TECHNISCHE UNIVERSITÄT WIEN

VIENNA UNIVERSITY OF TECHNOLOGY

D I P L O M A R B E I T

Abelsche Zahlkörper und das Klassenzahlproblem

Ausgeführt am Institut für
Diskrete Mathematik und Geometrie
der Technischen Universität Wien

unter Anleitung von
Univ.Prof. Dipl.-Ing. Dr. techn. Michael Drmota

durch
Johannes Schleischitz
Viehtrift 13
7000 Eisenstadt

Datum

Unterschrift

Inhaltsverzeichnis

Kapitel 1

Einführung

1.1 Inhalt der Arbeit

Die vorliegende Arbeit beschäftigt sich mit der reichhaltigen Arithmetik von algebraischen Zahlkörpern, also endlichdimensionalen Erweiterungen des Körpers der rationalen Zahlen. Als Hauptziel ist die Herleitung der Klassenzahlformel für Erweiterungen mit abelscher Galoisgruppe zu nennen. Sie gibt die Zahl der verschiedenen Idealklassen des Ganzheitsringes eines Zahlkörpers an und ist im Fall genannter abelscher Zahlkörper mit gewissen Standardkenngrößen des Zahlkörpers in einen einfachen formelmäïgen Zusammenhang zu bringen. Die Klassenzahl misst in einem gewissen Sinn, wie weit ein Ring von einer eindeutigen Primfaktorzerlegung entfernt ist, so bedeutet Klassenzahl 1 etwa, dass ein Hauptidealring vorliegt un ddamit eine eindeutige Primfaktorzerlegung. Nach einleitenden grundlegenden Definitionen und Ergebnissen über die Struktur des Ganzheitsringes und den wichtigen Begriffen von Spur und Norm wird im zweiten Kapitel nochmals auf entscheidende Eigenschaften der Ganzheitsringe eingegangen, wobei hier der Ansatz über deren Charakterisierung als Dedekindringe trotz einiger Überschneidungen neue Erkenntnisse bringt, die zum Begriff der Klassenzahl führen. Deren Endlichkeit wird exakt bewiesen, wobei hier als technische Hilfsmittel vor allem der Begriff der Diskriminante eines Körpers sowie der der Norm eines Ideals zu nennen sind. Die Endlichkeit der Klassenzahl dient als Grundlage für den analytischen Zugang. Mit der Zetafunktion eines Zahlkörpers wird in Kapitel 5 das wesentliche Hilfsmittel zur analytischen Beschreibung der Arithmetik von Zahlkörpern vorgestellt, und dann ein relativ kurzer Beweis der Klassenzahlformel im allgemeinen Fall auf dem Wege der Geometrie der Zahlen vorgestellt, wobei entscheidend auf Kapitel 1 zurückgegriffen wird. Die folgenden Kapitel schließen den Bogen zu abelschen Zahlkörpern mit ihrer speziellen Klassenzahlformel. Die Beschreibung von Primidealen, insbesondere von Primzahlen erzeugte Hauptideale sind von Interesse, im Zusammenhang mit den Begriffen des Verzweigungs- und Trägheitsindex, sind ein Eckpfeiler dafür. Ein weiterer ist die vermöge des hier nicht bewiesenen tiefliegenden Satzes von Kronecker-Weber im Zusammenhang mit abelschen Zahlkörpern stehende Theorie der Kreisteilungskörper und L-Reihen auf deren Teilkörpern. Weiters ist ein technischer Ausflug in die Theorie der P-adischen Körper zu nennen, wobei hier großteils Resultate ohne Beweise angeführt werden.
Generell ist zu betonen, dass auf den Aufbau in den ersten Kaptiteln viel Wert gelegt

wurde, wo der Ganzheitsring in seiner Modulstrukur sowie in seiner Struktur als Dedekindring auf zweierlei Arten beleuchtet wird, während technische Beweise gewisser für sich interessanter Resultate wie des Dirichletschen Einheitensatzes und des Satzes von Kronecker-Weber oder im Bereich der P-adischen Körper, die an manchen Stellen entscheidend eingehen, dafür ausgespart wurden.

1.2 Grundlegende Definitionen und Sätze

In der Arbeit werden algebraische Grundbegriffe wie Körper, Ring, Modul und Ideal vorausgesetzt sowie grundlegendes algebraisches Wissen, wie etwa den Begriff eines Quotientenkörpers eines Integritätsbereichs oder Basiswissen über Körpererweiterungen wie zB der Gradsatz für deren Hintereinanderausführung oder elementare Homomorphiesätze. Für eine Körpererweiterung im Sinne der Adjunktion von Elementen werden durchwegs runde Klammern benutzt werden, zum Beispiel $\mathbb{Q}(\alpha)$, während Polynomringe über einem Ring oder Körper mit eckigen Klammern stehen, etwa $\mathbb{Z}[a]$.

Definition 1.1. Durchwegs bezeichnen $\mathbb{R}$ die reellen Zahlen, $\mathbb{Q}$ die rationalen Zahlen, $\mathbb{Z}$ die ganzen Zahlen, $\mathbb{N}$ die natürlichen Zahlen, $\mathbb{C}$ die komplexen Zahlen und $\overline{\mathbb{Q}}$ die algebraischen Zahlen.

Definition 1.2 (Algebraischer Zahlkörper)**.** Ein algebraischer Zahlkörper ist ein endlichdimensionaler (insbesondere algebraischer) Erweiterungskörper der rationalen Zahlen.

Satz 1.1. Jede algebraische Zahl $a \in \overline{\mathbb{Q}}$, also Nullstelle eines Polynoms mit rationalen (oder äquivalent ganzzahligen Koeffizienten) hat ein eindeutig bestimmtes normiertes Polynom niedrigsten Grades mit rationalen Koeffizienten, dessen Nullstelle es ist.

Beweis: Da der Polynomring $\mathbb{Q}[x]$ mit dem Polynomgrad als Bewertung ein euklidischer Ring ist und die rationalen Zahlen ein Körper bilden, ist stets eine Polynomdivision mit Rest in $\mathbb{Q}[x]$ durchführbar. Das Restpolynom hat dabei kleineren Grad als das Polynom im Nenner. Es gibt nun aber klarerweise eine minimale positive ganze Zahl n, zu der es ein Polynom $p \in \mathbb{Q}[x]$ mit $p(a) = 0$ gibt. Für jedes Polynom $q \in \mathbb{Q}[x]$ mit Nullstelle a gilt aber $p(a) - q(a)r(a) = 0$ für alle Polynome $r(x) \in \mathbb{Q}[x]$, woraus aufgrund oben genannten Divisionsalgorithmus wegen der Minimalität von n folgt, dass alle solchen Polynome $q \in \mathbb{Q}[x]$ Vielfache von $p \in \mathbb{Q}[x]$ sein müssen (im Sinne der Teilbarkeit in $\mathbb{Q}[x]$). Das eindeutige geforderte Polynom der Aussage bekommt man offensichtlich, indem man $p \in \mathbb{Q}[x]$ normiert.

Definition 1.3 (Minimalpolynom)**.** Ein Polynom entsprechend obigen Satzes heißt *Minimalpolynom* von $a \in \overline{\mathbb{Q}}$.

Definition 1.4. Ein Element eines algebraischen Zahlkörpers heißt ganz, wenn es Nullstelle eines *normierten* Minimalpolynoms mit Koeffizienten aus $\mathbb{Z}$ ist.

Satz 1.2. Die Menge aller ganzen Elemente bilden einen Unterring des algebraischen Zahlkörpers K. Wir bezeichnen ihn im folgenden mit O_K und nennen ihn den *Ganzheitsring* von K.

Für den Beweis verwenden wir nachstehendes Lemma:

Lemma 1.1. $\mathbb{Z}[a]$ ist genau dann additiv endlich erzeugt, dh bezüglich + eine endlich erzeugte Gruppe, falls a ganz ist.

Allgemeiner gilt: Sei R ein Ring und S eine Ringerweiterung von R. Dann ist $a \in S$ genau dann ganz, wenn $R[s]$ als R-Modul endlich erzeugt ist.

Beweis: Wir beweisen nur die für den obigen Satz schwächere (nicht allgemeine) Aussage (der Beweis im allgemeinen Fall geht jedoch analog):
a ganz $\implies$ $\mathbb{Z}[a]$ endlich erzeugt: Jedes Element in $\mathbb{Z}[a]$ ist von der Form $f(a)$ mit einem Polynom $f \in \mathbb{Z}[x]$. Führe bei diesem Polynom die Polynomdivison durch das Minimalpolynom von g von a durch, also ein normiertes Polynom $g \in \mathbb{Z}[x]$ welches $g(a) = 0$ erfüllt. Wegen der Normiertheit ist das möglich. Man erhält also

$$f(a) = q(a)g(a) + r(a), \quad q \in \mathbb{Z}[x], \quad g(a) = 0, \quad \deg(r) < n$$

Dies zeigt, dass $\{1, a, a^2, ...a^{n-1}\}$ eine Basis von $\mathbb{Z}[a]$ ist.

$\mathbb{Z}[a]$ endlich erzeugt $\implies$ a ganz: Sei $\alpha_1, \alpha_2 \dots \alpha_s$ ein endliches Erzeugendensystem von $\mathbb{Z}[a]$. Da die α_i in $\mathbb{Z}[a]$ sind, haben sie eine Darstellung

$$\alpha_i = \sum_j \beta_{i,j} a^j, \qquad 1 \leq i \leq s$$

Offenbar treten nur endlich viele a-Potenzen auf, sei a^k die höchste. Weil ganz $\mathbb{Z}[a]$ von den α_i erzeugt wird und die ganzen Zahlen einen Ring bilden, lässt sich insbesondere a^{k+1} in der Form

$$a^{k+1} = \sum_{i=1}^{k} b_i a^i, \qquad b_i \in \mathbb{Z}$$

schreiben, was offensichtlich in eine Ganzheitsgleichung umgeschrieben werden kann. □

Nun folgt der Beweis von Satz 1.2.

Beweis: Seien a,b ganze Elemente des algebraischen Zahlkörpers K. Nach obigem Hilfssatz sind die Moduln $\mathbb{Z}[a]$ und $\mathbb{Z}[b]$ von Elementen $\{a_1, \dots, a_k\}$ bzw $\{b_1, \dots, b_l\}$ erzeugt. Die Ringe $\mathbb{Z}[a+b]$ und $\mathbb{Z}[ab]$ sind als Unterringe vom von den Elementen $(a_i b_j)_{i,j=1,\dots,n}$ erzeugten Ring ebenfalls endlich erzeugt, weshalb wieder aufgrund obigen Hilfssatzes die Elemente $a+b$ und ab ganz sind. Weil a,b beliebig gewählt waren handelt es sich folglich um einen Unterring. □

Der Ganzheitsring hat jedoch eine wesentlich stärkere Struktur als nur Unterring zu sein. Ein zentrales Resultat, das insbesondere für die geometrische Betrachtung wichtig und Beweisgrundlage des folgend erwähnten dirichletschen Einheitensatzes ist, ist die Tatsache dass er als $\mathbb{Z}$-Modul maximal (insbesondere mit maximaler Dimension) ist. Dieses Resultat wird nun vorbereitet.

Definition 1.5 (Ordnung)**.** Eine *Ordnung* eines Zahlkörpers K mit Dimension n über den rationalen Zahlen ist ein Unterring von K mit 1, der als (freier) $\mathbb{Z}$-Modul endlich erzeugt von maximalem Rang n ist.

Bemerkung: Jeder Ring kann als $\mathbb{Z}$-Modul aufgefasst werden.

Bemerkung: Ein Satz aus der Algebra besagt, dass über Ringen endlich erzeugte, torsionsfreie Moduln genau die freien Moduln sind, also eine Basis haben. Die Eigenschaft

endlich erzeugt zu sein bedeutet für einen algebraischen Zahlkörper also, dass er eine Basis über $\mathbb{Z}$ besitzt. In diesem Kapitel ist bei Moduln immer von *freien Moduln* die Rede.
Für nachstehendes Lemma sowie spätere Kapitel benötigt man die Begriffe der Norm und der Spur einer Körpererweiterung.

Definition 1.6 (Norm)**.** Unter der *Norm* eines Elements α einer algebraischen Körpererweiterung L/K verstehen wir den Ausdruck

$$N_{L/K}(\alpha) = \alpha_1\alpha_2 \dots \alpha_n \tag{1.1}$$

wobei die α_j die Nullstellen des Minimalpolynoms von α bezüglich L/K im Zerfällungskörper (normaler Abschluss von $K(\alpha)$) bezeichnen oder alternativ die Bilder von α unter den Monomorphismen (zu zweiterem siehe nächster Abschnitt)

Definition 1.7 (Spur)**.** Unter der *Spur* eines Elements α einer algebraischen Körpererweiterung L/K verstehen wir den Ausdruck

$$Sp_{L/K}(\alpha) = \alpha_1 + \alpha_2 + \ldots + \alpha_n \tag{1.2}$$

wobei die α_j die Nullstellen des Minimalpolynoms von α bezüglich L/K im Zerfällungskörper (normaler Abschluss von $K(\alpha)$) bezeichnen oder alternativ die Bilder von α unter den Monomorphismen (zu zweiterem siehe nächster Abschnitt).

Diese Größen sind sehr praktikabel und werden eine wichtige Rolle beim Beweis der Endlichkeit der Klassenzahl spielen. Eine wichtige Erkenntnis ist, dass Norm und Spur einer Körpererweiterung L/K bereits im kleinen Körper K enthalten sind. Dies kann man einerseits einsehen, indem man die Abbildung $g_\alpha : x \longmapsto \alpha \cdot x$ auf L betrachtet. Im Sinne der linearen Algebra ist das ein Automorphismus (für $\alpha \neq 0$), wenn man eine beliebige Basis von L/K wählt. Norm und Spur dieser linearen Abbildung sind gerade Norm und Spur wie oben definiert, andererseits aber Koeffizienten des Minimalpolynoms von α und als solche in K. Unten wird ein alternativer Beweis auf Basis von Moduln geführt.
Die Interpretation von Norm und Spur als Determinante und Spur von Matrizen ergibt auch sofort die *Multiplikativität der Norm* wegen der Multiplikativität von Determinanten sowie die *Additivität der Spur*. Eine weitere relativ einfach nachzuprüfende Eigenschaft ist

Proposition 1.1. Sind L/K und M/L endliche Erweiterungen, dann gilt für alle $\alpha \in M$: $N_{M/K}(\alpha) = N_{L/K}(N_{M/L}(x))$.

Lemma 1.2. Sei O eine Ordnung. Dann ist jedes $a \in O$ ist ganz. Insbesondere sind Norm und Spur ganze Zahlen.

Beweis: Man fasse O als Modul mit Basis $\mu_1, \ldots, \mu_n$ über den rationalen Zahlen auf. Klarerweise ist dann auch $a\mu_i \in O$ weil O Ring ist. Deswegen und weil die μ_i eine Basis sind kann das System

$$a\mu_i = a_{ij}\mu_i \qquad i, j \in 1, 2, \ldots, n$$

in *ganzen Zahlen* gelöst werden. Aus $a_{ij} \in \mathbb{Z}$ folgt aber, dass a ganz ist. □

Auf Norm und Spur wird in Kapitel 3 näher eingegangen.

Lemma 1.3. Wenn a ein ganzes Element von Grad m einer Ordnung O ist, dann ist der von $\{1, a, \ldots, a^{m-1}\}$ erzeugte Modul M ein Ring (also multiplikativ abgeschlossen).

Beweis: Es reicht zu zeigen, dass $a^k \in M$ für alle k. Für $k \leq m-1$ stimmt das per Definition, weil a ganz ist, ist $a^m = q(a)$ mit einem Polynom $q(a)$ von Grad kleiner als m, also stimmt es auch für $k = m$. Für $k \geq m$ ergibt sich folgende Induktionskonstruktion: Sei $a^{k-1} \in M$. Dann gilt

$$a^{k-1} = a_{m-1}a^{m-1} + \ldots + a_0 \tag{1.3}$$

Multiplikation beider Seiten von 1.3 mit a ergibt also

$$a^k = aa^{k-1} = a_{m-1}a^m + \ldots + a_0 a \tag{1.4}$$

und weil alle Elemente der rechten Seite von (1.4) in M liegen gilt dies auch für a^k. □

Lemma 1.4. Ist O eine Ordnung im Zahlkörper K und $a \in O$, dann ist auch der Polynomring $O[a]$ eine Ordnung von K.

Beweis: Da $O \subset O[a]$ gibt es offenbar $n(= K : \mathbb{R})$ linear unabhängige Basisvektoren, es ist also noch zu zeigen dass es sich bei $O[a]$ um einen Modul handelt, er also endlich erzeugt ist. Sei $\omega_1, \ldots, \omega_n$ Basis von O. Vom letzten Lemma 1.3 wissen wir, dass a^k eine Darstellung der Form $a_0 + a_1 a + a_2 a^2 + \ldots, a_{m-1}a^{m-1}$ besitzt wobei $m \leq n$ den Grad von a bezeichnet. Daher kann $O[a]$ als Linearkombination von Produkten $\omega_i a^j$ dargestellt werden, also ist $O[a]$ endlich erzeugter Modul. □

Korollar 1.1. Der Polynomring $O[a_1, a_2, \ldots, a_r]$ für beliebiges r und ganze Elemente $a_1, a_2, \ldots, a_r \in O$ ist eine Ordnung.

Beweis: Folgt unmittelbar durch Iteration obigen Lemmas 1.4. □

Zum Beweis der Hauptaussage dieses Abschnitts wird noch die Definiton der dualen Basis benötigt. Vorbereitend hierzu liegt folgendes Konzept zugrunde: Sei L/K eine n-dimensionale Körpererweiterung und $\omega_1, \ldots, \omega_n$ eine feste (Vektorraum)basis von L über K. Dann ist für jede Auswahl von Elementen $c_1, \ldots, c_n$ von K das lineare Gleichungssystem

$$Sp(\omega_i \alpha) = c_i \qquad i = 1, 2, \ldots, n \tag{1.5}$$

eindeutig für $\alpha \in L$ lösbar. Dies sieht man ein, indem man $\alpha = x_1\omega_1 + \ldots + x_n\omega_n$ schreibt und erkennt, dass die dem Gleichungssystem (1.5) entsprechende Matrix aufgrund der linearen Unabhängigkeit der ω_i invertierbar ist und somit $x_1, x_2 \ldots, x_n$ eindeutig bestimmt werden können. Damit ist die Sinnhaftigkeit folgender Definiton gewährleistet:

Definition 1.8. Zu einer gegebenen Basis $\omega_1, \omega_2 \ldots, \omega_n$ bezeichne $\omega_1^*, \omega_2^* \ldots, \omega_n^*$ die duale Basis, die durch die definierende Eigenschaft

$$Sp(\omega_i \omega_j^*) = \delta_{i,j}$$

bestimmt ist.

Satz 1.3. Der Ganzheitsring eines algebraischen Zahlkörpers K bildet die eindeutige bezüglich Inklusion maximale Ordnung des Körpers.

Beweis: Wir wissen bereits aus Satz 1.1, dass die ganzen Elemente einen Ring bilden. Wegen Lemma 1.2 und weil O als Ordnung per Definitionem n $\mathbb{Z}$-linear unabhängige Elemente besitzt exisiteren n $\mathbb{Z}$-linear unabhängige ganze Elemente. Es muss also nur gezeigt werden, dass die ganzen Elemente sogar einen freien $\mathbb{Z}$-Modul bilden.
Seien $\omega_1, \omega_2 \ldots, \omega_n$ eine Basis von O und $\omega_1^*, \omega_2^* \ldots, \omega_n^*$ die dazu duale Basis in K. Sei α beliebig ganz mit Darstellung

$$\alpha = c_1\omega_1^* + \ldots + c_n\omega_n^*$$

mit rationalen c_i. Multiplizieren mit ω_i und Bildung der Spur ergibt

$$c_i = Sp(\alpha\omega_i) \tag{1.6}$$

Da alle Produkte $a\omega_i$ aus (1.6) im Polynomring $O[\alpha]$ liegen, der nach Lemma 1.4 eine Ordnung ist und nach Lemma 1.2 daher alle c_i ganze Zahlen sind, ist $\alpha \in O^*$, wobei O^* der von den ω_i^* erzeugte Modul (über den rationalen Zahlen) ist. Deswegen ist die Menge ganzen Elemente von K in O^*. Weil jede additive Untergruppe eines Moduls in einem algebraischen Zahlkörper wieder ein (Unter)modul ist (ohne Beweis [1]), bilden die ganzen Elemente von K einen Modul. □

Definition 1.9. Ein $\mathbb{Q}$-linear unabhängiges Erzeugendensystem des Ganzheitsringes O_K eines Zahlkörpers K als $\mathbb{Z}$-Modul heißt *Ganzheitsbasis von K.*

Satz 1.3 besagt also insbesondere: Ist K algebraischer Zahlkörper mit $[K : \mathbb{Q}] = n$, dann besitzt O_K stets eine Ganzheitsbasis $w_1, w_2, \ldots w_n$.
Wie bereits erwähnt kann man zeigen, dass torsionsfreie endlich erzeugte Moduln über Ringen genau die freien Moduln sind. Unter Zuhilfenahme dieses nicht ganz einfach zu beweisenden Resultats erhielte man sofort die oben nicht bewiesene Tatsache, sowie zusätzlich, dass der Ganzheitsring ein Modul ist, da es über einem Körper ja keine Torsionselemente gibt und Ringe immer als unitäre $\mathbb{Z}$-Moduln aufgefasst werden können. Es sei auf Hungerford [Hu 1] verwiesen. Wir verfolgen hier einen etwas weniger allgemeinen Ansatz.

Als Abschluss dieses Unterkapitels wollen wir noch eine wichtige Feststellung festhalten, die sich mit einem kleinen Trick sofort aus dem bisher erarbeiteten gewinnen lässt, und in folgenden Kapiteln ohne explizite Referenz einfach verwendet werden wird. Es gilt:

$$\forall b \in K \quad \exists w \in O_K : \quad w \cdot b \in O_K$$

Denn ist $b \in K$ Nullstelle von

$$a_m x^m + a_{m-1}x^{m-1} + \ldots + a_0 = 0, \qquad a_i \in \mathbb{Z}$$

und multipliziert man die Gleichung mit a_m^{m-1}, so sieht man, dass a_m das geforderte w ist, denn ba_m erfüllt offensichtlich eine Ganzheitsgleichung. Damit ist des weiteren das suggestive Resultat bestätigt, *dass K der Quotientenkörper von O_K ist.*

[1] siehe [BS 66]

Jetzt bedarf es noch einiger weiterer Begriffsbildungen und einfacher Feststellungen um algebraische Zahlkörper noch besser beschreiben zu können.

1.3 Monomorphismen eines algebraischen Zahlkörpers

Vorbereitend für den Beweis des uns eigentlich interessienden Satzes braucht man ein paar algebraische Standardergebnisse. Obwohl wir uns später nur mit algebraischen Zahlkörper beschäftigen werden, sind einige Resultate allgemeiner gehalten, da sich ihr Beweis nicht wesentlichen verkürzen würde im Spezialfall. Die Existenz eines Zerfällungskörpers eines Polynoms im allgemeinen Fall wird ohne Beweis vorausgesetzt.

