq L'' \}, \qquad (6)$$

d.h. die Galois-Gruppe $G(K_{nr}/K)$ ist eine Untergruppe des direkten Produkts der endlichen Gruppe G(L/K). Dieser Isomorphismus bedeutet gerade, daß

$$G(K_{nr}/K)$$

inverser Limes der endlichen Gruppen G(L/K) bezüglich der Homomorphismen φ_L ist. Gruppen dieser Art heißen proendliche Gruppen.

2. Schritt: Beschreibung einer Topologie von $G(K_{nr}/K)$.
Wir versehen die endlichen Gruppen G(L/K) mit der diskreten Topologie, das direkte Produkt

$$\prod_{L\in X} G(L/K)$$

mit der Produkt-Topologie[65] und die Untergruppe $G(K_{nr}/K)$ mit der Unterraum-Topologie. Wir erhalten dann gerade die stärkste Topologie der Menge $G(K_{nr}/K)$, für welche alle Abbildungen

$$\varphi_L: G(K_{nr}/K) \longrightarrow G(L/K)$$

stetig sind. Diese Topologie heißt auch proendliche Topologie.

Die Mengen der Gestalt

$$\mathrm{Ker}(\varphi_L) = \varphi_L^{-1}(\mathrm{Id})$$

sind gleichzeitig offen und abgeschlossen. Für je zwei L', L'' $\in$ X liegt auch das Komposition in X und es gilt

$$\mathrm{Ker}(\varphi_{L'L''}) = \mathrm{Ker}(\varphi_{L'}) \cap \mathrm{Ker}(\varphi_{L''}).$$

Es ist nicht schwer zu sehen, die Mengen der Gestalt $\mathrm{Ker}(\varphi_L)$ bilden gerade eine Umgebungsbasis des neutralen Elements von $G(K_{nr}/K)$ für die proendliche Topologie, d.h. die offenen Mengen der proendlichen Topologie sind gerade die Vereinigungen aller Mengen der Gestalt

$$g\bullet \mathrm{Ker}(\varphi_L) \text{ mit } g \in G(K_{nr}/K) \text{ und } L \in X.$$

3. Schritt: Isomorphie von $G(K_{nr}/K)$ und $G(\overline{\kappa}^s/\kappa)$ als topologische Gruppen.
Aus der Isomorphie (6) und der Beschreibung der proendlichen Topologie der Gruppe $G(K_{nr}/K)$ ergibt sich, daß die topologische Gruppe $G(K_{nr}/K)$ durch die endlichen Gruppen der Gestalt G(L/K) mit L$\in$X und die Homomorphismen

$$\varphi_{L'',L'}$$

bereits eindeutig bestimmt ist.
Wenn wir die obigen Betrachtungen mit $\overline{\kappa}^s/\kappa$ anstelle von K_{nr}/K wiederholen, erhalten wir

[65] d.h. mit der stärksten Topologie, bei welcher für jedes L die Projektion auf die L-te Koordinaten stetig ist.

$$G(\overline{\kappa}^s/\kappa) \cong \{ (\sigma_\lambda) \in \prod_{\lambda\in Y} G(L/K) \mid \varphi_{\lambda'',\lambda'}(\sigma_{\lambda''}) = \sigma_{\lambda'} \text{ für } \lambda' \subseteq \lambda'' \}, \qquad (7)$$

wenn Y aus den endlichen Teilerweiterungen λ/κ von $\overline{\kappa}^s/\kappa$ besteht. Nun sind nach Konstruktion die $L \in X$ unverzweigte Galois-Erweiterungen von K, d.h. es gilt

$$G(L/K) \cong G(\lambda/\kappa),$$

wenn λ den Restekörper von L bezeichnet (vgl. 3.5.8). Bei diesen Isomorphismen entsprechen die Abbildungen $\varphi_{L'',L'}$ von Formel (6) gerade den Abbildungen $\varphi_{\lambda'',\lambda'}$ von Formel (7), d.h. die rechten Seiten von (6) und (7) sind isomorph zueinander als topologische Gruppen. Dasselbe gilt damit auch für die linken Seiten.
QED.
Bemerkung
Die endlichen Gruppen auf der rechten Seite von (6) bzw. (7) sind bezüglich der diskreten Topologie vollständig.[66] Nach dem Satz von Tichonov ist dann aber auch deren direktes Produkt vollständig. Dasselbe gilt dann aber auch für die abgeschlossenen Untergruppen (6) und (7), d.h.

$$G(K_{nr}/K) \cong G(\overline{\kappa}^s/\kappa) \text{ ist eine vollständige topologische Gruppe.}$$

(Dieselbe Argumentation zeigt für jede proendliche Gruppe deren Vollständigkeit).

3.5.13 Die Galois-Gruppe von K_{nr} im Fall lokaler Körper

Sei K ein lokaler Körper (vgl. 3.1.2) mit dem Restkörper κ, welcher aus

$$q = \# \kappa$$

Elementen bestehe..Dann gibt es genau einen Automorphismus

$$\sigma_q \in G(K_{nr}/K)$$

mit

$$\sigma_q(\alpha) \equiv \alpha^q \bmod \wp_L$$

für jede endliche Teilerweiterung L/K von K_{nr}/K und jedes Element $\alpha \in \mathcal{O}_L$. Die Abbildung

$$\mathbb{Z} \longrightarrow G(K_{nr}/K),\ n \mapsto \sigma_q^n,$$

induziert einen Isomorphismus topologischer Gruppen

$$\hat{\mathbb{Z}} \longrightarrow G(K_{nr}/K).$$

Dabei bezeichne $\hat{\mathbb{Z}}$ die Vervollständigung der additiven Gruppe $\mathbb{Z}$ bezüglich der Topologie, für welche die Untergruppen der Gestalt

$$n\mathbb{Z}$$

eine Umgebungsbasis des neutralen Elements $0 \in \mathbb{Z}$ bilden. Genauer, $\hat{\mathbb{Z}}$ ist die proendliche Gruppe

$$\hat{\mathbb{Z}} = \{ (x_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z} \mid \varphi_{dn,n}(x_{dn}) = x_n \text{ für alle } n, d \in \mathbb{N}\}$$

Dabei bezeichne $\varphi_{dn,n}$ die natürliche Abbildung

[66] Bezüglich der diskreten Topologie ist jede Cauchy-Folge stationär, also konvergent.

$$\varphi_{dn,n}: \mathbb{Z}/dn\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z},\ x \bmod dn\mathbb{Z} \mapsto x \bmod n\mathbb{Z}.$$

Beweis. Bezeichne

$$F := \mathbb{F}_p$$

den Primkörper des endlichen Körpers κ und

$$\ell := [\kappa: F]$$

dessen Grad über dem Primkörper, d.h. es sei

$$q = p^{\ell}.$$

Jede endliche Teilerweiterung L/K von K_{nr}/K ist unverzweigt (nach Definition von K_{nr} in 3.5.11). Die zugehörige Erweiterung der Restkörper

$$\kappa_L/\kappa$$

ist eine Erweiterung von endlichen Körpern. Sei

$$f := f(L/K) = [\kappa_L : \kappa]$$

der Grad der Erweiterung der Restekörper. Dann besteht der Körper κ_L aus

$$\# \kappa_L = q^n = p^{n\ell}$$

Elementen, nämlich der Null und den $(q^n\text{-}1)$-ten Einheitwurzeln, d.h. den Nullstellen des Polynoms

$$X^{q^n-1} - 1 \qquad (1)$$

in einer algebraischen Abschließung

$$\overline{F}$$

von F. Insbesondere ist κ_L der Zerfällungskörper dieses Polynoms, also normal über F und κ, also Galoissch. Die Galois-Gruppe über F wird erzeugt von der Frobenius-Abbildung,

$$G(\kappa_L/F) = < \sigma >, \sigma(x) = x^p$$

Man beachte, die Frobenius-Abbildung ist für jedes Element von $\overline{F}$ definiert, und läßt sich als Automorphismus von $\overline{F}$ auffassen,

$$\sigma: \overline{F} \longrightarrow \overline{F},\ x \mapsto x^p.$$

Weil die Einschränkung von σ auf κ_L die Galois-Gruppe erzeugt und diese die Ordnung

$$\# G(\kappa_L|F) = [\kappa_L:F] = [\kappa_L:\kappa]\cdot[\kappa:F] = n\ell$$

hat, gilt

$$\sigma \text{ hat die Ordnung } n\ell \text{ auf } \kappa_L.$$

Analog hat σ auf κ die Ordnung ℓ. Die Abbildung $i \mapsto \sigma^i$ definiert damit Isomorphismen

$$\psi_{\ell}: \mathbb{Z}/\ell\mathbb{Z} \longrightarrow G(\kappa/F),\ i \bmod \ell\mathbb{Z} \mapsto \sigma^i$$

$$\psi_{n\ell}: \mathbb{Z}/n\ell\mathbb{Z} \longrightarrow G(\kappa/F),\ i \bmod n\ell\mathbb{Z} \mapsto \sigma^i$$

und ein kommutatives Diagramm

$$\begin{array}{ccc} \mathbb{Z}/n\ell\mathbb{Z} & \xrightarrow{\psi_{n\ell}} & G(\kappa_L/F) \\ \downarrow \varphi_{n\ell,\ell} & & \downarrow \varphi_{\kappa_L, F} \\ \mathbb{Z}/\ell\mathbb{Z} & \xrightarrow{\psi_\ell} & G(\kappa/F) \end{array}$$

Dabei ist die linke vertikale Abbildung der natürlichen Homomorphismus und die rechte vertikale Abbildung der Einschränkungshomomorphismus. Der Kern der ersteren ist

$$\ell\mathbb{Z}/n\ell\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z},\ i\ell \bmod n\ell\mathbb{Z} \mapsto i \bmod n\mathbb{Z},$$

und der Kern der letzteren ist

$$G(\kappa_L/\kappa).$$

Da die horizontalen Abbildungen Isomorphismen sind, erhalten wir einen Isomorphismus der Kerne,

$$\psi_n: \mathbb{Z}/n\mathbb{Z} \xrightarrow{\cong} G(\kappa_L/\kappa),\ i \bmod n\mathbb{Z} \mapsto \sigma^{i\ell}$$

Insbesondere entspricht der Restklasse von 1 gerade der Erzeuger

$$\sigma^\ell: \kappa_L \longrightarrow \kappa_L,\ x \mapsto \sigma^\ell(x) = x^{p^\ell} = x^q$$

von $G(\kappa_L/\kappa)$. Die Isomorphismen ψ_n fügen sich in kommutative Diagramme der Gestalt

$$\begin{array}{ccccc} \mathbb{Z}/n"\mathbb{Z} & \xrightarrow{\psi_{n"}} & G(\kappa_{L"}/\kappa) & & i \mapsto \sigma^{i\ell} \\ \varphi_{n",n'}\downarrow & & \downarrow\varphi_{\kappa_{L"},\kappa_{L'}} & & \downarrow \quad\quad \downarrow \\ \mathbb{Z}/n'\mathbb{Z} & \xrightarrow{\psi_{n'}} & G(\kappa_{L'}/\kappa) & & i \mapsto \sigma^{i\ell} \end{array}$$

ein für je zwei endliche Teilerweiterungen L'/K und L"/K von K_{nr}/K mit $L' \subseteq L"$ und

$$n' := [L':K] \text{ und } n" := [L":K]$$

(man beachte, wegen $L' \subseteq L"$ gilt $n" = dn'$ mit $d := [L":L']$).

Die Abbildungen dieser Diagramme können wir auch als stetigen Abbildungen bezüglich der diskreten Topologien auffassen. Wir gehen zu den direkten Produkten der beteilligten n Gruppen über und dann zu den abgeschlossenen Untergruppen, welche die projektiven Limites darstellen.

$$\begin{aligned} G(K_{nr}/K) &\cong G(\overline{F}/\kappa) \\ &\cong^{67} \{ (\sigma_\lambda) \in \prod_{\lambda\in Y} G(L/K) \mid \varphi_{\lambda",\lambda'}(\sigma_{\lambda"}) = \sigma_{\lambda'} \text{ für } \lambda' \subseteq \lambda" \} \\ &\cong \{ (x_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z} \mid \varphi_{dn,n}(x_{dn}) = x_n \text{ für alle } n, d \in \mathbb{N} \} \\ &= \hat{\mathbb{Z}} \end{aligned}$$

Die Topologie der Gruppe $\hat{\mathbb{Z}}$ ist dabei gerade durch die Topologie-Basis des neutralen Elements gegeben, die aus den Kernen der natürlichen Surjektionen

---

[67] vgl. (7) von 3.5.12.

$$\hat{\mathbb{Z}} \longrightarrow \mathbb{Z}/n\mathbb{Z},\ (x_n)_{n\in\mathbb{N}} \mapsto x_n,$$

besteht. Wir haben noch $\hat{\mathbb{Z}}$ mit $\mathbb{Z}$ zu vergleichen. Dazu betrachten wir die Abbildung

$$\mathbb{Z} \longrightarrow \hat{\mathbb{Z}},\ x \mapsto (x + n\mathbb{Z})_{n\in\mathbb{N}},$$

welche jede ganze Zahl x auf die "konstante" Familie abbildet. Diese Abbildung ist ein wohldefinierter[68] Gruppen-Homomorphismus. Ihr Kern ist gerade der Durchschnitt

$$\bigcap_{n\in\mathbb{N}} n\mathbb{Z} = (0),$$

d.h. die Abbildung ist injektiv. Wir können also $\mathbb{Z}$ als Teilmenge von $\hat{\mathbb{Z}}$ auffassen. Die auf $\mathbb{Z}$ dadurch definierte Unterraum-Topologie ist durch die Umgebungsbasis der Null gegeben, die aus den Kernen der Abbildungen

$$\mathbb{Z} \longrightarrow \hat{\mathbb{Z}} \longrightarrow \mathbb{Z}/n\mathbb{Z}\ ,\ x \mapsto (x+n\mathbb{Z})_{n\in\mathbb{N}} \mapsto x_n\ ,$$

besteht, d.h. aus den Untergruppen der Gestalt $n\mathbb{Z}$.

Wir haben noch zu zeigen, $\mathbb{Z}$ liegt dicht in $\hat{\mathbb{Z}}$. Sei

$$(x_n)_{n\in\mathbb{N}} \in \hat{\mathbb{Z}}$$

Wir haben zu zeigen, dieses Element kann beliebig gut durch eine ganze Zahl approximiert werden. Zu zeigen ist, für jedes m gibt es ein $x \in \mathbb{Z}$ derart, daß die Differenz

$$(x_n)_{n\in\mathbb{N}} - (x+n\mathbb{Z})_{n\in\mathbb{N}},$$

im Kern der natürlichen Abbildung $\hat{\mathbb{Z}} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ liegt, d.h.mit

$$x_m = x \bmod m\mathbb{Z}.$$

Wegen $x_m \in \mathbb{Z}/m\mathbb{Z}$ kann man für x einen Repräsentanten von x_m in $\mathbb{Z}$ wählen.

QED.

Bemerkung

Für $n \in \mathbb{N}$ and betrachten wir die Zerlegung von n in ein Produkt von Primzahl-Potenzen betrachten, sagen wir

$$n = p_1^{a_1}\bullet\ldots\bullet p_r^{a_r}.$$

Nach dem chinesischen Reste-Satz erhalten wir eine Zerlegung in ein direktes Produkt

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/\, p_1^{a_1}\mathbb{Z} \times\ldots\times \mathbb{Z}/\, p_r^{a_r}\mathbb{Z}.$$

Wir können nun das direkte Produkt über alle $n \in \mathbb{N}$ bilden und dann zum projektiven Limes übergehen. Es ist nicht schwer, zu zeigen (Übungsaufgabe!), daß man so eine Zerlegung

$$\hat{\mathbb{Z}} \cong \prod_p \hat{\mathbb{Z}}_p$$

erhält, wobei das Produkt über alle Primzahlen p zu erstrecken ist und

[68] Sie ist zunächst als Abbildung mit Werten im direkten Produkt wohldefiniert. Ihre Werte liegen aber sogar in der Teilmenge $\hat{\mathbb{Z}}$.

$$\hat{\mathbb{Z}}_p := \{ (x_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z} \mid \varphi_{p^{dn},p^n}(x_{dn}) = x_n \text{ für alle } n, d \in\mathbb{N}\}$$

gilt, d.h. $\hat{\mathbb{Z}}_p$ ist die Vervollständigung von $\mathbb{Z}$ ch der Topologie, für welche die Ideale der Gestalt

$$p^n\mathbb{Z}$$

eine Umgebungsbasis der 0 bilden. Dies ist aber gerden die p-adische Topologie, d.h.

$$\hat{\mathbb{Z}}_p$$

ist gerade die Gruppe der p-adischen ganzen Zahlen (d.h. die additive Gruppe des Bewertungsrings von $\mathbb{Q}_p$).

3.5.14 Der Körper K_{nr} für lokale Körper K

Sei K ein lokaler Körper, dessen Restekörper κ die Charakteristik p besitzt. Dann wird

$$K_{nr}$$

über K erzeugt von den n-ten Einheitswurzeln, wobei n alle zu p teilerfrenden natürlichen Zahlen durchläuft.

Beweis. <u>1. Schritt</u>. Jede (endliche separable) unverzweigte Erweiterung von K entsteht durch Adjunktion einer n-ten Einheitswurzel mit n teilerfremd zu p.

Sei

$$L/K$$

eine endliche, separable unverzweigte Erweiterung. Dann gibt es nach dem Struktursatz für unverzweigte Erweiterungen 3.5.2 ein $x \in \mathcal{O}_L$ mit

$$L = K(x),\ \mathcal{O}_L = \mathcal{O}[x],\ \kappa_L = \kappa(\bar{x}),$$

wobei $\bar{x}$ die Restklass von x in κ_L bezeichne.Weil die Restekörper endlich sind, also aus Einheitswurzeln bestehen, ist insbesondere $\bar{x}$ eine Einheitswurzel, sagen wir

$$\bar{x}^n = 1.$$

O.B.d.A. sei $\bar{x}$ eine primitive n-te Einheitswurzel[69]. Angenommen $p \ne 0$ und $p \mid n$. Wir betrachten die Abbildung

$$\kappa_L \longrightarrow \kappa_L,\ x \mapsto x^p.$$

Weil die Charakteristik von κ_L gleich p ist, ist dies ein Homomorphismus von Ringen mit 1. Weil κ_L als Körper keine nilpotenten Elemente besitzt, der Kern trivial, und weil κ_L endlich ist, ist dies ein Isomorphismus. Insbesondere gilt mit

$$(\bar{x}^{n/p})^p = \bar{x}^n = 1 = 1^p.$$

auch $\bar{x}^{n/p}$ (wegen der Injektivität). Die Einheitswurzel ist somit nicht primitiv, im Widerspruch zu den Voraussetzungen. Wir haben gezeigt,

n ist teilerfremd zur Charakteristik p falls $p \ne 0$ ist.

Damit ist das Polynom $X^n - 1$ separabel, und $\bar{x}$ ist Nullstelle dieses Polynoms. Nach dem Henselschen Lemma gibt es ein eindeutig bestimmtes

[69] d.h. die n-te Potenz sei die erste, welche gleich 1 ist.

$$y \in \mathcal{O}_L \text{ mit } y^n = 1 \text{ und } \bar{y} = \bar{x}.$$

Weil L/K unverzweigt ist, gilt dasselbe auch für die Teilerweiterung

$$L'/K \text{ mit } L' := K(y).$$

Es folgt

$$\bar{x} = \bar{y} \in \kappa_{L'} \subseteq \kappa_L = \kappa(\bar{x}),$$

also $\kappa_{L'} = \kappa_L$, also

$$\begin{aligned} [L':K] &= f(L'|K) && \text{(L'/K ist unverzweigt)} \\ &= [\kappa_{L'}:\kappa] \\ &= [\kappa_L:\kappa] \\ &= f(L|K) \\ &= [L:K] && \text{(L/K ist unverzweigt),} \end{aligned}$$

also

$L = L' = L(y)$, y n-te Einheitswurzelt.

