Zahlentheorie

Di. 13-15 SR 1-15
ursprünglich Di. 11-13 Hs 14

4. Globale Körper

4.0 Wiederholung

Die Ausgangssituation

Der Gegenstand unserer Untersuchungen sind die ganzen rationalen Zahlen $\mathbb{Z} \subseteq \mathbb{Q}$ und allgemeiner deren ganze Abschließungen $\mathcal{O}_K$ in einer endlichen separablen Erweiterung $K/\mathbb{Q}$.

$$\begin{array}{ccc} \mathcal{O}_K & \subseteq & K \\ \cup & & \cup \\ \mathbb{Z} & \subseteq & \mathbb{Q} \end{array} \tag{1}$$

Wir sagen in dieser Situation, $\mathcal{O}_K$ ist der Ring der ganzen Zahlen von K.

Allgemeiner interessieren wir uns für das Verhalten von Primelementen beim Übergang zu endlichen separablen Erweiterungen der zugehörigen Körper, d.h. in der Situation

$$\begin{array}{ccc} \mathcal{O}_L & \subseteq & L \\ \cup & & \cup \\ \mathcal{O}_K & \subseteq & K \end{array} \tag{2}$$

wobei

L/K eine endliche separable Körpererweiterung ist,
$\mathcal{O}_K$ ein Dedekindring mit dem Quotientenkörper K und
$\mathcal{O}_L$ die ganze Abschließung von $\mathcal{O}_K$ in L.

Primfaktoerzerlegung und Lokalisierung

Wir wissen in dieser Situation, daß $\mathcal{O}_L$ ein Dedekindring und ein endlich erzeugter $\mathcal{O}_L$-Modul ist (vgl. 1.9.3).

Wir wissen außerdem, daß die Lokalisierungen von $\mathcal{O}_K$ bzw. $\mathcal{O}_L$ in den von Null verschiedenen Primidealen diskrete Bewertungsringe sind und daß man zum Verständniss der Situation in den Dedekindringen die in den diskreten Bewertungsringen verstehen muß. Insbesondere gilt für die zugehörigen Gruppen der gebrochenen Ideale (vgl. 1.5.5)

$$F(\mathcal{O}_K) \xrightarrow{\cong} \oplus''_p F(\mathcal{O}_{K,p}),\ I \mapsto (I\mathcal{O}_{K,p})_p \ ,$$

wobei p die Menge der von Null verschiedenen Primideale von $\mathcal{O}_K$ durchläuft und $\mathcal{O}_{K,p}$ die Lokalisierung von $\mathcal{O}_K$ in p bezeichnet. Die gebrochenen Ideale in $\mathcal{O}_{K,p}$ sind gerade von der Gestalt

$$p^n\mathcal{O}_{K,p}$$

mit einer eindeutig bestimmten ganzen Zahl n, d.h. die direkten Summanden auf der rechten Seite sind sämtlich isomorph zu $\mathbb{Z}$. (vgl. den Beweis von 1.4.10).

Lokalisierung und Vervollständigung

In unseren bisherigen Untersuchungen haben wir $\mathcal{O}_K$ und $\mathcal{O}_L$ durch übereinander liegende Bewertungsringe dieser Ringe betrachtet, d.h. wir haben von Null verschiedene Primideale

$$p \subseteq \mathcal{O}_K \text{ und } q \subseteq \mathcal{O}_L \text{ mit } p \subseteq q$$

fixiert und anstelle der Inklusion $\mathcal{O}_K \subseteq \mathcal{O}_L$ die zugehörige Inklusion der Lokalisierungen

$$\mathcal{O}_{K,p} \subseteq \mathcal{O}_{L,q}$$

betrachtet. Mit anderen Worten, unsere bisherigen Untersuchungen haben sich auf den lokalen Fall beschränkt. Wir haben dabei festgestellt, daß man in dieser Situation die beiden diskreten Bewertungsringe durch deren Vervollständigung ersetzen kann. In der Situation von (1), d.h. falls die Restekörper der Ringe endlich sind, sind die Quotientenkörper der Ringe sogenannte lokale Körper.

Verzweigung

Die Untersuchung der endlichen separablen Erweiterungen der lokalen Körper hat im wesentlichen die gesamte Vorlesung im vergangenen Semester in Anspruch genommen. Wesentlicher Bestandteil war das Verhalten von Norm, Spur, Diskriminante und Differente bei unverzweigten, zahm verzweigten und total verzweigten Erweiterungen lokaler Körper und die Konseqenzen dieses Verhaltens für unsere Ausgangsringe $\mathcal{O}_K$ und $\mathcal{O}_L$. Insbesondere haben wir gesehen, daß die Erweiterung

$$\mathcal{O}_{K,p} \subseteq \mathcal{O}_{L,q}$$

nur für endlich viele p und q verzweigt ist (vgl. 3.3.16).

Adele

Unser nächstes Ziel ist es, einen Kalkül zu entwickeln, mit dem wir weitere unserer Erkenntnisse in der lokalen Situation auf die globale Situation übertragen können. Insbesondere wollen wir im folgenden nicht einzelne Bewertungsringe $\mathcal{O}_{K,p}$ von $\mathcal{O}_K$ betrachten, sondern alle Bewertungsring gleichzeitig.

Etwas vergröbert könnte man sagen, wir interessieren uns für das direkte Produkt

$$\prod_p \mathcal{O}_{K,p} \text{ ,}$$

wobei wir wie bei allen bisherigen Untersuchungen auch hier eine geeignete Topologie einführen müssen. Bei dieser Topologie handelt es sich nicht um die gewöhnliche

Produkt-Topologie, sondern um eine speziell an die Eigenschaften von Bewertungen angepaßte sogenannte adelesche Topologie.

Außerdem wird es nicht reichen, nur die dieskreten Bewertungsringe von $\mathcal{O}_K$ ins Spiel zu bringen. Wir müssen auch die nicht-archimedischen Bewertungen von $\mathcal{O}_K$ beachten. Deshalb werden wir im folgenden das Gewicht wieder mehr auf die multiplikativen und weniger auf die additischen Bewertungen legen.

Multiplikative Bewertungen

Ich erinnere deshalb zunächst an die wichtigsten Ergebnisse, die wir im Zusammenhang mit den multiplikativen Bewertungen bewiesen haben.

Definition
Eine (multiplikative) Bewertung eines Körpers K ist eine Abbildung

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

mit folgenden Eigenschaften.

(i) $|x| \geq 0$ für jedes $x \in K$ und $|x| = 0 \Leftrightarrow x = 0$.

(ii) $|x \cdot y| = |x| \cdot |y|$ für beliebige $x, y \in K$.

(iii) Es gibt eine reelle Konstante C mit

$$|x + 1| \leq C \text{ für beliebige } x \in K \text{ mit } |x| \leq 1.$$

Eine Bewertung, für welche Axiom (iii) mit C = 1 gilt, heißt nicht-archimedisch.

Eigenschaften

- Ein Beispiel für eine (archimedische) Bewertung ist der gewöhnliche Absolut-Betrag für komplexe Zahlen. Jeder diskrete Bewertungsring definiert eine (nicht-archimedische) Bewertung.
- Jede Bewertung definiert auf K eine Topologie in derselben Weise wie der Absolut-Betrag dies auf den komplexen Zahlen tut. Genauer, die ε-Umgebungen

  $$U_\varepsilon(x) := \{ y \in K \mid |y-x| < \varepsilon \}$$

  mit $\varepsilon > 0$ und $x \in K$ bilden eine Umgebungsbasis dieser Topologie.
- Zwei Bewertungen heißen äquivalent, wenn sie dieselbe Topologie auf K definieren (vgl. 2.1.3 und 2.3.2).
- Jede Bewertung ist äquivalent zu einer Bewertung, für welche die Dreiecksunglechung besteht (2.1.4).
- Jeder archimedisch bewertete Körper ist ein Teilköper von $\mathbb{C}$, wobei die Bewertung gerade der Absolut-Betrag ist (vgl. 2.2.4 Satz von Gelfand-Tornheim).
- Jede Bewertung von $\mathbb{Q}$ kommt von einem der Bewertungsringe $\mathbb{Z}_{(p)}$ mit einer Primzahl p oder ist gerade die Einschränkung des gewöhnlichen Absolutbetrags (vgl. 2.1.15 Satz von Ostrovskij).
- Jeder bewertete Körper liegt dicht in einem vollständigen[1] bewerteten Körper, dessen Bewertung die des Ausgangskörpers fortsetzt und welcher Vervollständgung dieses Körpers heißt. Die Vervollständigung ist bis auf Isomorphie eindeutig bestimmt (vgl. 2.3.3). Die Eigenschaft der Bewertung, archimedisch oder nicht-archimedisch zu sein, bleibt beim Übergang zur Vervollständigung erhalten (vgl. 2.1.8).
- Für jede endliche Körpererweiterung K/k eines vollständig bewerteten Körpers k gibt es genau eine Fortsetzung der Bewertung von k auf K (vgl. 2.3.8).

[1] d.h. jede Cauchy-Folge ist konvergent.

- Für jede endliche Körpererweiterung K/k eines bewerteten Körpers k gibt es mindestens eine Fortsetzung und höchstens endlich viele Fortsetzungen der Bewertung von k auf K (vgl. 2.3.12).
- Schwacher Approximationssatz (vgl. 2.3.4)
  Seien k ein Körper und
  $$|?|_1 , \dots , |?|_N$$
  paarweise nicht-äquivalente Bewertungen von k. Bezeichne
  $$\overline{k}_i$$
  die Vervollständigung von k bezüglich der i-ten Bewertung $|?|_i$. Dann liegt das Bild von k im direkten Produkt der $\overline{k}_i$ bei der Diagonal-Einbettung dicht, d.h. für jedes N-Tupel aus diesen direkten Produkt gibt es eine Folge in k, welche für i = 1, ... , N bezüglich der i-ten Topologie gegen die i-te Koordinate des Tupels konvergiert.
- Sei K ein lokaler Körper, d.h. K ist diskret bewertet, vollständig bezüglich dieser Bewertung und hat einen endlichen Restekörper (3.1.2). Dann ist K lokal kompakt in der zugehörigen Topologie (vgl. 2.4.1). Insbesondere ist K mit einem Haarschen Maß versehen.
- Sei K ein lokaler Körper mit der Bewertung |?|. Dann gibt es unter den zu |?| äquivalenten Bewertungen genau eine mit
  $$|\pi| = \frac{1}{q} ,$$
  wobei π einen Parameter von K und q die Anzahl der Elemente des Restekörpers bezeichnet (vgl. 2.4.3). Diese Bewertung heißt normalisierte Bewertung von K und stimmt im wesentlichen gerade mit dem Haarschen Maß von K überein (vgl. 2.4.4).
- Die Topologie eines lokalen Körpers ist total unzusammenhängend, d.h. jede Zusammenhangskomponente besteht aus nur einem Punkt (vgl. 3.4.7).
- 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[2]
  $$K \otimes_k L \cong L_1 \times \dots \times L_r .$$
  Als Körper über k und L sind die L_i paarweise isomorph und gleich dem Kompositum von K und L ,
  $$L_i \cong K \bullet L.$$
  Für $\alpha \in K$ bezeichne
  $$\chi_\alpha \in k[x] , \chi_{i,\alpha} \in L_i[x]$$
  das Charakteristische Polynom[3] von α bezüglich K/k bzw. L_i/L. Dann gilt

---

[2] 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.

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

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

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)
  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.

Literatur

Wie bisher wird sich unser Darstelljung des Gegenstands eng am Buch von

Cassels, J.W.S., Fröhlich, A.: Algebraic number theory, Academic Press, London and New York 1967,

orientieren. Eine alternative Darstellung desselben Stoffs findet man in den folgenden Büchern.

Neukirch, J.: Algebraic number theory, Springer, Berlin-Heidelberg 1999.
Weil, A.: Basic number theory, Springer, Berlin-New York-Heidelberg 1967.

Zum weiteren Verlauf der Vorlesung

Wir beginnen mit einer leichten Verallgemeinerung unserer Aussagen zur Fortsetzbarkeit von Bewertungen im Kontext der normalisierten Bewergungen. Wir benötigen diese Verallgemeinerung, weil wir wie oben erwähnt im folgenden auch die archimedischen Bewertungen im Auge behalten müssen.

4.1 Fortsetzung normalisierter Bewertungen

4.1.1. Zum Begriff der normalisierten Bewertung (Ergänzung)

Sei k ein bewerteter Körper mit der Bewerung |?|, welcher eine der beiden folgenden Bedingungen erfüllt.

1. |?| ist diskret und nicht-archimedisch, und der Restekörper ist endlich.
2. |?| ist archimedisch.

Zu 1. In diesem Fall ist der Begriff der normalisierten Bewertung bereits definiert (vgl. 2.4.3). Bezeichne π einen Parameter der Bewertung. Dann hat jedes von Null verschiedene Element x die Gestalt

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

mit einer eindeutig bestimmten (von π unabhängigen) ganzen Zahl n und einer Einheit u. Der normalisierte Wert von x ist dann

$$\|x\| := (1/q)^n,$$

wobei q die Anzahl der Elemente des Restekörpers bezeichne.

Zu 2. In diesem Fall ist k als bewerteter Körper ein Teilkörper von $\mathbb{C}$ (vgl. 2.2.4 Gelfand-Tornheim). Insbesondere hat k die Charakteristik 0, d.h. es ist

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

Für die Vervollständigung von k bezüglich der gegebene Bewertung gilt deshalb

$$\mathbb{R} \subseteq \overline{k} \subseteq \mathbb{C},$$

d.h. k hat den Körpergrad 1 oder 2 über den reellen Zahlen. Damit gibt es nur die beiden folgenden Möglichkeiten.

2a. $\overline{k} = \mathbb{R}$.
Wir definieren die normalisierten Bewertung als

$$\|x\| := |x|$$

den gewöhnlichen Absolut-Betrag komplexer Zahlen.

2b. $\overline{k} = \mathbb{C}$.
Wir definieren die normalisierte Bewertung als

$$\|x\| := |x|^2$$

das Quadrat des gewöhnlichen Absolut-Betrags komplexer Zahlen.

Bemerkung

(i) In allen drei Fällen 1, 2a und 2b multipliziert die Abbildung

$$\mathrm{mult}_\alpha : \overline{k}^+ \longrightarrow \overline{k}^+,\ x \mapsto \alpha x,$$

für jedes $\alpha \in \overline{k}$ das Haarsche Maß der additiven Gruppe der Vervollständigung von $\overline{k}$ gerade mit dem Faktor $\|\alpha\|$, d.h. für jede meßbare Menge $U \subseteq \overline{k}$ ist

$$\mu(\mathrm{mult}_\alpha(U)) = \|\alpha\| \cdot \mu(U),$$

wobei μ ein Haarsches Maß von $\overline{k}^+$ bezeichne.[4]

(ii) Die in (i) beschriebene Bedingung charakterisiert die normalisierte Bewertung innerhalb der Klasse der zu $\|?\|$ äquivalenten Bewertungen.

4.1.2 Fortsetzungsformel für normalisierte Bewertungen (vollständiger Fall)

Seien k ein vollständig bewerteter Körper bezüglich einer normalisierten Bewertung $|?|$ wie in 4.1.1. und

$$K/k$$

eine Körpererweiterung des Grades

$$N := [K:k].$$

Weiter sei $\|?\|$ die normalisierte Bewertung zur eindeutig bestimmte Fortsetzung von $|?|$ auf K (vgl. 2.3.8). Dann gilt

$$\|x\| = |N_{K/k}(x)| \text{ für jedes } x \in K.$$

---

[4] Im Fall 1 ist das gerade die Aussage von Bemerkung 2.4.4. (ii). Im Fall 2a folgt dies aus der Tatsache, daß das Haarsche Maß auf $\mathbb{R}$ gerade mit Lebesque-Maß übereinstimmt (dieses ist invariant bei Verschiebungen) und die Multiplikation mit α die Intervall-Längen mit $|\alpha|$ multipliziert.

Im Fall 2b ist das Haarsche Maß gerade das 2-dimensionale Flächenmaß auf $\mathbb{C} = \mathbb{R}^2$ (diese ist verschiebungsinvarinat). Die Multiplikation mit einer komplexen Zahl α ist gerade die Zusammensetzung aus einer Drehung der komplexen Ebene (die das Maß unverändert läßt) und einer Strreckung um den Faktor $|\alpha|$, die das Maß mit dem Faktor $|\alpha|^2 = \|\alpha\|$ multipliziert.

Beweis.Nach 2.3.8 sind ||?|| und $\sqrt[N]{N_{K/k}(?)}$ äquivalente Bewertungen. Es gibt also eine (eindeutig bestimmte) positive reelle Konstante c mit

$$||x|| = |N_{K/k}(x)|^c \text{ für jedes } x \in K.$$

Wir haben zu zeigen, es gilt c = 1. Dazu fixieren wir eine Vektorraum-Basis von K über k, sagen wir

$$K = k\bullet\omega_1 + ... + k\bullet\omega_N.$$

Die Abbildung

$$k^n \longrightarrow K, (x_1, ... , x_N) \longrightarrow \sum_{i=1}^{N} x_i\omega_i ,$$

ist dann ein Isomorphismus der additiven Gruppen von k^n und K und gleichzeitig ein Homöomorphismus, wenn man k^n mit der Topologie des direkten Produktes versieht (vgl. 2.3.6). Insbesondere haben k^n und K dieselben Haarschen Maße.[5]

Sei jetzt b ∈ k. Die Multiplikation mit b auf K entspricht dann der Abbildung

$$k^n \longrightarrow k^n, (x_1, ... , x_N) \longrightarrow (bx_1, ... , bx_N) ,$$

Letztere Abbildung multipliziert das Haarsche Maß mit dem Faktor $|b|^N$.[6] Also gilt

$$||b|| = |b|^N = |b^N| = |N_{K/k}(b)|$$

(weil b im Grundkörper k liegt). Damit ist c = 1.

(Statt des obigen Beweises kann man die Konstante c auch durch direktes Nachrechnen in den Fällen 2a, 2b und 1 bestimmen).
QED.

4.1.3 Fortsetzungsformel für normalisierte Bewertungen (allgemeiner Fall)

Seien k ein bewerteter Körper bezüglich einer normalisierten Bewertung |?| wie in 4.1.1. und

$$K/k$$

eine endliche Körpererweiterung. Dann gilt

$$\prod_{i=1}^{r} ||x||_j = |N_{K/k}(x)| \text{ für jedes } x \in K.$$

Dabei seien $||?||_1, ... , ||?||_r$ die normalisierten Bewertungen zu den Fortsetzungen von |?| auf K.

Beweis. Seien $\overline{k}$ die Vervollständigung von k und

$$K\otimes_k\overline{k} \cong L_1\times...\times L_r$$

die Zerlegung von 2.3.11 bzw. 2.3.12. Dann gilt nach 2.3.11

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

---

[5] Und das Haarsche Maß auf k^n ist gerade des Produktmaß zum Haarschen Maß auf k.
[6] Weil die Multiplikation mit b auf k das Haarsche Maß mit b multipliziert.

und nach 2.3.12 sind die L_i gerade die Vervollständigungen von K bezüglich der Fortsetzungen von |?| auf K. Für die rechte Seite der zu beweisenden Formel erhalten wir

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

Nach 4.1.2 steht rechts das Produkt der $\|x\|_j$.

QED.

4.2 Globale Körper

4.2.1 Definition

Ein globaler Körper k ist entweder eine endliche Erweiterung des Körpers der rationalen Zahlen $\mathbb{Q}$ oder eine endliche separable Erweiterung des Körpers F(t) der rationalen Funktionen über einem endlichen Körper F.

Bemerkungen

(i) Das Hauptaugenmerk unserer Betrachtung liegt auf dem Fall, daß k eine enliche Erweiterung von $\mathbb{Q}$ ist, d.h. auf dem Fall eines Körpers algebraischer Zahlen. oder auch kurz von einem Zahlenkörper Ist k eine endliche separable Erweiterung von F(t) mit F endlich, so spricht man auch von einem Funktionenkörper.

(ii) Die Forderung der Separabilität im Funktionenkörper-Fall kann man weglassen.Nach dem Satz von der separierenden Transzendenzbasis, kann man die Unbestimmte t stets so wählen, das die Erweiterung k über F(t) separabel wird[7]. Siehe zum Beispiel van der Waerden [1], Teil II, §155, Satz von der separablen Erzeugung.

4.2.2 Die Anzahl der Bewertungen mit einem Wert > 1

Seien k ein globaler Körper und $\alpha \in k - \{0\}$. Dann gibt es nur endlich viele paarweise nicht-äquivalente Bewertungen |?| von k mit

$$|\alpha| > 1.$$

Beweis. 1. Fall: $k = \mathbb{Q}$.
Seien

$$\alpha = \pm p_1^{n_1} \cdot \ldots \cdot p_r^{n_r}, \; n_i \in \mathbb{Z}, \tag{1}$$

die Zerlegung von α in paarweise teilerfremde Primzahlpotenzen und p eine Primzahl. Dann ist der p-adische Wert von α genau dann von 1 verschieden,

$$|\alpha|_p = (\tfrac{1}{p})^{v_p(\alpha)} \neq 1,$$

wenn p in der Zerlegung von α echt vorkommt,

$$p \in \{p_1, \ldots, p_r\}.$$

Es gibt also für p nur endliche viele Möglichkeiten. Nach dem Satz von Ostrovskij (2.1.15) gibt es aber bis auf Äquivalenz nur die Bewertungen $|?|_p$ und den Absolutbetrag.
2. Fall: k = F(t), F endlicher Körper.

---

[7] weil endliche Körper F vollkommen sind, d.h. jede endliche Erweiterung von F ist separabel (oder äquivalent, jedes Element von F besitzt eine p-te Wurzel in F, wenn p die Charakteristik von k bezeichnet, siehe van der Waerden [1], Teil I, §45, Aussage II).

Weil k eine positive Charakteristik besitzt, ist jede Bewertung von k nicht-archimedisch (vgl. 2.1.10).

Weil F endlich ist, gibt es für jedes Element aus $x \in F^*$ eine endliche Potenz, welche gleich 1 ist, sagen wir

$$x^n = 1.$$

Für jede Bewertung |?| gilt deshalb $|x|^n = 1$, also

$$|x| = 1 \text{ für } x \in F^*.$$

Mit anderen Worten, jede Bewertung |?| von k ist trivial auf F. Betrachten wir den Wert der Unbestimmten bezüglich einer gegebenen Bewertung. Indem wir bei Bedarf t durch 1/t ersetzen, erreichen wir

$$|t| \leq 1.$$

Für jedes Polynom $f(t) = a_n t^n + a_{n-1} t^{n-1} + \ldots + a_0$ gilt auf Grund der nicht-archimedischen Dreiecksungleichung (2.1.7(i)).

$$|f(t)| \leq \max \{|a_n t^n|, |a_{n-1} t^{n-1}|, \ldots , |a_0|\} \leq 1$$

Mit anderen Worten, |?| ist eine Bewertung über dem Dedekind-Ring F[t] im Sinne von 2.1.14 und damit nach 2.1.14 von der Gestalt

$$|?| = \rho^{v_p(?)}$$

mit einer reellen Zahl $\rho \in (0, 1)$ und einem maximalen Ideal p von F[t]. Wir haben gezeigt:

Die Bewertungen von k sind gerade die p-adischen Bewertungen $|?| = \rho^{v_p(?)}$ mit einem maximalen Ideal p von F[t] oder F[1/t].

Es reicht also zu zeigen,

$$v_p(\alpha) = 0 \text{ für falls alle maximalen Ideale p von F[t] und F[1/t].}$$

Wir können uns dabei auf den Fall beschränken, daß p ein maximales Ideal von F[t] ist. Dazu betrachten wir die Zerlegung (1) von α in paarweise teilerfremde Potenzen von irreduziblen Polynomen p_i von F[t]. Die Bedingung $v_p(\alpha) = 0$ ist nur dann verletzt, wenn das maximale Ideal p von einem der p_i erzeugt wird, also nur für endlich viele p.

3. Fall: k beliebig.
Nach Voraussetzung ist k ein globaler Körper, also eine endliche separable Erweiterung eine Körpers ℓ der Gestalt $\mathbb{Q}$ oder F(t). Im Fall $\ell = \mathbb{Q}$ besitzt ℓ genau eine archimedische Bewertung (nach dem Satz von Ostrovskij 2.1.15) und im Fall $\ell = F(t)$ gibt es überhaupt keine archimedische Bewertung von ℓ (nach dem Satz von Gelfand-Tornheim 2.2.4). Da jede Bewertung nur endlich viele Fortsetzungen auf eine endliche separable Erweiterung besitzt (vgl. 2.3.12) ist die Anzahl der archimedischen Bewertungen von k endlich. Wir können uns deshalb beim Beweis auf die Betrachtung der nicht-archimedischen Bewertungen beschränken.

Weil k endlich ist über ℓ, besteht eine Relation der Gestalt

$$\alpha^n + a_1 \alpha^{n-1} + \ldots + a_n = 0 \text{ mit } a_1, \ldots , a_n \in \ell.$$

Für jede nicht-archimedische Bewertung |?| gilt damit

$$|\alpha|^n = | - a_1 \alpha^{n-1} - \ldots - a_n |$$

$$\leq \max \{ |a_1 \alpha^{n-1}| , \dots , |a_n| \}$$

$$\leq \max \{1, |\alpha|^{n-1}\} \bullet \max \{ |a_1| , \dots , |a_n| \}$$

also[8]

$$|\alpha| \leq \max \{1, |a_1| , \dots , |a_n| \}$$

Auf Grund der ersten beiden Fälle steht auf der rechten Seite nur für endlich viele Bewertungen |?| ein Wert > 1. Also gilt dasselbe auch für die linke Seite.
QED.

Bemerkungen

(i) Wie wir gesehen haben, sind alle Bewertungen eines globalen Körpers der Gestalt k = F(t) mit F endlich, von der Form

$$|?| = \rho^{v_p(?)}$$

mit einem maximalen Ideal p von F[t] oder F[1/t] und einer reellen Zahl

$$\rho \in (0, 1).$$

(ii) Aus dem Beweis ergibt sich weiter, daß mit Ausnahme von endlich vielen archimedischen Bewertungen, alle Bewertungen eines globalen Körpers diskret und nicht-archimedisch sind. Sie genügen also den Bedingungen von 4.1.1., d.h. jede Bewertung eines globalen Körpers äquivalent zu einer normierten Bewertung.

(iii) Sei der globlae Körper k endlich und separabel über ℓ mit $\ell = \mathbb{Q}$ oder $\ell = F(t)$, F endlich. Weiter sei V eine normalisierte Bewertung von ℓ. Für eine Bewertung v von k schreiben wir

$$v \mid V,$$

wenn die Einschränkung von v auf ℓ äquivalent ist zu V.

4.2.3 Das Produkt aller normalisierten Werte

Seien k ein globaler Körper und $\alpha \in k - \{0\}$. Dann gilt

$$|\alpha|_v = 1$$

für fast alle normalisierten Bewertungen $|?|_v$ von k. Man kann also deren Produkt bilden. Dieses ist gleich 1,

$$\prod_v |\alpha|_v = 1.$$

Bemerkung

Später werden wir einen etwas weiniger technischen Beweis als den nachfolgenden angeben.

Beweis. Nach 4.2.2 gilt $|\alpha|_v > 1$ nur für endlich viele v und dasselbe ist richtig für $1/\alpha$. Zusammen ist also $|\alpha|_v = 1$ für fast alle v.

---

[8] Ist $|\alpha| \geq 1$, so ist der erste Faktor rechts gleich $|\alpha|^{n-1}$ und Division durch diesen Faktor liefert die neue Abschätzung. Ist $|\alpha| < 1$, so ist der erste Faktor rechts gleich 1. Wir gehen zu den n-ten Wurzeln über - eine monotone Operation - und erhalten

$$|\alpha| \leq \sqrt[n]{\max \{|a_1|,\dots,|a_n|\}}$$

Ist die Wurzel auf der rechten Seite größer als 1, so Vergrößert man den Wert nur wenn man zur n-ten Potenz übergeht. Ist sie es nicht, so steht auf der linken Seite ein Wert ≤ 1, d.h. die neue Abschätzung besteht ebenfalls.

Sei jetzt k endlich und separabel über ℓ mit $\ell = \mathbb{Q}$ oder $\ell = F(t)$, F endlich. Weiter bezeichne V eine normalisierte Bewertung von ℓ. Für das Produkt übert alle normalisierten Bewertungen v von k gilt dann

$$\prod_v |\alpha|_v = \prod_V \prod_{v|V} |\alpha|_v$$

$$= \prod_V |N_{k/\ell}(\alpha)|_V \qquad \text{nach 4.1.3.}$$

Es reicht also zu zeigen, jeder Faktor auf der rechten Seite ist gleich 1, d.h. wir haben die Behauptung für ℓ anstellen von k zu beweisen. Wir können also annehmen, $k = \mathbb{Q}$ oder $k = F(t)$.

1. Fall: $k = \mathbb{Q}$.

Wir betrachten die Zerlegung

$$\alpha = \pm p_1^{n_1} \cdot \ldots \cdot p_r^{n_r} = \pm \prod_p p^{n_p}, \quad n_i, n_p \in \mathbb{Z},$$

von α in paarweise teilerfremde Primzahlpotenzen. Für die normalisierte Bewertung zur Primzahl p gilt dann

$$|\alpha|_p = p^{-n_p},$$

für das Produkt über alle nicht-archimedischen Bewertunten von $\ell = \mathbb{Q}$ also

$$\prod_p |\alpha|_p = \prod_p p^{-n_p} = \frac{1}{|\alpha|}$$

Durch Multiplikation beider Seiten mit dem archimedischen Wert $|\alpha|$ erhalten wir die Behauptung.

2. Fall: $k = F(t)$.

Wir betrachten die Zerlegung

$$\alpha = p_1^{n_1} \cdot \ldots \cdot p_r^{n_r} = \pm \prod_p p^{n_p}, \quad n_i, n_p \in \mathbb{Z},$$

von α in paarweite teilerfremde Potenzen irreduzibler Polynome $p \in F[t]$. Für die normalisierte Bewertung zum Primpolynom p gilt

$$|\alpha|_p = |p^{n_p}|_p = |p|_p^{n_p} = (\#\, F(t)/(p))^{n_p} = ((\#F)^{\deg p})^{-n_p} = (\#F)^{-n_p \cdot \deg p}$$

Für das Produkt über alle diese Werte erhalten wir

$$\prod_p |\alpha|_p = \prod_p (\#F)^{-n_p \cdot \deg p} = (\#F)^{-\Sigma_p n_p \cdot \deg p} = (\#F)^{-\deg \Pi_p p^{n_p}} = (\#F)^{-\deg \alpha} \qquad (1)$$

Der Körper $k = F(t)$ besitzt noch eine weitere Bewertung, nämlich die zum Primpolynom

$$p_\infty = 1/t \in F[1/t]$$

(vgl. 2.1.16). Zum Beweis der Behauptung reicht es zu zeigen, daß für den zugehörigen Wert

$$|\alpha|_\infty = (\#F)^{\deg \alpha} \qquad (2)$$

gilt, denn dann ergibt sich die zu beweisenden Identität aus (1) durch Multiplikation mit (2).

Zum Beweis von (2) können wir annehmen, daß α ein Polynom von F[t] ist, sagen wir

$$\alpha = a_d t^d + ... + a_0 \text{ , } d = \deg \alpha, a_i \in F, a_d \neq 0.$$

d.h.

$$\alpha = (1/t)^{-d} (a_d + a_{d-1}\frac{1}{t} + ... + a_0(\frac{1}{t})^n).$$

Der zweite Faktor rechts ist in F[1/t] teilerfremd zu 1/t. Es gilt also

$$|\alpha|_\infty = |(1/t)^{-d}|_\infty = |(\#F)|^d = |(\#F)|^{\deg \alpha}.$$

Also gilt (2), und damit die Behauptung.
QED.

4.2.4 Ein Vergleich von Bewertungsringen

Seien k ein globaler Körper und K/k eine endliche separable Erweiterung. Für jede normalisierte Bewertung v von k Betrachten wir die Zerlegung (vgl. 2.3.12)

$$k_v \otimes_k K = K_1 \oplus ... \oplus K_J.$$

Dabei bezeichne k_v die Vervollständigung von k bezüglich v und $K_1,...,K_J$ seien die Vervollständigungen von K bezüglich der Fortsetzungen $V_1,...,V_J$ von v auf K. Man beachte, die Zahl J = J(v) kann von v abhängen.
Weiter sei

$$\omega_1, ... , \omega_N$$

eine Vektorraumbasis von K über k. Dann besteht für fast jedes v die Identität

$$\omega_1 \mathcal{O}_{k_v} + ... + \omega_N \mathcal{O}_{k_v} = \mathcal{O}_{K_1} \oplus ... \oplus \mathcal{O}_{K_J}. \qquad (1)$$

Dabei bezeichne

$$\mathcal{O}_{k_v}$$

den Bewertungsring von k_v bezüglich der Bewertung v und

$$\mathcal{O}_{K_j}$$

den Bewertungsring von K_j bezüglich der Bewertung V_j.

