Diskriminanten, Differenten und Steinitzklassen relativer Zahlkörper

Dissertation

der Fakultät für Mathematik und Physik
der Eberhard-Karls-Universität Tübingen
zur Erlangung des Grades eines Doktors
der Naturwissenschaften

vorgelegt von
Rebecca Roy
aus Kapfenhardt

2003

Tag der mündlichen Qualifikation: 23.07.2003

Dekan:	Prof. Dr. H. Müther
1. Berichterstatter:	Prof. Dr. P. Schmid
2. Berichterstatter:	Prof. Dr. W. Knapp

Inhaltsverzeichnis

Einleitung

Gegeben ist eine Körpererweiterung $L|K$ algebraischer Zahlkörper mit $B|A$ als Ringe ganzer Zahlen und Idealklassengruppen $C\ell_L$, $C\ell_K$. Die Differente bzw. Diskriminante von $L|K$ bezeichnen wir mit $\mathcal{D}$ bzw. δ. Als A-Modul ist B endlich erzeugt und torsionsfrei, also projektiv. Allerdings ist B im Allgemeinen nicht frei über A. Nach Steinitz ist B als A-Modul charakterisiert durch seinen Rang und seine Steinitzklasse $s_A(B) \in C\ell_K$. Die Steinitzklasse $s_A(B)$ ist genau dann trivial, wenn eine A-Basis von B existiert. Eine solche Basis nennt man eine (relative) Ganzheitsbasis. Ist A ein Hauptidealring, so existiert immer eine Ganzheitsbasis für B. Für den allgemeinen Fall gibt es kaum Kriterien zur Untersuchung, ob B ein freier A-Modul ist oder nicht.
Das am häufigsten zitierte Resultat wurde von E. Artin im Jahre 1950 [Ar] veröffentlicht. Ist $\delta(m_\theta)$ die Diskriminante des Minimalpolynoms m_θ von θ, wobei $\theta \in B$ die Körpererweiterung $L|K$ erzeugt, so gilt

$$\delta = \delta(m_\theta) \cdot \mathfrak{a}^2$$

mit einem Ideal $\mathfrak{a} \in I_A$. Artin hat gezeigt, dass genau dann eine Ganzheitsbasis existiert, wenn das Ideal $\mathfrak{a} = \sqrt{\delta/\delta(m_\theta)}$ ein Hauptideal in A ist. In Kapitel 1 werden wir sehen, dass dieses Ideal in der Steinitzklasse $s_A(B)$ liegt.
Existiert eine Ganzheitsbasis für $B|A$, so ist die Diskriminante ein Hauptideal in A. Die Umkehrung gilt leider nicht, wie durch ein Gegenbeispiel von S. Pierce [Pie] belegt wird. Mit der Einführung der idealtheoretischen Diskriminante gelingt A. Fröhlich [Fr1] 1960 eine Vereinfachung dieses Kriteriums. Für eine Erweiterung $L|K$ existiert genau dann eine (relative) Ganzheitsbasis, wenn die idealtheoretische Diskriminante durch ein Hauptidel repräsentiert werden kann. Ein weiteres Resultat von Fröhlich in diesem Zusammenhang besagt, dass die idealtheoretische Diskriminante modulo Hauptidelen ein Quadrat x^2 ist, dessen Wurzel x unter der kanonischen Abbildung Ψ von der Idelgruppe J_K in die Idealgruppe I_K ein Ideal der Steinitzklasse $s_A(B)$ ergibt.
Hieraus oder aus obiger Gleichung $\delta = \delta(m_\theta) \cdot \mathfrak{a}^2$ ist es offensichtlich, dass die Diskriminante ein Quadrat in der Idealklassengruppe $C\ell_K$ ist. Nach einem tiefliegenden Satz von E. Hecke [He] von 1923 ist auch die Differente $\mathcal{D}$ ein Quadrat in $C\ell_L$. Diese Eigenschaft der Differente gilt, im Gegensatz zur entsprechenden Eigenschaft der Diskriminante, nur

für Differenten in algebraischen Zahlkörpern, wie Fröhlich, Serre und Tate [FST] 1962 zeigen konnten.
E. Hecke bewies (wie A. Weil [We] 1967) die Existenz einer Quadratwurzel der Differente in $C\ell_L$ mit Methoden der analytischen Zahlentheorie, wie etwa Untersuchungen von Gaußschen Summen oder L-Reihen. Auch J. V. Armitage [Arm] ging in seinem Beweis so vor, er studierte Funktionalgleichungen gewisser L-Reihen.
Schließlich gelang M. Knebusch und W. Scharlau 1971 in [KS] ein algebraischer Beweis des Satzes von Hecke, der aber keineswegs elementar ist. Sie studierten Witt-Gruppen algebraischer Zahlkörper und zeigten dann, dass die Differente ein "erzeugendes (quadratisches) Reziprozitätsgesetz" zulässt. Dies wiederum ist äquivalent zur Existenz einer Quadratwurzel in $C\ell_L$.

In dieser Arbeit versuchen wir zunächst Kriterien für die Existenz von relativen Ganzheitsbasen herzuleiten. In Kapitel 3 beschränken wir uns auf unverzweigte Erweiterungen, d.h. Erweiterungen, in denen die Diskriminante δ und die Differente $\mathcal{D}$ trivial sind. Wir werden sehen, dass in einer unverzweigten Galoiserweiterung $L|K$ die Frage nach der Existenz einer relativen Ganzheitsbasis anhand der Galoisgruppe G beantwortet werden kann. Dabei wird sich zeigen, dass in unverzweigten Erweiterungen $L|K$, deren Galoisgruppe G eine zyklische 2-Sylowgruppe hat, die Steinitzklasse $s_A(C)$ der dann einzigen quadratischen Teilerweiterung $F|K$ (C der Ring ganzer Zahlen in F) entscheidend für die Steinitzklasse $s_A(B)$ von $L|K$ ist.

Hauptsatz 1. *Sei $L|K$ galoissch und an allen endlichen Stellen unverzweigt. Genau dann ist $s_A(B) \neq 1$, wenn es genau eine quadratische Teilerweiterung $F|K$ in $L|K$ gibt und in dieser $s_A(C) \neq 1$ ist.*

Es ist eine wohlbekannte Tatsache, dass die Differente $\mathcal{D}$ unter der Norm $N_{L|K}$ auf die Diskriminante δ abgebildet wird und sowohl Differente als auch Diskriminante Quadrate in der entsprechenden Idealklassengruppe sind. Dies wirft die Frage auf, ob eine Quadratwurzel Δ der (Idealklasse der) Differente $[\mathcal{D}]$ existiert, deren Norm $N_{L|K}(\Delta) = s_A(B)$ die Steinitzklasse ist. Wir nennen eine solche Idealklasse eine *Steinitzwurzel*. Bezeichnet q_K bzw. q_L die Abbildung, die jeder Idealklasse in K bzw. L ihr Quadrat zuordnet, so haben wir für eine Steinitzwurzel die Gleichung

$$N_{L|K} \circ q_L(\Delta) = q_K \circ N_{L|K}(\Delta).$$

Eine Wurzel der Differente in $C\ell_L$ mit dieser Eigenschaft gibt es immer. Entscheidend ist, dass für eine Steinitzwurzel $N_{L|K}(\Delta) = s_A(B)$ gelten muss. Da die Umkehrabbildung zu q_K, das Ziehen der Quadratwurzel in $C\ell_K$, im Allgemeinen nicht eindeutig ist, ist es nur im Falle eines Körpers K mit ungerader Klassenzahl h_K offensichtlich, dass eine

Steinitzwurzel existieren muss.
Betrachten wir etwa die Körpererweiterung $L|K$ mit $L = \mathbb{Q}(\sqrt{-3}, \sqrt{5})$ und $K = \mathbb{Q}(\sqrt{-15})$, so ist leicht zu zeigen, dass es keine Steinitzwurzel geben kann. Da L Klassenzahl 1 hat [Ha2, Satz 43], existiert in $C\ell_L$ kein Element der Ordnung 2. Die Steinitzklasse $s_A(B)$ hat jedoch Ordnung 2 in $C\ell_K$ und kann demnach nicht im Bild der Norm $N_{L|K}$ liegen. Die Existenz einer Steinitzwurzel ist in diesem Fall also unmöglich.
Für eine Wurzel der Differente in $C\ell_L$ gibt es also keine allgemein gültige zahlentheoretische Interpretation wie etwa für eine Wurzel der Diskriminante in $C\ell_K$. J.-P. Serre hat in einer (brieflichen) Diskussion angemerkt, dass die (Galois-invariante) Differente in der Regel keine Galois-invariante Quadratwurzel in $C\ell_L$ hat.
Wir werden zeigen, dass in Erweiterungen ungeraden Grades immer eine Steinitzwurzel existiert. Für quadratische Erweiterungen werden wir allerdings zusätzliche Voraussetzungen benötigen. Einen Zugang zur Steinitzwurzel in Erweiterungen vom Grad 2 schaffen wir uns idealtheoretisch und führen nach dem Vorbild von A. Fröhlich in Kapitel 5 die *idealtheoretische Differente* $\mathcal{D}^*$ von $L|K$ ein. Damit ergibt sich in Kapitel 7 schließlich das folgende Resultat:

Hauptsatz 2. *Sei $L|K$ eine Galoiserweiterung mit auflösbarer Gruppe G. In jeder quadratischen Teilerweiterung $E|F$ von $L|K$ gelte $E = F(\sqrt{a})$ mit a ganz in F. Jedes Primideal von F, das (a) teilt, sowie jede dyadische Primstelle von F verzweige in E. Dann gibt es ein Ideal $\mathfrak{W}$ in L mit $\mathfrak{W}^2 = \mathcal{D}$ und die Idealklasse $[\mathfrak{W}]$ ist eine Steinitzwurzel für $L|K$. Ist die Gruppe G 2-überauflösbar, so ist die Steinitzwurzel Δ sogar Galois-invariant.*

Im Beweis dieses Satzes geht das Heckesche Resultat über die Existenz einer Quadratwurzel der Differente in $C\ell_L$ nicht ein. Verzichten wir allerdings auf die Forderung, dass G auflösbar ist, kommen wir um die Einbeziehung dieses Satzes von Hecke nicht herum. Wir finden dann zwar kein Ideal $\mathfrak{W}$ in L mit den beschriebenen Eigenschaften, aber zumindest eine Idealklasse Δ, die eine Steinitzwurzel ist. Die Existenz von Steinitzwurzeln in den eben beschriebenen Erweiterungen, insbesondere in Erweiterungen von ungeradem Grad ist somit geklärt. Zu einer allgemeineren Aussage für Erweiterungen geraden Grades kann diese Arbeit leider keinen weiteren Beitrag leisten. Wir werden allerdings anhand von Beispielen versuchen, Erkenntnisse über die Existenz einer Steinitzwurzel in Erweiterungen mit geradem, etwa 2-Potenz-Grad, zu erhalten. Daher widmen wir das abschließende Kapitel dem Studium einer innerhalb der algebraischen Zahlentheorie klassischen 2-Potenz-Erweiterung, der (kanonischen) zyklotomischen $\mathbb{Z}_2$-Erweiterung eines imaginär quadratischen Zahlkörpers K_0. Die Theorie der $\mathbb{Z}_p$-Erweiterungen wurde in den 60-er Jahren des vergangenen Jahrhunderts von K. Iwasawa entwickelt und zählt noch heute zu einem der fruchtbarsten Gebiete innerhalb der algebraischen Zahlentheorie.

Dabei ist die Situation mit einem imaginär quadratischen Grundkörper K_0 schon immer von besonderem Interesse gewesen.
Nach [Wa, Thm. 13.4] gibt es genau zwei verschiedene $\mathbb{Z}_2$-Erweiterungen von K_0. Bis heute ist jedoch nur die zyklotomische eingehender studiert worden. Sie entsteht durch Komposition von K_0 mit den maximal reellen Teilkörpern der 2-Potenz Kreisteilungskörper. Für diese erhalten wir

Hauptsatz 3. *Sei $K_\infty = \bigcup_{n\in\mathbb{N}} K_n$ die zyklotomische $\mathbb{Z}_2$-Erweiterung eines (imaginär) quadratischen Zahlkörpers K_0. Die Steinitzklasse jeder Teilerweiterung $K_m|K_n$ hat Ordnung 1 oder 2. Genauer gilt:*
Ist die Primzahl 2 in K_0 unverzweigt, oder $K_0 = \mathbb{Q}(\sqrt{-1})$ oder $\mathbb{Q}(\sqrt{-2})$, so ist die Steinitzklasse jeder Teilerweiterung $K_m|K_n$, $n \leq m$ trivial.
Verzweigt die 2 in $K_1|\mathbb{Q}$ mit Verzweigungsindex 2, so ist für die Teilerweiterungen $K_m|K_n$ für $(n,m) \neq (0,1)$ die Steinitzklasse trivial, und im Falle $(n,m) = (0,1)$ hat die Steinitzklasse Ordnung 2, wenn $\delta^{(2)}_{K_0|\mathbb{Q}} = 2^3$ ist.
Verzweigt die 2 in $K_1|\mathbb{Q}$ total, so hat die Steinitzklasse der Erweiterungen $K_m|K_n$ immer Ordnung 2, ausser im Fall $\delta^{(2)}_{K_0|\mathbb{Q}} = 2^3$ und $n = 0, m = 1$. Hier ist die Steinitzklasse trivial.

Der Beweis lässt sich problemlos auf reelle quadratische Körper übertragen. Einzig bei den Ordnungen der Steinitzklasse müssen wir Ordnung 2 durch Ordnung ≤ 2 ersetzen. Aus Haupsatz 3 folgt sofort, dass die (relativen) Differenten und Diskriminanten in jeder Erweiterung $K_m|K_n$ Hauptideale sind. Es gibt also in jeder Teilerweiterung von $K_\infty|K_0$ eine Galois-invariante Steinitzwurzel.

Mein herzlicher Dank geht an den Betreuer dieser Arbeit, Herrn Prof. Dr. P. Schmid. Seine wertvollen Anregungen und die freundliche Betreuung waren mir eine große Hilfe. Desweiteren danke ich Herrn PD Dr. U. Riese für die hilfreichen Diskussionen, sowie T. Stumpp, T. Jahnke, A. Schädle, G. Sautter, M. Kölle und M. Fröhlich für die kollegiale Unterstützung beim Entstehen dieser Arbeit.
Ein herzliches Dankeschön gilt der Konrad-Adenauer-Stiftung e.V., die mir mit einem Stipendium die Arbeit an dieser Dissertation ermöglichte.

Notation

L, K, E, F	algebraische Zahlkörper
A, B, C	Ringe ganzer Zahlen in K, L, F
$I_K = I_A$	Idealgruppe von K bzw. A
$H_K = H_A$	Gruppe der Hauptideale in K bzw. A
$C\ell_K = I_K/H_K$	Idealklassengruppe von K
h_K	Klassenzahl von K
$\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{e}$	Ideale in K bzw. A
$[\mathfrak{a}]$	Idealklasse des Ideals $\mathfrak{a}$
$\mathbb{P}_K$, $\mathbb{P}_K^\infty$	Menge der endlichen bzw. unendlichen Primstellen von K
$\overline{\mathbb{P}}_K$	Menge aller Primstellen von K
$\mathfrak{p}$, $\mathfrak{q}$	Primideale in K bzw. A
$\mathfrak{P}$, $\mathfrak{Q}$	Primideale in L bzw. B
$s_A(B)$	Steinitzklasse von B über A
$\iota = \iota_{L\|K}$	Einbettung von I_A in I_B
$N = N_{L\|K}$	Normabbildung von I_B nach I_A bzw. von L^* nach K^*
$Tr = Tr_{L\|K}$	Spurabbildung von L^* nach K^*
U'	Dualmodul des A-Moduls U
$\mathcal{D}$, δ	(relative) Differente bzw. Diskriminante
$m_\theta = m_{K,\theta}$, $m'_\theta = m'_{K,\theta}$	Minimalpolynom von θ über K bzw. dessen Ableitung
W_g	Menge der Wurzeln des Polynoms g
$\mathfrak{f}_\theta$	Führer eines für $L\|K$ primitiven Elementes $\theta \in B$
$v_\mathfrak{p}(\cdot)$	Exponentenbewertung zum Primideal $\mathfrak{p}$
$L_\mathfrak{P}$, $K_\mathfrak{p}$	lokale Körper in L, K bzgl. $\mathfrak{P}$, $\mathfrak{p}$
$B_\mathfrak{P}$, $A_\mathfrak{p}$	Bewertungsringe in $L_\mathfrak{P}$, $K_\mathfrak{p}$
J_K	Idelgruppe von K
$C_K = J_K/K^*$	Idelklassengruppe von K
Ψ	kanonische Abbildung $J_K \to I_K$
$\mathcal{D}^*$, δ^*	idealtheoretische Differente bzw. Diskriminante
ε_n, ζ_n	primitive n-te bzw. primitive 2^{n+2}-te Einheitswurzel
$\varphi(\cdot)$	Eulersche φ-Funktion
$\mathcal{E}_K$	Gruppe der Einheitswurzeln in K

Für ein Element $z \in \mathbb{Z}$ und die Diskriminanten $\delta(m_\theta)$, $\delta(\theta)$ des Minimalpolynoms m_θ bzw. des Elements θ bezeichnen wir mit z, $\delta(m_\theta)$ bzw. $\delta(\theta)$ sowohl die jeweiligen Elemente als auch die von ihnen erzeugten Hauptideale.

Kapitel 1

Steinitzklassen

Stets sind $K \subseteq L$ algebraische Zahlkörper vom Grad $[L : K] = n$ mit den Ringen ganzer Zahlen $A \subseteq B$ und Idealgruppen I_B bzw. I_A. Es bezeichne $C\ell_K = C\ell_A$ die Idealklassengruppe von K bzw. A und h_K ihre Ordnung, die Klassenzahl. Für die Idealklasse eines Ideals $\mathfrak{a}$ schreiben wir $[\mathfrak{a}]$.

1.1 Steinitzklassen

Sei U ein endlich erzeugter, torsionsfreier A-Modul. Dann ist U A-projektiv.
Ist $\{u_1, u_2, \dots u_n\}$, $u_i \in U$, $(i = 1 \dots n)$ eine K-Basis von KU ($\cong K \otimes_A U$), so existieren (geeignete) gebrochene Ideale $\mathfrak{a}_i$ von A , so dass

$$U \cong \mathfrak{a}_1 u_1 \oplus \cdots \oplus \mathfrak{a}_n u_n$$

gilt. Nach Steinitz charakterisieren der Rang $n = rg(U)$ und die Idealklasse $\left[\prod_{i=1}^n \mathfrak{a}_i\right] =: s_A(U)$ den Isomorphietyp von U als A-Modul. Dabei nennt man $s_A(U)$ die *Steinitzklasse* von U. Es ist

$$U \cong \mathfrak{a}_1 u_1 \oplus \cdots \oplus \mathfrak{a}_n u_n \cong Au_1 \oplus Au_2 \oplus \cdots \oplus Au_{n-1} \oplus (\prod_{i=1}^n \mathfrak{a}_i) u_n.$$

1.1 Folgerung. *Genau dann ist U frei über A, wenn $s_A(U) = 1$, also $\prod_{i=1}^n \mathfrak{a}_i$ ein Hauptideal ist.*

1.2 Satz. (Invariant Factor Theorem)
Seien V, U endlich erzeugte torsionsfreie A-Moduln vom gleichen Rang n, so dass $V \subseteq KU$. Dann existieren $\{u_1, \dots u_n\} \subseteq U$ und (gebrochene) Ideale $\mathfrak{a}_1, \dots, \mathfrak{a}_n$, $\mathfrak{e}_1, \dots, \mathfrak{e}_n$ von A mit $\mathfrak{e}_{i+1} \subseteq \mathfrak{e}_i$ $(i = 1, \dots n-1)$ mit der Eigenschaft

$$U \cong \bigoplus_{i=1}^n \mathfrak{a}_i u_i, \qquad V \cong \bigoplus_{i=1}^n \mathfrak{e}_i \mathfrak{a}_i u_i.$$

Die Ideale $\mathfrak{e}_1, \dots \mathfrak{e}_n$ sind durch U und V eindeutig bestimmt. Man nennt sie die Invarianten Faktoren *von V in U.*
Ist $V \subseteq U$, so sind die Ideale $\mathfrak{e}_1, \dots \mathfrak{e}_n$ ganz in A.

Beweis. [CR, p.150-153].

Im Folgenden seien V, U endlich erzeugte A-Moduln von gleichem Rang n.

Nach 1.2 existieren gebrochene Ideale $\mathfrak{a}_i$, $\mathfrak{e}_i$ in A und Elemente $u_i \in U$ $(i = 1, \dots n)$, dass $U \cong \bigoplus \mathfrak{a}_i u_i$ und $V \cong \bigoplus \mathfrak{e}_i \mathfrak{a}_i u_i$. Für $V \subseteq KU$ definieren wir den *Modulindex* oder das *Ordnungsideal*

$$[U : V] = \prod_i \mathfrak{e}_i.$$

Ist $V \subseteq U$, so ist

$$U/V \cong \bigoplus \mathfrak{a}_i u_i \Big/ \bigoplus \mathfrak{e}_i \mathfrak{a}_i u_i \cong \bigoplus \left(\mathfrak{a}_i u_i \Big/ \mathfrak{e}_i \mathfrak{a}_i u_i \right) \cong \bigoplus A/\mathfrak{e}_i$$

ein Torsionsmodul und der Modulindex $[U : V]$ ist ein ganzes Ideal in A.

Die für uns wichtigsten Eigenschaften des Modulindex $[U : V]$ beschreibt das folgende Lemma:

1.3 Lemma. *Sind U, V, W A-Moduln von gleichem Rang, die je eine Basis von L enthalten, so gelten die folgenden Aussagen:*

(i) $[U : W] = [U : V][V : W]$.

(ii) Sei $W \subseteq U$. Genau dann ist $[U : W] = A$, wenn $U = W$.

(iii) Ist $W \subseteq U$, so ist $[U : W]$ ein ganzes Ideal in A.

Beweis. [CF, p.10].

Wir betrachten nun eine nichtausgeartete, symmetrische K-Bilinearform h auf $W = KU$. Der A-Modul U sei ganz bezüglich h, es ist also $h(U \times U) \subseteq A$.

1.4 Definition. Der *Dualmodul* U' von U bezüglich der Bilinearform h ist definiert als

$$U' = \{x \in W | h(x, U) \subseteq A\}.$$

Offensichtlich ist, dass U in U' enthalten ist. Desweiteren ist mit U auch U' projektiv.

1.5 Lemma. *Ist $U \cong \bigoplus \mathfrak{a}_i u_i$, so gilt für den Dualmodul*

$$U' \cong \bigoplus \mathfrak{a}_i^{-1} v_i,$$

wobei $\{v_1, \dots v_n\}$ die Dualbasis von KU zu $\{u_1, \dots u_n\}$ bzgl. h ist $(h(v_i, u_j) = \delta_{ij})$.

Beweis. (Vgl. [OM, p.230]). Es ist $h(\mathfrak{a}_i u_i, \mathfrak{a}_j^{-1} v_j) = 0$ für $i \neq j$ und $h(\mathfrak{a}_i u_i, \mathfrak{a}_i^{-1} v_i) \subseteq A$. Also gilt $\bigoplus \mathfrak{a}_i^{-1} v_i \subseteq U'$. Sei $z = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n \in U'$. Dann folgt insbesondere mit der Bilinearität von h

$$\alpha_i \mathfrak{a}_i = h(\alpha_i v_i, \mathfrak{a}_i u_i) = h(z, \mathfrak{a}_i u_i) \subseteq h(z, U) \subseteq A \quad (z \in U).$$

Es ist also $\alpha_i \mathfrak{a}_i \subseteq A$ und $\alpha_i \in \mathfrak{a}_i^{-1}$, woraus die Behauptung folgt. □

1.6 Folgerung. *Es ist* $s_A(U') = s_A(U)^{-1}$.

1.7 Lemma. *Seien U, V A-Moduln vom gleichen Rang, so gilt:*

(i) Ist $U \subseteq V$, so $V' \subseteq U'$.

(ii) $[U' : V'] = [V : U]$.

Beweis. Teil (i) folgt unmittelbar aus der Definition des Dualmoduls, somit bleibt noch (ii) zu zeigen. Es existieren (gebrochene) Ideale $\mathfrak{a}_i, \mathfrak{e}_i$ in K und Elemente $u_i \in U$, so dass $U = \bigoplus \mathfrak{a}_i u_i$, $V = \bigoplus \mathfrak{e}_i \mathfrak{a}_i u_i$, also $[U : V] = \prod \mathfrak{e}_i =: \mathfrak{e}$.
Nach 1.5 ist mit geeigneten $v_i \in U$

$$U' = \bigoplus \mathfrak{a}_i^{-1} v_i = \bigoplus \mathfrak{e}_i \left(\mathfrak{e}_i^{-1} \mathfrak{a}_i u_i\right) \text{ und } V' = \bigoplus \mathfrak{e}_i^{-1} \mathfrak{a}_i^{-1} v_i,$$

deshalb $[V' : U'] = \prod \mathfrak{e}_i = \mathfrak{e}$. □

In dieser Arbeit interessieren uns algebraische Körperweiterungen $L|K$ eines Zahlkörpers K. Der Ring ganzer Zahlen B in L ist wie jedes seiner Ideale ein Modul vom Rang $n = [L : K]$ über A, dem Ring der ganzen Zahlen von K. Es gibt also auch hier eine K-Basis $\{u_1, \ldots u_n\}$ von $L = KB$ und gebrochene Ideale $\mathfrak{a}_1, \ldots \mathfrak{a}_n$ in A, so dass $B \cong \bigoplus \mathfrak{a}_i u_i$ ist.
Die Steinitzklasse $s_A(B)$ von $B|A$ ist die Idealklasse des Ideals $\prod \mathfrak{a}_i$ in der Idealklassengruppe von A. Ist $s_A(B) = 1$, so ist B als A-Modul frei. Man sagt, es existiert eine *(relative) Ganzheitsbasis* für $L|K$ bzw. $B|A$.

Für algebraische Körpererweiterungen $L|K$ spezifizieren wir nun die Bilinearform h.
Sei $Tr = Tr_{L|K}$ die Spurabbildung von $L|K$, die jedem Element x in L die Summe $\sum_\sigma x^\sigma (\in K)$ zuordnet, wobei σ alle K-Einbettungen von L (in seinen algebraischen Abschluss $\bar{L}$) durchläuft. Insbesondere ist das Bild von $b \in B$ unter der Spur ein Element von A.
Im Folgenden sei stets $h(x_i, x_j) = Tr(x_i x_j)$ für $x_i, x_j \in L$.

Der bezüglich der Spur Tr gebildete Dualmodul B' ist ein (echt) gebrochenes Ideal von B.

Sein Inverses, das ganze Ideal $(B')^{-1}$, nennt man die *Differente* von $L|K$. Diese bezeichnen wir mit $\mathcal{D} = \mathcal{D}_{L|K}$. Der Modulindex $[B' : B]$ heisst die *Diskriminante* von $L|K$ und wird mit $\delta = \delta_{L|K}$ bezeichnet. Bekanntlich sind die Primteiler der Diskriminante δ bzw. der Differente $\mathcal{D}$ gerade die in $L|K$ verzweigenden Primideale.