Definition 1.10 (separabel, vollkommen)**.** Ein Polynom $f \in K[x]$ heißt *separabel*, wenn die Nullstellen im Zerfällungskörper einfach sind. Sei L/K eine Körpererweiterung. Ein algebraisches Element von L heißt separabel über K, wenn sein Minimalpolynom über K separabel ist. Eine algebraische Erweiterung L/K heißt separable Erweiterung, wenn alle Elemente von L separabel sind. Ein Körper K heißt *vollkommen*, wenn alle irreduziblen $f \in K[x]$ separabel sind.

Satz 1.4. Körper K der Charakteristik 0- insbesondere $\mathbb{Q}$ und Erweiterungen von $\mathbb{Q}$- sind vollkommen.

Beweis: Weil $p \in K[x]$ folgt dass auch seine formale Ableitung $q \in K[x]$ erfüllt, und wegen char$K \neq 0$ ist $q \neq 0$ sowie $\deg(q) = \deg(p) - 1$. Sei ζ doppelte Nullstelle seines Minimalpolynoms $p \in K[x]$. Dann gilt $(x-\zeta)^2$ teilt $p \in L(x)$ im Sinne der Teilbarkeit in $L[x]$ für den Zerfällungskörper L von $p \in K[x]$. Daraus sieht man durch ableiten, dass $(x - \zeta)$ entsprechend das Polynom $q \in K[x]$ teilen muss. Also folgt, dass ζ Nullstelle von $q \in K[x]$ ist. Dies wiederspricht der Minimalität vom Grad von $p \in K[x]$ wegen anfänglicher Feststellung. □

Lemma 1.5. Sie $K \subset L$ eine Körpererweiterung und seien $f, g \in K[X]$. Weiters seien

$$d := \mathrm{ggT}(f,g) \quad in \quad K[X] \quad , \qquad \tilde{d} := \mathrm{ggT}(f,g) \quad in \quad L[X]$$

Dann gilt $d = \tilde{d}$, insbesondere $\tilde{d} \in K[X]$.

Beweis: Wir zeigen $\tilde{d}|d$, die umgekehrte Teilbarkeitsbeziehung ist trivial weil d auch in $L[X]$ gemeinsamer Teiler der beiden Polynome ist. Dazu stelle d dar als

$$d = pf + qg \quad p, q \in K[X] \tag{1.7}$$

und beobachte, dass man diese Gleichung (1.7) auch in $L[X]$ auffassen kann, dort gilt jedoch $\tilde{d}|f$, $\tilde{d}|g$, also $\tilde{d}|d$. Aus der wechselseitigen Teilbarkeit und der Normiertheit beider Polynome folgt das Resultat. □

Satz 1.5 (Satz vom primitiven Element)**.** Sei K ein Körper der Charakteristik 0 und L eine endlichdimensionale Erweiterung. Dann exisitiert ein (nicht eindeutiges) Element $a \in L$ mit $L = K(a)$.

Beweis: Offensichtlich gibt es endlich viele Zahlen $a_1, a_2 \ldots, a_n$ in L mit
$L = K(a_1, a_2, \ldots, a_k)$, denn immer wenn man ein beliebiges neues Element a_{r+1} aus $L \setminus K(a_1, \ldots, a_r)$ zu einer Erweiterung $K \subset K(a_1, \ldots, a_r) \subset L$ adjungiert erhöht sich deren Vektorraumdimension über K. Wegen der Endlichkeit von $L : K$ muss man nach endlich vielen Schritten ganz L erhalten, da bei jedem echten Zwischenkörper immer Elemente in $L \setminus K(a_1, \ldots, a_r)$ adjungiert werden können. Nun ist zu zeigen, dass jede man jede Erweiterung $L := K(a_1, \ldots, a_k)$ schreiben kann als $K(a_1, \ldots, a_k) = K(a)$. Dafür reicht es offensichtlich im Fall von 2 adjungierten Variablen a, b ein c zu finden mit

$$L := K(a, b) = K(c) \tag{1.8}$$

der Rest folgt durch eine triviale Induktion.
Seien f und g die Minimalpolynome von a bzw b. Folglich existiert eine Faktorisierung

$$f(X) = (X - a)(X - a_2) \ldots (X - a_r), \quad a_i \in R$$

$$g(X) = (X - b)(X - b_2) \ldots (X - b_s), \quad b_i \in R$$

für den Zerfällungskörper $R \supset K$ von $f \cdot g$.
Wir verfolgen bei der Suche nach c aus (1.8) den Ansatz

$$c_\lambda = a + \lambda b, \quad \lambda \in K$$

Wir erhalten die Körperkette

$$K \subset K(c_\lambda) \subset K(a, b) = L \subset R \tag{1.9}$$

Wir wollen zeigen, dass für fast alle $\lambda \in K$ gilt, dass $K(c_\lambda) = L$. Wegen Charakteristik 0 ist K ein unendlicher Körper und wir wären folglich fertig.
Wir werden $b \in K(c_\lambda)$ zeigen, daraus folgt unmittelbar, dass auch $a = c_\lambda - \lambda b \in K(c_\lambda)$ und damit $K(a, b) \subset K(c_\lambda)$ was zusammen mit (1.9) wie gewünscht die Gleichheit der beiden Körper liefert.
Dazu definiere ein Polynom

$$h_\lambda(X) := f(c_\lambda) - \lambda X \in K[c_\lambda]$$

das mit g die gemeinsame Nullstelle b hat, denn $h_\lambda(b) = f(a) = 0$. Fordern wir nun zusätzlich die Ungleichungen

$$c_\lambda - \lambda b_j \neq a_i, \quad i = 1, 2 \ldots, r \quad j = 1, 2, \ldots s$$

oder äquivalent

$$\lambda \neq \frac{a_i - a}{b - b_j}, \quad i = 1, 2 \ldots, r \quad j = 1, 2, \ldots s \tag{1.10}$$

so gibt es offensichtlich keine weiteren gemeinsamen Nullstellen in L. Dabei ist zu bemerken, dass weil g als irreduzibles Polynom nach Satz 1.4 nur einfache Nullstellen hat obige Ausdrücke wohldefiniert sind. Ebenfalls klar ist, dass fast alle und damit unendlich viele $\lambda \in K$ obigen Anforderungen (1.10) gerecht werden. Für ein solches zulässiges λ

ist nach Konstruktion und abermals Satz 1.4 der besagt, dass b einfache Nullstelle von g ist,

$$\mathrm{ggT}(g, h_\lambda) = (X - b)$$

aufgefasst als Elemente vom Polynomring $R[X]$. Aus Lemma 1.5 folgt diese Gleichheit aber auch in $K(c_\lambda)[X]$, also $(X - b) \in K(c_\lambda)[X]$ und folglich $b \in K(c_\lambda)$. □

Satz 1.6. Zu einem algebraischen Zahlkörper vom Grad n über den rationalen Zahlen existieren genau n Monomorphismen in die komplexen Zahlen.

Beweis: Sei σ_1 ein erzeugendes Element von K (Satz vom primitiven Element), also $K = \mathbb{Q}(\sigma_1)$. Seien $\sigma_2, \ldots, \sigma_n$ die anderen Nullstellen des separablen Minimalpolynoms von σ_1. Offensichtlich muss bei jedem Homomorphismus σ_1 auf eines der σ_j abgebildet werden. Andererseits induziert jede solche Zuordnung tatsächlich einen Isomorphismus von $K = \mathbb{Q}(\sigma_1)$ nach $L := \mathbb{Q}(\sigma_j)$ (im Fall einer normalen Erweiterung sind das K-Automorphismen). Da wegen $K = \mathbb{Q}(\sigma_1)$ jeder Homomorphismus von K in die komplexen Zahlen durch das Bild von σ_1 festgelegt ist, entstehen so also die n Monomorphismen.

Definition 1.11. Sei K ein algebraischer Zahlkörper vom Grad n und $\sigma_1, \ldots, \sigma_n$ die Monomorphismen nach $\mathbb{C}$. Dann heissen die s Monomorphismen mit reellem Bild $\sigma_1, \ldots, \sigma_s$ *reelle Monomorphismen* und die restlichen t Paare konjugiert komplexer Monomorphismen $\sigma_{s+1}, \ldots, \sigma_n = \sigma_{s+2t}$ *komplexe Monomorphismen*, wobei diese Notation im folgenden beibehalten wird.

Definition 1.12 (Signatur)**.** Mit obiger Notation wird das Paar (s, t) *Signatur* von K genannt.

Im hier nicht vorgeführten Beweis des Dirichletschen Einheitensatzes wird das Lemma von Minkowski benötigt, das wir später in Verbindung mit der Klassenzahl noch in ganz ähnlicher Ausführung brauchen werden und deswegen gleich hier in einem eigenen Unterkapitel bewiesen sei, weil es thematisch passt. Ein ebenfalls sofort präsentiertes Korollar daraus werden wir ebenfalls später benötigen

1.4 Geometrische Darstellung von Zahlkörpern, Gitter und Minkowskis Lemma

Definition 1.13. : Bezeichne mit $\Lambda^{s,t}$ die Menge aller Vektoren

$$x = (x_1, \ldots, x_s; x_{s+1}, \ldots, x_{s+t}) \tag{1.11}$$

deren erste s Komponenten reell und die übrigen komplexwertig sind, in Korrespondenz zu s, t vom vorigen Abschnitt.

Zusammen mit der komponentenweisen Addition und Multiplikation sowie Multiplikation mit *reellen* Skalaren kann man $\Lambda^{s,t}$ einerseits als einen kommutativen Ring und andererseits als einen $\mathbb{R}$-Vektorraum auffassen. Die Dimension als $\mathbb{R}$-Vektorraum ist $s + 2t$, denn eine Basis ist offenbar gegeben durch die Vektoren

$$\begin{array}{c}(1,0,\ldots,0;0,0,\ldots,0)\\(0,1,\ldots,0;0,0,\ldots,0)\\\ldots\\(0,0,\ldots,1;0,0,\ldots,0)\\(0,0,\ldots,0;1,0,\ldots,0)\\(0,0,\ldots,0;i,0,\ldots,0)\\\ldots\\(0,0,\ldots,0;0,0,\ldots,1)\\(0,0,\ldots,0;0,0,\ldots,i)\end{array}$$

(1.12)

Indem man die Standardbasis e_i des $\mathbb{R}^n$ auf diese neue durchnumerierte Basis abbildet erhält man also einen Isomorphismus zwischen $\mathbb{R}^n$ und $\Lambda^{s,t}$. Setzt man

$$x_{s+j} = y_j + i \cdot z_j \qquad (j = 1, \ldots, t)$$

für die komplexen Koordinaten, dann hat (1.11) bezüglich Basis (1.12) die Form

$$x{=}(x_1, \ldots, x_s; y_1, z_1, \ldots, y_t, z_t) \tag{1.13}$$

Definition 1.14. : Sei K ein algebraischer Zahlkörper der $\mathbb{R}$-Vektorraumdimension $n = s+2t$ in obigem Sinne, also mit Signatur (s, t). Betrachtet man die Bilder von $\alpha \in K$ unter den $s + t$ Monomorphismen σ_1,σ_2 ,...,σ_s,σ_{s+1}, ...,σ_{s+t} (von σ_1,σ_2 ,...,σ_s,σ_{s+1}, $\overline{\sigma_{s+1}}$,...,σ_{s+t}, $\overline{\sigma_{s+t}}$) und nennt diese Abbildung x so erhält man eine Darstellung vom Bildvektor von α der Form (1.11). Diese bezeichnen wir als die *geometrische Darstellung des Elements α des Zahlkörpers*, die Menge aller solcher Bilder als *geometrische Darstellung des Zahlkörpers*. In Formeln

$$x(\alpha) = (\sigma_1(\alpha), \ldots \sigma_s(\alpha); \sigma_{s+1}(\alpha), \ldots \sigma_{s+t}(\alpha))$$

Weiters sei die Zerlegung in Real- und Imaginärteile in der Basis von (1.12) mit F bezeichnet, also

$$F(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_s(\alpha); \mathrm{Re}(\sigma_{s+1}(\alpha)), \mathrm{Im}(\sigma_{s+1}(\alpha)), \ldots, \mathrm{Re}(\sigma_{s+t}(\alpha)), \mathrm{Im}(\sigma_{s+t}(\alpha))) \tag{1.14}$$

Einfach nachzuprüfende Eigenschaften der Abbildung x sind:

x ist injektiv

$$x(\alpha + \beta) = x(\alpha) + x(\beta)$$

$$x(\alpha\beta) = x(\alpha)x(\beta)$$

$$x(q\alpha) = q \cdot x(\alpha), \quad q \in \mathbb{Q}$$

Definition 1.15. Unter der *Norm* eines Elements $x \in \Lambda^{s,t}$ verstehen wir den Ausdruck

$$N_1(x) = |x_1 x_2 \dots x_s||x_{s+1}|^2 \dots |x_{s+t}|^2$$

Man sieht wegen $z\overline{z} = |z|^2$, dass die Normabbildung $N_1(x(\alpha)) = N(\alpha), \alpha \in K$ erfüllt.
Zusätzlich zur erörterten geometrischen Darstellung eines algebraischen Zahlkörpers ist eine weitere kruzial- einerseits für den Dirichletschen Einheitensatz andererseits für unsere analytsichen Observationen in Kapitel 4.

Definition 1.16 (logarithmische Darstellung)**.** Einem $x = (x_1, \dots, x_{s+t}) \in \Lambda^{s,t}$ mit sämtlichen Komponenten von Null verschieden werde folgender Ausdruck
$l(x) = (l_1(x), \dots, l_{s+t}(x)) \in \mathbb{R}^{s+t}$ zugeordnet:

$$l_k(x) = \log |x_k|, \qquad k = 1, 2, \dots, s$$

$$l_{s+j}(x) = \log |x_{s+j}|^2, \quad j = 1, 2, \dots, t$$

Definition 1.17. Die Menge aller Ausdrücke der Form

$$a_1 e_1 + \ldots + a_m e_m$$

mit fest vorgegebenen linear unabhängigen Vektoren $e_1, \dots, e_m \in \mathbb{R}^n, \quad m \leq n$ und $a_i \in \mathbb{Z}$ heißt *m-dimensionales Gitter im* $\mathbb{R}^n$. Im Fall $m = n$ heißt das Gitter *voll*, sonst *nichtvoll*. Weiters bezeichne die Menge aller Ausdrücke

$$\alpha_1 e_1 + \ldots + \alpha_m e_m, \quad (\alpha_1, \dots, \alpha_m) \in (\mathbb{Q} \cap [0, 1))^n$$

die *Grundmasche* zum von $e_1, \dots, e_n$ erzeugten Gitter.

Proposition 1.2. Bezeichne T die Grundmasche des vollen Gitters G. Dann ist $\mathbb{R}^n$ die disjunkte Vereinigung der

$$T_z = T + z, \quad z \in G.$$

Beweis: Sei $e_1, \dots, e_n$ die Basis bezüglich der T konstruiert ist. Für beliebiges $x = x_1 e_1 + \ldots + x_n e_n$ mit $x_i \in \mathbb{R}$ ist nachzuweisen, dass es in genau einem T_z liegt. Zerlege jedes x_i in ganzzahligen Anteil k_i und Nachkommaanteil α_i. Mit $u := k_1 e_1 + \ldots + k_n e_n$, $z := \alpha_1 e_1 + \ldots + \alpha_n e_n$ gilt nun

$$x = z + u \tag{1.15}$$

wobei per Konstruktion $u \in T, z \in M$.
Das bedeutet aber gerade $x \in T_z$ für genau dieses z. Die Eindeutigkeit ergibt sich

folgendermaßen: Für ein weiteres Paar $\overline{u}, \overline{z}$ muss wegen (1.15) die Beziehung $x = z+u = \overline{z} + \overline{u}$ gelten. Weil die e_i eine Basis bilden sowie wegen der Wertebereiche von $u, \overline{u}$ und $z, \overline{z}$, muss $u = \overline{u}$ gelten und weiter $z = \overline{z}$. □

Lemma 1.6. Hat ein beschränktes $Y \subset \mathbb{R}^n$ die Eigenschaft, dass alle Translate von Y um Gitterpunkte von G paarweise disjunkt sind, in Formeln

$$z_0, z_1 \in G, z_0 \neq z_1 \quad \Longrightarrow \quad Y_{z_0} \cap Y_{z_1} = \emptyset$$

dann gilt $V(Y) \leq \Delta$.

Beweis: Sei T Grundmasche des Gitters G. Wegen vorheriger Proposition 1.2 gilt

$$V(Y) = \sum_{z \in G} V(Y \cap T_{-z}) = \sum_{z \in G} V(Y_z \cap T) \tag{1.16}$$

wobei wegen der Beschränktheit von Y nur endlich viele Summanden von (1.16) einen Beitrag liefern. Laut Voraussetzung sind die Y_z paarweise disjunkt, also auch die Mengen der Form $Y_z \cap T$. Obige Summe (1.16) ist also die Summe der Volumina paarweise disjunkter Teilmengen von T. Daher kann sie durch $V(T) =: \Delta$ nach oben abgeschätzt werden. □

Lemma 1.7 (Lemma von Minkowski)**.** : Sei G volles Gitter im $\mathbb{R}^n$ dessen Grundmasche Volumen Δ hat. Sei weiters X eine symmetrische, konvexe Menge mit Volumen $V(X)$. Dann impliziert $V(X) > 2^n \cdot \Delta$ die Existenz mindestens eines vom Nullvektor verschiedenen Elements von $X \cap G$.

Beweis: Betrachte für festes $z \in G$ die Menge der Form $(X/2)_z := \{X/2 + z, \quad z \in G\}$, jeweils mit Volumen $V((X/2)_z) = V(X)/2^n$. Diese können nicht paarweise disjunkt sein, denn laut Voraussetzung beziehungsweise vorigem Lemma 1.6 müsste $V(X) > 2^n \cdot \Delta \geq 2^n V((X/2)_z) = V(X)$ gelten, ein Widerspruch. Es muss also eine Gleichung gelten von der Form

$$\frac{1}{2}x_1 + z_1 = \frac{1}{2}x_2 + z_2, \quad (z_1, z_2 \in G, \quad z_1 \neq z_2, \quad x_1, x_2 \in X)$$

beziehungsweise

$$0 \neq z_1 - z_2 = \frac{1}{2}x_2 - \frac{1}{2}x_1 \tag{1.17}$$

Weil X nun symmetrisch ist, kann man die rechte Seite von (1.17) als $\frac{1}{2}x_2 + \frac{1}{2}(-x_1)$ mit $-x_1 \in X$ schreiben und wegen der Konvexität ist die ganze rechte Seite von (1.17) ebenfalls in X. Die vom Nullvektor verschiedene linke Seite von (1.17) liegt damit offenbar in $X \cap G$, was den Beweis beschließt. □

Korollar 1.2 (Minkowskis Lineraformen Satz)**.** Sei

$$L_j(x_1, \ldots x_n) = \sum_{i=1}^{n} a_{ij} x_i$$

eine Menge komplexwertiger Linearformen, die mit einer Form L auch die komplexkonjugierte $\overline{L}$ enthält. Sei M Gitter im $\mathbb{R}^n$ mit $D := |\det[a_{ij}]|$. Seien weiters $c_1, \ldots c_n$ positive Zahlen mit $\prod c_i \geq Dd(M)$ und sodass

$$L_i = \overline{L_j} \Rightarrow c_i = c_j$$

Dann gibt es einen von Null verschiedenen Punkt $(x_1, \dots x_n) \in M$, der

$$|L_1(x_1, \dots x_n)| \leq c_1, \qquad |L_j(x_j, \dots x_n)| < c_j, \quad (2 \leq j \leq n)$$

erfüllt.

1.5 Der Dirichletsche Einheitensatz

Nun haben wir alle nötigen Definitionen um einen tiefliegenden Satz anzugeben, der die Struktur der Einheiten in einem algebraischen Zahlkörper vollständig beschreibt.

Satz 1.7 (Dirichletscher Einheitensatz)**.** Sei K ein algebraischer Zahlkörper mit Erweiterungsgrad $n = s + 2t$ über den rationalen Zahlen und O_K sein Ganzheitsring. Dann exisitieren $r = s + t - 1$ Einheiten $\epsilon_1, \dots, \epsilon_r$ in O_K, sodass jede Einheit ϵ von O_K eine eindeutige Darstellung der Form

$$\epsilon = \zeta \epsilon_1^{a_1} \dots \epsilon_r^{a_r}$$

besitzt mit $a_i \in \mathbb{Z}$ und einer in O_K enthaltenen Einheitswurzel $\zeta \in \mathbb{C}$.

Bemerkung: Wegen $\{1, -1\} \in O_K$ ist obige Menge der Einheiten nichtleer.

Der Beweis ist stark geometrisch geprägt. Er benutzt die Darstellung von Elementen des Zahlkörpers in $\Lambda^{s,t}$ sowie auch mit Hilfe der Monomorphismen die erwähnte logarithmische Darstellung. Dort bilden diese eine diskrete Untergruppe des euklidischen Raumes $\mathbb{R}^n$ mit der üblichen Vektoraddition, und diese können allgemein als Gitter ausgewiesen werden. Das macht das Problem geometrisch angreifbar.

Zur Illustration der Aussage des Satzes ein Beispiel: Wir wollen die Einheitengruppe von $\mathbb{Q}(\sqrt{2})$ bestimmen. Offenbar ist $n = 2$, da $x^2 - 2 = 0$ das Minimalpolynom darstellt. Da Bilder von $\sqrt{2}$ unter den Monomorphismen sind $\sqrt{2}$,$-\sqrt{2}$. Es gibt also 2 reelle Monomorphismen, in der eingeführten Notation bedeutet das $s = 2$,$t = 0$ und folglich $r = s + t - 1 = 1$. Da die Erweiterung reell ist sind offensichtlich die einzigen Einheitswurzeln die stets vorhandenen ± 1. Die Einheiten des Ganzheitsringes von $\mathbb{Q}(\sqrt{2})$, welcher als $\mathbb{Z}$-Modul im übrigen die Form $\mathbb{Z}[\sqrt{2}]$ hat, sind also von der Form $\pm\epsilon^n$ fuer eine Grundeinheit ϵ und ein $n \in \mathbb{Z}$. In der Tat findet man als solche $3 - 2\sqrt{2}$ deren Inverses $3 + 2\sqrt{2}$ ist, also $(3 - 2\sqrt{2})(3 + 2\sqrt{2}) = 3^2 - 2 \cdot 2^2 = 1$.

Damit ist im wesentlichen die Theorie der *Pellschen Gleichung* gefunden, also die Frage nach allen ganzzahligen Lösungen von

$$x^2 - dy^2 = 1$$

mit quadratfreiem d, wenn man in obigem Beispiel $\mathbb{Q}(\sqrt{d})$ statt $\mathbb{Q}(\sqrt{2})$ betrachtet. Offen bleibt hier lediglich das Auffinden der Grundeinheit.