Bemerkung
Nach Bemerkung 4.2.2 (ii) besitzt ein globaler Körper nur endlich viele archimedische Bewertungen. Bei der obigen Aussage können wir also annehmen, daß v eine nicht-archimedische Bewertung ist. Nur in diesem Fall ist $\mathcal{O}_k$ definiert und die Behauptung der Gleichheit in (1) eine sinnvolle Aussage.
Beweis. Wie gerade angemerkt können wir auf den Fall beschränken, daß v eine nicht-archimedische Bewertung ist.

1. Schritt. Beweis von "$\subseteq$" für fast alle v.

Weil die Körper-Erweiterung K/k endlich und separabel ist, ist mit k auch K ein globaler Körper. Für fast alle Bewertungen V von K gilt deshalb

$$|\omega_j|_V \leq 1 \text{ für } j = 1, ... , N.$$

Schließt man die endlich vielen Bewertungen von K aus, für die das nicht gilt, und deren Einschränkungen auf k, so sieht man, daß für fast alle Bewertungen v von k und deren Fortsetzungen $V_1,...,V_J$ von v auf K gilt

$$|\omega_j|_{V_i} \leq 1 \text{ für } j = 1, ... , N, i = 1, ... , J.$$

Bezeichnen wir die Fortsetzung von V_i auf die Vervollständigung K_i ebenfalls mit V_i, gilt für jedes Element

$$x = \omega_1 x_1 + ... + \omega_N x_N \qquad (x_1, ... , x_N \in \mathcal{O}_k \subseteq k \subseteq k_v \subseteq K_i)$$

der linken Seite von (1) auf Grund der nicht-archimedischen Dreiecksungleichung 2.1.7(i):

$$|x|_{V_i} \leq 1 \text{ für } i = 1, ... , N.$$

Mit anderen Worten, die linke Seite von (1) ist in der rechten Seite enthalten.

2. Schritt: Beweis von "$\supseteq$" für fast alle v.

Betrachten wir die Diskriminante

$$D(\gamma_1, ... , \gamma_N) = \det (Tr_{K/k}(\gamma_i\gamma_j))_{i,j=1,...,N}$$

für

$$\gamma_1, ... , \gamma_N \in k_v \otimes_k K = K_1 \oplus ... \oplus K_J.$$

Liegen die γ_i in K und in der rechten Seite von (1), d.h. gilt $|\gamma_i|_{V_\ell} \leq 1$ für alle i und alle ℓ. Nach der Spur-Formel von 2.3.1 gilt

$$Tr_{K/k}(\gamma_i\gamma_j) = \sum_{\ell=1}^{J} Tr_{K_\ell/k_v}(\gamma_i\gamma_j)$$

Wegen $|\gamma_i|_{V_\ell} \leq 1$ liegt γ_i in $\mathcal{O}_{K_\ell}$ für alle i. Die Produkte $\gamma_i\gamma_j$ liegen also auch in den $\mathcal{O}_{K_\ell}$ sind also ganz[9] über $\mathcal{O}_{k_v}$. Damit sind die Spuren rechts als Summen ganzer Element ganz über $\mathcal{O}_{k_v}$ und Elemente von k_v. Die Summe rechts liegt damit in $\mathcal{O}_{k_v}$, d.h.

$$Tr_{K/k}(\gamma_i\gamma_j) \in \mathcal{O}_{k_v} \text{ für } \gamma_1, ... , \gamma_N \text{ in der rechten Seite von (1) und in K.} \qquad (2)$$

Sei jetzt α in der rechten Seite von (1). Dann gilt erst recht

$$\alpha \in K_1 \oplus ... \oplus K_J = k_v \otimes_k K = k_v\omega_1 + ... + k_v\omega_N$$

Wir können $\alpha \in K$ in der Gestalt

$$\alpha = \sum_{i=1}^{N} a_i\omega_i \text{ mit } a_i \in k_v$$

schreiben. Für i = 1, ... , N gilt

$$D(\omega_1, ..., \omega_{i-1}, \alpha, \omega_{i+1}, ... , \omega_N) =^{10} a_i^2 \cdot D(\omega_1, ... , \omega_N).$$

---

[9] $\mathcal{O}_{K_\ell}$ ist die ganze Abschließung von $\mathcal{O}_{k_v}$ im vollständigen Körper K_ℓ.

[10] Sei

$$D(\gamma_1, ... , \gamma_N; \delta_1, ... , \delta_N) = \det (Tr_{K/k}(\gamma_i\delta_j))_{i,j=1,...,N}$$

Diese Funktion ist k-linear in jedem ihrer Argumennt und schiefsymmetrisch in den γ und in den δ. Insbesondere ist diese Funktion gleich Null, wenn zwei der γ oder zwei der δ übereinstimmen. Weiter sei

$$D(x, y) := D(\omega_1, ... ,x,..., \omega_N; \omega_1, ... ,y,..., \omega_N).$$

Für fast alle v liegen die $\omega_j \in K$ in der rechten Seite von (1). Wegen (2) liegt dann die linke Seite der letzten Identität in $\mathcal{O}_{k_v}$, d.h. für fast alle v gilt

$$a_i^2 d \in \mathcal{O}_{k_v} \quad (i = 1, \ldots, N)$$

mit

$$d = D(\omega_1, \ldots, \omega_N) \in k.$$

Weil die Erweiterung K/k separabel ist, ist die Bilinarform $Tr_{K/k}(xy)$ nicht entartet, d.h. die Determinante d dieser Form ist ungleich Null,

$$d \neq 0.$$

Für fast alle v ist damit aber d eine Einheit, d.h. es gilt

$$a_i^2 \in \mathcal{O}_{k_v} \text{ für jedes i.}$$

Dann ist aber auch[11]

$$a_i \in \mathcal{O}_{k_v} \text{ für jedes i,}$$

d.h. α liegt in der linken Seite von (1). Wir haben damit gezeigt, für fast alle v gilt

$$\omega_1 \mathcal{O}_{k_v} + \ldots + \omega_N \mathcal{O}_{k_v} \supseteq \mathcal{O}_{K_1} \oplus \ldots \oplus \mathcal{O}_{K_J} \bigcap K.$$

Nach dem schwachen Approximationssatz 2.3.4 liegt K dicht in $K_1 \oplus \ldots \oplus K_J$. Weil die hier auftretenden Bewertungen diskret sind, liegt auch der Durchschnitt auf der rechten Seite dicht in $\mathcal{O}_{K_1} \oplus \ldots \oplus \mathcal{O}_{K_J}$.[12]

Eine dichte Teilmenge der rechten Seite also in der linken Seite von (1). Die linke Seite ist aber ein direktes Produkt von kompakten Mengen (vgl. 2.4.1), also kompakt, also abgeschlossen. Also liegt die gesamte linke Seite in der rechten.
QED.

4.2.5 Unverzweigtheit an fast allen Stellen

Seien k ein globaler Körper und K/k eine endliche separable Erweiterung. Dann ist für fast jede Bewertung v von k unverzweigt in K.
Beweis. Seien

Diese Funktion ist Null für $x = \omega_u$ oder $y = \omega_u$ mit $u \neq i$.

Die linke Seite der zu beweisenden Identität ist gerade

$$D(\alpha,\alpha) = \sum_{u=1}^{N} \sum_{v=1}^{N} a_u a_v D(\omega_u, \omega_v) = a_i^2 D(\omega_i, \omega_i).$$

Dies ist gerade die linke Seite der zu beweisenden Identität.

[11] Weil der Wert des Quadrats gleich dem Quadrat des Werts ist.

[12] Jedes Element von $K_1 \oplus \ldots \oplus K_J$ läßt sich durch eine Folge aus K approximieren. Das gilt erst recht für jedes Element aus $\mathcal{O}_{K_1} \oplus \ldots \oplus \mathcal{O}_{K_J}$. Der Limes der zugehörigen Werte (bezüglichj der J Bewertungen) geht dann gegen eine reelle Zahl ≤ 1. Das die Bewertungen diskret sind, sind die Werte selbst schon von einer gewissen Stelle an ≤ 1, d.h. die Folge liegt von einer gewissen Stelle an in $\mathcal{O}_K$ und damit in jedem $\mathcal{O}_{K_\ell}$

k_v

die Vervolltändigung von k bezüglich der Bewertung v, die wir OBdA als normalisiert annehmen können,

$V_1, \dots, V_r$

die normalisierten Bewertungen von K, welche äquivalent zu einer Fortsetzeung von v sind, und

K_{V_i}

die Vervollständigung von K bezüglich der Bewertung V_i. Weiter bezeichne

$\mathcal{O}_{k_v}$

den Bewertungsring des bewerteten Körpers k_v und

$\mathcal{O}_{V_i}$

den Bewertungsring des bewerteten Körpers K_{V_i}. Dann gilt

v ist unverzweigt in K

$\Leftrightarrow$ K_{V_i}/k_v ist unverzweigt für i = 1, ... r

$\Leftrightarrow$ Für die Diskriminanten gilt $\delta(K_{V_i}/k_v) = \mathcal{O}_{k_v}$ (vgl. 3.3.14)

$\Leftrightarrow$ Es gibt für jedes $\ell = 1, \dots, r$ ein freies Erzeuggendensystem

$\gamma_1^{(\ell)}, \dots, \gamma_n^{(\ell)}$ von $\mathcal{O}_{V_i}$ über $\mathcal{O}_{k_v}$ mit

$D(\gamma_1^{(\ell)}, \dots, \gamma_n^{(\ell)}) = \det(\mathrm{Tr}(\gamma_i^{(\ell)}\gamma_j^{(\ell)}) \in \mathcal{O}_{k_v}^*$

(vgl. 1.6.13 (iii)).

Man beachte, die Determinante $D(\gamma_1^{(\ell)}, \dots, \gamma_n^{(\ell)})$ ist gerade die Determinante der Bilinearform

$$\mathrm{Tr}_i: K_{V_i} \times K_{V_i} \longrightarrow k_v, (x,y) \mapsto xy,$$

welche jedem Paar x, y von Elementen aus K_{V_i} die Spur der Multiplikation mit xy zuordnet. In analoger Weise könne wir die Spur

$$\mathrm{Tr}: (K_{V_1} \times \dots \times K_{V_r}) \times (K_{V_1} \times \dots \times K_{V_r}) \longrightarrow k_v,$$

betrachten, welche je zwei Elementen aus $K_{V_1} \times \dots \times K_{V_r}$ die Spur der Multiplikation mit deren Produkt zuordnet. Indem wir geeignete k_v-Vektorraum-Basen

$$\gamma_1^{(\ell)}, \dots, \gamma_n^{(\ell)} \in K_{V_i}$$

der K_{V_i} fixieren und jede bilineare Abbildung mit deren Matrix identifizieren, erhalten wir[13]

$$Tr = \begin{pmatrix} Tr_1 \dots 0 \\ \dots \dots \dots \\ 0 \dots Tr_r \end{pmatrix}$$

Für die Determinante der Matrix der Bilinearform Tr erhält man

$$\det(Tr(\gamma_i\gamma_j)_{i,j=1,\dots,N} = \prod_{\ell=1}^{r} \det(Tr_\ell(\gamma_i^\ell\gamma_j^\ell))_{i,j=1,\dots,n} = \prod_{\ell=1}^{r} D(\gamma_1^\ell, \dots, \gamma_n^\ell)$$

Dabei seien $\gamma_1,\dots,\gamma_N$ gerade die in geeigneter Weise aufgelisteten γ_i^ℓ.

Zusammen mit 4.2.4 erhalten wir:

v ist unverzweigt in K

$\Leftrightarrow$ Es Elemente $\gamma_1,\dots,\gamma_N \in \omega_1\mathcal{O}_{k_v} + \dots + \omega_N\mathcal{O}_{k_v}$ derart, daß

$$D(\gamma_1, \dots, \gamma_N) = \det(Tr(\gamma_i\gamma_j))$$

eine Einheit in $\mathcal{O}_{k_v}$ ist.

Dabei ist $D(\gamma_1, \dots, \gamma_N)$ die Determinante der k_v-Bilinearform

$$(k_v \otimes_k K) \times (k_v \otimes_k K) \longrightarrow k_v,\ (x, y) \mapsto Tr(xy),$$

welche je zwei Elemente $x, y \in k_v \otimes_k K$ abbildet auf die Spur der Multiplikation mit xy. Diese Bilinearform entsteht durch k_v-lineare Fortsetzung der k-Bilinearform

$$Tr: K \times K \longrightarrow k,\ (x, y) \mapsto Tr(xy).$$

Erstere hat also dieselbe Matrix wie letztere (bezüglich einer k-Vektorraum-Basis von K). Von letzterer wissen wir aber, daß sie nicht entartet ist (weil K/k separabel ist). Die Determinante ist somit ungleich Null. Für fast alle Bewertungen v können wir

$$\gamma_i = \omega_i \ (i = 1, \dots, N)$$

setzen. Für fast alle v ist, wie wir in 4.2.4 gesehen haben,

$$|D(\omega_1, \dots, \omega_N)| = 1,$$

d.h. v ist für fast alle v unverzweigt in K.

QED.

4.3 Eingeschränkte topologische Produkte

Wir beschreiben jetzt einen topologischen Kalkül, den wir später brauchen.

---

[13] Weil Addition und Multiplikation in $K_{V_1} \times \dots \times K_{V_r}$ koordinatenweise definiert sind, sind die Matrizen für die Mutliplikation mit Elementen aus $K_{V_1} \times \dots \times K_{V_r}$ Blockmatrizen, wobei die Einträge außerhalb der Hauptdiagonalen Null-Matrizen sind. Durch Übergang zur Spur erhält man wieder Block-Matrizen dieserr Art.

4.3.1 Die Situation

Seien

$$\{\Omega_\lambda\}_{\lambda\in\Lambda}$$

eine Familie von topologischen Räumen und

$$\{\Theta_\lambda\}_{\lambda\in\Lambda'},$$

eine Familie von offenen Teilmengen $\Theta_\lambda \subseteq \Omega_\lambda$, wobei die Index-Menge Λ' eine Teilmenge von Λ mit endlichem Komplement $\Lambda - \Lambda'$ sei. Weiter sei Ω die Menge

$$\Omega := \{ (\alpha_\lambda)_{\lambda\in\Lambda} \mid \alpha_\lambda\in\Omega_\lambda \text{ für jedes } \lambda \text{ und } \alpha_\lambda\in\Theta_\lambda \text{ für fast jedes } \lambda\}.$$

Wir führen in Ω eine Topologie ein, indem wir als Topologie-Basis alle Produkte der Gestalt

$$\prod_{\lambda\in\Lambda} \Gamma_\lambda$$

verwenden, wobei Γ_λ offen in Ω_λ für jedes λ und gleich Θ_λ für fast jedes λ sei. Die Menge Ω zusammen mit dieser Topologie heißt <u>eingeschränktes topologisches Produkt</u> der Ω_λ bezüglich der Θ_λ.

Beispiel

Λ die Menge der normalisierten Bewertungen eines globalen Körpers k

$\Omega_\lambda := k_\lambda$ die Vervollständigung von k bezüglich der Bewertung $\lambda\in\Lambda$

$\Lambda' \subseteq \Lambda$ die Teilmenge der nicht-archimedischen Bewertungen von k

$\Theta_\lambda := \mathcal{O}_{k_\lambda}$ der Bewertungsring von k_λ

4.3.2 Eine Familie von offenen Teilmengen von Ω

Sei in der Situation von 4.3.1 eine endliche Teilmenge $S \subseteq \Lambda$ gegeben mit Λ-$\Lambda' \subseteq S$ und bezeichne

$$\Omega_S \cong \prod_{\lambda\in S} \Omega_\lambda \prod_{\lambda\in\Lambda-S} \Theta_\lambda$$

die Menge aller Elemente $(\alpha_\lambda)_{\lambda\in\Lambda} \in \Omega$ mit

$$\alpha_\lambda \in \Theta_\lambda \text{ für } \lambda\notin S.$$

Dann ist Ω_S offen in Ω, und die Unterraum-Topologie von Ω_S in Ω ist gerade die Produkt-Topologie.

Bemerkung

Jede Menge der definierenden Topologie-Basis von Ω ist offen in einer der Mengen Ω_S

Beweis. Die Mengen Ω_S gehören zur Topologie-Basis, welche die Topologie von Ω definiert. Sie sind also insbesondere offen in Ω.

Weiter bilden die Mengen der Gestalt

$$\prod_{\lambda\in\Lambda} \Gamma_\lambda$$

mit Γ_λ offen im λ-ten Faktor von Ω_S für alle λ und Γ_λ gleich diesem Faktor für fast alle λ eine Topologie-Basis für die Produkt-Topologie von Ω_S und es sind gerade die Mengen, die man aus der Topologie-Basis von Ω durch Schneiden mit Ω_S erhält. Also stimmt die Unterraum-Topologie mit der Produkt-Topologie überein.
QED.

4.3.3 Abhängigkeit der Topologie von den Θ_λ

Sei in der Situation von 4.3.1 für fast jedes $\lambda\in\Lambda$ eine offene Teilmenge

$$\Theta'_\lambda \subseteq \Omega_\lambda$$

von Ω_λ gegeben, wobei für fast jedes λ

$$\Theta_\lambda = \Theta'_\lambda$$

gelte. Dann stimmt das eingeschränkte topologische Produkt der Ω_λ bezüglich der Θ_λ mit dem der Ω_λ bezüglich der Θ'_λ überein.

Beweis. In beiden Fällen sind die zugehörigen Mengen Ω dieselben und die definierenden Topologie-Basis stimmen überein.
QED.

4.3.4 Kriterium für lokale Kompaktheit

In der Situation von 4.3.1 seien die Räume Ω_λ lokal kompakt und die Unterräume Θ_λ kompakt. Dann ist das eingeschränkte topologische Produkt Ω der Ω_λ bezüglich der Θ_λ lokal kompakt.

Beweis. Mit den Bezeichnungen von 4.3.2 gilt

$$\Omega = \bigcup_S \Omega_S$$

wenn S die endlichen Teilmengen von Λ mit Λ-$\Lambda' \subseteq S$ durchläuft. Es reicht also, die lokale Kompaktheit der Mengen

$$\Omega_S \cong \prod_{\lambda\in S} \Omega_\lambda \prod_{\lambda\in\Lambda-S} \Theta_\lambda$$

zu beweisen. Da S endlich ist, kommen in der Faktor-Zerlegung nur endlich viele Faktoren vor, die eventuell nicht kompakt sind, vor. Alle Faktoren sind aber lokal kompakt. Die Ω_S sind also lokal kompakt.

QED.

4.3.5 Ein Maß auf dem eingeschränkten topologischen Produkt

In der Situation von 4.3.1 sei für jedes $\lambda\in\Lambda$ ein Maß μ_λ auf dem Raum Ω_λ gegeben, wobei

$$\mu_\lambda(\Theta_\lambda) = 1$$

gelte für jedes $\lambda\in\Lambda$'. Das Produkt-Maß auf Ω sei nach Definition das Maß, für welches eine Basis meßbarer Mengen[14] die Mengen der folgeneden Gestalt seien.

$$\prod_{\lambda\in\Lambda} M_\lambda$$

mit M_λ meßbar in Ω_λ von endlichem Maß für alle $\lambda\in\Lambda$ und $M_\lambda = \Theta_\lambda$ für fast alle λ. Dabei gelte für diese Mengen

$$\mu\Big(\prod_{\lambda\in\Lambda} M_\lambda\Big) = \prod_{\lambda\in\Lambda} \mu_\lambda(M_\lambda).$$

4.3.6 Das Maß auf den Teilmengen Ω_S

Die Einschränkung des in 4.3.5 definierten Maßes auf eine der Mengen Ω_S von 4.3.2 ist gerade das Produkt-Maß der μ_λ.

Beweis. Das ergibt sich aus der Definition des Produkt-Maßes.
QED.

4.4 Der Adele-Ring

4.4.1 Definition

Sei k ein globaler Körper. Für jede normalisierte Bewertung v von k bezeichnen wir mit k_v die Vervollständigung von k bezüglich dieser Bewertung und, falls v nicht-archimedisch ist, mit $\mathfrak{O}_v$ den zugehörigen Bewertungsring von k_v. Der Adele-Ring

$$V_k$$

von k ist dann definiert als das eingeschränkte topologische Produkt der k_v bezüglich der $\mathfrak{O}_v$. Addition und Multiplikation im Adele-Ring seien dabei koordinatenweise definiert.

$$(\alpha_v) + (\beta_v) := (\alpha_v + \beta_v)$$
$$(\alpha_v) \cdot (\beta_v) := (\alpha_v \cdot \beta_v)$$

Bemerkungen

(i) Die angegebenen Operationen sind korrekt, d.h. für je zwei Elemente

$$\alpha = (\alpha_v) \text{ und } \beta = (\beta_v)$$

aus V_k sind $\alpha+\beta$ und $\alpha\beta$ Elemente von V_k.[15]

(ii) Die durch Addition und Multiplikation definierten Abbildungen

$$V_k \times V_k \longrightarrow V_k,\ (\alpha, \beta) \mapsto \alpha+\beta,$$
$$V_k \times V_k \longrightarrow V_k,\ (\alpha, \beta) \mapsto \alpha\cdot\beta,$$

---

[14] d.h. die meßbaren Mengen seien die von diesen Mengen erzeugte σ-Algebra.
[15] Fast alle Komponenten von $\alpha+\beta$ und $\alpha\beta$ liegen in $\mathfrak{O}_v$ für fast alle v.

sind stetig, d.h. V_k ist mit diesen Operationen ein topologischer Ring.[16]

(iii) Der Ring V_k ist lokal kompakt, denn die Körper k_v sind lokal kompakt und die Ringe $\mathcal{O}_v$ sind kompakt (vgl. 4.3.4).

(iv) Die Diagonal-Einbettung

$$k \longrightarrow V_k,\ c \mapsto (c)_v\ ,$$

welche jedem Element c von k das Adel zuordnet dessen sämtliche Komponenten gleich c sind, ist wohl definiert[17] und ein injektiver Homomorphismus von Ringen mit 1. Die Elemente dieses Bildes heißen Haupt-Adele. Wir werden im folgenden meist k mit seinem Bild in V_k identifizieren und k als Teilkörper von V_k auffassen.

4.4.2 Verhalten bei endlichen separablen Körper-Erweiterungen

Sei K/k eine endliche separable Erweiterung des globalen Körpers k. Dann besteht ein (topologischer und algebraischer) natürlicher Isomorphismus

$$V_k \otimes_k K \xrightarrow{\cong} V_K. \qquad (1)$$

Die Diagonaleinbettung $k \hookrightarrow V_k$ induziert dabei eine Inklusion

$$K = k \otimes_k K \hookrightarrow V_k \otimes_k K \xrightarrow{\cong} V_K\ ,$$

welche gerade mit der Diagonaleinbettung von K in V_K zusammenfällt.

Beweis. Wir fixieren eine k-Vektorraumbasis von K, sagen wir

$$K = k\bullet\omega_1 + \ldots + k\bullet\omega_N \text{ mit } N := [K:k]$$

und verwenden diese zur Beschreibung der Abbildung (1). Wir identifizieren die ω_j mit ihren natürlichen Bildern

$$1 \otimes \omega_j \in V_k \otimes_k K$$

in $V_k \otimes_k K$, welche ein über dem Ring V_k linear unabhängiges Erzeugendensystem des Definitionsbereichs von (1) bilden. Dessen Elemente lassen sich also in der Gestalt

$$\alpha := (\alpha_v^1)\bullet\omega_1 + \ldots + (\alpha_v^N)\bullet\omega_N$$

schreiben mit eindeutig bestimmten Adelen $(\alpha_v^j) \in V_k$. Für fast alle v sind die α_v^j ganz, d.h. sie liegen im Ring $\mathcal{O}_v$ der ganzen Zahlen von k_v. Für jede über v liegende normalisierte Bewertung V von K ist das Element

$$\alpha_v^1\bullet\omega_1 + \ldots + \alpha_v^N\bullet\omega_N \in K_V \qquad (2)$$

wohldefiniert,

$$\alpha_v^j \in k_v \subseteq K_V\ ,\ \omega_j \in K \subseteq K_V\ ,$$

---

[16] Es reicht zu zeigen, durch Einschränken dieser Abbildungen auf die Mengen der Gestatl Ω_S erhält man stetige Abbildungen. Weil die Topologie der Ω_S gerade die Produkt-Topologie ist, reicht es, die Stetigkeit koordinatenweise zu beweisen. Die koordinatenweise Topologie besteht aber, weil die k_v topologische Ringe sind für jedes v.

[17] Weil der Wert von c für fast alle normalisierten Bewertungen gleich 1 ist.

und für fast alle V (und v) gilt

$$\alpha_v^j \in \mathcal{O}_v \subseteq \mathcal{O}_V \,,\ \omega_j \in \mathcal{O}_K \subseteq \mathcal{O}_V \,,$$

d.h. für fast alle V ist das Element (2) ganz. Die Elemente (2) bilden somit die Koordinaten eines Adels aus V_K, welches wir als das Bild von α bei der Abbildung (1) defininieren. Nach Konstruktion ist diese Abbildung V_k-linear.

Betrachten wir für festes v den Isomorphismus

$$k_v \otimes_k K \xrightarrow{\cong} K_{V_1} \times \ldots \times K_{V_r} \tag{3}$$

von 2.3.12, wobei $V_1, \ldots, V_r$ die über v liegenden normalisierten Bewertungen seien. Das Element (2) ist dann gerade die V-te Koordinate des Bildes von

$$\alpha_v^1 \bullet 1 \otimes \omega_1 + \ldots + \alpha_v^N \bullet 1 \otimes \omega_N \in k_v \otimes_k K$$

beim Isomorphismus (3). Insbesondere ist die eben definierte Abbildung (1) unabhängig von der Wahl der ω_j. Außerdem ist sie injektiv und koordinatenweise ein Homomorphismus von Ringen mit 1, also selbst ein injektiver Homomorphismus von Ringen mit 1.[18] Wie wir oben gesehen haben, induziert (3) für fast alle v eine Bijektion

$$\mathcal{O}_v \bullet \omega_1 + \ldots + \mathcal{O}_v \bullet \omega_N \xrightarrow{\cong} \mathcal{O}_{V_1} \times \ldots \times \mathcal{O}_{V_r} \tag{4}$$

(vgl. 4.2.4). Die Koordinaten eines vorgegebenen Adeles aus V_K zu Koordinaten über v definieren also für fast alle v ein Element der rechten Seite von (4) und damit auch ein Element der linken Seite. Das bedeutet aber, jedes Element von V_K liegt im Bild der Abbildung (1).

Wir haben gezeigt, Abbildung (1) ist ein Isomorphismus von Ringen mit 1. Zu zeigen ist noch, daß es sich um einen Homöomorphismus handelt.

Dazu vergleichen wir die Topologien der beiden Räume auf der linken und rechten Seite von (1). Der Raum auf der linken Seite ist als topologischer Raum ein direktes Produkt von N Exemplaren von V_k. Als Topologie-Basis können wir die N-fachen direkten Produkte von offenen Mengen aus V_k verwenden,

$$U_1 \times \ldots \times U_N \text{ mit } U_i \text{ offen in } V_k$$

Statt die Offeneheit der U_i in V_k können wir auch fordern. daß sie der definierenen Topologie-Basis von V_k angehören.[19] Indem wir Koordinaten zum selben v in diesen Produkten zusammenfassen, sehen wir, daß $V_k \otimes_k K$ gerade das eingeschränkte topologische Produkt der

$$k_v \otimes_k K = k_v \omega_1 + \ldots + k_v \omega_N$$

ist bezüglich der Teilmengen

$$\mathcal{O}_v \omega_1 + \ldots + \mathcal{O}_v \omega_N$$

---

[18] Auf Grund der koordinatenweisen Definition der Multiplikation des Adele-Rings.

[19] d.h. für jedes U_i gibt es eine endliche Menge S_i von Indizes, sodaß U_i aus allen Elementen von V_k besteht, für welche die λ-te Koordinate für jedes $\lambda \in S_i$ in einer vorgegebenen offenen Menge liegt und die übrigen Koordinaten beliebig (und fast alle ganz) sind.

Weil für fast alle v die Isomorphie (4) besteht, ist dies aber gerade das eingeschränkte topologische Produkt der K_V bezüglich der $\mathcal{O}_V$, also V_K.

QED.

4.4.3 Vergleich der additiven Gruppen des Adele-Rings

Sei K/k eine endliche separable Erweiterung des globalen Körpers k. Außerdem bezeichne

$$V_k^+ \text{ und } V_K^+$$

die additive Gruppe des Adele-Rings von k bzw. K. Dann ist

$$V_K^+ \cong V_k^+ \oplus ... \oplus V_k^+$$

isomorph zur direkten Summen von N := [K:k] Exemplaren von V_k^+. Bei diesem Isomorphismus entspricht die additive Gruppe

$$K^+ \subseteq V_K^+$$

der Hauptadele gerade der direkten Summe $k^+ \oplus ... \oplus k^+$ auf der rechten Seite.

Beweis. Ergibt sich aus dem Beweis von 4.4.2. Alternativ: für $\omega \in K - \{0\}$ ist die Untergruppe

$$\omega \bullet V_k^+ \subseteq V_K^+$$

isomorph zu V_k^+ (im topologischen und algebraischen Sinne)[20]. Damit ist aber

$$V_K^+ = V_k^+ \otimes_k K = \omega_1 V_k^+ + ... + \omega_N V_k^+ \cong V_k^+ \oplus ... \oplus V_k^+.$$

QED.

4.4.4 Die Topologie der Adele-Klassen

Sei k ein globaler Körper. Dann liegt der Ring der Hauptadele

$$k \subset V_k$$

diskret im Ring V_k der Adele. Außerdem ist ein die Faktor-Gruppe

$$V_k^+/k^+$$

kompakt.

Beweis. Nach Voraussetzung ist k endliche separable Körper-Erweiterung eines Teilkörpers

$$\ell \subseteq k$$

mit $\ell = \mathbb{Q}$ oder $\ell = F(t)$ mit F endlich. Nach 4.4.3 gilt

$$V_k^+ \cong V_\ell^+ \oplus ... \oplus V_\ell^+$$

wobei den Hauptiadelen die direkte Summe $\ell^+ \oplus ... \oplus \ell^+$. Insbesondere ist

$$V_k^+/k^+ = V_\ell^+/\ell^+ \oplus ... \oplus V_\ell^+/\ell^+.$$

Es reicht deshalb, die Behauptung für den Speziealfall

$$k = \ell$$

zu beweisen. Wir beschränken uns hier auf den Zahlenkörperfall

---

[20] Man erhält die Elemente von $\omega \bullet V_k^+$, indem man alle Koordinaten der Elemente von V_k^+ mit ω multipliziert.

$$k = \ell = \mathbb{Q}.$$

Der Funktionenkörperfall wird so ähnlich behandelt.

Wir haben zu zeigen, $\mathbb{Q}^+$ liegt diskret in $V_{\mathbb{Q}}^+$. Weil $\mathbb{Q}^+$ eine Untergruppe von $V_{\mathbb{Q}}^+$ ist, reicht es zu zeigen, es gibt in $V_{\mathbb{Q}}^+$ eine offene Umgebung U der Null,

$$0 \in U \subseteq V_{\mathbb{Q}}^+ ,$$

welche mit $\mathbb{Q}$ nur die Null gemeinsam hat. Sei

$$U := \{ (\alpha_v) \in V_{\mathbb{Q}}^+ \mid |\alpha_\infty|_\infty < 1 \text{ und } |\alpha_p|_p \leq 1 \text{ für jede Primzahl } p\}.$$

Dabei bezeichne $|?|_\infty$ den gewöhnlichen Absolutbetrag und $|?|_p$ die (normalisierte) p-adische Bewertung. Sei

$$b \in \mathbb{Q} \bigcap U.$$

Wir haben zu zeigen, b = 0. Angenommen b ist von Null verschieden. Sei

$$b = \prod_p p^{e(p)}$$

die Zerlegung von b in (endlich viele und paarweise teilfremde) Primzahlpotenzen. Wegen $b \in U$ gilt

$$1 \geq |\beta|_p = |p^{e(p)}|_p = (1/p)^{e(p)}$$

also $e(p) \geq 0$ für jedes p (und = 0 für fast jedes p). Insbesondere ist b eine ganze Zahl,

$$b \in \mathbb{Z}.$$

Außerdem ist aber wegen $b \in U$ der Absolutbetrag von b kleiner als 1. Also gilt

$$b = 0.$$

Wir haben noch zu zeigen, $V_{\mathbb{Q}}^+/\mathbb{Q}^+$ ist kompakt. Dazu betrachten wir die Menge

$$W := := \{ (\alpha_v) \in V_{\mathbb{Q}}^+ \mid |\alpha_\infty|_\infty \leq 1/2 \text{ und } |\alpha_p|_p \leq 1 \text{ für jede Primzahl } p\}.$$

Diese Menge ist gerade das topologische Produkt des kompakten Intervalls

$$\{\alpha_\infty \in \mathbb{R} \mid |\alpha_\infty|_\infty \leq 1/2 \}$$

mit den kompakten Mengen $\mathcal{O}_{\mathbb{Q}_p}$, d.h. W ist kompakt. Es reicht also zu zeigen, die Einschränkung der natürlichen Abbildung

$$V_{\mathbb{Q}}^+ \longrightarrow V_{\mathbb{Q}}^+/\mathbb{Q}^+$$

auf W ist surjektiv, denn dann ist $V_{\mathbb{Q}}^+/\mathbb{Q}^+$ als stetiges Bild einer kompakten Menge kompakt. Es reicht also, die folgende Aussage zu beweisen.