<u>1. Schritt</u>. Durch Adjunktion einer n-ten Einheitswurzel zu K mit n teilerfremd zu p entsteht eine unverzweigte Erweiterung.

Sei x eine n-te Einheitswurzel in einer algebraischen Abschließung

$$\bar{K}$$

von K, d.h.

$$x \in \bar{K},\ x^n = 1.$$

Wir setzen

$$L := K(x)$$

und haben zu zeigen, L/K ist unverzweigt.

O.B.d.A. sei x eine primitive n-te Einheitswurzel.[70]

Die Erweiterung ist offensichtlich endlich und nach Wahl von n auch separabel.[71] Für die Restklasse

$$\bar{x} \in \kappa_L$$

von x gilt ebenfalls

$$\bar{x}^n = 1.$$

Insbesondere ist die Teilerweiterung

$$\kappa'/\kappa \text{ mit } \kappa' := \kappa(\bar{x})$$

von κ_L/κ separabel. Es gibt deshalb eine unverzweigte Erweiterung $L' := L(\kappa')$ mit $\kappa_{L'} = \kappa'$ (nach 3.5.7):

L'/K ist unverzweigt über K

$\kappa_{L'} = \kappa' = \kappa(\bar{y})$

Wir wählen ein $y \in \mathcal{O}_{L'}$, mit $\bar{y} = \bar{x}$. Dann gilt

---

[70] Andernfalls können wir n durch einen Teiler von n ersetzen.

[71] Falls die Charakteristik von K ungleich Null ist, ist diese gleich der Charakteristik p von κ. Insbesondere ist dann n teilerfremd zur Charakteristik und die Ableitung nX^{n-1} des Polynoms $X^n - 1$ nicht identisch Null und teilerfremd zu $X^n - 1$, d.h. $X^n - 1$ hat keine mehrfachen Nullstellen, ist somit separabel.

$$L' := L(y)$$
$$\mathcal{O}_{L'} = \mathcal{O}[y]$$
(nach dem Struktursatz 3.5.2 für unverzweigte Erweiterungen).

Weil das Polynom $X^n - 1$ separabel ist (und L' vollständig), gibt es nach dem Henselschen Lemma ein eindeutig bestimmtes
$$z \in \mathcal{O}_{L'} \text{ mit } z^n = 1 \text{ und } \bar{z} = \bar{x}.$$
Die natürliche Einbettung $\kappa' := \kappa(\bar{x}) \hookrightarrow \kappa_L$ kommt, weil L'/K unverzweigt ist, von einer K-Einbettung
$$\sigma: L' \longrightarrow L.$$
Wegen $\bar{z} = \bar{x}$, $x^n = 1$, $z^n = 1$ und der Eindeutigkeitsaussage des Henselschen Lemmas folgt
$$\sigma(z) = x$$
(man beachte, $z \in L'$, $x \in L$, d.h. $\sigma(z)$ und x liegen beide in L). Wegen $z \in L'$ folgt
$$\sigma(z) \in \sigma(L') \subseteq L = K(x),$$
also $\sigma(L') = L$. Die K-Einbettung σ ist somit ein K-Isomorphismus. Dann ist aber mit L' auch L unverzweigt über K.
QED.
Bemerkungen
(i) Am Endes dieses Abschnitts wollen wir das Bild der Einheiten-Gruppen bei der Norm-Abbildung bestimmen.
(ii) Wir erinnern daran, die Einheitengruppe eines Bewertungsrings R haben wir bisher mit $U := R^*$. Entsprechend schreiben wir jetzt im Fall eines vollständigen diskret bewerteten Körpers K
$$U_K := \mathcal{O}_K^* = \{\alpha \in \mathcal{O}_K \mid v_K(\alpha) \ge 0\}$$
für dessen Einheiten-Gruppe. Die Gruppe der n-Einheiten wird in derselben Weise bezeichnet, d.h.
$$U_{K,n} := \{\alpha \in \mathcal{O}_K \mid v_K(1 - \alpha) \ge n\} = 1 + \wp_K.$$

3.5.15 Das Bild der Gruppe der n-Einheiten bei der Norm-Abbildung

Seien K ein vollständiger diskret bewerteter Körper und L/K eine (endliche separable und) unverzweigte Erweiterung. Dann gilt
$$N_{L/K}(U_{L,n}) = U_{K,n}$$
für jede natürliche Zahl n.
Beweis. Sei
$$\pi \in K,\ v_K(\pi) = 1,$$
ein Parameter von K. Weil L/K unverzweigt ist, ist dann π auch ein Parameter von L,
$$v_L(\pi) = 1.$$
Bezeichne m den Grad der Erweiterung L/K,
$$m := [L:K].$$
Nach Definition haben die Elemente $u \in U_{L,n}$ die Gestalt
$$u = 1 - \pi^n \cdot x \text{ mit } x \in \mathcal{O}_L.$$

Betrachten wir das charakteristische Polynom $\chi_u(T) \in K[T]$ von $1 - u = \pi^n \cdot x$ über K,

$$\chi_{1-u}(T) \quad = T^m - Tr(1-u) \cdot T^{m-1} \pm \ldots + (-1)^m N(1-u).$$

Der Koeffizient von X^{m-i} ist gerade die elementarsymmetrische Funktion σ_i des Grades i in den Konjugierten von $\pi^n \cdot x$. Wegen $\pi \in K$ ist jedes dieser Konjugierten ein $\mathcal{O}_L$-Vielfaches von π^n, d.h. σ_i ist ein σ_i-Vielfaches von π^{ni}. Das charakteristische Polynom hat deshalb die Gestalt

$$\chi_{1-u}(T) \quad = T^m - \pi^n \cdot Tr(x) \cdot T^{m-1} + \pi^{n+1} h(T) \qquad (1)$$

mit $h(T) \in \mathcal{O}_L[T]$. Wegen

$$\begin{aligned} \chi_{1-u}(T) &=^{72} \det(T \cdot Id - (1-u)) \\ &=^{73} \det((T-1) \cdot Id + u) \\ &= \chi_{-u}(T-1) \end{aligned}$$

erhalten wir

$$\begin{aligned} N_{L/K}(u) &= (-1)^m N_{L/K}(-u) && \text{(wegen } -1 \in K) \\ &= (-1)^m (-1)^m \chi_{-u}(0) && \text{(Definition der Norm in 1.7.2)} \\ &= \chi_{1-u}(1) \\ &= 1 - \pi^n \cdot Tr(x) + \pi^{n+1} \cdot y && \text{mit } y \in \mathcal{O}_K{}^{74} \end{aligned}$$

Insbesondere ergibt sich

$$N_{L/K}(U_{L,n}) \subseteq U_{K,n}$$

Wir haben noch die umgekehrte Inklusion zu beweisen. Dazu betrachten wir die gerade bewiesene Identität und versuch dort den störenden Summanden $\pi^{n+1} \cdot y$ loszuwerden, indem wir mit $1 - \pi^{n+1} \cdot z$ multiplizieren. Dabei sei z ein noch näher zu bestimmendes Element aus $\mathcal{O}_K$. Wir erhalten

$$\begin{aligned} N_{L/K}(u) \cdot (1 - \pi^{n+1} \cdot z) &= 1 - \pi^n \cdot Tr(x) + \pi^{n+1} \cdot y \\ &\qquad - \pi^{n+1} \cdot z \cdot (1 - \pi^n \cdot Tr(x) + \pi^{n+1} \cdot y) \\ &= 1 - \pi^n \cdot Tr(x) \\ &\qquad + \pi^{n+1} \cdot (y - z \cdot v) \end{aligned}$$

mit der Einheit $v = 1 - \pi^n \cdot Tr(x) + \pi^{n+1} \cdot y$ von $\mathcal{O}_K$. Mit $z := v^{-1} y$ erhalten wir

$$N_{L/K}(u) \cdot (1 - \pi^{n+1} \cdot z) = 1 - \pi^n \cdot Tr(x).$$

Wir haben gezeigt,

$$1 - \pi^n \cdot Tr(x) \in N_{L/K}(U_{L,n}) \cdot U_{K,n+1}$$

---

[72] vgl. 1.7.2. Wir identifizieren hier das Element 1-u mit der K-linearen Abbildung, welche in der Multiplikation mit 1-u besteht.

[73] Die Matrix der Multiplikation mit 1 ist die Einheitsmatrix.

[74] wegen (1) und $h(T) \in \mathcal{O}_L[T]$.

für jedes $x \in \mathcal{O}_L$. Weil L/K unverzweigt, also auch zahm verzweigt ist, gilt $Tr(\mathcal{O}_L) = \mathcal{O}_K$ (nach 3.3.18). Wir erhalten somit

$$U_{K,n} \subseteq N_{L/K}(U_{L,n}) \cdot U_{K,n+1}$$

Mit anderen Worten,für jedes $\alpha_n \in U_{K,n}$ gibt es Elemente

$$\beta_n \in U_{L,n} \text{ und } \alpha_{n+1} \in U_{K,n+1}$$

mit

$$\alpha_n = N_{L/K}(\beta_n) \cdot \alpha_{n+1}$$

Wir setzen diese Identitäten ineinander ein und erhalten

$$\begin{aligned}\alpha_n &= N_{L/K}(\beta_n) \cdot N_{L/K}(\beta_{n+1}) \cdot \alpha_{n+2} = N_{L/K}(\beta_n \cdot \beta_{n+1}) \cdot \alpha_{n+2} \\ &= N_{L/K}(\beta_n \cdot \beta_{n+1} \cdot \beta_{n+2}) \cdot \alpha_{n+3} \\ &\dots \\ &= N_{L/K}(\beta_n \cdot \ldots \cdot \beta_{n+i}) \cdot \alpha_{n+i+1}\end{aligned}$$

für i = 1,2,3, ... Für $i \longrightarrow \infty$ gilt $\alpha_{n+i+1} \longrightarrow 1$ und[75]

$$\beta_n \cdot \ldots \cdot \beta_{n+i} \longrightarrow \beta,$$

also[76]

$$\alpha_n = N_{L/K}(\beta).$$

Es reicht zu zeigen, $\beta \in U_{L,n}$. Für jedes i = 1,2, ... gilt

$$\beta_{n+i} \in U_{L,n+1} \subseteq U_{L,n}$$

also $\beta_n \cdot \ldots \cdot \beta_{n+i} \in U_{L,n}$, also

$$v_L(\beta_n \cdot \ldots \cdot \beta_{n+i} - 1) \geq n.$$

Weil die Folge der $\beta_n \cdot \ldots \cdot \beta_{n+i}$ konvergiert, erhalten wir für $i \longrightarrow \infty$ auch

$$v_L(\beta - 1) \geq n,$$

d.h. $\beta \in U_{L,n}$.

QED.

---

[75] Mit $\gamma_i := \beta_n \cdot \ldots \cdot \beta_{n+i}$ und $i > j$ gilt $\gamma_j/\gamma_i = \beta_{n+i+1} \cdot \ldots \cdot \beta_{n+j} \in U_{n+i+1}$, d.h.

$$v_L(\gamma_j/\gamma_i - 1) \geq n+i+1.$$

Weil γ_i eine Einheit ist, gilt $v_L(\gamma_j/\gamma_i - 1) = v_L((\gamma_j - \gamma_i)/\gamma_i) = v_L(\gamma_j - \gamma_i)$, d.h. es ist

$$v_L(\gamma_j - \gamma_i) \geq n+i+1$$

für alle j > i. Die γ_i bilden somit eine Cauchy-Folge. Weil K vollständig ist, ist dies Folge konvergent.

[76] Die Konjugerten der $\beta_n \cdot \ldots \cdot \beta_{n+i}$ konvergieren gegen die Konjugierten von β, also auch deren Produkt gegen das Produkt der Konjugierten von β.

3.5.16 Das Bild der Gruppe der Einheiten bei der Norm-Abbildung
Seien K ein vollständiger diskret bewerteter Körper und L/K eine (endliche separable und) unverzweigte Erweiterung. Für ein Element $u \in U_K$ sind dann die folgenden Aussagen äquivalent.

(i) u liegt im Bild der Norm-Abbildung

$$N_{L/K}: U_L \longrightarrow U_K$$

(ii) Die Restklasse $\bar{u}$ von u in κ_K liegt im Bild der Norm-Abbildung

$$N_{\kappa_L/\kappa_L}: \kappa_L \longrightarrow \kappa_K.$$

Ist insbesondere κ_L endlich (d.h. ist K ein lokaler Körper), so ist

$$N_{L/K}(U_L) = U_K.$$

Beweis. Nach 3.3.11 gilt für jedes $\alpha \in \mathcal{O}_L$

$$\overline{N_{L/K}(\alpha)} = N_{\kappa_L/\kappa}(\bar{\alpha})^e \qquad (1)$$

für jedes $\alpha \in \mathcal{O}_L$ mit e = e(L/K) = 1 (weil L/K unverzweigt ist). Insbesondere besteht die Implikation (i) $\Rightarrow$ (ii).

Wir haben die umgekehrte Implikation (ii) $\Rightarrow$ (i) beweisen. Liege also $\bar{u}$ im Bild der Norm-Abbildung N_{κ_L/κ_L}. Wegen (1) (mit e = 1) gibt es dann ein $\alpha \in \mathcal{O}_L$ mit

$$\bar{u} = \overline{N_{L/K}(\alpha)}$$

also

$$u - N_{L/K}(\alpha) \in \wp_K.$$

Insbesondere ist $N_{L/K}(\alpha)$ eine Einheit von $\mathcal{O}_K$. Deshalb muß α eine Einheit von $\mathcal{O}_L$ sein,

$$\alpha \in U_L.$$

Es folgt

$$u \cdot N_{L/K}(\alpha)^{-1} - 1 = (u - N_{L/K}(\alpha)) \cdot N_{L/K}(\alpha)^{-1} \in \wp_K,$$

also

$$u \cdot N_{L/K}(\alpha)^{-1} \in U_{K,1}$$

Nach 3.5.15 gibt es ein

$$\beta \in U_{L,1} \subseteq U_L$$

mit

$$N_{L/K}(\beta) = u \cdot N_{L/K}(\alpha)^{-1}.$$

Es folgt

$$u = N_{L/K}(\beta) \cdot N_{L/K}(\alpha) = N_{L/K}(\beta\alpha) \in N_{L/K}(U_L).$$

Damit ist auch die Implikation (ii) $\Rightarrow$ (i) bewiesen.
Wir haben noch zu zeigen, im Fall endlicher Restekörper ist Bedingung (ii) erfüllt. Es reicht zu zeigen, die Einschränkung

$$N_{\kappa_L/\kappa_L}: \kappa_L^* \longrightarrow \kappa_K^*. \qquad (2)$$

auf die multiplikativen Gruppen ist surjektiv. Seien p die Charakteristik der Restekörper,

$$q = p^a$$

die Anzahl der Elemente von κ_K (d.h. $a = [\kappa_K: \mathbb{F}_p]$) und

$$r = q^b$$

die Anzahl der Elemente von κ_L (d.h. $b = [\kappa_L : \kappa_K]$)).

Der Körper κ_K besteht dann aus den Nullstellen des Polynoms X^q-X,

$$\kappa_K = \{\alpha\in\overline{k} \mid \alpha^q - \alpha = 0\}.$$

und analog gilt

$$\kappa_L := \{\alpha\in\overline{k} \mid \alpha^r - \alpha = 0\}$$

Die Galoisgruppe $G(\kappa_L/\kappa_K)$ wird von der a-ten Potenz der Frobeniusabbildung F erzeugt und hat die Ordnung b. Also gilt

$$N_{k_L/k}(u) = \prod_{i=0}^{b-1} F^{ia}(u) = \prod_{i=0}^{b-1} u^{p^{ia}} = \prod_{i=0}^{b-1} u^{q^i} = u^s \text{ mit } s := \sum_{i=0}^{b-1} q^i$$

Die Fasern der Abbildung (2) bestehen daher aus

$$s := \sum_{i=0}^{b-1} q^i = \frac{q^b-1}{q-1}$$

Elementen[77]. Das Bild der Normabbildung (2) besteht also aus

$$\frac{\#k_L}{s} = \frac{r-1}{s} = \frac{q^b-1}{s} = q-1$$

Elementen. Mit anderen Worten, die Normabbildung (2) ist surjektiv.
QED.

3.5.17 Beispiel

Betrachten wir die globale Situation

$$\begin{array}{ccc} K & \subseteq & L \\ \cup & & \cup \\ R & \subseteq & S \end{array}$$

mit $R = \mathbb{Z}$, $K = \mathbb{Q}$ und $L = K(i)$. Dann ist die ganze Abschließung S von R in K gerade der Ring

$$S = \mathbb{Z}[i]$$

der ganzen Gaußschen Zahlen. Die Spur- und die Norm-Abbildungen haben die Gestalt

$$Tr: L \longrightarrow K,\ a + bi \mapsto (a+bi)+(a-bi) = 2a,$$

$$N: L \longrightarrow K,\ a + bi \mapsto (a+bi)(a-bi) = a^2 + b^2$$

Da S ein freier R-Modul mit dem linear unabhängigen Erzeugendensystem {1,i} ist, können wird die Diskriminante von S/R von der Determinante

---

[77] 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.

$$\det\begin{pmatrix} Tr(1) & Tr(i) \\ Tr(i) & Tr(i^2) \end{pmatrix} = \det\begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix} = -4$$

erzeugt (vgl. 1.6.13 (ii) und 1.9.1). Die Erweiterung L/K ist also nur an der Stelle 2 verzweigt, d.h. für jede Primzahl

$$p \ne 2$$

und jedes über $p\mathbb{Z}$ liegende Primideal

$$P \subseteq \mathbb{Z}[i], P \mid p$$

ist die Erweiterung der Vervollständigungen

$$L_P/K_p , K_p = \mathbb{Q}_p ,$$

unverzweigt. Da die zugehörige Erweiterung der Reste-Körper endlich ist, nach 3.5.16 die Normabbildung

$$N: L_P \longrightarrow K_p = \mathbb{Q}_p$$

surjektiv.

<u>1. Fall</u>: $p \equiv 1 \bmod 4$

Nach 1.1.3 gibt es zwei über $p\mathbb{Z}$ liegende Primideale von $S = \mathbb{Z}[i]$, sagen wir P_1 und P_2. Dann ist

$$L \otimes_K K_p = L_{P_1} \times L_{P_2}$$

Wegen $\dim_K L = 2$ folgt

$$2 = \dim_{K_p} L \otimes_K K_p = \dim_{K_p} L_{P_1} + \dim_{K_p} L_{P_2}$$

also dim $\dim_{K_p} L_{P_j} = 1$ für $j = 1,2$. Die Erweiterung der Vervollständigungen ist vom Grad 1 und N ist die identische Abbildung,

$$N = Id: L_P \longrightarrow K_p = \mathbb{Q}_p$$

und ist damit trivialerweise surjektiv.

Im Fall $p \equiv 1 \bmod 4$ ist $i = \sqrt{-1}$ bereits in K_p, und es ist

$$L_{P_j} = K_p(\pm i) = K_p \text{ für } j = 1,2.$$

<u>2. Fall</u>: $p \equiv -1 \bmod 4$.