Ist $\mathfrak{b} \in I_B$, dann ist $\mathfrak{b}$ ein A-Modul mit $rg(\mathfrak{b}) = rg(B) = n$ und wir definieren die Norm $N = N_{L|K}$ des Ideals $\mathfrak{b}$ als (vgl. [CF, p.14])

$$N(\mathfrak{b}) = [B : \mathfrak{b}].$$

Da $\mathfrak{b}$ ein Ideal von B ist, existieren nach 1.2 ganze Ideale $\mathfrak{e}_i$ und gebrochene Ideale $\mathfrak{a}_i$ in A, sowie Elemente $u_i \in L$ $(i = 1, \dots n)$, so dass $B \cong \bigoplus \mathfrak{a}_i u_i$ und $\mathfrak{b} \cong \bigoplus \mathfrak{e}_i \mathfrak{a}_i u_i$ gilt. Damit ist also

$$N(\mathfrak{b}) = [B : \mathfrak{b}] = \prod \mathfrak{e}_i.$$

Da $\prod \mathfrak{e}_i \mathfrak{a}_i = \prod \mathfrak{e}_i \prod \mathfrak{a}_i$ gilt, erhalten wir

$$s_A(\mathfrak{b}) = \big[N(\mathfrak{b})\big] s_A(B). \qquad (*)$$

1.8 Lemma. *Es ist $\delta = N(\mathcal{D})$.*

Beweis. Per Definition ist $\delta = [B' : B]$ und es gilt $1 = [B : B] = [B : B'][B' : B]$, also $[B : B'] = [B' : B]^{-1}$. Mit B' ist auch $\mathcal{D} = (B')^{-1}$ ein Ideal von B und es ist

$$1 = N_{L|K}(B) = N_{L|K}(B'(B')^{-1}) = N_{L|K}(B') N_{L|K}(\mathcal{D}),$$

also

$$N_{L|K}(\mathcal{D}) = N_{L|K}((B')^{-1}) = [B : B']^{-1} = [B' : B] = \delta.$$

□

Anmerkung. Aus dem Beweis ist ersichtlich, dass ebenso $[B' : B] = [B : (B')^{-1}]$ gilt. Auch für beliebige Ideale $\mathfrak{b} \in I_B$ erhalten wir $[B : \mathfrak{b}] = [\mathfrak{b} : B]^{-1}$.

1.9 Satz. *Ist B ein freier A-Modul, also $s_A(B) = 1$, so ist die Diskriminante δ ein Hauptideal. Ist δ ein Hauptideal, so gilt $s_A(B)^2 = 1$.*

Beweis. Nach Lemma 1.5 ist mit $s_A(B) = 1$ auch $s_A(B') = 1$. Nach $(*)$ ist $[N(B')] = \frac{s_A(B')}{s_A(B)} = 1$, also $N(B')$ ein Hauptideal, deshalb ist auch $\delta = N_{L|K}(\mathcal{D}) = N((B')^{-1}) = N_{L|K}(B')^{-1}$ trivial in der Idealklassengruppe $C\ell_K$.
Ist umgekehrt $\delta = [B' : B]$ ein Hauptideal, so ist $B' \cong_A B$, da sich B' und B nur um ein Hauptideal unterscheiden. Wir erhalten damit $s_A(B) = s_A(B')$ und mit 1.6 folgt $s_A(B)^2 = 1$. □

1.10 Folgerung. *Ist die Klassenzahl h_K ungerade, so existiert eine relative Ganzheitsbasis für $L|K$ genau dann, wenn δ ein Hauptideal von A ist.*

Anmerkung. Einen komplizierteren Zugang zu dieser Folgerung findet man etwa bei [Fr1], [Nar, Ch.7 §3].

1.11 Satz. *Es gilt $[\delta] = s_A(B)^2$.*

Beweis Definitionsgemäß ist $\delta = [B' : B]$. Nach 1.5 existieren Elemente $u_i, v_i \in L$ mit $Tr(u_i v_j) = \delta_{ij}$ und Ideale $\mathfrak{a}_i \subseteq A$, so dass

$$B \cong \bigoplus \mathfrak{a}_i u_i = \bigoplus \mathfrak{a}_i^2 \mathfrak{a}_i^{-1} u_i \text{ und } B' \cong \bigoplus \mathfrak{a}_i^{-1} v_i = \bigoplus \mathfrak{a}_i^{-1} u_i w_i$$

gilt. Dabei ist $w_i = u_i^{-1} v_i$. Es ist also $\delta = [B' : B] = \prod_i \mathfrak{a}_i^2 w_i = \prod \mathfrak{a}_i^2 \prod w_i$. Der Übergang zu Idealklassen liefert uns $[\delta] = [\prod \mathfrak{a}_i]^2 = s_A(B)^2$. □

Wir haben bisher die Diskriminante von $L|K$ betrachtet. Sie ist definiert als Modulindex von B in seinem Dualmodul B'. Auch für beliebige endlich erzeugte torsionsfreie A-Moduln $U \subseteq L$ vom Rang n definieren wir deren Diskriminante mutatis mutandis als

$$\delta(U) = [U' : U],$$

mit dem Dualmodul U' von U bezüglich der Spur Tr.

1.12 Lemma. *Sei $\{u_1, \ldots u_n\}$ eine K- Basis von L und $U = \langle u_1, \ldots, u_n \rangle_A$.*
Es gibt ein eindeutig bestimmtes Ideal $i(U)$ mit $\delta(U) = i(U)^2 \delta$ und $i(U) \in s_A(B)^{-1}$.

Beweis. Nach 1.3 und 1.7 gilt mit $i(U) = [B : U]$ für die Diskriminante

$$\begin{aligned} \delta(U) &= [U' : U] = [U' : B'][B' : B][B : U] \\ &= [B' : B][B : U]^2 = \delta \cdot i(U)^2. \end{aligned}$$

Die Eindeutigkeit des Ideals $i(U)$ folgt aus der Torsionsfreiheit der Idealgruppe. □

Sei $\theta \in B$ ein primitives Element für die Körpererweiterung $L|K$, also $L = K(\theta)$. Ist $U = \langle 1, \theta, \ldots, \theta^{n-1} \rangle_A = A[\theta]$, so nennt man das Ideal $i(U) = \big[B : A[\theta]\big] =: i(\theta)$ den *Index von θ* in $B|A$. Nach obigem Lemma ist $i(\theta) \in s_A(B)^{-1}$. Alle diese Indizees $i(\theta)$ liegen also in derselben Idealklassengruppe. Wir erhalten die nachstehende Folgerung.

1.13 Folgerung. *Genau dann ist B A-frei (also $s_A(B) = 1$), wenn für ein beliebiges primitives $\theta \in B$ der Index $i(\theta)$ ein Hauptideal ist.*

Anmerkung. Ist $U = A[\theta]$, so ist die Diskriminante $\delta(U)$ von $U = \langle 1, \theta, \dots \theta^{n-1} \rangle_A$ die (wohlbekannte) Diskriminante $\delta(m_\theta)$ des Minimalpolynoms $m_\theta = m_{K,\theta}$ von θ über K. Bekanntlich ist die Elementdiskriminante $\delta(\theta) = N\big(m'_\theta(\theta)\big)$ und es gilt $\delta(m_\theta) = (-1)^{n(n-1)/2}\delta(\theta)$. Als Hauptideale sind $\delta(\theta)$ und $\delta(m_\theta)$ identisch.

1.14 Folgerung. *Sei $\theta \in B$ ein primitives Element für $L|K$. Genau dann ist B frei über A, wenn die Diskriminante $\delta = (a)$ ein Hauptideal von A ist und Elemente $b \in A$ und $u \in A^*$ existieren, so dass für die Diskriminante des Minimalpolynoms $\delta(m_\theta) = uab^2$ gilt.*

1.15 Folgerung. *Ist für ein beliebiges primitives Element $\theta \in B$ die Diskriminante $\delta(m_\theta)$ ein Quadrat in K^*, so ist δ das eindeutige Quadrat eines Ideals von A, d.h. $\delta^{\frac{1}{2}}$ ist erklärt und $s_A(B) = [\delta^{\frac{1}{2}}]$.*

Beweis. Mit $(w)^2 = \delta(m_\theta)$, $w \in A$, ist $\delta = \delta(m_\theta)i(\theta)^{-2} = \big((w)i(\theta)^{-1}\big)^2$. Da die Idealgruppe I_A torsionsfrei ist, folgt die erste Behauptung. Weiterhin ist nach 1.12 $i(\theta)^{-1} = \delta^{\frac{1}{2}}(w)^{-1}$ ein Ideal in der Steinitzklasse $s_A(B)$. Damit ist $s_A(B) = [\delta^{\frac{1}{2}}]$. □

1.16 Definition. Für ein primitives $\theta \in B$ ist der Führer $\mathfrak{f}_\theta$ als größtes Ideal von B, das in $A[\theta]$ liegt, definiert. Der Führer $\mathfrak{f}_\theta$

$$\mathfrak{f}_\theta = \{a \in A | aB \subseteq A[\theta]\}$$

ist also der größte gemeinsame Teiler aller Ideale von B, die in $A[\theta]$ liegen. Ist etwa $B = A[\theta]$, so ist der Führer $\mathfrak{f}_\theta = B = (1)$.

Die Differente des Elementes θ ist definiert als $\mathcal{D}(\theta) = \mathcal{D}_{L|K}(\theta) = \big(m'_\theta(\theta)\big)$. Sie ist also insbesondere ein Hauptideal. Nach [Nar, Prop. 4.12] gilt für den Führer

$$\mathfrak{f}_\theta = \mathcal{D}(\theta)B'.$$

Der Führer $\mathfrak{f}_\theta$ liegt also in der zur Differente inversen Idealklasse in $C\ell_L$. Wir sehen auch sofort, dass für die Norm des Führers $\mathfrak{f}_\theta$ gilt

$$N(\mathfrak{f}_\theta) = N\big(\mathcal{D}(\theta) \cdot N(B')\big) = \delta(m_\theta)\delta^{-1} = i(\theta)^2.$$

Zum Zusammenhang zwischen der Differente $\mathcal{D}$ und den Elementdifferenten $\mathcal{D}(\theta)$ bleibt anzumerken, dass die Differente $\mathcal{D}$ der größte gemeinsame Teiler (als Ideal) aller Differenten $\mathcal{D}(\theta)$ von (über K) ganzen Elementen $\theta \in L$ ist.
Für die Diskriminante δ gilt dieser Zusammenhang nicht. Diese ist nicht der größte gemeinsame Teiler aller Elementdiskriminanten $\delta(\theta)$ für alle $\theta \in B$, sondern der größte gemeinsame Teiler (als Ideal) aller Diskriminanten $\delta(U) = \delta(u_1, \dots u_n)$ für alle möglichen ganzen K- Basen $\{u_1, \dots u_n\} \subseteq B$ von L.

1.2 Morphismen zwischen Klassengruppen

Wir betrachten die (kanonischen) Abbildungen zwischen den Idealgruppen von L und K und schränken sie auf die Idealklassen ein. Konkret geht es also um die Einbettung

$$\iota = \iota_{L|K} : I_A \to I_B; \mathfrak{a} \mapsto \mathfrak{a}B$$

und die Normabbildung

$$N = N_{L|K} : I_B \to I_A; \mathfrak{b} \mapsto N\mathfrak{b}.$$

Wir bezeichnen die von $\iota_{L|K}$ und $N_{L|K}$ auf die Idealklassengruppe induzierten Abbildungen ebenso. Das Kompositum $N_{L|K} \circ \iota_{L|K}$ dieser beiden Abbildungen bewirkt die Potenzierung mit $n = [L : K]$ auf I_A bzw. $C\ell_K$.

Unser Augenmerk liegt auf der Steinitzklasse $s_A(B)$. Im Allgemeinen gilt nicht, dass sie unter der Abbildung $\iota_{L|K}$ trivial wird, wie folgendes Beispiel belegt.

1.17 Beispiel. Nach [Ha1, p.551] existieren imaginär quadratische Zahlkörper K (etwa $K = \mathbb{Q}(\sqrt{-39})$) mit einer Idealklasse $\Gamma \in C\ell_K$, deren Ordnung durch 4 geteilt wird. Es existiert eine quadratische Erweiterung $L|K$, deren Steinitzklasse $s_A(B) = \Gamma$ ist [Nar, Prop. 7.19]. Damit ist $N_{L|K} \circ \iota_{L|K}(\Gamma) = \Gamma^2 \neq 1$, also ist auch $\iota_{L|K}(\Gamma) \neq 1$.

Ein positives Beispiel erhalten wir, wenn $L = Hi\ell(K)$ der Hilbertsche Klassenkörper von K ist. In L wird jedes Ideal von K zum Hauptideal, also wird auch $s_A(B)$ trivial in $C\ell_L$. In Kapitel 3 werden wir zeigen, dass dies nicht nur in der maximal unverzweigten abelschen Erweiterung, sondern in jeder unverzweigten Erweiterung gilt.

1.18 Lemma. *Es ist* $\iota_{L|K}(s_A(B)) = s_B(B \otimes_A B)$.

Beweis. Es ist $\mathfrak{a}B \cong B \otimes_A \mathfrak{a}$. Ist wie bisher auch $B \cong \oplus_{i=1}^n \mathfrak{a}_i u_i$, so ist

$$B \otimes_A B \cong \oplus_{i=1\ldots n} \mathfrak{a}_i u_i \otimes_A B \cong \oplus_{i=1\ldots n} (B\mathfrak{a}_i) u_i,$$

also ist $B \otimes_A B$ ein projektiver B-Modul vom Rang n. Es ist $\iota_{L|K}(s_A(B))$ die Klasse von $(\prod \mathfrak{a}_i)B = \prod (B\mathfrak{a}_i)$ und dies ist nach Definition genau die Steinitzklasse von $B \otimes_A B$ über B. □

Beim Untersuchen der Normabbildung $N_{L|K}$ konzentriert sich die Fragestellung darauf, ob die Steinitzklasse im Bild der Norm liegt. Da stets $N(\mathcal{D}) = \delta$ gilt, liegt das Quadrat der Steinitzklasse $s_A(B)^2$ immer im Bild der Norm.

Ist $L|K$ eine Galoiserweiterung mit $L \cap Hi\ell(K) = K$, d.h. $L|K$ enthält keine unverzweigte abelsche Teilerweiterung $F|K$ (nicht-trivial), so ist die Normabbildung $N_{L|K}$ auf den

Idealklassengruppen von L und K surjektiv [Wa, Thm. 10.1]. Insbesondere liegt also die Steinitzklasse $s_A(B)$ im Bild der Norm.
In Kapitel 4, 6 und 7 werden wir weitere positive Beispiele kennenlernen und sogar die Urbilder der Steinitzklasse unter der Norm eingehender studieren. Im Moment beschränken wir uns jedoch auf die nächsten zwei Resultate.

1.19 Lemma. *Seien $\mathfrak{a}, \mathfrak{b}$ Ideale in B. Es gilt $s_A(\mathfrak{a}) = s_A(\mathfrak{b})$ genau dann, wenn $[N\mathfrak{a}] = [N\mathfrak{b}]$.*

Beweis. Nach $(*)$ gilt für ein Ideal $\mathfrak{b}$ in A $s_A(\mathfrak{b}) = [N\mathfrak{b}]s_A(B)$. Die analoge Aussage haben wir für das Ideal $\mathfrak{a}$, woraus sofort die Behauptung folgt. □

1.20 Satz. *Genau dann liegt die Steinitzklasse $s_A(B)$ im Bild der Norm $N_{L|K}$, wenn ein Ideal $\mathfrak{b}$ in B existiert, das frei über A ist.*

Beweis. Sei $\mathfrak{b} \in I_B$ frei über A. Dann gilt wie in 1.12 $N\mathfrak{b} = i(\mathfrak{b}) = [B : \mathfrak{b}] \in s_A(B)^{-1}$. Also $N([\mathfrak{b}^{-1}]) = [N(\mathfrak{b}^{-1})] = s_A(B)$. Sei umgekehrt $s_A(B)$ im Bild der Normabbildung, d.h. es existiert ein Ideal $\mathfrak{b}'$ mit $[N\mathfrak{b}'] = s_A(B)$, also $[N\mathfrak{b}'^{-1}] = s_A(B)^{-1}$. Nach 1.19 folgt $s_A(\mathfrak{b}'^{-1}) = s_A(B)^{-1}s_A(B) = 1$, also ist $\mathfrak{b}'^{-1}$ A-frei. □

Für das folgende Lemma benötigen wir einen Satz von E. Hecke [He, Satz 176]. Er besagt, dass die Differente in der Idealklassengruppe von L ein Quadrat ist. Auch auf diesen Sachverhalt werden wir später noch weiter eingehen.
Leider gibt es bisher keinen "elementaren" algebraischen Zugang zu diesem tiefliegenden Satz. Er gilt auch nicht in beliebigen Dedekindringen, sondern nur in Ringen ganzer Zahlen von algebraischen Zahlkörpern, wie Fröhlich, Serre und Tate in [FST] zeigen.
In den Monographien von Hecke [He] und Weil [Wei] findet sich ein Beweis dieses Satzes, der Methoden der analytischen Zahlentheorie verwendet (L-Reihen, Gaußsche Summen). Armitage [Ar] benutzt Funktionalgleichungen gewisser L-Reihen, um das Resultat von Hecke zu erhalten. Sein Beweis geht letztlich auf Serre zurück. Einen algebraischen Beweis des Satzes von Hecke liefern Knebusch und Scharlau [KS]. Durch das Studium von Wittgruppen algebraischer Zahlkörper zeigen sie, dass die Differente ein Quadrat in $C\ell_L$ ist, da sie ein sogenanntes "erzeugendes Reziprozitätsgesetz" zulässt.

1.21 Lemma. *Ist die Klassenzahl h_K von K ungerade, so ist $s_A(B)$ im Bild der Norm. Ist h_K gerade, so ist $s_A(B)^2$ im Bild der Norm.*

Beweis. Es gilt immer $N[\mathcal{D}] = [N\mathcal{D}] = [\delta] = s_A(B)^2$. Ist h_K ungerade, so existiert in $C\ell_K$ kein Element mit Ordnung 2. Nach dem Satz von Hecke ist die Differente ein Quadrat in der Idealklassengruppe von L. Es ist etwa $\Delta^2 = [\mathcal{D}]$ für ein $\Delta \in C\ell_L$, und damit gilt

$N(\Delta)^2 = s_A(B)^2$. Da es kein Element der Ordnung 2 in $C\ell_K$ gibt, liefert das Ziehen der Quadratwurzel in $C\ell_K$ eine eindeutige Lösung. Damit ist $N(\Delta) = s_A(B)$. □

Die in diesem Beweis auftretende Idealklasse $\Delta \in C\ell_L$ wird auch im Folgenden immer wieder im Zentrum unserer Überlegungen stehen.

1.22 Definition. Sei $L|K$ eine Körpererweiterung algebraischer Zahlkörper. Eine Idealklasse $\Delta \in C\ell_L$ nennen wir eine *Steinitzwurzel*, wenn gilt

$$\Delta^2 \;=\; [\mathcal{D}_{L|K}] \qquad \text{und} \qquad N_{L|K}(\Delta) = s_A(B).$$

Ein erstes Beispiel für eine solche Steinitzwurzel haben wir im obigen Lemma kennengelernt. Wir folgern sofort, dass in einer Körpererweiterung $L|K$ eine Steinitzwurzel existiert, falls die Klassenzahl h_K von K ungerade ist.
Man beachte, dass die Existenz einer Steinitzwurzel nicht bedeutet, dass es auch ein Ideal $\mathfrak{b} \in I_B$ gibt mit $\mathfrak{b}^2 = \mathcal{D}_{L|K}$ und $N_{L|K}([\mathfrak{b}]) = s_A(B)$.
Mit den Abbildungen q_K, q_L, die jeder Idealklasse in K, L ihr Quadrat in $C\ell_K$ bzw. $C\ell_L$ zuordnen, erhalten wir folgendes kommutative Diagramm:

$$\begin{array}{ccc} \Delta & \xrightarrow{\quad q_L \quad} & [\mathcal{D}_{L|K}] \\ \Big\downarrow{\scriptstyle N_{L|K}} & /\!/ & \Big\downarrow{\scriptstyle N_{L|K}} \\ s_A(B) & \xrightarrow{\quad q_K \quad} & [\delta_{L|K}] \end{array}$$

Für eine Wurzel der Diskriminante in $C\ell_K$ haben wir bekanntlich die zahlentheoretische Interpretation als Steinitzklasse. Wir können an ihr ablesen, ob für $B|A$ eine relative Ganzheitsbasis existiert oder nicht.
Existiert in einer algebraischen Zahlkörpererweiterung eine Steinitzwurzel, so hat auch die Wurzel der Differente in $C\ell_L$ eine (zahlentheoretische) Interpretation, nämlich als Idealklasse, die unter der Norm auf die Steinitzklasse $s_A(B)$ abgebildet wird.
Leider gibt es nicht immer eine Steinitzwurzel, wie wir im folgenden Beispiel sehen werden. J.-P. Serre hat in einer (brieflichen) Diskussion darauf hingewiesen, dass die Galois-invariante Differente in der Regel keine Galois-invariante Quadratwurzel in $C\ell_L$ hat.

1.23 Beispiel. Sei $K = \mathbb{Q}(\sqrt{-15})$ und $L = \mathbb{Q}(\sqrt{-3}, \sqrt{5})$. Es ist $L|K$ an allen Stellen unverzweigt und $h_K = 2$. (Daher ist $L = Hi\ell(K)$ der Hilbertsche Klassenkörper von K). Nach Satz 43 in [Ha2] ist die Klassenzahl von L ungerade.
Die Erweiterung ist unverzweigt, darum sind die Differente $\mathcal{D}_{L|K}$ und die Diskriminante

$\delta_{L|K}$ Hauptideale in B bzw. A. Da h_L ungerade ist, existiert in $C\ell_L$ kein Element der Ordnung 2, d.h. die einzige Quadratwurzel Δ von $[\mathcal{D}_{L|K}]$ in $C\ell_L$ ist die triviale Klasse. Es ist also stets $N_{L|K}(\Delta) = 1$ in $C\ell_K$. Die Steinitzklasse $s_A(B)$ ist jedoch nicht trivial in $C\ell_K$, sie hat Ordnung 2 und erzeugt somit die Idealklassengruppe. Die Wurzel Δ der Differente in $C\ell_L$ kann also unmöglich ein Urbild von $s_A(B)$ unter der Norm sein.

Anmerkung. Argumente dafür, dass die Steinitzklasse $s_A(B)$ Ordnung 2 hat, werden uns ab Kapitel 3 zur Verfügung stehen.

Kapitel 2

Hilfsmittel

In diesem Abschnitt werden wir Hilfmittel zur Verfügung stellen, die im Laufe der folgenden Kapitel benötigt werden. Wie immer ist $L|K$ eine Körpererweiterung algebraischer Zahlkörper mit Ringen ganzer Zahlen B und A.

2.1 Lemma. *Sei F ein Zwischenkörper von $L|K$ mit Ring ganzer Zahlen C. Für die Differenten und Diskriminanten der relativen Erweiterungen besteht folgender Zusammenhang:*

(i) $\mathcal{D}_{L|K} = \mathcal{D}_{L|F}\mathcal{D}_{F|K}$ *(Transitivität der Differente).*

(ii) $\delta_{L|K} = (\delta_{F|K})^{[L:F]} N_{F|K}(\delta_{L|F})$.

Beweis. [CF, p.17].

2.2 Satz. *Sei F ein Zwischenkörper von $L|K$ mit Ring ganzer Zahlen C. Dann gilt für die Steinitzklassen*

$$s_A(B) = s_A(C)^{[L:F]} N_{F|K}(s_C(B)).$$

Beweis. Sei $\{u_i\} \subseteq C$ eine Basis für $F|K$ und $\{v_i\} \subseteq B$ eine Basis für $L|F$, dann ist $\{u_i v_j\} \subseteq B$ eine Basis für $L|K$. Seien U, V, W die freien A-Moduln, erzeugt von $\{u_i\}, \{v_i\}, \{u_i v_j\}$, und $S_Z = i(Z)^{-1}$ für $Z = U, V, W$; also S_Z ein Ideal aus der entsprechenden Steinitzklasse. Aus [Nar, Prop. 5.7] entnehmen wir, dass für die Diskriminanten der Basen von U, V, W ein zu 2.1 (ii) analoger Zusammenhang besteht, nämlich

$$\delta_{L|K}(W) = N_{F|K}(\delta_{L|F}(V))\delta_{F|K}(U)^{[L:F]}.$$

Nach 1.12 gilt für die Diskriminanten der Körpererweiterungen

$$\begin{aligned} \delta_{L|K} &= S_W^2 \delta_{L|K}(W), \\ \delta_{L|F} &= S_V^2 \delta_{L|F}(V), \\ \delta_{F|K} &= S_U^2 \delta_{L|K}(U). \end{aligned}$$

Eingesetzt in die wohlbekannte Formel 2.1 für Diskriminanten liefert dies

$$\begin{aligned} S_W^2\delta_{L|K}(W) &= \big(S_U^2\delta_{F|K}(U)\big)^{[L:F]}N_{F|K}\big(S_V^2\delta_{L|F}(V)\big) \\ &= S_U^{2[L:F]}\delta_{F|K}(U)^{[L:F]}\big(N_{F|K}S_V\big)^2N_{F|K}(\delta_{L|F}(V)), \end{aligned}$$

und mit dem oben zititerten Ergebnis aus [Nar] erhalten wir schliesslich

$$S_W^2 = \big(S_U^{[L:F]}\big)^2\big(N_{F|K}S_V\big)^2.$$

Da die Idealgruppe torsionsfrei ist, es also keine Elemente mit Ordnung 2 gibt, folgt hieraus $S_W = S_U^{[L:F]}N_{[F:K]}(S_V)$. Der Übergang zu Idealklassen liefert die Behauptung. □

2.3 Folgerung. *Ist C frei über A und B frei über C, so ist auch B frei über A.*

2.1 Zyklische Körpererweiterungen

2.4 Definition. [Wa, Ex.9.3] Sei K ein algebraischer Zahlkörper, der eine primitive p-te Einheitswurzel ε_p enthält, p eine Primzahl, $\mathfrak{p}$ ein Primideal in K über p. Sei $\pi = (\varepsilon_p - 1)$ und α ein Element aus K^* mit $\alpha \notin (K^*)^p$, α teilerfremd zu p, $\mathcal{P} = \prod_{\mathfrak{p}|p}\mathfrak{p}$. Bekanntlich ist $\pi^{p-1} = p$. Wir definieren

α ist primär, wenn $x^p \equiv \alpha \ (mod\ p\pi)$ eine Lösung in K^* hat,

α ist hyperprimär, wenn $x^p \equiv \alpha \ (mod\ p\pi\mathcal{P})$ eine Lösung in K^* hat,

α ist singulär primär, wenn α primär ist und $(\alpha) = \mathfrak{b}^p$ für ein $\mathfrak{b} \in I_K$.

2.5 Satz. *Es gelten die Voraussetzungen aus 2.4. Sei $L = K(\sqrt[p]{\alpha})$, $\mathfrak{p}|p$ und $v_\mathfrak{p}(\pi) = a$. Dann gilt:*

(i) *$\mathfrak{p}$ zerfällt total in L, falls $x^p \equiv \alpha \ (mod\ \mathfrak{p}^{ap+1})$ in K^* lösbar ist, also α hyperprimär ist,*

(ii) *$\mathfrak{p}$ ist träge in L, falls $x^p \equiv \alpha \ (mod\ \mathfrak{p}^{ap})$ in K^* lösbar , aber $x^p \equiv \alpha \ (mod\ \mathfrak{p}^{ap+1})$ unlösbar in K^*, also α primär ist,*

(iii) *$\mathfrak{p}$ verweigt total in L, wenn $x^p \equiv \alpha \ (mod\ \mathfrak{p}^{ap})$ unlösbar in K^* ist.*

Ist also $x^p \equiv \alpha \ (mod\ \mathfrak{p}^{ap})$ lösbar, also α primär, so ist $L|K$ unverzweigt für alle $\mathfrak{p}|p$.
Ist α singulär primär, so ist $L|K$ sogar unverzweigt für alle Primideale $\mathfrak{p}$ in K, außer für $p = 2$ und K reell. Hier verzweigen die unendlichen Stellen.