Kapitel 2

Dedekindringe und algebraische Grundlagen

Um die Struktur von algebraischen Zahlkörpern noch besser zu verstehen, untersucht man ihre Ganzheitsringe auf deren Idealstruktur. Die Ganzheitsringe sind stets sogenannte Dedekindringe und selbige erlauben eine eindeutige Faktorisierung von Idealen in Primideale. Diese Korrelation führt in natürlicher Weise zum Begriff der Idealklassengruppe und Klassenzahl, deren Endlichkeit Grundlage der analytischen Sichtweise auf algebraische Zahlkörper ist.

2.1 Algebraische Grundlagen

Definition 2.1 (ACC)**.** Ein Modul erfüllt die *aufsteigende Kettenbedingung (ACC)* falls jede aufsteigende Untermodulkette stationär wird, also aus $A_1 \subset A_2 \subset A_3 \ldots$ folgt bereits $A_i = A_n$ für ein n und alle $i \geq n$. Solche Moduln heißen *noethersch.*

Diese Definition lässt sich einfach auf Ringe und Ideale übertragen, da Ideale ja genau die Untermodule von Ringen sind.

Definition 2.2 (Noetherscher Ring)**.** Ein Ring heit *noethersch*, wenn jede Idealkette die *ACC* erfüllt.

Definition 2.3. Für eine Ringerweiterung $R \subset S$ heißt

$$\widehat{R} := \{s \in S : s \quad ganz \quad über \quad R\} \subset S$$

der ganze Abschluss von R in S. Gilt $\widehat{R} = R$ so heißt R *ganzabgeschlossen in* S. Ist zusätzlich S der Quotientenkörper von R, so heißt R *ganzabgeschlossen.*

Beispielsweise gilt:

1. $\mathbb{Z}$ ist ganz abgeschlossen in $\mathbb{Q}$, aber nicht in $\mathbb{C}$ (wegen $i^2 + 1 = 0$).
2. Faktorielle Ringe sind ganzabgeschlossen.
   Denn hätte man eine Gleichung

$$a_0 + a_1(\frac{a}{b}) + \ldots + a_{n-1}(\frac{a}{b})^{n-1} + (\frac{a}{b})^n = 0, \quad a_j \in R \tag{2.1}$$

mit $\frac{a}{b}$ im Quotientenkörper K eines faktoriellen Ringes R mit $a, b \in R$ teilerfremd, so sieht man durch Multiplikation von (2.1) mit b^n, dass b keine echten Teiler haben kann, also $b = 1$ gelten muss.

3. $K[x_1, \ldots, x_n]$ ist für jeden Körper K ganzabgeschlossen.

Offenbar ist der Ganzheitsring O_K eines Zahlkörpers K exakt der ganze Abschluss von $\mathbb{Z}$ in K. Dies wird der für uns weiterführend interessante Spezialfall folgender Sätze sein.

Definition 2.4 (Primideal)**.** Ein Ideal eines Ringes R heißt *Primideal*, falls für alle Ideale A, B gilt

$$AB \subset P \Rightarrow A \subset P \quad \textit{oder} \quad B \subset P$$

Satz 2.1. Ein Ideal P eines kommutativen Ringes R ist genau dann Primideal, wenn für alle $a, b \in R$ gilt

$$a \cdot b \in P \Rightarrow a \in P \quad \textit{oder} \quad b \in P$$

Beweis: Seien A, B Ideale mit $AB \subset P$ und $A \nsubseteq P$, so exisitert also ein $a \in A \setminus P$. Für jedes $b \in B$ gilt $ab \in AB \subset P$, also $b \in P$ weil $a \notin P$. Daher $B \subset P$, also ist P Primideal. Falls umgekehrt P irgendein Ideal und a, b Elemente mit $ab \in P$, dann ist das erzeugte Hauptideal (ab) in P enthalten. In kommutativen Ringen gilt aber $(a)(b) \subset (ab)$, also $(a)(b) \subset P$. Wenn nun P Primideal ist folgt $(a) \subset P$ oder $b \subset P$, insbesondere $a \in P$ oder $b \in P$. □

Definition 2.5 (maximales Ideal)**.** Ein echtes Ideal A eines Ringes R heißt *maximales Ideal*, wenn es für jedes Ideal B gibt mit $A \subset B \subset R$ bereits $B = A$ oder $B = R$ gilt.

Bemerkung: Jedes maximale Ideal ist Primideal in einem kommutativen Ring mit Einselement. Die Umkehrung muss extra gefordert werden.

2.2 Dedekindringe

Definition 2.6 (Dedekindring)**.** Ein *Dedekindring* ist ein noetherscher, ganzabgeschlossener Integritätsbereich in dem jedes von 0 verschiedene Primideal ein maximales Ideal ist und der kein Körper ist.

Um das Hauptresultat dieses Abschnitts herzuleiten bedarf es einiger Lemmata.

Lemma 2.1. Sei A noetherscher Ring. Dann enthält jedes Ideal $J \triangleleft A$ ein Produkt von vom Nullideal verschiedenen Primidealen.

Beweis: Weil A noethersch ist kann man J als maximales Gegenbeispiel wählen, so existent. Da J selbst nicht prim sein kann, exisitieren $a, b \in A$ mit $ab \in J$ und $a \notin J$, $b \notin J$. Die Ideale $J + (a)$, $J + (b)$ sind echt größer als J aber ihr Produkt ist in J. Da J als maximale Gegenbeispiel gewählt ist, müssen die Ideale $J + (a)$, $J + (b)$ ein Produkt von Primidealen enthalten und daher aber auch ihr Produkt J, ein Widerspruch. □

Definition 2.7. Zwei Ideale A, B eines Ringes R heißen relativ prim, wenn $A + B = R$ gilt.

Lemma 2.2. Sei A ein Ring und I, J zwei relativ prime Ideale und m, n natürliche Zahlen. Dann sind I^n und J^m relativ prim.

Beweis: Wären I, J nicht relativ prim, dann wären sie in einem Primideal P (sogar maximalen Ideal) enthalten. Wenn aber ein Primideal eine Potenz eines Elements enthält, so enthält sie sschon das Element selbst, wie aus der Charakterisierung aus Satz 2.1 mit einfacher Induktion folgt. Also folgt aus $I^n \lhd P$ bereits $I \lhd P$ sowie aus $J^m \lhd P$ bereits $J \lhd P$. Das widerspricht der Tatsache, dass die Ideale relativ prim sind. □

Man beachte, dass dieses Lemma unmittelbar auf Dedekindringe angewendet werden kann. Weil jedes Primideal maximal ist, folgt dass zwei verschiedene Primideale relativ prim sind. Daher sind Potenzen von relativ primen Primidealen in Dedekindringen wiederum relativ prim.
Für nachstehendes Lemma benötigen wir noch eine Begirffsbildung:

Definition 2.8 (Lokalisierung)**.** Sei A ein Integritätsbereich mit Quotientenkörper K. Eine Menge $S \subset A$ heißt multiplikativ, falls $0 \notin S, 1 \in S$ und sie unter Ringmultiplikation abgeschlossen ist. Für solches S definiert man einen Unterring von K durch

$$S^{-1}A := \{\frac{a}{b} \in K : b \in S\}$$

Ist speziell P Primideal von A, so ist $S_P := A \setminus P$ multiplikativ. Wir schreiben kurz A_P für $S_P^{-1}A$.

Beispielsweise gilt $\mathbb{Z}_{(p)} := \{\frac{m}{n} : p \nmid n\}$.

Lemma 2.3. Sei A ein Integritätsbereich und S eine multiplikative Teilmenge von A. Zu einem Ideal $J \lhd A$ ist klarerweise $S^{-1}J \lhd S^{-1}A$. Dieses Ideal $S^{-1}J$ sei mit J^* bezeichnet. Umgekehrt sei für $J \lhd S^{-1}A$ das Ideal $J \cap A$ als J° bezeichnet. Dann gilt:

$$J^{\circ *} = J \quad \textit{für} \quad \textit{alle} \quad J \lhd S^{-1}A \tag{2.2}$$

$$J^{*\circ} = J \quad \textit{für} \quad \textit{alle} \quad \textit{Primideale} \quad J \lhd A \quad \textit{mit} \quad A \cap S = \emptyset \tag{2.3}$$

Beweis: Um (2.2) zu zeigen sei $J \lhd S^{-1}A$. Wegen $A \cap J \lhd J$ und $J \lhd S^{-1}A$ folgt offenbar $(J \cap A)^* \lhd J$. Für die andere Richtung sei $b \in J$ beliebig gewählt. Dieses b besitzt eine Darstellung $b = \frac{a}{s}$ mit $a \in A$, $s \in S$. Daraus ergibt sich $a = s \cdot (\frac{a}{s}) \in A \cap J$, folglich $\frac{a}{s} = \frac{s \cdot \frac{a}{s}}{s} \in (A \cap J)^*$. Für die zweite Gleichung (2.3) sei P zu S disjunktes Primideal. Die Inklusion $P \subset A \cap (S^{-1}P)$ ist wieder trivial weil $1 \in S$. Für die Umkehrung sei $(\frac{a}{s}) \in S^{-1}P \cap A$, $a \in P, s \in S$. Es gilt $\frac{a}{s} \cdot s = a \in P$. Nun sind aber sowohl as als auch s in A und weil P Primideal ist, muss zumindest einer der Ausdrücke in P sein. Weil $S \cap P = \emptyset$ folgt $\frac{a}{s} \in P$. □

Dieses Lemma war vorbereitend für folgendes Ergebnis:

Lemma 2.4. Sei A ein Integritätsbereich und S eine multiplikative Teilmenge von A. Dann ist die Abbildung

$$P \longmapsto P^* := P \cdot (S^{-1}A)$$

eine Bijektion zwischen der Menge der zu S disjunkten Primideale von A auf die Primideale in $S^{-1}A$. Ihre Inverse ist durch

$$P \longmapsto P \cap A$$

gegeben.

Beweis: Man überzeugt sich schnell, dass die Abbildungen $P \longmapsto P^*$ und ihre im Lemma formulierte Inverse die richtigen Zielmengen haben. Aufgrund vorangehenden Lemmas 2.3 ist die Zuordnung sogar bijektiv. □

Satz 2.2. Sei P ein maximales Ideal eines Ringes A und Q das in A_P via $Q = P \cdot A_P$ erzeugte Ideal $Q \lhd P \cdot A_P$. Dann definiert die Abbildung

$$\Phi : A/P^m \longmapsto A/Q^m$$

$$a + P^m \longmapsto a + Q^m$$

einen Isomorphismus auf den Faktorringen.

Beweis: Die Abbildung ist wohldefiniert, man muss also Injektivität und Surjektivität nachprüfen. Für ersteres ist $Q^m \cap A = P^m$ nachzurechnen. Aufgrund von $S^{-1}Q^m = P^m$ ist also gleichwertig $P^m = (S^{-1}P^m) \cap A$ zu zeigen. Ein Element $a \in S^{-1}P \cap A$ kann geschrieben werden als $a = \frac{b}{s}, b \in P^m, s \in S$, daher

$$sa \in P^m \quad \Longrightarrow \quad sa = 0 \quad in \quad A/P^m \tag{2.4}$$

Weil das einzige maximale Ideal in P^m gleich P ist das einzige maximale Ideal in A/P^m gleich P/P^m, selbiger Faktorring ist also ein lokaler Ring (siehe kommende Definition 2.9). Da das Element $s+P^m \notin P/P^m$ muss es also eine Einheit sein in A/P^m. Daher folgt aus der Gleichung (2.4) bereits $a = 0$ in A/P^m, also $a \in P^m$. Damit ist die Injektivität gezeigt.
Um die Surjektivität zu zeigen kann man wie folgt argumentieren: Sei $\frac{a}{s} \in A_P$ wie oben. Wegen $s \notin P$ und P maximal, muss $(s)+P = A$ gelten und (s) und P sind relativ prime Ideale. Daher sind auch (s) und P^m relativ prim nach Lemma 2.2. Es exisiteren weiter also $b \in A, q \in P^m$ mit $b \cdot s + q = 1$. Dieses b bildet auf s^{-1} ab aufgefasst als Element von A_P^m und damit ist das Bild von ab genau $\frac{a}{s}$. Wegen der Beliebigkeit des Elements $\frac{a}{s} \in A_P$ ist die Abbildung surjektiv. □

Definition 2.9. Ein lokaler Ring ist ein kommutativer Ring mit 1 mit eindeutigem bezüglich Inklusion maximalem Ideal.

Lemma 2.5. Ein kommutativer Ring R mit 1 ist genau dann lokal wenn alle Nichteinheiten von R ein Ideal bilden. Insbesondere besteht in einem lokalen Ring mit maximalem Ideal J die Menge $R \setminus J$ nur aus Einheiten.

Beweis: Bezeichne die Einheiten von R mit R^*. Es ist leicht einzusehen, daß ein Ideal $J \lhd R$ genau dann ein echtes Ideal des Ringes ist, wenn es nur aus Nichteinheiten besteht, da mit $a \in J$ das ganze erzeugte Hauptideal $(a) \in J$ enthalten ist. In logischen Quantoren schreibt sich diese Überlegung als

$$J \lhd R, a \in J \Rightarrow (a) \lhd J$$

$$\Rightarrow (J \neq R \Leftrightarrow J \quad besteht \quad nur \quad aus \quad Nichteinheiten)$$

Mögen die Nichteinheiten R/R^* ein Ideal bilden. Dann ist R/R^* natürlich das eindeutig maximale Ideal nach obiger Überlegung.
Sei umgekehrt $a \in R/R^*$, sodass $(a) \neq R$. Dann ist (a) im maximalen Ideal M des Rings enthalten. Es existiert also zu jedem $a \in R/R^*$ ein Ideal $J_a \triangleleft M$. Dann ist die Vereinigung aller dieser J_a das eindeutige Ideal das per Konstruktion alle Nichteinheiten enthält, und weil alle $J_a \triangleleft M$ gilt das auch für die Vereinigung, es kommen also keine Einheiten in der Vereinigung vor. Damit Enthält das konstruierte Ideal also genau die Nichteinheiten. □

Als letzten standardalgebraischen Satz benötigen wir noch den chinesischen Restsatz, der besagt, dass ein System linearer Kongruenzen stets eine im wesentlichen eindeutige Lösung besitzt.

Satz 2.3 (Chinesischer Restsatz)**.** Seien $J_1, J_2, \ldots, J_n$ paarweise relativ prime Ideale eines Ringes A. Dann gibt es für alle $x_1, x_2, \ldots, x_n \in A$ eine gemeinsame Lösung $x \in A$ des Systems

$$x \equiv x_i \pmod{J_i}$$

Die Menge aller Lösungen ist gegeben durch $\{x + a : \quad a \in \cap J_i\}$, also ist x eindeutige Lösung modulo $\cap J_i$.

Beweis: Betrachte zuerst den Fall $n = 2$. Wegen $J_1 + J_2 = A$ gibt es Lösungen zu $a_1 + a_2 = 1, \quad a_i \in J_i$. Das Element $x = a_1x_2 + a_2x_1$ leistet beide Kongruenzen. Im allgemeinen Fall kann man induktiv auch von Lösungen von

$$a_i + b_i = 1, \quad a_i, b_i \in J_i, \quad i \geq 2$$

ausgehen (beachte $i \geq 2$). Das Produkt aller dieser $(a_i + b_i)$ ist 1 und liegt in $J_1 + \prod_{i\geq 2} J_i$, also

$$J_1 + \prod_{i\geq 2} J_i = A$$

Auf die beiden Ideale J_1 , $\prod_{i\geq 2} J_i$ kann man die bewiesene Behauptung des Falles $n = 2$ anwenden und bekommt eine Lösung y_1 zu

$$y_1 \equiv 1 \pmod{J_1}, \qquad y_1 \equiv 0 \pmod{\prod_{i\geq 2} J_i} \tag{2.5}$$

Klarerweise folgt aus (2.5), dass $y_1 \equiv 0 \pmod{J_i}, i \geq 2$. Ebenso sind alle anderen Systeme

$$y_k \equiv 1 \pmod{J_k}, \qquad y_k \equiv 0 \pmod{J_i}, \quad i \neq k$$

lösbar in y_k. Das Element $x = \sum_{i=1}^{n} x_i y_i$ ist das gesuchte x.
Es ist noch zu zeigen, dass

$$\cap J_i = \prod J_i \tag{2.6}$$

Allgemeingültig ist die Inklusion $J_1 J_2 \ldots J_n \subset J_1 \cap J_2 \ldots J_n$ für jedwede Ideale. Für die Umkehrung sei wieder erst $n = 2$ und

$$a_1 + a_2 = 1, \quad a_i \in J_i$$

Für $d \in J_1 \cap J_2$ ist $d = da_1 + da_2 \in J_1 \cdot J_2$. Sei die Aussage gültig bis $n-1$, also oBdA $\cap_{i\geq 2} J_i = \prod_{i\geq 2} J_i$. Wie oben gezeigt sind J_1 und $\prod_{i\geq 2} J_i$ relativ prim, also kann man wieder den Fall $n = 2$ bemühen und erhält

$$\prod_{i\geq 1} J_i = J_1 \cdot (\prod_{i\geq 2} J_i) = J_1 \cap (\prod_{i\geq 2} J_i) = \bigcap_{i\geq 1} J_i$$

was (2.6) zeigt. □

Jetzt können wir die Hauptaussage dieses Abschnitts beweisen.

Satz 2.4. Sei A ein Dedekindring. Dann besitzt jedes echte Ideal $J \triangleleft A$ eine eindeutige Faktorisierung in Primideale P_i, also erlaubt eine eindeutige Darstellung der Gestalt

$$J = P_1^{r_1} P_2^{r_2} \cdots P_n^{r_n}$$

Beweis: Nach Lemma 2.1 existiert zu jedem $J \triangleleft A$ ein $G \triangleleft J$ der Form

$$G = P_1^{r_1} P_2^{r_2} \cdots P_m^{r_m}$$

mit paarweise verschiedenen P_i. Wir erhalten weiter aus dem erarbeiteten

$$A/G \cong A/P_1^{r_1} \cdot A/P_2^{r_2} \ldots A/P_m^{r_m} \cong A_{P_1}/Q_1^{r_1} \cdot A_{P_2}/Q_2^{r_2} \ldots A_{P_m}/Q_m^{r_m}$$

wobei $Q_i = P_i A_{P_i}$ das eindeutige maximale Ideal in A_{P_i} ist.
Dabei ist der erste Isomorphismus eine Anwendung des chinesischen Restsatzes und Lemma 2.2 und der zweite in Satz 2.2 begründet. Das Bild von J/G unter diesem Isomorphismus ist

$$Q_1^{s_1}/Q_1^{r_1} \cdot Q_2^{s_2}/Q_2^{r_2} \ldots Q_m^{s_m}/Q_m^{r_m}$$

mit gewissen $s_i \leq r_i$. Weil dieses Ideal auch das Bild von $P_1^{s_1} P_2^{s_2} \ldots P_m^{s_m}$ ist unter Isomorphismus, gilt

$$J = P_1^{s_1} P_2^{s_2} \ldots P_m^{s_m}$$

in A/G. Da aber beide Ideale G enthalten und wegen der eindeutigen Korrelation zwischen Idealen von A die G enthalten und Idealen im Faktor A/G muss schließlich

$$J = P_1^{s_1} \cdot P_2^{s_2} \ldots P_m^{s_m}$$

gelten. Fehlt noch die Eindeutigkeit.
Seien also 2 verschiedene Darstellungen eines Ideals gegeben durch

$$J = P_1^{s_1} P_2^{s_2} \ldots P_m^{s_m} = P_1^{t_1} P_2^{t_2} \ldots P_m^{t_m}$$

wobei man hierbei $s_i = 0$ bzw $t_i = 0$ zulässt, sodass obige Darstellung keine Einschränkung darstellt. Im Existenzbeweis wurde gezeigt, dass mit obigen Bezeichnungen

$$Q_i^{s_1} = J \cdot A_{P_i} = Q_1^{t_i}$$

also $s_i = t_i$ für alle i. □

Korollar 2.1. Ein von Null verschiedenes Ideal I eines Dedekindringes kann nur von endlich vielen verschiedenen Idealen geteilt werden.

Beweis: Wegen der eindeutigen Darstellung von I als Produkt von Primidealen P_i zur Potenz a_i muss jeder Teiler offenbar die selbe Gestalt mit Potenzen $b_i \leq a_i$ haben. Dabei ergeben sich offenbar endlich viele Kombinationsmöglichkeiten. □

Bemerkung: Das bedeutet nicht, dass jedes Element eines Dedekindringes eine eindeutige Primfaktorzerlegung besitzt.

Bemerkung: Es gilt auch die Umkehrung des Satzes. Aus der eindeutigen Primidealzerlegung folgt, dass ein Integritätsbereich die Zusatzbedingungen für einen Dedekindring erfüllt.

Lemma 2.6. Ist $I = \prod P_i^{t_i}$ Ideal eines Dedekindringes, dann gilt

$$R/I \cong \oplus R/P_i^{t_i}$$

Beweis: Betrachte den Homomorphismus

$$f : R \longmapsto \oplus R/P_i^{t_i}$$

$$f(x) = [x \pmod{P_i^{t_i}}]_i$$

Nach dem chinesischen Restsatz ist f surjektiv, und für $x \in \ker(f)$ gilt notwendigerweise $x \in \cap_i P_i^{t_i}$, also $\ker(f) \subset I$ wegen der Beliebigkeit von x. Klarerweise aber auch $I \subset \ker(f)$, also ist unser Homomorphismus auch injektiv. □

Zum Abschluss noch ein Resultat auf das wir später zurückgreifen.

Proposition 2.1. Sei P von Null verschiedenes Primideal eines Dedekindringes R und $n \in \mathbb{N}$, dann haben die Faktorringe R/P und P^n/P^{n+1} isomorphe additive Gruppen.

Beweis: Bezeichne die additiven Gruppen mit $R^{\oplus}$ bzw $P^{n\oplus}$. Für $a \in P^n \setminus P^{n+1}$ definiere

$$g_a : R^{\oplus} \longrightarrow P^{n\oplus}$$

$$x \longrightarrow ax$$

Wegen $g_a(P) \subset P^{n+1}$ induziert g_a einen Homomorphismus $\overline{g_a}$ zwischen den additiven Gruppen $(R/P)^{\oplus}$ und $(P^n/P^{n+1})^{\oplus}$. Wir müssen zeigen, dass $\overline{g_a}$ bijektiv ist. Sei also $\overline{x} \in \ker(\overline{g_a})$, dann gilt für jedes $x \in \overline{x}$, dass $ax \in P^{n+1}$ und weiter $x \in P$. Daraus ergibt sich wieder $\overline{x} = 0$.
Für die Surjektivität, sei $\overline{y} \in P^n/P^{n+1}$ und y aus der Klasse von $\overline{y}$. Weil $(aR, P^{n+1}) = P^n$ ist die Kongruenz $ax \equiv y \pmod{P^{n+1}}$ lösbar, und für die Klasse $\overline{x}$ von x gilt $\overline{g_a}(\overline{x}) = \overline{y}$.
□

2.3 Ganzheitsringe von algebraischen Zahlkörpern sind Dedekindringe

Um die im letzten Abschnitt erarbeitete Theorie zu verwenden, weisen wir nach, dass Ganzheitsringe von algebraischen Zahlkörpern stets Dedekindringe sind. Es werden nun 3 Sätze vorgestellt, die im wesentlichen die drei Eigenschaften eines Dedekindringes im nachfolgenden Satz nachprüfen. Dieser impliziert die Hauptaussage des Abschnitts als einfaches Korollar. Der erste dieser Sätze sei ohne den detailreichen Beweis angegeben.