Nach 1.1.3 gibt es über $p\mathbb{Z}$ nur ein Primideal von $S = \mathbb{Z}[i]$, sagen wir P. Deshalb ist das Tensorprodukt

$$L \otimes_K K_p = L_P$$

selbst schon ein Körper und die Norm-Abbildung $L_P \longrightarrow K_p$ ergibt sich aus der Norm-Abbildung $L \longrightarrow K$ durch Anwenden des Funktors $\otimes_K K_p$. Sie hat also die Gestalt

$$N: L_P = \mathbb{Q}_p(i) \longrightarrow K_p = \mathbb{Q}_p, a + bi \mapsto a^2+b^2.$$

Auf Grund von 3.5.16 gibt es somit für jede Einheit u von $\mathbb{Q}_p$ zwei ganze p-adische Zahlen $a, b \in \hat{\mathbb{Z}}_p$ mit

$$a^2+b^2 = u. \tag{1}$$

Insbesondere ist das der Fall, wenn u eine zu p teilerfremde ganze rationale Zahl ist. Die diophantische Gleichung (1) ist dann zumindest in den p-adischen Zahlen $\hat{\mathbb{Z}}_p$ lösbar.

Allgemein gilt für quadratische diophantische Gleichungen das Hasse-Prinzip, d.h. die Gleichung ist über den ganzen rationalen Zahlen $\mathbb{Z}$ genau dann lösbar, wenn sie es über den reellen ist und für jedes p über den p-adischen ganzen Zahlen (siehe zum Beispiel Shafarevich, Borevich [1]).

Für die Gleichung (1) mit gegebenen ganzen u sagen unsere bisherigen Ergebnisse also, daß wir die Lösbarkeit der Gleichung in $\hat{\mathbb{Z}}_p$ für den Fall p = 2 und den Fall, daß p ein Teiler von u ist, untersuchen müssen, wenn wir wissen wollen, ob die Gleichung über $\mathbb{Z}$ lösbar ist.

Betrachtet man Körper-Erweiterungen L/K eines Grades > 2, so erhält man entsprechend (notwendige) Kriterien für die Lösbarkeit beliebiger diophantischer Gleichungen mit Koeffizienten aus $\mathbb{Z}$. Die Lösbarkeit von

$$f(x) = 0 \text{ für } f \in \mathbb{Z}[x]$$

reduziert man auf den Fall f irreduzibel und im letzteren Fall definiert f eine endliche Körpererweiterung, d.h. wir sind in der hier betrachteten (globalen) Situation.

3.6 Zahm verzweigte Erweiterungen

3.6.1 Die maximale zahm verzweigte Teilerweiterungen

(i) Sei K ein vollständiger diskret bewerteter Körper mit dem Bewertungsring $(\mathcal{O}, \wp)$ und dem Restekörper $\kappa = \mathcal{O}/\wp$. Sei weiter L/K eine endliche separable Körper-Erweiterung. Dann gibt es einen Zwischenkörper L_1

$$K \subseteq L_1 \subseteq L$$

mit der Eigenschaft, daß für jeden Zwischenkörper L',

$$K \subseteq L' \subseteq L,$$

die beiden folgenden Aussagen äquivalent sind.

1. L'/K ist zahm verzweigt.
2. $L' \subseteq L_1$.

Außerdem ist

$$[L:L_1] = p^{\ell}$$

eine Potenz der Charakteristik des Restekörpers κ, falls letztere ≠ 0 ist.[78]

Der Zwischenkörper L_1 heißt auch maximale zahm verzweigte Teilerweiterung der Erweiterung L/K.

(ii) Sei L/K außerdem eine Galois-Erweiterung. Dann gelten zusätzlich die folgenden Aussagen.

---

[78] und trivialerweise gleich 1, falls die Charakteristik von p von κ gleich Null ist.

1. L_1/K ist Galoissch und gleich

$$L_1 = L^{G_1}$$

dem Fixkörper der Gruppe

$G_1 = G_1(L/K) := \{ \sigma \in G(L/K) \mid v_L(\sigma(x) - x) \geq v_L(x) + 1$ für jedes $x \in \mathcal{O}_L \}$.

2. Ist Π ein Parameter von L,

$$v_L(\Pi) = 1,$$

so ist die Abbildung

$$\theta_0 : G_0(L/K) \longrightarrow \kappa^*_{L_0}, \sigma \mapsto \overline{\sigma(\Pi)/\Pi},$$

ein Gruppen-Homomorphismus, der nicht von der speziellen Wahl des Parameters Π abhängt und dessen Kern gleich G_1 ist,

$$G_1 = \mathrm{Ker}(\theta_0).$$

3. Die Gruppe $G_1(L/K)$ ist ein Normalteiler der Trägheitsgruppe, und die Gruppe

$$G_0(L/K)/G_1(L/K) \cong G(L_1/L_0)$$

ist zyklisch und isomorph zur Galois-Gruppe von L_1/L_0.

4. Ist $p = \mathrm{char}(\kappa) \neq 0$, so ist die Gruppe G_1 eine p-Sylow-Untergruppe der Trägheitsgruppe $G_0(L/K)$ (die als Normalteiler eindeutig bestimmt ist).

Bemerkung

Im Fall $p = 0$ ist die Erweiterung L/K stets zahm verzweigt, d.h. es ist $L = L_1$ und (im normalen Fall) $G_1 = 0$. In der obigen Aussage wird dann die Existenz des Homomorphismus θ_0 und die Zyklizität der Trägheitsgruppe G_0 behauptet.

Beweis. Zu (ii). Die Erweiterung L/K sei normal.

1. Schritt. G_1 ist ein Normalteiler der Trägheitsgruppe G_0.

Läßt man auf der rechten Seite der G_1 definierenden Bedingung

$$v_L(\sigma(x) - x) \geq v_L(x) + 1$$

den ersten Summanden $v_L(x)$ weg, so erhält man gerade die Bedingung, welche die Gruppe G_0 definiert. Also gilt

$$G_1 \subseteq G_0.$$

Wir haben noch zu zeigen, G_1 ist ein Normalteiler. Für $\sigma, \tau \in G_1$ gilt

$$\begin{aligned} v_L(\sigma\tau(x) - x) &= v_L(\sigma\tau(x) - \tau(x) + \tau(x) - x) \\ &\geq \min \{v_L(\sigma\tau(x) - \tau(x)), v_L(\tau(x) - x)\} \\ &\geq \min \{ v_L(\tau(x)) + 1, v_L(x) + 1\}. \end{aligned}$$

Nun haben $\tau(x)$ und x denselben Wert bezüglich v_L (zum Beispiel nach 3.5.5). Also gilt

$$v_L(\sigma\tau(x) - x) \geq v_L(x) + 1$$

für jedes $x \in \mathcal{O}_L$, d.h.

$$\sigma\tau \in G_1.$$

Weiter ist für $\sigma \in G_1$

$$\begin{aligned} v_L(\sigma^{-1}(x) - x) &= v_L(\sigma(\sigma^{-1}(x) - x)) && \text{(nach 3.5.5)} \\ &= v_L(x - \sigma(x)) \\ &= v_L(\sigma(x) - x) && \text{(wegen } v_L(-1) = 0) \\ &\geq v_L(x) + 1. \end{aligned}$$

für jedes $x \in \mathcal{O}_L$, d.h.

$$\sigma^{-1} \in G_1.$$

Wir haben gezeigt, G_1 genügt dem Untergruppen-Kriterium.

Seien jetzt $\sigma\in G_1$ und $\tau\in G_0$, d.h.

$$v_L(\sigma(x) - x) \geq v_L(x) +1 \text{ und } v_L(\tau(x) - x) \geq 1$$

für jedes $x \in \mathcal{O}_L$. Es folgt

$$\begin{aligned} &v_L(\tau\sigma\tau^{-1}(x) - x) \\ &= v_L(\tau(\sigma\tau^{-1}(x) - \tau^{-1}x)) \\ &= v_L(\sigma\tau^{-1}(x) - \tau^{-1}x) && \text{(nach 3.5.5)} \\ &\geq v_L(\tau^{-1}x) + 1 && \text{(wegen } \sigma\in G_1) \\ &= v_L(x) + 1 && \text{(nach 3.5.5)} \end{aligned}$$

für jedes $x \in \mathcal{O}_L$, d.h.

$$\tau\sigma\tau^{-1} \in G_1.$$

Wir haben gezeigt, G_1 ist ein Normalteiler in G_0.

<u>2. Schritt</u>. $\theta_0: G_0 \longrightarrow \kappa^*_{L_0}$ ist ein Gruppen-Homomorphismus mit dem Kern G_1

Sei neben Π auch Π' ein Parameter von L. Dann gilt

$$\Pi' = u\cdot\Pi$$

mit einer Einheit $u \in \mathcal{O}_L$. Für jedes $\sigma\in G_0$ erhalten wir

$$\sigma(\Pi')/\Pi' = \sigma(u\cdot\Pi)/(u\cdot\Pi) = \sigma(\Pi)/\Pi\cdot\sigma(u)/u.$$

Wegen $\sigma\in G_0$ ist $v_L(\sigma(u) - u) > 0$, also $\sigma(u) \equiv u \bmod \wp_L$, also $\sigma(u)/u \equiv 1 \bmod \wp_L$, also

$$\sigma(\Pi')/\Pi' \equiv \sigma(\Pi)/\Pi \bmod \wp_L$$

Mit anderen Worten, die Abbildung θ_0 hängt nicht von der speziellen Wahl des Paramters Π ab.

Für $\sigma, \tau \in G_0$ gilt

$$\theta_0(\sigma\tau) = \sigma\tau(\Pi)/\Pi \bmod \wp_L$$
$$= \sigma\tau(\Pi)/\tau(\Pi) \bullet \tau(\Pi)/\Pi \bmod \wp_L.$$

Nun ist mit Π auch $\tau(\Pi)$ ein Parameter (nach 3.5.5), d.h. es ist

$$\theta_0(\sigma\tau) = \theta_0(\sigma)\bullet \theta_0(\tau).$$

Die Abbildung

$$\theta_0 : G_0 \longrightarrow \kappa_L^*$$

ist somit ein Gruppen-Homomorphismus. Wir haben noch den Kern von θ_0 zu bestimmen. Ein Element $\sigma \in G_0$ liegt genau dann im Kern von θ_0, wenn

$$\sigma(\Pi)/\Pi \equiv 1 \bmod \wp_L$$

gilt. Wie wir oben gesehen haben, gilt

$$\sigma(u)/u \equiv 1 \bmod \wp_L$$

für jede Einheit $u \in \mathcal{O}_L$. Für $a \in \mathcal{O}_L$ können wir $a = u\bullet\Pi^{v_L(a)}$ schreiben, also

$$\sigma(a)/a = \sigma(u)/u \bullet \sigma(\Pi)^{v_L(a)}/\Pi^{v_L(a)},$$

also

$$\overline{\sigma(a)/a} = \theta_0(\sigma)^{v_L(a)} \text{ für jedes } a \in \mathcal{O}_L.$$

Es folgt

$$\sigma \in \mathrm{Ker}(\theta_0) \Leftrightarrow \overline{\sigma(a)/a} = 1 \text{ für jedes } a \in \mathcal{O}_L$$
$$\Leftrightarrow \sigma(a)/a - 1 \in \wp_L \text{ für jedes } a \in \mathcal{O}_L$$
$$\Leftrightarrow \sigma(a) - a \in \wp_L \bullet \wp_L^{v_L(a)} \text{ für jedes } a \in \mathcal{O}_L$$
$$\Leftrightarrow v_L(\sigma(a) - a) \geq v_L(a) + 1 \text{ für jedes } a \in \mathcal{O}_L$$
$$\Leftrightarrow \sigma \in G_1.$$

Es gilt also $\mathrm{Ker}(\theta_0) = G_1$.

<u>3. Schritt</u>: G_0/G_1 ist zyklisch und hat im Fall $p:=\mathrm{char}(\kappa)>0$ eine zu p teilerfremde Ordnung.

Als Kern von θ_0 (oder nach dem ersten Schritt) ist G_1 ein Normalteiler von G_0. Es reicht zu zeigen, das Bild von θ_0,

$$\mathrm{Im}/(\theta_0) \; (\cong G_0/G_1)$$

ist zyklisch.

Weil die Gruppe G_0 endlich ist, besteht $\mathrm{Im}(\theta_0)$ aus Einheitswurzeln. Faßt man diese Einheitswurzeln als primitive Einheitswurzeln auf, so sieht man, deren Ordnung ist teilerfremd zur Charakteristik p des Restekörpers (im Fall $p \neq 0$,vgl. den Beweis von 3.5.14). Insbesondere sind diese Einheitswurzeln separabel über κ, d.h.

$$\mathrm{Im}(\theta_0) \subseteq (\kappa_L^s)^* = \kappa_{L_0}^*$$

Damit ist $\mathrm{Im}(\theta_0)$ eine endliche abelsche Gruppe, deren Elemente eine zu p teilerfremde Ordnung besitzen. Nach dem Struktursatz für endliche abelsche Gruppen[79] (oder wegen der Existenz der Sylow-Untergruppen)[80] ist die Ordnung von $\mathrm{Im}(\theta_0)$ zu p teilerfremd,

$$m := \#\, \mathrm{Im}(\theta_0) \text{ ist teilerfremd zu } p := \mathrm{char}(\kappa) \text{ im Fall } p \neq 0.$$

Weil m teilerfremd ist zu p, gibt es in der algebraischen Abschließung von κ_L eine primitive m-te Einheitswurzel[81], sagen wir ζ. Die Ordnungen der Elemente von $\mathrm{Im}(\theta_0)$ teilen die Ordnung m der Gruppe $\mathrm{Im}(\theta_0)$, d.h. die Gruppe besteht aus lauter m-ten Einheitswurzeln. Letztere liegen aber sämtlich in der von $<\zeta>$ erzeugten zyklischen Gruppe,

$$\mathrm{Im}(\theta_0) \subseteq <\zeta>.$$

Als Untergruppe einer zyklischen Gruppe ist $\mathrm{Im}(\theta_0)$ zyklisch.

<u>4. Schritt</u>. $L_1 := L^{G_1}$ ist zahm verzweigt über L_0 und über K, und es gilt

$$G(L_1/L_0) = G_0/G_1.$$

Weil L_0/K unverzweigt ist (also auch zahm verzweigt) und die Zusammensetzung zahm verzweigter Erweiterungen zahm verzweigt ist (nach Definition 3.3.17), reicht es zu zeigen,

$$L_1/L_0 \text{ ist zahm verzweigt.}$$

Mit L/K ist auch L/L_0 eine Galois-Erweiterung. Ihre Galois-Gruppe ist gerade[82]

$$G_0.$$

Aus der Operation von G_0 auf L erhält man durch Einschränken auf L_1 eine Operation von G_0/G_1 auf L_1, und G_0/G_1 wird auf diese Weise zur Galois-Gruppe der Erweiterung L_1/L_0[83]. Insbesondere ist

$$\begin{aligned}
[L_1 : L_0] &= \#\, G_0/G_1 && \text{(Hauptsatz der Galois-Theorie)}\\
&= \#\, \mathrm{Im}(\theta_0)\\
&= m\\
&= \text{teilerfremd zu } p := \mathrm{char}(\kappa).
\end{aligned}$$

---

[79] Die Gruppe ist ein direktes Produkt von zyklischen Faktoren, deren Ordnung zu p teilerfremd ist.

[80] Wäre p ein Teiler der Gruppen-Ordnung, so wäre die p-Sylow-Untergruppe nicht trivial. Die Ordnung der Elemente dieser p-Sylow-Untergruppe ist aber eine Potenz von p.

[81] siehe zum Beispiel die Grundvorlesung “Algebra 1”, Kapitel 3, Abschnitt 3.6: Endliche Körper.

[82] Wegen $L_0 = L^{G_0}$.

[83] Weil der Kern der Einschränkungsabbildung $G_0 = G(L/L_0) \twoheadrightarrow G(L_1/L_0)$ gerade G_1 ist (nach dem Hauptsatz der Galois-Theorie).

Damit ist aber auch der Teiler $e(L_1: L_0)$ dieses Körpergrades teilerfremd zu p, d.h. für die Erweiterung L_1/L_0 ist Bedingung (i) der Definition zahmer Erweiterungen 3.3.17 erfüllt.

Wir haben noch zu zeigen, die Erweiterung der Reste-Körper ist separabel. Dazu reicht es zu zeigen, der Relativ-Grad $f(L_1/L_0)$ ist teilerfremd zu p. Das ist aber ebenfalls der Fall, weil $f(L_1/L_0)$ ein Teiler von $[L_1: L_0]$ ist.

<u>5. Schritt</u> Eine Teilerweiterung von L/K ist genau dann zahm verzweigt, wenn sie in L_1 liegt.

Wir verwenden die Tatsache, daß für jeden Turm

$$A \subseteq B \subseteq C$$

von endlichen Körper-Erweiterungen die beiden folgenden Aussagen äquivalent sind.[84]

a) C/A ist zahm verzweigt.

b) C/B und B/A sind zahm verzweigt.

Zusammen mit dem 4. Schritt ergibt sich daraus insbesondere, daß jede Teilerweiterung von L_1/K zahm verzweigt ist.

Sei jetzt L'/K umgekehrt eine zahm verzweigte Teilerweiterung von L/K. Wir haben zu zeigen,

$$L' \subseteq L_1.$$

Wir setzen

$$C := L'L_0 \ , B:= L'\cap L_0 \ , A := K.$$

Zum Beweis der Inklusion reicht es zu zeigen

$$C \subseteq L_1.$$

Wir werden dies zeigen, indem wir für die zugehörigen Untergruppen der Galois-Gruppe die umgekehrte Inklusion beweisen.

<u>Teilschritt A</u>. C/K ist zahm verzweigt.

Die Erweiterung L'/B ist zahm verzweigt[85]. Nach der Charakterisierung 3.3.18 zahm verzweigter Erweiterungen gibt es ein Element $a \in \mathcal{O}_{L'}$ mit $Tr_{L'/B}(a) = 1$. Zeigen wir, es gilt dann auch

$$Tr_{C/L_0}(a) = 1. \tag{1}$$

Zum Beweis betrachten wir die L_0-Einbettungen von C in eine algebraische Abschließung von C, sagen wir

$$\tau_1,...,\tau_u: C \to \overline{C}$$

Nun liegt C in L, und L ist nach Voraussetzung normal (über K also über L_0). Die Bilder dieser Einbettungen liegen also sämtlich in L, d.h. sie haben die Gestalt

---

[84] Das liegt daran, daß man äquivalente Aussagen bekommt, wenn man 'zahm verzweigt' durch 'separabel' ersetzt, und daß sich der Verzweigungsindex multiplikativ verhält.