Jedes $\beta \in V_{\mathbb{Q}}^+$ hat die Gestalt $\beta = b + \alpha$ mit $b \in \mathbb{Q}$ und $\alpha \in W$. (1).

Für jede Primzahl p ist die p-te Komponente $\beta_p \in \mathbb{Q}_p$ von β eine Laurent-Reihe in p, sagen wir

$$\beta_p = \sum_{n=-n(p)}^{\infty} a_n(p) \cdot p^n \text{ mit } a_n(p) \in \{0, 1, \dots , p-1\} \text{ und } n(p) \geq 0.$$

Den gebrochenen Anteil der Laurent-Reihe können wir in der Gestalt

$$r_p := \sum_{n=-n(p)}^{-1} a_n(p) \bullet p^n = z_p / p^{n(p)} \text{ mit } z_p \in \mathbb{Z}$$

schreiben. Für den ganzen Anteil erhalten wir

$$| \beta_p - r_p |_p \leq 1.$$

Da β ein Adel ist, d.h. β_p ist für fast alle p selbst schon ganz, können wir außerdem die r_p noch so wählen, daß

$$r_p = 0 \text{ für fast alle p}$$

gilt. Damit ist die Summe

$$r = \sum_p r_p \in \mathbb{Q}$$

eine wohldefinierte rationale Zahl.

Weiter ist β_∞ , und damit auch β_∞-r , eine reelle Zahl. Es gibt somit eine ganze Zahl

$$s \in \mathbb{Z}$$

mit

$$|\beta_\infty - r - s|_\infty \leq 1/2.$$

Wir setzen

$$b := r + s \in \mathbb{Q}.$$

Dann gilt

$$|\beta_\infty - b|_\infty \leq 1/2.$$

Für jede Primzahl p gilt außerdem auf Grund der nicht-archimedischen Dreiecksungleichung

$$\begin{aligned} |\beta_p - b|_p &= |(\beta_p - r_p) - (r - r_p) - s|_p \\ &\leq \max\{ |\beta_p - r_p|_p , |s|_p |r_{p'},|_p \mid p' \text{ prim und } \neq p\} \\ &\leq^{21} \max \{ |\beta_p - r_p|_p , 1\} \\ &\leq 1 \end{aligned}$$

Wir haben gezeigt, β läßt sich in der Gestalt

$$\beta = b + \alpha$$

schreiben mit $b \in \mathbb{Q}$ und $\alpha := \beta - b \in W$.

QED.

4.4.5 Eine Summen-Zerlegung für Adele

Sei k ein globaler Körper. Dann gibt es eine Teilmenge

$$W := \{ (\xi_v)_v \in V_k \mid |\xi_v|_v \leq \delta_v \}$$

des Adele-Rings von k, welche Ungleichungen der Gestalt

$$|\xi_v|_v \leq \delta_v$$

---

[21] Es gilt $|s|_p \leq 1$ weil s eine ganze Zahl ist und $|r_{p'},|_p \leq 1$, weil in der Primfaktor-Zerlegung von $r_{p'} = z_{p'}/p'^{,n(p')}$ der Exponent von p' nicht-negativ ist.

mit $\delta_v = 1$ für fast alle v definiert ist, so daß sich jedes Adel $\varphi \in V_k$ in der Gestalt

$$\varphi = \theta + \gamma \text{ mit } \theta \in W \text{ und } \gamma \in k$$

schreiben läßt.
Beweis. Wie im Beweis von 4.4.4 reduziert man den Beweis mit Hilfe von 4.4.3 auf die Fälle $k = \mathbb{Q}$ und $k = F(t)$.

Man beachte, wegen der Identität von 4.2.4

$$\omega_1 \mathcal{O}_{k_v} + \ldots + \omega_N \mathcal{O}_{k_v} = \mathcal{O}_{K_1} \oplus \ldots \oplus \mathcal{O}_{K_J}$$

für endliche separable Erweiterungen K/k und fast alle v ist die Bedingung

$$|\xi_j|_v \leq 1$$

für die Koordinaten aus dem Grundkörper und fast alle Bewertungen v äquivalent zu der entsprechenden Bedingung

$$|\sum_{j=1}^{N} \xi_j \omega_j|_V \leq 1$$

für die Elemente des Erweiterungskörpers und fast alle Bewertungen V.

Im Fall $k = \mathbb{Q}$ ist die im Beweis von 4.4.4 konstruierte Menge W von der gesuchten Art. Im Fall $k = F(t)$ ist die Argumentation so ähnlich.
QED.

4.4.6 Endlichkeit des Maßes von V_k^+/k^+

Sei k ein globaler Körper. Dann ist das Maß der Gruppe

$$V_k^+/k^+$$

bezüglich des Faktor-Maßes des Haar-Maßes von V_k^+ endlich.

Bemerkung
Diese Aussage hängt natürlich nicht von der Wahl der multiplikativen Konstanten ab, bis auf die das Haar-Maß der Gruppe V_k^+ festgelegt ist. Wir beschäftigen uns hier nicht mit der Frage nach der konkreten Berechung des Maßes.
Beweis. Wie bisher kann man den Beweis der Aussage mit Hilfe von 4.4.3 auf die Fälle $k = \mathbb{Q}$ und $k = F(t)$ mit F endlich zurückführen. In diesen Fällen ergibt sich die Aussage fast unmittelbar. Man beachte, die in 4.4.4 konstruierte Menge W, welche sich surjektiv auf den Faktor V_k^+/k^+ abbildet, hat das Maß 1.

Ein alternativer Beweis ergibt sich aus der Kompaktheit von V_k^+/k^+. Sei

$$F \subseteq V_k^+/k^+$$

eine offene Teilmenge endlichen Maßes. Dann bilden die Verschiebungen von F eine offene Überdeckung von V_k^+/k^+ . Weil V_k^+/k^+ kompakt ist, wird die Gruppe von endlich vielen Verschiebungen von F überdeckt, d.h. von endlich vielen Mengen endlichen Maßes. Also ist das Maß von V_k^+/k^+ ebenfalls endlich.
QED.

4.4.7 Ein alternativer Beweis für den Produktsatz 4.2.3

Als Konsequenz der obigen Endlickeitsaussage ergibt sich ein alternativer Beweis für die Identität

$$\prod_v |\xi|_v = 1$$

für jedes von Null verschiedene Eleemnt $\xi \in k^*$ eines globalben Körpers (vgl. 4.2.3). Wie wir gesehen haben wird bei der Multiplikation mit

$$\beta_v \in k_v$$

das Haarsche Maß der lokal kompakten Gruppe k_v^+ mit dem Faktor $|\beta_v|_v$ multipliziert (vgl. Bemerkung 2.4.4(ii)). Für jedes Adel

$$\beta = (\beta_v)_v \in V_k - \{0\}$$

wird deshalb bei der Multiplikation mit β das Haarsche Maß von V_k^+ mit dem Faktor

$$\prod_v |\beta_v|_v$$

multipliziert. Insbesondere verändert die Multiplikation mit dem Hauptadel

$$\xi = (\xi_v)_v$$

das Haar-Maß von V_k um den Faktor $\prod_v |\xi|_v$.

Andererseit überfführt die Multiplikation mit ξ die Hauptadele in sich, induziert also eine korrekt definierte Abbildung

$$\varphi: V_k^+/k^+ \longrightarrow V_k^+/k^+,\ \overline{(\beta_v)_v} \mapsto \overline{(\xi\beta_v)_v} \qquad (1)$$

welche das Maß von V_k^+/k^+ mit dem Faktor $\prod_v |\xi|_v$ multipliziert:

$$\mu(\varphi(F)) = \prod_v |\xi|_v \cdot \mu(F) \text{ für meßbares } F \subseteq V_k^+/k^+.$$

Nun ist aber (1) eine bijektive Abbildung und $F = V_k^+/k^+$ hat nach 4.4.6 endliches Maß.

Deshalb muß $\prod_v |\xi|_v = 1$ sein.

Bemerkung

Im nachfolgenden Abschnitt wollen wir eine neue Variante des Approximationssatzes 2.3.4 beweisen. Dazu benötigen wir die nachfolgende Aussage.

4.4.8 Eine nur von k abhängige Konstante

Sei k ein globaler Körper. Dann gibt es eine nur von k abhängige positive reelle Konstante

$$0 < C \in \mathbb{R}$$

mit folgender Eigenschaft.

Für jedes Element $\alpha \in V_k$ mit

$$C < \prod_v |\alpha_v|_v$$

gibt es ein von Null verschiedenes Hauptadel $\beta \in k \subseteq V_k$ mit

$$|\beta|_v \leq |\alpha_v|_v$$

für alle normalisierten Bewertungen v von k.

Beweis. 1. Schritt. Für fast alle v gilt $|\alpha_v|_v = 1$.

Nach Definition von V_k gilt

$$|\alpha_v|_v \leq 1 \text{ für fast alle v.}$$

Angenommen, die Ungleichung ist echt für unendlich viele v. Es reicht zu zeigen, dies steht im Widerspruch zur Wahl von α

Sei I die Menge der nicht-archimedischen normalisierten Bewertungen von k, mit

$$|\alpha_v|_v < 1.$$

Dann ist I unendlich und es gilt

$$\prod_v |\alpha_v|_v = A \bullet B$$

mit

$$A := \prod_{v \in I} |\alpha_v|_v \text{ und } B := \prod_{v \notin I} |\alpha_v|_v.$$

Nach Wahl von I ist das Produkt B endlich[22], d.h. B ist eine wohldefinierte nicht-negative reelle Zahl. Es reicht deshalb zu zeigen, aus der Unendlichkeit von I folgt

$$A = 0,$$

denn das steht im Widerspruch zur Wahl von α, d.h. zu

$$0 < C < \prod_v |\alpha_v|_v .$$

Bezeichne $\kappa(v)$ den Restekörper von v. Dann gilt

$$|\alpha_v|_v = (1/\#\, \kappa(v))^{e(v)}$$

mit einer ganzen Zahl e(v). Wegen $|\alpha_v|_v < 1$ ist e(v) sogar eine natürliche Zahl. Wir betrachten eine Folge $\{v_n\}_{n=1,2,..}$ von paarweise verschiedenen Elementen aus I und setzen

$$x_n = (\#\, k(v_1))^{e(v_1)} \bullet \ldots \bullet (\#\, k(v_n))^{e(v_n)}$$

Dies ist ein Produkt von natürlichen Zahlen > 1. Die Folge der x_n ist damit eine streng monoton wachsende Folge von natürlichen Zahlen, geht also gegen ∞. Damit geht aber das Teilprodukt von A,

$$\prod_{i=1}^{n} |\alpha_{v_i}|_{v_i} = \frac{1}{x_n} \longrightarrow 0.$$

---

[22] Dies v, welche nicht in I sind, sind archimedisch, d.h. es gibt nur endlich viele von Ihnen, oder es gilt für sie $|\alpha_v|_v = 1$, d.h. sie leisten keinen Beitrag zum Produkt B.

gegen Null. Da alle Faktoren im Produkt A echt kleiner als 1 sind (nach Definition von I), folgt

$$A = 0.$$

Dies ist der gewünschte Widerspruch.

2. Schritt. Eine Abschätzung für das Maß der Menge

$$S := \{\gamma=(\gamma_v) \in V_k^+ \mid \begin{array}{ll} |\gamma_v|_v \le 1/10 & \text{für v archimedisch} \\ |\gamma_v|_v \le 1 & \text{für v nicht-archimedisch} \end{array} \}$$

Genauer, wir zeigen

$$0 < \mu(S) < \infty .$$

Für jede der endlich vielen archimedischen Bewertungen ist

$$S_v := \{\gamma \in k_v \mid |\gamma|_v \le \frac{1}{10}\}$$

ein Intervall der Länge 2/10 auf der reellen Achse oder eine Kreisscheibe in der komplexen Ebene vom Radius 1/10. In beiden Fällen gilt für das Maß

$$0 < \mu_v(S_v) < \infty.$$

Für jede archimedische Bewertung ist

$$S_v := \{\gamma \in k_v \mid |\gamma|_v \le 1\} = \mathcal{O}_v$$

eine Menge vom Maß $\mu_v(S_v) = 1$. Zusammen erhalten wir, daß

$$\mu(S) = \prod_v \mu_v(S_v)$$

eine positive reelle Zahl ist.

3. Schritt. Berechnung des Maßes der Menge
und

$$T := \{\gamma=(\gamma_v) \in V_k^+ \mid \begin{array}{ll} |\gamma_v|_v < \frac{1}{10}|\alpha_{vv}| & \text{für v archimedisch} \\ |\gamma_v|_v < |\alpha_v|_v & \text{für v nicht-archimedisch} \end{array} \}$$

Genauer, wir zeigen

$$\mu(T) = \mu(S)\cdot\prod_v |\alpha_v|_v.$$

Für jede der endlich vielen archimedischen Bewertungen ist

$$T_v := \{\gamma \in k_v \mid |\gamma|_v \le \frac{1}{10}|\alpha|_v\}$$

ein Intervall der Länge $\frac{2}{10}\cdot|\alpha_v|_v$ auf der reellen Achse oder eine Kreisscheibe in der komplexen Ebene vom Radius $\frac{1}{10}\cdot\sqrt{|\alpha_v|_v}$[23], welches man aus dem Intervall bzw. dem Einheitskreis S_v durch Multiplikation mit α_v erhält. Insbesondere ist

$$\mu_v(S_v) = \mu_v(S_v)\cdot|\alpha_v|_v.$$

Für jede archimedische Bewertung ist

$$T_v := \{\gamma \in k_v \mid |\gamma|_v \le |\alpha|_v\} = \alpha_v\mathcal{O}_v$$

---

[23] Nach Definition des Begriffs der normalisierten Bewertung im archimedischen Fall.

eine Menge vom Maß

$$\mu_v(T_v) = |\alpha_v|_v = \mu_v(S_v)\bullet|\alpha_v|_v.$$

Zusammen erhalten wir

$$\mu(T) = \mu(S)\bullet\prod_v |\alpha_v|_v.$$

4. Schritt. Beweis der Behauptung.
Wir setzen

$$C := \mu(V_k^+/k^+)/\mu(S).$$

Dann gilt für $C < \prod_v |\alpha_v|_v$:

$$\mu(T) = \mu(S)\bullet\prod_v |\alpha_v|_v > \mu(S)\bullet C = \mu(V_k^+/k^+))$$

Das Bild der Menge T bei der natürlichen Abbildung

$$V_k^+ \longrightarrow V_k^+/k^+$$

hat also ein Maß $< \mu(T)$. Deshalb ist die Einschränkung dieser Abbildung auf T nicht injektiv. Es gilt zwei Adele, sagen wir

$$\tau', \tau'' \in T$$

mit demselben Bild in V_k^+/k^+, sagen wir

$$\tau' - \tau'' = \beta \in k^+.$$

Für jede normalisierte Bewertung v gilt also

$$|\beta|_v = |\tau'_v - \tau''_v|$$

Ist v nicht-archimedisch, so kann man die rechte Seite wie folgt abschätzen.

$$|\tau'_v - \tau''_v| \le \max\{|\tau'_v|_v, |\tau''_v|_v\} \le |\alpha_v|_v .$$

Das zweite Kleiner-Gleich-Zeichen gilt dabei wegen $\tau', \tau'' \in T$.
Ist v archimedisch, so kann man die rechte Seite wie folgt abschätzen.

$$|\tau'_v - \tau''_v| \le |\tau'_v|_v + |\tau''_v|_v \le \frac{1}{10}|\alpha_v|_v + \frac{1}{10}|\alpha_v|_v \le |\alpha_v|_v .$$

Das mittlere Kleiner-Gleich-Zeichen gilt dabei wegen $\tau', \tau'' \in T$.
Zusammen erhalten wir für jedes v:

$$|\beta|_v \le |\alpha_v|_v$$

wie behauptet.
QED.

4.4.9 Polyzylinder, in denen Hauptadele liegen

Seien k ein globaler Körper, v_0 eine normalisierte Bewertung von k und

$$\delta_v > 0$$

für jede normalisierte Bewertung $v \neq v_0$ eine positive reelle Zahl, wobei für fast alle v

$$\delta_v = 1$$

gelte. Dann enthält der durch die δ_v definierte Polyzylinder

$$P(\delta) := \{\alpha \in V_k \mid |\alpha_v|_v \leq \delta_v \text{ für alle } v \neq v_0\}$$

mindestens ein von Null verschiedenes Hauptadel: es gibt ein $\beta \in k-\{0\}$ mit

$$|\beta|_v \leq \delta_v \text{ für alle } v \neq v_0.$$

Beweis. Wir wählen für jedes $v \neq v_0$ ein $\alpha_v \in k_v$ mit

$$0 < |\alpha_v|_v \leq \delta_v \text{ und } |\alpha_v|_v = 1 \text{ im Fall } \delta_v = 1.$$

Dann kann man $\alpha_{v_0} \in k_{v_0}$ so wählen, daß gilt

$$C < \prod_v |\alpha_v|_v$$

wobei C die Konstante von 4.4.8 bezeichne. Nach 4.4.8 existiert dann ein Hauptadel α mit den geforderten Eigenschaften.
QED.
Bemerkungen

(i) Man kann zeigen, die Charaktergruppe der lokal kompakten Gruppe V_k^+ ist isomorph zu V_k^+. Die Gruppe k^+ spielt dabei eine besonder Rolle. Siehe:

S. Lang: Algebraic number, Addison Wesley, 1964.
A. Weil: Adeles and algebraic groups, Inst. Advanced Studies, Princeton 1 961.
Godement, R.: Seminarie Bourbaki, Exposes 171, 176

Diese besondere Rolle steht in engem Zusammenhang mit den Funktionalgleichungen der ζ- und L-Funktionen.

(ii) Iwasawa hat gezeigt, daß man den Adele-Ring durch topologisch-algebraische Eigenschaften charakterisieren kann. Siehe:

Iwasawa, K.: On the ring of valuation vectors, Ann. Math. 57 (1953), 331-356.

4.4.10 Starker Approximationssatz

Seien k ein globler Körper und v_0 eine normalisierte Bewertung von k. Bezeichne

$$V := V_{k,v_0}$$

das eingeschränkte topologische Produkt der Vervollständigungen k_v bezüglich der Bewertungsring $\mathcal{O}_v$, wobei v die von v_0 verschiedenen normalisierten Bewertungen von k durchlaufe. Dann liegt k dicht in V.
Bemerkung
Der schwache Approximationssatz 2.3.4 macht die analoge Aussage für jedes endliche Produkt von Vervollständiguungen k_v.

Beweis. Seien die folgenden Daten gegeben.

1. Eine endliche Menge S von normalisierten Bewertungen von k, die von v_0 verschieden sind.
2. Eine reelle Zahl $\varepsilon > 0$.
3. Für jedes $v \in S$ ein $\alpha_v \in k_v$.

Zum Beweis der Behauptung reicht es dann zu zeigen, es gibt ein $\beta \in k$ mit

$$|\beta - \alpha_v|_v < \alpha \text{ für jedes } v \in S \text{ und}$$
$$|\beta|_v \leq 1 \text{ für jedes } v \notin S \bigcup \{v_0\}. \qquad (1)$$

Man beachte, die Mengen der Gestalt

$$\prod_{v \neq v_0} \Gamma_v$$

mit

$$\Gamma_v := \begin{cases} U_\varepsilon(\alpha_v) & \text{für } v \in S \\ k_v & \text{für } v \notin S \bigcup \{v_0\} \text{ archimedisch} \\ \mathcal{O}_v & \text{für } v \in S \bigcup \{v_0\} \text{ nicht-archimedisch} \end{cases}$$

und

$$U_\varepsilon(\alpha_v) := \{x \in k_v : \ |x-\alpha_v|_v < \varepsilon\}$$

bilden eine Topologie-Basis von V.[24]
Beweisen wir also (1).
1. Schritt. Vorbemerkung.

---

[24] Weil k nur endlich viele archimedische Bewertungen besitzt, kann man S zum Beispiel so wählen, daß alle archimedischen Bewertungen in S liegen. Der mittlere Fall in der Definition von Γ_v kommt dann nicht vor.
Jede offene Umgebung U eines Elements $\alpha = (\alpha_v)_v$ von V_{k,v_0} enthält dann eine Umgebung der angegebenen Gestalt:
In U liegt zunächst eine Umgebung von α aus der definierenden Topologie-Basis, sagen wir $\prod_{v \neq v_0} \Gamma'_v$. Für S wähle man dann die Menge der v, die archimedisch sind oder für die $\Gamma'_v \neq \mathcal{O}_v$ gilt. Dann kann man $\varepsilon > 0$ so klein wählen, daß gilt

$$\Gamma_v := U_\varepsilon(\alpha_v) \subseteq \Gamma'_v$$

für die endlich vielen v aus S (jedes Γ'_v ist offen). Für $v \notin S \bigcup \{v_0\}$ ist

$$\Gamma_v := \mathcal{O}_v = \Gamma'_v$$

eine offene Umgebung von $\alpha_v \in \Gamma'_v = \mathcal{O}_v$, d.h. es gilt

$$\alpha \in \prod_{v \neq v_0} \Gamma_v \subseteq \prod_{v \neq v_0} \Gamma'_v \subseteq U.$$

Nach Konstruktion ist $\prod_{v \neq v_0} \Gamma_v$ eine offene Umgebung von α, deren Faktoren Γ_v durch Bedingungen der Gestalt (1) definiert sind.

Nach 4.4.5 gibt es eine Teilmenge $W \subseteq V_k$ der Gestalt

$$W := \{ (\xi_v)_v \in V_k \mid |\xi_v|_v \leq \delta_v \}$$

mit positiven reellen Zahlen δ_v , die fast alle gleich 1 sind,

$$\delta_v = 1 \text{ für fast alle } v,$$

mit der Eigenschaft, daß sich jedes $\varphi \in V_k$ in der Gestalt

$$\varphi = \theta + \gamma \text{ mit } \theta \in W \text{ und } \gamma \in k$$

schreiben läßt.

2. Schritt. Vorbemerkung.

Wir betrachten den Polyzylinder von 4.4.9, der duch die Familie der reellen Zahlen

$$\delta_v^{-1}\varepsilon \text{ , } v \in S, \text{ und } \delta_v^{-1}, \; v \notin S \cup \{v_0\}$$

definiert ist. Da fast alle diese reellen Zahlen gleich 1 sind, enthält dieser Polyzylinder nach 4.4.9 mindestens ein von Null verschiedenes Hauptadel, d.h. es gibt ein

$$\lambda \in k - \{0\}$$

mit[25]

$$|\lambda|_v < \delta_v^{-1}\varepsilon \text{ für } v \in S \text{ und } |\lambda|_v \leq \delta_v^{-1} \text{ für } v \notin S \cup \{v_0\}.$$

3. Schritt.

Sei jetzt $\alpha \in V_k$ das Adel, dessen v-te Koordinate für $v \in S$ gleich α_v und für $v \notin S$ gleich 0 ist. Nach dem ersten Schritt mit $\varphi = \lambda^{-1}\alpha$ hat dann α die Gestalt[26]

$$\alpha = \psi + \beta \text{ mit } \frac{1}{\lambda}\psi \in W \text{ und } \beta \in k.$$

Damit gilt für $v \in S$:

$$|\beta - \alpha_v|_v = |\psi_v|_v = |\lambda|_v \cdot |\frac{1}{\lambda}\psi_v|_v < \delta_v^{-1}\varepsilon \cdot \delta_v = \varepsilon$$

und für $v \notin S \cup \{v_0\}$:

$$|\beta|_v = |\beta - \alpha_v|_v = |\psi_v|_v = |\lambda|_v \cdot |\frac{1}{\lambda}\psi_v|_v \leq \delta_v^{-1} \cdot \delta_v = 1.$$

Mit anderen Worten, das Element $\beta \in k$ genügt den Bedingungen von (1).

QED.

Bemerkungen

(i) Der Beweis gestatttet die Formulierung einer quantitaven Variante des starken Approximationssatzes, in welcher man eine Schranke für

$$|\beta|_{v_0} = |\psi_{v_0}|_{v_0} = |\lambda|_{v_0} \cdot |\frac{1}{\lambda}\psi_{v_0}|_{v_0} \leq |\lambda|_{v_0} \cdot \delta_{v_0}$$

angeben kann.[27]

---

[25] Genaugenommen steht in 4.4.9 links keine echte Ungleichung. Indem wir die endlich vielen reellen Zahlen der Gestalt $\delta_v^{-1}\varepsilon$ noch etwas verkleinern, können wir eine echte Ungleichung erreichen.

[26] d.h. $\lambda^{-1}\alpha = \varphi = \theta + \gamma$ mit $\theta \in W$ und $\gamma \in k^*$, also

$$\alpha = \lambda\theta + \lambda\gamma = \psi + \beta$$

mit $\psi = \lambda\theta$ und $\beta = \lambda\gamma$.

(ii) Einen alternativen Beweis des starken Approximatikonssatzes findet man in der Arbeit

Mahler, K.: Inequalities for ideal bases, J. Austr. Math. Soc. 4 (1964), 425-448

4.5 Die Idele-Gruppe

4.5.1 Die Einheiten-Gruppe eines topologischen Rings

Sei R ein topologischer Ring mit 1 (d.h. ein Ring mit der Struktur eines topologischen Raums, sodaß die Operationen +, - und • stetig sind). Dann ist die Einheiten-Gruppe

$$R^* \subseteq R$$

bezüglich der Unterraum-Topologie im allgemeinen keine topologische Gruppe: der Übergang zum Inversen,

$$R^* \longrightarrow R^*,\ x \mapsto x^{-1},$$

muß dann im allgemeinen nicht stetig sein. Deshalb betrachtet man die Abbildung

$$R^* \longrightarrow R\times R,\ x \mapsto (x, x^{-1}), \qquad (1)$$

welche offensichtlich injektiv ist. Man kann also R* mit Hilfe dieser Abbildung als eine Teilmenge von R×R ansehen. Wir versehen R* mit der Unterraum-Topologie von R×R bezüglich dieser Abbildung.

Bemerkung

Bezüglich der so definierten Topologie von R* ist R* eine topologische Gruppe. Diese Topologie heißt auch Einheiten-Gruppen-Topologie.

Beweis der Stetigkeit der Abbildungen

$$R^* \longrightarrow R^*,\ x \mapsto x^{-1}, \qquad (2)$$

und

$$R^*\times R^* \longrightarrow R^*,\ (x, y) \mapsto xy, \qquad (3)$$

bezüglich der Einheiten-Gruppen-Topologie.

Die Stetigkeit von (2). Eine Teilmenge von R* ist genau dann offen, wenn sie Urbild einer offenen Menge bei (1) ist. Es reicht also, die Stetigkeit der Komposition

$$R^* \longrightarrow R^* \longrightarrow R\times R,\ x \mapsto x^{-1} \mapsto (x\,x^{-1}, x),$$

zu beweisen. Diese ist aber als Komposition stetiger Abbildungen stetig, nämlich als Komposition

$$R^* \longrightarrow R\times R \longrightarrow R\bullet R,\ x \mapsto (x, x^{-1}) \mapsto (x^{-1},x),$$

aus der stetigen Abbildung (1) mit der stetigen Abbildung, welche die Koordinaten vertauscht.

Die Stetigkeit von (3). Es reicht zu zeigen, die Zusammensetzung von (3) mit (1),

$$R^*\times R^* \longrightarrow R^* \longrightarrow R\times R,\ (x, y) \mapsto xy \mapsto (xy, y^{-1}x^{-1},$$

ist stetig. Sie ist es tatsächlich als Zusammensetzung stetiger Abbildungen:

$$R^*\times R^* \overset{(1)\times(1)}{\longrightarrow} R\times R\times R\times R \longrightarrow R\times R,\ (x, y) \mapsto (x,x^{-1},y,y^{-1}) \mapsto (xy,y^{-1}x^{-1}).$$

Die erste dieser Abbildungen ist stetig, weil (1) stetig ist. Die zweite ist stetig, weil die Multiplikation von R stetig ist.

QED.

---

[27] vgl. den Beweis von 4.4.9: den Wert von $|\lambda|_{v_0}$ kann man abschätzen durch eine reelle Zahl, deren Produkt mit den Polyzylinder-Radien $\delta_v^{-1}\varepsilon$ bzw. δ_v^{-1} größer ist als die reelle Konstante C von 4.4.8.

4.5.2 Definition der Idele Gruppe

Sei k ein globaler Körper. Die Idele-Gruppe von k ist definiert als die Einheiten-Gruppe

$$J_k := V_k^*$$

des Adele-Rings V_k von k, versehen mit der Einheiten-Gruppen-Topologie. Die Elemente von J_k heißen Idele von k.

Bemerkungen

(i) Wir werden J_k gewöhnlich als Teilmenge von V_k ansehen und von der J_k-Topologie von J_k und der V_k-Topologie von J_k sprechen. Mit der ersten meinen wir die Einheiten-Gruppen-Topologie mit der zweiten die Unterraum-Topologie.
Beispiel
Sei

$$\alpha^{(q)} \in J_{\mathbb{Q}}$$

für jede Primzahl das Idel über den rationalen Zahlen $k = \mathbb{Q}$ mit den Koordinaten

$$\alpha_v^{(q)} = \begin{cases} q \text{ falls v die q-adische Bewertung ist} \\ 1 \qquad\qquad\qquad \text{sonst} \end{cases}$$

Dann gilt

$$\alpha^{(q)} \longrightarrow 1 \text{ für } q \longrightarrow \infty$$

bezüglich der $V_{\mathbb{Q}}$-Topologie von $J_{\mathbb{Q}}$, nicht jedoch bezüglich der $J_{\mathbb{Q}}$-Topologie.[28]

---

[28] Es gilt

$$\alpha_v^{(q)} - 1 = \begin{cases} q-1 \text{ falls v die q-adische Bewertung ist} \\ 0 \qquad\qquad\qquad \text{sonst} \end{cases}$$

Für jede offene Umgebung $\prod_v \Gamma_v$ der 1 der definierenden Topologie-Basis von V_k gilt $\Gamma_v = \mathcal{O}_v$ für alle hinreichend großen Primzahlen v, d.h. füt alle hinreichend großen q liegt

$$\alpha^{(q)} - 1$$

in dieser Umgebung. Damit gilt

$$\alpha^{(q)} \longrightarrow 1$$

in der V_k-Topologie.

Ist v die q-adische Bewertung, so gilt dagegen

$$\left|\frac{1}{\alpha_v^{(q)}} - 1\right|_v = \left|\frac{1}{q} - 1\right|_v = \left|\frac{1-q}{q}\right|_v$$

$$= \left|\frac{1}{q}\right|_v \qquad \text{(weil 1-q teilerfremd zu q ist)}$$

$$= q$$

Die v-te Koordinate von $\frac{1}{\alpha^{(q)}}$ liegt damit nicht im Bewertungsring. Für hinreichend großes q liegt damit keines der Glieder von $\{\frac{1}{\alpha^{(q)}}\}_{q \text{ prim}}$ in der vorgegebenen Umgegung $\prod_v \Gamma_v$ der 1, d.h. die Folge der $\frac{1}{\alpha^{(q)}}$ geht nicht gegen 1. In der J_k-Topologie geht damit die Folge der $\alpha^{(q)}$ nicht gegen 1.

(ii) Weil sich k in natürlicher Weise in V_k einbettet, läßt sich k* in natürlicher Weise als Teilmenge von J_k auffassen,

$$k^* \subseteq J_k.$$

Die Elemente von k*, betrachtet als Elemente von J_k heißen Hauptidele von k.

4.5.3 Die Topologie der Hauptidele

Sei k ein globaler Körper. Dann bilden die Hauptidele

$$k^* \subseteq J_k$$

eine diskrete Untergruppe von J_k.

Beweis.Nach 4.4.4 liegt

$$k \subseteq V_k$$

diskret im Adele-Ring. Also liegt

$$k \times k \subseteq V_k \times V_k$$

diskret im direkten Produkt des Adele-Rings mit sich selbst. Dann liegt aber auch die Teilmenge k*×k* diskret in diesem direkten Produkt, d.h. k* liegt diskret in J_k.

QED.

4.5.4 Die J_k-Topologie als eingeschränkte Produkt-Topologie

Sei k ein globaler Körper. Dann ist J_k als topologischer Raum (mit der J_k-Topologie) gerade das eingeschränkte topologische Produkt der multiplikativen Gruppen k_v^* der Vervollständigungen von k bezüglich der Einheiten-Gruppen U_v .