Beweis. [He, Satz 119].

Anmerkung. Findet man für die Kongruenzen Lösungen x in K^*, so sind diese Lösungen Elemente des Rings der ganzen Zahlen A, wenn α selbst in A liegt. Sei etwa $x^p \equiv \alpha \ (mod\ \mathfrak{p}^l)$, also $x^p = \alpha + z$ mit $z \in \mathfrak{p}^l$, so ist x^p ein Element in A. Als Ring ganzer Zahlen ist A ganz abgeschlossen in K. Da $x \in K$ Nullstelle des ganzen Polynoms $X^p - x^p$ ist, muss x also schon in A liegen.

Anmerkung. Enthält K eine primitive p-te Einheitswurzel und ist $L = K(\sqrt[p]{\alpha})$, so kann das Primideal $\mathfrak{p}|p$ in K nur total verzweigen, total zerfallen oder träge bleiben. ($L|K$ ist galoissch vom Grad p.)

2.6 Lemma. *Sei $L|K$ eine Galoiserweiterung von Zahlkörpern mit zyklischer Galoisgruppe $G = \langle\sigma\rangle \neq 1$ und genau eine Primstelle $\mathfrak{p}$ von K verzweige in L mit Verzweigungsindex e. Ist $\iota_{L|K} : C\ell_K \to C\ell_L$ injektiv, so ist $N_{L|K}(U_L) = U_K$ (und $N_{L|K}(C\ell_L) = C\ell_K$).*

Beweis. Zum Beweis rufen wir kurz einige Resultate aus der Klassenkörpertheorie in Erinnerung.
Für zyklische Galoiserweiterungen gelten für die Cohomologiegruppen in den Dimensionen -1, 0, 1, 2 folgende Isomorphien:

$$H^0(G, U_L) := (U_L)_G / N_{L|K}(U_L) \cong H^2(G, U_L) \text{ und } H^{-1}(G, U_L) \cong H^1(G, U_L).$$

Die Ordnungen der Cohomologiegruppen hängen über den Herbrand-Quotient $h(U_L)$ voneinander ab. Es ist

$$h(U_L) = \frac{|H^2(G, U_L)|}{|H^1(G, U_L)|} = \frac{|H^0(G, U_L)|}{|H^{-1}(G, U_L)|} = \frac{|H^0(G, U_L)|}{|H^1(G, U_L)|}.$$

Den Herbrand-Quotient $h(U_L)$ können wir durch die lokalen Grade $[L_{\mathfrak{P}} : K_{\mathfrak{p}}]$ berechnen,

$$h(U_L) = h(L^{\mathbb{P}_K^\infty}) = \frac{1}{[L : K]} \prod_{\mathfrak{p} \in \mathbb{P}_K^\infty} [L_{\mathfrak{P}} : K_{\mathfrak{p}}].$$

Es gilt $H^1(G, U_L) \cong (H_L)_G / H_K$ [Sch, 12.5]. Damit werden wir im Folgenden eine Abschätzung für $|H^1(G, U_L)|$ erhalten:
Nach Voraussetzung ist $\iota_{L|K}$ injektiv, es werden insbesondere nur Hauptideale aus K zu Hauptidealen in L; also ist $I_K \cap H_L = H_K$. Nun gilt aber $I_K \cap (H_L)_G \subseteq I_K \cap H_L = H_K$ und $H_K \subseteq I_K \cap (H_L)_G$, demnach haben wir $I_K \cap H_L = H_K = I_K \cap (H_L)_G$. Aus der Klassenkörpertheorie [Sch, 5.5] wissen wir, dass $|(I_L)_G : I_K| = \prod_{\mathfrak{p} \in \mathbb{P}_K} e(\mathfrak{P}|\mathfrak{p})$.

Sei nun die einzige verzweigende Primstelle endlich, dann ist $|(I_L)_G : I_K| = e$. Da

$H_K = I_K \cap (H_L)_G$, gilt also $(H_L)_G/H_K = (H_L)_G/(I_K \cap (H_L)_G \cong (H_L)_G I_K/I_K$. Offensichtlich ist $(H_L)_G I_K \leq (I_L)_G$, deshalb haben wir

$$|H^1(G,U_L)| = |(H_L)_G/H_K| = |(H_L)_G I_K/I_K| \leq |(I_L)_G/I_K| = e \leq [L:K].$$

Für den Herbrand-Quotient $h(U_L)$ gilt $h(U_L) = \frac{1}{[L:K]}$, da keine archimedische Primstelle verzweigt. Insgesamt ergibt sich

$$\frac{1}{[L:K]} = h(U_L) = \frac{|H^0(G,U_L)|}{|H^1(G,U_L)|}, \text{ d.h. } |H^1(G,U_L)| = [L:K] \cdot |H^0(G,U_L)|.$$

Allerdings ist $|H^1(G,U_L)| \leq [L:K]$ und da $|H^0(G,U_L)|$ eine natürliche Zahl sein muss, erhalten wir $|H^0(G,U_L)| = 1$, also $N_{L|K}(U_L) = U_K$.

Ist die einzige verzweigende Stelle archimedisch, so ist $|(I_L)_G : I_K| = 1$. Damit ist auch

$$1 = |(H_L)_G : H_K| = |H^1(G,U_L)| \text{ und } h(U_L) = \frac{1}{[L:K]} \prod_{\mathfrak{p} \in \mathbb{P}_K^\infty} [L_\mathfrak{P} : K_\mathfrak{p}] = \frac{2}{[L:K]}.$$

Schließlich gilt also

$$\frac{2}{[L:K]} = h(U_L) = \frac{|H^0(G,U_L)|}{|H^1(G,U_L)|} = |H^0(G,U_L)|,$$

bzw. $2 = [L:K] \cdot |H^0(G,U_L)|$. Wegen $[L:K] > 1$ muss $[L:K] = 2$ gelten und folglich $|H^0(G,U_L)| = 1$. Somit ist wiederum die Norm auf den Einheiten surjektiv. □

2.7 Lemma. *Sei $L|K$ Galoiserweiterung von Zahlkörpern mit zyklischer Galoisgruppe $G = \langle\sigma\rangle$. Ist $N_{L|K}(U_L) = U_K$, so enthält jede G-invariante Idealklasse $\Gamma \in C\ell_L$ ein G-invariantes Ideal.*

Beweis. Sei Γ eine G-invariante Idealklasse von L, also $\Gamma^\sigma = \Gamma$, und $\mathfrak{a}$ ein Ideal in L mit $[\mathfrak{a}] = \Gamma$. Dann ist $[\mathfrak{a}] = [\mathfrak{a}]^\sigma = [\mathfrak{a}^\sigma]$, also $\mathfrak{a}^\sigma = \gamma\mathfrak{a}$ für ein $\gamma \in L^*$.
Es gilt $N_{L|K}(\mathfrak{a}) = N_{L|K}(\mathfrak{a}^\sigma) = N_{L|K}(\gamma\mathfrak{a}) = N_{L|K}(\gamma)N_{L|K}(\mathfrak{a})$ und $N_{L|K}(\gamma)$ ist eine Einheit in K. Da nach Voraussetzung die Norm auf den Einheiten surjektiv ist, existiert ein $u \in U_L$ mit $N_{L|K}(u) = N_{L|K}(\gamma)$, damit $N_{L|K}(\gamma u^{-1}) = 1$. Die Galoisgruppe ist zyklisch, daher existiert nach Hilberts Satz 90 ein $z \in L^*$ mit $\gamma u^{-1} = \frac{z^\sigma}{z}$. Ist nun $\mathfrak{b} = z^{-1}\mathfrak{a}$, also $[\mathfrak{b}] = [\mathfrak{a}] = \Gamma$, so folgt $\mathfrak{b}^\sigma = z^{-\sigma}\mathfrak{a}^\sigma = (z^{-1}\gamma^{-1}u)(\gamma\mathfrak{a}) = uz^{-1}\mathfrak{a} = u\mathfrak{b} = \mathfrak{b}$. Das Ideal $\mathfrak{b}$ ist G-invariant. □

2.2 Abelsche Körpererweiterungen

Sei $K|\mathbb{Q}$ eine Galoiserweiterung mit abelscher Galoisgruppe G. Nach dem Satz von Kronecker-Weber [Wa, Thm. 14.1] ist K Teilkörper eines geeigneten Kreisteilungskörpers $L = \mathbb{Q}(\varepsilon_m)$ ($m \in \mathbb{N}$), und deshalb auch $G = Gal(K|\mathbb{Q})$ eine Untergruppe von $Gal(L|\mathbb{Q}) = (\mathbb{Z}/m\mathbb{Z})^* =: G(m)$, der primen Restklassengruppe mod m.
Einen Homomorphismus $\chi : G \to \mathbb{C}^*$ nennt man einen Charakter von G. Ist $|G| = n$ endlich, so ist $\chi(x)$ eine n-te Einheitswurzel für ein $x \in G$. Alle Charaktere einer Gruppe G bilden die Charaktergruppe $\widehat{G}$ von G und es gilt $G \cong \widehat{G}$ (nicht natürlich). Insbesondere ist mit $G = X \times Y$ auch $\widehat{G} = \widehat{X} \times \widehat{Y}$.
Die Charaktere von $G(m)$ nennt man *Dirichlet-Charaktere mod* m, und es ist

$$X = X_K = \{\chi \in \widehat{G(m)} : Ker(\chi) \supseteq Gal(\mathbb{Q}(\varepsilon_m)|K)\}$$

die dem Körper K zugeordnete Gruppe von Dirichlet-Charakteren. Daher gilt

$$X = X_K = \widehat{G} \cong G.$$

Ein Dirichlet-Charakter mod m heisst primitiv, falls er sich nicht durch einen Dirichlet-Charakter mod m' für einen Teiler m' von m darstellen lässt. Ist dies der Fall, so nennen wir den ggT (als Ideal) aller solcher Teiler den *Führer* f_χ von χ. Der Führer f_K des Körpers K ist dann das kgV der Führer f_χ aller $\chi \in X_K$.
Ist $L = \mathbb{Q}(\varepsilon_m)$ der kleinste Kreisteilungskörper, in dem K enthalten ist, so ist $f_K = m$.
Wie üblich sei $[K : \mathbb{Q}] = n = r_1 + 2r_2$, wobei r_1 die Anzahl der reellen, r_2 die Anzahl der Paare komplexer Einbettungen von K bezeichnen. Zwischen der (absoluten) Diskriminante δ_K und den Führern besteht der folgende Zusammenhang.

2.8 Satz. *(Diskriminanten-Führer-Formel)*

$$\delta_K = (-1)^{r_2} \prod_{\chi \in X_K} f_\chi.$$

Beweis. [Nar, Prop. 8.4].

In Kapitel 8 werden wir von der Diskriminante nur den 2-Anteil benötigen.
Da $G(m) = G(2^k) \times G(m')$ (mit $m = 2^k m'$, m' ungerade) ist, gilt auch $\widehat{G(m)} = \widehat{G(2^k)} \times \widehat{G(m')}$. Für jeden Charakter $\chi \in \widehat{G(m)}$ existiert eine Darstellung $\chi = \chi_2 \chi_{m'}$, daher können wir uns in Kapitel 8 auf das Studium des 2-Anteils im Führer f_χ beschränken.

Anmerkung. Es gibt auch eine Version der Diskriminanten-Führer-Formel für relative Galoiserweiterungen $L|K$, siehe etwa [Neu, VII.11.9]. Wir benötigen sie nur für das folgende Beispiel.

2.9 Beispiel. Ist $L|K$ zyklisch von ungeradem Primzahlgrad p, so ist auch X zyklisch mit Ordnung p. Wir haben also einen trivialen Charakter und $(p-1)$ nichttriviale Charaktere mit gleichem Führer. Nach der Diskriminanten-Führer-Formel ist die Diskriminante δ eine $(p-1)$-te Potenz in I_A. In Kapitel 4 zeigen wir, dass in Galoiserweiterungen mit ungeradem Grad die Differente ein Quadrat in der Idealgruppe I_B ist und ihre Wurzel unter der Norm auf ein Ideal in der Steinitzklasse abgebildet wird. Es existiert also eine Steinitzwurzel für $L|K$. Die Steinitzklasse ist eine $\frac{p-1}{2}$-te Potenz in $C\ell_K$.

Kapitel 3

Unverzweigte Erweiterungen

Sei $L|K$ eine Galoiserweiterung algebraischer Zahlkörper mit Galoisgruppe $G = Gal(L|K)$. Eine Erweiterung heisst unverzweigt, wenn keine endliche Stelle verzweigt, also die Diskriminante $\delta = \delta_{L|K} = A$ und die Differente $\mathcal{D} = \mathcal{D}_{L|K} = B$ ist.
Diese Situation entspricht einer Galoiserweiterung von Ringen, wie sie von R. G. Swan [Sw, p.22] definiert wird:

> Seien $A \subseteq B$ kommutative Ringe und G eine endliche Automorphismengruppe von B. B ist eine Galoiserweiterung von A, wenn die beiden folgenden Aussagen gelten.
>
> (i) $B^G = A$
>
> (ii) Für alle Untergruppen $H \leq G$ und alle unter H stabilen Ideale $I \neq B$ wirkt H treu auf B/I.

Im Fall der algebraischen Zahlkörper ist Bedingung (i) immer gegeben, Bedingung (ii) nur dann, wenn eine unverzweigte Erweiterung vorliegt. Da B und A Dedekindringe sind, genügt es, diese Eigenschaft für Primideale $\mathfrak{P}$ von B zu zeigen.
Die Untergruppe H muss treu auf $B/\mathfrak{P}$ wirken, d.h. nur für $1 = \sigma \in H \leq G$ darf $\beta^\sigma \equiv \beta \ (mod\ \mathfrak{P})$ gelten. Dies bedeutet aber, dass die Trägheitsgruppe $T_\mathfrak{P}$ trivial sein muss und damit $e(\mathfrak{P}|\mathfrak{p}) = |T_\mathfrak{P}| = 1$ gilt, also $\mathfrak{P}$ unverzweigt ist.

Wie in Kapitel 1 schon angekündigt, beweisen wir nun, dass die Steinitzklasse in unverzweigten Erweiterungen unter der Einbettung $\iota_{L|K}$ trivial wird.

3.1 Satz. *Für eine unverzweigte Galoiserweiterung $L|K$ gilt $\iota_{L|K}(s_A(B)) = 1$.*

Beweis. Nach [Sw, Prop. 2.1(3)] ist $B \otimes_A B$ eine zerfallende Galoiserweiterung von B, d.h. $B \otimes_A B$ ist isomorph zu $\prod_{\sigma \in G} B$. Es existiert also eine B-Basis für $B \otimes_A B$, daher ist $s_B(B \otimes_A B)$ trivial und nach 1.18 auch $\iota_{L|K}(s_A(B)) = s_B(B \otimes_A B)$. □

Ob auch schon die Steinitzklasse $s_A(B)$ selbst trivial ist, lässt sich bei unverzweigten Galoiserweiterungen an der Galoisgruppe ablesen.

3.2 Satz. *Sei $L|K$ unverzweigt mit Gruppe G. Genau dann ist $s_A(B) = 1$, wenn eine der beiden folgenden Aussagen gilt:*

(i) Die 2-Sylowgruppen von G sind trivial, also $|G|$ ungerade, oder nicht zyklisch.

(ii) Die 2-Sylowgruppen von G sind nicht-trivial und zyklisch und der einzige über K quadratische Zahlkörper ist von der Form $K(\sqrt{u})$, wobei $u \in A^*$ eine Einheit ist.

Beweis. Nach Voraussetzung ist die Diskriminante $\delta = A$. Sei $\beta \in B$ primitiv für $L|K$ und $g = m_\beta$ das dazugehörige Minimalpolynom mit Diskriminante $\delta(g) = \delta(m_\beta)$. Für die Diskriminante von g gilt nach Vandermonde $\delta(m_\beta) = \prod_{i<j}(\beta_i - \beta_j)^2$, wobei $\beta_i,\ i = 1, \ldots, n = [L : K]$ die verschiedenen Nullstellen von g sind, die alle in L liegen (Die Erweiterung ist normal). Also ist auch $\sqrt{\delta(m_\beta)}$ in L und $F = K(\sqrt{\delta(m_\beta)})$ ist ein Zwischenkörper von $L|K$ mit Grad $[F : K] \leq 2$.
Ist $[F : K] = 1$, etwa bei $|G|$ ungerade, so ist $\sqrt{\delta(m_\beta)} \in K$. Mit 1.12 ergibt sich für die Diskriminante $A = \delta = \sqrt{\delta(m_\beta)}^2 i(\beta)^2$. Es folgt $\sqrt{\delta(m_\beta)} = i(\beta)^{-1} \in s_A(B)$ und damit ist nach 1.13 die Steinitzklasse $s_A(B)$ trivial.
Sei nun $[F : K] = 2$. Dann ist $\delta(m_\beta)$ kein Quadrat in K und somit die Galoisgruppe G als Permutationsgruppe auf den Wurzeln W_g von g nicht enthalten in $A_{|W_g|}$, der alternierenden Gruppe auf den Wurzeln von g. Es gibt also eine ungerade Permutation $\sigma \in G$ auf W_g. Da die Erweiterung unverzweigt ist, also insbesondere $|T_\mathfrak{P}| = |\{\sigma \in G_\mathfrak{P} : x^\sigma \equiv x \ (mod\ \mathfrak{P})\}| = 1$ für alle $\mathfrak{P} \in \mathbb{P}_L$, ist der Stabilisator G_α einer Nullstelle $\alpha \in W_g$ trivial, G operiert auf W_g also regulär. Wir können σ als Produkt von disjunkten Zykeln schreiben. Hätten diese unterschiedliche Ordnungen, so gäbe es Zykel $\neq 1$, die gewisse Elemente fest ließen. Da G regulär operiert, kann dies nicht sein. Die disjunkten Zykel haben demnach alle diesselbe Ordnung $o(\sigma)$ und es gibt $|G|/o(\sigma)$ viele disjunkte Zykel der Länge $o(\sigma)$. Da σ ungerade ist, ist $o(\sigma)$ gerade und $|G|/o(\sigma)$ ungerade. Also ist $o(\sigma)$ die maximale 2-Potenz in $|G|$ und $\langle\sigma\rangle \neq 1$ eine zyklische 2-Sylowgruppe von G.
Nach dem Verlagerungssatz von Burnside [Hu, Satz IV.2.6] hat G ein (eindeutiges) normales 2-Komplement mit zyklischer Faktorgruppe. Deshalb gibt es also genau einen quadratischen Teilkörper F von $L|K$, $F = K(\sqrt{\delta(m_\beta)})$.
Ist $s_A(B) = 1$, so gilt nach 1.14 für die Diskriminante des Minimalpolynoms $\delta(m_\beta) = ua^2$ mit $u \in U_K$ und $a \in A$ ($\delta = A$, unverzweigt). Also gilt einerseits $F = K(\sqrt{u})$. Ist andererseits $F = K(\sqrt{u})$ mit $u \in U_K$, so ist $\delta(m_{\sqrt{u}}) = 4u$ und $\delta(m_{\sqrt{u}}) = ua^2$ mit $a \in K^*$. Wieder folgt mit 1.14, dass die Steinitzklasse $s_A(B)$ trivial ist. □

3.3 Folgerung. *In einer unverzweigten Galoiserweiterung mit Gruppe G seien die 2-Sylowgruppen von G nicht-trivial und zyklisch. Ist F ein quadratischer Teilkörper von $L|K$ mit Ring der ganzen Zahlen C, so gilt $s_A(B) = 1$ genau dann wenn $s_A(C) = 1$.*

Beweis. Sei zunächst $s_A(B) = 1$. Da die 2-Sylowgruppen von G zyklisch und $\neq 1$ sind, existiert ein einziger quadratischer Zwischenkörper $F = K(\sqrt{u})$, mit $u \in U_K$. Damit ist nun $F|K$ eine unverzweigte Galoiserweiterung mit zyklischer, nicht-trivialer 2-Sylowgruppe mit einzigem quadratischen Zwischenkörper F, nach 3.2 gilt $s_A(C) = 1$.
Ist $s_A(C) = 1$, so haben wir mit 3.2, dass $F = K(\sqrt{u})$ mit $u \in U_K$ ist. Die Erweiterung $L|K$ erfüllt alle Voraussetzungen von 3.2, damit ist $s_A(B) = 1$. □

3.4 Hauptsatz 1. *Sei $L|K$ galoissch und an allen endlichen Stellen unverzweigt. Es gelten die obigen Bezeichnungen. Die Steinitzklasse $s_A(B)$ ist genau dann nicht trivial, wenn es genau eine quadratische Teilerweiterung $F|K$ in $L|K$ gibt und in dieser $s_A(C) \neq 1$ ist. Damit haben $s_A(B)$ und $s_A(C)$ Ordnung 2 in $C\ell_K$.*

Beweis. Ist $s_A(B) \neq 1$, so folgt aus 3.2, dass die 2-Sylowgruppe von G nicht trivial und zyklisch ist. Es existiert also genau ein quadratischer Zwischenkörper F in $L|K$. Wäre dessen Steinitzklasse $s_A(C) = 1$, so wäre dies ein Widerspruch zu 3.3. Da mit $L|K$ auch $F|K$ unverzweigt ist, sind die Diskriminanten in beiden Fällen trivial und beide Steinitzklassen haben Ordnung 2 in $C\ell_K$.
Ist andererseits F der einzige quadratische Zwischenkörper von $L|K$, so muss die Galoisgruppe eine zyklische (nicht-triviale) 2-Sylowgruppe enthalten. Aufgrund von 3.3 ist mit $s_A(C)$ auch $s_A(B)$ nicht trivial und wie eben folgt, dass ihre Ordnungen in $C\ell_K$ identisch, nämlich 2, sind. □

Anmerkung. Ähnliche Resultate hat E. Soverchia [So] im Jahr 2002 veröffentlicht. Anstelle einer unverzweigten Erweiterung betrachtet sie jedoch eine Galoiserweiterung $L|K$, die den Hilbertschen Klassenkörper $H = Hi\ell(K)$ von K enthält. Sie kann zeigen, dass die relative Diskriminante von $L|H$ stets ein Hauptideal ist. Ist die Klassenzahl von H ungerade, gibt es also eine relative Ganzheitsbasis für $L|H$. Ist die Klassenzahl h_H gerade, so hängt die Existenz der Ganzheitsbasis wie in unserem Satz von der Struktur der Galoisgruppe $G = Gal(L|H)$ ab:

(i) Ist die 2-Sylowgruppe von G nicht zyklisch oder trivial, so hat $L|H$ eine relative Ganzheitsbasis.

(ii) Ist die 2-Sylowgruppe von G nicht-trivial und zyklisch, so existiert genau dann eine relative Ganzheitsbasis für $L|H$, wenn für die quadratische Teilerweiterung $M|H$ eine relative Ganzheitsbasis existiert.

Auch die Bedingung an den quadratischen Teilkörper M in (ii) kommt uns bekannt vor, allerdings ist unser Resultat unabhängig von E. Soverchias entstanden.

Anmerkung. Existiert für eine unverzweigte Erweiterung $L|K$ eine relative Ganzheitsbasis, ist also $s_A(B) = 1$, so existiert stets eine Galois-invariante Steinitzwurzel Δ für $L|K$. Es ist dann $\Delta = [\mathcal{D}]$ trivial in $C\ell_L$.

Weiss man, dass für eine Erweiterung $L|K$ eine relative Ganzheitsbasis existiert, so kann man sich über die Form dieser Ganzheitsbasis weitere Gedanken machen. Wir erläutern kurz die beiden Begriffe, die in der Literatur dazu auftauchen.

Für $L|K$ bzw. $B|A$ existiert eine *ganze Potenzbasis*, wenn $B = A[\theta]$ für ein $\theta \in B$, also $\{1, \theta, \ldots \theta^{n-1}\}$ eine Ganzheitsbasis für $B|A$ ist. Man nennt den Ring B dann auch *monogen* und θ ein *primitives Element für* $B|A$. Ist F ein Zwischenkörper von $L|K$ mit Ring C, so gilt auch $B = C[\theta]$, also hat mit $L|K$ auch $L|F$ eine ganze Potenzbasis. Eine analoge Aussage gilt für (beliebige) Ganzheitsbasen nicht.
Eine ganze Potenzbasis $\{1, \theta, \ldots \theta^{n-1}\}$ existiert genau dann, wenn der Führer $\mathfrak{f}_\theta$ des primitiven (ganzen) Elements θ trivial, also $\mathfrak{f}_\theta = B$ ist. Nach [Nar, p.163] ist es im Lokalen immer möglich, ein Element $\theta \in B_\mathfrak{P}$ zu finden, dessen Führer nicht durch $\mathfrak{P}$ teilbar, also eine Einheit in $B_\mathfrak{P}$ ist. Damit exisitiert für die Ringe $B_\mathfrak{P}|A_\mathfrak{p}$ in lokalen Erweiterungen immer eine ganze Potenzbasis.

Wir nennen eine Ganzheitsbasis einer Galoiserweiterung $L|K$ eine *normale Ganzheitsbasis*, wenn die Basiselemente der A-Basis von B transitiv von der Galoisgruppe permutiert werden. Existiert eine normale Ganzheitsbasis, so ist die Spurabbildung $Tr : B \to A$ surjektiv, was in normalen Erweiterungen stets äquivalent dazu ist, dass die Erweiterung $L|K$ zahm verzweigt ist. Die zahme Verzweigung ist allerdings nur im Lokalen auch eine hinreichende Bedingung für die Existenz einer ganzen Normalbasis für $B|A$ ([Noe]). Im Globalen gilt dies im Allgemeinen nicht. Ein Gegenbeispiel hierzu findet sich etwa in [Mar].

Den restlichen Teil dieses Kapitels verwenden wir auf das Studium von ganzen Potenz- bzw. normalen Ganzheitsbasen in unverzweigten Erweiterungen.

3.5 Satz. *Für eine unverzweigte quadratische Erweiterung $L|K$ gibt es genau dann eine relative Ganzheitsbasis, wenn es eine ganze Potenzbasis gibt.*

Beweis. (Vgl. [Ih, Thm. 1]). Dass aus der Existenz einer ganzen Potenzbasis auch die Existenz einer relativen Ganzheitsbasis folgt, ist trivial. Zu beweisen ist also nur die Umkehrung.