[85] Es reicht zu zeigen, L'/L_0 und L_0/F sind zahm verzweigt. Das erste ist der Fall, weil L'/K zahm verzweigt ist. Das zweite ist der Fall, weil sogar L_0/K zahm verzweigt (sogar unverzweigt) ist.

$$\tau_1,\dots,\tau_u: C \to \bar{L}$$

Ihre Anzahl ist $u = [C:L_0]$. Die zu bestimmende Spur läßt sich schreiben als

$$\mathrm{Tr}_{C/L_0}(a) = \sum_{i=1}^{u} \tau_i(a).$$

Durch Einschränken der τ_i auf L' erhalten wir B-Einbettungen von L' in $\bar{C}$. Sind zwei der Einschränkungen $\tau_i|_{L'}$ gleich, so stimmen die zugehörigen τ_i auf L' und trivialerweise auf L_0 überein, d.h. sie sind auf $C = L'L_0$ gleich. Durch Einschränken der τ_i auf L' erhalten wir also paarweise verschiedene Abbildungen. Zum Beweis der Identität (1) reicht es zu zeigen, daß jede B-Einbettungen von L' in $\bar{C}$ von der Gestalt $\tau_i|_{L'}$ ist, denn dann berechnet sich die Spur $\mathrm{Tr}_{C/L_0}(a)$ nach derselben Formel wie die Spur $\mathrm{Tr}_{L'/B}(a)$:

$$\mathrm{Tr}_{C/L_0}(a) = \sum_{i=1}^{u} \tau_i|_{L'}(a) = \mathrm{Tr}_{L'/B}(a) = 1.$$

Die Anzahl der B-Einbettungen der Gestalt $\tau_i|_{L'}$ ist gleich $u = [C:L_0]$. Die der B-Einbettungen von L' insgesamt ist $[L':B]$. Es reicht also zu zeigen,

$$[C:L_0] = [L':B].$$

Alle hier betrachteten Körper-Erweiterungen sind separabel über K. Es gibt also ein Element $\alpha\in L$ mit

$$L' = B(\alpha) \text{ also } C = L'L_0 = L_0(\alpha)$$

Sei f das Minimalpolynom von α über B und g das von α über L_0.

$$f \in C[T],\ g \in L_0[T],\ f(\alpha) = g(\alpha) = 0,\ g \mid f.$$

Wir haben zu zeigen, f und g haben denselben Grad. Wir betrachten eine Zerlegung von f in irreduzible Faktoren über L_0,

$$f = g_1\cdot\ldots\cdot g_r .$$

Wir haben zu zeigen, $r = 1$. Dazu beachten wir, wegen $L' = B(\alpha) \subseteq L$ und L/B normal operiert die Galoisgruppe G(L/B) transitiv auf den Nullstellen des Minimalpolynoms f. Diese Operation induziert eine Operation auf der Menge der g_i,

$$G(L/B)\times\{g_1,\dots,g_r\} \to \{g_1,\dots,g_r\},\ (\sigma,g_i) \mapsto \sigma g_i. \qquad (2)$$

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

$$\sigma\gamma = \sigma\tau\beta = \sigma\tau\sigma^{-1}\sigma\beta.$$

Mit L/K ist auch die Körpererweiterung L_0/B normal[86]. Also ist $G(L/L_0)$ Normalteiler in $G(L/B)$, 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 (2) ist also korrekt definiert. O.B.d.A. sei $g_1=g$. Betrachten wir den Stabilisator $G(L/B)_g$ von g bei der Operation (2). Es gilt

$$\begin{aligned}
\sigma\in G(L/B)_g \quad & \Leftrightarrow \sigma(g) = g \\
& \Leftrightarrow \sigma(\alpha) \text{ ist Nullstelle von } g \\
& \Leftrightarrow \sigma(\alpha) \text{ ist } G(L/L_0)\text{-konjugiert zu } \alpha \\
& \Leftrightarrow \sigma(\alpha) = \tau(\alpha) \text{ für ein } \tau\in G(L/L_0) \\
& \Leftrightarrow (\tau^{-1}\sigma)(\alpha) = \alpha \text{ für ein } \tau\in G(L/L_0) \\
& \Leftrightarrow \tau^{-1}\sigma \text{ läßt } B(\alpha) = L' \text{ fest für ein } \tau\in G(L/L_0) \\
& \Leftrightarrow \tau^{-1}\sigma\in G(L/L') \text{ für ein } \tau\in G(L/L_0) \\
& \Leftrightarrow \sigma\in G(L/L_0)\bullet G(L/L') =^{87} G(L/L'\cap L_0) = G(L/B).
\end{aligned}$$

Der Stabilisator von g fällt also mit der gesamten Gruppe $G(L/B)$ 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. Damit ist (1) bewiesen. Nach der Charakterisierung 3.3.18 der zahm verzweigten Erweiterungen ist dann aber

$$C/L_0 \text{ zahm verzeigt.}$$

Weil L_0/K unverzweigt, also auch zahm verzweigt ist, ist

$$C/K \text{ zahm verzweigt.}$$

<u>Teilschritt B</u>. $(L' \subseteq)\ C \subseteq L_1$.

Wegen C/K zahm verweigt ist die zu C/K gehörige Erweiterung der Restekörper separabel,

$$k_C \subseteq k_L^s = k_{L_0}, \text{ d.h. } k_C =^{88} k_{L_0}.$$

Damit ist C/L_0 total verzweigt, d.h.

$$f(C/L_0) = 1 \text{ und } e(C/L_0) = [C:L_0]$$

Nach dem Struktursatz 3.4.3 für total verzweigte Erweiterungen gilt

$$\mathcal{O}_C = \mathcal{O}_{L_0}[c] \text{ und } C = L_0(c)$$

---

[86] L_0 ist sogar normal über K.

[87] Man beachte, $G(L/L_0)$ ist Normalteiler in $G(L/B)$, d.h. auf der linken Seite steht das Erzeugnis der Untergruppen $G(L/L_0)$ und $G(L/L')$.

[88] Nach Definition von C gilt $L_0 \subseteq C$, also $k_{L_0} \subseteq k_C$.

wenn $c \in L$ ein beliebig gewähltes Element mit $v_C(c) = 1$ ist. Auf Grund der Beschreibung der Diskriminante für einfache Ring-Erweiterungen 3.2.10 erhalten wir

$$\mathcal{D}(C/L_0) = h'(c)\mathcal{O}_C ,$$

wobei $h \in \mathcal{O}_{L_0}[x]$ das Minimalpolynom von c über L_0 bezeichne. Die Charakterisierung 3.3.18 der zahm verzweigten Erweiterungen liefert

$$e(C/L_0) - 1 = v_C(\mathcal{D}(C/L_0)) = v_C(h'(c)).$$

Wir multiplizieren diese Identität mit dem Verzweigungsindex $v_L(c)$ von L/C und erhalten

$$v_L(h'(c)) = (e(E/L_0) - 1)v_L(c). \qquad (3)$$

Zum Beweis der Behauptung $C \subseteq L_1$ dieses Teilschritts reicht es zu zeigen, daß die umgekehrte Inklusion zwischen den zugehörigen Galois-Gruppen besteht.

$$G(L/C) \supseteq G(L/L_1).$$

Wir sind jetzt soweit, daß wir die beiden Galois-Gruppen vergleichen können. Sei

$$\Delta = G(L/C).$$

Dann gilt $\Delta \subseteq G_0 = G(L/L_0)$ und

$$C = L^\Delta.$$

Durch Einschränken der Elemente von $G_0=G(L/L_0)$ auf C erhalten wir gerade die L_0-Einbettungen von C.

$$\begin{array}{ccccc} \Delta \rightarrowtail G(L/L_0) & \twoheadrightarrow & \{ C \hookrightarrow K \text{ über } L_0\} \\ \sigma & \mapsto & \sigma|_C \end{array}$$

Die Fasern dieser Einschränkungsabbildung sind gerade die Nebenklassen modulo Δ. Die Faktormenge G_0/Δ läßt sich also identifizieren mit der Menge der L_0-Einbettungen von C. 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

$$h'(c) = \prod_\gamma (c-\gamma(c)),$$

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 bezüglich v_L haben,

$$v_L(c-\gamma(c)) \geq^{89} v_L(c). \qquad (4)$$

Die Anzahl der Faktoren ist

$$\begin{aligned} \#G_0/\Delta - 1 &= [G_0:\Delta] - 1 \\ &= [L:L_0]/[L:C] - 1 \\ &= [C/L_0] - 1 \quad \text{(nach Definition von } \Delta) \end{aligned}$$

---

[89] Nach der verschärften Dreiecksungleichung.

$= e(C/L_0) - 1.$ (siehe oben)

Wegen (3) gilt also in den Ungleichungen (4) das Gleichheitszeichen,

$$v_L(c-\gamma(c)) = v_L(c),$$

d.h. es ist $\gamma \notin G_1$. Wir haben gezeigt, kein $\gamma \in G(L/L_0) - \Delta$ liegt in G_1, d.h. es gilt

$$G_1 \subseteq \Delta.$$

Wir gehen zu den Fixkörpern über und erhalten

$$L_1 \supseteq C = L'L_0,$$

also $L_1 \supseteq L'$.

<u>6. Schritt</u>. Die p-Sylow-Gruppen-Eigenschaft von G_1 , $p = \mathrm{char}(\kappa)$.

Die Aussage ist nur sinnvoll, wenn die Charakteristik $p := \mathrm{char}(\kappa) > 0$ ist (0-Sylow-Gruppen sind nicht definiert). Nach dem 3. Schritt ist die Ordnung von G_0/G_1 teilerfremd zu p, d.h. G_1 enthält eine p-Sylow-Untergruppe von G_0.[90] Es reicht deshalb zu zeigen, jede echte Untergruppe von G_1 hat einen durch p teilbaren Index[91].

Sei $G'' \subset G_1$ eine echte Untergruppe und sei

$$L'' := L^{G''} \ (\supset L_1)$$

deren Fixkörper. Es reicht zu zeigen,

$$p \mid [L'':L_1] \ (= [L:L_1]/[L:L''] = (G_1:G'')\ ).$$

Nach dem 5. 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

$$p \mid e(L''|L_1)\cdot f(L''|L_1) = [L'':L_1].$$

<u>7. Schritt</u>. Der Fall nicht-normaler Erweiterungen L/K.

Wird behandelt, indem man L/K in eine (endliche) normale Erweiterung $\tilde{L}/K$ einbettet. Seien $\tilde{L}_1/K$ die dann nach (ii) existierende maximale zahm verzweigte Teilerweiterung von $\tilde{L}/K$ und

$$L_1 := \tilde{L}_1 \cap L.$$

Für jeden Zwischenkörper L',

$$K \subseteq L' \subseteq L,$$

gilt dann:

---

[90] Jede p-Sylow-Untergruppe von G_1 ist eine solche von G_0.

[91] Das gilt dann insbesondere für die p-Sylow-Untergruppen 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.

$$L'/K \text{ ist zahm verzweigt} \Leftrightarrow L' \subseteq \tilde{L}_1$$
$$\Leftrightarrow L' \subseteq L_1 \quad (\text{wegen } L' \subseteq L)$$

d.h. L_1 ist die gesuchte maximale zahm verzweigte Erweiterung.
Wir haben noch den Körper-Grad

$$[L:L_1]$$

im Fall, daß $p := \mathrm{char}(\kappa)$ positiv ist, zu beschreiben.

Betrachten wir das kommutative Diagramm

$$\begin{array}{ccc} \tilde{L}_1 & \subseteq & \tilde{L} \\ \cup & & \cup \\ L_1 & \subseteq & L \end{array}$$

Bezeichne

$$\mathcal{E} = \{L \hookrightarrow \bar{L} \text{ über } L_1\}$$

die Menge der L_1-Einbettungen von L in eine algebraische Abschließung $\bar{L}$ von $\tilde{L}$. Die Einschränkung auf L definiert dann eine Surjektion

$$G(\tilde{L}/L_1) \twoheadrightarrow \mathcal{E}, \sigma \mapsto \sigma|_L$$

der Galois-Gruppe

$$G := G(\tilde{L}/L_1) = G(\tilde{L}/L \cap \tilde{L}_1) =^{92} G(\tilde{L}/L)\bullet G(\tilde{L}/\tilde{L}_1)$$

auf die Menge $\mathcal{E}$. Da die Elemente von $G(\tilde{L}/L)$ dabei in die identische Abbildung übergehen, ist sogar die Abbildung

$$G(\tilde{L}/\tilde{L}_1) \twoheadrightarrow \mathcal{E}, \sigma \mapsto \sigma|_L,$$

surjektiv. Zwei Elemente $\sigma, \tau \in G(\tilde{L}/\tilde{L}_1)$ werden dabei genau dann auf dieselbe Einbettung abgebildet, wenn $\tau^{-1}\sigma|_L = \mathrm{Id}$ ist, d.h. wenn σ und τ in derselben Nebenklasse modulo $G(\tilde{L}/L\tilde{L}_1)$ liegen. Die Menge $\mathcal{E}$ läßt sich so mit der Menge der Nebenklassen modulo $G(\tilde{L}/L\tilde{L}_1)$ identifizieren. Es folgt

$$\begin{aligned}[L:L_1] &= \# \mathcal{E} \quad (\text{die Erweiterung ist separabel}) \\ &= \# G(\tilde{L}/\tilde{L}_1)/G(\tilde{L}/L\tilde{L}_1) \\ &= \# G(\tilde{L}/\tilde{L}_1)/\# G(\tilde{L}/L\tilde{L}_1).\end{aligned}$$

---

92 $G(\tilde{L}/\tilde{L}_1)$ ist ein Normalteiler in $G(\tilde{L}/L_1)$, weil $\tilde{L}_1$ normal ist über L_1 (denn $\tilde{L}_1$ ist sogar normal über K).

Insbesondere ist $[L:L_1]$ ein Teiler der Ordnung von $G_1 = G(\widetilde{L}/\widetilde{L}_1)$. Es reicht also zu zeigen, letztere Ordnung ist eine Potenz der Charakteristik p von κ. Nun ist aber

$$G_1(\widetilde{L}/K)$$

nach dem 6. Schritt eine p-Sylow-Untergruppe von $G(\widetilde{L}/K)$, also von p-Potenz-Ordnung.
QED.

3.6.2 Die Auflösbarkeit der Trägheitsgruppe und der Galois-Gruppe lokaler Körper

Seien K ein vollständiger diskret bewerteter Körper mit dem Restekörper κ und L/K eine endliche Galois-Erweiterung. Dann ist die Trägheitsgruppe

$$G_0 = G_0\,(L/K)$$

auflösbar.
Genauer:

(i) Im Fall char(κ) = 0, ist G_0 zyklisch.

(ii) Im Fall p := char(κ) ≠ 0 ist G_0 die Erweiterung einer p-Gruppe mit einer zyklischen Gruppe, d.h. man hat eine exakte Sequenz von Gruppen-Homomorphismen

$$0 \longrightarrow G_1 \longrightarrow G_0 \longrightarrow G_0/G_1 \longrightarrow 0$$

mit einer p-Gruppe G_1 und einer zyklischen Gruppe G_0/G_1.

(iii) Ist K ein lokaler Körper (d.h. ist κ endlich), so ist die Galois-Gruppe jeder endlichen normalen Körpererweiterung von K auflösbar.

Beweis. Zu (i). Nach Aussage 3 von 3.6.1 (ii) ist (mit den dortigen Bezeichnungen)

$$G_0/G_1$$

zyklisch und nach der Bemerkung von 3.6.1 ist im Fall der Charakteristik 0 die Untergruppe G_1 trivial (weil jede Erweiterung $L = L_1$ zahm ist).

Zu (ii). Nach Aussage 4 von 3.6.1 (ii) ist (mit den dortigen Bezeichnungen) G_1 ein p-Sylow-Untergruppe von G_0, also von p-Potenzordnung. Nach Aussage 3 ist der Faktor G_0/G_1 zyklisch.

Zu (iii). Da jede p-Gruppe und jede zyklische Gruppe auflösbar ist, reicht es nach (ii) zu zeigen, daß

$$G(L/K)/G(L/L_0) \cong G(L_0/K)$$

auflösbar ist. Nun ist L_0/K unverzweigt. Nach dem Satz 3.5.9 von der maximalen unverzweigten Teilerweiterung gilt

$$G(L_0/K) \cong G(\kappa_{L_0}/\kappa).$$

Die Galois-Gruppe der Erweiterung κ_{L_0}/κ endlicher Körper ist aber sogar zyklisch (und wird von einer Potenz der Frobenius-Abbildung erzeugt).

QED.

3.6.3 Daa Kompositum zahm verzweigter Erweiterungen

Seien K ein vollständiger diskret bewerteter Körper und

$$L'/K \text{ und } L''/K$$

zwei (endliche) zahm verzweigte Teilerweiterungen einer separablen Abschließung $\overline{K}^s$ von K. Dann ist das Kompositum L'L" zahm verzweigt über K.

Beweis. Sei L/K eine endliche Teilerweiterung von $\overline{K}^s/K$, welche die beiden Körper L' aund L" enthält (zum Beispiel L := L'L"). Weiter sei L_1/K die maximale zahm verzweigte Teilerweiterung von L/K. Dann gilt

$$L' \subseteq L_1 \text{ und } L'' \subseteq L_1$$

also

$$L'L'' \subseteq L_1.$$

Dann ist aber L'L" zahm verzweigt über K.

QED.

3.6.4 Die maximale zahm verweigte Erweiterung

Seien K ein vollständiger diskret bewerteter Körper und $\overline{K}^s$ eine separable Abschließung von K. Die Vereinigung aller Zwischenkörper L,

$$K \subseteq L \subseteq \overline{K}^s$$

mit

L/K (endlich und) zahm verzweigt

wird mit[93]

$$K_{tr}$$

bezeichnet und heißt maximale zahm verzweigte Erweiterung von K.

Bemerkung

Die Menge K_{tr} ist auch die Vereinigung aller Zwischenkörper L,

$$K \subseteq L \subseteq \overline{K}^s$$

mit

L/K zahm verzweigt und normal,

d.h.

$$K_{tr} = \bigcup X \text{ mit } X := \{ L \mid K \subseteq L \subseteq K_{tr}, L/K \text{ zahm verzweigt und normal } \} \qquad (1)$$

Beweis. Die in der Bemerkung definierte Menge liegt als Vereinigung von weniger Mengen in K_{tr}. Wir haben die umgekehrte Inklusion zu beweisen. Dazu reicht es zu zeigen, zu jedem Zwischenkörper L,

$$K \subseteq L \subseteq \overline{K}^s$$

mit L/K zahm verzweigt gibt es einen Zwischenkörper L',

$$K \subseteq L' \subseteq \overline{K}^s$$

mit L'/K zahm verzweigt und normal, wobei gilt

$$L \subseteq L'.$$

Zur Konstruktion von L' wählen wir ein Element $\alpha \in L$, welches L über K erzeugt,

---

[93] 'tr' steht für 'tamely ramified'.

$$L = K(\alpha),$$

und betrachten den Zerfällungskörper L" des Minimalpolynoms von α über K. Es gilt[94]

$$K \subseteq L \subseteq L" \subseteq \bar{K}^S \text{ und } L"/K \text{ normal.}$$

Sei die maximale zahm verzweigte Teilerweiterung von L"/K. Weil L/K zahm verzweigt ist, gilt $L \subseteq L'$, zusammen also

$$K \subseteq L \subseteq L' \subseteq L" \subseteq \bar{K}^S.$$

Nach 3.6.1 ist mit L"/K auch L'/K eine zahm verzweigte Galois-Erweiterung,

L'/K zahm verzweigt und Galoissch.

Mit anderen Worten, L' ist ein Körper der gesuchten Art.

QED.

3.6.5 Eigenschaften von K_{tr}

Sei ein vollständiger diskret bewerteter Körper mit dem Restkörper κ und der separablen Abschließung $\bar{K}^S$. Dann gilt:

(i) K_{tr}/K ist eine <u>unendliche Galois-Erweiterung</u>, d.h.

1. K_{tr} ist ein Körper
2. Jedes Element von K_{tr} ist algebraisch separabel über K.
3. Liegt ein Element $\alpha \in \bar{K}^S$ in K_{tr}, so gilt dasselbe für alle zu α konjugierten Elemente von $\bar{K}^S$.

(ii) Jede endliche Teilerweiterung von K_{tr}/K ist zahm verzweigt über K.

(iii) Die maximale unverzweigte Erweiterung K_{nr} ist ein Teilkörper von K_{tr}.