Satz 2.5. Sei A ganzabgeschlossener Integritätsbereich mit Quotientenkörper K und B der ganze Abschluss von A in einer algebraischen Körpererweiterung L von K. Dann existiert ein freier A-Untermodul G von L mit $B \subset G$.

Der Beweis findet sich in [Mi1], Proposition 2.29, wobei auf einige andere Resultate verwiesen wird.

Satz 2.6. Sei A Integritätsbereich und K sein Quotientenkörper. Dann ist der ganze Abschluss von A in einer algebraischen Körpererweiterung L von K ganzabgeschlossen.

Um dies zu beweisen bedienen wir uns dreier Lemmata:

Lemma 2.7. Seien $A \subset B \subset C$ Ringe, sodass B endlich erzeugt als A-Modul und C endlich erzeugt über B-Modul ist. Dann ist C endlich erzeugt als A-Modul.

Beweis: Seien $\{\beta_1, \dots b_m\}$ die Erzeuger von B als A-Modul und $\{\gamma_1, \dots, \gamma_n\}$ die Erzeuger von C als B-Modul, dann ist $\{\beta_i\gamma_j : 1 \leq i \leq m, 1 \leq j \leq n\}$ Erzeugermenge von C als A-Modul. □

Lemma 2.8. Wenn B ganz über A ist und endlich erzeugt als A-Algebra ist, dann ist B bereits endlich erzeugt als A-Modul.

Beweis: Betrachte zunächst den Fall, dass B als A-Algebra von einem Element erzeugt wird, also $B = A[\beta]$. Dann hat jedes Element von B eine Darstellung der Form

$$b_0 + b_1\beta + \ldots + b_N\beta^N, \quad b_i \in A \tag{2.7}$$

Weil β ganz über A ist erfüllt es nun eine Ganzheitsgleichung

$$a_0 + a_1\beta + \ldots + a_{n-1}\beta^{n-1} + \beta^n = 0, \quad a_i \in A$$

Man kann also β^n als Linearkombination von niedrigeren Potenzen schreiben, daher hat jedes Element der A-Algebra B sogar schon eine Darstellung als

$$b_0 + b_1\beta + \ldots + b_{n-1}\beta^{n-1}, \quad b_i \in A$$

also $N \leq n-1$ in (2.7). Das bedeutet aber gerade, dass bereits $1, \beta, \ldots, \beta^{n^-1}$ endliches Erzeugendensystem für B als A-Modul sind.
Der allgemeine Fall folgt induktiv. Sei $\beta_1, \ldots, \beta_n$ Erzeugendensystem von B aufgefasst als A-Algebra und betrachte

$$A \subset A[\beta_1] \subset A[\beta_1][\beta_2] \subset \ldots \subset A[\beta_1][\beta_2]\ldots[\beta_n] = B$$

Jeder Term in der Kette ist endlich erzeugt als Modul bezüglich seines Vorgängerterms (also zum Beispiel $A[\beta_1][\beta_2]$ ist endlich erzeugt aufgefasst als A-Modul über $A[\beta_1]$), denn β_{k+1} ist stets ganz über β_k. Lemma 2.7 induktiv angewandt schließt den Beweis. □

Lemma 2.9. Seien $A \subset B \subset C$ Integritätsbereiche. Wenn B ganz über A ist und C ganz über B, dann ist C auch ganz über A.

Beweis: Sei $\beta \in C$ mit zugehöriger Minimalgleichung

$$\beta^n + a_{n-1}\beta^{n-1} \ldots + b_0 = 0, \quad b_i \in B$$

Sei $B^* := A[b_1, \ldots, b_n]$. Nach vorangehendem Lemma 2.8 ist B^* als A-Modul endlich erzeugt, und β ganz über B^*. Folglich ist $B^*[\beta]$ endlich erzeugt als A-Modul. Wegen $\beta B^*[\beta] \subset B^*[\beta]$ ist nach der allgemeineren Aussage von Lemma 1.1 β ganz über A. □

Der Beweis von Satz 2.6 ist nun einfach.

Beweis: Sei B der ganze Abschluss von A in L und C der ganze Abschluss von B in L. Dann ist nach letztem Lemma C ganz über A, und daher $C \subset B$. □

Bemerkung: Dies rechtfertigt erst den Ausdruck "ganzer Abschluss".

Satz 2.7. Enthält ein Integritätsbereich B einen Körper K und ist algebraisch über K, dann ist B schon ein Körper.

Beweis: Sei $0 \neq \beta \in B$ beliebig. Da β algebraisch über K ist, ist $[K[\beta] : K] = n$ eine endliche Körpererweiterung, also $K[\beta]$ endlichdimensionaler Vektorraum über K. Die Abbildung

$$\Sigma_\beta : K[\beta] \longmapsto K[\beta]$$

$$x \longmapsto \beta \cdot x$$

ein Endomorphismus, der zudem injektiv ist weil B nullteilerfrei vorausgesetzt ist. Damit muss Σ_β aber bijektiv sein, wie aus der linearen Algebra bekannt ist. Also ist $\beta \cdot x = 1$ lösbar in $K[\beta] \subset B$. Wegen der Beliebigkeit von β ist B ein Körper. □

Satz 2.8. Sei A ein Dedekindring mit Quotientenkörper K und B der ganze Abschluss von A in einer separablen, endlichdimensionalen Körpererweiterung von K. Dann ist B ebenfalls Dedekindring.

Beweis: Wir weisen die 3 definierenden Eigenschaften von Dedekinringen nach. Die Ganzabgeschlossenheit wurde separat in Satz 2.6 bewiesen. Wie bereits in Satz 2.5 angemerkt, ist B in einem endlich erzeugten A-Modul enthalten. Daher ist jedes Ideal von B als A-Modul endlich erzeugt und daher erst recht als B-Modul. Daher ist also auch jedes Ideal endlich erzeugt und B noethersch. Nun zeigen wir, dass jedes Primideal Q von B maximal ist.
Sei $0 \neq \alpha \in Q$. α ist ganz über A, erfüllt also eine Gleichung

$$\alpha^n + \ldots + \alpha a_1 + a_0 = 0, \quad a_i \in A$$

mit $a_0 \neq 0$. Wegen $a_0 \in \alpha B \cap A$ ist $Q \cap (\alpha) \neq (0)$. Als Primideal ist $P := Q \cap A$ aber auch maximal in A(Dedekindring), also ist nach einem algebraischen Standardresultat A/P ein Körper, sowie B/Q ein Integritätsring. Betrachte die Abbildung

$$\Phi : A/P \longmapsto B/Q$$

$$a + P \longmapsto a + Q$$

Das Bild dieser Abbildung ist ein Teilkörper des Integritätsbereichs B/Q isomorph zu A/P. Weil B ganz über A ist, ist B/Q algebraisch über A/P. Wegen Satz 2.7 ist B/Q sogar Körper und daher Q maximales Ideal von B wie gefordert. □

Korollar 2.2. Der Ganzheitsring eines algebraischen Zahlkörpers ist ein Dedekindring. Insbesondere gibt es eine eindeutige Zerlegung von Idealen in Primideale.

Beweis: Setze $A = \mathbb{Z}$ in Satz 2.8 und beachte, dass einerseits $\mathbb{Z}$ Dedekindring ist, weil es sogar ein Hauptidealring ist, und dass wegen Satz 1.4 die Separabilitätsbedingung gewährleistet ist. □

Bemerkung: Obig verwendete Implikation, dass Hauptidealringe stets Dedekindringe sind, ist allgemein gültig. Für den Spezialfall $\mathbb{Z}$ im Korollar sind alle defininierdenden Bedingungen eines Dedkindringes unmittelbar nachprüfbar, weshalb der allgemeine Beweis hier ausgelassen sei. Tatsächlich ist der Fall, dass Ganzheitsringe von Zahlkörpern Hauptidealringe sind, wünschenswert da genau in diesem Fall eine eindeutige Primfaktorzerlegung vorherrscht, wie abschließend bewiesen wird. Es wird sich aber herausstellen, dass Ganzheitsringe im allgemeinen keine Hauptidealringe sind, wodurch dann noch besser der Grund für die Einführung des Begriffs Dedekindring ersichtlich wird.

Lemma 2.10. In einem noetherschen Integritätsbereich kann jedes Element als Produkt von irrdeuziblen Ringelementen geschrieben werden. Dabei heißt ein Element a irreduzibel, wenn aus $a = bc$ folgt, dass b oder c eine Einheit ist.

Beweis: Wir verwenden dabei den Dualismus zwischen Teilbarkeit und Idealen gegeben durch

$$(a) \subset (b) \Longleftrightarrow b|a$$

$$(a) = (b) \Longleftrightarrow b = a$$

Sei nun a ein Gegenbeispiel, sodass (a) in keinem echt größeren Ideal (d) enthalten ist, sodass d ebenfalls keine solche Faktorisierung enthält. Dabei wurde noethersch verwendet. Das Element a kann nicht selbst irreduzibel sein, also hat es eine Darstellung $a = b \cdot c$ mit Nichteinheiten b, c. Also $(a) \subsetneq (b)$ und $(a) \subsetneq (c)$. Wegen der Maximalitätsaussage müssen nun aber b und c eine Zerlegung in irreduzible Elemente besitzen, und damit aber auch ihr Produkt a, ein Widerspruch.

□

Satz 2.9. Ein Dedekindring, der gleichzeitig faktorieller Ring ist, ist automatisch schon ein Hauptidealring.

Beweis: Sei A Dedekindring mit eindeutiger Primfaktorzerlegung. Es reicht wegen der eindeutigen Faktorisierung von Idealen in Primideale aus nachzuweisen, dass jedes Primideal P ein Hauptideal ist. Sei $0 \neq a \in P$. Dann besitzt a wegen Lemma 2.10 eine Faktorisierung in irreduzible Elemente, von denen einer in P enthalten sein muss (weil P Primideal ist). Nenne diesen Π. Es gilt nun $0 \subset (\Pi) \subset P$. Außerdem ist (Π) Primideal, weil Π irreduzibel ist. Weil jedes Primideal in einem Dedekindring maximal ist, muss bereits $(\Pi) = P$ gelten. Jedes Primideal ist also Hauptideal. □

Bemerkung: Die Tatsache, dass Hauptidealringe immer faktoriell sind, sei hier nochmals erwähnt. Die Beweisidee ist dabei ähnlich wie der Nachweis, dass Hauptidealringe stets noethersch sind. Nach letzter Bemerkung ist also die Umkehrung des Satzes ebenso korrekt.

Bemerkung: Bemerkenswerterweise ist Lemma 2.9 falsch für den Ganzheitsring von $\overline{\mathbb{Q}}$. Dieser ist insbesondere nicht noethersch.

Kapitel 3

Die Idealklassengruppe und die Klassenzahl

3.1 Definitionen

In diesem Abschnitt bezeichne stets R einen Dedekindring und K sein Quotientenkörper.

Definition 3.1 (gebrochenes Ideal)**.** Ein R-Modul I von K, sodass $aI \in R$ für ein von Null verschiedenes $a \in R$, heißt *gebrochenes Ideal*. Ist I zusätzlich Hauptideal, also von der Form aR, so heißt I gebrochenes Hauptideal. Das Produkt zweier gebrochener Ideale ist gegeben durch

$$IJ := \{a_1b_1 + \ldots + a_mb_m : a_i \in I, b_i \in J, m \in N\}$$

Diese Definition vom Produkt gebrochener Ideale führt nicht aus selbiger hinaus und ist daher wohldefiniert. Dies sieht man so ein:
Seien I, J R-Moduln und $0 \neq x, y \in R$ mit $xI \subset R$, $yJ \subset R$ und a_i, b_i gegeben. Die Gleichung

$$(xy)a = \sum_{i=1}^{m}(xa_i)(yb_i) \in R$$

zeigt, dass $z := xy$ ein Element ist, das der Bedingung $z(IJ) \in R$ genügt.

Die Menge der gebrochenen Ideale bildet klarerweise mit oben definiertem Komplexprodukt eine kommutative Halbgruppe mit Einselement R.

Proposition 3.1. Sei I gebrochenes Ideal. Dann ist auch

$$I^* := \{x \in K : xI \subset R\}$$

ein gebrochenes Ideal.

Beweis: I^* ist zunächst ein von Null verschiedener R-Modul. Seien $0 \neq y \in I$ und $0 \neq r \in R$ beliebig. Dann liegt ry in $R \cap I$ (beachte dass im Allgemeinen $R \nsubseteq I$) und für alle $a \in I^*$ ist $ary \in R$ wie gefordert. □

Definition 3.2 (invertierbares gebrochenes Ideal)**.** Die Inklusion $II^* \subset R$ ist klar. Gilt Gleichheit, so heißt das Ideal I *invertierbar* mit inversem Ideal $I^{-1} := I^*$

Proposition 3.2. Jedes gebrochene Hauptideal ist invertierbar, und die Menge aller invertierbaren Ideale von R bildet eine Gruppe $G(K)$ mit der Multiplikation. Wir nennen sie die *Idealgruppe von K.*

Beweis: Ist $I = aR$ Hauptideal, dann gilt $I^* = a^{-1}R$ und das ist offensichtlich ein zu I inverses Ideal. Klarerweise ist das Produkt invertierbarer Ideale wieder invertierbar nach der Regel $(IJ)^{-1} = J^{-1}I^{-1}$. Ebenso ist $(I^{-1-1}) = I$ klar. Wir zeigen noch, dass $IJ = R$ impliziert, dass $J = I^{-1}$. Dabei gilt $J \subset I^*$ nach Definition. Daraus folgt

$$R = IJ \subset II^* \subset R$$

also $II^* = R$. Zusammen mit $I^* = I^*R$ erhält man die Kette $I^* = I^*R = I^*IJ = RJ = J$. □

In Dedekindringen sind stets alle gebrochenen Ideale invertierbar, die invertierbaren Ideale bilden also ein Gruppe. Auf dieses Resultat steuern wir jetzt mithilfe einiger Ergänzungen zum vorigen Abschnitt zu.

Lemma 3.1. Seien $0 \neq J \subset I$ zwei Ideale eines Dedekindringes R. Dann ist $I = J + (a)$ für ein $a \in R$.

Beweis: Wegen der Inklusion kann man die Ideale wieder gegeben annehmen als

$$J = P_1^{r_1} \dots P_m^{rm}, \quad I = P_1^{s_1} \dots P_m^{sm}, \quad 0 \leq r_i \leq s_i$$

Wähle zu jedem $1 \leq i \leq m$ ein $x_i \in R$ mit $x_i \in P_i^{s_i}/P_i^{s_i-1}$. Der chinesischen Restsatz sichert die Existenz einer Lösung von

$$a \equiv x_i \pmod{P_i^{r_i}}, \quad 1 \leq i \leq m$$

in R. Es gilt $J + (a) = I$, weil sie in allen Lokalisierungen A_P die selben Ideale erzeugen. □

Lemma 3.2. Sei $0 \neq I$ ein Ideal eines Dedekindringes R. Dann existiert ein $J \triangleleft R$, sodass IJ ein Hauptideal ist. J kann darüber hinaus relativ prim zu einem vorgegebenen Ideal $0 \neq S \triangleleft R$ gewählt werden, oder so, dass $IJ = (a)$ für beliebiges fest vorgegebenes $a \in I$.

Beweis: Sei $0 \neq a \in I$. Natürlich gilt $(a) \subset I$, also

$$(a) = P_1^{r_1} \dots P_m^{r_m}, \quad I = P_1^{s_1} \dots P_m^{s_m}, \quad r_i \geq s_i$$

$J := P_1^{r_1-s_1} \dots P_m^{r_m-s_m}$ ist das im ersten Teil gesuchte Ideal J.
Wegen $IS \subset I$ folgt aus Lemma 3.1 die Existens eines $a \in I$ mit

$$I = IS + (a) \tag{3.1}$$

Andererseits zeigt der erste Teil obiger Aussage wegen $(a) \subset I$ die Existenz eines J mit

$$(a) = IJ \tag{3.2}$$

Insgesamt aus (3.1) und (3.2) also $I = IS + IJ = I(S + J)$. Wäre nun $J + S \neq R$ dann wäre es in einem Primideal P enthalten und weiter $I(S+J) \subset IP \subset P$ und daher insbesondere nicht ganz I, ein Widerspruch. Es muss also schon $J + S = R$ gelten, also J und S relativ prim. □

Satz 3.1. Die Gruppe der invertierbaren Ideale eines Dedekindringes R ist die von den Primidealen von R frei endlich erzeugte abelsche Gruppe. Jedes gebrochene Ideal I kann eindeutig dargestellt werden als

$$I = \prod_P P^{a_P}, \quad a_P \in \mathbb{Z}, \quad P \quad Primideal$$

Beweis: Wir spielen es auf den Fall echter Ideale zurück. Sei $0 \neq I$ ein (echtes) Ideal. Nach Lemma 3.2 gibt es ein Ideal J und ein $a \in R$ mit $IJ = (a)$. Wegen $I(a^{-1}J) = R$ ist $a^{-1}J$ das inverse zu I.
Für ein gebrochenes Ideal I wähle d so, dass dI echtes Ideal ist. Dieses besitzt wie eben gezeigt ein Inverses $(dI)^{-1}$, und $d(dI)^{-1}$ ist das gesuchte Inverse von I. Die Darstellung ergibt sich nun einfach. Wegen $d \in R$ und $dI \triangleleft R$ gilt

$$dI = P_1^{r_1} \dots P_m^{r_m}, \quad (d) = P_1^{s_1} \dots P_m^{s_m}$$

und schließlich

$$I = P_1^{r_1 - s_1} \dots P_m^{r_m - s_m}$$

mit eindeutig bestimmten Primidealen P_i. □

Es ist auch die Umkehrung zutreffend. Dedekindringe sind genau die Ringe in denen die gebrochenen Ideale eine Gruppe bilden.

Nun kommen wir zu einer ganz wesentlichen Definition die sich durch den Rest der Arbeit ziehen wird.

Definition 3.3 (Idealklassengruppe)**.** Die *Idealklassengruppe* $H(R)$ eines Dedekindringes R mit Quotientenkörper K ist die Faktorgruppe der Gruppe der gebrochenen Ideale $G(K)$ nach dem Normalteiler der gebrochenen Hauptideale. Ist speziell $R = O_K$ der Ganzheitsring eines algebraischen Zahlkörpers K, dann schreiben wir $H(K)$.
Es gilt: Ein Element dieser Gruppe ist eine Klasse bezüglich folgender Äquivalenzrelation auf den gebrochenen Idealen:

$$I \sim J \Longleftrightarrow \exists a \in K : aI = J$$

oder gleichwertig

$$I \sim J \Longleftrightarrow \exists a_1, a_2 \in R : a_1 I = a_2 J$$

Diese Definition bedarf noch einiger Erklärung. Die Gleichwertigkeit der beiden definierenden Eigenschaften und vor allem die Wohldefiniertheit der Faktoroperation liegt im Kern in diesem

Satz 3.2. Ist R Dedekindring mit Quotientenkörper K und M_1, M_2 endlich erzeugte R-Moduln, also von der Form

$$M_1 = I_1 \oplus I_2 \ldots \oplus I_m, \quad M_2 = J_1 \oplus J_2 \ldots \oplus J_n$$

mit von Null verschiedenen gebrochenen Idealen I_k, J_k von R, dann gilt

$$M_1 \cong M_2 \Longleftrightarrow m = n, \quad \exists a \in K : I_1 I_2 \ldots I_m = a J_1 J_2 \ldots J_n$$

Der Beweis ist technisch und hier aus umfangsgründen ausgelassen, er findet sich in [Na74], Theorem 1.14.

Nachfolgendes Korollar zeigt die Verträglichkeit von $\sim$ mit der Multiplikation von gebrochenen Idealen und rechtfertigt so die definierende Faktoroperation.

Korollar 3.1. Sind R, K wie oben und $I_1 \cong I_2, J_1 \cong J_2$ zwei Paare als R-Moduln isomorpher gebrochener Ideale von R, dann ist $I_1 J_1 \cong I_2 J_2$ als R-Moduln.

Beweis: Wegen $I_1 \oplus I_2 \cong J_1 \oplus J_2$, folgt aus vorigem Satz die Existenz eines $a \in K$ mit $I_1 J_1 = I_2 J_2$, deswegen ist $x \longmapsto ax$ Isomorphismus zwischen $I_1 J_1$ und $I_2 J_2$. □

Definition 3.4 (Klassenzahl)**.** Die Mächtigkeit der Idealklassengruppe heißt die *Klassenzahl* von R. Wir bezeichnen sie mit $h(R)$. Ist speziell $R = O_K$ der Ganzheitsring eines algebraischen Zahlkörpers K, dann schreiben wir $h(K)$.

Die Bedeutung der Klassenzahl wird durch eine mit den bereits erarbeiteten Mitteln einfache Beobachtung gestützt.

Satz 3.3. In einem Dedekindring R sind äquivalent:

1. $H(R) = 1$
2. R ist Haupidealring
3. R ist faktorieller Ring (PZE-Ring)

Beweis: Die Äquivalenz der beiden letzteren Punkte haben wir bereits bewiesen. Ist $H(R) = 1$, dann ist offenbar jedes Ideal von der Form aI für ein festes Ideal I. Die Wahl $I = R$ ist zulässig, also ist jedes Ideal tatsächlich Hauptideal. Sind umgekehrt in einem Hauptidealring R zwei Ideale als $(a) = aR$, $(b) = bR$ gegeben, dann unterscheiden sie sich offenbar nur durch das Element $\frac{a}{b}$ aus dem Quotientenkörper. □

Die Ganzheitsringe in algebraischen Zahlkörpern erfüllen noch eine wichtige Eigenschaft, die die Definition der Norm eines Ideals plausibel macht.

Definition 3.5 ((EN), Norm eines Ideals)**.** Falls in einem Dedekindring R jedes (echte) Ideal I die Eigenschaft hat, dass R/I endlich ist, sagen wir er hat die *endliche Norm Eigenschaft (EN)*. Die Anzahl der Elemente $|R/I|$ des Faktorrings bezeichnen wir als die *Norm eines Ideals* I in so einem Dedekindring und schreiben $N(I)$ dafür.

Ähnlich wie man für die ganzen Abschlüsse von Dedekindringen in Erweiterungen ihrer Quotientenkörper die definierenden Eigenschaften eines Dedekindringes nachrechnen kann, so geht auch die Eigenschaft (EN) nicht verloren, wie man wieder mithilfe der Lokalisierungen zeigen kann. Diese Tatsache sei als Satz hier ohne Beweis angegeben.

Satz 3.4. Sei R Dedekindring mit Quotientenkörper K, der (EN) erfüllt, L/K eine endliche Körpererweiterung und S der ganze Abschluss von R in L. Dann erfüllt auch S die Eigenschaft (EN).

Für den Beweis siehe Theorem 1.9, [Na74].