Sei $G = Gal(L|K) = \langle\sigma\rangle$. Nach 3.2 gibt es genau dann eine relative Ganzheitsbasis, wenn $L = K(\sqrt{u})$ ist mit u eine Einheit in A. Wir setzen $\mu = \sqrt{u}$. Da die Erweiterung unverzweigt ist, ist u ein primäres Element (2.4) und die Kongruenz $x^2 \equiv u \ (mod\ 4A)$ ist lösbar in K^*. Sei $\lambda \in K^*$ eine solche Lösung. Da $u = \mu^2$ in B gilt, ist $\lambda^2 \equiv \mu^2 \ (mod\ 4B)$. Es ist dann $(\mu - \lambda)(\mu + \lambda) = \mu^2 - \lambda^2 \equiv 0 \ (mod\ 4B)$. Überdies folgt

$$(\mu - \lambda)^2 = \mu^2 - 2\mu\lambda + \lambda^2 \equiv 2\mu^2 - 2\mu\lambda = 2\mu(\mu - \lambda) \ (mod\ 4B),$$

also $(\mu - \lambda)^2 \equiv 0 \ (mod\ 2B)$.
Sei nun $(\mu - \lambda) = \prod_{i\in I} \mathfrak{P}_i^{d_i}$ die eindeutige Primidealzerlegung von $(\mu - \lambda)$ in B, also $(\mu + \lambda) = (\mu - \lambda)^\sigma = \prod_{i\in I} (\mathfrak{P}_i^\sigma)^{d_i}$. Es sei $2B = \prod_{j\in J} \mathfrak{P}_j^{e_j}$ die Zerlegung von 2 in B. Damit haben wir auch $4B = \prod_{j\in J} \mathfrak{P}_j^{2e_j}$. Wir wissen bereits, dass

$$\begin{aligned} 4B = \prod_{j\in J} \mathfrak{P}_j^{2e_j} \quad &\Big| \quad \prod_{i\in I} \mathfrak{P}_i^{d_i} (\mathfrak{P}_i^\sigma)^{d_i}, \\ 2B = \prod_{j\in J} \mathfrak{P}_j^{e_j} \quad &\Big| \quad \prod_{i\in I} \mathfrak{P}_i^{2d_i}, \end{aligned}$$

gilt und sehen sofort, dass $J \subseteq I$ sein muss. Wir zeigen nun, dass 2 ein Teiler von $(\mu - \lambda)$ ist, bzw. dass für die Exponenten der $\mathfrak{P}_j$ $(j \in J)$ $e_j \leq d_j$ gilt.
Ist $\mathfrak{P}_j$ ein Teiler von 2, so auch das konjugierte Ideal $\mathfrak{P}_j^\sigma$. Da die Erweiterung $L|K$ unverzweigt ist, gibt es nur entweder träge oder zerfallende Primideale $\mathfrak{P}_i|\mathfrak{p}_i$, $\mathfrak{p}_i$ in K. Folglich ist entweder $\mathfrak{P}_j^\sigma = \mathfrak{P}_j$ im trägen Fall oder $\mathfrak{P}_j^\sigma = \mathfrak{P}_k$ (und $\mathfrak{P}_k^\sigma = \mathfrak{P}_j$) mit $j \neq k \in J$ geeignet, falls $\mathfrak{p}$ zerfällt. Der Exponent e_j lässt sich schreiben als $e_j = e(\mathfrak{p}_j|p_j)e(\mathfrak{P}_j|\mathfrak{p}_j)$, $(p_j) = \mathfrak{p}_j \cap \mathbb{Z}$. Da $\mathfrak{P}_k$ über demselben Primideal $\mathfrak{p}_j$ in K liegt wie $\mathfrak{P}_j$, haben $\mathfrak{P}_k = \mathfrak{P}_j^\sigma$ und $\mathfrak{P}_j$ denselben Exponenten. Wir erhalten also

$$4B = \prod_{j\in J} (\mathfrak{P}_j \cdot \mathfrak{P}_j)^{e_j} = \prod_{j\in J} (\mathfrak{P}_j \mathfrak{P}_j^\sigma)^{e_j} \Big| \prod_{i\in I} (\mathfrak{P}_i \mathfrak{P}_i^\sigma)^{d_i},$$

und insbesondere $e_j \leq d_j$, also ist $2B$ ein Teiler von $(\mu - \lambda)$. Damit haben wir $\mu = \lambda + 2\gamma$ mit $\gamma \in B$ und es ist $\gamma - \gamma^\sigma = \frac{1}{2}(\mu - \lambda - \mu^\sigma + \lambda) = \mu$. Das Element $\mu = (\gamma - \gamma^\sigma)$ liegt in $A[\gamma]$ $\big(\gamma^\sigma \in A[\gamma] = A[X]/(m_\gamma)\big)$ und da μ eine Einheit in B ist $(\mu\mu u^{-1} = 1)$, ist auch der Führer $\mathfrak{f}_\gamma = (\mu) = B$, also $B = A[\gamma]$. □

3.6 Satz. [Ch, Thm. B], [Ih, Thm. 2] *Sei $L|K$ eine Körpererweiterung vom Grad p mit $\varepsilon_p \in K$ (also eine Kummererweiterung). $L|K$ sei an den endlichen Stellen unverzweigt. Es existiert genau dann eine ganze Normalbasis für $B|A$, wenn $L = K(\sqrt[p]{\alpha})$ für eine Einheit $\alpha \in U_K$ mit $\alpha \equiv 1 \ (mod\ \pi^p)$ gilt. Insbesondere ist α singulär primär.*

Beweis. L. Childs beweist folgendes Theorem [Ch, Thm. B]:

Sei $L|K$ eine unverzweigte Kummererweiterung, zyklisch vom Grad p mit Gruppe $G = \langle\sigma\rangle$. Sei $\pi = (\varepsilon - 1)$, $\varepsilon = \varepsilon_p$ eine p-te Einheitswurzel. Folgende Aussagen sind äquivalent:

(i) Es existiert ein $z \in U_L \cap (1 + \pi B)$ mit $z^\sigma = \varepsilon z$.

(ii) Es existiert ein $x \in B$ mit $B = A[x]$ und $x^\sigma = \varepsilon x + 1$.

(iii) B hat eine normale Ganzheitsbasis über A.

Sei nun $L = K(\sqrt[p]{\alpha})$ mit $\alpha \equiv 1 \ (mod\ \pi^p)$. Wir zeigen, dass für $\sqrt[p]{\alpha}$ die Bedingung aus (i) gilt, woraus dann sofort die Existenz einer normalen Ganzheitsbasis folgt.
Die Wurzeln des Minimalpolynoms von $\sqrt[p]{\alpha}$ sind $\varepsilon_p^i \sqrt[p]{\alpha}$ $(i = 1, \dots (p-1))$, also ist insbesondere $\sqrt[p]{\alpha}^\sigma = \varepsilon_p \sqrt[p]{\alpha}$. Da $\alpha \in U_K$ ist, ist auch $\sqrt[p]{\alpha}$ eine Einheit in L. Es bleibt noch zu zeigen, dass ein $b \in B$ existiert, so dass $\sqrt[p]{\alpha} = 1 + \pi b$, also π ein Teiler von $1 - \sqrt[p]{\alpha}$ ist.
Wir gehen wie in 3.5 vor. Seien $\sqrt[p]{\alpha} - 1 = \prod_{i\in I} \mathfrak{P}_i^{d_i}$ und $\pi = \prod_{j\in J} \mathfrak{P}_j^{e_j}$ die eindeutigen Primidealzerlegungen in B. Es ist $1 - \alpha = \prod_{\sigma\in G}(\sqrt[p]{\alpha} - 1)^\sigma = \prod_\sigma \prod_{i\in I}(\mathfrak{P}_i^{d_i})^\sigma$. Da π^p das Ideal $(\alpha - 1)$ teilt, folgt, dass $J \subseteq I$ und $pe_j \le v_{\mathfrak{P}_j}\big(\prod_i (\mathfrak{P}_i^{d_i})^\sigma\big)$ ist. Es bleibt $e_j \le d_j$ für alle $j \in J$ zu zeigen.
Da $L|K$ galoissch vom Grad p ist, kann in $L|K$ das Primideal $\mathfrak{p}|\pi$ nur total verzweigen, total zerfallen oder träge bleiben. Ersteres ist in unserem Fall ausgeschlossen. Ist $\mathfrak{p}_i$ $(= \mathfrak{P}_i \cap A)$ träge in $L|K$, so bleibt $\mathfrak{P}_i$ unter σ fest, also $\prod_\sigma (\mathfrak{P}_i^{d_i})^\sigma = \mathfrak{P}_p^{pd_i}$. Demnach ist $e_j \le d_j$ für die träge Primideale $\mathfrak{P}_j$.
Zerfällt $\mathfrak{p}_i$ in $L|K$, so ist $\mathfrak{p}_i = \mathfrak{P}_{i_1} \cdots \mathfrak{P}_{i_p}$. Alle $\mathfrak{P}_{i_k}$ treten in der Faktorisierung von π auf und sind zueinander konjugiert. Sie werden durch die Galoisgruppe zyklisch permutiert, wobei der Exponent d_i für alle $\mathfrak{P}_{i_k}$ identisch bleibt. Wir haben also für zerfallende Primideale $\prod_i \prod_\sigma (\mathfrak{P}_i^{d_i})^\sigma = \prod_i \mathfrak{P}_i^{pd_i}$ und es folgt auch hier $e_j \le d_j$. Damit ist $\alpha \in 1 + \pi B$ und Bedingung (i) erfüllt.

Existiert andererseits für $B|A$ eine ganze Normalbasis, so gibt es nach Childs' Theorem auch eine ganze Potenzbasis mit Erzeugendem x, also $B = A[x]$. Aus dem Beweis in [Ch] ist ersichtlich, dass $x = \frac{z-1}{\varepsilon-1}$ mit z wie in (i), also $z^\sigma = \varepsilon z$, ist. Da weiterhin $\varepsilon \in K$ ist, erhalten wir

$$L = K(x) = K\Big(\frac{z-1}{\varepsilon-1}\Big) = K(z-1) = K(z),$$

mit $z \in U_L \cap (1 + \pi B)$. Folglich ist $z^p \in (1 + \pi^p B)$, also $\alpha := z^p \equiv 1 \ (mod\ \pi^p)$ und daher primär. Es ist $\alpha = z^p \in K$ bzw. A, weil $(z^p)^\sigma = \varepsilon^p z^p = z$ gilt. Trivialerweise ist $\alpha = (\sqrt[p]{\alpha})^p$ singulär. □

3.7 Satz. [Ih, Cor. 3] *Sei $L|K$ eine an den endlichen Stellen unverzweigte Galoiserweiterung vom Grad p mit $\varepsilon_p \in K$ und Gruppe G. Existiert eine ganze Normalbasis für $B|A$, so gibt es auch eine ganze Potenzbasis für $B|A$.*

Beweis. H. Ichimura zeigt in [Ih, Thm. 1] für eine zyklische Kummererweiterung vom Grad p mit $\varepsilon_p \in K$ und $\pi = \varepsilon_p - 1$ die folgende Äquivalenz:

(i) $L|K$ ist an den endlichen Stellen unverzweigt und es ist $B = A[\theta]$ für ein $\theta \in B$ mit $\theta^\sigma - \varepsilon_p\theta \in A$ für ein $\sigma \in G$.

(ii) Es ist $L = K(\sqrt[p]{\alpha})$ mit einer Einheit $\alpha \in U_K$, für die gilt $\alpha \equiv u^p \ (mod\ \pi^p)$, für ein $u \in A$.

Mit Theorem B in [Ch] folgt die Behauptung sofort. □

Anmerkungen. [Ih, p.105] Für eine Einheit $\epsilon \in K$ gilt, dass $K(\sqrt[p]{\epsilon})|K$ genau dann unverzweigt ist, wenn $\epsilon \equiv u^p \ (mod\ \pi^p)$ für ein $u \in A$ ist (d.h. ϵ ist singulär primär; vgl. Kapitel 2). Folglich hat eine unverzweigte Erweiterung $L|K$, K wie oben, eine ganze Potenzbasis, wenn $L = K(\sqrt[p]{\epsilon})$ ist.
Eine unverzweigte quadratische Erweiterung $L|K$ hat genau dann eine ganze Potenzbasis, wenn $L = K(\sqrt{\epsilon})$ für ein $\epsilon \in U_K$ ist. Die Kongruenz aus (ii) gilt, weil ϵ primär ist. Die Bedingung aus (i) gilt für jedes Element in B, da $\varepsilon_2 = -1$ und die angegebene Bedingung dann nichts anderes als die Spurabbildung ist. Dieses Ergebnis fasst 3.2 und 3.5 zusammen.

Satz 3.7 von H. Ichimura [Ih, Thm. 1] zeigt uns, dass unter bestimmten Voraussetzungen aus der Existenz einer normalen Ganzheitsbasis die Existenz einer ganzen Potenzbasis folgt. Im folgenden Satz geben wir eine Bedingung an, unter der im Falle einer unverzweigten quadratischen Erweiterung aus der Existenz einer ganzen Potenzbasis auch die Existenz einer normalen Ganzheitsbasis folgt.

3.8 Satz. *Ist $L|K$ eine unverzweigte Erweiterung vom Grad 2 und gilt $B = A[\theta]$, so existiert eine ganze Normalbasis für $B|A$, wenn $Tr(\theta) \in U_K$.*

Beweis. Wir setzen den Beweis von 3.5 fort. Aus der Existenz einer relativen Ganzheitsbasis haben wir abgeleitet, dass $L = K(\mu)$ ist, mit $\mu^2 = u \in U_K$ und $\mu = \theta - \theta^\sigma \in U_L$. Damit ergab sich, dass θ primitiv für $B|A$ ist. Wir betrachten nun das Element $x = \theta\mu^{-1} = \frac{\theta}{\theta - \theta^\sigma}$. Für x gilt

$$\begin{aligned} x^\sigma &= \theta^\sigma(\theta^\sigma - \theta^{\sigma^2})^{-1} = \frac{-\theta^\sigma}{\theta - \theta^\sigma} = \frac{-\theta^\sigma + \theta - \theta}{\theta - \theta^\sigma} \\ &= \frac{-\theta}{\theta - \theta^\sigma} + \frac{\theta - \theta^\sigma}{\theta - \theta^\sigma} = -x + 1. \end{aligned}$$

Damit haben wir ein Element aus B gefunden, das den zweiten Teil der Bedingung (ii) in Childs' Theorem ([Ch, Thm. B] bzw. 3.6 im Beweis) erfüllt. Es bleibt nur noch zu zeigen,

dass x primitiv für $B|A$ ist.
Wir betrachten den Ring $A[x]$ bzw. seine A-Basis $(1, x)$. Die Transformationsmatrix der A-Basis von B $(1, \theta)$ zur Basis $(1, x)$ ist $\begin{pmatrix} 1 & 0 \\ \frac{-2N_{L|K}(\theta)}{u} & \frac{Tr_{L|K}(\theta)}{u} \end{pmatrix}$. Sie ist genau dann in A invertierbar, wenn $Tr_{L|K}(\theta) \in U_K$ gilt. Also ist

$$A[\theta] = A[x] \quad \text{genau dann, wenn} \quad Tr_{L|K}(\theta) \in U_K.$$

Nach Voraussetzung ist also x primitiv für $B|A$ und nach 3.6 existiert eine normale Ganzheitsbasis für $L|K$. □

Anmerkung. Die normale Ganzheitsbasis für $B|A$ ist in diesem Fall die Basis $(\theta\mu^{-1}, (\theta\mu^{-1})^\sigma)$. Es ist nämlich $1 = \theta\mu^{-1} + (\theta\mu^{-1})^\sigma$. Somit ist unsere normale Ganzheitsbasis zur ganzen Potenzbasis $(1, \theta\mu^{-1})$ äquivalent.

Kapitel 4

Erweiterungen ungeraden Grades

In diesem Abschnitt untersuchen wir die Existenz von Steinitzwurzeln für Zahlkörper-Erweiterungen $L|K$ mit ungeradem Grad n. Nach Hecke [He, Satz 176] ist die Differente einer Körpererweiterung algebraischer Zahlkörper ein Quadrat in der Idealklassengruppe von L. Wir werden beweisen, dass in Körperweiterungen $L|K$ ungeraden Grades stets eine Steinitzwurzel Δ existiert. Ist $L|K$ zusätzlich galoissch, können wir sogar darauf verzichten, den tiefliegenden Satz von Hecke zu benutzen.

4.1 Satz. *Sei $L|K$ eine Galoiserweiterung von Zahlkörpern mit ungeradem Grad und Gruppe G. Dann gibt es ein Galois-invariantes Ideal $\mathfrak{W}$ in B, dessen Quadrat die Differente $\mathcal{D}$ ist. Seine Idealklasse $[\mathfrak{W}]$ ist eine Galois-invariante Steinitzwurzel für $L|K$. Das Ideal $\mathfrak{W}$ enthält alle in $L|K$ verzweigten Primideale.*

Beweis. Sei $G_{\mathfrak{P}} = \{\sigma \in G | \mathfrak{P}^\sigma = \mathfrak{P}\}$ die Zerlegungsgruppe eines Primideals $\mathfrak{P}$ in B. Wir definieren wie üblich die i-ten Verzweigungsgruppen $G^{(i)}$ als

$$G_{\mathfrak{P}}^{(i)} = \{\sigma \in G_{\mathfrak{P}} | x^\sigma \equiv x \ (mod\ \mathfrak{P}^{i+1}) \ \forall x \in B\}.$$

Es ist offensichtlich, dass $G_{\mathfrak{P}}^{(i)} \leq G_{\mathfrak{P}} \leq G$ und $|G_{\mathfrak{P}}^{(0)}| = e(\mathfrak{P}|\mathfrak{p})$ ist. Der Verzweigungsindex $e(\mathfrak{P}|\mathfrak{p})$ ist also immer ungerade. Sei $\mathcal{D} = \prod \mathfrak{P}^{m_{\mathfrak{P}}}$ die Primidealzerlegung der Differente in B. Nach [Nar, Prop. 6.6] gilt für die Exponenten

$$m_{\mathfrak{P}} = \sum_{i=0}^{s} (|G_{\mathfrak{P}}^{(i)} - 1|),$$

wobei $G_{\mathfrak{P}}^{(i)}$ die $(s+1)$-ten (nicht-trivialen) i-ten Verzweigungsgruppen von $L|K$ zum Primideal $\mathfrak{P}$ sind (Hilbert-Formel).
Ist nun eine Primstelle $\mathfrak{P}$ unverzweigt, so ist $G_{\mathfrak{P}}^{(0)}$ trivial und $m_{\mathfrak{P}} = 0$. Verzweigt die dyadische Primstelle, so ist sie zahm verzweigt, da 2 den Verzweigungsindex nicht teilt. Nach dem Exponentensatz für die Differente [Ha1, p.423] ist der Exponent von $\mathfrak{P}|2$ in der

Zerlegung der Differente gerade (nämlich $e(\mathfrak{P}|2)-1$).
Sei nun $\mathfrak{P}$ eine verzweigende Primstelle über einer ungeraden Primzahl p. Für alle (nichttrivialen) höheren Verzweigungsgruppen gilt, dass $|G_{\mathfrak{P}}^{(i)}|$ ungerade, also $|G_{\mathfrak{P}}^{(i)}|-1$ gerade ist. Damit ist auch $m_{\mathfrak{P}}$ gerade und somit die Differente $\mathcal{D}=\mathfrak{W}^2$ ($\mathfrak{W}=\prod\mathfrak{P}^{m_{\mathfrak{P}}/2}$) ein Quadrat in I_L und damit auch in $C\ell_L$.
Da die Erweiterung von ungeradem Grad ist, gilt für ein primitives $\beta\in B$, dass das Hauptideal $\delta(m_\beta)=(w)^2$ ein Quadrat in H_A, der Gruppe der Hauptideale von A, ist ($w\in A$). (Nach Vandermonde gilt $\delta(m_\beta)=\prod_{i<j}(\beta_i-\beta_j)^2$. Da keine quadratische Teilerweiterung existiert, gilt $K(\sqrt{\delta(m_\beta)})=K$, also $\delta(m_\beta)\in(K^*)^2$.) Mit 1.12 folgt $\delta=\delta(m_\beta)\mathfrak{a}^2$ mit $\mathfrak{a}\in s_A(B)$. Also ist

$$\big(N_{L|K}(\mathfrak{W})\big)^2=N(\mathcal{D})=\delta=\delta(m_\beta)\mathfrak{a}^2=\big((w^2)\mathfrak{a}^2\big)=\big((w)\mathfrak{a}\big)^2.$$

Es ist also $N_{L|K}(\mathfrak{W})=(w)\mathfrak{a}$, modulo Hauptideale haben wir also $[N_{L|K}(\mathfrak{W})]=[\mathfrak{a}]=s_A(B)$. Da die Erweiterung galoissch ist und das Ideal $\mathfrak{W}$ wie die Differente $\mathcal{D}$ alle verzweigten Primideale enthält, sind die Exponenten $m_{\mathfrak{P}}$ aller Primideale $\mathfrak{P}$ über einem festen Primideal $\mathfrak{p}$ in K identisch. Die Steinitzwurzel $[\mathfrak{W}]$ ist schließlich, wie das Ideal $\mathfrak{W}$ selbst, invariant unter G. □

Dieser Satz liefert uns im Falle einer Galoiserweiterung mit ungeradem Grad einen algebraischen Beweis zu Satz 176 von Hecke und eine Interpretation der Wurzel der Differente in $C\ell_L$ als das Urbild der Steinitzklasse $s_A(B)$ unter der Norm.
Für den Fall einer nicht-normalen Erweiterung benötigen wir das Resultat von Hecke, um zu solch einer Interpretation der Wurzel der Differente zu gelangen.

4.2 Satz. *Sei $L|K$ eine Erweiterung mit ungeradem Grad. Dann existiert eine Steinitzwurzel Δ für $L|K$.*

Beweis. Nach Hecke existiert eine Wurzel Δ_0 der Idealklasse der Differente $[\mathcal{D}]$. Es gilt $N_{L|K}(\Delta_0)=\Gamma_0\in C\ell_K$, mit $\Gamma_0^2=[N_{L|K}\mathcal{D}]=[\delta]$. Nach 1.11 ist $s_A(B)^2=[\delta]=\Gamma_0^2$, also gilt

$$\big(s_A(B)\Gamma_0^{-1}\big)^2=1,\ \text{damit ist } o(s_A(B)\Gamma_0^{-1})\le 2 \text{ in } C\ell_K.$$

Ist $o(s_A(B)\Gamma_0^{-1})=1$, so ist Δ_0 eine Wurzel der Differente mit $N_{L|K}(\Delta_0)=s_A(B)$.
Sei nun $o(s_A(B)\Gamma_0^{-1})=2$. Wir setzen $\Delta=\iota_{L|K}(s_A(B)\Gamma_0^{-1})$. Die Ordnung von Δ in $C\ell_L$ ist dann auch kleiner gleich 2. Da die Hintereinanderausführung der Abbildungen $\iota_{L|K}$ und $N_{L|K}$ auf $C\ell_K$ die Potenzierung mit dem Grad $[L:K]$ bewirkt, erhalten wir

$$N_{L|K}(\Delta)=N_{L|K}\circ\iota_{L|K}(s_A(B)\Gamma_0^{-1})=(s_A(B)\Gamma_0^{-1})^{[L:K]}=s_A(B)\Gamma_0^{-1}.$$

Die letzte Gleichheit folgt aus $[L:K]$ ungerade und $o(s_A(B)\Gamma_0^{-1})=2$. Wir setzen $\tilde{\Delta}=\Delta\Delta_0\in C\ell_L$ und erhalten wegen $\Delta^2=1$ in $C\ell_L$

$$\tilde{\Delta}^2=\Delta^2\Delta_0^2=[\mathcal{D}]$$

und

$$N_{L|K}\tilde{\Delta} = N_{L|K}\Delta N_{L|K}\Delta_0 = s_A(B)\Gamma_0^{-1}\Gamma_0 = s_A(B).$$

In diesem Fall ist $\tilde{\Delta}$ die gesuchte Steinitzwurzel für $L|K$. □

Wir haben also gesehen, dass es in Erweiterungen ungeraden Grades stets möglich ist, eine Steinitzwurzel zu finden. In Erweiterungen mit geradem Grad ist dies nicht der Fall, wie sich in Beispiel 1.23 am Ende von Kapitel 1 gezeigt hat.

Kapitel 5

Idealtheoretische Diskriminante und Differente

Schon in Kapitel 1 haben wir gesehen, dass die Existenz einer relativen Ganzheitsbasis mit der Idealklasse der Diskriminante zusammenhängt. Existiert eine Basis, so ist die Diskriminante ein Hauptideal. Die Umkehrung gilt jedoch nicht; dies belegen etwa unverzweigte Erweiterungen $L|K$, für die keine relative Ganzheitsbasis existiert. Es ist dann $\delta = A$ ein Hauptideal und $s_A(B) \neq 1$, wie etwa im Beispiel 1.23.

A. Fröhlich [Fr1] hat 1960 den Begriff der idealtheoretischen Diskriminante eingeführt. Mit dieser Formulierung gelingt es ihm, ein notwendiges und hinreichendes Kriterium für die Existenz einer relativen Ganzheitsbasis herzuleiten:

> Eine relative Ganzheitsbasis einer Körpererweiterung $L|K$ existiert genau dann, wenn die idealtheoretische Diskriminante ein Hauptidel ist.

Wir werden dieses Resultat im nächsten Lemma aufgreifen, doch zunächst geben wir eine kurze Einführung in die Theorie der Idele. Für das weitere Studium verweisen wir auf einschlägige Werke, etwa [Sch].
Ein Idel ist eine Familie $\alpha = (\alpha_\mathfrak{p})$ von Elementen $\alpha_\mathfrak{p} \in K_\mathfrak{p}^*$, die fast immer (lokale) Einheiten sind. Dabei durchläuft $\mathfrak{p}$ alle Primstellen von K. Die Idele bilden bezüglich komponentenweiser Multiplikation die (abelsche) Idelgruppe J_K. Der Körper K^* selbst wird via $x \mapsto (x, \dots x, \dots)$ in J_K eingebettet. Man nennt K^* die Gruppe der Hauptidele, J_K/K^* die Idelklassengruppe.
Die Koeffizienten eines Idels sind Elemente der lokalen Körper $K_\mathfrak{p}$. Seien $L_\mathfrak{P}|K_\mathfrak{p}$ die lokalen Körper zu $\mathfrak{P}|\mathfrak{p}$ in $L|K$, $B_\mathfrak{P}|A_\mathfrak{p}$ ihre Bewertungsringe mit Einheiten $U_\mathfrak{P}, U_\mathfrak{p}$. Ist $\mathfrak{p}$ eine endliche Stelle, so ist $A_\mathfrak{p}$ der Ring der ganzen $\mathfrak{p}$-adischen Zahlen in $K_\mathfrak{p}$ mit Einheiten $U_\mathfrak{p}$. Für archimedische Stellen $\mathfrak{p}$ ist der Ring der ganzen Zahlen $A_\mathfrak{p} = K_\mathfrak{p}$ und die Einheitengruppe $U_\mathfrak{p} = {K_\mathfrak{p}}^*$.

Im Lokalen existiert immer eine ganze Potenzbasis. Es ist also für geeignetes $\beta \in B_{\mathfrak{P}}$ $B_{\mathfrak{P}} = A_{\mathfrak{p}}[\beta]$. Damit ist die (lokale) Diskriminante $\delta_{\mathfrak{p}}$ die Diskriminante der ganzen Potenzbasis. Sie ist nach 1.12 bis auf ein Quadrat in $U_{\mathfrak{p}}$ (eindeutig) bestimmt, es ist also $\delta_{\mathfrak{p}} \equiv \delta_{\mathfrak{p}}(1, \beta, \beta^2 \cdots \beta^{n_{\mathfrak{p}}})$ $(mod\ {U_{\mathfrak{p}}}^2)$ mit lokalem Erweiterungsgrad $n_{\mathfrak{p}} = [L_{\mathfrak{P}} : K_{\mathfrak{p}}]$. Von der Elementdiskriminante $\delta_{\mathfrak{p}}(\beta)$ unterscheidet sich $\delta_{\mathfrak{p}}$ um eine Einheit. Es gilt

$$\delta_{\mathfrak{p}}(\beta) = N_{\mathfrak{p}}(m'_{K_{\mathfrak{p}},\beta}(\beta)) = (-1)^{n_{\mathfrak{p}}(n_{\mathfrak{p}}-1)/2}\delta_{\mathfrak{p}}(m_{K_{\mathfrak{p}},\beta}) = (-1)^{n_{\mathfrak{p}}(n_{\mathfrak{p}}-1)/2}\delta_{\mathfrak{p}},$$

mit dem Minimalpolynom $m_{K_{\mathfrak{p}},\beta}$ von β über $K_{\mathfrak{p}}$.