Beweis. Eine Einheit von V_k ist eine Familie

$$\alpha = (\alpha_v)_v$$

mit

$\alpha_v \in k_v$ für jedes v, $\alpha_v \in \mathcal{O}_v$ für fast jedes v

$\alpha_v \neq 0$ für jede v

$\alpha_v^{-1} \in k_v$ für jedes v, $\alpha_v^{-1} \in \mathbb{O}_v$ für fast jedes v.

d.h. es gilt

$$\alpha_v \in k_v^* \text{ für jedes v, } \alpha_v \in \mathcal{O}_v^* \text{ für fast jedes v.}$$

Als Menge ist damit J_k gerade das eingeschränkte topologische Produkt der k_v^* bezüglich der $\mathcal{O}_v^* = U_v$. Die Teilmengen von J_k der folgenden Gestalt bilden eine Umgebungsbasis von J_k:

$$\prod_v \Gamma_v$$

mit

$$\{(x,x^{-1}) \mid x \in \Gamma_v\} \text{ offen in } k_v^* \times k_v^* \text{ für jedes v}$$

und

$$\Gamma_v = \{x \mid (x,x^{-1}) \in \mathcal{O}_v^*\} \text{ für fast jedes } v.$$

Die zweite Bedingung bedeutet gerade $\Gamma_v = U_v$ für fast jedes v. Damit ist J_k gerade das beschriebene eingeschränkte topologische Produkt.
QED.

4.5.5 Der Inhalt eine Idels

Seien k ein globaler Körper und $\alpha := \{\alpha_v\}_v \in J_k$ ein Idel. Dann heißt

$$c(\alpha) := \prod_v |\alpha_v|_v$$

Inhalt[29] von α.

4.5.6 Stetigkeit des Inhalts

Sei k ein globaler Körper. Dann ist die Inhaltsabbildung

$$J_k \longrightarrow \mathbb{R}_{>0},\ \alpha \mapsto c(\alpha),$$

ein stetiger Homomorphismus der topologischen Gruppe J_k mit Werten in der topologischen Gruppe $\mathbb{R}_{>0}$ der positiven reellen Zahlen (mit der Multiplikation als Gruppen-Operation).
Beweis. Trivialerweise ist c ein Gruppen-Homomorphismus. Wir haben dessen Stetigkeit zu beweisen.

Seien r eine positive reelle Zahl und

$$U_\varepsilon(r) \subseteq \mathbb{R}_{>0}$$

eine ganz in $\mathbb{R}_{>0}$ liegende ε-Umgebung von r. Wir haben zu zeigen, die Menge

$$c^{-1}(U_\varepsilon(r)) = \{\alpha \in J_k \mid |c(\alpha)/r| < \varepsilon\}$$

ist offen. Weil J_k und $\mathbb{R}_{>0}$ topologische Gruppen sind und c ein Gruppen-Homomorphismus ist, reicht es die Stetigkeit im neutralen Element nachzuweisen, d.h. wir können r = 1 annehmen, und es reicht zu zeigen,

$$c^{-1}(U_\varepsilon(1)) = \{\alpha \in J_k \mid |c(\alpha)| < \varepsilon\}$$

enthält eine offene Umgebung des neutralen Elements $1 \in k^* \subseteq J_k$. Eine solche offene Umgebung ist

$$\prod_v \Gamma_v \tag{1}$$

mit

$$\Gamma_v = U_v \text{ für jedes nicht-archimedische } v \neq v_0$$

$$\Gamma_v = \{\alpha \in k_v^* \mid |\alpha|_v < 1\} \text{ für jedes archimedische } v \neq v_0$$

$$\Gamma_{v_0} = \{\alpha \in k_{v_0}^* \mid |\alpha|_{v_0} < \varepsilon\}$$

---

[29] c von Englisch ‘contents’.

Dabei sei v_0 eine beliebig aber fest gewählte normalisierte Bewertung von k. Man beachte, für $x \in U_v = \mathcal{O}_v^*$ gilt $|x|_v = 1$. Deshalb liegt $\prod_v \Gamma_v$ tatsächlich ganz im Urbild von $U_\varepsilon(1)$ bei c.

QED.

4.5.7 Verhalten des Haar-Maßes bei der Multiplikation mit Idelen

Seien k ein globaler Körper und $\alpha \in J_k$ ein Idel. Dann wird bei der Abbildung

$$V_k^+ \longrightarrow V_k^+, x \mapsto \alpha x,$$

das Haar-Maß von V_k^+ mit dem Inhalt $c(\alpha)$ multipliziert.

Beweis. vgl. 4.4.7.

QED.

4.5.8 J_k-Topologie als Operator-Topologie

Sei k ein globabler Körper. Wir betrachten die Operation der Idele-Gruppe auf dem Adele-Ring durch Multiplikation,

$$J_k \times V_k \longrightarrow V_k, (\alpha, x) \mapsto \alpha x.$$

Für je zwei Teilmengen $C, U \subseteq V_k$ sei

$$S(C, U) := \{\alpha \in J_k \mid (1-\alpha)C \subseteq U \text{ und } (1-\alpha^{-1})C \subseteq U\}.$$

Dann bilden die Mengen der Gestalt

$$S(C, U) \text{ mit C kompakt in } V_k \text{ und U offen in } V_k$$

eine Topologie-Basis der J_k-Topologie von J_k.

Korrektur

In der angegebenen Formulierung kann die Aussage nicht richtig sein, denn nach Defintion gilt

$$\alpha \in S(C,U) \Leftrightarrow \alpha^{-1} \in S(C,U).$$

Jede offene Menge, die α enthält, enthielte somit auch α^{-1}, im Widerspruch dazu, daß die J_k-Topologie nach Definition separiert ist.

Richtig ist, daß die Mengen S(C, U), welche das Einselement enthalten, eine Umgebungsbasis der Eins bilden.

Beweis.

1. Schritt: Die Mengen S(C,U) sind offen in der J_k-Topologie.

Sei $\alpha \in S(C, U)$. Wir haben zu zeigen, eine ganze offene Umgebung von α liegt auch in S(C,U). Im Fall $C = \varnothing$ gilt $S(C,U) = J_k$ und die Aussage ist trivial. Sei also

$$C \neq \varnothing.$$

Da α in S(C,U) liegt, kann dann U nicht leer sein. Wir können annehmen[30], U ist eine offene Menge der definierenden Topologie-Basis von V_k, sagen wir

$$U = \prod_v U_v$$

[30] Die allgemeinen S(C,U) sind Vereinigungen der S(C,U) mit den speziell gewählten U.

Für die nicht-archimedischen v können wir weiter annehmen,

$$U_v = u'_v + u''_v \mathfrak{O}_v \text{ , } u'_v \in k_v, u''_v \in k_v - \{0\}, \text{ für v nicht-archimedisch.}$$

Mengen dieser Gestalt, sagen wir $a + b\mathfrak{O}_v$ wollen wir hier Standard-Umgebungen (von a) nennen.

Sei jetzt $x \in C$ und $x_v \neq 0$. Es gilt dann

$$(1-\alpha_v)x_v \in U_v = u'_v + u''_v \mathfrak{O}_v$$

$$x_v - \alpha_v x_v \in U_v = u'_v + u''_v \mathfrak{O}_v$$

$$x_v - \alpha_v x_v + u''_v \mathfrak{O}_v \in U_v = u'_v + u''_v \mathfrak{O}_v$$

$$(x_v + u''_v \mathfrak{O}_v) - \alpha_v (x_v + u''_v / \alpha_v \mathfrak{O}_v) \in U_v = u'_v + u''_v \mathfrak{O}_v$$

Sie $y_v \mathfrak{O}_v$ die kleinere der beiden Mengen $u''_v \mathfrak{O}_v$ und $u''_v / \alpha_v \mathfrak{O}_v$. Dann gilt

$$(x_v + y_v \mathfrak{O}_v) - \alpha_v (x_v + y_v \mathfrak{O}_v) \in U_v = u'_v + u''_v \mathfrak{O}_v$$

$$(1-\alpha_v)(x_v + y_v \mathfrak{O}_v) \in U_v = u'_v + u''_v \mathfrak{O}_v$$

$$(1-\alpha_v)(x_v + y_v \mathfrak{O}_v) \in U_v = u'_v + u''_v \mathfrak{O}_v$$

Das Produkt des zweiten Faktors links mit einer hinreichend hohen Potenz eines Parameters von $\mathfrak{O}_v$ ist eine Teilmenge von des zweiten Summanden rechts. Die Enthaltenseinsrelation bleibt erhalten, wenn wir zu α_v links Vielfache dieser Potenz addieren. Außerdem könnn wir annehmen, y_v ist eine solche Potenz dieses Parameters. Zusammen ergibt sich

$$(1-\alpha_v + y_v \mathfrak{O}_v)(x_v + y_v \mathfrak{O}_v) \in U_v = u'_v + u''_v \mathfrak{O}_v$$

Indem wir besagt Parameterpotenz bei Bedarf noch erhöhen, erhalten wir

$$(1-\alpha_v(1+y_v \mathfrak{O}_v))(x_v + y_v \mathfrak{O}_v) \in U_v = u'_v + u''_v \mathfrak{O}_v$$

Im Fall $x_v = 0$ können wir annehmen, daß auch $u'_v = 0$ ist. Dann besteht die letzte Enthaltenseinsrelation aber auch (mit y_v geeignet).

Wir haben damit ein Produkt V von Standard-Umgebungen der Null gefunden mit

$$(1-\alpha(1+V))(x+V) \subseteq U.$$

Wir können annehmen $u'_v = 0$, $u''_v = 1$ für fast alle v. Außerdem ist für fast alle v auch $\alpha_v \in \mathfrak{O}_v^*$ und $x_v \in \mathfrak{O}_v$. Deshalb kann man annehmen, fast alle Faktoren von V sind gleich dem Bewertungsring. Mit anderen Worten, V ist eine offene Menge der definierenden Topologie-Basis von V_k (und eine Umgebung der Null). Durchläuft x die kompakte Menge V, so durchlaufen die x+V eine Überdeckung von C. Bereits endlich viele der x+V überdecken C. Sei V' der Durchschnitt der zugehörigen endlich vielen V. Dann gilt

$$(1-\alpha(1+V'))C \subseteq U.$$

Ersetzt man die Faktoren von V', welche gleich $\mathfrak{O}$ sind, durch $\mathfrak{O}^*$, so erhält man

$$(1-\alpha W)C \subseteq U.$$

mit einem Produkt W von offenen Untergruppen der Einheiten-Gruppen $\mathfrak{O}_v^*$, wobei fast alle Faktoren gleich der entsprechenden Einheiten-Gruppe sind. Insbesondere ist W eine Umgebung der 1 bezügich J_k-Topologie (nach 4.5.4).

Ersetzt man in der obigen Argumentation α durch α^{-1}, so erhält man eine offene Umgebung W' der 1 bezüglich der J_k mit

$$(1-\alpha^{-1}W')C \subseteq U$$

d.h.

$$(1-(\alpha W'^{-1})^{-1})C \subseteq U$$

Es gilt also

$$\alpha\bullet(W' \cap W'^{-1}) \subseteq S(C, U).$$

Nun ist aber mit W' auch W'^{-1} eine offene Umgebung von 1 in der J_k-Topologie.[31]

Dasselbe gilt somit auch für $W' \cap W'^{-1}$. Mit α liegt also eine ganze Umgebung von α in S(C, U). Mit anderen Worten S(C,U) ist offen.

2. Schritt. Die Operator-offenen Mengen S(C,U), welche das Einselement enthalten, bilden eine Umgebungsbasis von 1.

Nach 4.5.4 reicht es zu zeigen, daß die Mengen der folgenden Gestalt offen in der Operator-Topologie sind.

$$\prod_v \Gamma_v$$

mit

$\Gamma_v = 1 + \pi_v^{e(v)}\mathfrak{O}_v$ oder $= \mathfrak{O}_v^*$ für v nicht-archimedisch
(und für fast alle v trift der zweite Fall zu)

$\Gamma_v = U_\varepsilon(1)$ für v archimedisch

$\varepsilon > 0$ beliebig.

Dazu reicht es zu zeigen, die Mengen Γ_v sind offen für jedes v.

1. Fall: v ist nicht-archimedisch.

Es reicht zu zeigen,

$$\Gamma_v = 1 + \pi_v^{e(v)}\mathfrak{O}_v$$

ist gerade die Menge

$$S_v(\{1\}, \pi_v^{e(v)}\mathfrak{O}_v) = \{\alpha \in k_v^* \mid (\alpha-1)\bullet 1 \in \pi_v^{e(v)}\mathfrak{O}_v \text{ und } (\alpha^{-1}-1)\bullet 1 \in \pi_v^{e(v)}\mathfrak{O}_v\},$$

Beweis von "$\supseteq$". Für $\alpha \in S_v(\{1\}, \pi_v^{e(v)}\mathfrak{O}_v)$ gilt $\alpha-1 \in \pi_v^{e(v)}\mathfrak{O}_v$ also

$$\alpha \in 1+\pi_v^{e(v)}\mathfrak{O}_v = \Gamma_v.$$

Beweis von "$\supseteq$". Für $\alpha \in \Gamma_v$ gilt $\alpha = 1 - \beta$ mit $\beta \in \pi_v^{e(v)}\mathfrak{O}_v$, also

$$\alpha^{-1} = \frac{1}{1-\beta} = 1 + \beta + \beta^2 + \ldots \in 1 + \pi_v^{e(v)}\mathfrak{O}_v$$

---

[31] Weil der Übergang zum Inversen ein Homöomorphismus von J_k ist.

Man beachte, k_v ist vollständig. Es folgt

$$(\alpha\text{-}1)\bullet 1 \in \pi_v^{e(v)}\mathfrak{O}_v \text{ und } (\alpha^{-1} - 1)\bullet 1 \in \pi_v^{e(v)}\mathfrak{O}_v,$$

also

$$\alpha \in S_v(\{1\}, \pi_v^{e(v)}\mathfrak{O}_v).$$

2. Fall: v archimedisch.

Wir haben zu zeigen, für $\varepsilon>0$ ist $U_\varepsilon(1)$ offen in der Operator-Topologie. Dazu reicht es zu zeigen, für jedes $x \in U_\varepsilon(1)$ gilt

$$x \in S(\{1, -x\}, U_\varepsilon(0)) \subseteq U_\varepsilon(1).$$

denn dann ist $U_\varepsilon(1)$ Vereinigung von Operator-offenen Mengen.

Beweis der Inklusion rechts.

Für $\alpha \in S(\{1, -x\}, U_\varepsilon(0))$ gilt $(\alpha\text{-}1)\bullet 1 \in U_\varepsilon(0)$, also $\alpha \in 1 + U_\varepsilon(0) = U_\varepsilon(1)$.

Beweis der Relation links.

Es gilt

$$x \in U_\varepsilon(1) \Leftrightarrow x = 1 - y \text{ mit } |y| < \varepsilon$$

also

$$(x\text{-}1)\bullet 1 = y \in U_\varepsilon(0).$$

Weiter ist

$$(x^{-1} - 1)(-x) = -1 + x = y \in U_\varepsilon(0).$$

Zusammen erhalten wir

$$x \in S(\{1, -x\}, U_\varepsilon(0))$$

QED.

4.5.9 Die Topologie des Kerns der Inhaltsabbildung

Sei k ein globaler Körper. Dann ist der Kern der Inhaltsabbildung

$$J_k^1 := \mathrm{Ker}(c: J_k \longrightarrow \mathbb{R}_{>0})$$

abgeschlossen in V_k (bezüglich der V_k-Topologie) und in J_k (bezüglich der V_k- und der J_k-Topologie). Die J_k-Topologie induziert auf J_k^1 dieselbe Topologie wie die V_k-Topologie.

Beweis. 1. Schritt: Für jedes $\alpha \in V_k - J_k^1$ gibt es eine V_k-Umgebung W von α mit

$$W \bigcap J_k^1 = \varnothing.$$

1. Fall: $\prod_v |\alpha_v|_v < 1$.

Wir lassen dabei den Fall zu, daß das Produkt auf der linken Seite gleich Null ist. Wegen $\alpha \in V_k$ ist für fast alle v der Wert $|\alpha_v|_v$ kleiner oder gleich 1. Es gibt deshalb eine endliche Menge S von normalisierten Bewertungen v von k mit

a) S enthält alle Bewertungen v mit $|\alpha_v|_v > 1$ und alle archimedischen Bewertungen.

b) $\prod_{v\in S} |\alpha_v|_v < 1$.[32]

Wir setzen

$$W := \{\xi \in V_k \mid |\xi_v - \alpha_v|_v < \varepsilon \text{ für } v\in S \text{ und } |\xi_v|_v \le 1 \text{ für } v\notin S\}.$$

Dies ist eine offene Umgebung von α.[33] Für ε hinreichend klein, kommt das Produkt $\prod_{v\in S} |\xi_v|_v$ dem Produkt $\prod_{v\in S} |\alpha_v|_v$ beliebig nahe, d.h. für kleines ε ist

$$\prod_{v\in S} |\xi_v|_v < 1.$$

Die übrigen Faktoren $|\xi_v|_v$ sind aber nach Definition von W sämtlich ≤ 1. Deshalb gilt für $\xi\in W$ stets $\prod_v |\xi_v|_v < 1$, d.h. W enthält keine Elemente von J_k^1.

2. Fall: $\prod_v |\alpha_v|_v > 1$.

Wir setzen

$$C := \prod_v |\alpha_v|_v \ . \qquad (1)$$

Dann gibt es eine endliche Menge S von normalisierten Bewertungen von k mit

a) S enthält alle Bewertungen v mit $|\alpha_v|_v > 1$ und alle archimedischen Bewertungen.

b) $1 < \prod_{v\in S} |\alpha_v|_v < 2C$.

c) Für jedes $v \notin S$ und jedes $\xi\in V_k$ mit $|\xi_v|_v < 1$ gilt $|\xi_v|_v < \frac{1}{2C}$.

In Bezug auf die zweite Bedingung beachte, daß die endlichen Teilprodukte von (1) dem Wert C beliebig nahe kommen, wennn man nur genügend viele Faktoren aufnimmen. Wegen

$$1 < C < 2C$$

kann man also durch die Aufnahme genügt vieler Bewertungen v in die Menge S erreichen, daß die Bedingung von b) erfüllt ist.

In Bezug auf die dritte Bedingung beachte man, daß im Zahlenkörper-Fall $k \supseteq \mathbb{Q}$ jede nicht-archimedische Bewertung v über einer p-adischen Bewertung von $\mathbb{Q}$ liegt, wobei p eine Primzahl ist. Die Werte von v sind dann ganzzahlige Potenzen von p. Nimmt man in die Menge S alle v mit

$$p \le 2C$$

---

[32] Da das Produkt aller $|\alpha_v|_v$ ist ein Wert $p < 1$ ist, und das Produkt von hinreichend aber endlich vielen von ihnen kommt dem Wert $p < 1$ beliebig nahe.

[33] Nach Wahl von S ist α_v ganz für jedes $v\notin S$, d.h. α liegt in W.

auf (von denen es nur endlich viele gibt), gilt für die Werte eines $v \notin S$ und das zugehörige p,

$$|\xi_v|_v = (\frac{1}{p})^e \text{ und } p > 2C.$$

Weil der Wert von ξ_v kleiner als 1 sein soll, muß e ein natürliche Zahl sein. Es folgt also

$$|\xi_v|_v = (\frac{1}{p})^e < (\frac{1}{2C})^e \leq \frac{1}{2C}$$

(wegen $C > 1$ nach Voraussetzung). Im Funktionenkörper-Fall $k \supseteq F(t)$ ist die Situation analog: die Werte $|\xi_v|_v$ sind Potenzen $\# \kappa$, wobei κ die endlichen Erweiterungen von F durchläuft, und es gibt nur endlich viele Körper κ mit $\# \kappa \leq \frac{2}{C}$.

Es gibt also tatsächlich eine endliche Menge S, die den drei obigen Bedingungen a), b) und c) genügt.

Wir wählen eine reelle Zahl $\varepsilon>0$, die so klein ist, daß für jedes $\xi \in V_k$ mit

$$|\xi_v - \alpha_v|_v < \varepsilon \text{ für alle } v \in S$$

gilt

$$0 < \prod_{v \in S} |\xi_v|_v < 2C$$

Das ist möglich auf Grund von Bedingung b). Wir setzen wieder

$$W := \{\xi \in V_k \mid |\xi_v - \alpha_v|_v < \varepsilon \text{ für } v \in S \text{ und } |\xi_v|_v \leq 1 \text{ für } v \notin S\}.$$

Für $\xi \in W$ gilt dann

$$0 < \prod_{v \in S} |\xi_v|_v < 2C$$

Falls es ein $v \notin S$ gibt mit $|\xi_v|_v < 1$, so ist wegen Bedingung c) sogar

$$|\xi_v|_v < \frac{1}{2C}.$$

Wegen $|\xi_v|_v \leq 1$ für alle $v \notin S$ ist dann

$$c(\xi) = \prod_{v \in S} |\xi_v|_v \cdot \prod_{v \notin S} |\xi_v|_v < 2C \cdot \frac{1}{2C} = 1,$$

d.h. ξ liegt nicht im Kern von c.

Falls es kein $v \notin S$ gibt mit $|\xi_v|_v < 1$, so

$$c(\xi) = \prod_{v \in S} |\xi_v|_v \cdot \prod_{v \notin S} |\xi_v|_v = 2C \cdot 1 = 2C > 1,$$

d.h. auch in diesem Fall liegt ξ nicht im Kern von c.
Damit ist die Aussage des ersten Schritts bewiesen.

2. Schritt: J_k^1 ist abgeschloss3n in J_k bezüglich der J_k-Topologie.

Nach dem ersten Schritt ist J_k^1 abgeschlossen in J_k bezüglich der V_k-Topologie von J_k. Nun ist aber die natürliche Einbettung

$$J_k \hookrightarrow V_k$$

stetig (als Zusammensetzung von $J_k \hookrightarrow V_k \times V_k$, $x \mapsto (x,x^{-1})$ mit der Projektion auf den ersten Faktor), d.h. jede V_k-offene Menge von J_k ist auch J_k-offen. Dann ist aber auch jede V_k-abgeschlossene Menge von J_k auch J_k-abgeschossen. Insbesondere ist J_k^1 auch J_k-abgeschossen.

Zum Beweis der Behauptung fehlt noch die folgende Aussage.

2. Schritt. Die J_k-Topologie von J_k^1 stimmt mit der V_k-Topologie überein.

Wie wir eben gesehen haben, ist jede V_k-offene Menge auch J_k-offen. Es reicht also zu zeigen:

$$\text{Für } \alpha \in J_k^1 \text{ ist jede } J_k\text{-offene Umgebung } H \subseteq J_k^1 \text{ von } \alpha \text{ auch } V_k\text{-offen.} \qquad (3)$$

Die J_k-offene Umgebung H von α enthält eine J_k-Umgebung der Gestalt:

$$W \cap J_k^1$$

mit

$$W := \{\xi \in V_k \mid |\xi_v - \alpha_v|_v < \varepsilon \text{ und } |\xi_v^{-1} - \alpha_v^{-1}|_v < \delta \text{ für } v \in S \text{ und } |\xi_v|_v = 1 \text{ für } v \notin S\}.$$

Dabei enthalte die endliche Menge S alle archimedischen Bewertungen von k und alle v mit $|\alpha_v|_v \neq 1$.[34] Für ε klein genung und $v \in S$ gilt mit $|\xi_v - \alpha_v|_v < \varepsilon$ auch

$$|\xi_v^{-1} - \alpha_v^{-1}|_v = |\xi_v - \alpha_v|_v \cdot 1/|\alpha_v \xi_v|_v \text{ und } |\alpha_v|_v \leq 2|\xi_v|_v$$

also

$$|\xi_v^{-1} - \alpha_v^{-1}|_v \leq |\xi_v - \alpha_v|_v \cdot 2/|\alpha_v|_v^2 < \delta,$$

d.h. für hinreichend kleine ε (und fest gewählte δ) kann man die Bedingungen an die Inversen der Koordinaten weglassen:

$$W := \{\xi \in V_k \mid |\xi_v - \alpha_v|_v < \varepsilon \text{ für } v \in S \text{ und } |\xi_v|_v = 1 \text{ für } v \notin S\}.$$

Wegen $|\alpha_v|_v = 1$ und v nicht-archimedisch für $v \notin S$ ist die Bedingung

$$|\xi_v - \alpha_v|_v < \varepsilon$$

für diese v und hinreichend kleines ε äquivalent zur Bedingung $|\xi_v|_v = 1$. Wir können also bei Bedarf die Mengen S vergrößern ohne die Menge W zu verändern (falls $\varepsilon \leq 1$ ist). Deshalb können wir S so groß wählen, daß für $v \notin S$ die Implikation

$$|x|_v < 1 \Rightarrow |x|_v < 1/2 \text{ (für } v \notin S) \qquad (3)$$

---

[34] Für fast alle v gilt v nicht-archimedisch, $|\alpha_v|_v = 1$ und die einzige Bedingung, die man an die v-te Koordinate stellt, ist die Ganzheit der Koordinate und des Inversen der Koordinate.

besteht (siehe oben).

Wegen

$$\prod_v |\alpha_v|_v = 1$$

kann man ε so klein wählen, daß für $\xi \in J_k^1$ und $|\xi_v - \alpha_v|_v < \varepsilon$ auch gilt[35]

$$\prod_{v \in S} |\xi_v|_v < 2.$$

Ist $|\xi_v|_v < 1$ für ein $v \notin S$ und $|\xi_v|_v \leq 1$ für alle $v \notin S$, so ist wegen (3) das Produkt

$$\prod_v |\xi_v|_v < 2 \cdot \frac{1}{2} = 1,$$

was im Widerspruch zu $\xi \in J_k^1$ steht. Es muß also $|\xi_v|_v = 1$ für alle $v \notin S$ sein. Wir haben gezeigt,

$$W \cap J_k^1 = \widetilde{W} \cap J_k^1$$

mit

$$\widetilde{W} = \{\xi \in V_k \mid |\xi_v - \alpha_v|_v < \varepsilon \text{ für } v \in S \text{ und } |\xi_v|_v \leq 1 \text{ für } v \notin S\}.$$

Nun ist aber $\widetilde{W}$ eine V_k-offene Menge, also $W \cap J_k^1$ eine V_k-offene Umgebung von α. Für jedes $\alpha \in H$ gibt es somit eine V_k-offene Umgebung vn α, die ganz in H liegt. Also ist H auch V_k-offen.

QED.

4.5.10 Die Kompaktheit des Faktors J_k^1/k^*

Sei k ein globaler Körper. Auf Grund der Produkt-Formel 4.2.3 gilt dann

$$k^* \subseteq J_k^1.$$

Die Faktor-Gruppe J_k^1/k^* ist kompakt bezüglich der Faktor-Topologie.

Beweis. Auf Grund der gerade bewiesenen Aussage 4.5.9 stimmt die Topologie von J_k^1 mit der von V_k kommenden Unterraum-Topologie überein. Es reicht deshalb eine kompakte Teilmenge

$$W \subseteq V_k$$

von V_k zu finden mit der Eigenschaft, daß sich $W \cap J_k^1$ surjektiv auf J_k^1/k^* abbildet,

$$W \cap J_k^1 \twoheadrightarrow J_k^1/k^*.$$

Man beachte, weil J_k^1 abgeschlossen in V_k ist (nach 4.5.9), ist der Durchschnitt $W \cap J_k^1$ eine abgeschlossene Teilmenge von W. Mit W ist somit auch dieser Durchschnitt

[35] Fast alle Faktoren sind gleich 1, für das Produkt der endlich vielen übrigen kann man durch Verkleinern von ε erreichen, daß es sich dem Wert 1 beliebig nähert.

kompakt. Dazu wählen wir ein Idel $\alpha \in J_k$, dessen Inhalt größer ist als die reelle Zahl C von 4.4.8,

$$C < c(\alpha).$$

Wir setzen

$$W := \{\xi \in V_k \mid |\xi_v|_v \leq |\alpha_v|_v \text{ für alle } v\}.$$

Als direktes Produkt kompakter Mengen ist W kompakt.

Sei jetzt $\eta \in J_k^1$ beliebig vorgegeben. Dann gilt $c(\eta) = 1$, also auch

$$C < c(\eta^{-1}\alpha).$$

Nach 4.4.8 enthält der durch $\eta^{-1}\alpha$ definierte Polyzylinder

$$\{\xi \in V_k \mid |\xi_v|_v \leq |\eta^{-1}\alpha_v|_v \text{ für alle } v\}$$

ein von Null verschiedenes Hauptidel, sagen wir $\beta \in k^*$. Für jedes v gilt somit

$$|\beta|_v \leq |\eta^{-1}\alpha_v|_v ,$$

d.h. es ist $\beta\eta \in W$. Die Restklasse modulo k^* des vorgegebenen Elements $\eta \in J_k^1$ besitzt also das Urbild $\beta\eta$ in W (und wegen der Produktformel 4.2.3 für Hauptidele sogar in $W \bigcap J_k^1$).
QED.

4.6 Ideale und Divisoren

4.6.1 Die Gruppe der Ideale im Zahlenkörper-Fall

Sei k eine endliche Körper-Erweiterung des Körpers $\mathbb{Q}$ der rationalen Zahlen. Dann heißt die freie abelsche Gruppe

$$I_k := \{ \sum_{v \text{ nicht-archimedisch}} n_v \cdot v \},$$

die von den nicht-archimedischen normalisierten Bewertungen von k erzeugt wird, Gruppe der Ideale von k. Die Gruppe I_k besteht also aus den formalen ganzzahligen Linearkombinationen

$$\sum_{v \text{ nicht-archimedisch}} n_v \cdot v$$

der normalisierten nicht-archimedischen Bewertungen von k, wobei die Anzahl der von Null verschiedenen Koeffizienten n_v endlich ist. Eine solche Linearkombination heißt auch (gebrochenes) Ideal von k. Sind alle Koeffizienten nicht-negativ,

$$n_v \geq 0,$$

so heißt das Ideal auch ganz.

Bemerkungen

(i) Die obige Terminologie ist dadurch gerechtfertigt, daß sich I_k mit der Gruppe der gebrochenen Ideale im gewöhnlichem Sinne des Dedekind-Rings

$$\mathcal{O} = \bigcap_{v \text{ nicht-archimedisch}} \mathcal{O}_v$$

identifizieren läßt.

(ii) Für jedes Idel $\alpha = (\alpha_v)_v \in J_k$ und jede nicht-archimedischen normalisierte Bewertung v von k bezeichne

$$ord_v(\alpha) = ord_v(\alpha_v)$$

den Wert der v-ten Koordinate von α bezüglich der zu v gehörigen additiven Bewertung (d.h. den Exponenten der höchsten Potenz des Bewertungsideals von $\mathfrak{O}_v$, die das Element α_v enthält). Dann ist die Abbildung

$$J_k \longrightarrow I_k\ ,\ \alpha = (\alpha_v)_v \mapsto \sum_{v \text{ nicht-archimedisch}} ord_v(\alpha)\bullet v\ ,$$

ein Gruppen-Homomorphismus der multiplikativen Gruppe J_k in die additive Gruppe I_k. Versieht man die Gruppe I_k mit der diskreten Topologie, so ist dieser Homomorphismus stetig.[36] Das Bild von $k^* \subseteq J_k$ bei dieser Abbildung heißt Gruppe der Hauptideale. Die Faktorgruppe von I_k modulo der Untergruppe der Hauptideale heißt Ideal-Klassen-Gruppe.

4.6.2 Die Endlichkeit der Ideal-Klassen-Gruppe

Sei k ein Zahlenkörper. Dann ist die Ideal-Klassen-Gruppe endlich.

Beweis. Die Abbildung

$$J_k^1 \longrightarrow I_k$$

ist surjektiv (weil I_k von den nicht-archimedischen normalisierten Bewertungen erzeugt wird und jede dieser Bewertungen im Bild liegt).[37] Damit ist die Ideal-Klassen-Gruppe stetiges Bild der kompakten Gruppe J_k^1/k^*, also kompakt. Als diskrete kompakte Gruppe muß sie aber endlich sein.

QED.

---

[36] Das vollständige Urbild von

$$\sum_{v \text{ nicht-archimedisch}} n_v \bullet v$$

ist gerade

$$\prod_v \wp_v^{n_v} \cap J_k\ ,$$

wobei $\wp_v$ für jedes nicht-archimedische v das Bewertungsideal von $\mathfrak{O}_v$ und für archimedische Bewertungen v den Körper k_v bezeichne (wobei im letzterem Fall n_v=1 sei). Dies ist offensichtlich eine V_k- offene also auch J_k-offene Menge.

[37] Zu vorgegebenen v wähle man ein Idel α, dessen einzige von 1 verschiedene nicht-archimedische Koordinate die v-te sei und dessen v-te Koordinate ein Parameter von $\mathfrak{O}_v$ sei. Die endlich vielen archimedischen Koordinaten richte man so ein, daß der Inhalt von α gleich 1 wird. Dann ist α ein Urbild von v in der Gruppe J_k^1.

4.6.3 Die Gruppe der Divisoren im Funktionenkörper-Fall

Seien F ein endlicher Körper, t eine Unbestimmte und k eine endliche separable Erweiterung von F(t). Dann heißt die freie abelsche Gruppe

$$D_k := \{\sum_v n_v \bullet v \}$$

die von allen normalisierten Bewertungen von k erzeugt wird, Gruppe der Divisoren von k. Die Gruppe D_k besteht also aus den formalen ganzzahligen Linearkombinationen

$$\sum_v n_v \bullet v$$

der normalisierten Bewertungen von k, wobei die Anzahl der von Null verschiedenen Koeffizienten n_v endlich ist. Eine solche Linearkombination heißt auch Divisor von k.