Damit erfüllen die Ganzheitsringe algebraischer Zahlkörper diese Bedingung (EN). Wir gehen nun näher auf die Normabbildung ein.

Satz 3.5. 1. Für zwei Ideale I, J gilt $N(IJ) = N(I)N(J)$

2. Zu jeder positiven Zahl N gibt es nur endlich viele $I \triangleleft R$ die $N(I) < N$ erfüllen

Beweis: Aus Proposition 2.1 folgt insbesondere, dass der Faktorring P^n/P^{n+1} für jedes Primideal P stets $N(P)$ Elemente hat. Wegen $|R/P^{n+1}|/|R/P^n| = N(P)$ folgt induktiv $N(P^n) = N(P)^n$ für Primideale. Wegen der allgemeinen Darstellung von Idealen als Produkt selbiger folgt der allgemeine Fall.
Für den zweiten Punkt bemühen wir den chinesischen Restsatz. Zu jeder mindestens $(N+1)$-elementigen Menge wähle verschiedene $a_1, \ldots, a_{N+1}$. Für jedes Ideal I ist die Kongruenz $a_i - a_j \equiv 0 \bmod I$ lösbar, also auch das System bezüglich aller Ideale gleichzeitig. Nun gibt es aber nur endlich viele Differenzen $a_i - a_j$ die also nur in endlich vielen Idealen enthalten sein können nach Korollar 2.1. □

Noch ein weiteres später benötigtes Resultat sei gleich vorgestellt, das ein Standardresultat aus der elementaren Zahlentheorie auf das Level algebraischer Zahlkörper hebt.

Satz 3.6. Ist P Primideal in R, dann besteht für alle $x \in R$ die Gleichung

$$x^{N(P)} \equiv x \pmod{P}$$

und $N(P)$ ist der kleinste Exponent sodass dieser Sachverhalt (für alle x) gilt.

Beweis: Für $x \in P$ ist die Aussage trivial. Für $x \notin P$ gilt aber $x^{N(P)-1} \equiv 1 \pmod{P}$ weil R/P ein Körper mit $N(P)$ Elementen ist und folglich die multiplikative Gruppe $N(P)-1$ Elemente hat. Dabei ist die Formel $a^{|G|} = 1$ für Gruppen G eingegangen. Die Minimalität erhält man, weil endliche Körper zyklische multiplikative Gruppen haben, man muss nur für x eine Primitivwurzel wählen und die Potenzen $1, x \ldots x^{N(P)-2}$ sind von einander verschieden. □

Die Normabbildung ist also ein Homomorphismus zwischen der Halbgruppe der von Null verschiedenen Ideale von R und den natürlichen Zahlen. Nach Satz 3.1 können wir diesen Homomorphismus in natürlicher Weise zu einem Homomorphismus von den gebrochenen Idealen von R in die positiven rationalen Zahlen ausdehnen. Die so definierte Norm möge ebenfalls $N(I)$ heißen.

3.2 Endlichkeit der Klassenzahl

In diesem Abschnitt werden wir zeigen, dass Ganzheitsringe algebraischer Zahlkörper immer eine endliche Klassenzahl besitzen.

Zunächst sei $K/\mathbb{Q}$ ein Zahlkörper mit $[K:\mathbb{Q}] = n$. Wie in Satz 1.6 bereits zum Ausdruck gekommen ist, gibt es genau n Einbettungen $\sigma_1, \dots \sigma_n$ von L in die algebraischen Zahlen $\overline{\mathbb{Q}}$. Für $v_1, \dots, v_n \in K$ bezeichne

$$d_{K/\mathbb{Q}}(v_1, \dots, v_n) := (\det[\sigma_j(v_i)]_{i,j})^2 \tag{3.3}$$

deren *Diskriminante*. Für ein einzelnes Element $a \in K$ sei

$$d_{K/\mathbb{Q}}(a) := d_{K/\mathbb{Q}}(1, a, a^2, \dots, a^{n-1})$$

Lemma 3.3. Mit der Spur (1.2) aus Kapitel 1 gilt

$$d_{K/\mathbb{Q}}(v_1, \dots, v_n) = \det[Sp_{K/\mathbb{Q}}(v_i v_j)]$$

Beweis: Es gilt

$$\det[Sp_{K/\mathbb{Q}}(v_i v_j] = \det[\sum_{k=1}^{n} \sigma_k(v_i)\sigma_k(v_j)] = \det([\sigma_k(v_i)][\sigma_k(v_j)]^T) = d_{K/\mathbb{Q}}(v_1, \dots, v_n)$$

□

Weiters gilt

$$d_{K/\mathbb{Q}}(a) = \prod_{i<j} (\sigma_i(a) - \sigma_j(a))^2 \tag{3.4}$$

wie man sich leicht überzeugt, wenn man die rechte Seite obiger Gleichung als Quadrat der Determinante der Van der Monde-Matrix erkennt.
Die folgenden bewiesenen Tatsachen dienen dazu, die Wohldefiniertheit der *Diskriminante eines Zahlkörpers* zu gewährleisten, wie sie im Anschluss definiert wird.

Definition 3.6. Eine unimodulare Matrix ist eine Matrix mit ganzzahligen Einträgen und Determinante 1.

Satz 3.7. Sei M freier $\mathbb{Z}$-Modul mit freien Erzeugendensystemen $a_1, \dots, a_n$ sowie $b_1, \dots, b_n$. Dann existiert eine unimodulare Matrix die die beiden Matrizen ineinander überführt. Umgekehrt führt eine unimodulare Transformation ein Erzeugendensystem wieder in ein Erzeugendensystem über.

Beweis: Weil sich insbesondere die a_i sich aus den b_i ganzzahlig linear kombinieren lassen können und umgekehrt, also auch die Inverse Matrix diese Eigenschaft hat, muss die Matrix zwingend unimodular sein, wie man mithilfe der Cramerschen Regel einsieht. Aus der Cramerschen Regel folgt ebenfalls, dass die Inverse unimodularer Matrizen wieder unimodular sind. □

Bemerkung: Hier ist eine enge Verwandtschaft zu reellen Gittern erkennbar. Obiger Satz tritt im geometrischen Teil des Beweises des Dirichletschen Einheitensatzes auf.

Proposition 3.3. Sei K algebraischer Zahlkörper mit Ganzheitsring O_K und $v_1, \dots v_n \in O_K$. Dann gilt:

1. Die Diskriminante von $v_1, \dots v_n$ liegt wieder in O_K.
2. Für $a_{ij} \in \mathbb{Q}$ gilt

$$u_i = \sum_{j=1}^{n} a_{ij} v_j, \quad 1 \leq i \leq n \quad \Longrightarrow \quad d_{K/\mathbb{Q}}(u_1, \dots, u_n) = (\det[a_{ij}])^2 \cdot d_{K/\mathbb{Q}}(v_1, \dots, v_n) \tag{3.5}$$

3.

$$v_1, \dots v_n \in K \quad sind \quad \mathbb{Q} - linear \quad abhängig \quad \Longleftrightarrow \quad d_{K/\mathbb{Q}}(v_1, \dots v_n) = 0 \tag{3.6}$$

4. Wenn a die Erweiterung L/K erzeugt und $P \in K[x]$ das Minimalpolynom von a ist, dann gilt

$$d_{L/K}(a) = (-1)^m \det[a_{ij}] = (-1)^m N_{L/K}(P'(a))$$

mit $m = \frac{n(n-1)}{2}$, die a_{ij} sind definiert durch

$$a^j P'(a) = \sum_{i=0}^{n-1} a_{ij} a^i$$

wobei P' die formale Ableitung des Polynoms P ist und $N_{L/K}$ die Spurabbildung der Erweiterung L/K.

Beweis: Die erste Eigenschaft folgt aus Lemma 3.3, die zweite gilt wegen

$$\det[\sigma_j(u_i)] = \det[a_{ij}] \cdot \det[\sigma_j(v_i)]$$

Für den dritten Punkt ist zu bemerken, dass aus der linearen Abhängigkeit der v_i die Lösbarkeit des Systems

$$\sum_{i=1}^{n} x_i \sigma_j(v_i) = 0, \quad j = 1, 2 \dots n$$

für $x_i \in \mathbb{Q}$ folgt und wie aus der linearen Algebra bekannt weiter $d_{K/\mathbb{Q}}(v_1, \dots v_n) = 0$. Damit ist $\Longrightarrow$ gezeigt. Falls umgekehrt $d_{K/\mathbb{Q}}(v_1, \dots v_n) = 0$ gilt, besitzt das System

$$\sum_{i=1}^{n} x_i Sp_{K/\mathbb{Q}}(v_i v_j) = 0, \quad j = 1, 2 \dots n$$

eine eindeutige Lösung $y_1 = x_1, \dots, y_n = x_n$ für die x_i-Werte über $\mathbb{Q}$. Wären nun die v_i linear abhängig, so wäre $Y := \sum_{i=1}^{n} y_i v_i$ eine von Null verschiedene gemeinsame Lösung des Systems

$$Sp(Y \cdot v_i) = 0, \quad i = 1, 2 \dots n$$

Wegen der linearen Unabhängigkeit der v_i also $Yz = 0$ für alle $z \in K$. Dies widerspricht $0 \neq n = Sp_{K/\mathbb{Q}}(1)$. Um den letzten Punkt zu erhalten seien $\{a_1 = a, a_2, \dots a_n\}$ die Konjugierten von a und $b_i := P'(a_i)$. Man berechnet mittels (3.4)

$$d_{L/K}(a) = \prod_{i<j}(a_i - a_j)^2 = (-1)^m \prod_{i=1}^{n}\prod_{j\neq i}(a_i - a_j) =$$

$$(-1)^m \prod_{i=1}^{n} P'(a_i) = (-1)^m b_1 b_2 \dots b_n = (-1)^m N_{L/K}(P'(a))$$

was einen Teil der Gleichung zeigt. Weiters

$$b_1 b_2 \dots b_n \det[a_i^j] = \det[a_i^j b_i] = \det[\sum_{k=1}^{n} a_{kj} a_k^i] = \det[a_{kj}] \det[a_j^k] \tag{3.7}$$

und wegen Punkt 2 gilt $\det[a_j^k] \neq 0$, Division von (3.7) durch diesen Term ergibt letztlich

$$b_1 b_2 \dots b_n = \det[a_{ij}]$$

die zweite Gleichung.

□

Nachfolgendes Korollar steht in enger Verbindung zum Begriff der Ganzheitsbasis aus Definition 1.9.

Korollar 3.2. Sei K algebraischer Zahlkörper und M freier $\mathbb{Z}$-Untermodul von O_K vom Grad n. Dann hängt die Diskriminante einer Basis von M nicht von der konkreten Basis ab. Im Falle $M = O_K$ nennen wir sie die *Diskriminante von* K und schreiben $d(K)$.

Beweis: Kombination von Satz 3.7 und (3.5) aus Proposition 3.3. □

Beispiel: Für einen quadratischen Zahlkörper $n = [K : \mathbb{Q}] = 2$ kann man stets $K = \mathbb{Q}(\sqrt{d})$ mit quadratfreiem $d \in \mathbb{Z}$ schreiben, wie die quadratische Lösungsformel von Vieta zeigt. Man kann sich mit elementarer Zahlentheorie vergewissern, dass

1. im Fall $d \equiv 2, 3 \pmod 4$ $\implies$ $\{1, \sqrt{d}\}$ ist Ganzheitsbasis $\implies$ $d(K) = 4d$
2. im Fall $d \equiv 1 \pmod 4$ $\implies$ $\{1, \frac{-1+\sqrt{d}}{2}\}$ ist Ganzheitsbasis $\implies$ $d(K) = d$

Für genauere Ausführungen siehe [Za1].

Lemma 3.4. Sei K algebraischer Zahlkörper vom Grad n, und seien $a_1, \dots a_n \in O_K$ $\mathbb{Q}$-linear unabhängig. Dann existiert eine Ganzheitsbasis $w_1, \dots w_n$ von K sodass

$$a_j = c_{j1} w_1 + \dots + c_{jj} w_j, \quad c_{ij} \in \mathbb{Z} \quad j = 1, 2 \dots n$$

Beweis: Sei für jedes $i = 1, 2 \dots n$ die Zahl $d_{ii} \in \mathbb{N}$ als die minimale positive ganze Zahl gewählt, so dass für gewisse $d_{i1}, \dots d_{i,i-1} \in \mathbb{Z}$- die nun ebenfalls durch diese Eigenschaft als fixiert betrachtet werden- die Zahl

$$w_i := d_{K/\mathbb{Q}}(a_1, \dots a_n)^{-1} \sum_{j=1}^{i} d_{ij} a_j$$

in O_K liegt. Das ist sicher möglich, weil ein algebraischer Zahlkörper der Quotientenkörper seines Ganzheitsringes ist und es so ein minimales d_{ii} natürlich geben muss weil $\mathbb{N}$ nach unten beschränkt ist. Die erste Beobachtung ist, dass die w_i linear unabhängig sind. Proposition 3.3 impliziert nämlich einerseits mit (3.5)

$$d_{K/\mathbb{Q}}(w_1, \dots w_n) = (d_{K/\mathbb{Q}}(a_1, \dots a_n)^{-n} \det[d_{ij}])^2 d_{K/\mathbb{Q}}(a_1, \dots a_n)$$

und andererseits zeigt (3.6), dass $d_{K/\mathbb{Q}}(a_1, \dots a_n)$ nicht 0 ist. Die Matrix mit Einträgen d_{ij} ist aber eine Diagonalmatrix mit nichtverschwindenden Diagonaleinträgen, also ist die Determinante ebenfalls nicht 0. Abermals (3.6) aus Proposition 3.3 zeigt, dass also die Vektoren w_i auf der linken Seite linear unabhängig sind.
Als nächstes beweisen wir: Falls $c \in O_K$ eine Darstellung

$$c = d_{K/\mathbb{Q}}(a_1, \dots a_n)^{-1}(c_1 a_1 + \dots + c_j a_j), \quad c_i \in \mathbb{Z}$$

besitzt (und ein festes j), dann muss notwendigerweise

$$d_{jj} | c_j \tag{3.8}$$

gelten. Wäre nämlich $c_j = s d_{jj} + r, r, s \in \mathbb{Z}, 0 < r < d_{jj}$ dann hätten wir mit

$$c - s w_j = d_{K/\mathbb{Q}}(a_1, \dots a_n)^{-1})((c_1 - d_{j1})a_1 + \dots + r a_j)$$

ein Element von O_K das der Minimalitätsbedingung der d_{jj} widerspricht.
Um zu zeigen, dass $\{w_1, \dots w_n\}$ eine Ganzheitsbasis bilden, müssen wir zeigen, dass der von ihnen erzeugte $\mathbb{Z}$-Modul- er heiße M- ganz O_K ist. Dazu zeigen wir induktiv: Ist ein Element von O_K von der Form

$$d_{K/\mathbb{Q}}(a_1, \dots, a_n)^{-1}(N_1 a_1 + \dots + N_j a_j), \quad N_i \in \mathbb{Z}$$

dann liegt es in M. Die Behauptung folgt dann einfach mit $j = n$.
Für $j = 1$ ist die Behauptung trivial. Sie gelte für $j = i - 1$ und betrachte ein beliebiges Element der gefragten Form

$$y = d_{K/\mathbb{Q}}(a_1, \dots, a_n)^{-1}(N_1 a_1 + \dots + N_i a_i) \in O_K, \quad N_i \in \mathbb{Z}$$

Wie bereits oben in (3.8) festgestellt gilt $N_i = L \cdot d_{ii}, L \in \mathbb{Z}$. Deshalb und nach Induktionsannahme gilt $y - L w_i \in O_K$. Weil klarerweise $L w_i \in M$ und wegen der Induktionsannahme lässt sich das beliebig gewählte y also als Summe zweier Elemente von M darstellen und ist daher wieder in M.

□

Proposition 3.4. Für $\mathbb{Q}$-linear unabhängige $a_1, \dots a_n \in O_K$ besteht die Identität

$$d_{K/\mathbb{Q}}(a_1, \dots, a_n) = m^2 \cdot d(K)$$

wobei m den Index von M in O_K bezeichnet.

Beweis: Sei $w_1, \dots w_n$ Ganzheitsbasis von K und wähle $b_1, \dots, b_n \in M$ so, dass

$$b_i = \sum_{k=1}^{i} c_{ik} w_k, \quad c_{ik} \in \mathbb{Z}$$

sodass c_{ii} positiv und kleinst möglich sind. Wie in Beweis von Lemma 3.4 ersichtlich bilden die b_i ein freies Erzeugendensystem für M und für ganze Zahlen N_i impliziert $N_1 w_1 + \ldots + N_i w_i \in M$, dass c_{ii} teilt N_i. Das bedeutet die $c_{11}c_{22}\dots c_{nn}$-elementige Menge

$$\{\alpha_1 w_1 + \ldots + \alpha_n w_n : 0 \leq \alpha_i < c_{jj}; j = 1, 2 \dots n\}$$

besteht aus paarweise inkongruenten Zahlen modulo M (also keine Differenz zweier Terme ist in M). Tatsächlich sind bereits alle Restklassen mod M vertreten. Könnten wir das zeigen hätte das

$$d_{K/\mathbb{Q}}(a_1, a_2 \dots a_n) = d_{K/\mathbb{Q}}(b_1, b_2 \dots b_n) = (c_{11}c_{22}\dots c_{nn})^2 \cdot d(K)$$

zur Folge, wobei die zweite Gleichheit auf (3.5) zurückgeht und die Tatsache ausnutzt, dass untere Dreiecksmatrizen das Produkt der Diagonalelemente als Determinante haben. Wir zeigen nun die Behauptung. Sei $\zeta = \sum_{k=1}^{n} \lambda_k w_k, \lambda_k \in \mathbb{Z}$ aus O_K beliebig. Sei μ_n der kleinste nichtnegative Rest von $\lambda_n \bmod(c_{nn})$ und weiter $A_n := (\lambda_n - \mu_n)/c_{nn}$. Nach Konstruktion ist dann

$$\zeta = A_n b_n + \mu_n w_n + \sum_{k=1}^{n} (\lambda_k - A_n c_{nk}) w_k$$

Nun iterieren wir diesen Gedanken. Wählt man μ_{n-1} als kleinsten nichtnegativen Rest von $\lambda_{n-1} - A_n c_{n,n-1} \bmod(c_{n-1,n-1})$ und definiert $A_{n-1} := (\lambda_{n-1} - A_n c_{n,n-1} - \mu_{n-1})/c_{n-1,c-1}$, so erhält man

$$\zeta = A_n b_n + A_{n-1} b_{n-1} + \mu_n w_n + \mu_{n-1} w_{n-1} + \sum_{k=1}^{n-2} (\lambda_k - A_n c_{n,k} - A_{n-1} c_{n-1,k}) w_k$$

Schließlich hat man die Form

$$\zeta = \sum_{k=1}^{n} \alpha_k b_k + \sum_{k=1}^{n} \mu_k w_k, \quad (0 \leq \mu_j < c_{jj}; \quad \mu_j, \alpha_j \in \mathbb{Z})$$

also $\zeta \equiv \sum_{k=1}^{n} \mu_k w_k \bmod M$.

□

Korollar 3.3. Sei $0 \neq a \in K$ und $I := aO_K$ das erzeugte gebrochene Hauptideal. Dann gilt

$$N(I) = |N_{K/\mathbb{Q}}(a)|$$

Beweis: Weil beide Seiten multiplikativ im Argument sind, kann man $a \in O_K$ voraussetzen. Sei $w_1, \dots w_n$ Ganzheitsbasis von K. Dann kann man $a \cdot O_K$ als $\mathbb{Z}$-Modul erzeugt von $aw_1, \dots aw_n$ auffassen und wegen vorangehender Proposition 3.4

$$N(I)^2 = d_{K/\mathbb{Q}}(aw_1, \dots aw_n) \cdot d(K)^{-1} \tag{3.9}$$

Andererseits gilt offenbar

$$d_{K/\mathbb{Q}}(aw_1, \dots aw_n) = N^2_{K/\mathbb{Q}}(a) \cdot d(K) \tag{3.10}$$

wie durch einfache Determinantenregeln und den Definitionen ersichtlich. Beide Gleichungen (3.9), (3.10) zusammen ergeben das geforderte Resultat. □

Nun wollen wir noch eine weitere wichtige Eigenschaft der Diskriminanten von Körpererweiterungen von $\mathbb{Q}$ angeben von der wir später Gebrauch machen werden.

Proposition 3.5. Gilt $\mathbb{Q} \subset K \subset L$, dann teilt $d(K)$ die Zahl $d(L)$.

Beweis: Sei $[K : \mathbb{Q}] = m$, $[L : K] = n$. Nach dem Gradsatz ist $[L : \mathbb{Q}] = mn$. Sei $a_1, a_2 \dots a_m$ eine Ganzheitsbasis von K und wähle $a_{m+1}, \dots a_{mn} \in O_L$ sodass $a_1, a_2, \dots a_{mn}$ linear unabhängig über $\mathbb{Q}$ sind. Sei $w_1, \dots w_{mn}$ eine Ganzheitsbasis gemäß Lemma 3.4, also derart, dass

$$a_j = c_{j1}w_1 + \dots + c_{jj}w_j \quad (1 \le j \le n), \quad c_{ij} \in \mathbb{Z}$$

Nach Konstruktion gilt $w_1, \dots w_n \in K$ und der von ihnen erzeugte $\mathbb{Z}$-Modul enthält eine Ganzheitsbasis von K. Daher müssen $w_1, \dots w_n$ selbst diese Ganzheitsbasis von K sein. Bezeichne mit $w_i^{(k)}$ die Konjugierten von w_i und bezeichne die Monomorphismen von L in die komplexen Zahlen, so dass $\sigma_k(w_1) = w_1^{(k)}$ für $1 \le k \le m$ mit $\sigma_1, \dots \sigma_m$. Die übrigen Monomorphismen seien $\sigma_{m+1}, \dots \sigma_{mn}$ und so nummeriert, dass $\sigma_k(w_j) = w_j^{(k)}$, für $1 \le j \le m$, $m+1 \le k \le mn$. Man kann oBdA weiter von

$$i \equiv j \pmod m \Rightarrow \quad \sigma_i \equiv \sigma_j \pmod m$$

ausgehen. Mit dieser Vorgabe berechnet man

$$d(L) = (\det[\sigma_i(w_j)])^2 = \det \begin{pmatrix} w_1^{(1)} & \dots & w_1^{(m)} & w_1^{(1)} & \dots & w_1^{(m)} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots \\ w_m^{(1)} & \dots & w_m^{(m)} & w_m^{(1)} & \dots & w_m^{(m)} \\ w_{m+1}^{(1)} & \dots & w_{m+1}^{(m)} & w_{m+1}^{(m+1)} & \dots & w_{m+1}^{(mn)} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ w_{mn}^{(1)} & \dots & w_{mn}^{(m)} & w_{mn}^{(m+1)} & \dots & w_{mn}^{(mn)} \end{pmatrix}^2$$

$$= \det \begin{pmatrix} w_1^{(1)} & \dots & w_1^{(m)} & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots \\ w_m^{(1)} & \dots & w_m^{(m)} & 0 & \dots & 0 \\ w_{m+1}^{(1)} & \dots & w_{m+1}^{(m)} & w_{m+1}^{(m+1)} - w_{m+1}^{(1)} & \dots & w_{m+1}^{(mn)} - w_{m+1}^{(m)} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ w_{mn}^{(1)} & \dots & w_{mn}^{(m)} & w_{mn}^{(m+1)} - w_{mn}^{(1)} & \dots & w_{mn}^{(m)} \end{pmatrix}^2$$

$$= d(K) \cdot b$$

mit einer algebraischen ganzen Zahl $b \in O_L$, da sämtliche $w_i \in O_L$, die Determinantenbildung nur Summen und Produkte verwendet und O_L einen Ring bildet. Wegen $b = \frac{d(K)}{d(L)} \in \mathbb{Q}$ und $\mathbb{Q} \cap O_L = \mathbb{Z}$ muss b eine ganze Zahl sein.