Sei nun J_K die Idelgruppe in K und $C_K = J_K/K^*$ die Idelklassengruppe. Der kanonische Epimorphismus $\Psi : J_K \to I_K$ bildet das Idel $\alpha = (\alpha_{\mathfrak{p}})_{\mathfrak{p}}$ auf das Ideal $\prod_{\mathfrak{p}\in\mathbb{P}_K} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})}$ ab. Diese Abbildung ist sinnvoll, da laut Definition des Idels fast immer $v_{\mathfrak{p}}(\alpha_{\mathfrak{p}}) = 0$ ist. Der Kern von Ψ ist $U_K = J_K^{\infty} = \prod_{\mathfrak{p}\in\mathbb{P}_K^{\infty}} {K_{\mathfrak{p}}}^* \times \prod_{\mathfrak{p}\in\mathbb{P}_K} U_{\mathfrak{p}}$, wir erhalten also $J_K/U_K \cong I_K$ und $J_K/U_K K^* \cong C\ell_K$.
Die idealtheoretische Diskriminante $\delta^* = (\delta_{\mathfrak{p}})_{\mathfrak{p}}$ setzt sich nun wie folgt zusammen:
An den endlichen Stellen haben wir als Einträge den $\mathfrak{p}$-Anteil der idealtheoretischen Diskriminante δ. Dieser ist identisch mit dem Produkt der Diskriminanten $\delta_{\mathfrak{P}} = \delta(L_{\mathfrak{P}}|K_{\mathfrak{p}})$ der lokalen Erweiterungen $L_{\mathfrak{P}}|K_{\mathfrak{p}}$, d.h. $\delta_{\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} \delta_{\mathfrak{P}}$.
An den unendlichen Stellen schreiben wir für die lokale Diskriminante $\delta_{\mathfrak{p}} = (-1)^r$, wobei r die Anzahl der komplexen Körper $L_{\mathfrak{P}}$ über dem reellen Körper $K_{\mathfrak{p}}$ ist (siehe [Fr1, Thm. 4.5]). Jede Stelle ist modulo ${U_{\mathfrak{p}}}^2$ eindeutig bestimmt, daher ist die idealtheoretische Diskriminante als Element in J_K/U_K^2 wohldefiniert.
Durch die Einbettung von U_K^2 in U_K wird ein Homomorphismus von J_K/U_K^2 nach $J_K/U_K (\cong I_K)$ induziert; dieser bildet die idealtheoretische Diskriminante δ^* wieder auf die übliche Diskriminante δ von $L|K$ ab [Fr1, p.21].

5.1 Lemma. *δ^* ist ein Element von $J_K^2 K^*/U_K^2$. Ist $\delta^* = \alpha(x_{\mathfrak{p}})^2 U_K^2$ mit $\alpha \in K^*$ und einem Idel $x = (x_{\mathfrak{p}}) \in J_K$, so ist die Steinitzklasse $s_A(B) = [\Psi(x)]$. Insbesondere ist also $s_A(B) = 1$, genau dann wenn δ^* durch ein Hauptidel repräsentiert werden kann.*

Beweis. [Fr2, p.17f].

Unser Augenmerk liegt auf der Differente und deren Quadratwurzel in $C\ell_L$. Wir führen dazu die idealtheoretische Differente ein. Eine sinnvolle Definition muss leisten, dass

$$\mathcal{D} = \Psi(\mathcal{D}^*) \text{ bzw. } [\mathcal{D}] = [\Psi(\mathcal{D}^*)]$$

gilt, also die idealtheoretische Differente unter der kanonischen Abbildung zum wohlbekannten Differenten-Ideal bzw. zur Klasse der Differenten in $C\ell_L$ wird.

Wünschenswert wäre, dass die idealtheoretische Differente zusätzlich auch die aus der Idealtheorie bekannte Tatsache

$$N_{L|K}(\mathcal{D}^*) = \delta^*$$

erfüllt. Dieser Punkt wird uns allerdings einige Schwierigkeiten bereiten und wir werden sehen, dass er nicht ohne weitere Voraussetzungen an die Körpererweiterung $L|K$ zu realisieren sein wird.

Wir wissen, dass für die Bewertungsringe in lokalen Erweiterungen immer eine ganze Potenzbasis existiert. Seien $B_\mathfrak{P}|A_\mathfrak{p}$ die Ringe in $L_\mathfrak{P}|K_\mathfrak{p}$. Dann gibt es ein Element $\theta \in B_\mathfrak{P}$ mit $B_\mathfrak{P} = A_\mathfrak{p}[\theta]$. Sei $m_{K_\mathfrak{p},\theta} = \prod_{i=1}^{n}(X - \theta_j)$ das Minimalpolynom von θ über $K_\mathfrak{p}$ mit der Zerlegung in Linearfaktoren im Zerfällungskörper und $m'_{K_\mathfrak{p},\theta}$ seine Ableitung. Für den Dualmodul ${B_\mathfrak{P}}'$ gilt nach [Nar, Prop. 4.11]

$${B_\mathfrak{P}}' = \frac{1}{m'_{K_\mathfrak{p},\theta}(\theta)} B_\mathfrak{P}.$$

Damit ist also die (lokale) Differente $\mathcal{D}_\mathfrak{P} = \mathcal{D}_{B_\mathfrak{P}|A_\mathfrak{p}} = (m'_{K_\mathfrak{p},\theta}(\theta))$, wobei $m'_{K_\mathfrak{p},\theta}(\theta) = \prod_{j\neq 1}(\theta - \theta_j)$ für $\theta = \theta_1$.
Sei λ ein weiteres primitives Element für $B_\mathfrak{P}|A_\mathfrak{p}$ mit Minimalpolynom $m_{K_\mathfrak{p},\lambda}$ und Zerlegung in Linearfaktoren $\prod_{i=1}^{n}(X - \lambda_i)$ mit $\lambda = \lambda_1$. Dann gilt also auch $\mathcal{D}_\mathfrak{P} = (m'_{K_\mathfrak{p},\lambda}(\lambda)) = \prod_{j\neq 1}(\lambda - \lambda_j)$. Die beiden Differenten unterscheiden sich also um den Faktor $c = \frac{\prod(\theta-\theta_j)}{\prod(\lambda-\lambda_j)}$. Wir zeigen, dass die Norm von c in ${U_\mathfrak{p}}^2$ liegt, und damit c eine Einheit in $B_\mathfrak{P}$ ist, weswegen die beiden Differenten (als Ideale) identisch sind. Es gilt

$$\begin{aligned} N_\mathfrak{P}(c) &= N_\mathfrak{P}\left(\frac{\prod(\theta-\theta_j)}{\prod(\lambda-\lambda_j)}\right) = N_\mathfrak{P}\left(\frac{m'_{K_\mathfrak{p},\theta}(\theta)}{m'_{K_\mathfrak{p},\lambda}(\lambda)}\right) = \frac{(-1)^{n(n-1)/2}\delta_\mathfrak{p}(m_{K_\mathfrak{p},\theta})}{(-1)^{n(n-1)/2}\delta_\mathfrak{p}(m_{K_\mathfrak{p},\lambda})} \\ &= \frac{\left[\ B_\mathfrak{P} : A_\mathfrak{p}[\theta]\ \right]^2 \delta_\mathfrak{p}}{\left[\ B_\mathfrak{P} : A_\mathfrak{p}[\lambda]\ \right]^2 \delta_\mathfrak{p}} = \frac{u_1^2}{u_2^2} = u_3^2 \in {U_\mathfrak{p}}^2, \end{aligned}$$

mit $u_i \in U_\mathfrak{p}$ geeignet.
Damit ist die lokale Differente $\mathcal{D}_\mathfrak{P}$ bis auf (noch näher zu spezifizierende) Einheiten eindeutig bestimmt und wir können nun die idealtheoretische Differente definieren.

5.2 Definition. Mit den obigen Bezeichnungen sei

$${U_\mathfrak{P}}^* := \{u \in U_\mathfrak{P} : u \in {N_\mathfrak{P}}^{-1}({U_\mathfrak{p}}^2)\}$$

das Urbild von ${U_\mathfrak{p}}^2$ in $U_\mathfrak{P}$ unter der Normabbildung. Für jede endliche Primstelle $\mathfrak{P}|\mathfrak{p}$ setzen wir $\mathcal{D}_\mathfrak{P} = m'_{K_\mathfrak{p},\theta}(\theta)$, wobei θ primitiv für $B_\mathfrak{P}|A_\mathfrak{p}$ ist. An den unendlichen Stellen setzen wir $\mathcal{D}_\mathfrak{P} = 1$. Desweiteren sei $U_L^* = \prod_\mathfrak{P} {U_\mathfrak{P}}^*$. Damit wird die idealtheoretische Differente $\mathcal{D}^*$ definiert als

$$\mathcal{D}^* = ({\mathcal{D}_\mathfrak{P}}^*)U_L^*.$$

Anmerkung. Die Wahl $\mathcal{D}_{\mathfrak{P}} = 1$ für unendliche Stellen ist sinnvoll. An den unverzweigten unendlichen Stellen ist die Differente offensichtlich trivial. Ist $\mathfrak{p}$ eine verzweigende archimedische Stelle, so ist $L_{\mathfrak{P}} = \mathbb{C}$ und $K_{\mathfrak{p}} = \mathbb{R}$, also $L_{\mathfrak{P}} = K_{\mathfrak{p}}(i)$, damit auch $B_{\mathfrak{P}} = A_{\mathfrak{p}}[i]$. Die Differente des Elementes i berechnen wir mit der Ableitung des Minimalpolynoms und erhalten

$$\mathcal{D}_{\mathfrak{P}} \equiv 2i \equiv 1 \ (mod\ {U_{\mathfrak{P}}}^*),$$

da die Norm $N(2i) = -4i^2 = 4$ in ${U_{\mathfrak{p}}}^2$ $(= ({K_{\mathfrak{p}}}^*)^2)$, also $2i$ in ${U_{\mathfrak{P}}}^*$ liegt.

5.3 Satz. *Für die idealtheoretische Differente $\mathcal{D}^*$ gilt $\Psi(\mathcal{D}^*) = \mathcal{D}$. Ist -1 ein Quadrat in K^* oder $L|K$ galoissch mit durch 4 teilbarem Grad, so gilt die Gleichung $N_{L|K}(\mathcal{D}^*) = \delta^*$, sonst gilt sie nur bis auf lokale Vorzeichen.*

Beweis. Da sowohl die archimedischen Stellen als auch die Einheiten $U_L \supseteq {U_{\mathfrak{P}}}^*$ im Kern der Abbildung Ψ liegen, müssen wir nur noch das Verhalten der endlichen Stellen unter Ψ untersuchen. Nach [Ha1, p.429] gilt bekanntlich für die (globale) Differente

$$\mathcal{D} = \prod_{\mathfrak{P}} \mathcal{D}_{\mathfrak{P}} \text{ und } \mathcal{D}_{\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathcal{D}_{\mathfrak{P}},$$

wobei $\mathcal{D}_{\mathfrak{P}}$ die Differente der Erweiterung $L_{\mathfrak{P}}|K_{\mathfrak{p}}$ ist. Laut Definition gilt $\Psi({\mathcal{D}_{\mathfrak{P}}}^*) = \prod_{\mathfrak{P}} \mathfrak{P}^{v_{\mathfrak{P}}(\mathcal{D}_{\mathfrak{P}})}$, wobei die Faktoren $\mathfrak{P}^{v_{\mathfrak{P}}(\mathcal{D}_{\mathfrak{P}})}$ gerade der lokalen Differente $\mathcal{D}_{\mathfrak{P}}$ entsprechen. Mit obigem Zusammenhang zwischen globaler und lokaler Differente folgt die erste Behauptung.

Zur weiteren Argumentation erinnern wir auch hier an den Produktsatz für die Diskriminante δ [Ha1, p.429]

$$\delta = \prod_{\mathfrak{p}} \delta_{\mathfrak{p}} \text{ und } \delta_{\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} \delta_{\mathfrak{P}},$$

wobei $\delta_{\mathfrak{p}}$ den $\mathfrak{p}$-Anteil in δ bezeichnet und $\delta_{\mathfrak{P}}$ die Diskriminante der Erweiterung $L_{\mathfrak{P}}|K_{\mathfrak{p}}$. Für die Norm eines Idels $(\alpha_{\mathfrak{P}})$ gilt $N_{L|K}((\alpha_{\mathfrak{P}})) = (\prod_{\mathfrak{P}|\mathfrak{p}} N_{\mathfrak{P}}(\alpha_{\mathfrak{P}}))_{\mathfrak{p}}$. Definitionsgemäß wird U_L^* durch die Norm wie gewünscht auf U_K^2 abgebildet.
Wir unterscheiden endliche und unendliche Stellen. Sei $n_{\mathfrak{P}}$ der lokale Erweiterungsgrad. Ist $\mathfrak{P}|\mathfrak{p}$ endlich, so gilt für geeignetes $\theta \in B_{\mathfrak{P}}$ und dem Minimalpolynom $m_{K_{\mathfrak{p}},\theta}$ von θ über $K_{\mathfrak{p}}$, dass $\mathcal{D}_{\mathfrak{P}} = (m'_{K_{\mathfrak{p}},\theta}(\theta))$ und $N_{\mathfrak{P}}(\mathcal{D}_{\mathfrak{P}}) = (-1)^{n_{\mathfrak{P}}(n_{\mathfrak{P}}-1)/2}\delta_{\mathfrak{P}}$ gilt. Es ist also

$$\delta_{\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} \delta_{\mathfrak{P}} = \prod_{\mathfrak{P}|\mathfrak{p}} (-1)^{n_{\mathfrak{P}}(n_{\mathfrak{P}}-1)/2} N_{\mathfrak{P}}(\mathcal{D}_{\mathfrak{P}}).$$

Wir haben bis auf ein lokales Vorzeichen $(\prod_{\mathfrak{P}|\mathfrak{p}} (-1)^{n_{\mathfrak{P}}(n_{\mathfrak{P}}-1)/2})$ den Eintrag an der Stelle $\mathfrak{p}$ in δ^* erhalten.

Sei $\mathfrak{P}|\mathfrak{p}$ archimedisch. Der lokale Erweiterungsgrad $n_{\mathfrak{P}}$ ist 2, wenn $L_{\mathfrak{P}}$ komplex und $K_{\mathfrak{p}}$ reell (verzweigender Fall) ist, sonst ist $n_{\mathfrak{P}} = 1$. Es gilt auch hier die Gleichung

$$\delta_{\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} \delta_{\mathfrak{P}} = \prod_{\mathfrak{P}|\mathfrak{p}} (-1)^{n_{\mathfrak{P}}(n_{\mathfrak{P}}-1)/2} N_{\mathfrak{P}}(\mathcal{D}_{\mathfrak{P}}).$$

Ist $L_{\mathfrak{P}}|K_{\mathfrak{p}}$ verzweigt, so ist $n_{\mathfrak{P}} = 2$. Für jede verzweigte Erweiterung erhalten wir das Vorzeichen -1. Insgesamt ergibt sich also der Faktor $(-1)^r$, wobei r die Anzahl der komplexen Körper $L_{\mathfrak{P}}$ über dem reellen Körper $K_{\mathfrak{p}}$ ist. Da $N_{\mathfrak{P}}(\mathcal{D}_{\mathfrak{P}}) = 1$ ist, haben wir $\delta_{\mathfrak{p}} = (-1)^r$.
Wir sehen auch hier, dass sich die Norm der idealtheoretischen Differente (an den verzweigenden Stellen) um lokale Einheiten von der idealtheoretischen Diskriminante unterscheidet.
Ist hingegen -1 ein Quadrat in K^*, so liegt -1 auch in ${U_{\mathfrak{p}}}^2$ und die lokalen Vorzeichen bei den archimedischen und nicht-archimedischen Stellen "verschwinden" alle modulo ${U_{\mathfrak{p}}}^2$. Wir haben dann also wie gewünscht $N(\mathcal{D}^*) = \delta^*$.
Ist $L|K$ galoissch mit durch 4 teilbarem Grad n, so sind auch die lokalen Erweiterungen $L_{\mathfrak{P}}|K_{\mathfrak{p}}$ galoissch vom Grad $n_{\mathfrak{P}} = e(\mathfrak{P}|\mathfrak{p})f(\mathfrak{P}|\mathfrak{p})$. Ist $n_{\mathfrak{P}} \equiv 1$ oder 0 $(mod\ 4)$, so ist $(-1)^{n_{\mathfrak{P}}(n_{\mathfrak{P}}-1)/2}$ immer 1. Ist $n_{\mathfrak{P}} \equiv 2$ oder 3 $(mod\ 4)$, so muss die Zerlegungszahl r gerade sein, denn es ist $n = [L : K] = r \cdot [L_{\mathfrak{P}} : K_{\mathfrak{p}}]$. Da wir eine Galoiserweiterung betrachten, ist der lokale Grad $n_{\mathfrak{P}}$ für jedes der r verschiedenen Primideale $\mathfrak{P}$ über $\mathfrak{p}$ identisch. Für die Diskriminante $\delta_{\mathfrak{p}}$ gilt dann

$$\delta_{\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} (-1)^{n_{\mathfrak{P}}(n_{\mathfrak{P}}-1)/2} N_{\mathfrak{P}}(\mathcal{D}_{\mathfrak{P}}) = \left((-1)^{n_{\mathfrak{P}}(n_{\mathfrak{P}}-1)/2}\right)^r \prod_{\mathfrak{P}} N_{\mathfrak{P}}(\mathcal{D}_{\mathfrak{P}}) = \prod_{\mathfrak{P}} N_{\mathfrak{P}}(\mathcal{D}_{\mathfrak{P}}).$$

Wiederum haben wir kein Problem mehr mit den (lokalen) Vorzeichen. □

Kapitel 6

Quadratische Erweiterungen

Nachdem wir in Kapitel 4 Erweiterungen ungeraden Grades studiert haben, widmen wir uns nun dem quadratischen Fall. Sei also $L|K$ eine Körpererweiterung vom Grad 2.
In Kapitel 3, 3.3 haben wir gesehen, welche Bedeutung dieser Fall haben kann. Obwohl die quadratischen Körpererweiterungen zunächst relativ elementar erscheinen, sehen wir bald, dass es uns hier im Vergleich zu den Erweiterungen ungeraden Grades deutlich schwerer fallen wird, die Frage nach der Existenz einer Steinitzwurzel positiv zu beantworten.
Allerdings ist uns für quadratische Erweiterungen $L|K$ mit Theorem 3.1 in [Fr1] ein Rezept gegeben, um die lokalen Erweiterungen $L_{\mathfrak{P}}|K_{\mathfrak{p}}$ zu untersuchen. Mit Hilfe der idealtheoretischen Differente aus dem vorangehenden Kapitel können wir auf die Frage nach der Steinitzwurzel eine positive Antwort geben; allerdings nicht ohne weitere Voraussetzungen an die Erweiterung $L|K$. Zu Beginn rufen wir uns Theorem 3.1 aus [Fr1] in Erinnerung.

6.1 Satz. *Sei $K_{\mathfrak{p}}$ ein $\mathfrak{p}$-adischer Zahlkörper mit Ring ganzer Zahlen $A_{\mathfrak{p}}$ und Einheitengruppe $U_{\mathfrak{p}}$. Sei $a \in A_{\mathfrak{p}} \setminus {A_{\mathfrak{p}}}^2$, wobei $\mathfrak{p}^2$ kein Teiler von (a) ist. Sei $\pi_{\mathfrak{p}}$ ein lokaler Parameter, also ein Element in $\mathfrak{p} \setminus \mathfrak{p}^2$.*
Ist $L_{\mathfrak{P}} = K_{\mathfrak{p}}(\sqrt{a})$ und $B_{\mathfrak{P}}$ der Ring der ganzen Zahlen in $L_{\mathfrak{P}}$, so tritt einer der folgenden Fälle ein:

(i) Ist $\pi_{\mathfrak{p}}$ kein Teiler von $2a$, dann ist

$$B_{\mathfrak{P}} = A_{\mathfrak{p}}[\sqrt{a}] \text{ und } \delta_{\mathfrak{P}} = \delta(L_{\mathfrak{P}}|K_{\mathfrak{p}}) = a \ (mod\ {U_{\mathfrak{p}}}^2).$$

(ii) Ist $\pi_{\mathfrak{p}}$ ein Teiler von a, dann ist

$$B_{\mathfrak{P}} = A_{\mathfrak{p}}[\sqrt{a}] \text{ und } \delta_{\mathfrak{P}} = \delta(L_{\mathfrak{P}}|K_{\mathfrak{p}}) = 4a \ (mod\ {U_{\mathfrak{p}}}^2).$$

(iii) Ist $\pi_{\mathfrak{p}}$ ein Teiler von 2, aber nicht von a, so sei
$s = max\{l \in \mathbb{N} : \mathfrak{p}^l | 2A_{\mathfrak{p}}$ und $x^2 \equiv a \ (mod\ \mathfrak{p}^{2l})$ ist lösbar in $A_{\mathfrak{p}}\}$ und $b \in A_{\mathfrak{p}}$ eine

Lösung dieser Kongruenz. Dann gilt

$$B_{\mathfrak{P}} = A_{\mathfrak{p}}[(b+\sqrt{a})\pi_{\mathfrak{p}}{}^{-s}] \text{ und } \delta_{\mathfrak{P}} = \delta(L_{\mathfrak{P}}|K_{\mathfrak{p}}) = 4a\pi_{\mathfrak{p}}{}^{-2s} \ (mod\ U_{\mathfrak{p}}{}^{2}).$$

Beweis. [Nar, Thm. 5.9].

Wir wissen nun, wie wir die lokalen Diskriminanten berechnen können. Wir benötigen sie, um die idealtheoretische Diskriminante zu bilden. Die $\mathfrak{p}$-Komponenten $\delta_{\mathfrak{p}}$ des Idels δ^* setzen sich ja aus den (verschiedenen) lokalen Diskriminanten $\delta_{\mathfrak{P}} = \delta(L_{\mathfrak{P}}|K_{\mathfrak{p}})$ zusammen. Im quadratischen Fall besteht dieses Produkt aber nur dann aus mehr als einem Faktor, wenn $\mathfrak{p}$ zerfällt. Verzweigt $\mathfrak{p}$ oder ist $\mathfrak{p}$ träge, so gibt es nur eine lokale Erweiterung $L_{\mathfrak{P}}$ über $K_{\mathfrak{p}}$. Zerfällt $\mathfrak{p}$, so gibt es zu den beiden Primidealen $\mathfrak{P}_1$, $\mathfrak{P}_2$ über $\mathfrak{p}$ je eine Erweiterung, diese ist allerdings trivial. Wir haben also $\delta(L_{\mathfrak{P}_1}|K_{\mathfrak{p}}) = \delta(L_{\mathfrak{P}_2}|K_{\mathfrak{p}}) = 1$ und damit auch für zerfallende Primideale $\delta_{\mathfrak{p}} = \delta_{\mathfrak{P}}$ für ein $\mathfrak{P}|\mathfrak{p}$.

In Kapitel 1 haben wir den engen Zusammenhang zwischen der Klasse der globalen Diskriminante und der Steinitzklasse $s_A(B)$ studiert. In Kapitel 5 zeigte uns die idealtheoretische Formulierung nach A. Fröhlich eine weitere Verbindung zwischen (idealtheoretischer) Diskriminante und der Steinitzklasse:
Die idealtheoretische Diskriminante ist modulo Hauptidelen ein Quadrat x^2. Das Idel x wird unter $\Psi : J_K \to I_K$ auf ein Ideal in der Steinitzklasse abgebildet.
Es ist evident, dass das Zusammenspiel dieser beiden Resultate einen weiteren Zugang zur Steinitzklasse $s_A(B)$ liefert.

6.2 Lemma. *Sei $L = K(\sqrt{a})$ mit $a \in A$ und $(a) = \prod_{\mathfrak{p}} \mathfrak{p}^{a_{\mathfrak{p}}}$. Sei $\pi_{\mathfrak{p}}$ ein Element in $\mathfrak{p} \setminus \mathfrak{p}^2$. Sei $k_{\mathfrak{p}}$ die größte ganze Zahl $\leq a_{\mathfrak{p}}/2$. Für jedes $\mathfrak{p}$ mit $a_{\mathfrak{p}}$ gerade definieren wir*

$$s_{\mathfrak{p}} = max\{s \in \mathbb{N} : \mathfrak{p}^s | 2A \text{ und } x^2 \equiv a\pi_{\mathfrak{p}}^{-a_{\mathfrak{p}}} \ (mod\ \mathfrak{p}^{2s}) \text{ ist lösbar } \}.$$

Für die übrigen Ideale $\mathfrak{p}$ setzen wir $s_{\mathfrak{p}} = 0$. Dann enthält die Steinitzklasse $s_A(B)$ das Ideal

$$\prod_{\mathfrak{p}} \mathfrak{p}^{-s_{\mathfrak{p}}-k_{\mathfrak{p}}}.$$

Beweis. [Nar, Lemma 7.19].

Mit den Methoden von Satz 6.1 lassen sich nicht nur die lokalen Diskriminanten bestimmen, sondern, was für uns von größerer Bedeutung ist, die primitiven Elemente für die lokalen Ringe $B_{\mathfrak{P}}|A_{\mathfrak{p}}$. Mit ihren Minimalpolynomen bzw. deren Ableitungen können wir die lokalen Differenten bis auf Einheiten in $U_{\mathfrak{P}}{}^*$ berechnen und erhalten damit die idealtheoretische Differente $\mathcal{D}^*$. Genau so werden wir im folgenden Satz vorgehen. Er wird zu einem wesentlichen Baustein von Hauptsatz 2 werden.

6.3 Satz. *Sei $L = K(\sqrt{a})$ mit $a \in A$. Jeder Primteiler $\mathfrak{p}$ von (a) und jede dyadische Primstelle verzweige in $L|K$. Dann gibt es ein Galois-invariantes Ideal $\mathfrak{W}$ in B, das genau die in $L|K$ verzweigten Primideale enthält und dessen Idealklasse $[\mathfrak{W}]$ eine Galois-invariante Steinitzwurzel für $L|K$ ist.*

Beweis. Wir gehen idealtheoretisch vor. Sei $\mathfrak{P}|\mathfrak{p}$ in L und $\mathcal{D}^* = (\mathcal{D}_\mathfrak{P})$ die idealtheoretische Differente von $L|K$. Zu den endlichen Primidealen $\mathfrak{p}, \mathfrak{P}$ haben wir die (lokalen) Erzeuger $\pi_\mathfrak{p}, \Pi_\mathfrak{P}$. Für die nicht-archimedischen Stellen betrachten wir die verschiedenen lokalen Körpererweiterungen $L_\mathfrak{P}|K_\mathfrak{p}$, dabei ist $m_{K_\mathfrak{p}}$ das Minimalpolynom des jeweiligen primitiven Elements für $B_\mathfrak{P}|A_\mathfrak{p}$.

(i) Ist $\pi_\mathfrak{p}$ kein Teiler von $2a$, so gilt $s_\mathfrak{p} = k_\mathfrak{p} = 0$ und $2 \in U_\mathfrak{p} \subseteq U_\mathfrak{P}$.
Nach 6.1 (i) ist $B_\mathfrak{P} = A_\mathfrak{p}[\sqrt{a}]$, also $m_{K_\mathfrak{p}} = X^2 - a$ und folglich

$$\mathcal{D}_\mathfrak{P} = 2\sqrt{a} \equiv 2\sqrt{a}{\pi_\mathfrak{p}}^{-k_\mathfrak{p}-s_\mathfrak{p}} \ (mod\ {U_\mathfrak{P}}^*).$$

Die Differente ist eine Einheit, es liegt also Unverzweigtheit vor.