Sind alle Koeffizienten nicht-negativ,

$$n_v \geq 0,$$

so heißt das Divisor auch effektiv. Bezeichne

$$d_v := [\kappa(v):F]$$

die Anzahl der Elemente des Restkörpers der Bewertung v. Diese Zahl heißt auch Grad des Divisors v. Allgemeiner ist der Grad eines beliebigen Divisors von k definiert als

$$\deg(\sum_v n_v \bullet v) := \sum_v n_v \bullet d_v.$$

Der Grad definiert einen Gruppen-Homomorphismus

$$\deg: D_k \longrightarrow \mathbb{Z},$$

und der Kern dieses Homomorphismus wird mit

$$D_k^0 := \mathrm{Ker}(\deg: D_k \longrightarrow \mathbb{Z})$$

bezeichnet.

Zu jedem Element $c \in k^*$ gehört ein Divisor

$$\mathrm{div}(c) = \sum_v \mathrm{ord}_v(c) \bullet v \in D_k$$

Man beachte, die Bewertungen des Funktionenkörpers k sind sämtlich nicht-archimedisch, sodaß für jedes v die zugehörige additive Bewertung ord_v wohldefiniert ist. Die Divisoren dieser Gestalt heißen Hauptdivisoren.

Bemerkungen

(i) Die Hauptdivisoren bilden offensichtlich eine Untergruppe von D_k.

(ii) Nach Definition besteht zwishen der zu v gehörigen multiplikativen Bewertung und der additiven Bewertung für jedes $c \in k$ die Relation

$$|c|_v = (\#\, k(v))^{-\mathrm{ord}_v c} = (\#F)^{-d_v \bullet \mathrm{ord}_v c} \qquad (1)$$

Für den zu $c \in k$ gehörigen Divisor

$$\mathrm{div}(c) = \sum_v \mathrm{ord}_v(c) \bullet v$$

gilt damit

$$\begin{aligned} -\deg \operatorname{div}(c) &= \sum_v -\operatorname{ord}_v(c)\bullet d_v = \log_{\#F}(\#F)^{-\sum_v d_v \bullet \operatorname{ord}_v c} \\ &= \log_{\#F} \prod_v (\#F)^{-d_v \bullet \operatorname{ord}_v c} \\ &= \log_{\#F} \prod_v |c|_v \\ &= \log_{\#F} 1 \\ &= 0. \end{aligned}$$

Wir haben gezeigt, die Hauptdivisoren bilden sogar eine Untergruppe von D_k^0.

(iii) Jedes Idel $\alpha = (\alpha_v)_v \in J_k$ definiert einen Divisor

$$\operatorname{div}(\alpha) = \sum_v \operatorname{ord}_v(\alpha_v)\bullet v \in D_k.$$

Wir haben damit einen Gruppen-Homomorphismus

$$\operatorname{div}: J_k \longrightarrow D_k, \alpha \mapsto \operatorname{div}(\alpha).$$

Wie im Fall des Homomorphismus $J_k \longrightarrow I_k$ von 4.6.1 sieht man, daß dieser Homomorphismus stetig ist, wenn man die Gruppe der Divisoren mit der diskreten Topologie versieht. Außerdem ist der Homomorphismus surjektiv, da sämtliche Divisoren der Gestalt $1\bullet v$ im Bild liegen.[38]

(iv) Dieselbe Rechnung wie in (ii) zeigt

$$\deg \operatorname{div}(\alpha) = 0 \Leftrightarrow \prod_v |\alpha_v|_v = 1 \Leftrightarrow c(\alpha) = 1.$$

Das vollständige Urbild von D_k^0 bei der Abbildung div ist somit gerade J_k^1. Wir erhalten damit eine stetige Surjektion

$$\operatorname{div}: J_k^1 \twoheadrightarrow D_k^0, \alpha \mapsto \operatorname{div}(\alpha).$$

4.6.4 Die Endlichkeit der Picard-Gruppe im Funktionenkörperfall

Sei k eine endliche separable Körpererweiterung eines Körpers der Gestalt F(t) mit F endlich. Dann isit die Faktorgruppe

$$\operatorname{Pic}_k^0$$

der Gruppe der Divisoren D_k^0 des Grades 0 modulo der Hauptdivisoren endlich.

Beweis. Auf Grund von Bemerkung 4.6.3 (iv) hat man eine stetige Surjektion

$$\operatorname{div}: J_k^1 \twoheadrightarrow D_k^0, \alpha \mapsto \operatorname{div}(\alpha).$$

Da die Hauptidele dabei gerade in die Hauptdivisoren übergehen, induziert diese eine stetige Surjektion

$$\operatorname{div}: J_k^1/k^* \twoheadrightarrow \operatorname{Pic}_k^0.$$

---

[38] Als Urbild wähle man ein Idel, dessen sämtliche Koordinaten außer der v-ten gleich 1 sind und dessen v-te Koordinate ein Parameter von $\mathcal{O}_v$ ist.

Mit J_k^1/k^* ist somit auch Pic_k^0 kompakt und damit (als diskrete kompakte Gruppe) sogar endlich.
QED.

4.7 Einheiten

In diesem Abschnitt wollen wir unsere Ergebnisse über Idel-Klassen verwenden, um den klassischen Dirichletschen Einheitensatz abzuleiten.

4.7.1 Einheitengruppen

Seien k ein globaler Körper und S eine nicht-leere endliche Mengen von normalisierten Bewertungen von k, welche sämtliche archimedischen Bewertungen enthält. Wir setzen

$$H_S := H_{S,k} := \{ c \in k \mid |c|_v = 1 \text{ für jedes } v \notin S\}.$$

Dies ist eine Untergruppe der multiplikativen Gruppe von k und heißt Gruppe der S-Einheiten von k.

Beispiel
Ist k ein Zahlenkörper und S die Menge der archimedischen Bewertungen von k, so ist H_S gerade die Einheitengruppe U des Rings $\mathcal{O}_k$ der ganzen Zahlen von k.

4.7.2 Die S-Einheiten mit Werten in einem kompakten Kreisring

Seien

$$k$$

ein globaler Körper,

$$S$$

eine endliche Menge von normalisierten Bewertungen von k, die alle archimedischen Bewertungen enthält, und c, C reelle Konstanten mit

$$0 < c \le C \ (< \infty).$$

Dann ist die Menge der S-Einheiten η von k mit

$$c \le |\eta|_v \le C \text{ für alle } v \in S$$

endlich.
Beweis. Betrachten wir die Menge von Idelen:

$$W := \{\alpha = (\alpha_v) \in J_k \mid |\alpha_v|_v = 1 \text{ für } v \notin S,\ c \le |\eta|_v \le C \text{ für } v \in S\}$$

Diese Menge ist als direktes Produkt kompakter Mengen kompakt. Die in der Behauptung betrachtete Menge ist gerade der Durchschnitt

$$W \bigcap k^*$$

von W mit der Menge $k^* \subseteq J_k$ der Hauptidele. Nun liegt k^* diskret in J_k (nach 4.5.3).

Als diskrete liegend Teilmengen der kompakten Menge W ist $W \bigcap k^*$ endlich: für jedes $x \in k^*$ gibt es eine offene Umgebung von x, welche außer x keinen weiteren Punkt von k^* enthält. Zu diesen offenen Mengen lassen sich weitere offene Mengen hinzufügen, welche disjunkt zu k^* sind, sodaß man eine offene Überdeckung von W erhält. Weil W kompakt ist, gibt es eine endliche Teilüberdeckung. Insbesondere ist $W \bigcap k^*$ endlich.
QED.

4.7.3 Elemente vom Betrag 1

Seien k ein globaler Körper. Dann ist die Menge der Elemente $\varepsilon \in k$ mit

$$|\varepsilon|_v = 1$$

für alle normalisierten Bewertungen v von k, endlich. Alle diese Elemente sind Einheitswurzeln.

Beweis. Für jede Einheitswurzel $\varepsilon \in k$ gilt trivialerweise $|\varepsilon|_v = 1$ für alle v. Wir wenden 4.7.2 mit beliebigem S und c = C = 1 an. Wir sehen so, die Menge

$$\{\varepsilon \in k \mid |\varepsilon|_v = 1 \text{ für alle } v\}$$

ist endlich. Nun ist diese Menge eine Untergruppe der multiplikativen Gruppe von k. Da ihre Ordnung endlich ist, besitzt jedes Element endliche Ordnung, ist also eine Einheitswurzel.
QED.

4.7.4 Einheitensatz von Dirichlet

Seien

$$k$$

ein globaler Körper unf

$$S$$

eine endliche Menge von normalisierten Bewertungen von k, die alle archimedischen Bewertungen enthält. Dann ist die Gruppe

$$H_S$$

der S-Einheiten von k das direkte Produkt aus einer endlichen zyklischen Gruppe und einer freien abelschen Gruppe vom Rang s -1 mit s := # S.
Beweis. Wir setzen

$$J_S := \{ \alpha = (\alpha_v)_v \in J_k \mid |\alpha_v|_v = 1 \text{ für jedes } v \notin S\}$$

und

$$J_S^1 := J_S \cap J_k^1.$$

Die Gruppe J_S^1 ist offen in J_k^1.[39] Weil die natürliche Abbildung auf die Faktorgruppe offen ist, ist damit auch

$$J_S^1/H_S = J_S^1/J_S^1 \cap k^* \text{ offen in } J_S^1/k^*.$$

Letztere Untergruppe ist als Komplement einer Vereinigung von Nebenklassen nicht nur offen, sondern auch abgeschlossen. Als abgeschlossene Teilmenge einer kompakten Menge ist sie damit kompakt,

$$J_S^1/H_S \text{ ist kompakt.}$$

Seien

$$v_1, \dots, v_s \in S$$

die Elemente von S. Betrachten wir die stetige Abbildung

$$\lambda: J_S \longrightarrow \mathbb{R}^S, \alpha \mapsto (\log |\alpha_{v_1}|_{v_1}, \dots, \log |\alpha_{v_s}|_{v_s}).$$

Es gilt

$$\mathrm{Ker}(\lambda|_{H_S}) = \{ \varepsilon \in k^* \mid |\varepsilon|_v = 1 \text{ für jedes } v \}$$

Diese Menge ist endlich nach 4.7.3, und damit - als Untergruppe der multiplikativen Gruppe eines Körpers[40] - eine endliche zyklische Gruppe,

---

[39] Auf Grund der Beschreibung von J_k^1 als eingeschränktes topologisches Produkt.

$$\mathrm{Ker}(\lambda|_{H_S}) \text{ ist eine endliche zyklische Gruppe.}$$

Zum Beweis der Behauptung reicht es somit zu zeigen[41], daß

$$\lambda(H_S) \text{ freie abelsche Gruppe vom Rang s-1} \qquad (1)$$

ist.

Nach 4.7.2 gibt es nur endlich viele $\eta \in H_S$ mit

$$\frac{1}{2} \le |\eta|_v \le 2 \text{ für alle } v \in S$$

Deshalb ist die additive Untergruppe

$$\Lambda := \lambda(H_S)$$

eine diskrete Untergruppe[42] der additiven Gruppe $\mathbb{R}^S$ und damit frei[43] vom Rang $\le s$

---

[40] Siehe den Beweis für die Tatsache, daß die multiplikative Gruppe eines endlichen Körpers zyklisch ist.

[41] denn die exakte Sequenz

$$0 \longrightarrow \mathrm{Ker}(\lambda|_{H_S}) \longrightarrow H_S \longrightarrow \mathbb{Z}^{s-1} \longrightarrow 0$$

zerfällt dann (weil der $\mathbb{Z}$-Modul rechts projektiv ist).

[42] Man ersetze die Kleiner-Gleichzeichen durch Kleiner-Zeichen und gehe zum Logarithmus über, um eine eine offene Menge Umgebung der Null zu erhalten, die nur endlich viele Punkte von Λ enthält.

[43] Seien $G \subseteq \mathbb{R}^S$ diskrete Untergruppe der additiven Gruppe von $\mathbb{R}^S$ und V der von G erzeugte $\mathbb{R}$-lineare Unterraum. Dann ist G eine direkte Summe von d = dim V Exeamplaren von $\mathbb{Z}$.
Der Beweis erfolgt durch Induktion nach d := dim V.

Im Fall d = 0 ist nichts zu beweisen. Sei also d > 0. Wir wählen ein reelles $\varepsilon>0$ derart, daß

$$U_\varepsilon(0) \subseteq V$$

nur den Null-Vektor mit G gemeinsam hat. In der abgeschlossenen Menge $V - U_\varepsilon(0)$ wähle man ein $v_1 \in G$, welches minimalen Abstand vom Ursprung hat. Dann besteht

$$G \cap \mathbb{R}v_1 = \mathbb{Z}v_1$$

gerade aus den ganzzahligen Vielfachen von v_1 (denn andernfalls könnte man einen Vektor mit noch kleinerer Länge in G finden). Wir betrachten das Bild $\overline{G}$ von G bei der natürlichen Abbildung auf den Faktorraum von V modulo $\mathbb{R}v_1$,

$$V \longrightarrow V/\mathbb{R}v_1 =: \overline{V} \supseteq \overline{G}.$$

Es reicht zu zeigen, $\overline{G}$ ist eine diskrete Untergruppe von $\overline{V}$, denn dann gilt $\overline{G} \cong \mathbb{Z}^{d-1}$ und man hat eine exakte Sequenz

$$0 \longrightarrow G \cap \mathbb{R}v_1 \longrightarrow G \longrightarrow \mathbb{Z}^{d-1} \longrightarrow 0,$$

die wegen der Freiheit der Gruppe rechts zerfällt, d.h. es gilt

$$G \cong \mathbb{Z}^{d-1} \oplus G \cap \mathbb{R}v_1 = \mathbb{Z}^{d-1} \oplus \mathbb{Z} = \mathbb{Z}^d.$$

Angenommen,

$$\overline{G} = G/G\cap\mathbb{R}_{v_1} = G/v\mathbb{Z}_1$$

ist keine diskrete Untergruppe von $\overline{V}$. Dann gibt es in $\overline{G}$ eine Folge von Vektoren, die ungleich Null sind und gegen Null konvergieren. Wir gehen zu den Repräsentante in G über und erhalten Folge $\{u_n\}_{n=1,2,..}$ und $\{c_n\}_{n=1,2,..}$ mit

$$\Lambda \cong \mathbb{Z}^t \text{ mit } t \leq s.$$

Weil der Inhalt der Elemente von H_S ($\subseteq k^*$) gleich 1 ist (nach dem Produktsatz 4.2.3), liegt das Bild Λ von H_S in der Hyperebene

$$H := \{ (x_1, ..., x_s) \in \mathbb{R}^s \mid x_1 + ... + x_s = 0\}$$

mit der Gleichung $x_1 + ... + x_s = 0$ (vgl. die Bemerkungen 4.6.3 (ii) und (iv)),

$$\Lambda \subseteq H.$$

Deshalb gilt

$$t \leq s\text{-}1.$$

Zum Beweis der Behauptung des Satzes reicht es zu zeigen, daß sogar das Gleichheitszeichen gilt. Dazu reicht es zu zeigen,

$$H/\Lambda \text{ ist kompakt.}^{44}$$

<u>Spezialfall</u>: $\mathbb{Q} \subseteq k$ und S = die Menge der archimedischen Bewertungen von k.
Die Abbildung

$$\lambda: J_S \longrightarrow \mathbb{R}^s, \alpha \mapsto (\log |\alpha_{v_1}|_{v_1}, ... , \log |\alpha_{v_s}|_{v_s}).$$

ist dann surjektiv (weil jede positive reelle Zahl als Absolutbetrag auftriit).
Die Bewertungen, die in der Definition der Abbildung λ vorkommen, sind sämtlich archimedisch. Alle übrigen Bewertungen haben auf J_S^1 konstant den Wert 1. Gibt man die Werte aller archimedischen Bewertunge mit einer Ausnahme beliebig vor, so gibt es zu diesen Vorgaben ein Element aus J_S^1. Der Wert der verbleibenden archimedischen Bewertung ist durch die Bedingung, daß der Inhalt gleich 1 sein soll, festgelegt. Das bedeutet, es gilt

$$\lambda(J_S^1) = H.$$

Damit induziert λ eine stetige Surjektion

$$J_S^1/H_S \twoheadrightarrow H/\lambda(H_S) = H/\Lambda.$$

Da der Raum links kompakt ist, gilt dasselbe auch für den Raum rechts.

$u_n \in G \subseteq V$, $u_n \notin \mathbb{R}v_1$, $c_n \in \mathbb{Z}$, und $u_n - c_n v_1 \longrightarrow 0$.

(d.h. die Folge der Projektionen auf die zu $\mathbb{R}v_1$ komplementäre Hyperebenen geht gegen Null). Für alle n gilt dann

$$0 \neq u_n - c_n v_1 \in G$$

und für hinreichend großes n ist

$$u_n - c_n v_1 \in U_\varepsilon(0).$$

Das steht aber im Widerspruch zu $\varepsilon > 0$.

[44] Bezeichne V den von Λ erzeugten reellen Vektorraum. Dann gilt

$$H = V \times \mathbb{R}^{s-1-t},$$

also

$$H/\Lambda = V/\Lambda \times \mathbb{R}^{s-1-t}.$$

Im Fall $t < s-1$ ist diese Menge nicht kompakt.

Allgemeiner Fall.

Im allgemeinen Fall können einige der in der Definition von λ auftretenden Bewertungen nicht-archimedisch sein. Das Bild von J_S bei λ hat dann die Gestalt[45]

$$\lambda(J_S) \cong \mathbb{R}^u \times \mathbb{Z}^v \text{ mit } u+v = s-1.$$

Die Abbildung φ induziert eine stetige Surjektion

$$J_S^1/H_S \twoheadrightarrow \mathbb{R}^u \times \mathbb{Z}^v/\lambda(H_S) = \mathbb{R}^u \times \mathbb{Z}^v/\Lambda,$$

d.h der Raum $\mathbb{R}^u \times \mathbb{Z}^v/\Lambda$ ist kompakt. Wir betrachten die Projektion auf den zweiten Faktor,

$$p: \mathbb{R}^u \times \mathbb{Z}^v \twoheadrightarrow \mathbb{Z}^v.$$

Diese induziert eine stetig Surjektion

$$\mathbb{R}^u \times \mathbb{Z}^v/\Lambda \twoheadrightarrow \mathbb{Z}^v/p(\Lambda).$$

Da links ein Kompaktum steht, gilt dasselbe auch für die Gruppe rechts. Da letztere diskret ist, muß sie endlich sein. Nach dem Elementarteilersatz gilt[46]

$$p(\Lambda) \cong \mathbb{Z}^v.$$

Wir erhalten damit eine exakte Sequenz[47]

$$0 \longrightarrow \Lambda \bigcap \mathbb{R}^u \times 0 \longrightarrow \Lambda \longrightarrow \mathbb{Z}^v \longrightarrow 0,$$

d.h. es ist

$$\Lambda \cong \mathbb{Z}^v \oplus \Lambda \bigcap \mathbb{R}^u.$$

Es reicht also zu zeigen,

$$\Lambda \bigcap \mathbb{R}^u \cong \mathbb{Z}^u.$$

Weil Λ diskret ist in $\mathbb{R}^u \times \mathbb{Z}^v$ ist $\Lambda \bigcap \mathbb{R}^u$ eine diskrete Untergruppe von $\mathbb{R}^u$. Es reicht zu zeigen,

$$\mathbb{R}^u/\Lambda \bigcap \mathbb{R}^u \text{ ist kompakt.} \qquad (2)$$

Zum Beweis betrachten wir das folgende kommutative Diagramm von stetigen Gruppen-Homomorphismen.

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & \mathbb{R}^u/\Lambda \bigcap \mathbb{R}^u & \longrightarrow & \mathbb{R}^u \times \mathbb{Z}^v/\Lambda & \longrightarrow & \mathbb{Z}^v/\Lambda & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & \mathbb{R}^u & \xrightarrow{q} & \mathbb{R}^u \times \mathbb{Z}^v & \xrightarrow{p} & \mathbb{Z}^v & \longrightarrow & 0 \\
 & & \cup & & \cup & & \cup & & \\
0 & \longrightarrow & \Lambda \bigcap \mathbb{R}^u & \longrightarrow & \Lambda & \longrightarrow & \Lambda/\Lambda \bigcap \mathbb{R}^u & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

---

[45] Die archimedischen Bewertungen nehmen jeden reellen Wert an, die Werte jeder der nicht-archimedischen Bewertungen sind gannnahlige Potenzen einer festen reellen Zahl aus (0,1). Die Gruppe der Werte ist somit isomorph zu $\mathbb{Z}$.

[46] $p(\Lambda)$ ist das Bild einer $\mathbb{Z}$-linearen Abbildung $\mathbb{Z}^v \longrightarrow \mathbb{Z}^v$ und die Elementarteiler der Matrix dieser Abbildung sind sämtlich von Null verschieden.

[47] Der Kern von p ist gleich $\mathbb{R}^u \times 0$.

Dabei bezeiche die Abbildung q in der mittleren Zeile die natürliche Einbettung des ersten Faktors. Die untere Zeile entstehe aus der mittleren durch Einschränken auf Λ. Die vertikalen Zeilen seien durch die Forderung, daß sie exakt sein sollen, definiert. Nach dem 3×3-Lemma ist dann auch die obere Zeile exakt. Insbesondere ist damit (2) als Kern eines stetigen Homomorphismus ein abgeschlossener Unterraum des Kompaktums $\mathbb{R}^u \times \mathbb{Z}^v/\Lambda$, also kompakt.s
QED.

Bemerkungen

(i) Der Einheitensatz von Dirichlet und die Endlichkeit der Zahl der Idealklassen (Minkovskij) waren lange vor der Einführung des Begriffs des Idels bekannt. Bekannter als die hier angeführten Beweise ist die Ableitung der Kompaktheit der Idel-Klassen-Gruppe aus diesen beiden Sätze.

(ii) Wir beschließen dieses Kapitel mit der Verallgemeinerung des Normbegriffs auf den Fall von Adelen, Idelen und Idealen.

4.7.5 Die Konorm

Seien k ein globaler Körper und

$$K/k$$

eine endliche separable Körper-Erweiterung. Nach 4.4.2 besteht dann ein natürlicher Isomorphismus

$$V_k \otimes_k K \longrightarrow V_K$$

im topologischen und im algebrarischen Sinne. Insbesondere kann man V_k als Teilring von V_K ansehen, welcher abgeschlossenen ist in der Topologie von V_K.[48] Wir führen für die natürliche Einbettung die Bezeichnung

$$con = con_{K/k}: V_k \longrightarrow V_K$$

ein und nenne sie auch Konorm-Abbildung. Nach Definition gilt für jede normalisierte Bewertung V von K, welche über der normalisierten Bewertung v von k liegt,

$$con(\alpha)_V = \alpha_v \in k_v \subseteq K_V.$$

Dabei bezeichne k_v wie bisher die Vervollständigung von k bezüglich v und K_V die von K bezüglich V.

Bemerkung

(i) Für globale Körper k und endliche separable Körper-Erweiterungen

$$k \subseteq K \subseteq L$$

gilt

$$con_{L/k} = con_{L/K} \circ con_{K/k}$$

4.7.6 Norm und Spur von Adelen

Seien k ein globaler Körper und

$$K/k$$

eine endliche separable Körper-Erweiterung. Wir fixieren eine k-Vektorraum-Basis von K über k, sagen wir

$$K = k\bullet\omega_1 + ... + k\bullet\omega_n \text{ , } n := [K:k].$$

---

[48] Mit n := [K:k] kann man V_K als die Menge der n-Tupel mit Koordinaten aus V_k ansehen. V_k erhält man damit aus V_K, indem man n-1 Koordinaten gleich Null setzt.

Wegen des Isomorphísmus $V_k \otimes_k K \longrightarrow V_K$ läßt sich dann jedes Adel $A \in V_K$ auf genau eine Weise in der folgenden Gestalt schreiben.

$$A = \sum_{j=1}^{n} \alpha_j \omega_j \text{ mit } \alpha_j \in V_k.$$

Entsprechend haben auch die Produkte $A\omega_i$ eine Darstellung

$$A\omega_i = \sum_{j=1}^{n} \alpha_{ij} \omega_j$$

mit eindeutig bestimmten Adelen

$$\alpha_{ij} = \alpha_{ij}(A) \in V_k.$$

Wir setzen

$$S(A) = S_{K/k}(Á) := \sum_{i=1}^{n} \alpha_{ii} \in V_k$$

und

$$N(A) = N_{K/k}(Á) := \det(\alpha_{ij}) \in V_k$$

und nennen S(A) Norm des Adels A und S(A) die Spur des Adels A über V_k.

Bemerkungen

(i) Die n×n-Matrix $(\alpha_{ij}(A))$ hängt in stetiger Weise von $A \in V_k$ ab und die Adele

$$S(A), N(A) \in V_k$$

sind unabhängig von der speziellen Wahl der Basis $\omega_1, \ldots, \omega_n$ von K über k und hängen in stetiger Weise von A ab.

(ii) $S_{K/k}(A'+A'') = S_{K/k}(A') + S_{K/k}(A'')$ für $A', A'' \in V_K$.

(iii) $S_{K/k}(\mathrm{con}_{K/k}\, \alpha) = [K:k] \bullet \alpha$ für $\alpha \in V_k$.

(iv) $N_{K/k}(A'A'') = N_{K/k}(A') \bullet N'_{K/k}(A'')$ für $A', A'' \in V_K$.

(v) $N_{K/k}(\mathrm{con}_{K/k}\, \alpha) = \alpha^{[K:k]}$

(vi) Transitivität. Für globale Körper k und endliche separable Erweiterungen

$$k \subseteq K \subseteq L$$

gilt

$$S_{L/k}(A) = S_{K/k}(S_{L/K}(A))$$

und

$$N_{L/k}(A) = N_{K/k}(N_{L/K}(A)).$$

(vii) Komponentenweise Beschreibung von Spur und Norm I. Seien

$$V_1, \ldots, V_r$$

die normalisierten Bewertungen von K über der normalisierten Bewertung v von k. Wir schreiben dann

$$K_v := K_{V_1} \omega_1 + \ldots + K_{V_r} \omega_r = K_{V_1} \times \ldots \times K_{V_r} = k_v \otimes_k K,$$

wobei K_{V_i} die Vervollständigung von K bezüglich V_i und k_v die von k bezüglich v bezeichne. Die Elemente

$$A \in V_K$$

kann man dann als Familien von Elementen aus den K_v ansehen,

$$A = \{A_v\}_v \text{ mit } A_v \in K_v$$

Für Norm und Spur erhält man dann

$$S_{K/k}(A) = \{S_{K_v/k_v}(A_v)\}_v$$

$$N_{K/k}(A) = \{N_{K_v/k_v}(A_v)\}_v .$$

Dabei seien S_{K_v/k_v} und N_{K_v/k_v} gerade Norm und Spur der endlich erzeugten freien k_v-Algebra K_v.(vgl. 1.7.2).

(viii) Komponentenweise Beschreibung von Spur und Norm II. Für jedes Adel $A = (A_V)_V \in V_k$ gilt

$$S_{K/k}(A) = \{ \sum_{V|v} S_{K_V/k_v}(A_V)\}_v$$

$$N_{K/k}(A) = \{ \prod_{V|v} N_{K_V/k_v}(A_V)\}_v .$$

Die Summen und Produkte rechtes werden dabei über alle normalisierten Bewertungen V von K erstreckt, die über der normalisierten Bewertung v von k liegen.

Beweis. Zu (i). Die Unabhängigkeitsaussage wird in derselben Weise bewiesen, wie die Unabhängigkeitsaussage im Fall der Körpernorm für K/k.[49] Zum Beweis der Stetigkeitsaussage reicht es zu zeigen, die Abbildungen

$$\alpha_{ij} : V_K \longrightarrow V_k , A \mapsto \alpha_{ij}(A),$$

sind stetig. Das ist aber der Fall, weil die Multiplikation mit A eine stetige Abbildung

$$V_K \xrightarrow{A} V_K$$

ist und die Projektion auf die erste Koordinate $V_K \longrightarrow V_k$ ebenfalls stetig ist.

Zu (ii). Die Behauptung ergibt sich unmittelbar aus der Definition der Spur.

Zu (iii). Die Matrix der Multiplikation mit einem Element $\alpha \in V_k$ ist eine n×n-Diagonal-Matrix mit n = [K:k], deren Einträge auf der Hauptdiagonalen sämtlich gleich α sind.

Zu (iv).Die Behauptung ergibt sich unmittelbar aus der Definition der Norm: der Zusammensetzung der beiden Multiplikationen mit A' und A" entspricht das Produkt der beiden Matrizen zur Multiplikation mit A' und A". Die Determinante dieses Produkts ist aber gleich dem Produkt der beiden Determinanten.

Zu (v). Man verwendet dieselbe Argumentation wie beim Beweis von (iii).

Zu (vi). Die Behauptung ist ein Spezialfall der allgemeinen Transitivitätsaussage 1.7.7.

---

[49] d.h. man wähle zwei verschiedene Basen von K über k und zeige, daß die zu diesen Basen gehörigen charakteristischen Polynome übereinstimmen: das ist so, weil die beiden zu diesen Basen gehörigen Matrizen für die Multiplikation mit einem Element konjugiert sind und die Determinante sich beim Komjugieren nicht ändert.

Zu (vii). Man betrachte in der Definitioin von $S_{K/k}$ und $N_{K/k}$ die Komponenten zu den Bewertungen über einem festen v und fasse diese zusammen.
Zu (viii). Nach (vii) reicht es zu zeigen,

$$S_{K_v/k_v}(A_v) = S_{K_{V_1}/v}(A_{V_1}) + \ldots + S_{K_{V_r}/v}(A_{V_r})$$

und

$$N_{K_v/k_v}(A_v) = N_{K_{V_1}/v}(A_{V_1}) \bullet \ldots \times N_{K_{V_r}/v}(A_{V_r}))$$

wenn $V_1, \ldots, V_r$ die über v liegenden normalisierten Bewertungen von K sind.
Da die Multiplikation mit

$$A_v = (A_{V_1}, \ldots, A_{V_r})$$

in $K_v = K_{V_1} \times \ldots \times K_{V_r}$ koordinatenweise erfolgt, ist zerfällt die Matrix dieser Multiplikation in eine Diagonal-Matrix von Blöcken, wobei der i-te Block auf der Hauptdiagonalen gerade die Matrix der Multiplikation mit A_{V_i} ist. Für Spur und Determinante dieser Matrix erhält man damit gerade die angegebene Summe bzw. das angegebene Produkt.
QED.

4.7.7 Die Norm von Idelen

Seien k ein globaler Körper und

$$K/k$$

eine endliche separable Körper-Erweiterung. Aus der Definition der Konorm in 4.7.5 ergibt sich, daß die Konorm eines Idels stets ein Idel ist, d.h. die Konorm für Adele definiert eine Abbildung

$$con = con_{K/k}: J_k \longrightarrow J_K .$$

welche ebenfalls Konorm heißt. Diese ist ein Gruppen-Homomorphismus, welcher ein Homöomorphismus von J_k mit einer abgeschlossenen Untergruppe von J_K ist.
Auf Grund der Multiplikativität der Adele Norm (Bemerkung 4.7.6 (iv)) ist die Norm eines Idels stets ein Idel. Die Adele-Norm definiert also eine stetige Abbildung

$$N = N_{K/k}: J_K \longrightarrow J_k.$$

welche Norm heißt. Diese ist eine stetige Abbildung mit

(i) $N_{K/k}(A'A'') = N_{K/k}(A') \bullet N'_{K/k}(A'')$ für $A', A'' \in J_K$.

(ii) $N_{K/k}(con_{K/k}\, a) = a^{[K:k]}$ für $a \in V_k$.

(iii) $N_{L/k}(A) = N_{K/k}(N_{L/K}(A))$ für Körpertürme $k \subseteq K \subseteq L$ endlicher separabler Erweiterungen und $A \in J_K$.

(iv) $N_{K/k}(A) = \{N_{K_v/k_v}(A_v)\}_v$ für $A \in J_K$.

(v) $N_{K/k}(A) = \{\prod_{V|v} N_{K_V/k_v}(A_V)\}_v$ für $A \in J_K$.