□

Folgende überaus nützliche Resultate, beruhend auf Lemma 1.7, dem *Lemma von Minkowski* aus Kapitel 1, bereiten den Beweis der Endlichkeit der Klassenzahl vor. Die Notation ist von Kapitel 1 übernommen.

Lemma 3.5. Sei K Zahlkörper mit Signatur (s,t) und M ein $\mathbb{Z}$-Modul mit endlichem Index m in O_K. Dann existiert ein $0 \neq a \in M$, so dass

$$|N_{K/\mathbb{Q}}(a)| \leq (\frac{4}{\pi})^t \cdot \frac{n!}{n^n} \cdot \sqrt{|d(K)|}$$

Beweis: Wir machen von der Abbildung F aus (1.11) aus Kapitel 1 Gebrauch. Diese ist injektiv und das Bild von M unter F ist ein Gitter dessen Erzeuger die Bilder der Erzeuger von M sind (folgt aus den Eigenschaften von x, siehe Ende Abschnitt 1.4). Das Volumen der Grundmasche kann zu $\sqrt{|d(K)|}2^{-t}m$ bestimmt werden. Definiere nun für $u > 0$ die Hilfsmenge

$$X_u = \left\{ [x_1, \ldots, x_s; y_{s+1}, z_{s+1}, \ldots y_{s+t}, z_{s+t}] \in \mathbb{R}^n : \sum_{i=1}^{s} |x_i| + 2 \sum_{i=s+1}^{s+t} \sqrt{y_j^2 + z_j^2} < u \right\} \tag{3.11}$$

Diese Menge ist sicher konvex und symmetrisch um den Ursprung, wie für Minkowskis Lemma nötig. Induktiv kann man nachrechnen, dass

$$V(X_u) = 2^s (\frac{\pi}{2})^t u^n / n!$$

für $n = s + 2t$ gilt, was hier nicht explizit durchgeführt sei.
Zu $\epsilon > 0$ bestimme $u = u(\epsilon)$ aus der impliziten Gleichung

$$u^n = m \cdot n! (\frac{4}{\pi})^t \sqrt{|d(K)|} + \epsilon \tag{3.12}$$

Dieses u eingesetzt in die Formel (3.11) von X_u ergibt

$$V(X_u) > (2^{-t} m \sqrt{|d(K)|}) 2^n$$

und Minkowskis Lemma rechtfertigt die Existenz eines $0 \neq a = a(\epsilon) \in M$ mit $F(a) \in X_u$. Schreibt man für $F(a) = [x_1, \ldots, z_k]$ bedeutet das gerade

$$\sum_{i=1}^{s} |x_i| + 2 \sum_{i=s+1}^{t} \sqrt{|y_i^2 + z_i^2} < u$$

Die Definition der Norm eines Elements (1.1) sowie die arithmetisch-geometrische Mittelungleichung liefern

$$|N_{K/\mathbb{Q}}(a)|^{1/n} = (\prod_{i=1}^{s} |x_i| \prod_{i=1+s}^{t} \sqrt{|y_i^2 + z_i^2|})^{1/n} \leq \frac{u}{n}$$

Diese Ungleichung zur n-ten Potenz schreibt sich unter Berücksichtigung von (3.12) als

$$|N_{K/\mathbb{Q}}(a)| \leq \frac{u^n}{n^n} \leq (\frac{4}{\pi})^s \frac{n!}{n^n} \sqrt{d(K)} m + \frac{\epsilon}{n^n}$$

Geht man oBdA von $\epsilon < 1$ aus, dann gibt es nur endlich viele in Frage kommende $a = a(\epsilon)$. Dies folgt aus Satz 3.5 und Korollar 3.3, denn aus der Existenz unendlich vieler $a = a(\epsilon)$ würde via Korollar 3.3 die Existenz unendlich vieler Hauptideale mit fest beschränkter Norm folgen im Widerspruch zu Satz 3.5. Lässt an in letzter Gleichung ϵ gegen 0 gehen, folgt also die Existenz eines dieser endlich vielen $a = a(\epsilon)$, das die Gleichung ohne letzten ϵ-Term erfüllt, wie gefordert. □

Lemma 3.6. Sei K algebraischer Zahlkörper vom Erweiterungsgrad n und Signatur (s, t). Dann enthält jede Idealklasse ein Ideal $J \triangleleft O_K$ mit

$$N(J) \leq \frac{n!}{n^n} (\frac{4}{\pi})^t \sqrt{|d(K)|}$$

Beweis: Nach Lemma 3.2 ist es möglich zu gegebem $I \triangleleft O_K$ ein $J \triangleleft O_K$ zu finden mit $IJ = (a)$ für ein $a \in O_K$. Weil J als $\mathbb{Z}$-Modul in O_K endlichen Index $N(J)$ hat, ergibt Lemma 3.5 die Existenz eines $0 \neq d \in J$ mit

$$|N_{K/\mathbb{Q}}(d)| \leq \frac{n!}{n^n} (\frac{4}{\pi})^t \cdot \sqrt{|d(K)|} \cdot N(J) \tag{3.13}$$

Weil das Hauptideal (d) durch J teilbar ist, ist $B := dJ^{-1}$ wohldefiniertes Ideal. Dieses B liegt aber in der selben Idealklasse wie I (nämlich J^{-1}), und zuerst Korollar 3.3 und anschließend Anwendung von (3.13) implizieren

$$N(B) = |N_{K/\mathbb{Q}}(d)| \cdot N(J)^{-1} \leq \frac{n!}{n^n} (\frac{4}{\pi})^t \cdot \sqrt{|d(K)|} \cdot 1$$

Wegen der Beliebigkeit von I ist der Beweis abgeschlossen. □

Satz 3.8. Jeder algebraische Zahlkörper hat eine endliche Klassenzahl.

Beweis: Nach Lemma 3.6 besitzt jede Klasse einen Repräsentanten dessen Norm durch eine feste Zahl beschränkt ist. Da aber nach Satz 3.5 nur endlich viele Ideale mit beschränkter Norm existieren, muss die Zahl der Klassen endlich sein. □

Kapitel 4

Zetafunktionen und die analytische Klassenzahlformel

4.1 Die Zetafunktion eines algebraischen Zahlkörpers und ihre Eigenschaften

Die eindeutige Zerlegung von Idealen in Primideale in einem algebraischen Zahlkörper und die Endlichkeit der Klassenzahl erlauben einen analytischen Zugang zur Bestimmung bzw Beschreibung der Klassenzahl mittels der ihm zugeordneten Zetafunktion. Dieser Abschnitt beschäftigt sich mit deren analytischen Grundlagen.

Definition 4.1. Für einen algebraischen Zahlkörper K bezeichnen wir die durch die formale Reihe

$$\zeta_K(s) = \sum_{0 \neq I \lhd O_K} N(I)^{-s}, \quad s \in \mathbb{C}$$

definierte komplexe Funktion als seine *Zetafunktion*.

Ein kleines technisches Hilfsmittel zur Konvergenz der Zetafunktion stellt folgende Proposition dar:

Proposition 4.1. Eine Reihe $\sum_{n=1}^{\infty} a_n$ mit von Null verschiedenen a_n konvergiert genau dann absolut, wenn das Produkt $\prod_{n=1}^{\infty}(1 + a_n)$ absolut konvergiert.

Beweis: Die absolute Konvergenz des Produkts ist gleichbedeutend mit der absoluten Konvergenz vom Logarithmus des Produkts, und damit mit der absoluten Konvergenz der Reihe

$$\sum_{n=1}^{\infty} \log(1 + a_n)$$

Die absolute Konvergenz dieser Reihe ist mit der absoluten Konvergenz der Reihe $\sum_{n=1}^{\infty} a_n$ gleichwertig. Dies is der Fall, weil Logarithmusfunktion an der Stelle 1 Ableitung 1 hat, man also in einer Nullumgebung von $x \in \mathbb{R}$ die Abschätzung

$$\frac{1}{2}|\log(1 + x)| \leq |x| \leq 2|\log(1 + x)|$$

hat. Da die Folgenglieder konvergenter Reihen gegen Null konvergieren müssen und die ersten endlich vielen Folgenglieder sowie konstante Faktoren bei der Konvergenz keine Rolle spielen, folgt die Behauptung. □

Proposition 4.2. In der Halbebene $\mathrm{Re}(s) > 1$ konvergiert die Zetafunktion ζ_K absolut und lokal gleichmäßig. Die Zetafunktion ist holomorph auf $\mathrm{Re}(s) > 1$.

Beweis: Sei $[K : \mathbb{Q}] = n$. Weil es höchstens n Primideale mit vorgegebener Norm in O_K gibt und diese eine Primzahlpotenz ist (weil der Faktorring ein Körper ist) ist obige Reihe sicher auf $\mathrm{Re}(s) > 1$ konvergent, wenn man die Summe nur über Primideale erstreckt und die Konvergenz ist sogar gleichmäßig, weil

$$\sum_q n q^{-\mathrm{Re}(s)}$$

eine Majorante darstellt, wobei q die Primzahlpotenzen von $\mathbb{Z}$ durchläuft. Nun gilt aber

$$\sum_{N(I)\leq T} |N(I)^{-s}| \leq \prod_{N(P)\leq T} (1 + N(P)^{-\mathrm{Re}(s)} + N(P)^{-\mathrm{Re}(s)} + \ldots)$$

wobei P die Primideale seien und T beliebig fest. Man kann nun jeden Faktor rechts abschätzen mit $1 + 3N(P)^{-\mathrm{Re}(s)}$ und deren Produkt konvergiert lokal gleichmäßig weil die Reihe wie bereits festgestellt gleichmäßig konvergiert und obiger Proposition 4.1. Die Analytizität solcher lokal gleichmäßig konvergenter Reihen ist ein Standardresultat aus der Funktionentheorie. □

Von Bedeutung ist die Faktorisierung der Zetafunktionen:

$$\zeta_K(s) = \prod_P (1 - N(P))^{-s})^{-1}$$

wobei das Produkt über die Menge aller Primideale erstreckt wird. Diese lässt sich rechtfertigen, indem man zu $T > 0$ die Menge aller Ideale in O_K betrachtet, sodass alle Primideale die sie teilen Norm kleiner als T haben, ansieht. Diese Menge heiße J_T. Betrachtet man zu $Re(s) > 1$ nun endliche Produkte

$$\prod_{N(P)\leq T} \sum_{m=0}^{\infty} N(P)^{-ms} = \sum_{I\in J_T} N(I)^{-s}$$

und folgert

$$|\prod_{N(P)\leq T} \sum_{m=0}^{\infty} N(P)^{-ms} - \sum_{N(I)\leq T} N(I)^{-s}| \leq \sum_{N(I)>T} |N(I)^{-s}|$$

wobei die rechte wegen der Konvergenz der Reihe gegen 0 konvergiert, erhält man die Konvergenz des unendlichen Produkts gegen den Reihenwert, und die Summenformel für geometrische Reihen beschließt den Beweis. □

Bemerkung: Obige Beweisidee lässt sich unmittelbar auf Reihen mit der Form $\sum_I f(I)N(I)^{-s}$ mit multiplikativem f (dh $f(IJ) = f(I)f(J)$ für relativ prime Ideale) verallgemeinern.

Bemerkung: Aus der Produktdarstellung gewinnen wir sofort

Korollar 4.1. Die Zetafunktionen $\zeta_K(s)$ sind auf $\mathrm{Re}(s) > 1$ nullstellenfrei.

Im folgenden Abschnitt verwenden wir nun wieder Abschnitt 1.4 und 1.5 und dessen Notation. Für das weitere Studium ist zusätzlich noch der Begriff des Regulators hilfreich.

Definition 4.2 (Regulator)**.** Sei die Matrix $A \in \mathbb{R}^{(s+t)\times(s+t-1)}$ gegeben als

$$\mathbf{A} = \begin{pmatrix} \log\|\epsilon_1\|_1 & \log\|\epsilon_2\|_1 & \dots & \log\|\epsilon_{s+t-1}\|_1 \\ \log\|\epsilon_1\|_2 & \log\|\epsilon_2\|_2 & \dots & \log\|\epsilon_{s+t-1}\|_2 \\ \dots & & & \\ \log\|\epsilon_1\|_{s+t} & \log\|\epsilon_2\|_{s+t} & \dots & \log\|\epsilon_{s+t-1}\|_{s+t} \end{pmatrix}$$

wobei $\|\alpha\|_i := |\sigma_i(\alpha)|$ für $i \leq s$ bzw $\|\alpha\|_i := |\sigma_i(\alpha)|^2$ für $s+1 \leq i \leq s+t-1$ und ϵ_i die Grundeinheiten (Erzeuger) des freien Anteils aus dem dirichletschen Einheitensatz.
Sei weiters A_i die Matrix die aus A bei Streichen der i-ten Zeile hervorgeht. Dann ist $|\det(A_i)|$ von i unabhängig, heißt der *Regulator von K* und wird in Folge mit R_K bezeichnet.

4.2 Die allgemeine Klassenzahlformel eines Zahlkörpers

Dieser Abschnitt ist dem Beweis der allgemeinen Klassenzahlformel gewidmet.

Satz 4.1. Die Funktion $\zeta_K(s)$ hat an der Stelle $s = 1$ einen Pol mit Residuum

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2^s(2\pi)^t R_K h(K)}{\sqrt{|d(K)|}\omega(K)} \tag{4.1}$$

dabei ist $\omega(K)$ die Ordnung des Torsionsanteils ζ aus dem Dirichletschen Einheitensatz Satz 1.7.

Zuerst splitten wir die Summe auf in

$$\zeta_K(s) = \sum_{A\in H(K)} (\sum_{I\in A} \frac{1}{N(I)^s})$$

und setzen zur Vereinfachung

$$f_A(s) := \sum_{I\in A} \frac{1}{N(I)^s}$$

Wählt man nun $\boldsymbol{a} \in A^{-1}$ so, dass für alle $I \in A$ das Ideal $\boldsymbol{a}I$ Hauptideal ist, dann induziert Multiplikation mit $\boldsymbol{a}$ eine Bijektion zwischen (ganzen) Idealen von A und durch $\boldsymbol{a}$ teilbaren Hauptidealen. Man kann also f_A schreiben als

$$f_A(s) = N(\boldsymbol{a})^s \sum_{(\alpha):\boldsymbol{a}|(\alpha)} \frac{1}{|N(\alpha)|^s}$$

Sei B ein Repräsentantensystem von α-Werten wobei von jeder Menge assoziierter Elemente genau eines in B sein soll. Weiters sei $\Gamma = x(\boldsymbol{a}) := \{y \in \Lambda^{s,t} : \exists b \in \boldsymbol{a}| \quad y = x(b)\}$

und $\Theta = x(B) := \{y \in \Lambda^{s,t} : \exists b \in B| \quad y = x(b)\}$ mit der die geometrische Darstellung beschreibenden Abbildung x aus Kapitel 1.4. f_A bekommt dann die Form

$$f_A(s) = N(\boldsymbol{a})^s \sum_{\alpha \in \Theta} \frac{1}{|N(\alpha)|^s} \tag{4.2}$$

Es gilt diese Ausdrücke auszurechnen. Dazu braucht es ein paar Vorbereitungen.

Lemma 4.1 (Geometrisches Lemma)**.** Sei X ein Kegel im $\mathbb{R}^n$ und die Funktion $F : X \longrightarrow [0, \infty)$ erfülle:

1. $F(\varsigma x) = \varsigma^n F(x)$, $\varsigma > 0$
2. $\boldsymbol{F} := \{x \in X : F(x) \leq 1\}$ ist beschränkt mit Volumen $V > 0$.

Sei weiter Γ ein Gitter im $\mathbb{R}^n$ mit Volumen der Grundmasche Δ. Dann konvergiert die Reihe

$$\zeta_{F,\Gamma}(s) = \sum_{x \in \Gamma \cap X} \frac{1}{F(x)^s}$$

auf $\mathrm{Re}(s) > 1$ und hat Residuum $\lim_{s\to 1}(s-1)\zeta_{F,\Gamma}(s) = \frac{V}{\Delta}$.

Beweis: Man überzeugt sich leicht von

$$V = \lim_{r\to\infty}(\frac{\Delta}{r^n} \cdot \sharp\{\frac{1}{r}\Gamma \cap \boldsymbol{F}\}) = \Delta \lim_{r\to\infty} \frac{\sharp\{\frac{1}{r}\Gamma \cap \boldsymbol{F}\}}{r^n} \tag{4.3}$$

Wegen der 1. Voraussetzung an F gilt weiter $\sharp\{\frac{1}{r}\Gamma \cap \boldsymbol{F}\} = \sharp\{x \in \Gamma \cap X : F(x) \leq r^n\}$. Ordnet man die Punkte in $X \cap \Gamma$ so, dass $0 \leq F(x_1) \leq F(x_2) \ldots$ und setze $r_k := F(x_k)^{1/n}$ sowie $\gamma(r) := \sharp\{\frac{1}{r}\Gamma \cap \boldsymbol{F}\}$. Mit dieser Wahl gilt für alle $\epsilon > 0$ die Ungleichung $\gamma(r_k - \epsilon) < k \leq \gamma(r_k)$ oder äquivalent

$$\frac{\gamma(r_k-\epsilon)}{(r_k-\epsilon)^n}(\frac{r_k-\epsilon}{r_k})^n < \frac{i}{r_i^n} \leq \frac{\gamma(r_k)}{r_k^n}$$

Wegen $r_k^n = F(x_k)$ führt $\epsilon \to 0$ zu $\lim_{k\to\infty} \frac{k}{r_i^n} = \frac{V}{\Delta}$ wegen (4.3). Deswegen kann man zu festem $\epsilon > 0$ ein k_0 finden, sodass für $k \geq k_0$

$$(\frac{V}{\Delta} - \epsilon)^s \frac{1}{k^s} < \frac{1}{F(x_k)^s} < (\frac{V}{\Delta} + \epsilon)^s \frac{1}{k^s}$$

Unsere Zetafunktion lässt sich aber schreiben als

$$\zeta_{F,\Gamma}(s) = \sum_{k=1}^{\infty} \frac{1}{F(x_k)^s}$$

Summiert man über alle $k \geq k_0$- was die Residuen nicht verändert- und multipliziert mit $(s-1)$ so erhält man

$$(\frac{V}{\Delta} - \epsilon)\mathrm{Res}_{s=1}\zeta(s) \leq \lim_{s\to 1}(s-1)\zeta_{F,\Gamma}(s) \leq (\frac{V}{\Delta} + \epsilon)\mathrm{Res}_{s=1}\zeta(s)$$

mit der riemannschen Zetafunktion $\zeta = \zeta_{\mathbb{Q}}$. Diese hat aber bekanntermaßen Residuum 1 bei $s = 1$, und $\epsilon \to 0$ ergibt das Gewünschte. □

Proposition 4.3. Sei $\epsilon \in O_K$ eine Einheit von O_K. Dann gilt $|N(\epsilon)| = 1$.

Beweis: Sei $\overline{\epsilon}$ die Inverse zu ϵ. Weil Norm ein Homomomorphismus ist, gilt $1 = N(1) = N(\epsilon\overline{\epsilon}) = N(\epsilon)N(\overline{\epsilon})$. Weil Norm und Spur ganze Zahlen sind (wie zB in Lemma 1.2 bewiesen) folgt die Behauptung. □

Seien nun $\epsilon_1, \ldots, \epsilon_{s+t-1}$ Grundeinheiten des freien Anteils aus dem dirichletschen Einheitensatz wie bei der Defintion des Regulators. Wähle weiters $\lambda := (1, 1, \ldots 1; 2, 2, \ldots 2) \in \mathbb{R}^{s+t}$. Die Menge $\{\lambda, l(\epsilon_1), \ldots, l(\epsilon_{s+t-1})\}$ ist eine Basis von R^{s+t} wie man nachprüfen kann. Dafür zeigt man schnell mit der Norm und obiger Proposition, dass die logarithmische Darstellung der Grundeinheiten in der Hyperebene $H := \{(x_1, \ldots x_{s+t}) \in \mathbb{R}^n : x_1 + \ldots + x_s + 2x_{s+1} + \ldots + 2x_{s+t} = 0\}$ enthalten sind, nämlich

$$\prod_{i=1}^{s}(|\sigma_i(\epsilon)|)(\prod_{i=s+1}^{s+t}|\sigma_i(a)|^2) = |N_{K/\mathbb{Q}}(a)| = 1$$

und logarithmieren ergibt den Nachweis. Der Nachweis dass $H \cong \mathbb{R}^{s+t-1}$ ganz aufgespannt wird ist aber mit einiger Mühe verbunden und ein wesentliches Resultat zum Beweis des dirichletschen Einheitensatzes. Es sei hier ohne Beweis nur erwähnt. Weil darüber hinaus λ als orthogonales Komplement von H linear unabhängig zum Unterraum H aufgespannt von den $l(\epsilon_i)$ ist erlaubt nun jedes $y \in \Lambda^{s,t}$ eine Darstellung

$$l(y) = c + \sum_{i=1}^{s+t-1} c_i x(\epsilon_i), \quad c = \frac{\log(N(y))}{n}, \quad c_i \in \mathbb{R} \tag{4.4}$$

wobei sich c aus der Tatsache ergibt dass Einheiten Norm 1 haben. Wir wollen das geometrische Lemma anwenden auf die Normfunktion und den Kegel X der gegeben ist durch die Menge der $y \in \Lambda^{s,t} \cong \mathbb{R}^n$ die

$$N(y) \neq 0$$

$$0 \leq c_i \leq 1, \quad 1 \leq i \leq s + t - 1$$

$$0 \leq \arg(y_1) < \frac{2\pi}{\omega(K)}$$

erfüllen wobei y_1 die erste Koordinate von y sei. Das ist ein Kegel wegen $l(cy) = \log(c)\lambda + l(y)$ die Koeffizienten c_i unverändert lässt und $\arg(cy_1) = \arg(y_1)$.

Lemma 4.2. Seien $\Xi(\alpha)$ die Menge der zu $\alpha \in O_K$ assoziierten Elemente. Dann hat genau ein Element von $\Xi(\alpha)$ Bild in X.