(iv) Ist char(κ) = 0, so ist die Galois-Gruppe von K_{tr}/K_{nr} isomorph zur Vervollständigung

$$G(K_{tr}/K_{nr}) \cong \hat{\mathbb{Z}} = \prod_p \hat{\mathbb{Z}}_p$$

von $\mathbb{Z}$ wie in 3.5.13, wobei das Prokt über alle Pimzahlen p zu erstrecken ist.

(v) Ist p := char(κ) $\neq$ 0, so ist die Galois-Gruppe von K_{tr}/K_{nr} isomorph zum direkten Produkt

$$G(K_{tr}/K_{nr}) \cong \prod_{q \neq p} \hat{\mathbb{Z}}_q$$

wobei das direkte Produkt über alle von p verschiedenen Primzahlen q zu erstrecken ist.

Beweis. Der Beweis erfolgt im selben Stil wie der von 3.5.12 und 3.5.13.

Beim Beweis von (vi) verwendet man die Tatsache, daß die endlichen normalen Teilerweiterungen von K_{tr}/K_{nr} nach 3.6.2 eine zyklische Galois-Gruppe besitzen. Man

---

[94] Die Inklusion links besteht trivialerweise. Der Körper L" wird von α und den Konjugierten von α erzeugt. Also gilt

$$L \subseteq L".$$

Mit α sind auch alle Konjugierten von α separabel über K, also gilt

$$L" \subseteq \bar{K}^S.$$

muß zeigen, daß dabei jede endliche zyklische Gruppe als Galois-Gruppe vorkommt, und zwar genau einmal.

Beim Beweis von (v) verwendet man die Tatsache, daß die endlichen normalen Teilerweiterungen von K_{tr} / K_{nr} nach 3.6.2 eine zyklische Galois-Gruppe mit einer zu p teilerfremden Ordnung besitzen. Man muß zeigen, daß dabei jede endliche zyklische Gruppe dieser Art als Galois-Gruppe vorkommt, und zwar genau einmal.

Die Existenz dieser Erweiterungen ergibt sich im wesentlichen aus der Existenz total verzweigter Erweiterungen vorgegebener Ordnung (vgl. 3.4.5), die Eindeutigkeit aus der Tatsache, daß zyklische Gruppen höchstens eine Untergruppe vorgegebener Ordnung besitzen.

Man beachte, im Fall $p := \mathrm{char}(\kappa) > 0$ ist eine total verzweigte Erweiterung, deren Grad ein p-Vielfaches ist, nicht zahm.

Wir ersparen uns die Einzelheiten.
QED.

3.6.6 Bemerkungen

(i) <u>Eine Charakterisierung der Gruppe</u> G_1. Die Untergruppe $G_1 \subseteq G := G(L/K)$ im Satz 3.6.1 von der maximalen zahm verzweigten Teilerweiterung besitzt eine interessante Beschreibung in den Begriffen der Theorie der Moduln. Weil G auf dem Ring $\mathcal{O}_L$ operiert, besitzt dieser die Struktur eines Moduls über dem Gruppen-Ring

$$\mathcal{O}_K[G].$$

Man kann zeigen, für eine Untergruppe $\Delta \subseteq G$ sind die beiden folgenden Aussagen äquivalent.

1. $G_1 \subseteq \Delta$.
2. $\mathcal{O}_L$ ist <u>schwach projektiv</u>[95] über dem Gruppen-Ring $\mathcal{O}_K[\Delta]$ (genauer bezüglich der natürlichen Einbettung $\mathcal{O}_K \hookrightarrow \mathcal{O}_K[\Delta]$).

(ii) Aus der Beschreibung der maximalen zahm verzweigten Teilerweiterung in 3.6.2 ergibt sich, daß man eine zahm verzweigten Erweitung stets in zwei Schritten gewinnen kann:

1. Man konstruiere zunächst eine unverzweigte Erweiterung (wie wir sie in 3.5 behandelt haben).
2. Anschließend konstruiere man eine Erweiterung, welche gleichzeitig zahm und total verzweigt ist.

Den zweiten Schritt kann man ebenfalls in expliziter Weise beschreiben. Dazu braucht man aber eine Theorie, die sogenannte Kummer-Theorie, die wir später behandeln werden. Wir beschränken uns deshalb auf die Beschreibung der Ergebnisse und verschieben die Beweise auf später.

---

[95] Seien A ein kommutativer Ring mit 1 und B ein (nicht-notwendig kommutativer) Ring mit 1, $f: A \longrightarrow B$ ein Homomorphismus von Ringen mit 1 und M ein rechter B-Modul. Dann heißt M schwach projektiv bezüglich f, wenn der Kern der natürlichen Abbildung

$$M\otimes_A B \longrightarrow M,\ m\otimes b \mapsto mb,$$

ein direkter Summand von $M\otimes_A B$ ist (als rechter B-Modul bezüglich der B- Modulstruktur des Tensor-Produkts welches von der rechten B-Modulstruktur von B kommt (nicht von der B-Modulstruktur von M !). Siehe auch Cartan & Eilenberg [1], Kapitel X, Abschnitt 8).

3.6.7 Total und zahm verwzeigte Erweiterungen
Sei K ein vollständiger diskret bewerteter Körper. Dann gelten die folgenden beiden Aussagen.

(i) Ist L/K eine normale, totol und zahm verzweigte Erweiterung, so enthält K eine primitive Einheitswurzel der Ordnung

$$e = e(L/K) = [L:K],$$

und es gibt ein Element $c \in K^*$ mit

$$v_K(c) = 1 \text{ und } L = K(\sqrt[e]{c}).$$

Außerdem fällt der Homomorphismus $\bar\psi_e$: $G(L/K) \longrightarrow \kappa_L^*$ mit dem Homomorphismus θ_0 von 3.6.1 zusammen.

Für jedes Element $b \in K^*$ sind weiterhin die beiden folgenden Aussagen äquivalent.

1. $L = K(\sqrt[e]{b})$ und $v_K(b) = 1$.
2. $\overline{b/c} \in (\kappa_K^*)^e$.

(ii) Ist e teilerfremd zur Charakteristik $p := \mathrm{char}(\kappa)$ und enthält K eine primitive e-te Einheitswurzel, so ist für jedes Element $c \in K$ mit $v_K(c) = 1$ die Körpererweiterung

$$L := K(\sqrt[e]{c})$$

normal über K, total und zahm verzweigt über und besitzt den Grad e.

3.6.8 Die Erweiterung K_{tr}/K_{nr} für lokale Körper K
Seien K ein lokaler Körper und $c \in K$ ein Parameter. Dann ist

$$K_{tr}$$

gerade die Vereinigung der Teilerweiterungen der Gestalt

$$K_{nr}(\sqrt[e]{c})$$

wobei e die Menge aller natürlichen Zahlen durchläuft, welche zur Charakteristik des Restekörpers von K teilerfremd sind.

3.6.9 Das Bild der Norm-Abbildung auf den 1-Einheiten
Seien K ein vollständiger diskret bewerteter Körper und L/K ein zahm verzweigte Körper-Erweiterung. Dann gilt

$$N_{L,K}(U_{L,1}) = U_{K,1}.$$

3.7 Die Verzweigungsgruppen
Das Ziel dieses Abschnitts besteht darin, die Folge der Gruppen

$$G_0 , G_1$$

fortzusetzen.

Wie überall in diesem Kapitel bezeichnet K einen vollständigen diskret bewerteten Körper. Die Körper-Erweiterung

$$L/K$$

sei in diesem Abschnitt eine endliche Galois-Erweiterung. Außerdem nehmen wir hier stets an, daß die zugehörige Erweiterung

$$\kappa_L/\kappa$$

separabel ist, d.h. es gelte

$$\kappa_L = \kappa_{L_0}.$$

Den allgemeinen Fall werden wir hier nicht betrachten.

3.7.1 Die einfache Erzeugbarkeit von $\mathcal{O}_L$

Seien K ein vollständiger diskret bewerteter Körper und L/K eine endliche Galois-Erweiterung mit κ_L/κ separabel.

Dann gibt es ein Element $\alpha \in \mathcal{O}_L$ mit

$$\mathcal{O}_L = \mathcal{O}_K[\alpha].$$

Beweis. Nach dem Struktursatz für unverzweigt Erweiterungen 3.5.2 gibt es ein Element $a \in \mathcal{O}_{L_0}$, dessen Restklasse $\bar{a}$ die zu L_0/K gehörige Erweiterung der Restekörper erzeugt,

$$\kappa_L = \kappa_{L_0} = \kappa(\bar{a}).$$

Für jedes solche Element a hat das Minimalpolynom

$$g \in \mathcal{O}_K[X]$$

von a über K die Eigenschaft, daß das zugehörige Polynom

$$\bar{g} \in \kappa[X]$$

irreduzibel und separabel ist, und es gilt

$$\mathcal{O}_{L_0} = \mathcal{O}_K[a] \text{ und } L_0 = K(a).$$

Insbesondere ist $\bar{a}$ keine mehrfache Nullstelle von $\bar{g}$, d.h. es gilt

$$\bar{g}'(\bar{a}) \neq 0. \tag{1}$$

Sei jetzt Π ein Parameter von L und

$$\alpha := a + \Pi.$$

Aus der Taylor-Entwicklung des Polynoms g an der Stelle a erhalten wir

$$\begin{aligned} g(\alpha) &= g(a) + g'(a)\cdot\Pi + \tilde{g}\cdot\Pi^2 \text{ mit } \tilde{g} \in \mathcal{O}_{L_0} \\ &= g'(a)\cdot\Pi + \tilde{g}\cdot\Pi^2 \end{aligned}$$

Wegen (1) folgt

$$v_L(g(\alpha)) = 1.$$

Die Restklasse von α im Restekörper ist dieselbe wie die von a, d.h. es ist

$$\kappa_L = \kappa_{L_0} = \kappa(\bar{\alpha}).$$

Es gibt deshalb ein Repräsentantensystem von κ_L in $\mathcal{O}_L$, welches aus Polynomen in α mit Koeffizienten aus $\mathcal{O}_K$ besteht. Die Elemente von $\mathcal{O}_L$ sind dann (nach 3.4.4) Potenzreihen der Gestalt

$$\sum_{n=0}^{\infty} a_n \Pi_n \qquad (2)$$

wobei die Koeffizienten $a_n \in \mathcal{O}_K[\alpha]$ aus diesem Repräsentantensystem sind und

$$\Pi_n \in \mathcal{O}_L$$

für jedes n ein fest vorgegebenes Element mit $v_L(\Pi_n) = n$ bezeichne. Ist π ein Paramter von K und

$$n = me + r \text{ mit } e = e(L/K) \text{ und } 0 \le r < e$$

so können wir zum Beispiel

$$\Pi_n = g(\alpha)^r \cdot \pi^m$$

setzen. Durch Umordnen der Reihe (2) erhält diese die Gestalt

$$\sum_{r=0}^{e-1} \left(\sum_{m=0}^{\infty} a_{me+r}\, \pi^m \right) \cdot g(\alpha)^r$$

Da die inneren "Summen" in $\mathcal{O}_K[\alpha]$ liegen, erhalten wir $\mathcal{O}_L \subseteq \mathcal{O}_K[\alpha]$, und da die umgekehrte Inklusion trivial ist, folgt

$$\mathcal{O}_L = \mathcal{O}_K[\alpha],$$

QED.

3.7.2 Definition der Verzweigungsgruppen

Seien K ein vollständiger diskret bewerteter Körper und L/K eine endliche Galois-Erweiterung mit κ_L/κ separabel.

Weiter sei α ein Element $\alpha \in \mathcal{O}_L$ wie in 3.7.1, d.h.

$$\mathcal{O}_L = \mathcal{O}_K[\alpha].$$

Wir betrachten die Funktion

$$\iota = \iota_{L/K}: G(L/K) \longrightarrow \mathbb{Z} \cup \{\infty\},\ \sigma \mapsto v_L(\sigma\alpha - \alpha),$$

und setzen für jedes $i \ge -1$

$$\Gamma_i := \Gamma_i(L/K) := \{\sigma \in G(L/K) \mid v_L(\sigma x - x) \ge i + 1 \text{ für jedes } x \in \mathcal{O}_L\}$$

Die Γ_i heißen Verzweigungsgruppen der Erweiterung L/K.

Bemerkungen

(i) Nach Definition ist

$$\Gamma_{-1} = G(L/K)$$

gerade die Galois-Gruppe von L/K.

(ii) Ebenfalls direkt nach Definition ist

$$\Gamma_0 = G_0(L/K)$$

gerade die Trägheitsgruppe von L/K.

(iii) Wir werden gleich sehen, daß

$$\Gamma_1 = G_1(L/K)$$

die in 3.6.1 eingeführte Gruppe ist.

(iv) Die nachfolgende Aussage stellt eine Verbindung zwischen den Verzweigungsgruppen und der Funktion ι her.

3.7.3 Eigenschaften der Funktion ι

Seien K ein vollständiger diskret bewerteter Körper und L/K eine endliche Galois-Erweiterung mit κ_L/κ separabel.

Weiter sei α ein Element $\alpha\in\mathcal{O}_L$ wie in 3.7.1, d.h.

$$\mathcal{O}_L = \mathcal{O}_K[\alpha].$$

und ι die in 3.7.2 definierte zu α gehörige Funktion.

(i) Für $\sigma\in G(L/K)$ gilt $\sigma\in\Gamma_i \Leftrightarrow \iota(\sigma) \ge i + 1$.

(ii) $\iota(\sigma\tau) \ge \inf \{ \iota(\sigma), \iota(\tau) \}$ für beliebige $\sigma, \tau \in G(L/K)$.

(iii) $\iota(\tau\sigma\tau^{-1}) = \iota(\sigma)$ für beliebige $\sigma, \tau \in G(L/K)$.

(iv) $\iota(\sigma^{-1}) = \iota(\sigma)$ für beliebige $\sigma \in G(L/K)$.

Die Funktion ι hängt nicht von der speziellen Wahl von α ab.

Beweis. Zu (i). Sei

$$f(a, \sigma) := v_L(\sigma a - a) \text{ für } a \in \mathcal{O}_L \text{ und } \sigma\in G(L/K).$$

Dann gilt

$$\begin{aligned}
f(ab, \sigma) &= v_L(\sigma ab - ab)\\
&= v_L(\sigma(a)(\sigma(b) - b) + (\sigma(a) - a)b)\\
&\ge \inf \{ v_L(\sigma(a)(\sigma(b) - b) , v_L((\sigma(a) - a)b))\}\\
&\ge \inf \{ v_L(\sigma(a)) + v_L(\sigma(b) - b) , v_L(\sigma(a) - a) + v_L(b))\}\\
&\ge \inf \{ v_L(\sigma(b) - b) , v_L(\sigma(a) - a)\}
\end{aligned}$$

also

$$f(ab, \sigma) \ge \inf \{ f(a, \sigma) , f(b, \sigma)\}$$

Analog folgt

$$f(a+b, \sigma) \ge \inf \{ f(a, \sigma) , f(b, \sigma)\}$$

Durch wiederholtes Anwenden der beiden Abschätzungen zusammen mit der Tatsache, daß $f(a, \sigma) = \infty$ gilt für $a \in \mathcal{O}_K$ erhalten wir

$$f(p(a), \sigma) \ge f(a, \sigma)$$

für jedes $a \in \mathcal{O}_L$ und jedes Polynom $p \in \mathcal{O}_K[a]$. Wegen $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ ergibt sich

$$\iota(\sigma) = f(\alpha, \sigma) = \inf \{f(x, \sigma) \mid x \in \mathcal{O}_L\}$$

also ist

$$\begin{aligned}
\iota(\sigma) \ge i + 1 &\Leftrightarrow f(x, \sigma) \ge i + 1 \text{ für jedes } x \in \mathcal{O}_L\\
&\Leftrightarrow \sigma\in\Gamma_i
\end{aligned}$$

Zu (ii). Es gilt

$$\begin{aligned}\iota(\sigma\tau) &= v_L(\sigma\tau\,\alpha - \alpha)\\ &= v_L(\sigma\tau\,\alpha - \sigma\,\alpha + \sigma\alpha - \alpha)\\ &\geq \inf\{\, v_L(\sigma\tau\,\alpha - \sigma\,\alpha\,),\, v_L(\sigma\,\alpha - \alpha)\,\}\\ &= \inf\{\, v_L(\sigma(\tau\,\alpha - \alpha)),\, v_L(\sigma\,\alpha - \alpha)\,\}\end{aligned}$$

Weil v_L invariant bei der Operation der Galois-Gruppe ist, kann man σ bei der Berechnung des ersten Werts von v_L weglassen:

$$\begin{aligned}\iota(\sigma\tau) &\geq \inf\{\, v_L(\tau\,\alpha - \alpha\,),\, v_L(\sigma\,\alpha - \alpha)\,\}\\ &= \inf\{\, \iota(\sigma), \iota(\tau)\,\}\end{aligned}$$

<u>Zu (iii)</u>. Nach (i) gilt mit den dort eingeführten Bezeichnungen

$$f(\alpha, \sigma) \geq n+1 \;\Leftrightarrow\; \sigma\in\Gamma_n$$

für jede ganze Zahl $n \geq -1$. Weil die Funktion f nur Werte ≥ 0 annimmt, hängt der Wert von $f(\alpha, \sigma)$ damit nicht von der speziellen Wahl des Erzeugers α ab. Weil auch

$$\mathcal{O}_L = \mathcal{O}_K[\tau^{-1}\alpha]$$

für jedes $\tau\in G(L/K)$ gilt, folgt

$$\begin{aligned}\iota(\sigma) &= f(\alpha, \sigma)\\ &= f(\tau^{-1}\alpha, \sigma)\\ &= v_L(\sigma\tau^{-1}\alpha - \tau^{-1}\alpha).\end{aligned}$$

Nun ist v_L invariant bei den Automorphismen der Galois-Gruppen (vgl. 3.5.5), d.h.es ist

$$\begin{aligned}\iota(\sigma) &= v_L(\tau(\sigma\tau^{-1}\alpha - \tau^{-1}\alpha))\\ &= v_L(\tau\sigma\tau^{-1}\alpha - \alpha)\\ &= \iota(\tau\sigma\tau^{-1}).\end{aligned}$$

<u>Zu (iv)</u>. Es gilt

$$\begin{aligned}\iota(\sigma^{-1}) &= v_L(\sigma^{-1}\alpha - \alpha) && \text{(Definition von } \iota\text{)}\\ &= v_L(\alpha - \sigma\alpha) && \text{(Invarianz von } v_L\text{, 3.5.5)}\\ &= \iota(\sigma) && \text{(Definition von } \iota\text{)}\end{aligned}$$

QED.

3.7.4 Die Normalteiler-Eigenschaft der Gruppen Γ_i

Seien K ein vollständiger diskret bewerteter Körper und L/K eine endliche Galois-Erweiterung mit κ_L/κ separabel.

(i) Γ_i ist für jedes i ein Normalteiler der Galois-Gruppe G(L/K).

(ii) $\Gamma_{i+1} \subseteq \Gamma_i$ für jedes i.

(iii) $\Gamma_i = \{Id\}$ für hinreichend großes i.

Beweis. Die ersten beiden Aussage folgen unmittelbar aus 3.7.3. Sei

$$m := \sup \{ \iota(\sigma) \mid \sigma \in G(L/K) - \{1\}\}.$$

Dann ist m endlich, d.h. ein natürliche Zahl. Auf Grund der ersten Aussage von 3.7.3 ist dann

$$\Gamma_m = \{Id\}.$$

QED.

3.7.5 Eine weitere Eigenschaft der Funktion ι

Seien K ein vollständiger diskret bewerteter Körper und L/K eine endliche Galois-Erweiterung mit κ_L/κ separabel.