(ii) Ist $\pi_\mathfrak{p}$ ein Teiler von a mit ungeradem Exponenten, also $v_\mathfrak{p}(a) = 2k_\mathfrak{p} + 1$, so ist nach Voraussetzung $\mathfrak{p}$ verzweigt in $L|K$. Nach Definition in 6.2 haben wir $s_\mathfrak{p} = 0$.
Sei $a_0 = a{\pi_\mathfrak{p}}^{-2k_\mathfrak{p}}$, damit ist $L_\mathfrak{P} = K_\mathfrak{p}(\sqrt{a}) = K_\mathfrak{p}(\sqrt{a_0})$, also nach 6.1, (ii) $B_\mathfrak{P} = A_\mathfrak{p}[\sqrt{a_0}]$ und $m_{K_\mathfrak{p}} = X^2 - a_0$. Für die Differente gilt somit

$$\mathcal{D}_\mathfrak{P} = 2\sqrt{a_0} = 2\sqrt{a{\pi_\mathfrak{p}}^{-2k_\mathfrak{p}}} \equiv 2\sqrt{a}{\pi_\mathfrak{p}}^{-k_\mathfrak{p}-s_\mathfrak{p}} \ (mod\ {U_\mathfrak{P}}^*).$$

(iii) Ist $\pi_\mathfrak{p}$ ein Teiler von a mit geradem Exponenten echt größer 0, so setzen wir wieder $a_0 = a{\pi_\mathfrak{p}}^{-2k_\mathfrak{p}}$, also ist $K_\mathfrak{p}(\sqrt{a}) = K_\mathfrak{p}(\sqrt{a_0})$. Da wir uns in der Situation von 6.1, (i) und (iii) befinden, müssen wir nun noch die Fälle unterscheiden, ob $\pi_\mathfrak{p}$ dyadisch ist oder nicht.

(a) Ist $\pi_\mathfrak{p}$ kein Teiler von 2, so haben wir $s_\mathfrak{p} = 0$ und $2 \in {U_\mathfrak{P}}^*$. Damit folgt nach 6.1 (i) für die Differente

$$\mathcal{D}_\mathfrak{P} = 2\sqrt{a_0} = 2\sqrt{a}{\pi_\mathfrak{p}}^{-k_\mathfrak{p}-s_\mathfrak{p}} \equiv 2\sqrt{a}{\pi_\mathfrak{p}}^{-k_\mathfrak{p}-s_\mathfrak{p}} \ (mod\ {U_\mathfrak{P}}^*).$$

Wir sehen, dass die Differente eine Einheit in $U_\mathfrak{P}$ ist und $\mathfrak{p}$ damit nicht verzweigen kann. Es muss also nach Voraussetzung $k_\mathfrak{p} = 0$ sein.

(b) Ist $\pi_\mathfrak{p}$ ein Teiler von 2, so befinden wir uns in der Situation von 6.1(iii). Ist $b \in A_\mathfrak{p}$ eine Lösung der Kongruenz, so gilt $B_\mathfrak{P} = A_\mathfrak{p}[\frac{b+a_0}{{\pi_\mathfrak{p}}^{s_\mathfrak{p}}}]$. Das Minimalpolynom dieses primitiven Elements ergibt sich dann zu $m_{K_\mathfrak{p}} = X^2 - \frac{2b}{{\pi_\mathfrak{p}}^{s_\mathfrak{p}}}X + \frac{b^2-a_0}{{\pi_\mathfrak{p}}^{s_\mathfrak{p}}}$. Damit ist die Differente $\mathcal{D}_\mathfrak{P} = 2\frac{b+\sqrt{a_0}}{{\pi_\mathfrak{p}}^{s_\mathfrak{p}}} - \frac{2b}{{\pi_\mathfrak{p}}^{s_\mathfrak{p}}} = \frac{2\sqrt{a_0}}{{\pi_\mathfrak{p}}^{s_\mathfrak{p}}}$, also

$$\mathcal{D}_\mathfrak{P} = 2\sqrt{a}{\pi_\mathfrak{p}}^{-k_\mathfrak{p}-s_\mathfrak{p}} \equiv 2\sqrt{a}{\pi_\mathfrak{p}}^{-k_\mathfrak{p}-s_\mathfrak{p}} \ (mod\ {U_\mathfrak{P}}^*).$$

(iv) Bleibt zuletzt noch der Fall zu untersuchen, wo $\pi_\mathfrak{p}$ ein Teiler von 2, aber nicht von a ist. Hier haben wir $k_\mathfrak{p} = 0$ und für die Differente gilt nach 6.1(iii) $\mathcal{D}_\mathfrak{P} = 2\frac{b+\sqrt{a}}{{\pi_\mathfrak{p}}^{s_\mathfrak{p}}} - \frac{b}{{\pi_\mathfrak{p}}^{s_\mathfrak{p}}} = 2\sqrt{a}{\pi_\mathfrak{p}}^{-s_\mathfrak{p}}$, also

$$\mathcal{D}_\mathfrak{P} \equiv 2\sqrt{a}{\pi_\mathfrak{p}}^{-k_\mathfrak{p}-s_\mathfrak{p}} \ (mod\ {U_\mathfrak{P}}^*).$$

Wir erhalten damit insgesamt für jede lokale Erweiterung $L_\mathfrak{P}|K_\mathfrak{p}$ bezüglich endlichen Primstellen $\mathfrak{P}|\mathfrak{p}$ die Differente

$$\mathcal{D}_\mathfrak{P} \equiv 2\sqrt{a}{\pi_\mathfrak{p}}^{-k_\mathfrak{p}-s_\mathfrak{p}} \ (mod\ {U_\mathfrak{P}}^*),$$

mit $k_\mathfrak{p}, s_\mathfrak{p}$ wie oben.
Verzweigt $\mathfrak{p}$ in $L_\mathfrak{P}|K_\mathfrak{p}$, so gilt $\pi_\mathfrak{p} = u{\Pi_\mathfrak{P}}^2$ mit einem $u \in U_\mathfrak{P}$. Für die Norm von u ergibt sich

$$N(u) = N(\frac{\pi_\mathfrak{p}}{{\Pi_\mathfrak{P}}^2}) = {\pi_\mathfrak{p}}^2 N(\Pi_\mathfrak{P})^2 \in {U_\mathfrak{p}}^2.$$

Damit ist $u \in {U_\mathfrak{P}}^*$, und wir haben für die lokalen Erweiterungen, in denen $\mathfrak{p}$ verzweigt, (mit $v = u^{-k_\mathfrak{p}-s_\mathfrak{p}} \in {U_\mathfrak{P}}^*$)

$$\mathcal{D}_\mathfrak{P} \equiv 2\sqrt{a}{\Pi_\mathfrak{P}}^{2(-k_\mathfrak{p}-s_\mathfrak{p})}v \equiv 2\sqrt{a}({\Pi_\mathfrak{P}}^{-k_\mathfrak{p}-s_\mathfrak{p}})^2 \ (mod\ {U_\mathfrak{P}}^*).$$

Im Falle der Unverzweigtheit gilt jedoch auch, dass

$$\mathcal{D}_\mathfrak{P} \equiv 2\sqrt{a}({\Pi_\mathfrak{P}}^{-k_\mathfrak{p}-s_\mathfrak{p}})^2 \ (mod\ {U_\mathfrak{P}}^*)$$

ist, da der Exponent $-k_\mathfrak{p} - s_\mathfrak{p} = 0$ erfüllt.

Wir setzen nun $x_\mathfrak{P} = {\Pi_\mathfrak{P}}^{-k_\mathfrak{p}-s_\mathfrak{p}}$ für alle endlichen Primstellen, $x_\mathfrak{P} = 1$ sonst und erhalten damit das Idel $x = (x_\mathfrak{P})$ von L.
Wir setzen $\mathfrak{W} = \Psi(x)$. Damit ist $\mathfrak{W} = (2\sqrt{a})\prod_\mathfrak{P} \mathfrak{P}^{-k_\mathfrak{p}-s_\mathfrak{p}}$ ein Ideal in L. Es enthält genau die in $L|K$ verzweigten Primstellen, ist also Galois-invariant wie jeder seiner Primteiler selbst. An dieser Stelle sei angemerkt, dass die Exponenten $-k_\mathfrak{p} - m_\mathfrak{p}$ aller Primideale $\mathfrak{P}$ über einem festen $\mathfrak{p} \in \mathbb{P}_K$ identisch sind, da sie nur von $\mathfrak{p}$ abhängen.
Es ergibt sich nun die Galois-invariante Idealklasse $[\mathfrak{W}] = [\prod_\mathfrak{P} \mathfrak{P}^{-k_\mathfrak{p}-s_\mathfrak{p}}]$ und wir sehen sofort, dass $[\mathfrak{W}]^2 = [\mathcal{D}]$ ist.

Abschliessend betrachten wir das Bild von $[\mathfrak{W}]$ unter der Norm, also die Idealklasse von $N(\prod_\mathfrak{P} \mathfrak{P}^{-k_\mathfrak{p}-s_\mathfrak{p}})$. Da alle im Produkt auftretenden Primideale $\mathfrak{P}$ (total) verzweigt sind, ist $N_{L|K}(\mathfrak{P}) = \mathfrak{p}$ $(= \mathfrak{P} \cap A)$. Damit ist $N_{L|K}\big([\mathfrak{W}]\big) = [\prod_\mathfrak{p} \mathfrak{p}^{-k_\mathfrak{p}-s_\mathfrak{p}}]$, was nach 6.2 der Steinitzklasse $s_A(B)$ entspricht. Wir haben mit $[\mathfrak{W}]$ eine Steinitzwurzel gefunden. □

Anmerkung. Wir haben im Beweis die idealtheoretische Differente zwar nicht in einer geschlossenen Form $\mathcal{D}^* = \alpha x^2 \cdot U_L^*$ mit einem Hauptidel α und einem Idel x angegeben, sind aber trotzdem in der Lage, die idealtheoretische Differente zu bestimmen. Da die Einheiten U_L^* und die archimedischen Stellen im Kern der Abbildung Ψ liegen, erhalten wir aus der Gleichung $\Psi(\mathcal{D}_{L|K}^*) = \mathcal{D}_{L|K}$ (5.3) die idealtheoretische Differente $\mathcal{D}_{L|K} = (2\sqrt{a})(\Pi_{\mathfrak{P}}{}^{-k_\mathfrak{p}-s_\mathfrak{p}})^2$.

Kapitel 7

Steinitzwurzeln in relativen Zahlkörpern

Wir haben nun alle Vorarbeiten geleistet, um Hauptsatz 2 beweisen zu können. Er setzt sich zusammen aus den Resultaten der Kapitel 2, 4 und 6. Um uns die Formulierung etwas zu erleichtern, führen wir eine neue Bezeichnung ein.

Eine quadratische Körpererweiterung $L|K$ hat die Eigenschaft ($\diamondsuit$), wenn gilt:

> Es ist $L = K(\sqrt{a})$ mit $a \in A$. Jeder Primteiler $\mathfrak{p}$ von (a) und jedes dyadische Primideal verzweigt in $L|K$.

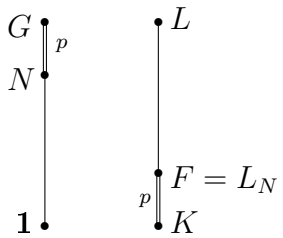
In Hauptsatz 2 beweisen wir die Existenz einer Steinitzwurzel Δ für auflösbare Körpererweiterungen $L|K$. Für die Galois-Invarianz von Δ benötigen wir eine weitere Voraussetzung an die Galoisgruppe G, die wir im Folgenden definieren werden.

7.1 Definition. [Hu, VI.8.5] Eine Gruppe G heisst *p-überauflösbar*, wenn für jeden Hauptfaktor von G mit Ordnung p^a gilt, dass $a = 1$, der Hauptfaktor also zyklisch von Ordnung p ist.

7.2 Hauptsatz 2. *Sei $L|K$ eine Galoiserweiterung algebraischer Zahlkörper mit auflösbarer Gruppe G. Jede quadratische Teilerweiterung $E|F$ von $L|K$ habe die Eigenschaft ($\diamondsuit$). Dann gibt es ein Ideal $\mathfrak{W}$ in L, dessen Idealklasse Δ eine Steinitzwurzel für $L|K$ ist. Ist G 2-überauflösbar, so ist die Steinitzwurzel Δ sogar Galois-invariant.*

Beweis. Wir gehen per Induktion nach der Gruppenordnung $|G|$ vor:

Sei N ein echter, maximaler Normalteiler von G und $F = L_N$ der dazugehörige Fixkörper mit Ring ganzer Zahlen C. Die Voraussetzung bezüglich der quadratischen Erweiterungen überträgt sich auf $L|F$ und $F|K$. Wegen der Maximalität von N ist $H = G/N = Gal(F|K)$ einfach. Weil G auflösbar ist, muss H von Primzahlordnung sein.



Laut 4.1 (für $|H|$ ungerade) bzw. 6.3 (für $|H| = 2$) gibt es ein Ideal $\mathfrak{W}_F$ in F bzw. C mit $[\mathfrak{W}_F^2] = [\mathcal{D}_{F|K}]$ und $N_{F|K}([\mathfrak{W}_F]) = s_A(C)$. Nach Induktionsvoraussetzung existiert für die Erweiterung $L|F$ ein Ideal $\mathfrak{W}_L$ in L bzw. B mit $[\mathfrak{W}_L^2] = [\mathcal{D}_{L|F}]$ und $N_{L|F}([\mathfrak{W}_L]) = s_C(B)$. Wir setzen

$$\mathfrak{W} = \iota_{L|F}(\mathfrak{W}_F) \cdot \mathfrak{W}_L$$

und haben damit $[\mathfrak{W}^2] = [(\mathfrak{W}_F B)^2] \cdot [\mathfrak{W}_L^2] = [\mathcal{D}_{F|K} B] \cdot [\mathcal{D}_{L|F}] = [(\mathcal{D}_{F|K} B)\mathcal{D}_{L|F}]$. Aufgrund der Transitivität der Differente folgt

$$[\mathfrak{W}^2] = [\mathcal{D}_{L|K}].$$

Weiterhin ist $N_{L|K}([\mathfrak{W}]) = N_{F|K}\big(N_{L|F} \circ \iota_{L|F}([\mathfrak{W}_F])\big) \cdot N_{F|K}\big(N_{L|F}([\mathfrak{W}_L])\big)$, also

$$N_{L|K}([\mathfrak{W}]) = N_{F|K}([\mathfrak{W}_F])^{[L:F]} \cdot N_{F|K}(N_{L|F}[\mathfrak{W}_L]) = s_A(C)^{[L:F]} \cdot N_{F|K}\big(s_C(B)\big) = s_A(B)$$

nach 2.2. Die Idealklasse $[\mathfrak{W}] = \Delta$ ist also eine Steinitzwurzel für $L|K$.
Für eine 2-überauflösbare Galoisgruppe G bleibt nun noch die Galois-Invarianz von Δ zu zeigen. Mit Induktion nach $|G|$ können wir sogar beweisen, dass das Ideal $\mathfrak{W}$ Galois-invariant ist. Sei dazu M ein minimaler Normalteiler von G. Dann ist M elementarabelsch, d.h. $M \cong Z_p \times \ldots \times Z_p$ ist das direkte Produkt zyklischer Gruppen der Primzahlordnung p. Sei L_M der Fixkörper von M in $L|K$.
Ist $|M|$ ungerade, so ist $L|F$ eine Galoiserweiterung ungeraden Grades. Wir haben also nach 4.1 ein Ideal $\mathfrak{W}_L$ in L, das genau die Primteiler der Differente $\mathcal{D}_{L|F}$ enthält. Es ist sogar $\mathfrak{W}_L^2 = \mathcal{D}_{L|F}$. Da die Differente $\mathcal{D}_{L|F}$ Galois-invariant unter $Gal(L|K)$ ist, muss auch das Ideal $\mathfrak{W}_L$ invariant unter $Gal(L|K)$ sein. Wäre dies nicht der Fall, so wäre aufgrund der Torsionsfreiheit der Idealgruppe auch die Differente nicht Galois-invariant.
Das Ideal $\mathfrak{W}_F$ bzw. $\iota_{L|F}(\mathfrak{W}_F)$ ist nach Induktionsvoraussetzung invariant unter $Gal(F|K)$ und als Ideal in F auch invariant unter $Gal(L|F)$. Damit ist auch das zusammengesetzte Ideal $\mathfrak{W} = \iota_{L|F}(\mathfrak{W}_F) \cdot \mathfrak{W}_L$ invariant unter $G = Gal(L|K)$ und $\Delta = [\mathfrak{W}]$ eine Galois-invariante Steinitzwurzel für $L|K$.
Ist $|M|$ gerade, so ist aufgrund der 2-Überauflösbarkeit von G die Erweiterung $L|F$ eine Galoiserweiterung vom Grad 2 und somit nach Voraussetzung von der Form ($\diamondsuit$). Es gilt also $L = F(\sqrt{a})$ mit $a \in C$ und jeder Primteiler von (a) sowie jedes dyadische Primideal

verzweigt in $L|K$. Laut 6.3 existiert ein Ideal $\mathfrak{W}_L$, das invariant unter $Gal(L|F)$ und dessen Idealklasse eine Steinitzwurzel für $L|F$ ist. Nach Induktionsvoraussetzung gibt es ein unter $Gal(F|K)$ invariantes Ideal $\mathfrak{W}_F$, das als Ideal von F natürlich unter $Gal(L|F)$ fest bleibt und somit insgesamt invariant unter $Gal(L|K)$ ist. Es bleibt also noch zu zeigen, dass das Ideal $\mathfrak{W}_L$ auch unter Operationen der Gruppe $Gal(L|K)$ fest bleibt. Sei $\sigma \in Gal(L|K)$. Weil $F|K$ galoissch ist, gilt für das Element $a \in C$, dass auch $a^\sigma \in C$ und $N_{F|K}(a) = N_{F|K}(a^\sigma)$ ist. Damit ist $N_{F|K}(\frac{a}{a^\sigma}) \in U_K$ und somit $\frac{a}{a^\sigma}$ eine Einheit in F. Die Hauptideale (a) und (a^σ) haben also dieselben Primteiler mit denselben Vielfachheiten. Ist etwa $\mathfrak{q}^m$ die maximale Potenz von $\mathfrak{q}$, die in (a) aufgeht, so geht auch $\mathfrak{q}^\sigma$ mit der Vielfachheit m in (a^σ) und somit in (a) auf. Für ein Primideal $\mathfrak{q}$ in F ist also insbesondere $v_\mathfrak{q}(a) = v_{\mathfrak{q}^\sigma}(a)$. Ist $\mathfrak{q}$ ein Teiler von (a), so verzweigen $\mathfrak{q}$ und $\mathfrak{q}^\sigma$ in L mit Verzweigungsindex 2. Sei $\mathfrak{P}$ das Ideal in L über $\mathfrak{q}$ und $\widetilde{\mathfrak{P}}$ das Ideal über $\mathfrak{q}^\sigma$. Es ist

$$v_\mathfrak{P}(a) = v_\mathfrak{q}(a) \cdot e(\mathfrak{P}|\mathfrak{q}) = v_{\mathfrak{q}^\sigma}(a) \cdot e(\widetilde{\mathfrak{P}}|\mathfrak{q}^\sigma) = v_{\widetilde{\mathfrak{P}}}(a).$$

Da $a = \sqrt{a}^2$ in L gilt, ist auch $v_\mathfrak{P}(\sqrt{a}) = v_{\widetilde{\mathfrak{P}}}(\sqrt{a})$. Da sowohl $L|F$ als auch $F|K$ galoissch sind, gilt auch $v_\mathfrak{P}(2) = v_{\widetilde{\mathfrak{P}}}(2)$. Insgesamt haben wir also $v_\mathfrak{P}(2\sqrt{a}) = v_{\widetilde{\mathfrak{P}}}(2\sqrt{a})$. Nach 6.3 ist die Differente $\mathcal{D}_{L|F} = (2\sqrt{a})(\prod_\mathfrak{P} \mathfrak{P}^{-k_\mathfrak{p}-s_\mathfrak{p}})^2$. Sie ist bekanntlich Galois-invariant unter $Gal(L|K)$ und für sie gilt daher ebenso $v_\mathfrak{P}(\mathcal{D}_{L|F}) = v_{\widetilde{\mathfrak{P}}}(\mathcal{D}_{L|F})$. Damit haben wir

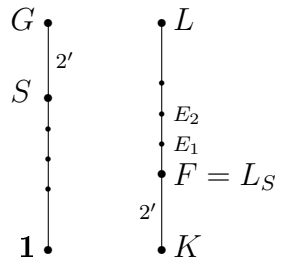
$$2 \cdot v_\mathfrak{P}(\mathfrak{W}_L) = v_\mathfrak{P}\Big(\frac{\mathcal{D}_{L|F}}{(2\sqrt{a})}\Big) = v_{\widetilde{\mathfrak{P}}}\Big(\frac{\mathcal{D}_{L|F}}{(2\sqrt{a})}\Big) = 2 \cdot v_{\widetilde{\mathfrak{P}}}(\mathfrak{W}_L).$$

Die Primideale $\mathfrak{P}|\mathfrak{q}$ und $\widetilde{\mathfrak{P}}|\mathfrak{q}^\sigma$ gehen also mit derselben Vielfachheit in $\mathfrak{W}_L$ auf. Die Abbildung σ lässt das Ideal $\mathfrak{W}_L$ also auch fest. Folglich ist $\mathfrak{W}_L$ invariant unter $G = Gal(L|K)$. Damit ist auch das zusammengesetzte Ideal $\mathfrak{W} = \iota_{L|F}(\mathfrak{W}_F) \cdot \mathfrak{W}_L$ invariant unter G und $\Delta = [\mathfrak{W}]$ eine Galois-invariante Steinitzwurzel für $L|K$. □

Die Auflösbarkeit, die wir in den Voraussetzungen fordern, bewirkt, dass wir in jedem Zwischenschritt Galoiserweiterungen haben. Daher können wir auch Satz 4.1 statt 4.2 verwenden. Das Besondere daran ist, dass wir für den auflösbaren Fall die Aussage des Hecke'schen Satzes gleich mitbewiesen haben.
Verzichten wir in den Voraussetzungen auf die Auflösbarkeit der Gruppe G, so finden wir zwar kein Ideal $\mathfrak{W}$ mit obigen Eigenschaften, dafür aber zumindest eine Idealklasse in $C\ell_L$, die eine Steinitzwurzel für $L|K$ ist. Hierfür benötigen wir allerdings, wie auch schon in 4.2, Heckes Satz 176 über die Existenz einer Quadratwurzel von $[\mathcal{D}]$ in $C\ell_L$.

7.3 Satz. *Sei $L|K$ eine Galoiserweiterung algebraischer Zahlkörper mit Gruppe G. Jede quadratische Teilerweiterung $E|F$ von $L|K$ habe die Eigenschaft ($\diamondsuit$). Dann existiert eine Steinitzwurzel für $L|K$.*

Beweis. Sei $S = Syl_2(G)$ die 2-Sylowgruppe von G und $F = L_S$ der dazugehörige Fixkörper in $L|K$ mit Ring ganzer Zahlen C.



Die Erweiterung $F|K$ hat ungeraden Grad. Nach 4.2 existiert also eine Steinitzwurzel $\Delta_F \in C\ell_F$ für $F|K$. Sei $E_1|F$ eine quadratische Erweiterung von F in $L|K$ mit Ring C_1. Die Erweiterung erfüllt die Eigenschaft ($\diamondsuit$), mit 6.3 existiert also auch hier eine Steinitzwurzel $\Delta_{E_1} \in C\ell_{E_1}$.

Wie im Beweis zu Hauptsatz 2 setzen wir die Idealklassen Δ_F und Δ_{E_1} zusammen und erhalten mit $\Delta_{E_1|K} = \iota_{E_1|F}(\Delta_F) \cdot \Delta_{E_1}$ die beiden Gleichungen

$$\begin{aligned} N_{E_1|K}(\Delta_{E_1|K}) &= N_{F|K}(\Delta_F)^{[E_1:F]} \cdot N_{F|K}\big(N_{E_1|F}(\Delta_{E_1})\big) = s_A(C)^{[F:K]} N_{F|K}(s_C(C_1)) = s_A(C_1), \\ \Delta^2_{E_1|K} &= \iota_{E_1|F}(\Delta_F)^2 \cdot \Delta^2_{E_1} = [\mathcal{D}_{E_1|F}\mathcal{D}_{F|K}] = [\mathcal{D}_{E_1|K}]. \end{aligned}$$

Die Idealklasse $\Delta_{E_1|K}$ ist also eine Steinitzwurzel für $E_1|K$.
Wir gehen induktiv weiter in dieser Weise vor. Sei hierfür $E_2|E_1$ eine quadratische Erweiterung von E_1, die nach Voraussetzung die Eigenschaft ($\diamondsuit$) erfüllt. Es existiert eine Steinitzwurzel für $E_2|E_1$ und für $E_1|K$, also auch für $E_2|K$. Induktiv erhalten wir die Existenz einer Steinitzwurzel für $L|K$. □

Wir wollen nun ein Beispiel studieren, in dem die Voraussetzungen von Hauptsatz 2 nicht gegeben sind. Eine Erweiterung von ungeradem Grad scheidet also aus. Hier wissen wir bereits nach 4.1, dass eine Galois-invariante Steinitzwurzel existiert.

In Kapitel 8 werden wir uns darüberhinaus mit einer ganz speziellen 2-Potenz-Erweiterung, der (kanonischen) zyklotomischen $\mathbb{Z}_2$-Erweiterung eines imaginär quadratischen Zahlkörpers, beschäftigen. Wir werden sehen, dass seine relativen Steinitzklassen Ordnung ≤ 2 haben und die (relativen) Diskriminanten und Differenten stets Hauptideale sind.

Als Abschluss dieses siebten Kapitels betrachten wir nun eine Erweiterung vom Grad 4: Sei K ein imaginär quadratischer Zahlkörper $K = \mathbb{Q}(\sqrt{-d})$, wobei d eine Primzahl kongruent 3 (*mod* 4) ist. Wir wählen die Primzahl d so, dass die Klassenzahl $h_K = 4$ und für die Idealklassengruppe $C\ell_K \cong Z_4$, also zyklisch vom Grad 4 ist. Dies ist etwa für die Primzahlen $d = 17, 73, 97$ der Fall.
In $K|\mathbb{Q}$ verzweigen die Zahlen 2 und d, da die (Absolut)Diskriminante $\delta = 4d$ ist. Das Primideal $\mathfrak{p}|d$ ist ein Hauptideal, wohingegen für $\mathfrak{q}|2$ mit einem einfachen Normargument folgt, dass $\mathfrak{q}$ kein Hauptideal sein kann. Die Idealklasse $[\mathfrak{q}]$ hat Ordnung 2 in $C\ell_K$.
Wir nehmen nun eine Primzahl p, die in $K|\mathbb{Q}$ zerfällt (davon gibt es unendlich viele), also

etwa $p = \mathfrak{p}_1\mathfrak{p}_2$. Durch Nachrechnen sehen wir, dass $[\mathfrak{p}_i]$ die Ordnung 4 in $C\ell_K$ hat und damit die Idealklassengruppe erzeugt. Es ist also $(\alpha) = \mathfrak{q}\mathfrak{p}_1^2$ ein Hauptideal.
Sei $L = K(\sqrt{\alpha})$. Zur Bestimmung der Steinitzklasse und der Diskriminante wenden wir 6.1 an:
Ist $\mathfrak{p}$ eine Primstelle, die weder (α) noch 2 teilt, so ist die (lokale) Diskriminante $\delta_\mathfrak{p} = 4\alpha \cdot {U_\mathfrak{p}}^2$ eine Einheit.
Für $\mathfrak{p}_1$ gilt ($\mathfrak{p}_1$ ist ein Teiler von α, aber nicht von 2) $\delta_{\mathfrak{p}_1} = 4\alpha\pi_{\mathfrak{p}_1}^{-2} \cdot U_{\mathfrak{p}_1}^2$, wobei $\pi_{\mathfrak{p}_1}$ das (lokale) Primideal $\mathfrak{p}A_\mathfrak{p}$ erzeugt. Diese Diskriminante ist eine lokale Einheit, also verzweigt $\mathfrak{p}_1$ in $L|K$ nicht.
Das Primideal $\mathfrak{q}$ teilt (α) und 2 und wir erhalten somit die lokale Diskriminante $\delta_\mathfrak{q} = 4\alpha\pi_\mathfrak{q}^0 \cdot U_\mathfrak{q}^2$.
In $L|K$ verzweigt also nur das Primideal $\mathfrak{q}$. Wir erfüllen damit die Voraussetzungen für 2.6, aber nicht die von Hauptsatz 2 (7.2). Hierzu müsste auch $\mathfrak{p}_1$ in $L|K$ verzweigen, da $\mathfrak{p}_1$ ein Primteiler von (α) ist. Nach 6.2 ergibt sich für die Steinitzklasse

$$s_A(B) = [\mathfrak{p}_1^{-1}] = [\mathfrak{p}_2] \text{ von Ordnung 4 in } C\ell_K.$$

Wegen $[\delta] = s_A(B)^2$ ist $[\delta] = [\mathfrak{p}_2^2] = [\mathfrak{q}]$ von Ordnung 2, und da nur $\mathfrak{q}$ in $L|K$ verzweigt, erhalten wir

$$\delta = \mathfrak{q}^{2k+1} \text{ mit } k \in \mathbb{N}.$$

Da $N_{L|K}(\mathcal{D}) = \delta_{L|K}$ ist, muss auch für die Differente gelten

$$\mathcal{D} = \mathfrak{Q}^{2k+1} \text{ für } \mathfrak{Q}|\mathfrak{q} \text{ in } L|K.$$

Weil die Diskriminante kein Hauptideal ist, kann auch die Differente kein Hauptideal sein. Es ist also die Ordnung der Differente ≥ 2 in $C\ell_L$ und da die Differente selbst ein Quadrat in $C\ell_L$ ist, folgt sofort $h_L \geq 4$.