Beweis: Wir konstruieren zu $z \in \mathbb{R}^n$ ein $y \in X$ das mit komponentenweiser Multiplikation $z = y \cdot x(\epsilon)$ mit einer Einheit ϵ erfüllt und gleichzeitig wird sich die Eindeutigkeit einer solchen Darstellung ergeben. Schreibe $l(z) = c\lambda + \sum_{i=1}^{s+t-1} c_i x(\epsilon_i)$ und schreibe $c_i = m_i + \mu_i$ mit $m_i \in Z$ und $0 \leq \mu_i < 1$. Setze $u := \epsilon_1^{m_1}\epsilon_2^{m_2}\ldots\epsilon_{s+t-1}^{m_{s+t-1}}$ und weiter $f := y \cdot x(u^{-1})$, das die gewünschten c_i Werte für den Bereich X hat. Um $\arg(f_1)$ in den richtigen Bereich zu befördern sei $r \in \mathbb{Z}$ die Zahl mit $0 \leq \arg(f_1) - \frac{2\pi r}{\omega(K)} < \frac{2\pi}{\omega(K)}$ und einen Einheitswurzel

κ mit $\sigma_1(\kappa) = e^{\frac{2\pi i}{\omega_K}}$. Mit dieser Konstruktion ist $y := f \cdot x(\kappa^{-r}) = z \cdot x(u^{-1})x(\omega^{-r}) \in X$ das gesuchte Element und eindeutig weil deterministisch bestimmt. □

Dieses Lemma erlaubt uns (4.2) anzuschreiben als

$$f_A(s) = N(\boldsymbol{a})^s \sum_{x \in \Gamma \cap X} \frac{1}{N(x)^s} \tag{4.5}$$

was wir mit Hilfe des geometrischen Lemmas berechnen können wenn wir die Werte Δ und V zur Hand haben. Dabei entspricht hier V dem Volumen von $\{x \in X : N(x) \leq 1\}$ und Δ dem Volumen der Grundmasche des Gitters $\Gamma = x(\boldsymbol{a}) = \{y \in \Lambda^{s,t} : \exists b \in \boldsymbol{a} : y = x((b)\}$. Diesen Grössen sind die nachstehenden beiden Lemmata gewidmet.

Lemma 4.3. $\Delta = N(\boldsymbol{a})\sqrt{|d(K)|}$

Beweis: Sei das Ideal $\boldsymbol{a}$ additiv erzeugt von $\alpha_1, \dots \alpha_n$ sodass Γ von $x(\alpha_1), \dots x(\alpha_n)$ erzeugt wird. Sei B die Matrix mit Einträgen $(b_{i,j})_{i,j=1}^n = \sigma_i(\alpha_j), \quad 1 \leq i \leq n$. Dann ergibt Proposition 3.4 und die Definition von $d(K)$ dass $d_{K/\mathbb{Q}}(\boldsymbol{a}) = N(\boldsymbol{a})^2 d(K) = \det(B)^2$, weil die Norm eines Ideals per definitionem genau mit dem Index aus Proposition 3.4 übereinstimmt. Andererseits ist $|\det(B)| = \Delta$, weil die Zeilen von B über die isometrische Abbildung x das Gitter aufspannen. Diese beiden Erkenntnisse zusammen liefern die Gleichung. □

Lemma 4.4. $V = \frac{2^{s+t}\pi^t R_K}{\omega(K)}$

Beweis: Bezeichne wieder $\boldsymbol{F}$ die Menge um deren Volumen V es hier geht. Seien weiters $\boldsymbol{F}_K$ die Abbildungen $\boldsymbol{F}_K(x) = e^{\frac{2\pi k}{\omega(K)}} x, \quad 0 \leq k \leq (K)$ auf $\boldsymbol{F}$ definiert. Die Multiplikation mit Einheiten änder das Volumen nicht, daher $\mathrm{vol}(\boldsymbol{F}) = \mathrm{vol}(\boldsymbol{F}_k)$. Darüber hinaus bezeichne $\overline{\boldsymbol{F}}$ den Durchschnitt von $\cup_{k=0}^{\omega(K)} \boldsymbol{F}_k$ mit der Menge $\boldsymbol{G} := \{(x_1, \dots x_s; x_{s+1}, \dots x_{s+t}) \in \Lambda^{s,t} : \quad x_1 > 0, \dots x_s > 0\}$. Nach dieser Restriktion für $\boldsymbol{G}$ erkennt man durch Multiplikation mit je einem der 2^s Elementen aus $(\pm 1, \pm 1, \dots \pm 1; 1, \dots 1)$ dass

$$V = \mathrm{vol}(\boldsymbol{F}) = \frac{2^s}{\omega(K)} \mathrm{vol}(\overline{\boldsymbol{F}}). \tag{4.6}$$

Es ist also hinreichend, $\overline{\boldsymbol{F}}$ zu berechnen, was mit Hilfe geeigneter Koordinatentransformationen gelingt.
Fasse jedes $x \in \overline{\boldsymbol{F}} \subset \Lambda^{s,t}$ als reellen Punkt auf via

$$(x_1, \dots x_s; x_{s+1}, \dots x_{s+t}) = (\rho_1, \dots \rho_s; \rho_{s+1}, \phi_{s+1}, \dots \rho_{s+t}, \phi_{s+t}), \quad \rho_i := |x_i|, \quad \phi_i := \arg(x_i)$$

Aus der Umrechnung gegenüber den kartesischen Parametern wenn man $x_j = y_j + i \cdot z_j$ anschreibt ergibt sich elementar die Funktionaldeterminante $\rho_{s+1}\rho_{s+2} \dots \rho_{s+t}$, die in der abschließenden Rechnung eingeht. Es ergibt sich weiter, dass sich der Bereich $\overline{\boldsymbol{F}}$, der nun durch die beschränkte Normbedingung und weitere Einschränkungen gegeben ist, sich zur Menge transformiert die folgende Eigenschaften hat

$$\rho_i \geq 0, \quad 1 \leq j \leq s + t$$

$$\prod_{i=1}^{s+t} \rho_j^{e_j} \leq 1$$

wobei e_i die i-te Koordinate von $\lambda = (1, 1, \dots 1; 2, \dots 2)$ bezeichnet, und

$$0 \leq \xi_i < 1, \quad 1 \leq i \leq s+t-1$$

wobei die ξ_i gegeben sind also Koeffizienten der logarithmischen Darstellung (4.4), also

$$\log(\rho_j^{e_j}) = \frac{e_j}{n} \log(\prod_{k=1}^{s+t} \rho_k^{e_k}) + \sum_{k=1}^{s+t-1} \xi_k l_j(\epsilon_k), \quad 1 \leq j \leq s+t$$

Die Winkel $\phi_{s+1}, \dots \phi_{s+t}$ sind gänzlich uneingeschränkt in $[0, 2\pi)$.
Wir führen eine weitere Variablentransformation durch, wobei wir nun gemäß der Beziehungen

$$\log(\rho_j^{e_j}) = \frac{e_j}{n} \log(\xi) + \sum_{k=1}^{s+t-1} \xi_k l_j(\epsilon_k) \tag{4.7}$$

die ρ_i durch $\xi, \xi_1, \dots \xi_{s+t-1}$ ersetzen. Beachtet man

$$\sum_{i=1}^{s+t} e_i = n, \qquad \sum_{i=1}^{s+t} l_j(\epsilon_k) = 0 \tag{4.8}$$

und wendet man die Exponentialfunktion auf (4.7) an erkennt man: $\xi = \prod_{i=1}^{s+t} \rho_i^{e_i}$ und der Bereich $\overline{\boldsymbol{F}}$ ist neuen Koordinaten nun einfach gegeben durch $\{(\xi, \xi_1, \dots \xi_{s+t}) : 0 < \xi \leq 1, 0 \leq \xi_k < 1, \quad 1 \leq k \leq s+t-1\}$. Wir benötigen noch die Funktionaldeterminante T der zweiten Transformation:

$$\text{T= det} \begin{pmatrix} \frac{\rho_1}{n\xi} & \frac{\rho_1}{e_1} l_1(\epsilon_1) & \dots & \frac{\rho_1}{e_1} l_1(\epsilon_{s+t-1}) \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ \frac{\rho_{s+t}}{n\xi} & \frac{\rho_{s+t}}{e_{s+t}} l_{s+t}(\epsilon_1) & \dots & \frac{\rho_{s+t}}{e_{s+t}} l_{s+t}(\epsilon_{s+t-1}) \end{pmatrix}$$

Indem man den $n\xi$-Term aus der 1. Spalte herauszieht sowie jeweils ρ_i aus der i-ten Spalte und mit dem Produkt der e_i gleich 2^t erweitert ergibt sich weiter

$$T = \frac{\rho_1 \rho_2 \cdots \rho_{s+t}}{n\xi 2^t} \det \begin{pmatrix} e_1 & l_1(\epsilon_1) & \dots & l_1(\epsilon_{s+t-1}) \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ e_{s+t} & l_{s+t}(\epsilon_1) & \dots & l_{s+t}(\epsilon_{s+t-1}) \end{pmatrix}$$

$$= \det \begin{pmatrix} n & 0 & \dots & 0 \\ e_2 & l_2(\epsilon_1) & \dots & l_2(\epsilon_{s+t-1}) \\ \dots & \dots & \dots & \dots \\ e_{s+t} & l_{s+t}(\epsilon_1) & \dots & l_{s+t}(\epsilon_{s+t-1}) \end{pmatrix}$$

wegen (4.8). Diese Determinante ist nR_K. Folglich $J = \frac{\rho_1 \dots \rho_{s+t}}{n(\rho_1 \dots \rho_s \rho_{s+1}^2 \dots \rho_{s+t}^2)2^t} nR_K$. Mithilfe des Transforamtionssatzes für Integrale und unseren beiden errechneten Funktionaldeterminanten haben wir

$$\begin{aligned} \mathrm{vol}(\overline{\boldsymbol{F}}) &= 2^t \int \dots \int_{\boldsymbol{F}} dx_1 \dots dx_s dy_{s+1} dz_{s+1} \dots dy_{s+t} dz_{s+t} \\ &= 2^t \int \dots \int_{\boldsymbol{F}} \rho_{s+1} \dots \rho_{s+t} d\rho_1 \dots d\rho_{s+t} d\phi_1 \dots d\phi_{s+t} \\ &= 2^t (2\pi)^t \int_0^1 \dots \int_0^1 \rho_{s+1} \dots \rho_{s+t} |T| d\xi d\xi_1 \dots d\xi_{s+t} d\phi_1 \dots d\xi_{s+t} \\ &= 2^t (2\pi)^t \frac{R_K}{2^t} = 2^t \pi^t R_K \end{aligned}$$

Aufgrund von (4.6) ist somit unser Lemma bewiesen. □

Nun ist der Beweis von Satz 4.1 gründlich vorbereitet.

Beweis: Das geometrische Lemma mit den eben erarbeiteten Formeln für Δ und V eingesetzt zusammen mit (4.5) liefern

$$\lim_{s \to 1} (s-1) f_A(s) = N(\boldsymbol{a}) \frac{2^{s+t} \pi^t R_K}{\omega(K) N(\boldsymbol{a}) \sqrt{|d(K)|}} = \frac{2^{s+t} \pi^t R_K}{\omega(K) \sqrt{|R_K|}}$$

Summation dieser von A unabhängigen Größe über die $h(K)$ Idealklassen $A \in H(K)$ ergibt $\lim_{s \to 1}(s-1)\zeta_K(s) = \sum_{A \in H(K)} \lim_{s \to 1}(s-1) f_A(s) = \frac{2^{s+t} \pi^t R_K}{\omega(K)\sqrt{|R_K|}} \cdot h(K)$ □

Diese Formel ermöglicht also die Berechnung der Klassenzahl bei guter Kenntnis der zum Zahlkörper gehörigen Zetafunktion- abgesehen von den anderen auftretenden Größen die meist etwas weniger problematisch sind. Diese ist allerdings im allgemeinen schwer verständlich, wie bespielsweise der noch immer offene Beweis der Riemannvermutung untermauern. Für den Spezialfall abelscher Zahlkörper wie sie später vorgestellt werden, lässt sich die Zetafunktion in der Formel durch etwas leichter verständliche analytische Ausdrücke beschreiben. Dafür sind aber viele weitere Definitonen und Vorbereitungen von Nöten, die in den nächsten Kapiteln aufgebaut werden. Darauf steuern wir nun hin.

Kapitel 5

Abelsche Zahlkörper

5.1 Bewertungen und L-Reihen

Definition 5.1 (Bewertung)**.** Sei K ein Körper. Ein Homomorphismus v der multiplikativen Gruppe $K \setminus \{0\}$ in die Gruppe der positiven reellen Zahlen, der

$$v(x+y) \leq v(x) + v(y)$$

erfüllt, an die Stelle 0 fortgesetzt durch $v(0) = 0$, heißt *Bewertung von* K.

Jede Bewertung v induziert eine Metrik via $d(x,y) = v(x-y)$, und macht die additive und multiplikative Gruppe von K zu topologischen Gruppen, da die Stetigkeit der Operationen jeweils gewährleistet ist (was bei der Addition trivial ist). Diese Gruppen sind im allgemeinen nicht lokalkompakt oder vollständig. Die konstante Einsfunktion als Bewertung heißt *triviale Bewertung.*

Definition 5.2 (äquivalente Bewertungen)**.** Zwei Bewertungen heißen äquivalent, wenn sie die selbe Topologie erzeugen.

Proposition 5.1. Sind v, w äquivalente Bewertungen dann existiert ein $a > 0$ mit

$$w(x) = v(x)^a \tag{5.1}$$

Beweis: Ist v die triviale Bewertung, dann erzeugt es die diskrete Topologie und gäbe es ein x mit $0 < w(x) < 1$ so führt $\lim x^n = 0$ ebenso auf einen direkten Widerspruch wie $w(x) > 1$. Sei v nun nichttrivial und x_0 ein festes Element mit $v(x_0) \neq 0$ und setze $a := (\log(w(x_0)))/(\log(v(x_0)))$. Es gilt nun

$$\{x \in K : v(x) > 1\} = \{x \in K : w(x) > 1\} \tag{5.2}$$

weil das genau die Menge der x sind für die x^n in der laut Voraussetzung gleichen Topologie gegen 0 konvergiert. Definiere nun zu $x \in K$

$$b_1(x) := \frac{\log(w(x))}{\log(w(x_0))}, \qquad b_2(x) := \frac{\log(v(x))}{\log(v(x_0))}$$

und sei $b_1 < q = m/n \in \mathbb{Q}$. Es folgt $w(x_0^m) > w(x^n)$ und weiter $w(x_0^m x^{-n}) > 1$ und nach voriger Feststelung (5.2) auch $v(x_0^m x^{-n}) > 1$ und in Folge $v(x_0^m) > v(x^n)$. Daraus folgt

$b_1 \geq q \geq b_2$. Vertauschung von v, w liefert insgesamt $b_1 = b_2$ oder $\frac{b_1}{b_2} = 1$ unabhängig von x was zur Behauptung (5.1) gleichwertig ist. □

Definition 5.3 ((nicht-)archimedische Bewertung)**.** Erfüllt eine Bewertung v die Beziehung

$$v(x+y) \leq \max\{v(x), v(y)\}, \qquad x, y \in K$$

so heißt sie *nichtarchimedisch*, ansonsten *archimedisch*.

Eine Bewertung heißt weiter *diskret*, wenn die Werte von $\log(v)$ diskret sind. Diese sind verwandt mit dem Begriff des Exponents:

Definition 5.4. Ein surjektiver Homomorphismus $n : K^* \mapsto \mathbb{Z}$, der die Bedingung

$$n(a+b) \geq \min(n(a), n(b))$$

erfüllt, heißt *Exponent von K*.
Sei weiter $P \triangleleft R$ Primideal in einem Ring R mit Quotientenkörper K und $x \in K^*$ und schreibe das Hauptideal xR als $xR = P^{n(x)}I$ mit einem gebrochenen Ideal I in dessen Primidealzerlegung kein P-Faktor vorkommt. Dies ist ein Exponent n nach obiger Definiton. Dann nennen wir die Bewertung die durch

$$v(x) = N(P)^{-n(x)}$$

entsteht *normalisierte Bewertung zu P*. Die von P über die von zu oben definiertem Exponent gehörige Bewertung erzeugte Topologie heißt *P-adische Topologie* auf K. Ist speziell $R = \mathbb{Z}$ und $P = p\mathbb{Z}$ so nennen wir die Topologie *p-adische Topologie*.

Man kann für beliebiges $c \in R$ durch $v := c^{n(x)}$ eine (nichtnormalisierte) Bewertung definieren.

Lemma 5.1. Sei zu gegebenem Exponent n auf K

$$R_n := \{x \in K : \quad n(x) \geq 0\}, \quad P_n := \{x \in K : n(x) > 0\}$$

dann gilt: R_n ist Hauptidealring und P_n das eindeutige von Null verschiedene Primideal von R_n. Es wird von jedem $a \in K$ mit $n(a) = 1$ erzeugt.

Beweis: Aus der Definition von n folgt sofort, dass Addition und Multiplikation in R_n uneingeschränkt möglich ist, es sich daher um einen Ring handelt. Ebenso leicht sieht man dass $P_n \triangleleft R_n$. Um einzusehen, dass P_n das einzige Primideal von R_n ist, betrachte zunächst $a \in R_n \setminus P_n$. Die Definitonen von R_n, P_n zeigen $n(a) = 0$, weil n Homomorphismus ist auch $n(a^{-1}) = 0$, und $a^{-1} \in R_n$. Das heißt aber, dass P_n genau aus den invertierbaren Elementen von R_n besteht. Nach Lemma 2.5 ist es das eindeutige maximale Ideal. Wir zeigen, dass P_n Hauptideal ist. Sei a mit $n(a) = 1$ gewählt. Aus der Homomorphieeigenschaft kann man weiter schließen: Es gilt $aP_n \subset R_n$ und für beliebiges $b \in P_n$ mit $n(b) = m$ (m beliebig) gilt $a^{-m}b \in R_n$. Weiter also $b = a^m(ba^{-m}) \in a^m R_n$ und $P_n \subset aR_n$ zeigt die andere Inklusion, also

$$P_n = aR_n \tag{5.3}$$

Um den Beweis abzuschließen zeigen wir, dass jedes von Null verscheidene Ideal von R_n Hauptideal und Potenz von P_n ist. Der Beweisgedanke der letzten Feststellung (5.3) iteriert liefert $P_n^k = a^k R_n = \{a \in K : \quad n(a) = k\}$. Sei $I \triangleleft R_n$ Ideal. Weil P_n eindeutig maximal ist gilt $I \subset P_n$, da jedes Ideal in einem maximalen Ideal enthalten ist. Wähle N so, dass $I \subset P^N$, $I \nsubseteq P^{N+1}$. Wegen $\cap_N P^N = 0$ ist dies wohldefiniert. Sei $c \in I$ mit $n(c) = N$ (beachte dass n nach Definition surjektiv ist). Dann $c = a^N d$ mit $d \in R_n$ und $n(d) = 0$. Deshalb ist d invertierbar in R_n und die Elemente $a^N R_n$ und cR_n stimmen überein. Daraus kann man $P_n^N = a^N R_n = bR_n \subset I$. Die umgekehrte Inklusion ist aber trivial, weil P_n maximal ist. Also $P_n^N = I$. Weiters wird es von a^N erzeugt. □

Definition 5.5. R_n und heißt *Exponentenring* von n oder auch *Bewertungsring zu* v wenn v eine Bewertung induziert von n ist. P_n heißt *Ideal zum Exponent* n bzw *Ideal zur Bewertung* v.

Für den Fall einess von einem Primideal induzierten Exponenten geben wir einige Eigenschaften an.

Proposition 5.2. Sei R Dedekindring mit Quotientenkörper K, $0 \neq P \triangleleft R$ Primideal und n der von P erzeugte Exponent in K. Dann gilt:

1. $$R_n = \{(\frac{a}{b} \in K : \quad a, b \in R, \quad b \notin P\}, \quad P_n = \{(\frac{a}{b} \in K : \quad a, b \in R, \quad a \in P \quad b \notin P\}$$

2. $$P_n^m \cap R = P^m, \qquad m \geq 1$$

3. $$P_n^m = P^m R_n, \qquad m \geq 1$$

4. $$R/P^m \cong R_n/P_n^m, \qquad m \geq 1$$

5. $$\bigcap_{P \triangleleft R} R_n = R$$

   wobei der Durchschnitt über die Primideale von R erstreckt wird.

Beweis:

1. Seien $a, b \in R$, $b \notin P$, dann ist $n(\frac{a}{b}) \geq 0$, also $\frac{a}{b} \in R_n$. Ist umgekehrt $x \in R_n$, so kann man $xR = IJ$ schreiben mit I, J Ideale von R mit $P \nmid J$. Aus dem Kontext des chinesischen Restsatzes lässt sich herleiten, dass stets ein Ideal $A \triangleleft R$ existiert mit $P \nmid A$ und AJ ist Hauptideal. Es sei hier ohne genauen Beweis nur erwähnt. Wir haben dann weiter $xR = (AI)/(AJ)$ mit Hauptidealen AI, AJ- denn wäre AI nicht Hauptideal, könnten nicht xR und A/J welche sein- mit Erzeugern die wir a, b nennen, also $AI = aR$, $AJ = bR$. Nach Voraussetzung $b \notin P$ und $x = \frac{ac}{b}$ mit $c \in R$. Dies zeigt die andere Inklusion

$$R_n \subset \{(\frac{a}{b} \in K : \quad a, b \in R, \quad b \notin P\}$$

und damit die erste Gleichung. Für P_n sieht man obige Formel indem man bemerkt, dass für beliebiges $\theta \in P \setminus P^2$ nach dem Beweis von Lemma 5.1 $P_n = \theta R_n$ gilt.

2. Der zweite Punkt folgt unmmittelbar aus der evidenten Gleichheit $P^m = \{a \in R : n(a) \geq m\}$.

3. Wieder wegen $P_n = \theta R_n$ für $\theta \in P \setminus P^2$ sieht man $P_n \subset PR_n$. Andererseits ist nach Punkt 1 jedes $x \in PR_n$ von der Form

$$x = a_1 b_1 + \ldots + a_n b_n, \qquad a_i \in R, \quad n(a_i) \geq 1, \quad n(b_i) \geq 0$$

Daher $n(x) \geq \min_i\{n(a_i b_i)\} \geq 1$ was $x \in P_n$ nach sich zieht, wegen der Beliebigkeit von x gilt auch die andere Inklusion $PR_n \subset P_n$ und damit natürlich $P_n^m = P^m R_n$, der dritte Punkt.

4. Die Einbettung $R \subset R_n$ induziert wegen $P^m \subset P^m R_n = P_n^m$ einen Homomorphismus

$$\varphi : R/P^m \longmapsto R_n/P_n^m$$

Sei $\overline{a} \in R/P$ im Kern von φ, $a \in \overline{a}$. Weil $\varphi(\overline{a})$ die Klasse von $a \pmod{P_n^m}$ in R_n ist, gilt

$$a \in P^m R_n \cap R = P^m \tag{5.4}$$

wobei obiger Punkt 2 in (5.4) verwendet wurde. (5.4) heißt aber gerade $\overline{a} = 0$, also ist φ injektiv. Sei nun $a \in R_n$. Um zu zeigen, dass φ surjektiv ist, konstruieren wir ein $x \in R$ mit $a - x \in P_n^m$. Schreibe a als $\frac{a_1}{b_1}$ und setze $r := n(a_2)$. Nach Definiton von R_n gilt $n(a_1) \geq r$ also $a \in P^{m+r} + a_2 R = P^r$. Nach dem chinesischen Restsatz hat $a_2 x \equiv a_1 \pmod{P^{m+r}}$ eine Lösung x in R. Diese leistet angesichts

$$n(a - x) = n(a_1 - a_2 x) - n(a_2) \geq m \quad \Leftrightarrow \quad a - x \in P_n^m$$

das Gewünschte. Also ist φ Isomorphismus.