Für je zwei Automorphismen $\sigma, \tau \in G(L/K)$ mit $\iota(\sigma) \neq \iota(\tau)$ gilt dann

$$\iota(\sigma\tau) = \inf \{\iota(\sigma), \iota(\tau)\}.$$

Beweis. Es gilt $\ge$ nach Aussage (ii) von 3.7.3:

$$\iota(\sigma\tau) \ge \inf \{\iota(\sigma), \iota(\tau)\}. \qquad (1)$$

Zum Beweis der Umgekehrten Ungleichung können wir annehmen,

$$\iota(\sigma) < \iota(\tau). \qquad (2)$$

Nach 3.7.3 folgt

$$\begin{aligned}\inf \{\iota(\sigma), \iota(\tau)\} = \iota(\sigma) = \iota(\tau^{-1}\sigma\tau) &\ge \inf \{\iota(\tau^{-1}), \iota(\sigma\tau)\}\\ &= \inf \{\iota(\tau), \iota(\sigma\tau)\}\end{aligned}$$

Das Infimum auf der rechten Seite kann nicht $\iota(\tau)$ sein, denn das stünde im Widerspruch zu (2). Also steht rechts $\iota(\sigma\tau)$,

$$\inf \{\iota(\sigma), \iota(\tau)\} \ge \iota(\sigma\tau).$$

QED.

3.7.7 Verhalten bei Vergrößerung des Grundkörpers

Seien K ein vollständiger diskret bewerteter Körper und L/K eine endliche Galois-Erweiterung mit κ_L/κ separabel.

Weiter sei $\Delta \subseteq G(L/K)$ eine Untergruppe. Dann ist (offensichtlich)

$$\Delta = G(L/K'),\ K' := L^{\Delta},$$

die Galois-Gruppe von L über dem Fixkörper K' von Δ. Für die Verzweigungsgruppen gilt

$$\Gamma_i(L/K') = \Gamma_i(L/K) \cap \Delta.$$

Beweis. Sei $\alpha \in \mathcal{O}_L$ derart, daß gilt

$$\mathcal{O}_L = \mathcal{O}_K[\alpha]$$

(vgl. 3.7.1). Dann gilt auch

$$\mathcal{O}_L = \mathcal{O}_{K'}[\alpha].$$

Die zur Erweiterung L/K' gehörige Funktion ι ist also gerade die Einschränkung der Funktion ι zur Erweiterung L/K. Die Behauptung folgt jetzt aus der Beschreibung 3.7.3 (i) der Verzweigungsgruppen mit Hilfe der Funktion ι.

QED.

3.7.8 Die Homomorphismen θ_i

Seien K ein vollständiger diskret bewerteter Körper, L/K eine endliche Galois-Erweiterung mit κ_L/κ separabel und $i \ge 1$ eine natür liche Zahl. Dann gilt:

(i) $\Gamma_i(L/K) = \{\sigma\in G(L/K) \mid \sigma(x)/x \in U_{L,i}$ für jedes $x \in L^*\}$.

Dabei bezeichne $U_{L,i} := 1 + \wp_L^i$ die Gruppe der i-Einheiten von L.

(ii) Bezeichne Π einen Parameter von L, $v_L(\Pi) = 1$.Dann ist die Abbildung

$$\theta_i: \Gamma_i \longrightarrow U_{L,i}/U_{L,i+1},\ \sigma \mapsto \sigma(\Pi)/\Pi \bmod U_{L,i+1},$$

ein Homomorphismus, der nicht von der speziellen Wahl des Parameters Π abhängt und den Kern

$$\mathrm{Ker}(\theta_i) = \Gamma_{i+1}$$

besitzt.

Bemerkung

Nach dem Satz von der maximalen zahm verzweigten Erweiterung (3.6.1) ist damit die Verzweigungsgruppe

$$\Gamma_1 = G_1$$

gerade die dort eingeführten Gruppe G_1.

Beweis. 1. Schritt. Es gilt "$\supseteq$" in Aussage (i).

Sei σ aus der Menge auf der rechten Seite der behaupteten Identität von (i), d.h. sei

$$\sigma(x)/x \in U_i := U_{L,i} \text{ für jedes } x \in \mathcal{O}_L. \qquad (1)$$

Dann operiert σ trivial[96] auf den Restklassen modulo $\wp_L$, d.h. σ liegt in der Tragheitsgruppe,

$$\sigma \in G_0 = G_0(L/K).$$

Wegen $\kappa_L = \kappa_{L_0}$ besitzt die Restklasse von $x \in \mathcal{O}_L$ einen Repräsentanten in $\mathcal{O}_{L_0}$, d.h.

$$x = y + z \text{ mit } y \in \wp_L \text{ und } z \in \mathcal{O}_{L_0}.$$

Damit gilt für $\sigma\in G(L/K)$

$$\begin{aligned} v_L(\sigma x - x) &= v_L(\sigma y + \sigma z - y - z) \\ &= v_L(\sigma y - y) \quad (\sigma z = z \text{ wegen } \sigma\in G_0 \text{ und } z \in \mathcal{O}_{L_0} \subseteq L_0) \\ &= v_L(\sigma y/y - 1) + v_L(y) \end{aligned}$$

---

[96] σx und x unterscheiden sich um einen Faktor, dessen Restklasse gleich 1 ist.

$\geq i + 1$ (wegen (1) und $y \in \wp_L$)

Da $x \in \mathcal{O}_L$ beliebig gewählt war, folgt $\sigma \in \Gamma_i$.

<u>2. Schritt</u>. Ist $\sigma \in \Gamma_i$, so gilt $\sigma x/x \in U_{i+1}$ für jedes $x \in U := U_L := \mathcal{O}_L^*$

Mit anderen Worten, die Bedingung für die Elemente der rechten Seite von (i) ist sogar mit i+1 anstelle von i erfüllt für die Einheiten x von L.

Seien $\sigma \in \Gamma_i$ und $x \in U$. Dann gilt

$$v_L(\sigma x/x - 1) = v(\sigma x - x) - v_L(x)$$
$$\geq i + 1 + v_L(x) \quad \text{(wegen } \sigma \in \Gamma_i\text{)}$$
$$= i + 1 \quad \text{(wegen } x \in U\text{)}.$$

Also ist $\sigma x/x - 1 \in \wp_L^{i+1}$, also $\sigma x/x \in U_{i+1}$.

<u>3. Schritt</u>. Die Abbildung θ_i von (ii) ist korrekt definiert und unabhängig von der speziellen Wahl des Parameters Π von L.

Für $\sigma \in \Gamma_i$ gilt

$$v_L(\sigma\Pi/\Pi - 1) = v_L(\sigma\Pi - \Pi) - v_L(\Pi)$$
$$\geq i + 1 - v_L(\Pi) \quad \text{(wegen } \sigma \in \Gamma_i\text{)}$$
$$= i \quad \text{(weil } \Pi \text{ ein Parameter ist)}$$

Es folgt $\sigma\Pi/\Pi - 1 \in \wp_L^i$, also $\sigma\Pi/\Pi \in U_i$. Wir haben gezeigt, das Bild von θ_i liegt tatsächlich in U_i/U_{i+1}, d.h. θ_i ist korrekt definiert.

Sei Π' ein zweiter Parameter von L. Dann gilt $\Pi' = u \bullet \Pi$ mit einer Einheit u von L. Es folgt

$$\sigma\Pi'/\Pi' = \sigma\Pi/\Pi \bullet \sigma u/u$$

Nach dem zweiten Schritt liegt der zweite Faktor rechts in U_{i+1}. Das Bild von σ bei θ_i hängt also nicht von der speziellen Wahl von Π ab.

<u>4. Schritt</u>. $\sigma x/x \in U_i$ und $\theta_i(\sigma)^{v_L(x)} = \sigma x/x \bmod U_{i+1}$ für $\sigma \in \Gamma_i$ und $x \in L^*$.

Wir schreiben x in der Gestalt

$$x = u \bullet \Pi^n \text{ mit einer Einheit u von L und } n \in \mathbb{N}.$$

Dann ist

$$\sigma x/x = \sigma u/u \bullet (\sigma\Pi/\Pi)^n,\ n = v_L(x)$$

Der erste Faktor rechts liegt nach dem zweiten Schritt in U_{i+1}. Da θ_i nach dem dritten Schritt wohldefiniert ist, liegt der zweite Faktor rechts in U_i. Also liegt auch das Element auf der linken Seite in U_i. Durch Übergang zu den Restklassen modulo U_{i+1} ergibt sich die behauptete Identiät.

<u>5. Schritt</u>. Beweis von (ii).

Wir haben noch zu zeigen:

1. θ_i ist ein Homomorphismus.

2. Der Kern von θ_i ist gleich Γ_{i+1}.

<u>Zu 1</u>. Es gilt für $\sigma, \tau \in \Gamma_i$:

$$\sigma\tau(\Pi)/\Pi = \sigma\tau(\Pi)/\tau(\Pi) \bullet \tau(\Pi)/\Pi.$$

Nun ist mit Π auch $\tau(\Pi)$ ein Parameter von L. Durch Übergang zu den Restklassen erhalten wir die Homomorphismus-Eigenschaft von θ_i (nach dem dritten Schritt).

<u>Zu 2</u>. Für $\sigma\in\Gamma_i$ gilt

$\sigma\in\mathrm{Ker}(\theta_i) \Leftrightarrow \theta_i(\sigma) = 1$

$\Leftrightarrow \sigma\Pi'/\Pi' \in U_{i+1}$ für jeden Paramter Π' von L (nach dem 3.Schritt)

$\Leftrightarrow \sigma u/u \bullet \sigma\Pi/\Pi \in U_{i+1}$ und $\sigma\Pi/\Pi \in U_{i+1}$ für jede Einheit u von L

$\Leftrightarrow$[97] $\sigma u/u \bullet (\sigma\Pi/\Pi)^n \in U_{i+1}$ für $u \in U$ und $n\in\mathbb{N}$

$\Leftrightarrow$[98] $\sigma x/x \in U_{i+1}$ für jedes $x \in L^*$

$\Leftrightarrow \sigma\in\Gamma_{i+1}$ ($\Rightarrow$ nach dem 1. Schritt, $\Leftarrow$ nach dem 4. Schritt)

<u>6. Schritt</u>. Beweis von (i).

Die Inklusion “$\supseteq$” besteht nach dem ersten Schritt. Die umgekehrte Inklusion “$\subseteq$” besteht nach dem 4. Schritt.

QED.

Bemerkungen

(i) Wir wissen bereits, haben die Restekörper die Charakteristik Null,

$$\mathrm{char}(\kappa) = 0,$$

so gilt bereits

$$G_1 = \{1\}.$$

(ii) Ist dagegen die Charakteristik der Restekörpers positiv,

$$\mathrm{char}(\kappa) =: p > 0,$$

so gilt nach 1.4.17

$$U_{L,i}^p \subseteq U_{L,i}.$$

3.7.9 Die Faktorgruppen Γ_i/Γ_{i+1}

Seien K ein vollständiger diskret bewerteter Körper, L/K eine endliche Galois-Erweiterung mit κ_L/κ separabel und $i \geq 1$ eine natür liche Zahl. Dann gilt:

(i) $\Gamma_i(K/L) = \{1\}$ im Fall $\mathrm{char}(\kappa) = 0$.

(ii) $\Gamma_i(K/L)/\Gamma_{i+1}(L/L)$ ist eine elementare abelsche p-Gruppe[99] im Fall $\mathrm{char}(\kappa) > 0$.

---

[97] weil U_{i+1} eine Gruppe ist.

[98] Jedes $x \in L$ hat die Gestalt $x = u\bullet\Pi^n$ mit $u \in U$.

Beweis. Zu (i). Im Fall der Charakteristik 0 ist jede Erweiterung zahm verzweigt. Deshalb gilt

$$G_0 = G(L/L_0) = G(L/L) = \{1\}.$$

Die Verzweigungsgruppen Γ_i sind als Untergruppen von G_0 damit ebenfalls trivial.

Zu (ii).

Nach 3.7.8 gibt es einen injektiven Homomorphismus

$$\Gamma_i/\Gamma_{i+1} \longrightarrow U_{L,i}/U_{L,i+1}$$

Insbesondere ist Γ_i/Γ_{i+1} eine endliche abelsche Gruppe. Nach 1.4.17 hat jedes Element von Γ_i/Γ_{i+1} - $\{1\}$ die Ordnung p. Nach dem Struktursatz für endliche abelsche Gruppen ist Γ_i/Γ_{i+1} eine direkte Summe zyklischer Gruppen. Jeder der zyklischen direkten Summanden hat die Ordnung p.

QED.

3.7.10 Bemerkungen zum inseparablen Fall

Wenn die Erweiterung κ_L/κ nicht separabel ist, muß man zwei Arten von Verzweigungsgruppen definieren. Bezeichnen wir die durch die Bedingung

$$v_L(\sigma x - x) \ge i + 1$$

definierten Verzweigungsgruppen (vgl. 3.7.2) vorübergehend mit

$$\Gamma_{i*}\ .$$

Daneben hat die durch die Bedinung

$$\sigma(x)/x \in U_i$$

definierten Gruppen zu betrachten (vgl. 3.7.8(i)), die wir mit

$$\Gamma_i^*$$

bezeichnen wollen.

Wir erhalten so zwei absteigende Folgen von ineinander liegenden Gruppen. Das in 3.7.7 beschriebene Verhalten dieser Gruppen bei einer Vergrößerung des Grundkörpers,

$$\Gamma_i(L/K') = \Gamma_i(L/K) \cap \Delta,\ K' := L^{\Delta},$$

besteht auch in der allgemeinen Situation. Dasselbe gilt auch für die gerade bewiesene Aussage, d.h. die Faktoren

$$\Gamma_{i*}/\Gamma_{i+1*} \text{ und } \Gamma_i^*/\Gamma_{i+1}^*$$

sind elementare abelsche p-Gruppen.

Zwischen beiden Arten von Gruppen besteht ein enger Zusammenhang. Es gilt

$$\Gamma_{i*} \supseteq \Gamma_{i+1}^* \supseteq \Gamma_{i+1*}\ .$$

Wie wir wissen, steht rechts das Gleichheitszeichen im Fall κ_L/κ separabel. Das Gleichheitszeichen links hat man im Fall $e(L/L_1) = 1$.

---

[99] d.h.direkte Summe von zyklischen Gruppen der Ordnung p.

Wenden wir uns jetzt wieder dem Fall κ_L/κ separabel zu. Die Verzweigungsgruppen gestatten eine explizite Beschreibung der Differente, welche die im zahm verzweigten Fall bekannte Formel $v(\mathcal{D}) = e - 1$ verallgemeinert (3.3.18).

3.7.10 Bezeichnung: die Ordnung der Verzweigungsgruppen

Seien K ein vollständiger diskret bewerteter Körper, L/K eine endliche Galois-Erweiterung mit κ_L/κ separabel und $i \geq -1$ eine ganze Zahl. Dann bezeiche

$$g_i = g_i(L/K) = \Gamma_i(L/K)$$

die Ordnung der i-ten Verzweigungsgruppe.

Beispiel

$$\begin{aligned} g_0 &= \# G_0 && \text{(nach Definition von } g_0\text{)} \\ &= \# G(L/L_0) && \text{(nach Definition von } L_0\text{)} \\ &= [L:L_0] && \text{(Hauptsatz der Galois-Theorie)} \\ &= e(L|L_0) && \text{(}L/L_0 \text{ ist total verzweigt, d.h. } f = 1\text{)} \\ &= e(L/K) && \text{(}L_0/K \text{ ist unverzweigt)} \end{aligned}$$

3.7.11 Eine Formel für die Differente

Seien K ein vollständiger diskret bewerteter Körper und L/K eine endliche Galois-Erweiterung mit κ_L/κ separabel und der Differente

$$\mathcal{D} = \mathcal{D}(L/K).$$

Dann gilt

$$v_L(\mathcal{D}) = \sum_{\sigma \in G(L/K) - \{1\}} \iota(\sigma) = \sum_{i=0}^{\infty} (g_i(L/K) - 1)$$

Beweis. Wir schreiben den Ring der ganzen Zahlen von L wie in 3.7.1 in der Gestalt

$$\mathcal{O}_L = \mathcal{O}_K[\alpha].$$

Bezeichne $g \in \mathcal{O}_K[X]$ das Minimalpolynom von α über $\mathcal{O}_K$.

Nach 3.2.10 gilt dann

$$\mathcal{D} = g'(\alpha)\ \mathcal{O}_L,$$

also

$$\begin{aligned} v_L(\mathcal{D}) &= v_L(g'(\alpha)) \\ &= v_L\Big(\prod_{\sigma \in G(L/K) - \{1\}} (\alpha - \sigma(\alpha))\Big) \\ &= \sum_{\sigma \in G(L/K) - \{1\}} \iota(\sigma) \end{aligned}$$

$$=^{100} \sum_{i=0}^{\infty} i\cdot(g_{i-1} - g_i)$$

$$= \sum_{i=0}^{\infty} i\cdot(g_{i-1} - 1) - i\cdot(g_i - 1)$$

$$=^{101} \sum_{i=0}^{\infty} (g_i - 1)$$

QED.

3.7.12 Der Wert der Differente eines Zwischenkörpers

Seien K ein vollständiger diskret bewerteter Körper und L/K eine endliche Galois-Erweiterung mit κ_L/κ separabel. Weiter sei

$$\Delta \subseteq G(L/K)$$

eine Untergruppe der Galois-Gruppe mit dem Fixkörper

$$F = L^{\Delta}.$$

Dann gilt

$$e(L/F)\cdot v_F(\mathcal{D}(F/K)) = \sum_{\sigma\in G(L/K)-\Delta} \iota_{L/K}(\sigma).$$

Beweis. Weil sich die Differente bei iterierten Körper-Erweiterungen multiplikativ verhält (3.2.11), gilt

$$v_L(\mathcal{D}(L/K)) = v_L(\mathcal{D}(L/F)) + v_L(F/K).$$

Die linke Seite der zu beweisenden Identät hat also den Wert

$$v_L(F/K) \quad = v_L(\mathcal{D}(L/K)) - v_L(\mathcal{D}(L/F))$$

Wir wenden die Formel von 3.7.11 für die beiden Werte auf der rechten Seite an und erhalten

$$v_L(F/K) \quad = \sum_{\sigma\in G(L/K) - \{1\}} \iota_{L/K}(\sigma) - \sum_{\sigma\in G(L/F) - \{1\}} \iota_{L/F}(\sigma)$$

Nach Definition der Funktion ι gilt aber $\iota_{L/F}(\sigma) = \iota_{L/K}(\sigma)$ für alle σ, in denen beide Seiten definiert sind, d.h. die Summanden der zweiten Summe heben sich gegen solche der ersten weg. Als Ergebnis erhalten wir die Behauptung.
QED.

3.7.13 Vergleich der verschiedenen Funktionen ι

Seien K ein vollständiger diskret bewerteter Körper und L/K eine endliche Galois-Erweiterung mit κ_L/κ separabel. Weiter sei

$$\Delta \subseteq G := G(L/K)$$

ein Normalteiler mit dem Fixkörper

$$F := L^{\Delta}.$$

---

[100] Auf jedem Element von $\Gamma_{i-1} - \Gamma_i$ hat die Funktion ι den Wert i.

[101] im (i+1)-ten Summanden steht das (i+1)-fache von g_i - 1 und im i-ten das (-i)-fache.

(d.h. F/K ist normal mit der Galois-Gruppe G/Δ). Dann besteht für jedes

$$\omega \in G/\Delta \cong G(F/K)$$

die Identität

$$e(L/F)\cdot\iota_{F/K}(\omega) = \sum_{\sigma\mapsto\omega} \iota_{L/K}(\sigma).$$

Die Summe auf der rechten Seite wird dabei übe alle $\sigma\in G$ mit der Restklasse ω erstreckt.