4.7.8 Die Norm von Idealen

Seien k ein Zahlenkörper (d.h. eine endliche Körpererweiterung von $\mathbb{Q}$) und
K/k
eine endliche Körpererweiterung. Der Kern des Homomorphismus

$$J_k \longrightarrow I_k \tag{1}$$

der Idele-Gruppe in die Gruppe der Ideale (vgl. 4.6.1) ist gerade die Untergruppe

$$U_k := \{ \alpha = (\alpha_v)_v \in J_k \mid |\alpha_v|_v = 1 \text{ für v nicht-archimedisch}\}$$

der Idele mit dem Wert 1 für alle nicht-archimedischen Bewertungen v von k. Für jede über v liegende normalisierte Bewertung V von K gilt

$$|A_V|_V = |\sqrt[n]{N_{K_V/k_v}(A_V)}|_v \text{ mit } n := [K_V:k_v] \tag{2}$$

(nach 2.3.8). Insbesondere gilt[50]

$$con_{K/k}(U_k) \subseteq U_K.$$

Zusammen mit 4.7.7 (iv) ergibt sich weiter[51]

$$N_{K/k}(U_K) \subseteq U_k .$$

Konorm und Norm definieren somit Homomorphismen

$$con_{K/k} : J_k/U_k \longrightarrow J_K/U_K \text{ und } N_{K/k}: J_K/U_K \longrightarrow J_k/U_k.$$

Weil (1) surjektiv ist und den Kern U_k hat, können wir diese Abbildungen auch als Homomorphismen

$$con_{K/k} : I_k \longrightarrow I_K \text{ und } N_{K/k}: I_K \longrightarrow I_k$$

auffassen. Wir haben damit Konorm und Norm für die Ideal-Gruppen konstruiert. Diese sind verträglich mit der Konorm und der Norm für Elemente aus K und k, wenn man diese als Hauptideale ansieht (vgl. 4.7.7.(v) und 3.2.3).

Bemerkungen

(i) Für jede normalisierte Bewertung $v \in I_k$ von k gilt

$$con_{K/k}(v) = \sum_{V|v} e_V \cdot V$$

Dabei werde die Summe rechts über alle normalisierten Bewertungen V von K über k erstreckt und

$$e_V = e(V|v)$$

bezeichne den Verzweigungsindex von V über v.

(ii) Für jede normalisierte Bewertung $V \in I_K$ von K, welche über $v \in I_k$ liegt, gilt

$$N_{K/k}(V) = f_V v$$

---

[50] Man nehme in (2) an, A_V liegt in k_v und hat dort den Wert 1. Die Konjugierten von A_V sind alle gleich A_V. Formel (2) bekommt so die Gestalt

$$|A_V|_V = |A_V|_v = 1.$$

[51] Mit $|A_V|_V = 1$ gilt nach (2) auch $|N_{K/k}(A_V)|_v = 1$. Die $N_{K/k}(A_V)$ sind aber nach 4.7.7 (iv) gerade die Komponenten von $N_{K/k}(A)$.

Beweis. Zu (i). Betrachten wir das folgende Urbild $\alpha \in J_k$ von v in I_k ,

$$\alpha = (\alpha_{v'})_v, \text{ mit } \alpha_{v'} = \begin{cases} \pi_v & \text{für } v'=v \\ 1 & \text{sonst} \end{cases} .$$

Dabei sei π_v ein Parameter der Bewertung v. Für jede über v liegende normalisierte Bewertung V von K gilt dann

$$ord_V(\alpha_v) = ord_V(\pi_v) = e_V \cdot ord_v(\pi_v) = e_V \cdot 1 = e_V.$$

Ist V' eine Bewertung von K, welche über der Bewertung v' $\neq$ v von k liegt, so gilt

$$ord_{V'}(\alpha_{v'}) = ord_{V'}(1) = 0.$$

Zusammen erhalten wir die behauptete Identität.

Zu (ii). Wir repräsentieren $V \in I_K$ durch das Ideal $\alpha = (\alpha_{V'})_V \in J_K$ mit

$$\alpha_{V'} = \begin{cases} \Pi_V & \text{für } V'=V \\ 1 & \text{sonst} \end{cases} .$$

Dabei bezeichne Π_V einen Parameter der Bewertung V. Betrachten wir

$$N_{K/k}(\alpha) = \{ \prod_{V'|v} N_{K_{V'}/k_v}(\alpha_{V'}) \}_v,$$

Liegt V' nicht über v, so gilt $\alpha_{V'} = 1$, also $N_{K_{V'}/k_v}(\alpha_{V'}) = 1$, d.h. die entsprechende Komponente von $N_{K/k}(\alpha)$ ist 1. Damit erhalten wir

$$N_{K/k}(V) = ord_v \prod_{V'|v} N_{K_{V'}/k_v}(\alpha_{V'}) \cdot v.$$

Für V' $\neq$ V ist $\alpha_{V'} = 1$, also $N_{K_{V'}/k_v}(\alpha_{V'}) = 1$. Wir erhalten

$$N_{K/k}(V) = ord_v N_{K_V/k_v}(\Pi_V) \cdot v. \qquad (1)$$

Sei π_v ein Parameter von v. Dann ist $\pi_v = u \cdot \Pi_V^{eV}$ mit einer Einheit u von K_V. Es folgt

$$\pi_v^{[K_V:k_v]} = N_{K_V/k_v}(\pi_v) = N_{K_V/k_v}(u) \cdot N_{K_V/k_v}(\Pi_V)^{eV}$$

also

$$ord_v(\pi_v^{[K_V:k_v]}) = ord_v(N_{K_V/k_v}(u) \cdot N_{K_V/k_v}(\Pi_V)^{eV}).$$

Weil die Norm einer Einheit, eine Einheit ist, folgt

$$[K_V:k_v] \cdot ord_v(\pi_v) = e_V \cdot ord_v(N_{K_V/k_v}(\Pi_V)),$$

also

$$ord_v(N_{K_V/k_v}(\Pi_V)) = [K_V:k_v]/e_V = f_V$$

(vgl. 3.3.7). Einsetzen in (1) liefert die Behauptung.
QED.

4.7.9 Bemerkung zum Funktionenkörperfall

Im Funktionenkörperfall werden Konorm und Norm eines Divisors in analoger Weise definiert und die entsprechenden Eigenschaften bewiesen.

5. Kreisteilungskörper und Kummer-Erweiterungen

5.1. Kreisteilungskörper

5.1.1 Primitive Einheitswurzeln und der Körper $K(\sqrt[m]{1})$

Seien K ein Körper der Charakteristik Null,

$$\mathrm{char}(K) = 0$$

und

$$m > 1$$

eine natürliche Zahl.
Dann existiert eine minimale Körpererweiterung

$$L/K,$$

über welcher das Polynom

$$x^m - 1 \qquad (1)$$

in Linearfaktoren zerfällen (der Zerfällungskörper dieses Polynom).

Die Nullstellen des Polynoms (1) bilden eine Untergruppe der multiplikativen Gruppe L* des Körper L. Als endliche Untergruppe der multiplikativen Gruppe eines Körpers ist diese Gruppe zyklisch. Die Erzeugenden dieser Gruppe heißen primitive m-te Einheitswurzeln.
Ist ζ eine primitive m-te Einheitswurzel, so ist jede Nullstelle von (1) eine Potenz von ζ, d.h.

$$L = K(\zeta)$$

ist eine normale Körpererweiterung. Wir werden auch die folgende Bezeichung für den Körper L verwenden.

$$L = K(\sqrt[m]{1}).$$

Eine Nullstelle ζ^a von (1) ist genau dann primitive Einheitswurzel, wenn der Exponent teilerfremd zu m ist,

$$\zeta^a \text{ primitiv} \Leftrightarrow (a, m) = 1.$$

Der Exponent a ist durch ζ^a modulo m eindeutig bestimmt. Es besteht deshalb eine Bijektion

$$G(m) \longrightarrow \{\text{primitive m-te Einheitswurzeln }\},\ a \bmod m \mapsto \zeta^a.$$

Dabei bezeichne

$$G(m) := (\mathbb{Z}/m\mathbb{Z})^*$$

die Gruppe der primen Restklassen modulo m (d.h. die multiplikative Gruppe des Rings der Restklassen modulo m).

5.1.2. Die Galois-Gruppe von $K(\sqrt[m]{1})/K$

Seien K ein Körper der Charakteristik Null, m > 1 eine natürliche Zahl, ζ eine primitive m-te Einheitswurzel und

$$L = K(\zeta) = K(\sqrt[m]{1})$$

Für jedes Element

$$\sigma \in G(L/K)$$

der Galois-Gruppe von L/K ist dann $\sigma(\zeta) = \zeta^a$ wieder eine primitive m-te Einheitswurzel, d.h. a ist teilerfremd zu m. Wir erhalten so eine injektive Abbildung

$$G(L/K) \longrightarrow G(m),\ \sigma \mapsto a \text{ mit } \zeta^a = \sigma(\zeta), \qquad (1)$$

Ist $\tau \in G(L/K)$ ein weiteres Element der Galois-Gruppe und $\tau(\zeta) = \zeta^b$, so gilt

$$\tau(\sigma(\zeta)) = \tau(\zeta^a) = \tau(\zeta)^a = \zeta^{ab}.$$

Der Zusammensetzung von Abbildungen in der Galois-Gruppe entspricht also das Produkt der Bilder bei (1), Mit anderen Worten, (1) ist ein Gruppen-Homomorphismus. Wir können die Galois-Gruppe als Untergruppe der Gruppe der primen Restklassen modulo m auffassen,

$$G(L/K) \subseteq G(m).$$

5.1.3 Reduktion auf den Fall, daß m eine Primzahlpotenz ist

Seien K ein Körper der Charakteristik Null, m > 1 eine natürliche Zahl, ζ eine primitive m-te Einheitswurzel und

$$L = K(\zeta) = K(\sqrt[m]{1})$$

Weiter sei

$$m = rs \text{ mit r und s teilerfrem.}$$

Dann gibt es ganze Zahlen a und b mit

$$ar + bs = 1.$$

Insbesondere ist

$$\zeta = (\zeta^r)^a(\zeta^s)^b,$$

also

$$K(\zeta) = K(\zeta^r, \zeta^s),$$

d.h. die Erweiterung $K(\zeta)$ ist gerade die Komposition der Erweiterungen $K(\zeta^r)$ und $K(\zeta^s)$. Dabei ist ζ^r eine s-te und ζ^s eine r-te primitive Einheitswurzel.
Man kann deshalb in vielen Situationen die Untersuchung der Erweiterung

$$K(\sqrt[m]{1})/K$$

auf den Fall reduzieren, daß m eine Primzahlpotenz ist.

$$m = p^n \text{ , p Primzahl.}$$

5.1.4 Die Gruppe $G(p^n)$

Seien p eine Primzahl, n eine natürliche Zahl und

$$G(p^n) := (\mathbb{Z}/m\mathbb{Z})^*$$

die Gruppe der primen Restklassen modulo p^n. Dann gilt:

(i) $G(p^n)$ ist zyklisch im Fall $p \neq 2$.

(ii) $G(2^n) = \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}} = \langle \overline{-1}, \overline{5} \rangle$ ist direktes Produkt einer zyklischen Gruppe der Ordnung 2, die von der Restklasse von -1 erzeugt wird und einer zyklischen Gruppe der Ordnung 2^{n-2}, die von der Restklasse von 5 erzeugt wird.

Beweis. (vgl. H. Hasse: Zahlentheorie, Verlag der Wissenschaften, 1963, Kapitel I, §4, Abschnitt 5). 1. Schritt. Eine Produktzerlegung von $G(p^n) = U(n)\times V(n)$.
Eine Restklasse von $\mathbb{Z}/m\mathbb{Z}$ ist genau dann eine Einheit, wenn sie durch eine zu $m = p^n$ teilerfremde Zahl repräsentier wird. Die nicht zu p^n teilerfremden ganzen Zahlen im Intervall $[0, p^n]$ sind

$$p, 2p, 3p, \ldots p^{n-1}p$$

Ihre Anzahl ist p^{n-1}, also gilt

$$\# G(p^n) = \varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1).$$

Weil p^{n-1} und p-1 teilerfremd sind, zerfällt $G(p^n)$ in ein direktes Produkt[52]

$$G(p^n) = U(n)\times V(n) \qquad (1)$$

mit

$$\#U(n) = p^{n-1} \text{ und}$$
$$\#V(n) = p - 1.$$

Es gilt[53]

$$U(n) := \{x \in G(p^n\} \mid x^{p^{n-1}} = 1 \} \qquad (2)$$
$$V(n) := \{x \in G(p^n\} \mid x^{p-1} = 1 \}$$

Wir betrachten die Homomorphismen

$$\alpha: G(p^n) \longrightarrow G(p^n),\ x \mapsto x^{p-1},$$
$$\beta: G(p^n) \longrightarrow G(p^n),\ x \mapsto x^{p^{n-1}}.$$

Nach (2) gilt

$$\mathrm{Im}(\alpha) \subseteq U(n),\ \mathrm{Im}(\beta) = V(n).$$

Außderdem hat die Einschränkung von α auf U(n) einen trivialen Kern (weil p-1 teilerfremd zur Ordnung von U(n) ist) und analog hat die Einschränkung von β auf V(n) einen trivialen Kern. Weil die beteiligten Gruppen endlich sind, sind diese Einschränkungen Isomorphismen,

---

[52] Nach dem Hauptsatz über endlich erzeugte abelsche Gruppe ist $G(p^n)$ direktes Produkt zykischer Gruppe von Primzahlpotenzordnung. Das direkte Produkt der direkten Summanden von p-Potenzordnung sei U(n). Die übrigen Primzahlpotenzen sind teilerfremd zu p, also ein Teiler von p-1. Des direkte Produkt der zugehörigen direkten Faktoren sei V(n). Wir erhalten eine Zerlegung

$G(p^n) = U(n) \times V(n)$
mit

u := #U(n) = eine p-Potenz
v := #V(n) = eine zu p teilerfremde natürlich Zahl
$uv = p^{n-1}(p-1)$.

Dann gilt aber $u = p^{n-1}$ und v = p-1.

[53] Auf Grund der Ordnungen dieser Gruppen gilt trivialerweise '$\subseteq$'. Sei umgekehrt

$$x = yz,\ y \in U(n),\ z \in V(n)$$

ein Element dessen Ordnung die Zahl p^{n-1} teilt. Dann gilt

$$1 = x^{p^{n-1}} = y^{p^{n-1}} v^{p^{n-1}} = v^{p^{n-1}}.$$

Weil p^{n-1} teilerfremd zur Ordnung von v ist, folgt v = 1, d.h. x liegt in U(n). Damit gilt der erste der beiden behaupteten Gleichheitszeichen. Das zweite wird analog bewiesen.

$$\alpha|_{U(n)} : U(n) \xrightarrow{\cong} U(n),\ \beta|_{V(n)} : V(n) \xrightarrow{\cong} V(n).$$

Insbesondere ist

$$\mathrm{Im}(\alpha) = U(n) \text{ und } \mathrm{Im}(\beta) = V(n)$$

und wir erhalten zerfallende exakte Sequenzen abelscher Gruppen

$$0 \longrightarrow V(n) \longrightarrow G(p^n) \xrightarrow{\alpha} U(n) \longrightarrow 0 \tag{3}$$

$$0 \longrightarrow U(n) \longrightarrow G(p^n) \xrightarrow{\beta} V(n) \longrightarrow 0.$$

2. Schritt.Die Gruppe V(n) ist zyklisch (von der Ordnung p-1).
Der natürliche Ring-Homomorphismus

$$\mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z},\ x \bmod p^n \mapsto x \bmod p,$$

überführt Einheiten in Einheiten, induziert also einen Gruppen-Homomorphismus

$$\gamma : U(n) \times V(n) = G(p^n) \twoheadrightarrow G(p),\ x \bmod p^n \mapsto x \bmod p, \tag{4}$$

Dieser Homomorphismus ist surjektiv, denn jede zu p teilerfremde ganze Zahl ist auch zu p^n teilderfremd. Der Kern dieses Homomorphismus hat somit den Index

$$\#\, G(p) = \varphi(p) = p-1,$$

also die Ordnung

$$\#\, \mathrm{Ker}(\gamma) = \#\, G(p^n)/(p-1) = p^{n-1}.$$

Wegen (2) gilt damit

$$\mathrm{Ker}(\gamma) = U(n).$$

Auf Grund der zweiten exakten Sequenz (3) erhalten wir einen Isomorphismus

$$G(p) = \mathrm{Im}(\gamma) \xrightarrow{\cong} G(p^n)/\mathrm{Ker}(\gamma) = G(p^n)/U(n) \xrightarrow{\cong} V(n) \tag{5}$$

$$x \bmod p \mapsto (x \bmod p^n) + \mathrm{Ker}(\gamma) \mapsto \beta(x) \bmod p^n = x^{p^{n-1}} \bmod p^n$$

Die Gruppe G(p) ist aber gerade die multiplikative Gruppe des Körpers $\mathbb{Z}/p\mathbb{Z}$ und als solche zyklisch. Also ist auch V(n) zyklisch.

3. Schritt. (weglassen?) Für jede zu p teilerfremde ganze Zahl a_0 gibt es modulo p^n genau eine ganze Zahl a mit

$$a \equiv a_0 \bmod p \text{ und } a^{p-1} \equiv 1 \bmod p^n \tag{6}$$

nämlich die ganze Zahl a mit

$$a \equiv a_0^{p^{n-1}} \bmod p^n \tag{7}$$

Beweis der Eindeutigkeit der Restklasse von a.

Die zweite Identität (6) besagt, daß a mod p^n im Kern von α liegt, also in V(n). Da die Surjektion (4) den Kern U(n) bestitzt, induziert sie einen Isomorphismus

$$\gamma : V(n) \xrightarrow{\cong} G(p),\ x \bmod p^n \mapsto x \bmod p,$$

Die erste Identität (6) besagt gerade, das Bild der Restklasse von a ist bei γ gerade die Restklasse a_0. Die Restklasse von a ist dadurch eindeutig festgelegt (weil γ ein Isomorphismus ist).

Exitenz der Restklasse von a.

Nach dem kleinen Fermatschen Satz gilt

$$a_0^{p-1} \equiv 1 \bmod p.$$

Wir wenden den Isomorphismus (5) an und erhalten

$$(a_0^{p-1})^{p^{n-1}} \equiv 1 \bmod p^n.$$

Mit anderen Worten, für $a := a_0^{p^{n-1}}$ ist die zweite Bedingung von (6) erfüllt. Die erste Bedingung ist es ebenfalls (nach dem kleinen Fermatschen Satz):

$$a \equiv a_0^{p^{n-1}} \equiv a_0^{p^{n-2}} \equiv \ldots \equiv a_0 \bmod p.$$

4. Schritt. U(n) ist im Fall $p \neq 2$ zyklisch (von der Ordnung p^{n-1}).

Als Folgerung aus diesem Schritt ergibt Aussage (i), denn $G(p^n)$ ist direktes Produkt der Gruppen U(n) und V(n) (nach dem 1. Schritt), und beide sind zyklisch (nach dem 2. und diesem 4. Schritt) und haben außerdem eine teilerfremde Ordnung (nach dem ersten Schritt, siehe zwischen (1) und (2)). Als direktes Produkt zyklischer Gruppe mit teilerfremder Ordnung ist $G(p^n)$ zyklisch.[54]

Zum Beweis der Aussage des 4.Schritts reicht es zu zeigen, die Restklasse von 1+ p ist ein Erzeuger der Gruppe U(n). Wegen

$$\# U(n) = p^{n-1}$$

ist die Ordnung der Restklasse von 1 + p ein Teiler von p^{n-1}, d.h.

$$\text{ord } (1 + p \bmod p^n) = p^t \text{ mit } t \leq n - 1.$$

Wir haben zu zeigen, t = n-1. Dazu reicht es zu zeigen[55],

$$(1 + p)^{p^{n-2}} \neq 1 \bmod p^n.$$

Dazu wiederum reicht es zu zeigen, die p^{n-2} - te Potenz von 1 + p hat die Gestalt

$$(1 + p)^{p^{n-2}} = 1 + g \cdot p^{n-1} \text{ mit g teilerfremd zu p.} \qquad (8)$$

Für n = 2 ist diese Aussage richtig (mit g = 1). Nehmen wir an, sie ist richtig für n-1 anstelle von n und beweisen sie für das gegebene n. Nach Voraussetzung ist dann

$$(1 + p)^{p^{n-3}} = 1 + g \cdot p^{n-2} \text{ mit g teilerfremd zu p.}$$

Wir gehen zur p-ten Potenz über und erhalten

$$\begin{aligned} (1 + p)^{p^{n-2}} &= (1 + g \cdot p^{n-2})^p \\ &= 1 + g \cdot p^{n-2} \cdot \binom{p}{1} + \text{ein Vielfaches von}^{56}\ p(p^{n-2})^2 = p^{2n-3} = p^{n+(n-3)} \end{aligned}$$

d.h.

$$(1 + p)^{p^{n-2}} \equiv 1 + g \cdot p^{n-1} \bmod p^n$$

Damit hat aber $(1 + p)^{p^{n-2}}$ die behautptete Gestalt (8), d.h. die Aussage des 4. Schritts ergibt sich durch Induktion nach n.

Es ist noch die Aussage (ii) des Satzes zu beweisen. Wir nehmen also an,

$$p = 2.$$

Die Gruppe V(n) (der Ordnung p-1) ist dann trivial, d.h.

$$G(2^n) = U(n) = \{x \in G(2^n\} \mid x^{2^{n-1}} = 1 \}.$$

---

[54] Man nehme aus jedem der beiden Faktoren einen Erzeuger. Deren Produkt erzeugt dann die Gruppe.

[55] Im Fall $t < n-1$ ist die (n-2)-te Potenz von 1 + p kongruent 1 modulo p^n.

[56] $\binom{p}{2} = p(p-1)/2$ ist ein p-Vielfaches, jeder Faktor der höheren Potenzen von p^{n-2} ist ein p-Vielfaches.

5. Schritt. U(n) ist das direkte Produkt der von $-\overline{1}$ erzeugten zyklischen Untergruppe

$$U'(n) := < -\overline{1} >$$

der Ordnung 2 und der Untergruppe

$$U''(n) := \{ x \bmod p^n \mid x \in \mathbb{Z} \text{ und } x \equiv 1 \bmod 4 \}.$$

Die Untergruppe U"(n) hat die Ordnung 2^{n-2}, ist zyklisch und wird von der Restklasse von 5 erzeugt.

Der Fall n = 1 ist trivial. Es gilt

$$G(2) = \{\overline{1}\}$$

und die beiden Untergruppen U'(1) Und U"(1) sind ebenfalls trivial.

Nehmen wir an, es gilt $n \geq 2$. Der Ring-Homomorphismus

$$\mathbb{Z}/2^n\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z},\ x \bmod 2^n \longrightarrow x \bmod 4,$$

induziert einen surjektiven[57] Gruppen-Homomorphismus der Einheiten-Gruppen

$$\delta: G(2^n) \twoheadrightarrow G(4) = \{\overline{1}, -\overline{1}\}.$$

Der Kern dieses Homomorphismus ist gerade

$$U''(n) := \mathrm{Ker}(\delta).$$

Da das Bild von δ aus zwei Elementen besteht, hat U"(n) den Index 2 in U(n), also die Ordnung

$$\#\, U''(n) = \#\, U(n)/2 = \varphi(2^n)/2 = 2^{n-1}(2-1)/2 = 2^{n-2}.$$

Wir haben eine exakte Sequenz

$$1 \longrightarrow U''(n) \longrightarrow U(n) \xrightarrow{\delta} \{\pm\overline{1}\} \longrightarrow 1.$$

Diese Sequenz zerfällt, weil δ die Untergruppe U'(n) isormorph auf $\{\pm\overline{1}\}$ abbildet, d.h. es ist

$$U(n) \cong U'(n) \times U''(n).$$

Wir haben noch zu zeigen, U"(n) wird von der Restklasse von 5 erzeugt. Das ist trivial im Fall n = 2, denn dann ist U"(n) von der Ordnung 1, also trivial. Sei also

$$n \geq 3.$$

Es reicht zu zeigen, die Ordnung dieser Restklasse von 5 ist 2^{n-2}. Weil die Gruppenordnung 2^{n-2} ist, gilt

$$\mathrm{ord}\,(5 \bmod 2^n) = 2^t \text{ mit } t \leq n-2.$$

Wir haben zu zeigen, t = n-2. Dazu reicht es zu zeigen,

$$5^{2^{n-3}} \not\equiv 1 \bmod 2^n.$$

Dazu wiederum reicht es zu zeigen,

$$5^{2^{n-3}} = 1 + g \cdot 2^{n-1} \text{ mit g ungerade.} \qquad (9)$$

Für n = 3 ist dies der Fall (mit g = 1). Sei jetzt n > 3. Wir nehmen an, eine Identität dieser Gestalt besteht, wenn man n durch n-1 ersetzt, d.h. es ist

$$5^{2^{n-4}} = 1 + g \cdot 2^{n-2} \text{ mit g ungerade.}$$

Wir quadrieren und erhalten

$$\begin{aligned} 5^{2^{n-3}} &= (1+g\cdot 2^{n-2})^2 \\ &= 1 + 2\cdot g\cdot 2^{n-2} + g^2\cdot 2^{2n-4} \\ &= 1 + (g + g^2\cdot 2^{n-3})\cdot 2^{n-1}. \end{aligned}$$

---

[57] Weil die zu 4 teilerfremden ganzen Zahlen auch teilfremd zur n-ten Potenz von 2 sind.

Wegen n > 3 hat der letzte Ausdruck die Gestalt der rechten Seite von (9).
QED.

5.1.5 Die Galois-Gruppe von $K(\sqrt[m]{1})/K$ im Fall $m = p^n$, $p \neq 2$.

Seien K ein Körper der Charakteristik Null, $m = p^n$ mit einer ungeraden Primzahl p, ζ eine primitive m-te Einheitswurzel und

$$L = K(\zeta) = K(\sqrt[m]{1}).$$

Dann ist die Galois-Gruppe G(L/K) zyklisch.
Beweis. Nach 5.1.2 ist G(L/K) eine Untergruppe der Gruppe G(m) der primen Restklassen modulo m. Wegen p ungerade ist G(m) nach 5.1.4 zyklisch. Als Untergruppe einer zyklischen Gruppe ist dann aber auch G(L/K) zyklisch.
QED.

5.1.6 Zum Fall p = 2

Seien K ein Körper der Charakteristik Null, $m = 2^n$, ζ eine primitive m-te Einheitswurzel und

$$L = K(\zeta) = K(\sqrt[m]{1}).$$

Dann gilt

(i) $L = K(i, \eta)$ mit $\eta = \zeta+\zeta^{-1}$.

(ii) $G(L/K' = G(K'(\eta)/K')$ mit $K' := K(i)$ ist zyklisch.

(iii) $G(K(\eta)/K)$ ist zyklisch (vom Grad 2^{n-2}).

Beweis. Zu (i). Weil ζ eine primitive 2^n-te Einheitswurzel ist, ist $\zeta^{2^{n-1}}$ eine primitive 2-te Einheitswurzel, d.h.

$$\zeta^{2^{n-1}} = \pm i.$$

Insbesondere gilt

$$i \in L,$$

also

$$K(i, \eta) \subseteq K(\zeta) = L.$$

Aus der Definition von η ergibt sich (durch Multiplikation der definierenden Identität mit ζ)

$$\zeta^2 - \eta\zeta + 1 = 0,$$

also

$$[K(\zeta):K(\eta)] \leq 2.$$

Speziell für $K = \mathbb{Q}$ ist

$$[\mathbb{Q}(\zeta):\mathbb{Q}(\eta)] = 2,$$

denn η ist eine reelle Zahl[58] und $\mathbb{Q}(\zeta)$ enthält die imaginäre Einheit. Wegen

$$\mathbb{Q}(\eta) \subset \mathbb{Q}(i,\eta) \subseteq \mathbb{Q}(\zeta)$$

muß rechts das Gleichheitszeichen gelten,

$$\mathbb{Q}(\zeta) = \mathbb{Q}(i,\eta).$$

---

[58] Es gilt $1 = |\zeta|^2 = \zeta\overline{\zeta}$, also $\zeta^{-1} = \overline{\zeta}$, also ist $\eta = \zeta+\zeta^{-1} = \zeta+\overline{\zeta}$ reell.

Also läßt sich ζ als Polynom in i und η mit Koeffizienten aus $\mathbb{Q}$ schreiben. Weil K ein Körper der Charakteristik Null ist, liegt $\mathbb{Q}$ in K, und damit auch ζ in $K(i,\eta)$. Wir haben gezeigt

$$L = K(\zeta) = K(i, \eta).$$

Zu (ii). Mit L/K ist auch L/K' Galoissch. Betrachten wir die Galois-Gruppe. Die Körper-Erweiterung K'/K ist trivial oder vom Grad 2, also in jedem Fall eine Galois-Erweiterung. Die Einschränkung auf K' definiert eine Surjektion

$$G(L/K) \twoheadrightarrow G(K'/K),\ \sigma \mapsto \sigma|_K,\ .$$

Ihr Kern ist gerade die uns interessierende Galois-Gruppe G(L/K'). Betrachten wir den Gruppen-Homomorphismus

$$G(L/K') \hookrightarrow G(L/K) \hookrightarrow G(2^n) = <-\overline{1}> \times <\overline{5}> \twoheadrightarrow <\overline{5}> = \mathbb{Z}_{2^{n-2}},$$

wobei die Surjektion rechts die natürliche Projektion auf den zweiten Faktor bezeichne.

Zum Beweis der Behauptung reicht es zu zeigen, dieser Homomorphismus ist injektiv, denn dann kann man G(L/K') als Untergruppe der zyklischen Gruppen $< 5 >$ betrachten, d.h. G(L/K') ist ebenfalls zyklisch.

Zum Beweis der Injektivität reicht es zu zeigen,

$$G(L/K') \bigcap <-\overline{1}> = \{Id\}$$

Angenommen, diese Identität ist falsch. Dann definiert die Restklasse von -1 einen Automorphismus von L über K', d.h. durch

$$\sigma(\zeta) = \zeta^{-1}$$

ist ein Automorphismus von L über K' = K(i) gegeben. Das ist aber nicht der Fall, denn i bleibt bei diesem Automorphismus nicht fest: es ist

$$\sigma(\zeta^{2^{n-1}}) = \sigma(\zeta)^{2^{n-1}} = (\zeta^{-1})^{2^{n-1}} = 1/\zeta^{2^{n-1}}$$

Wegen $\zeta^{2^{n-1}} = \pm i$ erhalten wir

$$\sigma(i) = 1/i = -i.$$

Zu (iii). 1. Fall: K = $\mathbb{Q}$.
Wir betrachten das kommutative Diagramm

$$\begin{array}{ccccc} \mathbb{Q}(i) & \overset{2^{p-2}}{\hookrightarrow} & \mathbb{Q}(\zeta) & = & \mathbb{Q}(i,\eta) \\ 2\bigcup & \nearrow 2^{p-1} & 2\bigcup & \nwarrow 2 & \\ \mathbb{Q} & \overset{2^{p-2}}{\hookrightarrow} & \mathbb{Q}(\eta) & \overset{i}{\hookrightarrow} & \mathbb{Q}(\zeta)\bigcap\mathbb{R} \end{array} \qquad (1)$$

Die natürlichen Zahlen neben oder über den Pfeilen und Inklusionszeichen bezeichnen dabei die Grade der zugehörigen Körpererweiterungen.

Für den linken schrägen Pfeil dies die Aussage der des nachfolgenden Abschnitts 5.1.8. Für übrigen veritkalen Inklusionen ergibt sich das, weil i Nullstelle des Polynoms

$$X^2 + 1$$

ist und alle Inklusionen echt sind (die Körper der unteren Zeile liegen alle in $\mathbb{R}$, während i nicht in $\mathbb{R}$ liegt). Für die ohere horizontale Inklusion ergibt sich der Wert aus der Multiplikativität des Grades. Dasselbe gilt auch für die horizontale Inklusion unten links.
Für die horizontale Inklusion unten rechts erhalten wir

$$i = 1,$$

d.h.

$$\mathbb{Q}(\eta) = \mathbb{Q}(\zeta) \bigcap \mathbb{R}.$$

Die Konjugierten von $\eta = \zeta + \zeta^{-1}$ über $\mathbb{Q}$ haben die Gestalt

$$\eta' = \zeta^{i} + \zeta^{-i} = \zeta^{i} + \overline{\zeta}^{-1} \in \mathbb{Q}(\zeta) \bigcap \mathbb{R} = \mathbb{Q}(\eta).$$

Diese Konjugierten liegen in $\mathbb{Q}(\eta)$, d.h.

$\mathbb{Q}(\eta)/\mathbb{Q}$ ist eine normale Erweiterung (also Galoissch).

Zur Beschreibung der Galois-Gruppe betrachten wir den Einschränkungshomomorphismus

$$h: G(\mathbb{Q}'(\eta)/\mathbb{Q}') = G(\mathbb{Q}(i,\eta)/\mathbb{Q}(i)) \longrightarrow G(\mathbb{Q}(\eta)/\mathbb{Q}), \tau \mapsto \tau|_{\mathbb{Q}(\eta)}.$$

Ein Automorphismus τ aus den Definitionsbereich von h ist durch das Bild von η bei τ bereits eindeutig bestimmt (weil η die Körpererweiterung erzeugt). Deshalb ist h injektiv. Weil auf Grund des kommutativen Diagramms (1) die beiden linken horizontalen Körpererweiterungen denselben Grad haben, haben Definitions- und Wertebereich von h dieselben Ordnung, d.h.

h ist ein Isomorphismus.

Nach (ii) (mit $K = \mathbb{Q}$) ist der Definitionsbereich von h zyklisch. Dasselbe gilt somit auch für der Wertevorrat.