Wir untersuchen nun die Ordnung der Differente $[\mathcal{D}] = [\mathcal{D}_{L|K}]$ in der Idealklassengruppe von L. Es ist $\mathfrak{q}B = \mathfrak{Q}^2$, da $\mathfrak{q}$ in L verzweigt. Wir haben also $N_{L|K}(\mathfrak{Q}^2) = N_{L|K}(\mathfrak{q}B) = N_{L|K} \circ \iota_{L|K}(\mathfrak{q}) = \mathfrak{q}^2 = (2)$. Existiert ein Element mit (relativer) Norm 2 bzw. Absolutnorm 4, so ist $\mathfrak{q}B = \mathfrak{Q}^2$ ein Hauptideal. Für die oben beschriebenen Körper $L = K(\sqrt{\alpha})$, mit $(\alpha) = \mathfrak{q}\mathfrak{p}_1^2$, suchen wir Elemente mit Absolutnorm 4. Dabei berechnen wir die Fälle $d = 17, 73, 97$ mit Primideal $\mathfrak{p}_1$ über einer in $K|\mathbb{Q}$ zerfallenden Primzahl $p = \mathfrak{p}_1 \cap \mathbb{Z} < 200$ mit dem Programmpaket KASH [KANT]. Es ergibt sich, dass in jedem Fall ein Element $\beta \in B$ mit (relativer) Norm 2 existiert. Das Ideal $\mathfrak{q}B = \mathfrak{Q}^2$ ist also ein Hauptideal in L. Somit gilt, dass die Idealklasse der Differente $[\mathcal{D}] = [\mathfrak{Q}^{2k+1}] = [\mathfrak{Q}]$ Ordnung 2 in $C\ell_K$ hat. Insbesondere folgt, dass die Einbettung $\iota_{L|K} : C\ell_K \to C\ell_L$ nicht injektiv ist, da das Element $[\mathfrak{q}]$ von Ordnung 2 in $C\ell_K$ in $C\ell_L$ trivial wird. In $C\ell_L$ existiert nach Hecke eine

Quadratwurzel Δ der Differente. Die Idealklasse Δ hat Ordnung 4 in $C\ell_L$.
Wir untersuchen, ob Δ eine Steinitzwurzel für $L|K$ ist. Es ist $\Delta^2 = [\mathcal{D}]$ und $N(\Delta)^2 = [\delta] = [\mathfrak{q}]$. In $C\ell_K$ ist $[\mathfrak{q}] = [\mathfrak{p}_1]^2 = [\mathfrak{p}_2]^2$. Die Idealklassen von $\mathfrak{p}_1$ und $\mathfrak{p}_2$ unterscheiden sich um ein Element der Ordnung 2, nämlich $[\mathfrak{q}]$. Es ergibt sich $N(\Delta) = [\mathfrak{p}_1]$ oder $N(\Delta) = [\mathfrak{p}_2]$. Ist $N(\Delta) = [\mathfrak{p}_2]$, so ist Δ eine Steinitzwurzel, da $[\mathfrak{p}_2] = s_A(B)$. Ist $N(\Delta) = [\mathfrak{p}_1]$, so betrachten wir die Idealklasse $\tilde{\Delta} = [\mathcal{D}^{-1}]\Delta$. Für $\tilde{\Delta}$ gilt

$$\begin{aligned} \tilde{\Delta}^2 &= [\mathcal{D}]^{-2} \cdot \Delta^2 = \Delta^2 = [\mathcal{D}] \text{ und} \\ N_{L|K}(\tilde{\Delta}) &= N_{L|K}([\mathcal{D}])^{-1} \cdot N_{L|K}(\Delta) = [\delta]^{-1}[\mathfrak{p}_1] = [\mathfrak{q}]^{-1}[\mathfrak{p}_1] = [\mathfrak{p}_2] = s_A(B). \end{aligned}$$

In diesem Fall ist also $\tilde{\Delta} = [\mathcal{D}]^{-1}\Delta$ eine Steinitzwurzel für $L|K$. Insgesamt haben wir somit folgendes gezeigt.

7.4 Beispiel. Sei K ein imaginär quadratischen Zahlkörper $K = \mathbb{Q}(\sqrt{-d})$, wobei $d = 17, 73, 97$ ist. Es ist dann $h_K = 4$. Sei $\mathfrak{q}$ das dyadische Primideal in K und $p = \mathfrak{p}_1 \cdot \mathfrak{p}_2$ die Zerlegung einer in $K|\mathbb{Q}$ (total) zerfallenden Primzahl $p < 200$. Dann ist $\mathfrak{q} \cdot \mathfrak{p}_1^2 \in H_K$. Wir setzen

$$(\alpha) = \mathfrak{q} \cdot \mathfrak{p}_1^2 \text{ und } L = K(\sqrt{\alpha}).$$

Dann gibt es eine Steinitzwurzel für $L|K$.

Kapitel 8

Iwasawa-Erweiterungen

In diesem Kapitel sei stets ζ_n eine primitive 2^{n+2}-te Einheitswurzel und ε_m eine primitive m-te Einheitswurzel.

Die Theorie der $\mathbb{Z}_p$-Erweiterungen ist etwa 40 Jahre alt und geht auf K. Iwasawa zurück. Eine $\mathbb{Z}_p$-Erweiterung eines Zahlkörpers K_0 ist eine Erweiterung $K_\infty|K_0$ mit Galoisgruppe $Gal(K_\infty|K_0) \cong \mathbb{Z}_p$, der additiven Gruppe der ganzen p-adischen Zahlen. Dies ist äquivalent zur Existenz eines Körperturms

$$K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_\infty = \bigcup K_n,$$

wobei

$$Gal(K_n|K_0) \cong \mathbb{Z}/p^n\mathbb{Z}$$

zyklisch vom Grad p^n ist. Nur Primideale über p verzweigen in diesem Körperturm.
K. Iwasawa hat diese Erweiterungen untersucht. Ein wesentliches Resultat [Iw] beschreibt den p-Anteil der Klassenzahl in einer $\mathbb{Z}_p$-Erweiterung. Ist p^{e_n} die maximale Potenz von p, die in h_{K_n} aufgeht, so gibt es ein n_0, dass $e_n = \mu p^n + \lambda n + t$ ist für alle $n \geq n_0$. Dabei sind μ und λ die sogenannten Iwasawa-Invarianten der $\mathbb{Z}_p$-Erweiterung und t eine Konstante. Ferrero und Washington konnten in [FW] zeigen, dass für die zyklotomische $\mathbb{Z}_p$-Erweiterung eines abelschen Zahlkörpers die Invariante μ stets $= 0$ ist.
Eine Einführung in diese Theorie findet man etwa in [Wa, §13].

Wir beschäftigen uns im Folgenden mit $p = 2$ und einem imaginär quadratischen Zahlkörper $K_0 = \mathbb{Q}(\sqrt{-d})$ mit Diskriminante $-d$. Wir studieren eine $\mathbb{Z}_2$-Erweiterung von K_0. Damit haben wir in jedem Schritt eine Erweiterung vom Grad 2, die wir mit den Methoden aus Kapitel 6 untersuchen können.
Nach [Wa, Thm. 13.4] gibt es genau $r_2 + 1$ nicht-äquivalente $\mathbb{Z}_2$-Erweiterungen von K_0, in unserem Fall also zwei Stück ("Leopoldt-Vermutung"). Von diesen beiden ist eigentlich nur eine studiert, die zyklotomische $\mathbb{Z}_2$-Erweiterung $K_\infty|K_0$. Es wäre interessant zu wissen,

ob für die (weitgehend unbekannte) zweite $\mathbb{Z}_2$-Erweiterung von K_0 ähnliche Gesetzmäßigkeiten gelten, wie die, die wir im Folgenden darstellen werden.

8.1 Definition. Sei $B_n = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ der maximal reelle Teilkörper des 2^{n+2}-ten Kreisteilungskörpers. Die zyklotomische $\mathbb{Z}_2$-Erweiterung von K_0 ist gegeben durch

$$K_n = K_0 \cdot B_n.$$

Anmerkung. Bekanntlich ist $\mathbb{Z}[\zeta_n+\zeta_n^{-1}]$ der Ring der ganzen Zahlen von B_n. Es existiert also eine ganze Potenzbasis für $B_n|\mathbb{Q}$ und damit auch für die relativen Erweiterungen $B_m|B_n$, $m \geq n \geq 0$. Die absoluten Diskriminanten der B_n sind stets 2-Potenzen, da nur die Primzahl 2 verzweigt.

Für unsere Überlegungen benötigen wir die beiden folgenden Sätze:

8.2 Satz. [We]

(i) Die Klassenzahl h_{B_n} von B_n ist ungerade. [We, II,9]

(ii) Jede total positive Einheit u in B_n (d.h. u^σ positiv für alle $\mathbb{Q}$-Einbettungen σ von B_n) ist ein Quadrat (in U_{B_n}). [We, II,6]

Anmerkung. Da die Klassenzahl von B_n ungerade ist, wissen wir nach 1.21, dass in jeder algebraischen Körpererweiterung $L|B_n$ eine Steinitzwurzel existiert.
Desweiteren gilt für jede Erweiterung $B_m|B_n$, $m > n \geq 0$ die Eigenschaft ($\diamondsuit$) aus dem vorangegangenen Kapitel.

8.3 Satz. [Ha2, Sätze 6 und 25] *Sei L eine imaginär quadratische Erweiterung von B_n, $n \geq 0$, und sei L abelsch über $\mathbb{Q}$. Dann ist jede Einheit von L darstellbar als Produkt einer Einheit in B_n und einer Einheitswurzel in L. Sind insbesondere in L nur die Einheitswurzeln ± 1 enthalten, so ist $U_L = U_{B_n}$.*

8.4 Lemma. *Sei ε_m eine m-te Einheitswurzel, p eine Primzahl. Für $r \geq 1$ gilt $\mathbb{Q}(\varepsilon_{p^r}, \varepsilon_{p^{r+1}} + \varepsilon_{p^{r+1}}^{-1}) = \mathbb{Q}(\varepsilon_{p^{r+1}})$.*

Beweis. Offensichtlich gilt ε_{p^r} und $\varepsilon_{p^{r+1}} + \varepsilon_{p^{r+1}}^{-1} \in \mathbb{Q}(\varepsilon_{p^{r+1}})$, also $\mathbb{Q}(\varepsilon_{p^r}, \varepsilon_{p^{r+1}} + \varepsilon_{p^{r+1}}^{-1}) \subseteq \mathbb{Q}(\varepsilon_{p^{r+1}})$. Weiterhin ist $[\mathbb{Q}(\varepsilon_{p^{r+1}}) : \mathbb{Q}(\varepsilon_p^r)] = p$ und $[\mathbb{Q}(\varepsilon_{p^r}, \varepsilon_{p^{r+1}} + \varepsilon_{p^{r+1}}^{-1}) : \mathbb{Q}(\varepsilon_{p^r})] > 1$, woraus die Behauptung folgt. □

Sei nun $d = 4$, also $K_0 = \mathbb{Q}(\sqrt{-4}) = \mathbb{Q}(i) = \mathbb{Q}(\zeta_0)$. Mit obigem Lemma ($p = 2$) erhalten wir, dass $K_1 = \mathbb{Q}(\zeta_0)$ und für alle $n \in \mathbb{N}$ der Körper $K_n = \mathbb{Q}(\zeta_n)$, also der 2^{n+2}-te Kreisteilungskörper ist. Dieser besitzt immer eine ganze Potenzbasis.

Dasselbe gilt für $d = 8$. Hier haben wir $K_0 = \mathbb{Q}(\sqrt{-2})$. Dieser Körper ist aber neben B_1 und $\mathbb{Q}(i)$ der dritte quadratische Teilkörper in $K_1|\mathbb{Q}$ und es ist $K_1 = K_0 \cdot B_1 = \mathbb{Q}(i) \cdot B_1 = \mathbb{Q}(\zeta_1)$. Wie im Fall $d = 4$ ist somit $K_n = \mathbb{Q}(\zeta_n)$.

Wir betrachten $K = K_n$ und $L = K_m$ für natürliche Zahlen $0 \leq n < m$. Die Ringe ganzer Zahlen in K, L bezeichnen wir mit $A = A_n$, $B = A_m$, Primideale mit $\mathfrak{p} = \mathfrak{p}_n$ und $\mathfrak{P} = \mathfrak{p}_m$. Man beachte, dass $K_0 = \mathbb{Q}(\sqrt{-d})$ mit Diskriminante $-d$ ist.

8.5 Lemma. *Ist d ungerade (also 2 unverzweigt), so ist die Steinitzklasse $s_A(B)$ von $L|K$ trivial. Es existiert sogar eine ganze Potenzbasis für $L|K$.*

Beweis. Die Diskriminaten von K_0 und B_n sind teilerfremd, damit ist die ganze Potenzbasis von $B_n|\mathbb{Q}$ auch eine Ganzheitsbasis (bzw. ganze Potenzbasis) für $K_n|K_0$. Also besitzen auch die relativen Erweiterungen $L|K$ eine ganze Potenzbasis und die jeweiligen (relativen) Steinitzklassen sind trivial. □

Im Folgenden sei $-d = 2^* q_1^* \cdots q_r^*$ (< 0 und $r > 0$) gerade mit Primdiskriminanten $q_i^* = (-1)^{(q_i-1)/2} q_i$ für ungerade Primzahlen q_i (also stets $q_i^* \equiv 1 \ (mod\ 4)$) und $2^* = -4$ oder ± 8. Wir setzen $q^* = q_1^* \cdots q_r^*$.

8.6 Lemma. *Sei $2^* = 8$. Dann hat die Steinitzklasse $s_{A_0}(A_1)$ Ordnung 2, und für alle anderen Fälle $(n, m) \neq (0, 1)$ gilt $s_A(B) = 1$.*

Beweis. Wir setzen $K_0' = \mathbb{Q}(\sqrt{q_1^* \cdots q_r^*}) = \mathbb{Q}(\sqrt{q^*})$, den neben B_1 und K_0 weiteren quadratischen Teilkörper von $K_1|\mathbb{Q}$. K_0' hat ungerade Diskriminante. Es ist also $K_1 = K_0 \cdot B_1 = K_0' \cdot B_1$, damit haben wir ab K_1 denselben Körperturm wie in der Situation von 8.5, also triviale Steinitzklassen $s_{A_n}(A_m)$ für $0 < n \leq m$. Wir müssen nur noch den Fall $n = 0$ untersuchen. Sei also $K = K_0$ und zunächst $m = 1$, also $L = K_1$. In K_0' ist 2 unverzweigt (ungerade Diskriminante), in B_1 und K_0 verzweigt. Darum verzweigt 2 in $L|\mathbb{Q}$ mit Verzweigungsindex $e(\mathfrak{p}_1|2) = 2$. Die Erweiterungen $K_1|B_1$ bzw. $K_1|K_0$ sind deshalb unverzweigt über 2. $K_1|K_0$ ist sogar überall unverzweigt, da die ungeraden Primzahlen schon in K_0 verzweigen, aber nicht in B_1.
In $K = K_0$ gilt also $2A = \mathfrak{p}^2$. Da in A kein Element mit Norm 2 existiert, ist $\mathfrak{p}$ kein Hauptideal, hat also Ordnung 2. Sei nun $\pi_\mathfrak{p}$ ein Element aus K mit Ordnung 1 bei $\mathfrak{p}$. Da $\mathfrak{p}$ in $L|K$ unverzweigt ist, existiert nach 2.5 ein Element $x \in K$ mit $x^2 \equiv 2{\pi_\mathfrak{p}}^{-2} \ (mod\ 4)$ $(4A = \mathfrak{p}^4)$. Es ist also $x^2 \in U_\mathfrak{p} + \mathfrak{p}^4 \in A_\mathfrak{p}$ und folglich $x \in A_\mathfrak{p}$, da A ganz abgeschlossen ist. Da $L = K(\sqrt{2})(= K(\sqrt{2{\pi_\mathfrak{p}}^{-2}}))$ ist, gilt nach 2.5 und 6.2, dass $s_A(B) = [\mathfrak{p}^{-1-2}] = [\mathfrak{p}^{-1}] = [\mathfrak{p}]$ ist und wie $\mathfrak{p}$ Ordnung 2 hat.
Für $n = 0$ und $m > 1$ bemühen wir 2.2. Damit erhalten wir

$$s_A(B) = s_A(A_1)^{[L:K_1]} \cdot N_{K_1|K}(s_{A_1}(B)) = [\mathfrak{p}]^{2^{m-1}} \cdot 1 = 1 \text{ in } C\ell_K.$$

□

Haben wir $2^* = -4, -8$, so verzweigt die 2 total in $K_1|\mathbb{Q}$. Der Körperturm oberhalb von K_1 ist also nicht mit dem aus 8.5 identisch, wie es im Fall $2^* = 8$ gewesen war.
Die Bestimmung der (relativen) Steinitzklassen $s_{A_n}(A_n)$ teilen wir auf. Zunächst behandeln wir den ersten Schritt der zyklotomischen Erweiterung, also $K_1|K_0$, bevor wir die übrigen Erweiterungen $K_m|K_n$ betrachten.

8.7 Lemma. *Sei $L = K_1$, $K = K_0$. Ist $2^* = -8$, so ist $s_A(B) = 1$. Ist $2^* = -4$, dann ist $s_A(B) = [\mathfrak{p}]$ mit $\mathfrak{p}|2$ von Ordnung 2.*

Beweis. Ist $2^* = -8$, so ist $K = K_0 = \mathbb{Q}(\sqrt{-2q_1^* \cdots q_r^*})$ und der neben B_1 und K_0 quadratische Teilkörper in L ist $K_0'' = \mathbb{Q}(\sqrt{-q_1^* \cdots q_r^*})$ (der Körper mit 2-Anteil der Diskriminante $2^* = -4$). Damit sind ab K_1 die Körpertürme für $2^* = -4$ bzw. -8 identisch. Sei nun $\pi_\mathfrak{p} = \sqrt{-2q_1^* \cdots q_r^*}$, also $\pi_\mathfrak{p}$ ein Element mit Ordnung 1 bei $\mathfrak{p}$. Da in allen drei Körpern B_1, K_0, K_0'' die 2 (über $\mathbb{Q}$) verzweigt, verzweigt sie in $L|\mathbb{Q}$ total (sonst gäbe es einen maximal unverzweigten Zwischenkörper), d.h. insbesondere in $L|K$. Deshalb ist nach 2.5 die Kongruenz $X^2 \equiv 2{\pi_\mathfrak{p}}^{-2}$ $(mod\ 4)$ nicht lösbar in K bzw. $A_\mathfrak{p}$.
Da $2{\pi_\mathfrak{p}}^{-2} = -(q_1^* \cdots q_r^*)^{-1} \equiv -1$ $(mod\ 4)$ ist auch $2{\pi_\mathfrak{p}}^{-2} \equiv 1$ $(mod\ 2)$, und deshalb $X^2 \equiv 2{\pi_\mathfrak{p}}^{-2}$ $(mod\ \mathfrak{p}^2)$ lösbar. Nach 6.2 ist also $\mathfrak{p}^{-1-1} \in s_A(B)$, also $s_A(B)$ trivial.

Für $2^* = -4$ ist $K = K_0'' = \mathbb{Q}(\sqrt{q^*})$ wie oben. Es ist $q^* \equiv 1$ $(mod\ 4)$ und damit $(1+\sqrt{-q^*})(1-\sqrt{-q^*}) = 1 + q^* \equiv 2$ $(mod\ 4)$. Für $\mathfrak{p}|2$ gilt dann $v_\mathfrak{p}(1+q^*) = 2$. Wäre $\mathfrak{p}^2$ ein Teiler von $1+\sqrt{-q^*}$, so wäre auch $\mathfrak{p}^2 = (\mathfrak{p}^\sigma)^2$ ein Teiler von $(1+\sqrt{-q^*})^\sigma = 1-\sqrt{-q^*}$. Folglich müsste $4 = \mathfrak{p}^4$ ein Teiler von $1+q^*$ sein, was zum Widerspruch führt. Also ist $1+\sqrt{-q^*}$ ein Element mit Ordnung 1 bei $\mathfrak{p}$ und wir setzen $\pi_\mathfrak{p} = 1+\sqrt{-q^*}$. Da in $L|K_0''$ $\mathfrak{p}|2$ verzweigt, ist die Kongruenz $X^2 \equiv 2{\pi_\mathfrak{p}}^{-2}$ $(mod\ 4)$ wieder unlösbar in K bzw. $A_\mathfrak{p}$. Nun gilt

$$(2{\pi_\mathfrak{p}}^{-2}) = \frac{{\pi_\mathfrak{p}}^2}{2} = \frac{1}{2}\big(1 - q^* + 2\sqrt{-q^*}\big) \equiv \sqrt{-q^*}\ (mod\ 2),\ \text{da } 1 - q^* \equiv 0\ (mod\ 2).$$

Es ist $\sqrt{-q^*} \in U_\mathfrak{p}$ für $\mathfrak{p}|2$. Weil $U_\mathfrak{p}/{U_\mathfrak{p}}^{(1)} \cong k_\mathfrak{p}^* = \mathbb{F}_2^* = 1$ gilt ($\mathfrak{p}|2$ hat den Trägheitsindex 2), ist $\sqrt{-q^*} \in U_\mathfrak{p} = {U_\mathfrak{p}}^{(1)} = 1 + \mathfrak{p}A_\mathfrak{p}$.
Für jedes $u = 1 + \pi_\mathfrak{p} z \in {U_\mathfrak{p}}^{(1)}$, $z \in A_\mathfrak{p}$, gilt $u^2 \in {U_\mathfrak{p}}^{(2)}$, denn es ist

$$u^2 = 1 + {\pi_\mathfrak{p}}^2 z^2 + 2\pi_\mathfrak{p} z = 1 + {\pi_\mathfrak{p}}^2 z^2 + {\pi_\mathfrak{p}}^2 v \pi_\mathfrak{p} z \quad \in 1 + \mathfrak{p}^2 A_\mathfrak{p} = {U_\mathfrak{p}}^{(2)},$$

mit $v = 2{\pi_\mathfrak{p}}^{-2} \in U_\mathfrak{p}$. Ist also u kein Element von ${U_\mathfrak{p}}^{(2)}$, so ist es auch kein Quadrat in $A_\mathfrak{p}$. Wir nehmen an, dass $\sqrt{-q^*} = y^2$ ein Quadrat in $A_\mathfrak{p}$ ist. Dann gilt $\sqrt{-q^*} = \pi_\mathfrak{p} - 1 \in 1 + \mathfrak{p}A_\mathfrak{p}$, also $\pi_\mathfrak{p} - 1 - 1 = \pi_\mathfrak{p} - 2 \in \mathfrak{p}^2 A_\mathfrak{p}$. Dies liefert den Widerspruch, da $2 \in \mathfrak{p}^2 A_\mathfrak{p}$, aber $\pi_\mathfrak{p} \notin \mathfrak{p}^2 A_\mathfrak{p}$. Damit ist $\sqrt{-q^*}$ kein Quadrat mod $2A_\mathfrak{p}$ und somit auch die Kongruenz

$X^2 \equiv 2\pi_{\mathfrak{p}}^{-2}$ $(mod\ 2)$ unlösbar. Deshalb ist nach 6.2 die Steinitzklasse $s_A(B) = [\mathfrak{p}]$. Sie hat Ordnung 2 in $C\ell_K$, da das Primideal $\mathfrak{p}|2$ kein Hauptideal ist (Normargument). □

Anmerkung. Aus dem Beweis entnehmen wir, dass für $2^* = -4, -8$ die Körpertürme ab K_1 identisch sind.