Beweis. Im Fall $\omega = 1$ steht auf beiden Seiten der zu beweisenden Identität ∞.[102] Sei also im folgenden

$$\omega \neq 1.$$

Wie in 3.7.1 schreiben wir

$$\mathcal{O}_L = \mathcal{O}_K[\alpha].$$

Bezeichne

$$g \in \mathcal{O}_F[X]$$

das Minimalpolynom von α über F. Wir lassen die Elemente σ der Galois-Gruppe G koeffizientenweise auf g operieren und bezeichnen das Ergebnis mit σg. Für $x \in \mathcal{O}_F$ und $\sigma \in G(F/K)$ liegt $\sigma x - x$ in $(\wp_F)^{\iota_{F/K}(\sigma)}$ (nach Definition von ι), also liegen die Koeffizienten des Polynoms

$$\omega g - g$$

in $(\wp_F)^{\iota_{F/K}(\omega)}\mathcal{O}_L = (\wp_L)^{e(L/F)\cdot\iota_{F/K}(\omega)}$. Wir setzen $\alpha\in \mathcal{O}_L$ für die Unbestimmte ein ein und erhalten

$$(\omega g)(\alpha) = (\omega g)(\alpha) - g(\alpha) \in (\wp_L)^{e(L/F)\cdot\iota_{F/K}(\omega)} \tag{1}$$

Das Polynom links können wir wie folgt in Linearfaktoren zerlegen.

$$\begin{aligned}(\omega g)(\alpha) = (\omega g)(X)|_{X=\alpha} &= (\omega\cdot \prod_{\sigma\in G(L/F)} (X-\sigma(\alpha))|_{X=\alpha}\\ &= (\prod_{\sigma\in\Delta} (X-\omega\sigma(\alpha))|_{X=\alpha}\\ &= (\prod_{\sigma\mapsto\omega} (X-\sigma(\alpha))|_{X=\alpha}\\ &= (\prod_{\sigma\mapsto\omega} (\alpha-\sigma(\alpha))\end{aligned}$$

Wir wenden v_L auf diesen Ausdruck an und erhalten wegen (1)

---

[102] Eines der σ über welche die Summe rechts erstreckt wird, ist 1.

$$\sum_{\sigma\mapsto\omega} \iota_{L/K}(\sigma) \geq e(L/F)\cdot\iota_{F/K}(\omega). \qquad (2)$$

Zum Beweis der Gleichheit bilden wir auf beiden Seiten die Summe über alle $\omega \neq 1$ und zeigen, daß die beiden entstehenden Summen gleich sind.

Dazu berechnen wir den Ausdruck $e(L/F)\cdot\iota_{F/K}(\mathcal{D}(F/K))$ zunächst mit Hilfe von 3.7.11 (mit F anstelle von L),

$$e(L/F)\cdot v_{F/K}(\mathcal{D}(F/K)) = \sum_{\omega\in G(F/K) - \{1\}} e(L/F)\cdot \iota_{F/K}(\omega)$$

und dann mit Hilfe der Folgerung 3.7.12:

$$e(L/F)\cdot v_F(\mathcal{D}(F/K)) = \sum_{\sigma\in G(L/K)-\Delta} \iota_{L/K}(\sigma)$$

$$= \sum_{\omega\in G/\Delta - \{1\}} \sum_{\sigma\mapsto\omega} \iota_{L/K}(\sigma)$$

Vergleich liefert

$$\sum_{\omega\in G/\Delta - \{1\}} e(L/F)\cdot \iota_{F/K}(\omega) = \sum_{\omega\in G/\Delta - \{1\}} \sum_{\sigma\mapsto\omega} \iota_{L/K}(\sigma),$$

d.h. durch Summieren der Abschätzungen (2) über alle $\omega\in G/\Delta - \{1\}$ erhalten wir zwei Summen, die gleich sind. Deshalb muß in (2) das Gleichheitszeichen gelten, d.h. es gilt die Behauptung.

QED.

Bemerkungen

(i) Wenden wir uns jetzt den in $G/\Delta = G(F/K)$ liegenden Verzweigungsgruppen zu.

Für i = 0 oder 1 ergibt sich aus den Abschnitten 3.5 und 3.6 über unverzweigte bzw. zahm verzweigte Erweiterungen

$$(G/\Delta)_i \cong \Gamma_i\Delta/\Delta$$

Für i = 0 ist nämlich:

$(G/\Delta)_0 = G(F/K)_0 = G(F/F\cap L_0)$ (Definition der Trägheitsgruppe)

$= G(L/F\cap L_0)/G(L/F)$

$= G(L/L_0)\cdot G(L/F)/G(L/F)$

$= G_0\cdot\Delta/\Delta.$

Für i = 1 ist die Rechnung analog.

(ii) Für beliebiges i ist diese Aussage nicht richtig. Sie wird jedoch richtig, wenn man die Idizierung dieser Gruppen ändert. Unser nächstes Ziel besteht deshalb darin, die Indizierung so zu ä daß die obigen Isomorphien für alle Indizes bestehen. Dazu führen für zunächst die Gruppen

$$\Gamma_x$$

für reelle x ≥ -1 ein. Danach führen wir die Funktion ein, welche die alte in die neue Indizierung übersetzt.

3.7.14 Die Gruppen Γ_x für reelle x

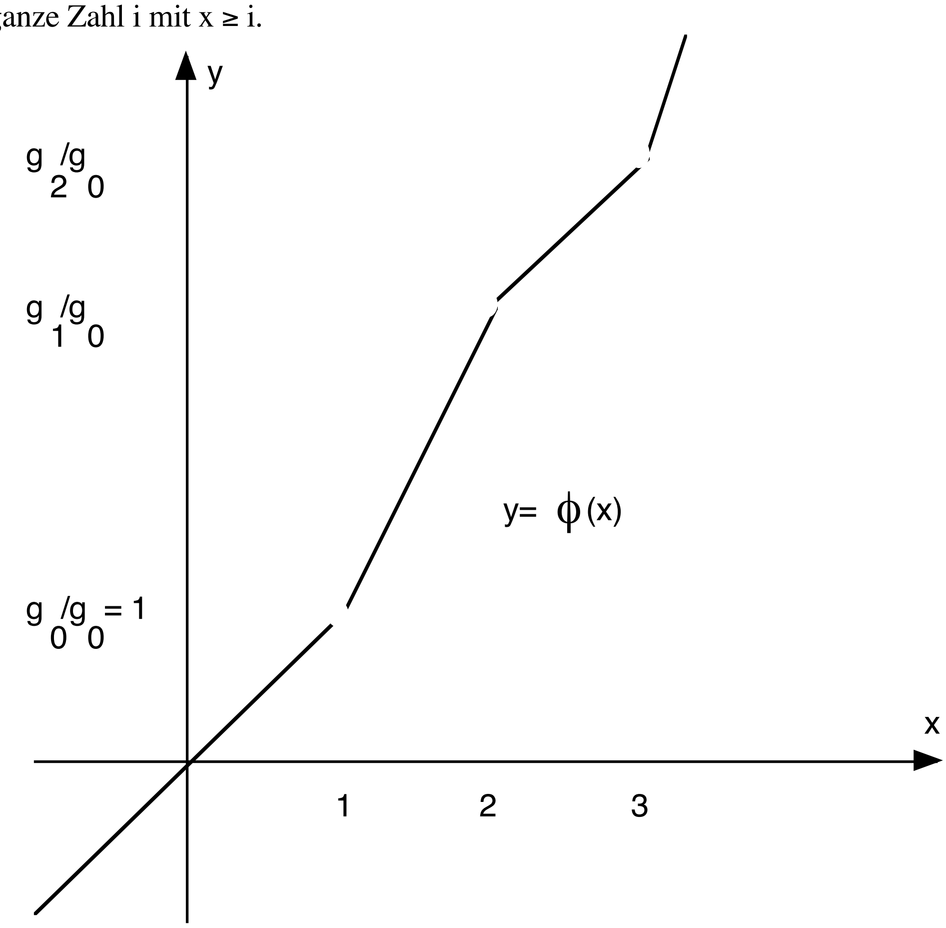
Für jede reelle Zahl x ≥ -1 sei

$$\Gamma_x := \Gamma_{-[-x]}$$

d.h. es sei $\Gamma_x := \Gamma_i$, wobei i die kleinste ganze Zahl ≥ x bezeichne. Wie üblich bezeichne hier

$$[x]$$

die größte ganze Zahl i mit x ≥ i.



3.7.15 Die Herbrand-Funktion und die Gruppen Γ^y

Seien K ein vollständiger diskret bewerteter Körper und L/K eine endliche Galois-Erweiterung mit κ_L/κ separabel. Für jede reelle Zahl x ≥ -1 setzen wir

$$\phi(x) := \phi_{L/K}(x) := \left\{ \begin{array}{ll} x & \text{falls } -1 \le x < 0 \\ \frac{1}{g_0}(g_1 + ... + g_m + (x-m)g_{m+1}) & \text{falls } x \ge 0 \text{ und } m=[x] \end{array} \right\}$$

Dabei bezeichne $g_i := \# \Gamma_i$ wie bisher die Ordnung von Γ_i.

Bemerkungen

(i) Nach Konstruktion ist ϕ stückweise linear, stetig und streng monoton steigend. Insbesondere gibt es eine (stückweise lineare, stetige und streng monoton steigende) Umkehrfunktion

$$\psi := \phi^{-1},$$

welche auf demselben halboffenen Intervall definiert ist wie ϕ.

(ii) Für jede rationale Zahl $y \ge -1$ setzen wir

$$\Gamma^y := \Gamma_x \text{ mit } x := \psi(y), \text{ d.h. } y = \phi(x).$$

(iii) Bevor wir uns der Untersuchung der Gruppen Γ^y zuwenden können, benötigen wir einige formale Eigenschaften der Funktion ϕ.

3.7.16 Eine Charakterisierung der Herbrand-Funktion

Die im vorangehenden Abschnitt definierte Funktion ϕ genügt den folgenden Bedingungen und ist durch diese eindeutig bestimmt.

(i) $\phi(0) = 0$.

(ii) $\phi : [-1, \infty) \longrightarrow [-1, \infty)$ ist stetig.

(iii) Ist m eine ganze Zahl ≥ -1, so ist die Funktion ϕ linear auf dem Intervall

$$[m, m+1\ ]$$

und besitzt im offenen Intervall $(m, m+1\ )$ die Ableitung

$$\phi'(x) = (\#\,\Gamma_x)/e(L/K).$$

Beweis. einfach.
QED.

3.7.17 Die ganzzahligen Werte der Herbrand-Funktion

Seien K ein vollständiger diskret bewerteter Körper, L/K eine endliche Galois-Erweiterung mit κ_L/κ separabel und

$$\phi = \phi_{L/K}.$$

Ist $\phi(x)$ eine ganze Zahl, so auch x.

Beweis. Für $x \in [-1, 0]$ ist die Aussage trivial. Sei also

$$x \in [m, m+1] \text{ mit } m \ge 0$$

(und m ganzzahlig) und

$$y = \phi(x).$$

Dann gilt

$$y = \frac{1}{g_0}(g_1+...+g_m + (x - m)g_{m+1})$$

also

$$g_0 y - g_1 -...-g_m = (x - m)g_{m+1}$$

$$x = m + \frac{1}{g_{m+1}}(g_0 y - g_1 -...-g_m)$$

Wegen $\Gamma_{m+1} \subseteq \Gamma_m \subseteq ... \subseteq \Gamma_0$ ist die Ordnung g_{m+1} von Γ_{m+1} ein Teiler von g_0, ..., g_m. Mit y ist deshalb auch x ganzzahlig.
QED.

3.7.18 Berechnung der Herbrand-Funktion mit Hilfe der Funktion ι
Seien K ein vollständiger diskret bewerteter Körper, L/K eine endliche Galois-Erweiterung mit κ_L/κ separabel und der Galois-Gruppe G := G(L/K). Wir schreiben

$$\phi := \phi_{L/K}, \iota := \iota_{L/K}.$$

Dann gilt

$$\phi(x) + 1 = \frac{1}{g_0} \sum_{\sigma\in G} \inf \{\iota(\sigma), x + 1\}, \tag{1}$$

Beweis. 1. Fall: $-1 \le x \le 0$.
Es gilt dann

$$\phi(x)+1 = x+1 \tag{2}$$

und

$$0 \le x + 1 < 1.$$

Für $\sigma\in\Gamma_i - \Gamma_{i+1}$ ist $\iota(\sigma) = i+1$, also

$$\inf \{\iota(\sigma), x + 1\} = \inf \{i+1, x + 1\} = \begin{cases} 0 & \text{für } i =-1 \\ x+1 & \text{für } i\ge 0\end{cases}$$

Für $\sigma\in G - G_0$ ist der Beitrag des zu σ gehörigen Summanden auf der rechten Seite von (1) gleich Null und für $\sigma\in G_0$ ist er gleich $\frac{1}{g_0}(x + 1)$. Die Anzahl der Summanden ist gleich $g_0 = \# G_0$. Die rechte Seite von (1) ist damit gleich x + 1. Zusammen mit (2) ergibt sich die Behauptung.
2. Fall: $0 < x$.
Sei m die ganze Zahl mit

$$m< x \le m+1.$$

Dann ist

$$\begin{aligned} x + 1 = \inf \{\iota(\sigma), x + 1\} &\Leftrightarrow x + 1 \le \iota(\sigma) \\ &\Leftrightarrow m+2 \le \iota(\sigma) \qquad \text{(m+2 ist die kleinste ganze Zahl} \ge \text{x+1)} \\ &\Leftrightarrow \sigma\in\Gamma_{m+1}. \end{aligned}$$

Es folgt

$$\begin{aligned} \frac{1}{g_0} \sum_{\sigma\in G} \inf \{\iota(\sigma), x + 1\} &= \frac{1}{g_0}\Big(\sum_{\sigma\notin\Gamma_{m+1}} \iota(\sigma) + (x+1)\cdot g_{m+1}\Big) \\ &=^{103} \frac{1}{g_0}\Big(\sum_{i=0}^{m+1} (g_{i-1}-g_i)\cdot i + (x+1)\cdot g_{m+1}\Big) \\ &=^{104} \frac{1}{g_0}\Big(\sum_{i=0}^{m} g_i - (m+1)\cdot g_{m+1} + (x+1)\cdot g_{m+1}\Big) \end{aligned}$$

---

[103] Auf $\Gamma_{i-1} - \Gamma_i$ hat die Funktion ι konstant den Wert i.

[104] Im i-ten Summanden kommt g_i mit dem Faktor -i vor, in (i+1)-ten Summanden mit dem Faktor (i+1). In allen anderen Summanden kommt g_i überhautpt nicht vor.

$$= \frac{1}{g_0}(g_0 + \sum_{i=1}^{m} g_i + (x - m)\cdot g_{m+1})$$
$$= \phi(x) + 1.$$

QED.

3.7.19 Satz von Herbrand

Seien K ein vollständiger diskret bewerteter Körper, L/K eine endliche Galois-Erweiterung mit κ_L/κ separabel und der Galois-Gruppe $\Gamma := G(L/K)$. Weiter seien

$$\Delta \subseteq \Gamma \text{ , } F := L^\Delta$$

ein Normalteiler bzw. dessen Fixkörper. Dann gilt:

(i) $\phi_{L/K}(x) = \phi_{F/K}(\phi_{L/F}(x))$ für jede reelle Zahl $x \ge -1$.

(ii) $(\Gamma/\Delta)^y = \Gamma^y\Delta/\Delta$. für jede reelle Zahl $y \ge -1$.

Beweis. Für

$$\omega \in \Gamma/\Delta = G(F/K)$$

bezeichne

$$j(\omega) := \sup \{\iota_{L/K}(\sigma) \mid \sigma \mapsto \omega\} = \sup \{ \iota_{L/K}(\sigma) \mid \sigma \in \omega\}$$

das Supremum, welches $\iota_{L/K}$ auf der Restklasse ω annimmt.

<u>1. Schritt</u>. $\iota_{F/K}(\omega) -1 = \phi_{L/F} (j(\omega) - 1)$.

Sei $\sigma_0 \in \Gamma$ ein Element aus der Restklasse ω, in welchem die Funktion $\iota_{L/K}$ das Supremum annimmt, d.h.

$$\iota_{L/K}(\sigma_0) = j(\omega), \sigma_0 \in \omega.$$

Die Elemente von ω haben die Gestalt $\sigma_0\tau$ mit $\tau\in\Delta$. Die Formel von 3.7.13 bekommt dammit die Gestalt

$$e(L/F)\cdot\iota_{F/K}(\omega) = \sum_{\sigma\mapsto\omega} \iota_{L/K}(\sigma) = \sum_{\tau\in\Delta} \iota_{L/K}(\sigma_0\tau) \qquad (1)$$

Die Beweisidee für die Formel des ersten Schritts besteht darin, die Summanden auf der rechten Seite so umzuformen, daß sie die Gestalt der Summanden auf der rechten Seite der Formel 3.7.18 für ϕ bekommen.

Ist $\iota_{L/K}(\tau) < j(\omega)$, so gilt

$$\iota_{L/K}(\sigma_0\tau) =^{105} \inf(\iota_{L/K}(\sigma_0), \iota_{L/K}(\tau)) = \iota_{L/K}(\tau) = \inf\{ \iota_{L/K}(\tau), j(\omega)\}.$$

Ist $\iota_{L/K}(\tau) \ge j(\omega)$, so gilt

$$j(\omega) \ge^{106} \iota_{L/K}(\sigma_0\tau) \ge^{107} \inf \{ \iota_{L/K}(\sigma_0), \iota_{L/K}(\tau) \} \ge^{108} \inf\{ \iota_{L/K}(\tau), j(\omega)\} = j(\omega).$$

---

[105] nach 3.7.5 und weil $\iota_{L/K}(\sigma_0) = j(\omega)$ nach Wahl von σ_0 gilt.

[106] Nach Definition von j.

[107] auf Grund der allgemeinen Eigenschaften von ι, vgl. 3.7.3.

[108] Nach Definiton von j und Wahl von σ_0.

In der letzten Abschätzung gilt somit überall das Gleichheitszeichen. Zusammen ergibt sich,

$$\iota_{L/K}(\sigma_0\tau) = \inf\{ \iota_{L/F}(\tau), j(\omega)\} \tag{2}$$

für jedes $\tau\in\Delta$. Man beachte, in $\sigma\in\Delta$ haben $\iota_{L/F}$ und $\iota_{L/K}$ denselben Wert.[109] Wir setzen (2) in (1) ein und erhalten

$$e(L/F)\bullet\iota_{F/K}(\omega) = \sum_{\tau\in\Delta} \inf\{ \iota_{L/F}(\tau), j(\omega)\}.$$

Nach 3.7.18 ist die Summe auf der rechten Seite gerade gleich

$$g_0(L/F)\bullet(\phi_{L/F}(x) + 1) \text{ mit } x = j(\omega) - 1.$$

Wegen $g_0(L/F) =$[110] $e(L/F)$ folgt

$$\iota_{F/K}(\omega) = \phi_{L/F}(x) + 1,\ x = j(\omega) - 1.$$

Dies ist aber gerade die behauptete Formel.