2. Fall: K beleibig.

Weil $\mathbb{Q}(\eta)/\mathbb{Q}$ nach dem ersten Fall normal ist, also Zerfällungskörper eines Polynoms f, ist auch $K(\eta)/K$ als Zerfällungskörper desselben Polynoms normal, also eine Galois-Erweiterung,

$K(\eta)/K$ ist eine Galois-Erweiterung.

Zur Beschreibung der Galois-Gruppe betrachten wir den Einschränkungshomomorphismus

$$\phi.G(K(\eta)/K) \longrightarrow G(\mathbb{Q}(\eta)/\mathbb{Q}), \tau \mapsto \tau|_{\mathbb{Q}(\eta)}.$$

Ein Automorphismus τ aus den Definitionsbereich von h ist durch das Bild von η bei τ bereits eindeutig bestimmt (weil η die Körpererweiterung erzeugt). Deshalb ist h injektiv. Wir können also $G(K(\eta)/K)$ als Untergruppe von $G(\mathbb{Q}(\eta)/\mathbb{Q})$ ansehen. Letztere ist nach (ii) zyklisch. Also ist auch $G(K(\eta)/K)$ zyklisch.

QED.

5.1.7 Zum Gegenstand dieses Abschnitts

Von besonderem Interesse sind für uns die Erweiterungen

$$\mathbb{Q}(\sqrt[m]{1})/\mathbb{Q} \text{ und } \mathbb{Q}_p(\sqrt[m]{1})/\mathbb{Q}_p.$$

Wie wir aus der Theorie der lokalen Körper wissen, muß man, um die Zerlegung einer Primzahl p in der Erweiterung

$$\mathbb{Q}(\sqrt[m]{1})$$

des Körpers $\mathbb{Q}$ der rationalen Zahlen zu finden, die Erweiterung

$$\mathbb{Q}_p(\sqrt[m]{1})$$

des Körpers $\mathbb{Q}_p$ der p-adischen Zahlen betrachten.

Um die abstrakten Sätze etwas durchsichtiger zu machen, werden wir manchmal mehrere Beweise für ein und dieselbe Behauptung angeben.

Eine gute Übersicht zur Theorie der Kreisteilungskörper findet man in den folgenden Büchern:

Weyl, H.: Algebraic theory of numbers, Annals of Mathematics Studies, Princeton 1940.

Weiss, E.: Algebraic number theory, GcGraw Hill, New York 1963

5.1.8 Die Galois-Gruppe von $\mathbb{Q}(\sqrt[m]{1})/\mathbb{Q}$

Die Körper-Erweiterung $\mathbb{Q}(\sqrt[m]{1})/\mathbb{Q}$ ist normal vom Grad $\varphi(m)$. Ihre Galois-Gruppe ist isomorph zur Gruppe der primen Restklassen

$$G(m) := (\mathbb{Z}/m\mathbb{Z})^*$$

modulo m.

Beweis (van der Waerden). Sei ζ eine primitive m-te Einheitswurzel. Dann gilt

$$\mathbb{Q}(\sqrt[m]{1}) = \mathbb{Q}(\zeta),$$

und die Nullstellen von $X^m - 1$ sind gerade die Potenzen von ζ. Insbesondere ist die Erweiterung

$$\mathbb{Q}(\sqrt[m]{1})/\mathbb{Q}$$

gerade der Zerfällungskörper von $X^m - 1$ und als solcher normal. Nach 5.1.2 können wir die Galois-Gruppe dieser Erweiterung mit einer Untergruppe von G(m) identifizieren. Es reicht also zu zeigen, die Galois-Gruppe hat die Ordnung $\varphi(m)$, d.h. es reicht zu zeigen, der Grad der Körper-Erweiterung ist $\varphi(m)$,

$$[\mathbb{Q}(\sqrt[m]{1}):\mathbb{Q}] = \varphi(m).$$

Wir wissen bereits, der Grad dieser Erweitungung ist $\leq \varphi(m)$. Deshalt reicht es, die folgende Aussage zu beweisen.

$$\text{Für } f(x)\in\mathbb{Z}[x] \text{ mit } f(\zeta) = 0 \text{ gilt auch } f(\zeta^a) = 0 \text{ für jedes a mit ggT(a, m) = 1.} \quad (1)$$

(weil es $\varphi(m)$ verschiedene primitive m-te Einheitswurzeln gibt hat dann jedes solche f einen Grad $\geq \varphi(m)$ oder ist 0). Es reicht, (1) für den Fall

$$a = p \text{ ist eine Primzahl}$$

(die teilerfremd zu m ist) zu beweisen, denn dann erhält man durch wiederholtes Anwenden dieses Spezialfalls[59] den allgemeinen Fall (1).

Seien

$$k_p := \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$$

---

[59] Man wende die Aussage an mit ζ^a anstelle von ζ , usw.

der Körper mit p Elementen und

$$*: \mathbb{Z}[x] \longrightarrow k_p[x],$$

der Homomorphismus von Ringen mit 1, der die Koeffizienten aller ganzzahligen Polynome in x durch deren Restklassen in k_p ersetzt. Weiter seien

$$L \text{ der Zerfällungskörper über } k_p \text{ von } x^m - 1$$

und

$$x^m - 1 = f_1(x) \bullet f_2(x) \bullet \ldots \bullet f_r(x) \qquad (1)$$

die Zerlegung von $x^m - 1$ in irreduzible Faktoren über $\mathbb{Z}$. Die Bezeichnungen seien dabei so gewählt, daß gilt

$$f_1(\zeta) = 0 \text{ und } f_j(\zeta^p) = 0.$$

Zum Beweis der Behauptung reicht es zu zeigen,

$$j = 1.$$

Weil f_1 irreduzibel ist, gilt

$$f_1(x) \mid f_j(x^p) \text{ in } \mathbb{Z}[x],$$

also

$$f_1^*(x) \mid f_j^*(x^p) \text{ in } k_p[x].$$

Für jede Nullstelle $\zeta^* \in L$ von f_1^* gilt damit auch

$$f_j^*(\zeta^{*p}) = 0.$$

Außerdem ist

$$f_1^*(\zeta^{*p}) = f_1^*(\zeta^*)^p = 0^p = 0.$$

Wir haben gezeigt, f_1^* und f_j^* haben eine gemeinsame Nullstelle. Mit (1) gilt aber auch

$$x^m - 1 = f_1^*(x) \bullet f_2^*(x) \bullet \ldots \bullet f_r^*(x) \qquad (2)$$

Nun sind das Polynom $x^m - 1$ und dessen Ableitung mx^{m-1} über k_p teilerfremd[60], d.h. das Polynom $x^m - 1$ hat über k_p keine mehrfachen Nullstellen. Weil f_1^* und f_j^* eine gemeinsame Nullstelle haben, muß damit $j = 1$ gelten.
QED.

---

[60] Weil nach Voraussetzung p und m teilerfremd sind.

5.1.9 Die Frobenius-Automorphismen von $\mathbb{Q}(\sqrt[m]{1})/\mathbb{Q}$

Seien $m > 1$ eine natürliche Zahl und p eine zu m teilerfremde Primzahl,

$$(m, p) = 1.$$

Dann gibt es genau einen Automorphismus

$$\sigma_p \in G(\mathbb{Q}(\sqrt[m]{1})/\mathbb{Q})$$

mit

$$\sigma_p(\alpha) \equiv \alpha^p \bmod p\mathcal{O}_{\mathbb{Q}(\sqrt[m]{1})} \text{ für jedes } \alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt[m]{1})}.$$

Dabei bezeichne

$$\mathcal{O}_{\mathbb{Q}(\sqrt[m]{1})} \subseteq \mathbb{Q}(\sqrt[m]{1})$$

den Ring der ganzen Zahlen des Zahlenkörpers $\mathbb{Q}(\sqrt[m]{1})$, d.h. die ganze Abschließung von $\mathbb{Z}$ in $\mathbb{Q}(\sqrt[m]{1})$.

Ist ζ eine primitive m-te Einheitswurzel, so ist σ_p durch die folgende Formel gegeben.

$$\sigma_p\Big(\sum_{i=0}^{\varphi(m)-1} a_i\zeta^i\Big) = \sum_{i=0}^{\varphi(m)-1} a_i\zeta^{ip} \text{ für } a_i \in \mathbb{Q}. \qquad (1)$$

Der Automorphismus σ_p heißt <u>Frobenius-Automorphismus</u> zur Primzahl p.

Beweis. Nach Definition gilt

$$L := \mathbb{Q}(\sqrt[m]{1}) = \mathbb{Q}(\zeta)$$

mit einer primitiven m-ten Einheitswurzeln und nach 5.1.8 ist

$$[L:\mathbb{Q}] = \varphi(m) := \#\,(\mathbb{Z}/m\mathbb{Z})^*.$$

Insbesondere bilden die ersten $\varphi(m)$-ten Potenzen von ζ eine $\mathbb{Q}$-Vektorraum-Basis von L,

$$L = \mathbb{Q}\bullet\zeta^{\varphi(m)-1} + \mathbb{Q}\bullet\zeta^{\varphi(m)-2} + \ldots + \mathbb{Q}\bullet\zeta^0.$$

1. <u>Schritt</u>: $d_m := \det\,(\mathrm{Tr}_{L/\mathbb{Q}}(\zeta^{i+j}))_{i,j=0,\ldots,\varphi(m)-1} \in \mathbb{Z} - \{0\}$ ist teilerfremd zu p.

Sei $\phi(X)$ das Minimalpolynom von ζ über $\mathbb{Q}$. Weil ζ ganz ist über $\mathbb{Z}$, sind auch die Koeffizientien von $\phi(X)$ ganz über $\mathbb{Z}$, liegen also in $\mathcal{O}_L \bigcap \mathbb{Q} = \mathbb{Z}$, d.h.

$$\phi(X) \in \mathbb{Z}[X].$$

Da der höchste Koeffizient von ϕ gleich 1 ist, ist

$$\mathbb{Z}[\zeta] \cong \mathbb{Z}[X]/(\phi)$$

ein freier $\mathbb{Z}$-Modul vom Rang $\varphi(m)$. Nach 1.6.13 erzeugt d_m die Diskriminante von $\mathbb{Z}[\zeta]$

$$d_m\bullet\mathbb{Z} = \delta(\mathbb{Z}[\zeta]/\mathbb{Z}) = N_{L/\mathbb{Q}}(\phi'(\zeta))\mathbb{Z}$$

(das rechte Gleichheitszeichen besteht nach 3.2.10 (ii)). Es folgt

$$d_m\bullet\mathbb{Z} = \phi'(\zeta_1)\bullet\ldots\bullet\phi'(\zeta_{\varphi(m)})\mathbb{Z}, \qquad (2)$$

wenn $\{\zeta_1, ..., \zeta_{\varphi(m)}\}$ die Menge der primitiven m-ten Einheitswurzeln ist, d.h.

$$d_m \cdot \mathbb{Z} = \prod_{i,j=1, i \neq j}^{\varphi(m)} (\zeta_i - \zeta_j) \cdot \mathbb{Z}$$

Insbesonder ist der Erzeuger des linken Ideals ein Teiler des Erzeugers des rechten:

$$d_m \text{ teilt } \prod_{i,j=1, i \neq j}^{\varphi(m)} (\zeta_i - \zeta_j) \text{ in } \mathbb{Z} \text{ also auch in } \mathcal{O}_{\mathbb{Q}(\sqrt[m]{1})}.$$

Wir fügen jetzt zu den Faktoren auf der rechten Seite weitere Faktoren aus $\mathcal{O}_{\mathbb{Q}(\sqrt[m]{1})}$ hinzu. Die Teilbarkeitsrelation in $\mathcal{O}_{\mathbb{Q}(\sqrt[m]{1})}$ bleibt dabei erhalten. Statt das Produkt über alle Differenzen von primitiven m-ten Einheitswurzeln zu bilden, bilden wir es über alle Differenzen von Nullstellen von

$$F(X) := X^m - 1,$$

Wir erhalten, daß d_m in $\mathcal{O}_{\mathbb{Q}(\sqrt[m]{1})}$ das folgende Produkt teilt:

$$\begin{aligned}
\prod_{i,j=0, i \neq j}^{m-1} (\zeta^i - \zeta^j) &= \prod_{i=0}^{m-1} F'(\zeta^i) \cdot \mathbb{Z} \\
&= \prod_{i=0}^{m-1} m(\zeta^i)^{m-1} \\
&= \prod_{i=0}^{m-1} m(-1)^{m-1}(-\zeta^i)^{m-1} \\
&= (m(-1)^{m-1})^m \prod_{i=0}^{m-1} (-\zeta^i)^{m-1} \\
&= m^m (-1)^{m(m-1)} (\prod_{i=0}^{m-1} -\zeta^i)^{m-1} \\
&= m^m F(0)^{m-1} \\
&= -m^m
\end{aligned}$$

Es gilt also eine ganze Zahl $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt[m]{1})}$ mit

$$d_m \cdot \alpha = m^m.$$

Als Quotient ganze Zahlen ist α rational, liegt also in $\mathbb{Q} \bigcap \mathcal{O}_{\mathbb{Q}(\sqrt[m]{1})} = \mathbb{Z}$, d.h.

$$d_m \text{ teilt } m^m \text{ in } \mathbb{Z}.$$

Nun ist m^m teilerfremd zu p, also d_m teilerfremd zu p.

2. Schritt. $\mathbb{Z}[\zeta] \subseteq \mathcal{O}_L \subseteq \frac{1}{d_m} \mathbb{Z}[\zeta]$

Für das Dual des $\mathbb{Z}$-Moduls $\mathcal{O}_L$ gilt

$$D(\mathcal{O}_L) = \{ u \in L \mid Tr_{L/\mathbb{Q}}(u\mathcal{O}_L\} \subseteq \mathbb{Z} \} \supseteq \mathcal{O}_L,$$

Damit ist

$$\begin{aligned}
\mathcal{O}_L \quad &\subseteq D(\mathcal{O}_L) \\
&\subseteq D(\mathbb{Z}[\zeta]) && \text{(wegen } \mathbb{Z}[\zeta] \subseteq \mathcal{O}_L\text{)} \\
&= \frac{1}{\phi'(\zeta)}\mathbb{Z}[\zeta] && \text{(nach 3.2.10(i))} \\
&\subseteq \frac{1}{d_m}\mathbb{Z}[\zeta] && \text{(nach (2))}
\end{aligned}$$

3. Schritt: Existenz von σ_p.

Nach 5.1.8 ist die Galois-Gruppe

$$G := G(\mathbb{Q}(\sqrt[m]{1})/\mathbb{Q})$$

isomorph zu G(m), wobei der Isomorphismus gerade die in 5.1.2 beschriebene Einbettung ist. Insbesondere gibt es einen Automorphismus

$$\sigma \in G,$$

welcher der Restklasse von p in G(m) entspricht, d.h. einen $\mathbb{Q}$-Automorphismus mit

$$\sigma(\zeta) = \zeta^p,$$

wobei ζ eine (vorgegebene) primitive m-te Einheitwurzel bezeichne.Damit ist σ durch die Formel (1) gegeben.

Zum Beweis der Existenz von σ_p, reicht es zu zeigen

$$\sigma(\alpha) \equiv \alpha^p \bmod p\mathcal{O}_L \text{ für jedes } \alpha \in \mathcal{O}_L,$$

denn dann genügt σ allen Bedingungen, die wir an σ_p stellen.

Jedes $\alpha \in \mathcal{O}_L$ können wir nach dem 2.Schritt in der Gestalt

$$\alpha = \frac{1}{d_m} \cdot \sum_{i=0}^{\varphi(m)-1} a_i\zeta^i \text{ mit } a_i \in \mathbb{Z}$$

schreiben. Modulo p erhalten wir

$$\begin{aligned}
d_m\sigma(\alpha) &\equiv \sigma\Big(\sum_{i=0}^{\varphi(m)-1} a_i\zeta^i\Big) \\
&\equiv \sum_{i=0}^{\varphi(m)-1} a_i\sigma(\zeta)^i \\
&\equiv \sum_{i=0}^{\varphi(m)-1} a_i\zeta^{ip} \\
&\equiv \sum_{i=0}^{\varphi(m)-1} a_i^p\zeta^{ip} && \text{(kleiner Fermatscher Satz)} \\
&\equiv \Big(\sum_{i=0}^{\varphi(m)-1} a_i\zeta^i\Big)^p && \text{(modulo p ist } x \mapsto x^p \text{ ein Ring-Homomorphismus)}
\end{aligned}$$

$$\equiv d_m^p \left(\frac{1}{d_m} \cdot \sum_{i=0}^{\varphi(m)-1} a_i \zeta^i\right)^p$$

$$\equiv d_m^p \cdot \alpha^p$$

$$\equiv d_m \cdot \alpha^p \qquad \text{(kleiner Fermatscher Satz).}$$

Nach dem ersten Schriit ist die ganze Zahl d_m teilerfremd zu p, also eine Einheit modulo p. Wir multiplizieren mit dem Inversen und erhalten

$$\sigma(\alpha) \equiv \alpha^p \bmod p\mathcal{O}_L.$$

Damit ist die Existenz von σ_p bewiesen.

4. Schritt. Eindeutigkeit von σ_p.

Ein Element $\sigma \in G(L/\mathbb{Q})$ ist durch das Bild

$$\sigma(\zeta) = \zeta^a \text{ , } (m, a) = 1,$$

der primitiven m-ten Einheitswurzel bereits eindeutig festgelegt. Es reicht somit zu zeigen, daß die folgende Implikation besteht.

$$\zeta^a \equiv \zeta^b \bmod p\mathcal{O}_L \text{ , a, b teilerfremd zu m} \Rightarrow \zeta^a = \zeta^b. \qquad (3)$$

Zum Beweis dieser Implikation wiederum reicht es die folgende zu beweisen[61].

$$\zeta^a \equiv 1 \bmod \bmod p\mathcal{O}_L \text{ , a teilerfremd zu m} \Rightarrow \zeta^a = 1.$$

Angenommen, es gilt $\zeta^a \neq 1$. Wegen

$$x^m - 1 = \prod_{i=1}^{m} (x - \zeta^i)$$

gilt

$$mx^{m-1} = \sum_{j=1}^{m} \prod_{i \neq j} (x - \zeta^i)$$

Wir setzen x = 1 und erhalten

$$m = \prod_{i=1}^{m-1} (1 - \zeta^i)$$

Wegen $\zeta^a \neq 1$ kommt $1 - \zeta^a$ unter den Faktoren auf der rechten Seite vor, d.h.

$$1 - \zeta^a$$

---

[61] Aus

$$\zeta^a \equiv \zeta^b \bmod p\mathcal{O}_L$$

folgt durch Multiplikation mit der Einheit ζ^{-b}

$$\zeta^{a-b} \equiv 1 \bmod p\mathcal{O}_L$$

also auf Grund der nachfolgenden Implikation

$$\zeta^{a-b} \equiv 1,$$

also $\zeta^a = \zeta^b$.

ist im Ring $\mathcal{O}_L$ ein Teiler von m. Deshalb kann p in diesem Ring kein Teiler von $1 - \zeta^a$ sein (denn dann wäre p ein Teiler von m) im Widerspruch zur Voraussetzung $\zeta^a \equiv 1$.
5. Schritt. Alternativer Beweis für die Eindeutigkeit.
Es reicht, die Implikation (3) zu beweisen. Dazu setzen wir

$$L := \mathbb{Q}(\zeta) \text{ und } \mathcal{O}_L := \text{ganze Abschließung von } \mathbb{Z} \text{ in } L$$

betrachten wir das folgende kommutative Diagramm

$$\begin{array}{ccc} \mathbb{Q} \supseteq & \mathbb{Z} & \twoheadrightarrow \mathbb{F}_p \\ \downarrow & \downarrow & \downarrow \\ L \supseteq & \mathcal{O}_L & \twoheadrightarrow \kappa_L \end{array}$$

Dabei sollen die vertikalen Pfeile die natürlichen Einbettungen bezeichnen und die horizontalen Surjektionen die natürlichen Abbildungen auf die Restklassenringe bezüglich der p-adischen Bewertung bzw. bezüglich einer Forsetzung der p-adischen Bewertung auf L. Wegen $\zeta \in \mathcal{O}_L$ ist

$$x^m - 1 = \prod_{i=1}^{m} (x - \zeta^i)$$

eine Zerlegung mit Koeffizienten aus $\mathcal{O}_L$. Bezeichne $\overline{\zeta}$ das Bild von ζ bei der rechten unteren Surjektion. Dann ist

$$x^m - 1 = \prod_{i=1}^{m} (x - \overline{\zeta}^i)$$

eine Zerlegung mit Koeffizienten aus κ_L. Weil die Charakteristik von κ_L gleich p und p teilerfremd zu m ist, sind die Polynome $x^m - 1$ und mx^{m-1} über κ_L teilerfremd. Das Polynom $x^m - 1$ hat über κ_L keine mehrfachen Nullstellen, d.h. die Potenzen

$$\overline{\zeta}1, \overline{\zeta}2, \ldots, \overline{\zeta}m$$

sind paarweise verschieden. Also besteht die Implikatioin (3).

QED.

5.1.10 Total verzweigte Primzahlen: der Fall $m = p^n$

Seien p eine Primzahl, $n \geq 1$ eine natürliche Zahl und

$$L := \mathbb{Q}(\sqrt[m]{1}) = \mathbb{Q}(\zeta)$$

mit einer primitiven m-ten Einheitswurzel ζ.
Dann ist die Primzahl p in L total verzweigt. Genauer, im Ring $\mathcal{O}_L$ der ganzen Zahlen von L gilt

$$p\mathcal{O}_L = (1-\zeta)^{\varphi(m)}\mathcal{O}_L.$$

Dabei ist $1-\zeta$ ein Parameter von L über p.

Beweis 1. Die nicht-primitiven m-ten Einheitswurzeln sind gerade die Nullstellen von

$$x^{m/p} - 1.$$

Das Minimalpolynom von ζ ist damit gleich

$$f(x) = \frac{x^m-1}{x^{m/p}-1} = \frac{(x^{m/p})^p-1}{x^{m/p}-1} = (x^{m/p})^{p-1} + (x^{m/p})^{p-2} + ... + 1$$

Das Element $\lambda = 1-\zeta$ ist damit Nullstelle des irreduziblen Polynoms

$$g(y) := f(1-y)$$

Das Polynom $g(-y) = f(y+1)$ hat den höchsten Koeffizienten 1 und das Absolutglied

$$g(0) = f(1) = (1)^{p-1} + (1)^{p-2} + ... + 1 = 0$$

Modulo p gilt $x = y+1$ und $z = x^{m/p}$

$$g(-y) = f(y+1) = f(x) = \frac{(x^{m/p})^p-1}{x^{m/p}-1} = \frac{z^p-1}{z-1}$$

$$\equiv \frac{(z-1)^p}{z-1} \bmod p$$

$$= (z-1)^{p-1}$$

$$= (x^{m/p} - 1)^{p-1}$$

$$\equiv (x-1)^{m(p-1)/p} \bmod p \qquad \text{(weil m eine p-Potenz ist)}$$

$$= y^{m(p-1)/p}$$

Dies zeigt, alle Koeffizienten von $g(-y)$ außer dem höchsten sind durch p teilbar. Zusammen erhalten wir, daß $g(-y)$ ein Eisenstein-Polynom ist. Nach 3.4.3 ist

$$\mathbb{Q}_p(\lambda)/\mathbb{Q}_p \text{ total verzweigte Erweiterung}$$

und λ ein Parameter von

$$L_p := \mathbb{Q}_p(\lambda) = \mathbb{Q}_p(\zeta)$$

Insbesondere ist $g(-y)$ irreduzibel (vgl. den Beweis in 3.4.4). Insbesondere hat die Körpererweiterung den Grad

$$[\mathbb{Q}_p(\lambda):\mathbb{Q}_p] = \deg g = m(p-1)/p = p^{n-1}(p-1) = \varphi(p^n) = \varphi(m),$$

d.h. es gilt in L_p

$$p\mathcal{O}_{L_p} = \lambda^{\varphi(m)}\mathcal{O}_{L_p} \qquad (1)$$

Sei jetzt $L := \mathbb{Q}(\zeta)$ und

$$\mathbb{Q}_p \otimes_{\mathbb{Q}} L = L_1 \times ... \times L_r$$

Dabei seine die L_i die Vervollständigungen von L bezüglich der Fortsetzungen der p-adischen Bewertung von $\mathbb{Q}$ auf L. Einer der direkten Faktoren rechts ist L_p. Deshalb gilt

$$\varphi(m) \geq [L:\mathbb{Q}] = \dim_{\mathbb{Q}} L = \dim_{\mathbb{Q}_p} \mathbb{Q}_p \otimes_{\mathbb{Q}} L \geq \dim_{\mathbb{Q}_p} L_p = \varphi(m)$$

Also gilt überall das Gleichheitszeichen (und es folgt erneut die Gradaussage von 5.1.8 in diesem Spezialfall). Außerdem gibt es nur eine Fortsetzung der p-adischen Bewertung auf L,

$$r = 1.$$

Weil λ bereits in der ganzen Abschließung $\mathcal{O}_L$ von $\mathbb{Z}$ in L liegt, gilt mit (1) sogar

$$p\mathcal{O}_L = \lambda^{\varphi(m)}\mathcal{O}_L$$

und λ ist ein Parameter von $\mathcal{O}_L$ bezüglich der Bewertung, die über der p-adischen liegt.

QED.

Beweis 2. Für ganze Zahle a, b mit

$$(a, m) = (b, m) = 1$$

besitzt die Kongruenz

$$a \equiv ps \bmod m$$

eine Lösung. Damit gilt

$$\frac{1-\zeta^a}{1-\zeta^b} = \frac{1-\zeta^{bs}}{1-\zeta^b} = 1 + \zeta^b + \zeta^{2b} + ... + \zeta^{(s-1)b} \in \mathcal{O}_L \qquad (2)$$

Dasselbe gilt auch mit a und b vertauscht. Insbesondere ist

$$\frac{1-\zeta^a}{1-\zeta^b} \text{ Einheit von } \mathcal{O}_L \text{ für beliebige zu m teilerfremde a und b.} \qquad (3)$$

Außerdem ist

$$p = \lim_{x \longrightarrow 1} \frac{x^m-1}{x^{m/p}-1} \qquad \text{(vgl. (2))}$$

$$= \lim_{x \longrightarrow 1} \prod_{0<a<m,(a,m)=1} (x - \zeta^a)$$

$$= (1-\zeta)^{\varphi(m)} \cdot \prod_{0<a<m,(a,m)=1} \frac{1-\zeta^a}{1-\zeta}$$

Die Faktoren unter dem Produkt-Zeichen auf der rechten Seite sind nach (3) Einheiten in $\mathcal{O}_L$, d.h. es gilt

$$p\mathcal{O}_L = \lambda^{\varphi(m)}\mathcal{O}_L$$

QED.

5.1.11 Unverzweigte Primzahlen

Seien m > 1 eine natürliche Zahl und p eine zu m teilerfremde Primzahl

$$(m, p) = 1, \text{ p Primzahl.}$$

Dann gilt:

(i) p ist unverzweigt in $L := \mathbb{Q}(\sqrt[m]{1})$

(ii) Der Relativgrad von $L/\mathbb{Q}$ in p ist gleich der kleinsten ganzen Zahl $f \geq 1$ mit

$$p^f \equiv 1 \bmod m.$$

Beweis (nach Serre [1]). Betrachten wir die Körpererweiterung

$$L_p := \mathbb{Q}_p(\sqrt[m]{1})$$

von $\mathbb{Q}_p$. Der Restekörper

$$\kappa_p := \mathbb{F}_p$$

von $\mathbb{Q}_p$ besteht aus p Elementen. Das Polynom

$$X^m - 1$$

zerfällt genau dann über der Körper-Erweiterung

$$\kappa_{p^f}$$

von κ_p in Linearfaktoren, wenn gilt[62]

$$m \mid p^f - 1.$$

Sei f jetzt die kleinste natürliche Zahl mit

$$p^f \equiv 1 \bmod m.$$

und bezeichne L_p die unverzweigte Erweiterung von κ_p mit

$$\kappa_{L_p} = \kappa_{p^f}.$$

Diese existiert nach 3.5.7. Weil $X^m - 1$ nach Konstruktion über κ_{L_p} in Linearfaktoren zerfällt, gibt es ein Element der Ordnung m in der multiplikativen Gruppe dieses Körpers, sagen wir

$$\overline{\zeta} \in \kappa^*_{L_p}, \ \overline{\zeta} \text{ von der Ordnung m.}$$

Weil p teilerfremd zu m ist, ist das Polynom $X^m - 1$ separabel. Weil L_p vollständig ist, gibt es nach dem Henselschen Lemma (2.4.5, zweiter Spezialfall) ein Element im Ring der ganzen Zahlen von L_p

$$\zeta \in \mathcal{O}_{L_p} \text{ mit der Restklasse } \overline{\zeta},$$

welches ebenfalls Nullstelle von $X^m - 1$ ist. Weil die Restklasse von ζ die Ordnung m hat, gilt dasselbe für ζ, d.h. ζ ist eine primitive m-te Einheitswurzel, und $X^m - 1$ zerfällt über L_p in Linearfaktoren,

$$\mathbb{Q}_p(\sqrt[m]{1}) = \mathbb{Q}_p(\zeta) \subseteq L_p. \qquad (1)$$

Als Teilerweiterung einer unverzweigten Erweiterung ist $\mathbb{Q}_p(\zeta)/\mathbb{Q}_p$ ebenfalls unverzweigt. Wäre die Inklusion auf der rechten Seite von (1) echt, so wäre die zugehörige Erweiterung der Restekörper ebenfalls echt, d.h. κ_{L_p}/κ_p wäre nicht die kleinste Erweiterung, über welcher das Polynom $X^m - 1$ in Linearfaktoren zerfallt. Es gilt also

---

[62] Die Multiplikative Gruppe $\kappa^*_{p^f}$ wird von einer primitiven (p^f-1)-ten Einheitswurzel erzeugt. Im Fall

$$m \mid p^f - 1$$

ist eine geeignete Potenz dieser Einheitswurzel eine m-te primitive Einheitswurzel. Die Potenzen letzterer sind gerade die Nullstellen von X^m-1. Dieses Polynom zerfallt also über κ_{p^f}.

Nehmen wir umgekehrt an, das Polynom X^m-1 zerfüllt über κ_{p^f}. Die Nullstellen dieses Polynom bilden eine Untergruppe der zyklischen Gruppe $\kappa^*_{p^f}$. Diese Untergruppe ist ist also auch zyklisch und hat, weil p teilerfremd zu m also X^m-1 separabel ist, die Ordnung m. Die Gruppe $\kappa^*_{p^f}$ enthält somit ein Element der Ordnung m, d.h. es gilt

$$m \mid p^f - 1.$$

$$L_p = \mathbb{Q}_p(\zeta)$$

und

$$[\mathbb{Q}_p(\zeta) : \mathbb{Q}_p] = [L_p : \mathbb{Q}_p] = e \bullet f = 1 \bullet f = [\kappa_{pf} : \kappa_p] = f.$$

Betrachten wir jetzt den Körperturm

$$\mathbb{Q} \subseteq \mathbb{Q}(\zeta) \subseteq \mathbb{Q}_p(\zeta). \qquad (2)$$

Weil $\mathbb{Q}_p(\zeta)$ über $\mathbb{Q}_p$ unverzweigt ist, ist p in $\mathbb{Q}_p(\zeta)$ ein Parameter. Dann ist aber p auch in $\mathbb{Q}(\zeta)$ ein Parameter, d.h. p hat in $\mathbb{Q}(\zeta)$ den Verzweigungsindex 1. Bestimmen wir den Relativgrad. Die Inklusionen (2) induzieren die entsprechende Inklusionen der Restekörper über p,

$$\kappa_p \subseteq \kappa_L \subseteq \kappa_{L_p}.$$

Weil $X^m - 1$ über $\mathbb{Q}(\zeta)$ in Linearfaktoren zerfällt und Koeffizienten im Ring der ganzen Zahlen hat, zerfällt dieses Polynom auch über κ_L. Nun ist aber κ_{L_p} der kleinste Körper über welchem dieses Polynom in Linearfaktoren zerfällt. Deshalb gilt

$$\kappa_L = \kappa_{L_p}$$

und für den Relativgrad erhalten wir

$$[\kappa_L : \kappa_p] = [\kappa_{L_p} : \kappa_p] = f.$$

QED.

5.1.12 Vollständig zerfallende Primzahlen

Seien $m > 1$ eine natürliche Zahl und p eine zu m teilerfremde Primzahl. Dann sind folgende Aussagen äquivalent.

(i) p zerfällt vollständig in $L = \mathbb{Q}(\sqrt[m]{1})$, d.h. $p\mathcal{O}_L$ ist das Produkt von

$$\varphi(m) = [L:\mathbb{Q}]$$

paarweise verschiedenen Primidealen von $\mathcal{O}_L$.

(ii) $p \equiv 1 \bmod m$.

Beweis. Bezeichne e den Verzweigungsindex von p in L und f den Relativgrad. Dann ist

$$[L:\mathbb{Q}]/ef$$

die Anzahl der Primideale von $\mathcal{O}_L$, welche über $p\mathbb{Z}$ liegen (nach 3.8.3). Bedingung (i) ist somit genau dann erfüllt, wenn

$$e = f = 1$$

gilt. Nach 5.1.11 ist dies äquivalent zu (ii).
QED.