8.8 Lemma. (Vgl. [Fe, Thm. 5]). *Sei $2^* = -4$ oder -8, $K = K_n$, $L = K_m$, $0 \leq n < m$. Das Primideal $\mathfrak{p}|2$ ist das einzige Primideal von K, das in L verzweigt und es verzweigt total.*

Beweis. Bekanntlich verzweigt in $B_m|B_n$ nur die 2 und das total. Wir zeigen zunächst, dass in $K_m|K_n$ kein q_i verzweigt.
Wir wissen, dass $K_m = B_m K_0$ mit $[K_m : \mathbb{Q}] = 2^{m+1}$ ist und in $K_m|\mathbb{Q}$ die Primzahlen 2 und q_i $(i = 1, \ldots, r)$ verzweigen. Wir nehmen an, dass der Verzweigungsindex $e(\mathfrak{q}_i|q_i) > 2$ ist für ein Primideal $\mathfrak{q}_i$ in K_m, also etwa $e(\mathfrak{q}_i|q_i) = 2^l$, $l > 1$. Es muss also eine Teilerweiterung $F_{\mathfrak{q}_i}|\mathbb{Q}$ vom Grad 2^{m+1-l} geben, die maximal unverzweigt bei q_i ist. Insbesondere ist der Grad $[F_{\mathfrak{q}_i} : \mathbb{Q}] \leq 2^{m-1}$. Dies liefert aber den Widerspruch, denn in $B_m|\mathbb{Q}$ ist q_i unverzweigt, d.h. $B_m \subseteq F_{\mathfrak{q}_i}$. Dies ist aus Dimensionsgründen nicht möglich. Damit haben wir für alle q_i den Verzweigungsindex $e(\mathfrak{q}_i|q_i) = 2$. Die Verzweigung findet statt in K_0 bzw. K_0'. Deshalb ist q_i unverzweigt in $K_m|K_0$ bzw. $K_m|K_0'$ und somit in jeder Teilerweiterung $K_m|K_n$. Es bleibt noch zu zeigen, dass die 2 in $K_m|K_n$ stets verzweigt.
Wir wissen, dass 2 in $B_m|\mathbb{Q}$ mit Index 2^m und in K_1 mit Index 4 verzweigt. Wir nehmen an, dass 2 in K_m nicht total verzweigt, also den Verzweigungsindex 2^m hat. Dann existiert eine maximal unverzweigte Teilerweiterung $F_{\mathfrak{p}}$ in $K_m|\mathbb{Q}$ mit $[K_m : F_{\mathfrak{p}}] = 2^m$ und $[F_{\mathfrak{p}} : \mathbb{Q}] = 2$. Aber in jeder (der drei) quadratischen Teilerweiterungen von $K_m|\mathbb{Q}$ verzweigt die 2. Daher ist 2 total verzweigt in $K_m|\mathbb{Q}$ und somit in jeder Teilerweiterung $K_m|K_n$. □

8.9 Satz. *Sei $2^* = -4$ und $K = K_n$, $L = K_m$, $A = A_n$, $B = A_m$, $(q^* \neq 1)$. Dann hat $s_A(B) = [\mathfrak{p}]$ die Ordnung 2 mit $\mathfrak{p} = \mathfrak{p}_n|2$ in $K = K_n$ für alle $0 \leq n < m$.*

Beweis. Nach dem Beweis von 8.7 wissen wir, dass in $K_1|K_0$ nur die 2 verzweigt und nach 8.8, dass auch in allen Erweiterungen $L|K$ nur die dyadischen Primideale verzweigen (sogar total). Sei zunächst $m = n + 1$. Der Fall $n = 0$ ist nach 8.7 erledigt.
Wir setzen $\pi_n = (1 - \zeta_n)(1 - \zeta_n^{-1})$. Das von π_n erzeugte Ideal (π_n) ist ein Primideal und bekanntlich in B_n das einzige über der Primzahl 2, da die 2 in B_n total verzweigt mit Verzweigungsindex $2^n = \varphi(2^{n+2})/2$. Nach 8.8 verzweigt auch (π_n) in K, also etwa $\pi_n A = \mathfrak{p}^2$ (damit hat $\mathfrak{p}$ Ordnung 2 in $C\ell_K$) und $\mathfrak{p}$ verzweigt auch in L. Es gilt $L = K_{n+1} = K(\zeta_{n+1} + \zeta_{n+1}^{-1})$. Für π_n haben wir $\pi_n = 2 - \zeta_n - \zeta_n^{-1}$. Es folgt

$$(\zeta_{n+1} + \zeta_{n+1}^{-1})^2 = 2 + \zeta_n + \zeta_n^{-1} = 4 - \pi_n \text{ und damit } L = K(\sqrt{4 - \pi_n}).$$

Für eine Einbettung σ gilt $\pi_n^\sigma = (1-\zeta_n^\sigma)(1-(\zeta_n^\sigma)^{-1}) = 2-2Re(\zeta_n^\sigma) \geq 0$. Es ist also π_n total positiv und weiterhin $\pi_n(4\pi_n^{-1}-1) = 4-\pi_n = (\zeta_{n+1}+\zeta_{n+1}^{-1})$. Da $(\zeta_{n+1}+\zeta_{n+1}^{-1})^2$ ganz offensichtlich total positiv ist, ist es auch $w = 4\pi_n^{-1}-1$. Wir zeigen im Folgenden, dass w eine Einheit in B_n ist.
Es ist $v_{(\pi_n)}(4-\pi_n) = 1$, also auch $v_{(\pi_n)}(w) = v_{(\pi_n)}(\frac{4-\pi_n}{\pi_n}) = 0$. Wir müssen noch zeigen, dass für alle Primideale $\mathfrak{q} \neq (\pi_n)$ ebenfalls $v_\mathfrak{q}(w) = 0$ gilt. Da $w = \frac{4-\pi_n}{\pi_n} = \frac{(\zeta_{n+1}+\zeta_{n+1}^{-1})^2}{\pi_n}$ist, bleibt zu zeigen, dass $v_\mathfrak{q}((\zeta_{n+1}+\zeta_{n+1}^{-1})^2) = 0$ gilt. Wir nehmen an, dass $(\zeta_{n+1}+\zeta_{n+1}^{-1})^2 = 2+\zeta_n+\zeta_n^{-1}$ in $\mathfrak{q}$ ($\not/2$) enthalten ist. Damit liegen auch

$$(2+\zeta_n+\zeta_n^{-1})\cdot(2-(\zeta_n+\zeta_n^{-1})) = 4-(\zeta_n+\zeta_n^{-1})^2 = 4-(2+\zeta_{n-1}+\zeta_{n-1}^{-1}) = 2-(\zeta_{n-1}+\zeta_{n-1}^{-1})$$

sowie $(2-(\zeta_{n-1}+\zeta_{n-1}^{-1}))\cdot(2+(\zeta_{n-1}+\zeta_{n-1}^{-1})) = (2-(\zeta_{n-2}+\zeta_{n-2}^{-1}))$ im Ideal $\mathfrak{q}$. Induktiv folgt, dass auch $2-(\zeta_0+\zeta_0^{-1}) = 2$ in $\mathfrak{q}$ liegen muss, was den Widerspruch liefert. Damit ist w eine total positive Einheit in B_n. Nach dem Satz von Weber 8.2 ist $w = 4\pi_n^{-1}-1$ ein Quadrat in U_{B_n}. Wir haben also

$$B_{n+1} = B_n(\zeta_{n+1}+\zeta_{n+1}^{-1}) = B_n(\sqrt{w\pi_n}) = B_n(\sqrt{\pi_n}),$$

und damit insbesondere $L = K(\sqrt{\pi_n})$. In K ist $\pi_n A = \mathfrak{p}^2$ und $[\mathfrak{p}]$ hat Ordnung 2 in $C\ell_K$. Nach 6.2 ist die Steinitzklasse $s_A(B) = [\mathfrak{p}]$ oder trivial. Wegen $[\delta] = s_A(B)^2$ ist die Diskriminante in beiden Fällen ein Hauptideal. Laut 8.8 verzweigt nur das (dyadische) Primideal $\mathfrak{p}$ in L, daher kommt für die Diskriminante nur die Form $\delta = \mathfrak{p}^l$ ($l \in \mathbb{N}$ geeignet) in Frage. Wäre $\delta = \mathfrak{p}^{2k+1}$ ($k \in \mathbb{N}$), so wäre $[\delta] = [\mathfrak{p}]^{2k+1} = [\mathfrak{p}] \neq 1$, also kein Hauptideal. Folglich ist

$$\delta = \mathfrak{p}^{2r} = (\pi_n A)^r.$$

Ist $s_A(B)$ trivial, so existiert nach 1.14 ein Element $u \in U_K$ und ein $c \in A$ mit

$$4\pi_n = \delta(m_{\pi_n}) = \delta u c^2 = \pi_n^r u c^2.$$

Nach Hasse 8.3 gilt $U_K = U_{B_n} \cdot \mathcal{E}_K$, wobei $\mathcal{E}_K$ die Gruppe der Einheitswurzeln in K bezeichnet.
Wir nehmen an, dass $\mathcal{E}_K \neq \{\pm 1\}$ ist. Dann enthält K (aus Dimensionsgründen) die vierten oder p-ten Einheitswurzeln, wobei p eine Fermatsche Primzahl ist. Im ersten Fall wäre $\mathbb{Q}(i) \subseteq K$. Da die (einzigen) quadratischen Teilkörper aber B_1, K_0, und K_0'' alle ungleich $\mathbb{Q}(i)$ sind, kann dies nicht sein. Ist $p = 3$, so müsste ein Teilkörper $F = \mathbb{Q}(\sqrt{-3})$ von K existieren; für die anderen Fermatschen Primzahlen p ein Teilkörper $F = \mathbb{Q}(\sqrt{p})$. Auch dies ist unmöglich, da $K_0 = \mathbb{Q}(\sqrt{-q^*})$ ist mit $-q^* \equiv 3 \ (mod\ 4)$ und $-3, p \equiv 1 \ (mod\ 4)$. Dass $F \neq B_1, K_0''$ ist klar.
Es gibt in K also nur die trivialen Einheitswurzeln und damit ist $U_K = U_{B_n}$, also $u \in U_{B_n}$.

Da π_n total positiv ist, ist es auch u und damit u ein Quadrat in U_{B_n}. Weil $v_{(\pi_n)}(4\pi_n) = 2v_{(\pi_n)}(2) + 1$ und $v_{(\pi_n)}(\pi_n^r uc^2) = 2v_{(\pi_n)}(c) + r$ ist, muss r ungerade sein. Ist r gerade, so folgt umgekehrt $s_A(B) \neq 1$.
Wir zeigen nun, dass r gerade ist, die Steinitzklasse also wie behauptet Ordnung 2 hat.
In K verzweigt die 2 total; wir setzen $e = v_{\mathfrak{p}}(2) = 2^{n+1}$. Das Ideal $\mathfrak{p}$ verzweigt allerdings wild und nur $\mathfrak{p}$ verzweigt in $L|K$. Nach [Neu, III.2.6] gilt dann für die Differente und $\mathfrak{P}|\mathfrak{p}$ in L

$$\mathcal{D} = \mathfrak{P}^s \qquad \text{mit } 2 \leq s \leq 1 + e_{\mathfrak{P}}(2) = 1 + 2e.$$

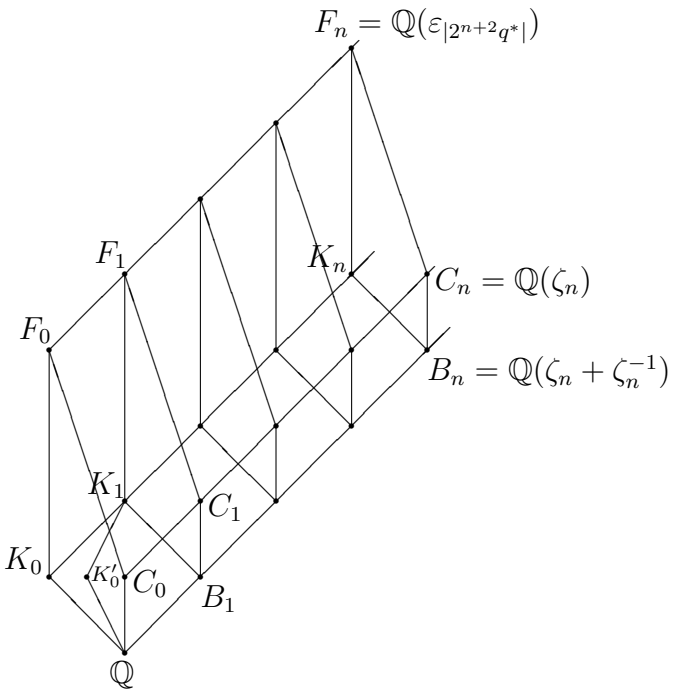
Da $\mathfrak{p}$ total verzweigt, ist $N_{L|K}(\mathfrak{P}) = \mathfrak{p}$. Wegen $N_{L|K}(\mathcal{D}) = \delta$ erhalten wir $s = 2r$, also

$$2 \leq 2r \leq 1 + 2e \qquad \text{bzw.} \qquad 1 \leq r \leq \frac{1}{2} + e, \qquad \text{also} \qquad r \leq e.$$

Den Zugang zur relativen Diskriminante δ schaffen wir uns über die Absolut-Diskriminanten δ_L und δ_K von L bzw. K. Da L und K abelsche Körper sind, lassen sich ihre absoluten Diskriminanten mit der Diskriminanten-Führer-Formel in 2.8 berechnen. Weil in $L|K$ sowieso nur die dyadische Primstelle verzweigt, interessiert uns nur der 2-Anteil $\delta^{(2)}$ der absoluten Diskriminante.
Nach Voraussetzung ist $\delta_{K_0} = 4 = 2^{2^1 \cdot 1}$ und induktiv sei

$$\delta_K^{(2)} = \delta_{K_n}^{(2)} = 2^{2^{n+1}(n+1)}.$$

Sei F_n der kleinste Kreisteilungskörper, der K_n enthält, also $F_n = \mathbb{Q}(\varepsilon_{t_n})$ mit $t_n = 2^{n+2}q^*$. Der 2-Führer von $K = K_n$ bzw. $L = K_{n+1}$ ist also 2^{n+2} bzw. 2^{n+3}.
(Im nebenstehenden Verbandsdiagramm ist C_n der 2^{n+2}-te Kreisteilungskörper, dessen maximal reeller Teilkörper B_n ist. Klein eingezeichnet ist K_0', der dritte quadratische Zahlkörper neben K_0 und B_1.)



Da $K \subseteq L$, gilt auch für die Charaktergruppen $X_K \subseteq X_L$. In X_L gibt es $2^{n+2} = [L : \mathbb{Q}]$ Charaktere. Die Hälfte davon sind auch Charaktere in X_K, es liegen also in $X_L \setminus X_K$

genau 2^{n+1} Charaktere mit 2-Führer $f_\chi^{(2)} = 2^{n+3}$. Folglich gilt nach der Diskriminanten-Führer-Formel

$$\begin{aligned}\delta_{K_{n+1}}^{(2)} &= \prod_{\chi\in X_{K_{n+1}}} f_\chi^{(2)} = \prod_{\chi\in X_{K_n}} f_\chi^{(2)} \prod_{\chi\in X_{K_{n+1}}\setminus X_{K_n}} f_\chi^{(2)} \\ &= \delta_{K_n}^{(2)} \prod_{\chi\in X_{K_{n+1}}\setminus X_K} f_\chi^{(2)} = \delta_{K_n}(2^{n+3})^{2^{n+1}}.\end{aligned}$$

Nach Induktionsvoraussetzung ist $\delta_{K_n}^{(2)} = 2^{2^{n+1}(n+1)}$, also ist

$$\delta_{K_{n+1}} = 2^{2^{n+1}(n+1)} \cdot 2^{2^{n+1}(n+3)} = 2^{2^{n+1}2(n+2)} = 2^{2^{n+2}(n+2)}$$

und die Formel für $\delta_{K_n}^{(2)}$ bewiesen. Mit Hilfe der Formel für Diskriminanten aus 2.1 können wir nun die Diskriminante von $L|K$ bestimmen. Für ihre Norm gilt

$$N_{K|\mathbb{Q}}(\delta) = \frac{\delta_L}{\delta_K^2} = \frac{\delta_L^{(2)}}{(\delta_K^{(2)})^2} = 2^{2^{n+2}(n+2)-2^{n+2}(n+1)} = 2^{2^{n+2}}.$$

Da 2 in K total verzweigt, ist $N_{K|\mathbb{Q}}(\mathfrak{p}) = 2$. Wegen $2A = \mathfrak{p}^{2^{n+1}}$ ist also $\delta = \mathfrak{p}^{2^{n+2}} = 4A$. Wir haben gezeigt, dass r gerade ist und deshalb die Steinitzklasse $s_A(B)$ nicht trivial sein kann. Es ist $s_A(B) = [\mathfrak{p}]$ (und damit die Kongruenz $X^2 \equiv \pi_n\pi_\mathfrak{p}{}^{-2}$ auch $(mod\ \mathfrak{p}^2)$ nicht lösbar). Für $m = n+1$ ist unser Satz bewiesen.

Ist $1 \le n = m + l$ $(l > 1)$ so folgt zunächst mit 2.2

$$s_{A_n}(A_m) = s_{A_n}(A_{n+1})^{2^{m-(n+1)}} N_{K_{n+1}|K_n}(s_{A_{n+1}}(A_m)).$$

Da $m > n+1$ ist und $s_{A_n}(A_{n+1})$ Ordnung 2 hat, ist der erste Faktor trivial. Wir wenden für $s_{A_{n+1}}(A_m)$ wiederholt 2.2 an. Nach dem l-ten Mal $(m = n+l)$ erhalten wir

$$s_{A_n}(A_m) = N_{K_{m-1}|K_n}\Big(s_{A_{m-1}}(A_m) N_{K_m|K_{m-1}}\big(s_{A_m}(A_m)\big)\Big).$$

Offensichtlich ist $s_{A_m}(A_m)$ trivial. Die Klasse $s_{A_{m-1}}(A_m) = [\mathfrak{p}_{m-1}]$ ist von Ordnung 2 nach dem bisher Bewiesenen. Da $\mathfrak{p}_{m-1}$ total verzweigt ist (8.8), gilt $s_{A_n}(A_m) = N_{K_{m-1}|K_n}\big([\mathfrak{p}_{m-1}]\big) = [\mathfrak{p}_n]$ mit Ordnung 2. □

Zusammenfassend haben wir also für $2^* = -4$ und für alle $0 \le n < m$

$$s_{A_n}(A_m) = [\mathfrak{p}_n] \text{ von Ordnung 2 in } C\ell_{K_n}.$$

Der Körperturm für $2^* = -8$ stimmt ab K_1 mit dem von $2^* = -4$ überein, damit gilt diese Aussage für alle $0 < n < m$ auch im Falle $2^* = -8$. Ist $n = 0$ und $m = 1$, so liefert 8.7 eine triviale Steinitzklasse. Es bleibt für $2^* = -8$ noch der Fall $n = 0$ und $m > 1$ zu untersuchen.

8.10 Lemma. *Ist $2^* = -8$, $n = 0$ und $m > 1$, so gilt $s_{A_0}(A_m) = [\mathfrak{p}_0]$ von Ordnung 2.*

Beweis. Es ist

$$s_{A_0}(A_m) = N_{K_1|K_0}(s_{A_1}(A_m)) \cdot s_{A_0}(A_1)^{[K_m:K_1]} = N_{K_1|K_0}([\mathfrak{p}_1]) = [\mathfrak{p}_0],$$

und $\mathfrak{p}_0$ hat Ordung 2 in $C\ell_{K_0}$. □

Wir erhalten also das Hauptresultat dieses Kapitels.

8.11 Hauptsatz 3. *Sei $K_\infty = \bigcup_{n\in\mathbb{N}} K_n$ die zyklotomische $\mathbb{Z}_2$-Erweiterung eines (imaginär) quadratischen Zahlkörpers K_0. Die Steinitzklasse jeder Teilerweiterung $K_m|K_n$ hat Ordnung 1 oder 2. Genauer:*
Ist die Primzahl 2 in K_0 unverzweigt, oder $K_0 = \mathbb{Q}(\sqrt{-1})$ oder $\mathbb{Q}(\sqrt{-2})$, so existiert für jede Teilerweiterung $K_m|K_n$, $n \le m$ eine ganze Potenzbasis.
Verzweigt die 2 in $K_1|\mathbb{Q}$ mit Verzweigungsindex 2, so existiert für die Teilerweiterungen $K_m|K_n$ für $(n,m) \neq (0,1)$ jeweils eine Ganzheitsbasis und im Falle $(n,m) = (0,1)$ hat die Steinitzklasse Ordnung 2, wenn $\delta_{K_0}^{(2)} = 2^3$ ist.
Verzweigt die 2 in $K_1|\mathbb{Q}$ total, so hat die Steinitzklasse der Erweiterungen $K_m|K_n$ immer Ordnung 2, ausser im Fall $\delta_{K_0}^{(2)} = 2^3$ und $n = 0, m = 1$. Hier ist die Steinitzklasse trivial.

8.12 Folgerung. *Die Differente $\mathcal{D}$ und die Diskriminante δ der relativen Erweiterungen $K_m|K_n$ sind stets Hauptideale für alle $0 \le n \le m$.*

Beweis. Es ist $[\delta] = s_A(B)^2 = 1$ in $C\ell_K$, da die Ordnung von $s_A(B) \le 2$ ist. Für jedes Primideal $\mathfrak{p}_n$ über 2 in K_n ist $\mathfrak{p}_n^2 = (\pi_n)$ ein Hauptideal. Da die Diskriminante selbst ein Hauptideal ist, muss $\delta = \mathfrak{p}^{2k}$ sein, mit $k \in \mathbb{N}$ geeignet. Das Primideal $\mathfrak{p}$ verzweigt total, also ist $N(\mathfrak{P}) = \mathfrak{p}$ für $\mathfrak{P}|\mathfrak{p}$ in K_m. Deshalb muss auch für die Differente $\mathcal{D} = \mathfrak{P}^{2k}$ gelten. Auch dies ist ein Hauptideal. □

8.13 Folgerung. *Für jede relative Erweiterung $K_m|K_n$ existiert ein Galois-invariante Steinitzwurzel Δ.*

Beweis. Ist die Steinitzklasse trivial, so ist alles gezeigt, da die Differente immer ein Hauptideal ist. Sei also $s_A(B) = [\mathfrak{p}]$ von Ordnung 2 in $C\ell_K$. Die Differente $\mathcal{D}$ und die Diskriminante δ sind Hauptideale und $\mathfrak{P}|\mathfrak{p}$ verzweigt total. Es hat auch $[\mathfrak{P}]$ Ordnung 2 in $C\ell_L$, da $\mathfrak{P}^2 = (\pi_m B)$ ein Hauptideal ist. Wir haben also $N([\mathfrak{P}]) = [\mathfrak{p}] = s_A(B)$ aufgrund der totalen Verzweigung und $[\mathfrak{P}]^2 = 1 = [\mathcal{D}]$ in $C\ell_L$. Damit ist die gesuchte Steinitzwurzel $\Delta = [\mathfrak{P}]$. Mit $\mathfrak{P}$ ist auch Δ Galois-invariant. □

Anmerkung. Das Resultat von Hauptsatz 3 lässt sich problemlos auf reell quadratische Teilkörper übertragen. Einzig bei der Ordnung der Steinitzklasse kann es zu Unterschieden

kommen, denn im Gegensatz zu den imaginären Zahlkörpern lässt sich im reellen Fall das Normargument (zur Untersuchung, ob ein Ideal Hauptideal ist oder nicht) nicht so einfach anwenden.
Die Aussage, dass die Steinitzklasse Ordnung 2 in $C\ell_K$ hat, muss durch Ordnung ≤ 2 ersetzt werden.

Literaturverzeichnis

[Arm] J. V. Armitage, On a theorem of Hecke in number fields and function fields, *Invent. Math.* **2** (1967), 238-246.

[Ar] E. Artin, Questions de base minimale dans la théorie des nombres algébriques, *Colloques Internat. Centre Nat. Rech. Sci. 24 (Algebre et theorie des nombres, Paris 25.9.-1.10.1949)* (1950), 19-20.

[CF] J. W. S. Cassels; A. Fröhlich, "Algebraic Number Theory", Academic Press London, New York 1967.

[Ch] L. N. Childs, The group of unramified Kummer extensions of prime degree, *Proc. London Math. Soc.* **35** (1977), 407-422.

[CR] C. W. Curtis; I. Reiner, "Representation theory of finite groups and associative algebras", Wiley, New York - London, 1962.

[Fe] B. Ferrero, The cyclotomic $\mathbb{Z}_2$-extension of imaginary quadratic fields, *Am. J. Math.* **102** (1980), 447-459.

[FW] B. Ferrero; L. C. Washington, The Iwasawa-invariant μ_p vanishes for abelian number fields, *Ann. of Math.* **109** (1979), 377-395.

[Fr1] A. Fröhlich, Discriminants of algebraic number fields, *Math. Z.* **74** (1960), 18-28.

[Fr2] A. Fröhlich, The discriminant of relative extensions and the existence of a integral basis, *Mathematika* **7** (1960), 15-22.

[FST] A. Fröhlich; J.-P. Serre; J. Tate, A different with an odd class, *J. Reine Angew. Math.* **209** (1962), 6-7.

[Ha1] H. Hasse, "Number Theory", Grundlehren der mathematischen Wissenschaften **229**, Springer-Verlag, Berlin - Heidelberg - New York, 1980.

[Ha2] H. Hasse, "Über die Klassenzahl abelscher Zahlkörper", Akademie - Verlag, Berlin, 1952.

[He] E. Hecke, "Vorlesungen über die Theorie der algebraischen Zahlen", Akademische Verlagsgesellschaft, Leipzig, 1923.

[Hu] B. Huppert, "Endliche Gruppen I", Grundlehren der mathematischen Wissenschaften **134**, Springer-Verlag, Berlin - Heidelberg - New York, 1979.

[Ih] H. Ichimura, On power integral basis of unramified cyclic extensions of prime degree, *J. Algebra* **235** (2001), 104-112.

[Iw] K. Iwasawa, On $\mathbb{Z}_l$-extensions of algebraic number fields, *Ann. Math.* **98** (1973), 246-326.

[KANT] M. Daberkow; C. Fieker; J. Klüners; M. Pohst; K. Roegner and K. Wildanger, KANT V4, *J. Symbolic Comp.* **24** (1997), 267-283.

[KS] M. Knebusch; W. Scharlau, Quadratische Formen und quadratische Reziprozitätsgesetze über algebraischen Zahlkörpern, *Math. Z.* **121** (1971), 346-368.

[La] S. Lang, "Algebraic Number Theory", Graduate Texts in Mathematics **110**, Springer-Verlag, Berlin - Heidelberg - New York, 1986.

[Mar] J. Martinet, Modules sur l'algèbre du groupe quaternionien, *Ann. Sci. Éc. Norm. Supér., IV. Sér.* **4** (1971), 399-408.

[Nar] W. Narkiewicz, "Elementary and Analytic Theory of Algebraic Numbers", 2nd ed., Springer-Verlag, Berlin - Heidelberg - New York, 1990.

[Neu] J. Neukirch, "Algebraische Zahlentheorie", Springer-Verlag, Berlin - Heidelberg - New York, 1992.

[Noe] E. Noether, Normalbasis bei Körpern ohne höhere Verzweigung, *J. Reine Angew. Math.* **167** (1932), 147-152.

[OM] O. T. O'Meara, "Introduction to Quadratic Forms", 3. Aufl., Grundlehren der mathematischen Wissenschaften **117**, Springer-Verlag, Berlin - Göttingen - Heidelberg, 1973.

[Pie] S. Pierce, Steinitz classes in quartic fields, *Proc. Am. Math. Soc.* **43** (1974), 39-41.

[Sch] P. Schmid, "Klassenkörpertheorie", Skript zur Vorlesung, Math. Institut der Universität Tübingen, Sommersemester 1997.

[Se] J. P. Serre, "Local Fields", Graduate Texts in Mathematics **67**, Springer-Verlag, Berlin - Heidelberg - New York, 1979.

[So] E. Soverchia, Relative integral basis over a Hilbert class field, *J. Number Theory* **97** (2002), 199-203.

[Sw] R. G. Swan, Noether's Problem in Galois Theory, *Emmy Noether in Bryn Mawr*, Proc. Symp., Bryn Mawr/USA 1982, 21-40, 1983.

[Wa] L. C. Washington, "Introduction to Cyclotomic Fields", Graduate Texts in Mathematics **83**, Springer-Verlag, Berlin - Heidelberg - New York, 1982.

[We] H. Weber, Theorie der Abelschen Zahlkörper, *Acta Math.* **8** (1886), 193-263.

[Wei] A. Weil, "Basic number theory", Grundlehren der mathematischen Wissenschaften **144**, Springer-Verlag, Berlin - Heidelberg - New York, 1967.

Lebenslauf

	Rebecca Roy
29.11.1973	geboren in Pforzheim/Enzkreis
1980 - 1984	Grundschule Unterreichenbach
1984 - 1993	Hilda-Gymnasium Pforzheim
Mai 1993	Abitur
WS 1993/94 - SS 1999	Studium der Mathematik und Physik, Staatsexamen an der Eberhard-Karls Universität in Tübingen
WS 1999/2000	Zweitstudium Mathematik - Diplom mit Nebenfach Physik
Dezember 1999	Diplomprüfung Mathematik
seit SS 2000	Doktorandin an der Math. Fakultät der Universiät Tübingen
Oktober 2000	Stipendium nach dem Landesgraduiertenförderungsgesetz
seit November 2000	Stipendium der Konrad-Adenauer-Stiftung e.V.

Meine akademischen Lehrer in Mathematik waren die Herren Professoren und Dozenten

R. Bödi, U. Felgner, W. Knapp, C. Lubich, F. Räbiger, U. Riese, H. Salzmann, P. Schmid, M. Voit, M. Wolff, H. Yserentant.