2. Schritt. $\Gamma_x\Delta/\Delta = (\Gamma/\Delta)_y$ mit $y = \phi_{L/F}(x)$.

Eine Element $\omega\in\Gamma/\Delta$ liegt genau dann in $\Gamma_x\Delta/\Delta$, wenn es ein $\sigma\in\Gamma_x$, welches die Restklasse ω repräsentiert, d.h. ein $\sigma\in\omega$ mit $\iota_{L/K}(\sigma) \geq x + 1$. Wir können dann σ noch so wählen, daß ι den maximal möglichen Wert $j(\omega)$ annimmt. Damit gilt

$$\begin{aligned} \omega \in \Gamma_x\Delta/\Delta \quad &\Leftrightarrow j(\omega) \geq x + 1 \\ &\Leftrightarrow j(\omega) - 1 \geq x \\ &\Leftrightarrow \phi_{L/F}(j(\omega) - 1) \geq \phi_{L/F}(x) \quad (\phi \text{ ist streng monoton}) \\ &\Leftrightarrow \iota_{F/K}(\omega) -1 \geq \phi_{L/F}(x) \quad (\text{nach dem 1. Schritt}) \\ &\Leftrightarrow \omega \in (\Gamma/\Delta)_y \text{ mit } y := \phi_{L/F}(x). \end{aligned}$$

3. Schritt. Beweis von Aussage (i).

Wir setzen

$$\theta(x) := \phi_{F/K}(\phi_{L/F}(x)).$$

Zeigen wir, die Funktion θ hat gerade die Eigenschaften, welche nach 3.7.16 die Funktion $\phi := \phi_{L/K}$ charakterisieren, d.h.

1. $\phi(0) = 0$.
2. $\phi : [-1, \infty) \longrightarrow [-1, \infty)$ ist stetig.
3. Ist m eine ganze Zahl ≥ -1, so ist die Funktion ϕ linear auf dem Intervall
$$[m, m+1]$$
und besitzt im offenen Intervall $(m, m+1)$ die Ableitung
$$\phi'(x) = (\#\, \Gamma_x)/e(L/K).$$

Für die ersten beiden Eigenschaften ist dies offenischtlich der Fall. Beschäftigen wir uns mit der dritten. Sei m eine ganze Zahl ≥ -1. Wenn x im offenen Intervall $(m, m + 1)$ variiert,

---

[109] Weil mit $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ auch $\mathcal{O}_L = \mathcal{O}_F[\alpha]$ gilt.

[110] Vgl. das Beispiel von 3.7.10.

$$x \in (m, m + 1),$$

so liegt im Intervall

$$(\phi_{L/F}(m), \phi_{L/F}(m+1))$$

keine ganze Zahl (nach 3.7.17). Die Funktion $\phi_{F/K}$ ist deshalb auf dem zugehörigen abgeschlossenen Intervall linear[111]. Dann ist aber θ als Zusammensetzung linearer Funktionen auf dem Intervall [m, m+1] linear. Wir haben noch die Ableitungen von θ und $\phi_{L/K}$ in den Punkten mit nicht-ganzzahligen Koordinaten zu bestimmen. Es gilt für nicht ganzzahlige x :

$$\theta'(x) \quad =^{112} \phi_{F/K}'(y)\bullet\phi_{L/F}(x)' \text{ mit } y = \phi_{L/F}(x).$$

Nach 3.7.16 mit F/K anstelle von L/K ist

$$\phi_{F/K}'(y) = \# (\Gamma/\Delta)_y / e(F/(K).$$

Nach derselben Formel 3.7.16 und 3.7.7 berechnet sich die Ableitung des zweiten Faktors zu

$$\phi_{L/F}(x)' = \# (\Gamma_x \cap \Delta)/e(L/F).$$

Damit erhalten wir

$$\begin{aligned}
\theta'(x) \quad &= \# (\Gamma/\Delta)_y \bullet \# (\Gamma_x \cap \Delta)/(e(F/(K)\bullet e(L/F)) \\
&= \# (\Gamma/\Delta)_y \bullet \# (\Gamma_x \cap \Delta)/e(L/(K) && \text{(e verhält sich multiplikativ)} \\
&= \# (\Gamma_x\Delta/\Delta)\bullet \# (\Gamma_x \cap \Delta)/e(L/(K) && \text{(nach dem 2. Schritt).} \\
&= \# (\Gamma_x / \Gamma_x \cap \Delta))\bullet \# (\Gamma_x \cap \Delta)/e(L/(K) && \text{(Isomorphie-Satz)} \\
&= \# \Gamma_x / e(L/K) \\
&= \phi_{L/K}(x) && \text{(nach 3.7.16).}
\end{aligned}$$

Damit ist Aussage (i) bewiesen.

<u>4. Schritt</u>: Beweis von Aussage (ii).

Nach dem zweiten Schritt gilt

$$\Gamma_x\Delta/\Delta = (\Gamma/\Delta)_y \text{ mit } y = \phi_{L/F}(x).$$

Nach Definition der Verzweigungsgruppen bezüglich der Herbrand-Indizierung (vgl. 3.7.15) ist weiter

$$\begin{aligned}
\Gamma^z \quad &= \Gamma_x \qquad \text{mit } z := \phi_{L/K}(x) \\
(\Gamma/\Delta)^w \quad &= (\Gamma/\Delta)_y
\end{aligned}$$

mit $w = \phi_{F/K}(y) = \phi_{F/K}(\phi_{L/F}(x)) =^{113} \phi_{L/K}(x) = z$. Zusammen erhalten wir

$$\begin{aligned}
(\Gamma/\Delta)^w \quad &= (\Gamma/\Delta)_y \\
&= \Gamma_x\Delta/\Delta && \text{(nach dem 2. Schritt)} \\
&= \Gamma^z\Delta/\Delta && \text{(s.o.)}
\end{aligned}$$

---

[111] Nur in Punkten mit ganzzahligen Koordinaten kann nach Definiton von ϕ eine Änderung des Anstiegs stattfinden.

[112] Beim Zusammensetzen linearer Funktionen multiplizieren sich deren Anstiege.

[113] Nach (i).

$$= \Gamma^w\Delta/\Delta \qquad \text{(wegen } w = z\text{)}.$$

QED.

Bemerkungen

(i) Weitere Aussagen zu den Verzweigungsgruppen findet man im Buch über lokale Körper von Serre (Serre [1], Kapitel IV).

(ii) Weitere Aussagen zur Herbrand-Funktion ϕ findet man im selben Buch in den Kapiteln IV und V.

3.8 Der globale Fall

In diesem Abschnitt seien R ein beliebiger Dedekind-Ring mit dem Quotientenkörper K,

$$L/K$$

eine endliche separable Körper-Erweiterung und

$$S \subseteq L$$

die ganze Abschließung von R in L. Wir schreiben dann auch

$$\mathcal{O}_K := R,\ \mathcal{O}_L := S.$$

3.8.1 Körpergrad und Verzweigungsindex

Seien R ein beliebiger Dedekind-Ring mit dem Quotientenkörper K,

$$L/K$$

eine endliche separable Körper-Erweiterung und

$$S \subseteq L$$

die ganze Abschließung von R in L. Für jedes von Null verschieden Primideal $p \subseteq R$ gilt dann

$$[L:K] = \sum_{P|p} e(P|p)\cdot f(P|p).$$

Dabei werde die Summe über alle Primideale $P \subseteq S$ erstreckt, welche über p liegen.

Beweis. Bezeichne K_p die Vervollständigung von K bezüglich der p-adischen Topologie.

Weiter seien

$$P_1, \dots , P_r$$

die über p liegenden Primideale von S, und für

$$P \in \{ P_1, \dots , P_r\}$$

bezeichne L_P die Vervollständigung von L bezüglich der P-adischen Topologie. Nach 2.3.12 gilt dann

$$L\otimes_K K_p \cong L_{P_1} \oplus\dots\oplus L_{P_r},$$

also

$$[L:K] = \dim_K L = \dim_{K_p} L\otimes_K K_p = \dim_{K_p} L_{P_1}\oplus\dots\oplus L_{P_r} = \sum_{i=1}^r \dim_{K_p} L_{P_i}$$

$$= \sum_{i=1}^r [L_{P_i} : K_p]$$

$$= \sum_{i=1}^{r} e(P_i|p)\cdot f(P_i|p).$$

Das letzte Gleichheitszeichen gilt nach 3.3.7.
QED.

3.8.2 Der normale Fall: die Konjugiertheit der Primideale über demselben Primideal.

Seien R ein beliebiger Dedekind-Ring mit dem Quotientenkörper K,

$$L/K$$

eine endliche Galois-Erweiterung und

$$S \subseteq L$$

die ganze Abschließung von R in L. Weiter seien $\wp \subseteq R$ ein von Null verschiedenes Primideal und $P \subseteq S$ ein über $\wp$ liegendes Primideal von S. Dann sind die über $\wp$ liegenden Primideale von S gerade die Ideale der Gestalt

$$\sigma(P) \text{ mit } \sigma \in G(L/K).$$

Beweis. Sei

$$G = \{\sigma_1, \dots, \sigma_r\},\ r = [L:K]$$

und sei P' ein weiteres über $\wp$ liegendes Primideal von S. Angenommen,

$$P' \neq \sigma(P)$$

für jedes $\sigma \in G$. Dann ist P in keinem der $\sigma^{-1}(P')$ ganz enthalten, d.h. es gibt ein

$$a \in P,$$

das in keinem der $\sigma^{-1}(P')$ enthalten ist, d.h.

$$\sigma(a) \notin P' \text{ für } \sigma \in G.$$

Wir setzen

$$b := \prod_{i=1}^{r} \sigma_i(a) \notin P'. \tag{1}$$

Dann gilt

$$b := N_{L/K}(a) \in K,$$

und b ist ganz über R, d.h. es ist

$$b \in R.$$

Nun ist eines der σ_i die identische Abbildung, d.h. es gilt

$$b \in P,$$

also

$$b \in P \cap R = \wp \subseteq P'$$

im Widerspruch zu (1).
QED.

3.8.3 Vergleich von e und f für verschiedene Primideal über demselben Primideal

Seien R ein beliebiger Dedekind-Ring mit dem Quotientenkörper K,

$$L/K$$

eine endliche Galois-Erweiterung und

$$S \subseteq L$$

die ganze Abschließung von R in L. Weiter seien $\wp \subseteq$ R ein von Null verschiedenes Primideal und P $\subseteq$ S ein über $\wp$ liegendes Primideal von S. Dann hängen

$$e := e(P|p) \text{ und } f := f(P|p)$$

nicht von der speziellen Wahl von P ab. Ist g die Anzahl der über p liegenden Primideal von S, so gilt

$$[L:K] = e\bullet f\bullet g.$$

Beweis. Sei P' ein weiteres über p liegendes Primideal von S. Nach 3.8.2 gibt es ein

$$\sigma\in G := G(L/K)$$

mit

$$P' = \sigma(P).$$

Nach Definition von e := e(P|p) gilt

$$pS_P = P^eS_P .$$

Wir wenden σ an und erhalten

$$pS_{P'} = P'^eS_{P'}.$$

Insbesondere ist

$$e(P'|p) = e = e(P|p).$$

Die Einschränkung von σ auf S ist ein Isomorphismus

$$\sigma: S \longrightarrow S$$

von Ringen mit 1, welcher den Teilring R elementweise fest läßt und P in P' überführt. Deshalb induziert diese Abbildung einen Isomorphismen

$S/P \longrightarrow S/P'$

der Restkörper, welcher den Restekörper von R elementweise fest läßt. Damit gilt

$$f(P'|p) = \dim_{R/p} S/P' = \dim_{R/p} S/P = f(P|p).$$

Zusammen mit 3.8.1 ergibt sich schließlich

$$[L:K] = e\bullet f\bullet g.$$

QED.

3.8.4 Die Zerlegungsgruppe

Seien R ein beliebiger Dedekind-Ring mit dem Quotientenkörper K,

$$L/K$$

eine endliche Galois-Erweiterung und

$$S \subseteq L$$

die ganze Abschließung von R in L. Weiter seien $\wp \subseteq$ R ein von Null verschiedenes Primideal und P $\subseteq$ S ein über $\wp$ liegendes Primideal von S. Dann heißt

$$\Gamma_P := \{ \sigma \in G(L/K) \mid \sigma(P) = P \}$$

<u>Zerlegungsgruppe</u> von P über p.

Bemerkungen

(i) Sei v: $L^* \longrightarrow \mathbb{Z}$ die durch P definierte Bewertung von L. Dann gilt

$$\begin{aligned}\Gamma_P &= \{\sigma\in G(L/K) \mid v(\sigma x) = v(x) \text{ für jedes } x \in L\}\\ &= \{\sigma\in G(L/K) \mid v(\sigma x) = v(x) \text{ für jedes } x \in S\}\end{aligned}$$

(ii) Für jedes σ∈G(L/K) gilt

$$\Gamma_{\sigma(P)} = \sigma\Gamma_P\sigma^{-1}.$$

Beweis. Zu (i). Sei $\sigma\in\Gamma_P$. Dann gilt $\sigma P = P$ und für jedes $x \in L$ ist

$$\begin{aligned} v(\sigma x) &= \sup\{n \mid \sigma x \in P^n S_P\} \\ &= \sup\{n \mid x \in \sigma^{-1}(P^n S_P)\} \\ &= \sup\{n \mid x \in \sigma^{-1}(P)^n S_P)\} \\ &= \sup\{n \mid x \in P^n S_P)\} \\ &= v(x). \end{aligned}$$

Sei umgekehrt

$$v(\sigma x) = v(x)$$

für jedes $x \in S$. Dann gilt

$$x \in P \Leftrightarrow v(x) > 0 \Leftrightarrow v(\sigma^{-1}x) > 0 \Leftrightarrow \sigma^{-1}x \in P \Leftrightarrow x \in \sigma(P).$$

Mit anderen Worten, es gilt $\sigma(P) = P$, d.h. $\sigma\in\Gamma_P$.

Zu (ii). Es gilt

$$\begin{aligned} \tau \in \Gamma_{\sigma(P)} &\Leftrightarrow \tau\sigma(P) = \sigma(P) \\ &\Leftrightarrow \sigma^{-1}\tau\sigma(P) = P \\ &\Leftrightarrow \sigma^{-1}\tau\sigma \in \Gamma_P \\ &\Leftrightarrow \tau \in \sigma\,\Gamma_P\sigma^{-1} \end{aligned}$$

QED.

3.8.5 Beschreibung der Zerlegungsgruppe mit Hilfe lokaler Daten

Seien R ein beliebiger Dedekind-Ring mit dem Quotientenkörper K,

$$L/K$$

eine endliche Galois-Erweiterung und

$$S \subseteq L$$

die ganze Abschließung von R in L. Weiter seien $\wp \subseteq R$ ein von Null verschiedenes Primideal und $P \subseteq S$ ein über $\wp$ liegendes Primideal von S. Dann gilt:

(i) Die Körper-Erweiterung L_P/K_p der Vervollständigungen von L und K bezüglich der P-adischen bzw. p-adischen Topologien ist eine Galois-Erweiterung.

(ii) Die Einschränkungsabbildung

$$G(L_P/K_p) \longrightarrow G(L/K),\ \sigma \mapsto \sigma|_L\ ,$$

ist ein injektiver Gruppen-Homomorphismus, dessen Bild gerade die Zerlegungsgruppe Γ_P ist.

Beweis. Zu (i). Sei $\bar{L}$ ein algebraische Abschließung von L_P und

$$h: L_P \longrightarrow \bar{L}$$

eine K_p-Einbettung. Wir identifizieren L_P mit seinem Bild in $\bar{L}$ und h mit der natürlichen Einbettung. Dann ist die Einschränkung dieser Abbildung auf L eine K-Einbettung in einen algbraisch abgeschlossenen Körper. Weil L normal ist über K ist, folgt

$$h(L) = L \subseteq L_P \subseteq \overline{L}.$$

Die Abbildung h ist (als identische Abbildung) stetig in der P-adischen Topologie. Insbesondere gilt $h(L_P) \subseteq L_P$. Weil h eine K_p-Einbettung ist, folgt (aus Grad-Gründen)

$$h(L_P) = L_P.$$

Wir haben gezeigt, die Erweiterung L_P/K_p ist normal.

Als endliche separable Erweiterung ist L/K einfach, sagen wir

$$L = K(\alpha).$$

Sei f das Minimalpolynom von α über K. Dann ist auch L_P/K_p einfach, wobei man als zugehörigen Minimalpolynom einen über K_p irreduziblen Teiler g von f verwenden kann (siehe 2.3.11 und 2.3.12). Insbesondere hat mit f auch g keine mehrfachen Nullstellen. Die Erweiterung L_P/K_p ist somit separabel.

Zu (ii). Die Abbildung $\sigma \mapsto \sigma|_L$ ist nach Konstruktion ein Gruppen-Homomorphismus.

Weil jedes $\sigma \in G(L_P/K_p)$ das Bewertungsideal von L_P in sich abbildet, gilt

$$\sigma(P) = P. \tag{1}$$

Insbesondere ist die Einschränkung von σ auf L stetig. Weil L dicht liegt in seiner Vervollständigung L_P gibt es genau eine stetige Fortsetzung von $\sigma|_L$ auf L_P. Mit anderen Worten, die Abbildung ist injektiv.

Wir haben noch das Bild des Homomorphismus zu bestimmen. Wie wir bereits gesehen haben, gilt (1) für jedes σ, d.h. das Bild des Homomorphismus liegt ganz in der Zerlegungsgruppe.

Sei jetzt umgekehrt

$$\tau \in \Gamma_P$$

ein Element aus der Zerlegungsgruppe von P. Dann ist die Abbildung

$$\tau: L \longrightarrow L$$

stetig in der P-adischen Topologie, besitzt also eine eindeutig bestimmte stetige Fortsetzung

$$\hat{\tau}: L_P \longrightarrow L_P$$

auf die P-adische Vervollständigung von L. Weil τ ein Homomorphismus von Ringen mit 1 ist, gilt dasselbe (aus Stetigkeitsgründen) für $\hat{\tau}$. Weil τ den Körper K elementeweise in sich abbildet und K dicht liegt in K_p, wird K_p bei der Fortsetzung $\hat{\tau}$ elementweise in sich abgebildet. Es ist also

$$\hat{\tau} \in G(L_P/K_p).$$

Nach Konstruktion ist die Einschränkung von $\hat{\tau}$ auf L gerade τ. Das Bild des Homomorphismus (ii) ist somit die Zerlegungsgruppe.

QED.

3.8.6 Definition der Verzweigungsgruppen im globalen Kontext

Seien R ein beliebiger Dedekind-Ring mit dem Quotientenkörper K,

$$L/K$$
eine endliche Galois-Erweiterung und
$$S \subseteq L$$
die ganze Abschließung von R in L. Weiter seien $\wp \subseteq R$ ein von Null verschiedenes Primideal und $P \subseteq S$ ein über $\wp$ liegendes Primideal von S.
Weiter bezeichne
$$v_P: L^* \longrightarrow \mathbb{Z}$$
die durch P auf L definierte Bewertung. Dann heißt
$$\Gamma_{P,i} := \{\sigma \in \Gamma_P \mid v_P(\sigma x - x) \geq i + 1 \text{ für } x \in S\}$$
i-te <u>Verzweigungsgruppe</u> von P über p.

Bemerkungen

(i) Man kann in der Definiton von $\Gamma_{P,i}$ die Zerlegungsgruppe Γ_P durch die Galois-Gruppe ersetzen,
$$\Gamma_{P,i} := \{\sigma \in G(L/K) \mid v_P(\sigma x - x) \geq i + 1 \text{ für } x \in S\}$$

(ii) Identifiziert man die Zerlegungsgruppe Γ_P mit der Galois-Gruppe $G(L_P/K_p)$ der zugehörigen Erweiterung der Vervollständigungen, so entsprechen den gerade definierten Verzweigungsgruppen $\Gamma_{P,i}$ den früher in der lokalen Situation definierten Verzweigungsgruppen (weil der Ring S dicht liegt im Bewertungsring von L_P).

Index

Inhalt