5.1.13 Die Diskriminante von $\mathbb{Q}(\sqrt[m]{1})/\mathbb{Q}$ im Fall $m = p^n$

Seien p eine Primzahl, $n \geq 1$ eine natürliche Zahl,

$$m = p^n,$$

und

$$L := \mathbb{Q}(\sqrt[m]{1}).$$

Dann gilt für die Diskriminante

$$\delta(L/\mathbb{Q}) := \delta(\mathcal{O}_L/\mathbb{Z}) = (m^{\varphi(m)}/p^{m/p})\mathbb{Z}.$$

Außerdem bilden die Potenzen

$$1, \zeta, \zeta^2, \ldots, \zeta^{\varphi(m)-1}$$

ein linear unabhängiges Erzeugendensystem von $\mathcal{O}_L$ über $\mathbb{Z}$.

Beweis. Nach 5.1.11 sind alle von p verschiedenen Primzahlen in L unverzweigt. Als einziger Teiler der Diskriminante kommt damit nur p in Frage,

$$\delta(\mathcal{O}_L/\mathbb{Z}) = p^x\mathbb{Z} \text{ mit } x \geq 0.$$

(vgl. 3.3.4). Wie im 2. Schritt des Beweises von 5.1.9 sehen wir

$$\mathbb{Z}[\zeta] \subseteq \mathcal{O}_L \subseteq \frac{1}{p^x}\mathbb{Z}[\zeta]$$

d.h.

$$p^x\mathcal{O}_L \subseteq \mathbb{Z}[\zeta] \subseteq \mathcal{O}_L. \qquad (1)$$

Weil die Erweiterung $L/\mathbb{Q}$ nach 5.1.10 in p total verzweigt ist, ist die zugehörige Erweiterung der Restekörper tivial, d.h.

$$\mathcal{O}_L/\lambda\mathcal{O}_L = \mathbb{Z}/p\mathbb{Z} \text{ mit } \lambda = \zeta - 1.$$

Es folgt

$$\mathcal{O}_L = \mathbb{Z} + \lambda\mathcal{O}_L.$$

Erst recht gilt damit auch

$$\mathcal{O}_L = \mathbb{Z}[\zeta] + \lambda\mathcal{O}_L.$$

Wir können für den Ring $\mathcal{O}_L$ auf der rechten Seite die gesamte Seite einsetzen und erhalten

$$\mathcal{O}_L = \mathbb{Z}[\zeta] + \lambda^2\mathcal{O}_L.$$
$$\mathcal{O}_L = \mathbb{Z}[\zeta] + \lambda^3\mathcal{O}_L.$$
$$\ldots$$
$$\mathcal{O}_L = \mathbb{Z}[\zeta] + \lambda^s\mathcal{O}_L \text{ für jedes } s \geq 1.$$

Speziell für $s = x\varphi(m)$ ergibt sich

$$\begin{aligned} \mathcal{O}_L &= \mathbb{Z}[\zeta] + \lambda^{x\varphi(m)}\mathcal{O}_L \\ &= \mathbb{Z}[\zeta] + p^x\mathcal{O}_L \qquad \text{(wegen } \lambda^{\varphi(m)}\mathcal{O}_L = p\mathcal{O}_L \text{ nach 5.1.10)} \\ &= \mathbb{Z}[\zeta] \qquad \text{(nach (1)).} \end{aligned}$$

Damit ist der zweite der Teil der Behauptung bewiesen. Wir haben noch die Diskriminante zu berechnen.

Wegen $\mathcal{O}_L = \mathbb{Z}[\zeta]$ ist die Diskriminanten nach 3.2.10 gleich

$$\delta(\mathcal{O}_L/\mathbb{Z}) = (N_{L/\mathbb{Q}}f'(\alpha))\bullet\mathbb{Z}.$$

Dabei bezeichne $f(x)\in\mathbb{Z}[x]$ das Minimalpolynom von ζ über $\mathbb{Q}$, d.h.

$$f(x) = \frac{x^m-1}{x^{m/p}-1} = x^{m(p-1)/p} + x^{m(p-2)/p} + \ldots + x^{m/p} + 1.$$

Mit $F(x) := x^m - 1$ und $G(x) := x^{m/p} - 1$ erhalten wir:

$$\begin{aligned} F(x) &= f(x)G(x) \\ F'(x) &= f'(x)G(x) + f(x)G'(x) \\ F'(\zeta) &= f'(\zeta)G(\zeta) \\ m\zeta^{m-1} &= f'(\zeta)\bullet(\zeta^{m/p} - 1) \\ m\zeta^{-1} &= f'(\zeta)\bullet(\xi - 1) \end{aligned}$$

mit der p-ten primitiven Einheitswurzel $\xi = \zeta^{m/p}$. Anwenden der Norm $N = N_{L/\mathbb{Q}}$ der Körpererweiterung vom Grad $\varphi(m)$ liefert:

$$m^{\varphi(m)}N(\zeta)^{-1} = N(f'(\zeta))\bullet N(\xi - 1).$$

Das Minimalpolynom f von ζ hat das Absolutglied 1, also gilt $N(\zeta) = \pm 1$. Es folgt

$$N(f'(\zeta))N(\xi-1) = \pm m^{\varphi(m)}.$$

Zum Beweis der Behauptung reicht es zu zeigen,

$$N(\xi - 1) = \pm p^{m/p}.$$

Aus den Körpererweiterungen

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[p]{1}) \subseteq L$$

der Grade $\varphi(p) = p - 1$ und $\varphi(m)/\varphi(p) = p^{n-1} = m/p$ lesen wir ab, es gilt[63]

$$N(\xi-1) = (N_{\mathbb{Q}(\sqrt[p]{1})/\mathbb{Q}}(\xi-1))^{m/p}$$

Es reicht somit, zu zeigen,

$$N_{\mathbb{Q}(\sqrt[p]{1})/\mathbb{Q}}(\xi-1) = \pm p.$$

Das Minimalpolynom von ξ über $\mathbb{Q}$ ist

$$g(x) = \frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + ... + x + 1.$$

Damit ist

$$\begin{aligned} N_{\mathbb{Q}(\sqrt[p]{1})/\mathbb{Q}}(\xi-1) &= \pm\, N_{\mathbb{Q}(\sqrt[p]{1})/\mathbb{Q}}(1 - \xi) \\ &= \pm\, g(1) \\ &= \pm\, p. \end{aligned}$$

QED.

5.1.14 Die Diskriminante von $\mathbb{Q}(\sqrt[m]{1})/\mathbb{Q}$, allgemeiner Fall

Seien $m > 1$ ein natürliche Zahl, ζ eine primitive m-te Einheitswurzel und

$$L := \mathbb{Q}(\sqrt[m]{1}) = \mathbb{Q}(\zeta).$$

Dann gilt:

(i) $[L:\mathbb{Q}] = \varphi(m)$.

(ii) $\delta(\mathcal{O}_L/\mathbb{Z}) = m^{\varphi(m)} / \prod_{p|m} p^{\varphi(m)/(p-1)}$

(iii) Die Potenzen

---

[63] Weil ξ-1 bereits im mittleren Körper liegt.

$$1, \zeta, \zeta^2, \ldots, \zeta^{\varphi(m)-1}$$

bilden ein linear unabhängiges Erzeugendensystem des $\mathbb{Z}$-Moduls $\mathcal{O}_L$.

Beweis. Aussage (i) gilt nach 5.1.8. Die beiden anderen Aussagen gelten nach 5.1.13 zumindest für den Fall, daß m eine Primzahlpotenz ist.
Es reicht also zu zeigen, aus der Gültigkeit von (ii) und (iii) für zwei teilerfremde Zahlen m' und m",

$$(m', m") = 1,$$

folgt deren Gültigkeit für deren Produkt

$$m = m' \bullet m".$$

Wir bezeichnen mit

$$\zeta', \zeta"$$

primite m'-te bzw. primitive m"-te Einheitswurzeln und setzen

$$L' := \mathbb{Q}(\zeta'),$$
$$L" := \mathbb{Q}(\zeta").$$

Nach 5.1.3 gilt

$$L = L'L",$$

und nach 5.1.8 ist

$$[L:\mathbb{Q}] = \varphi(m)$$
$$[L':\mathbb{Q}] = \varphi(m')$$
$$[L":\mathbb{Q}] = \varphi(m")$$

Weil m' und m" teilerfremd sind, induzieren die natürlichen Abbildungen auf den Faktorring (nach dem chinesischen Restesatz) einen Isomorphismus

$$\mathbb{Z}/m\mathbb{Z} \xrightarrow{\cong} \mathbb{Z}/m\#\mathbb{Z} \times \mathbb{Z}/m"\mathbb{Z},\ x \bmod m \mapsto (x \bmod m', x \bmod m").$$

Dabei entspricht die Multiplikation links gerade der koordinatenweisen Multiplikation rechts. Der zugehörige Isomorphismus der Einheitengruppen hat deshalb die Gestalt

$$G(m) \xrightarrow{\cong} G(m') \times G(m"),\ x \bmod m \mapsto (x \bmod m', x \bmod m").$$

Nach 5.1.8 sind die primen Restklassengruppen isomorph zu den Galois-Gruppen der hier betrachteten Körper-Erweiterungen. Der letzte Isomorphismus bekommt dadurch die Gestalt

$$G(L/\mathbb{Q}) \xrightarrow{\cong} G(L'/\mathbb{Q}) \times G(L"/\mathbb{Q}),\ \sigma \mapsto (\sigma|_{L'}, , \sigma|_{L"}). \qquad (1)$$

Diese Faktor-Zerlegung impliziert, daß die exakten Sequenzen

$$1 \longrightarrow G(L/L') \longrightarrow G(L/\mathbb{Q}) \xrightarrow{\alpha} G(L'/\mathbb{Q}) \longrightarrow 1,\ \alpha(\sigma) = \sigma|_{L'},$$

$$1 \longrightarrow G(L/L") \longrightarrow G(L/\mathbb{Q}) \xrightarrow{\beta} G(L"/\mathbb{Q}) \longrightarrow 1,\ \beta(\sigma) = \sigma|_{L"},$$

zerfallen, wobei die Kerne von α bzw. β mit den beiden Faktoren der Zerlegung (1) identifiziert werden:

$$G(L"L'/L') \xrightarrow[\beta]{\cong} G(L"/\mathbb{Q}),\ G(L'L"/L") \xrightarrow[\alpha]{\cong} G(L'/\mathbb{Q}),$$

Die Faktorzerlegung (1) wird dadurch eine Zerlegung der Galois-Gruppe links in ein direktes Produkt der beiden Untergruppen:

$$G(L'L"/\mathbb{Q}) = G(L'L"/L") \times G(L"L'/L').$$

Aus dem Hauptsatz der Galois-Theorie erhalten wir

$$\mathbb{Q} = L^{G(L/\mathbb{Q})} = L^{G(L/L'')} \bigcap L^{G(L/L')} = L' \bigcap L''.$$

Zum Beweis der Behauptung reicht es deshalb, die nachfolgende Aussage zu beweisen. **QED**.

5.1.15 Verhalten der Diskriminante bei linear disjunkten Erweiterungen

Seien K ein Zahlenkörper,

$$L'/K \text{ und } L''/K$$

zwei Galois-Erweiterungen der Grade

$$[L':K] = n' \text{ und } [L'':K] = n''$$

mit

$$L' \bigcap L'' = K$$

und

$$\omega'_1, \ldots, \omega'_{n'} \in L' \text{ bzw. } \omega''_1, \ldots, \omega''_{n''} \in L''$$

K-Vektorraumbasen, welche die Ganzheitsringe $\mathcal{O}_{L'}$, bzw. $\mathcal{O}_{L''}$ über $\mathcal{O}_K$ erzeugen. Wir nehmen außerdem an, die Diskriminanten

$$d' := \det(Tr_{L'/K}(\omega'_i \omega'_j)) \text{ und } d'' := \det(Tr_{L''/K}(\omega''_i \omega''_j))$$

dieser Basen[64] sind teilerfremd in dem Sinne, daß es Elemente $x', x'' \in \mathcal{O}_K$ gibt mit

$$x'd' + x''d'' = 1.$$

Dann bilden die Produkte

$$\omega'_i \omega''_j \text{ mit } i = 1, \ldots, n' \text{ und } j = 1, \ldots, n''$$

ein Erzeugendensystem des Ganzheitsrings $\mathcal{O}_L$ von $L = L'L''$ über $\mathcal{O}_K$ mit der Diskriminante

$$d = d'^{n''} d''^{n'}.$$

Beweis (vgl. Neukirch, J.: Algebraic number theory, Prop. 2.11). Man beachte, mit L' und L'' ist auch L ein Galois-Erweiterung von K.[65] Wegen $L' \bigcap L'' = K$ ergibt sich aus dem kommutativen Diagramm

$$\begin{array}{ccc} L'' & \overset{x}{\hookrightarrow} & L \\ {\scriptstyle n''}\bigcup & & \bigcup{\scriptstyle y}, \\ K & \overset{n'}{\hookrightarrow} & L' \end{array}$$

in welchen die eingetragenene Zahlen die Grade der zugehörigen Körper-Erweiterungen bezeichnen sollen, daß[66]

---

[64] Dies sind gerade Erzeuger der Diskriminanten der freien $\mathcal{O}_K$-Moduln $\mathcal{O}_{L'}$, bzw. $\mathcal{O}_{L''}$.

[65] Ist L' Zerfällungskörper von $f' \in K[x]$ und L'' Zerfällungskörper von $f'' \in K[x]$, so ist $L = L'L''$ Zerfällungskörper von $f'f''$ über K.

[66] Es reicht zu zeigen, $x = n'$. Die zweite Identität folgt analog. Betrachten wir den Einschränkungshomomorphismus

$$h: G(L/L'') \longrightarrow G(L'/K), \sigma \mapsto \sigma|_{L'}, .$$

Weil jedes Erzeugendensystem von L' über K auch ein Erzeugendensystem von $L = L'L''$ über L'' is, ist dieser Homomorphismus injektiv. Es reicht zu zeigen, er ist surjektiv. Es gilt

$$x = n' \text{ und } y = n''$$

also

$$[L: K] = n'n''$$

gilt. Die Produkte $\omega'_i\omega''_j$ bilden also eine K-Vektorraumbasis von L. Sei jetzt $\alpha \in \mathcal{O}_L$. Dann hat α die Gestalt

$$\alpha = \sum_{i,j} a_{ij}\, \omega'_i\omega''_j \text{ mit } a_{ij} \in K. \quad (1)$$

Wir haben zu zeigen,

$$a_{ij} \in \mathcal{O}_K \text{ für alle i und j} \quad (2)$$

Aus (1) folgt

$$\alpha = \sum_j \beta_j\omega''_j \text{ mit } \beta_j = \sum_i a_{ij}\omega'_i \in L' \quad (3).$$

Wir führen Bezeichnungen für die Elemente der Galois-Gruppen von L/L' und L/L'' ein:

$$G(L''L'/L') = \{\sigma''_1,...,\sigma''_{n''}\}$$

$$G(L'L''/L'') = \{\sigma'_1,...,\sigma'_{n'},\}$$

Dann gilt

$$G(L/K) =^{67} \{\sigma'_k\sigma''_\ell \mid k = 1, \dots, n', \ell = 1, \dots, n''\}. \quad (4)$$

Wir setzen

$$A := (\sigma''_i(\omega''_j)),\ a := \begin{pmatrix} \sigma''_1\alpha \\ \dots \\ \sigma''_{n''}\alpha \end{pmatrix},\ b := \begin{pmatrix} \beta_1 \\ \dots \\ \beta_{n''} \end{pmatrix}$$

Dann gilt

$$\det(A)^2 = \det(A \bullet A^T) = d''$$

und wegen (3) auch

$$a = Ab.$$

Sei A* die Matrix der Eintrag in der Position (i,j) die Adjunkte von A zur Position (j,i) ist. Durch Multiplikation von links mit A* erhält man dann auf Grund der Formel für die inverse Matrix

$$\det(A)b = A^*a$$

also

$$d''b = \det(A)^2 b = \det(A)A^*a.$$

Nun sind mit α auch die Einträge von a, A und von A* ganz über $\mathcal{O}_K$. Also sind auch die Einträge von d''b ganz über $\mathcal{O}_K$, d.h. die Elemente

---

$$K = L' \bigcap L'' = L^{G(L/L')} \bigcap L^{G(L/L'')} = L' \bigcap L^{G(L/L'')} = L^{,\mathrm{Im}(h)} \supseteq L^{,G(L'/K)} = K.$$

Also gilt überall das Gleichheitszeichen

$$L^{,\mathrm{Im}(h)} = L^{,G(L'/K)},$$

d.h. es ist Im(h) = G(L'/K).

[67] Jedenfalls sind die $\sigma'_k\sigma''_\ell$ Elemente von G(L/K). Wegen # G(L/K) = [L:K] = n'n'' reicht es zu zeigen, sie sind paarweise verschieden. Dazu reicht es zu zeigen,

$$G(L/L') \bigcap G(L/L'') = \{e\}.$$

Ein Element aus dem Durchschnitt läßt alle Elemente von L' fest und alle Elemente von L'', also auch alle Elemente von L'L'' = L.

$$d''\beta_j = \sum_i d''a_{ij}\omega'_i \in L'$$

sind ganz über $\mathcal{O}_K$ (vgl. (3)), d.h. sie liegen on $\mathcal{O}_L$,. Nach Voraussetzung liegen dann die Koeffizienten dieser Linearkombination in $\mathcal{O}_K$:

$$d''a_{ij} \in \mathcal{O}_K \text{ für alle i und alle j.}$$

Indem wir die Rollen von L' und L'' vertauschen, sehen wir analog

$$d''a_{ij} \in \mathcal{O}_K \text{ für alle i und alle j.}$$

Also liegen auch die Elemente

$$a_{ij} = 1 \bullet a_{ij} = (x'd' + x''d'') \bullet a_{ij} = x'(d'a_{ij}) + x''(d''a_{ij}) \in \mathcal{O}_K$$

im Ring der ganzen Zahlen von K.

Wir haben noch die Diskriminante Δ der Basis der $\omega'_i\omega''_j$ zu berechnen. Wegen (4) ist Δ das Quadrat der Determinante

$$\Delta = (\det M)^2$$

der Matrix M mit den Einträgen

$$\sigma'_k\sigma''_\ell\omega'_i\omega''_j = \sigma'_k\omega'_i \bullet \sigma''_\ell\omega''_j$$

wobei hier (k, ℓ) als Zeilen-Index und (i, j) als Spalten-Index diene. Betrachten wir M als n''×n''-Matrix, deren Einträge n'×n'-Matrizen sind. Genauer, der Eintrag von M in der Position (j,ℓ) ist die Matrix

$$Q \bullet \sigma''_\ell\omega''_j,$$

wobei Q die n'×n'-Matrix

$$Q' = (\sigma'_j\omega'_i)$$

bezeichne. Mit anderen Worten,

$$M = \begin{pmatrix} Q' & \dots & 0 \\ \dots & \dots & \dots \\ 0 & \dots & Q' \end{pmatrix} \bullet \begin{pmatrix} \sigma''_1\omega''_1 \bullet Id & \dots & \sigma''_{n''}\omega''_1 \bullet Id \\ \dots & \dots & \dots \\ \sigma''_1\omega''_{n''} \bullet Id & \dots & \sigma''_{n''}\omega''_{n''} \end{pmatrix}$$

wobei hier Id die Einheitsmatrix vom Type (n',n') bezeichne. Durch Permutieren von Zeilen und Spalten kann man erreichen, daß die zweite Matrix die Gestalt der ersten bekommt mit n' Exemplaren einer Matrix Q'' auf der Hauptdiagonalen. Damit gilt

$$\Delta = (\det M)^2 = (\det Q')^{2n''} \bullet (\det Q'')^{2n'}$$

mit $Q'' = (\sigma''_j\omega''_i)$. Die Quadrate der Determinanten von Q' und Q'' sind aber gerade die Diskriminanten d' bzw. d''. Wie behauptet ergibt sich

$$\Delta = d'^{n''}d''^{n'}.$$

QED.

5.2 Kummer-Erweiterungen

5.2.1 Vereinbarungen und Definition

In diesem Abschnitt bezeichnet n eine natürliche Zahl und K einen Körper, der eine n-te primitive Einheitswurzel enthält, sagen wir

$$\zeta \in K, \zeta^n = 1, \zeta^i \neq 1 \text{ für } i = 1, \dots, n-1.$$

Insbesondere ist die Charakteristik von K teilerfremd zu n,

$$ggT(n, char(K)) = 1.$$

Wir wollen in diesem Abschnitt zeigen, daß die zyklischen Erweiterungen von K, deren Grad die Zahl n teilt, sogenannte Kummer-Erweiterungen sind, d.h. Erweiterungen der Getstalt

$$K(\sqrt[n]{a}).$$

5.2.2. Eine Einbettung der Galois-Gruppe in die multiplikative Gruppe des Körpers

Seien n eine natürliche Zahl und K ein Körper, der eine n-te primitive Einheitswurzel

$$\zeta \in K$$

enthält.

(i) Für jedes Element $a \in K - \{0\}$ gibt es dann eine endliche Galois-Erweiterung

$$K(\sqrt[n]{a}),$$

welche von einer (und von jeder) Nullstelle des Polynoms

$$X^n - a \qquad (1)$$

über K erzeugt wird, und mit dem Zerfällungskörper dieses Polynoms zusammenfällt.

(ii) Ist α eine Nullstelle dieses Polynoms, so ist die Abbildung

$$\psi_\alpha : G(K(\sqrt[n]{a})/K) \longrightarrow K^*, \sigma \mapsto \sigma(\alpha)/\alpha,$$

ein injektiver Gruppen-Homomorphismus, der nicht von der speziellen Wahl von α abhängt.

(iii) Repräsentiert a ein Element der Ordnung n in der multiplikativen Gruppe

$$K^*/(K^*)^n,$$

so ist das Polynom (1) irreduzibel über K. Die Galois-Gruppe ist zyklisch von der Ordnung n und wird von dem Automorphismus σ mit

$$\sigma(\alpha) = \alpha\zeta$$

erzeugt.

Beweis. Zu (i). Seien α eine Nullstelle von (1) in einer algebraischen Erweiterung von K und

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

Dann liegen sämtliche Nullstellen

$$\alpha, \alpha\zeta, \alpha\zeta^2, \ldots, \alpha\zeta^{n-1} \qquad (2)$$

dieses Polynoms in L, d.h. L ist der Zerfällungskörper von L über K, und wir verwenden die Bezeichnung

$$L = K(\sqrt[n]{a}).$$

Weil n teilerfremd zur Charakteristik von K ist, ist das Polynom (1) separabel, d.h. L/K ist separabel, also eine endliche Galois-Erweiterung.

Zu (ii). Jeder Automorphismus σ von L/K permutiert die Nullstellen (2) von (1). Insbesondere ist

$$\sigma(\alpha) = \alpha\zeta^b.$$

Der Automorphismus ist durch seinen Wert an der Stelle α bereits vollständig festgelegt, d.h. die Abbildung

$$\psi_\alpha: \sigma \mapsto \zeta^b = \sigma(\alpha)/\alpha$$

ist injektiv. Sie hängt nicht von der speziellen Wahl von α ab: ist nämlich β eine weitere Nullstelle des Polynoms (1), so gilt

$$\beta = \alpha\zeta^c,$$

also

$$\begin{aligned}\psi_\beta(\sigma) &= \sigma(\beta)/\beta \\ &= \sigma(\alpha\zeta^c)/(\alpha\zeta^c) \\ &= \sigma(\alpha)/\alpha \qquad \text{(weil } \zeta \in K \text{ invariant ist bei } \sigma) \\ &= \psi_\alpha(\sigma).\end{aligned}$$

Schließlich ist ψ_α ein Gruppen-Homomorphismus:

$$\begin{aligned}\psi_\alpha(\sigma\tau) &= \sigma\tau(\alpha)/\alpha \\ &= \sigma\tau(\alpha)/\tau(\alpha) \bullet \tau(\alpha)/\alpha \\ &= \psi_{\tau(\alpha)}(\sigma) \bullet \psi_\alpha(\tau) \\ &= \psi_\alpha(\sigma) \bullet \psi_\alpha(\tau) \qquad \text{(Unabhängigkeit von } \psi_\alpha \text{ von } \alpha)\end{aligned}$$

Zu (iii). Repräsentiere a ein Element der Ordnung n in $K^*/(K^*)^n$. Dann ist a^r genau dann eine n-te Potenz in K*, wenn n ein Teiler von r ist:

$$a^r \text{ ist n-te Potenz in } K^* \Leftrightarrow n \mid r \qquad (3)$$

Zeigen wir die Irreduzibilität des Polynoms (1) über K. Angenommen,

$$X^n - a = f(X) \bullet g(X) \text{ mit } f, g \in K[X] \text{ normiet.}$$

Sei $r > 0$ der Grad von f. Dann ist f Produkt von r Faktoren der Gestalt $X - \zeta^i\alpha$. Das Absolutglied $b \in K$ von f läßt sich dann schreiben als

$$b = f(0) = (-1)^r\zeta'\alpha^r$$

mit einer n-ten Einheitswurzel ζ'. Es folgt

$$b^n = (-1)^{nr}\alpha^{nr} = (-1)^{nr}a^r.$$

Insbesondere ist a^r eine n-te Potenz, d.h. nach (3) gilt $n \mid r$. Dann ist aber $r = n$ und

$$X^n - a = f(X).$$

Wir haben gezeigt, das Polynom (1) ist irreduzibel. Damit gilt

$$\#\, G(K(\sqrt[n]{a})/K) = [K(\sqrt[n]{a}) : K] = n.$$

Wir verwenden den Injektiven Homomorphismus ψ_α, um die Galois-Gruppe mit einer Untergruppe von K* zu identifizieren. Diese Untergruppe besteht dann aus Elementen deren Ordnung n teilt, d.h. aus n-ten Einheitswurzeln,

$$\psi_\alpha(G(K(\sqrt[n]{a})/K)) \subseteq <\zeta>.$$

Auf beiden Seiten stehen Gruppen der Ordnung n, d.h. es gilt das Gleichheitszeichen. Rechts steht aber eine zyklische Gruppe. Also ist auch die Galois-Gruppe zyklisch (und von der Ordnung n).

Sei σ der K-Automorphismus von $K(\sqrt[n]{a})$ mit

$$\sigma(\alpha) = \alpha\zeta.$$

Einen solchen K-Åutomorphismus gibt es, weil die Galois-Gruppe transitiv auf den Nullstellen des irreduziblen Polynoms (1) operiert. Er ist durch die angegebene Identität eindeutig bestimmt, weil α die Erweiterung $K(\sqrt[n]{a})$ über K erzeugt. Wegen

$$\sigma^i(\alpha) = \alpha\zeta^i \neq \alpha \text{ für } i = 1, \ldots, n-1$$

hat σ die Ordnung n, erzeugt also die Galois-Gruppe.

QED.

5.2.3 Zyklische Erweiterungen sind Kummersch

Seien n eine natürliche Zahl und K ein Körper, der eine n-te primitive Einheitswurzel

$$\zeta \in K$$

enthält. Für jede zyklische Erweiterung L/K des Grades n (d.h. jede Galois-Erweiterung mit zyklischer Galois-Gruppe der Ordnung n) gibt es dann ein Element $b \in K^*$ mit

$$L = K(\sqrt[n]{b}).$$

Jedes solche Element b repräsentiert ein Element der Ordnung n in $K^*/(K^*)^n$.

Beweis. Sei σ ein Erzeuger der Galois-Gruppe G(L/K). Nach dem Satz von der Normal-Basis gibt es ein $\gamma \in L$ derart, daß die Elemente

$$\gamma, \sigma\gamma, \sigma^2\gamma, \ldots, \sigma^{n-1}\gamma \qquad (1)$$

eine K-Vektorraum-Basis von L bilden. Sei

$$\beta := \sum_{s=0}^{n-1} \zeta^s \sigma^s(\gamma).$$

Dann gilt $\beta \neq 0$ (weil die Element (1) K-linear unabhängig sind) und

$$\sigma(\beta) = \zeta^{-1}\beta.$$

Es folgt

$$\sigma(\beta^i) = \zeta^{-i}\beta^i$$

also $\sigma(\beta^i) \neq \beta^i$ für i = 1, ... , n-1 und $\sigma(\beta^n) = \beta^n$, d.h.

$$\beta^n \in K \text{ und } \beta^i \notin K \text{ für } i = 1 , \dots , n-1. \qquad (2)$$

Damit repräsentiert $\beta^n =: b$ ein Element der Ordnung n in $K^*/(K^*)^n$.[68] Nach 5.2.2 ist dann aber

$$K(\beta) = K(\sqrt[n]{b})$$

eine Körpererweiterung des Grades n von K, die ganz in L liegt. Weil L denselben Grad n über K besitzt, folg

$$L = K(\sqrt[n]{b}). \qquad (3)$$

Sei umgekehrt $b \in K$ ein Element, so daß (3) gilt. Bezeichne β einen Erzeuger der Erweiterung (3) mit $\beta^n = b$. Angenommen, die Ordnung des durch b in $K^*/(K^*)^n$ repräsentierten Elements ist kleiner als n, sagen wir

$$b^r = a^n \text{ für ein } a \in K \text{ und ein } r \in \{1, \dots , n-1\}.$$

Dann gilt $\beta^{nr} = b^r = a^n$, d.h. β^r/a ist eine n-te Einheitswurzel (und damit in K). Indem wir a durch das Produkt mit dieser n-ten Einheitwurzel ersetzten, erreichen wir $\beta^r/a = 1$, d.h. β ist Nullstelle des Polynoms

$$X^r - a \in K[X].$$

Dann ist aber

$$\begin{aligned} [L:K] &= [K(\sqrt[n]{b}) : K] \\ &= [K(\beta) : K] && \text{(nach Wahl von } \beta) \\ &\leq \deg X^r - a && (\beta \text{ ist Nullstelle von } X^r - a) \\ &= r \\ &< n \end{aligned}$$

im Widerspruch dazu, daß L/K zyklisch vom Grad n sein soll.
QED.

---

[68] Wäre b^r bereits für ein r < n eine n-te Potenz in K*, sagen wir $b^r = a^n$ mit $a \in K$, so wäre $\beta^{nr} = a^n$, also wäre

$$\beta^r/a$$

eine n-te Einheitswurzel und damit ein Element von K. Dann würde aber auch β^r in K liegen im Widerspruch zu (2).

Anhang: der Satz von Kummer

6. Gruppen-Kohomologie

7. Proendliche Gruppen

8. Lokale Klassenkörpertheorie

9. Globale Klassenkörpertheorie

10. ζ-Funktionen und L-Funktionen

11. Zum Klassenkörper-Turm

12. Halbeinfache algebraische Gruppen

13. Anwendung von Berechnungen in der Klassenkörpertheorie

14. Komplexe Multiplikation

15. ℓ-Erweiterungen

Aufgaben

Literatur

Bundschuh, P.
[1] Einführung in die Zahlentheorie, Springer, Berlin 1992

Cartan, H., Eilenberg, S.
[1] Homological algebra, Princeton University Press 1956

Cassels, J.W.S., Fröhlich, A.
[1] Algebraic number theory, Academic Press, London and New York 1967

Hartshorne, R.
[1] Algebraic geometry, Springer, Berlin 1977

Kochendörffer, R.
[1] Einführung in die Algebra, VEB Deutscher Verlag der Wissenschaften, Berlin 1966

Matsumura, H.
[1] Commutative ring theory, Cambridge University Press, Cambridge 1980

Neukirch, Jürgen,
[1] Algebraic number theory, Springer, Berlin-Heidelberg 1999.

Noether, E.
[1] Normalbasis bei Körpern ohne höhere Verzweigung, J. reine und angew. Math. 167 (1932), 147-152.

Pieper, H.
[1] Variationen über ein zahlentheoretisches Thema von C.F. Gauß, VEB Deutscher Verlag der Wissenschaften, Berlin 1978
Serre, J.-P.
[1] Corps locaux, Hermann, Paris 1962.

Silverman, J.H.
[1] The arithmetic of elliptic curves, Springer, New York 1986

Swan, R.S.
[1] Induced representations and projective modules, Ann. Math. 71 (1960),552-578.

Shafarevich, I.R., Borevich, S.I.
[1] Number theory, Moscow 1972

Waerden, B.L. van der
[1] Algebra, Heidelberger Taschenbücher I und II, Springer, Berlin-Heidelberg-New York 1966 und 1967
Weil, Andrè
[1] Algebraic theory of numbers, Annals of Math. Studies, Princeton 1940
[2] Adeles and algebraic groups, Inst. Adv. Studies, Princeton 1961.
[3] Basic number theory, Springer, Berlin-New York-Heidelberg 1967
[4] The apprenticeship of a mathematician, Birkhäuser, Basel-Boston-Berlin 1992

Weiss, E.
[1] Algebraic number theory, McGraw Hill, New York 1963
Zariski, O., Samuel, P.
[1] Commutative algebra I + II, Springer, New York Heidelberg Berlin 1958 und 1960.

Index

Inhalt