5. Die Inklusion $R \subset \cap R_n$ ist trivial, ist umgekehrt $a \in K$ im Durchschnitt so sind die Exponenten zu a bezüglich jedem Primideal nichtnegativ, also ist aR echtes Ideal von R und daher $a \in R$. Das zeigt den letzten Punkt.

□

Definition 5.6 (Dirichlet-Charakter)**.** Ein Homomorphismus χ einer Gruppe G in den komplexen Torus heißt *Dirichletcharakter der Gruppe.*

Bemerkung: Das Bild eines Homomorphismus einer endlichen Gruppe in die komplexen Zahlen ist ohnehin wegen $a^{|G|} = 1$ stets im Torus enthalten. Die Charaktere bilden bezüglich der Hintereinanderausführung eine Gruppe, die insbesondere im Fall endlicher abelscher Gruppen isomorph zur Gruppe selbst ist. Dies sieht man mithilfe des Hauptsatzes für endlich erzeugte abelsche Gruppen ein, da es für zyklische Gruppen offenbar gilt- sie sind durch das Bild eines Erzeugers vollständig festgelegt- und damit auch für

direkte Produkte selbiger.

Dieses Konzept wollen wir auf Ideale übertragen.
Sei K Zahlkörper mit Ganzheitsring O_K und $0 \neq I \triangleleft O_K$ und bezeichne $G(I)$ die Gruppe der zu I relativ primen Klassen Modulo I. Dann definiert für jeden Dirichletcharakter χ

$$\chi(a) = \begin{cases} \chi(a \pmod I), & (a \pmod I) \in G(I) \\ 0, & sonst \end{cases}$$

einen Dirichletcharakter auf $G(I)$, denn die Multiplikativität bleibt erhalten. Diesen Charakter auf der Faktorgruppe nennen wir fortan *Heckecharakter* statt Dirichletcharakter.

Definition 5.7. Ein Heckecharakter auf $G(I)$ wie oben heißt *primitiv*, falls es kein Ideal $J \neq I$, $J|I$ gibt mit der Eigenschaft, dass

$$(xO_K, I) = 1 \quad \wedge \quad x \equiv 1(J) \quad \Longrightarrow \quad \chi(x) = 1$$

Bemerkung: Für Primideale ist jeder nichttriviale Charakter von $G(I)$ primitiv und der triviale Charakter ist nur für auf $G(1)$ primitiv.

Beispiel: Ein Charakter auf $(\mathbb{Z}/m\mathbb{Z})^*$ ist primitiv wenn es keine Darstellung

$$(\mathbb{Z}/m\mathbb{Z})^* \longrightarrow (\mathbb{Z}/\overline{m}\mathbb{Z})^* \longrightarrow \mathbb{C}$$

gibt mit $\overline{m}|m, \overline{m} \neq m$ und einem Dirichletcharakter $\overline{\chi} : (\overline{m}Z)^* \longrightarrow \mathbb{C}$.

Eine wichtige Erkenntnis ist, dass jeder Charakter χ_0 von $G(I)$ als primitiver Charakter von $G(J)$ für ein $J|I$ aufgefasst werden kann. Dazu bemerke man für zunächst beliebiges $I_1|I$ den kanonischen Isomorphismus zwischen der Untergruppe der Charaktergruppe von $G(I)$ die trivial auf der Klasse 1 mod (I_1) wirkt und der Gruppe der Charaktere auf $G(I/I_0)$. Wählt man I_0 als kleinstes gemeinsames Vielfaches aller Ideale I_1 die I teilen für die der zugehörige Charakter trivial auf der Restklasse 1 mod(I/I_1) wirkt, so ist $J := I/I_0$ das gefordere Ideal. J heiße *Führer* von χ_0.
Es wird also jeder Charakter von einem primitiven Charakter $\pmod J$ induziert. Weiters kann man aus dem chinesischen Restsatz schließen, dass für paarweise relativ prime Ideale $I_1, I_2 \ldots, I_k$ gilt

$$G(I_1 I_2 \ldots I_k) = G(I_1) \times G(I_2) \ldots \times G(I_k)$$

Insbesondere muss man einen Charakter nur auf solchen Bausteinen kennen:

$$\chi(x \pmod{\prod_{j=1}^{k} I_j}) = \prod_{j=1}^{k} \chi(x \pmod{I_j})$$

wobei χ_j als Charakter auf $G(I_j)$ definiert ist durch

$$\chi(x \pmod{I_j}) = \chi(u)$$

mit

$$u \equiv x \pmod{I_j} \quad \wedge \quad u \equiv 1 \pmod{I/I_j}.$$

Proposition 5.3. Ist $I = I_1 I_2 \dots I_k$ mit paarweise relativ primen Idealen I_j und χ ein Charakter auf $G(I)$ so ist dieser primitiv genau dann wenn alle von den I_i wie oben induzierten χ_i primitiv sind.

Beweis: Seien $J_1, \dots J_k$ die Führer von $\chi_1, \dots \chi_k$. Bemerke zunächst, dass für $x \equiv 1 \pmod{J}$ mit $J := J_1 J_2 \dots J_k$ gilt

$$\chi(x) = \prod_{i=1}^{k} \chi_i(x) = 1 \tag{5.5}$$

Ist nun ein χ_i nicht primitiv, so heißt das per definitionem genau $I_i \neq J_i$, woraus mithilfe von (5.5) $I \neq J$ folgt und daher ist χ nicht primitiv. Ist umgekehrt χ nicht primitiv, dann gibt es ein echtes Ideal $J = J_1 \dots J_k$ von I mit $\chi(x) = 1$ für $x \equiv 1 \pmod{J}$, wobei $J_i | I_i$ für alle i. Daraus folgt aber $I_{i_0} \neq J_{i_0}$ für mindestens ein i_0. Dieses i_0 liefert wegen $\chi_{i_0}(x) = 1$ für $x \equiv 1 \pmod{J_{i_0}}$, dass χ_{i_0} nicht primitiv ist. Damit sind beide Richtungen gezeigt. □

In Analogie zu den Zetafunktionen eines Zahlkörpers kann man für Heckecharaktere und gegebenes Ideal $M \triangleleft O_K$ komplexwertige Reihen der Form

$$L(\chi, s) := \sum_{\boldsymbol{a} \triangleleft O_K} \chi(\boldsymbol{a}) N(\boldsymbol{a})^{-s}$$

definieren, wobei $\boldsymbol{a}$ die ganzen Ideale des Ganzheitsrings von K durchläuft und χ ein Heckecharakter auf $G(\boldsymbol{a})$ ist der durch $\chi(\boldsymbol{a}) = 0$ wenn $\boldsymbol{a}$ nicht relativ prim zu M ist, auf alle ganzen Ideale fortgesetzt wird. Diese nennen wir die zum Charakter χ gehörige *L-Reihe*. Im Fall von $\boldsymbol{a} = m \cdot \mathbb{Z}$ entspricht diese Reihe einfach

$$L(\chi, s) := \sum_{n=0}^{\infty} \chi(n) n^{-s}$$

Man sieht ganz ähnlich wie bei der Zetafunktion eines Zahlkörpers:

Proposition 5.4. L-Reihen sind in der Halbebene $\mathrm{Re}(s) > 1$ lokal gleichmäßig konvergent und stellen dort folglich holomorphe Funktionen dar. Weiters gilt die Produktdarstellung

$$L(\chi, s) = \prod_{P} (1 - \chi(P) N(P)^{-s})^{-1}$$

wobei P die Primideale von O_K durchläuft.

5.2 Abelsche Zahlkörper

Definition 5.8. Die *Galoisgruppe* einer normalen Körpererweiterung L/K ist die Menge der Automorphismen von L die K fest lassen, in Zeichen $Gal(L/K)$, oder wenn keine Verwechslungsgefahr besteht auch $G(L/K)$. Diese bilden bezüglich der Hintereinanderausführung eine Gruppe. Insbesondere ist $Gal(K/\mathbb{Q})$ die Menge der Körperautomorphismen eines Zahlkörpers K.

Bemerkung: Man beachte, dass der Buchstabe G auch für die Idealgruppe $G(I)$ eines Ideals sowie später $G(m)$ für die Gruppe von multiplikativ invertierbaren Elementen (mod m) von $(\mathbb{Z}/m\mathbb{Z}, \cdot)$ verwendet wird. Verwechslungen sind wegen der verschiedenen Argumente aber ausgeschlossen.

Bemerkung: Die Gruppeneigenschaften sind unmittelbar nachzurechnen und die 2. Behauptung folgt, weil $\mathbb{Q}$ bei jedem Automorphismus fixiert wird.

Definition 5.9. Ein abelscher Zahlkörper ist ein Zahlkörper mit abelscher Galoisgruppe $Gal_{K/\mathbb{Q}}$

Definition 5.10 (normal)**.** Eine Körpererweiterung L/K heißt *normal*, wenn L Zerfällungskörper einer Menge von Polynomen über K ist.

Definition 5.11. Eine *Galoiserweiterung* ist eine endlichdimsensionale, normale, separable Körpererweiterung.

Bemerkung: Man sieht sofort aus der Definition, dass wenn $M \subset K \subset L$ Körpererweiterungen sind und $L : M$ Galoiserweiterung ist, dann ist auch $L : K$ Galoiserweiterung. Wir formulieren nun eine Variante des bekannten Hauptsatzes der Galoistheorie im für uns relevanten Fall.

Satz 5.1 (Hauptsatz der Galoistheorie)**.** Für eine Galoiserweiterung ist der Verband der Untergruppen der Galoisgruppe isomorph zum Verband der Zwischenkörper der Erweiterung. Genauer gilt: Sei $M \subset L$ Galoiserweiterung. Es gilt für alle Untergruppen H der Automorphismengruppe $G := Gal(L/M)$ sowie alle Zwischenkörper $M \subset K \subset L$ mit

$$fix(K) := \{\sigma \in G : \sigma(x) = x \quad \forall x \in K\}$$

$$FIX(H) := \{x \in L : \sigma(x) = x \quad \forall \sigma \in H\}$$

dass fix und FIX Bijektionen zwischen der Menge der Untergruppen der Galoisgruppe G und der Menge der Zwischenkörper darstellen. Es gilt $fix(FIX(H)) = H$, sowie $FIX(fix(K)) = K$. Die Untergruppen der Galoisgruppe stehen in einem 1:1 Verhältnis mit Zwischenkörpern. Weiters ist $[L : K] = |Gal(L/K)|$, insbesondere $[L : M] = |Gal(L/M)|$.

Obiger Satz zeigt, dass wenn eine Galoiserweiterung L/K vorliegt- und nur in diesem Fall- die Monomorphismen aus Satz 1.6 Körperautomorphismen von L sind.

Im uns interessierenden Fall von Zahlkörpern wird oft $M = \mathbb{Q}(\alpha)$ ein Zahlkörper sein. Allerdings erfordert die Herleitung der Klassenzahlformel auf unserem Weg auch das Studium allgeinerer Strukturen wie P-adischer Körper. Wir werden den Hauptsatz der Galoistheorie immer wieder implizit verwenden indem wir von der einem Unterkörper $M \subset K \subset L$ einer Körpererweiterung L/K entsprechenden Untergruppe $Gal(K/M)$ der Galoisgruppe $Gal(L/M)$ der Erweiterung im Sinne der Galoistheorie sprechen.

Definition 5.12. Ein algebraischer Zahlkörper heißt *Kreisteilungskörper*, wenn er durch Adjunktion einer komplexen Einheitswurel zu $\mathbb{Q}$ entsteht, $K = \mathbb{Q}(\zeta_m)$.

Eine k-te Einheitswurzel ζ heiße im folgenden *primitiv*, wenn ihre multiplikative Ordnung k ist.

Wir studieren nun die Galoisgruppen von Kreisteilungskörpern.

Satz 5.2. Sei ζ eine primitive p^n-te Einheitswuzel, $r := \varphi(p^n) - 1 = p^{n-1}(p-1) - 1$, $N := n\varphi(p^n) - p^{n-1}$. Betrachte $K = \mathbb{Q}(\zeta)$. Diese Erweiterung $K/\mathbb{Q}$ ist normal von Grad

$$[K : \mathbb{Q}] = \varphi(p^n) \tag{5.6}$$

Die Elemente $1, \zeta, \ldots \zeta^r$ bilden eine Ganzheitsbasis von K und es gilt

$$d(K) = (-1)^{p(p-1)/2} p^N$$

Die Galoisgruppe von $K/\mathbb{Q}$ ist isomorph zur multiplikativen Gruppe $G(p^n)$ der nicht durch p teilbaren Restklassen $\pmod{p^n}$.

Beweis: Weil ζ primitiv ist, sind alle anderen Einheitswurzeln in $\mathbb{Q}(\zeta)$ enthalten. Diese sind aber die Konjugierten von ζ, also ist K normale Erweiterung. Um (5.6) zu zeigen müssen wir zeigen, dass das Polynom $W(x) = (x^{p^n} - 1)/(x^{p^{n-1}} - 1)$ irreduzibel über $\mathbb{Q}$ ist, denn $W(\zeta) = 0$. Setze $F(x) := W(x + 1)$. Einfache Induktion zeigt

$$(1 + x)^{jp^{n-1}} = (1 + x^{p^{n-1}})^j + pW_j(x), \quad (j \geq 1)$$

mit einem Polynom $W_j(x)$ vom Grad kleiner als jp^{n-1}. Es ergibt sich weiter

$$F(x) = pV(x) + \sum_{j=0}^{p-1} (1 + x^{p^{n-1}})^j = pV(x) + \sum_{j=1}^{p} \binom{p}{j} x^{p^{n-1}(j-1)}$$

mit einem Polynom $V(x)$ vom Grad kleiner als $(p-1)p^{n-1}$. Wegen $F(0) = W(1) = p$ zeigt das, dass F Eisensteinpolynom bezüglich p ist und daher irreduzibel, natürlich gleiches für W.
Fehlt noch die Aussage über die Diskriminante. Nach Proposition 3.3 haben wir

$$d_{K/\mathbb{Q}}(\zeta) = (-1)^{p(p-1)/2} N_{K/\mathbb{Q}}(W'(\zeta)) \tag{5.7}$$

Es gilt

$$W'(x)(x^{p^{n-1}} - 1) + p^{n-1} W(x) x^{p^{n-1}-1} = p^n x^{p^n - 1}$$

Weil $\eta := \zeta^{p^{n-1}}$ primitive p-te Einheitswurzel ist vereinfacht sich die obige Gleichung zu $W'(\zeta)(\eta - 1) = p^n \zeta^{-1}$ und weiter

$$N_{K/\mathbb{Q}}(W'(\zeta)) = N_{K/\mathbb{Q}}(p^n(\eta - 1)\zeta)^{-1} = p^{n\varphi(p^n)} N^{-1}_{K/\mathbb{Q}}((\eta - 1)\zeta) \tag{5.8}$$

Wir bemerken nun dass $N_{K/\mathbb{Q}}(\zeta) = 1$, sowie dass $\eta - 1$ Nullstelle des Polynoms $(x+1)^{p-1} + \ldots + (x+1) + 1$ ist. Setzt man nun $L := \mathbb{Q}(\eta)$ so führt das zu

$$N_{K/\mathbb{Q}}(\eta - 1) = N_{L/\mathbb{Q}}(N_{K/L}(\eta - 1)) = N_{L/\mathbb{Q}}((\eta - 1)^{p^{n-1}}) = p^{p^{n-1}} \tag{5.9}$$

(Dabei ist Proposition 1.1 eingegangen). (5.7), (5.8) und (5.9) rückwärts ineinander eingesetzt, die Multiplikativität der Norm in der rechten Seite von (5.8) ausgenutzt ergeben die gewünschte Formel

$$d_{K/\mathbb{Q}}(\zeta) = (-1)^{p(p-1)/2} p^N$$

Aus der Produktdarstellung von $d_{K/\mathbb{Q}}$ folgt sofort $d_{K/\mathbb{Q}}(\zeta) = d_{K/\mathbb{Q}}(\zeta - 1)$ und $(\zeta - 1)$ erfüllt eine Eisensteingleichung $\pmod p$. Daher ist $d_{K/\mathbb{Q}}(\zeta) = d(K)$ und damit bilden die Potenzen von ζ eine Ganzheitsbasis, siehe Korollar 3.3.
Wegen der Irreduzibilität von W sind alle primitiven p^n-ten Einheitswurzeln zueinander konjugiert. Das bedeutet aber, dass

$$\zeta \longmapsto \zeta^a, \qquad 0 < a < p^n, \quad p \nmid a$$

einen Automorphismus $G_a \in Gal(K/\mathbb{Q})$ induziert. Die zugehörige Abbildung $G(p^n) \mapsto Gal(K/\mathbb{Q})$ ist offenbar ein Isomorphismus. □

Um den allgemeinen Fall zu behandeln bedarf es einiger Vorbereitungen. Zunächst ein

Lemma 5.2. Jeder algebraische Zahlkörper $K \neq \mathbb{Q}$ erfüllt $|d(K)| > 1$.

Beweis: Sei $w_1, \dots w_n$ Ganzheitsbasis von K und bezeichne $w_i^{(j)}$ die Konjugierten zu $\sigma_j(w_i)$, $(1 \leq i, j \leq n)$. Wendet man Minkowskis Satz über Linearformen (Korollar 1.2) angewandt auf das System

$$L_j(x_1, \dots x_n) = \sum_{k=1}^{n} w_k^{(j)} x_k \qquad (1 \leq j \leq n)$$

und $M := \{(z_1, \dots, z_n) \in \mathbb{R}^n : z_i \in \mathbb{Z}\}$- dieses hat $d(M) = 1$- unter Berücksichtigung von $|\det[w_i^{(j)}]| = \sqrt{|d(K)|}$ ergibt eine nichttriviale Lösung $(X_1, \dots X_n)$ von

$$|N_{K/\mathbb{Q}}(X_1 w_1 + \dots + X_n w_n)| = \prod_{j=1}^{n} |L_j(X_1, \dots X_n)| < \sqrt{|d(K)|}$$

Die linke Seite ist aber eine von Null verschiedene ganze Zahl, also muss die rechte echt größer als 1 sein. □

5.3 Normabbildung und Inverse Normabbildung

Bzezeichne wieder durchgehend R einen Dedekindring mit Quotientenkörper K, L eine nedliche Erweiterung von K und S den ganzen Abschluss von R in L, sowie $G(K)$ bzw $G(L)$ Gruppen der gebrochenen Ideale von R respective S, und bezeichne mit $I(K)$ bzw $I(L)$ die Halbgruppe der echten Ideale von R bzw S. Um Zusammenhänge zwischen $G(L)$ und $G(K)$ zu verstehen, führen wir zwei Abbildungen ein:

Definition 5.13 (Inverse Normabbildung)**.** Die Abbildung

$$i_{L/K} : G(K) \mapsto G(L)$$

$$A \mapsto AS$$

nennen wir *inverse Normabbildung.*

Unmittelbare Eigenschaften der inversen Normabbildung sind: $i_{L/K}(A)$ ist der kleinste S-Untermodul, der A enthält, und wegen $(AS)(BS) = ABS$ ist sie ein Homomorphismus. Sie ist auch als Mengenfunktion monoton und bildet Hauptideale wieder auf Hauptideale ab.

Primideale von R werden durch die inverse Normabbildung nicht respektiert, gehen also nicht in Primideale in S über. Wir sagen, die in der eindeutigen Primidealzerlegung des Bildes eines Primideals P

$$i_{L/K}(P) = \wp_1^{e_1} \dots \wp_s^{e_s}$$

vorkommenden Primideale $\wp_i$ *liegen über* P und der Exponent e_i heißt *Verzweigungsindex* von $\wp_i$ über K und wir schreiben dafür $e_{L/K}(\wp_i)$. Das Ideal $\wp_i$ heißt im Falle $e_{L/K}(\wp_i) > 1$ *verzweigt*, sonst *unverzweigt*.
Ein Primideal P von R heißt *verzweigt in* L/K, falls mindestens ein Primideal von S das über P liegt verzweigt ist.
Eine Erweiterung L/K heißt *unverzweigt*, falls alle Primideale von S unverzweigt sind.
Teilt darüber hinaus $e_{L/K}(\wp_i)$ die Charakteristik des Körpers $S/\wp_i$, so heißt $\wp_i$ *wild verzweigt*, ansonsten *schwach verzweigt*.

Proposition 5.5. Ist $\wp$ Primideal in S, dann ist $P := \wp \cap R$ das eindeutige Primideal in R, das unter $\wp$ liegt.

Beweis: Sei $J := \wp \cap R$. Es gilt

$$0 \subsetneq J \subsetneq R \tag{5.10}$$

denn J enthält mit jedem $a \in \wp$ auch $N_{L/K}(a)$- die Norm liegt ja stets in R- was die linke Seite von (5.10) zeigt, aber auch $1 \notin J$. Die Einbettung von R in S führt J in $\wp$ über und induziert damit einen Homomorphismus von R/J nach $S/\wp$, der wegen $J = \wp \cap R$ sogar eine Einbettung ist. Letzteres ist aber ein Köper weil $\wp$ Primideal ist, und R/I kann als Unterring eines Körpers keine Nullteiler haben, und das gleiche Argument in die andere Richtung liefert, dass J Primideal in R ist. Wegen $i_{L/K}(J) = S(\wp \cap R) \subset S\wp \cap SR = \wp$ liegt $\wp$ über J. Jedes andere Primideal von R das unter $\wp$ liegt müsste in $\wp \cap R = J$ enthalten sein, und weil Primideale in Dedekindringen maximal sind muss es J gleichen. □

Der Beweis der Proposition zeigt, dass wenn $\wp$ über P liegt, es eine Einbettung von $R/P \mapsto S/\wp$ gibt. Es gilt $[(S/\wp)/(R/P)] \leq [L : K]$, denn ein $a \in S$ erfüllt definionsgemäß eine Gleichung

$$a^n + \sum_{i=1}^{n-1} c_i a^{n-1} = 0, \qquad (c_i \in R, \quad n = [L : K])$$

und für die zugehörige Klasse $\overline{a} \pmod{\wp}$ gilt

$$\overline{a}^n + \sum_{i=1}^{n-1} \overline{c_i} \overline{a}^{n-1} = 0, \qquad (\overline{c_i} \in R/\wp)$$

Definition 5.14. Für ein Primideal über P bezeichnen wir den Grad $[S/\wp : R/P]$ als *Trägheitsgrad von $\wp$ über K* und schreiben dafür $f_{L/K}(\wp)$.

Lemma 5.3. Schreibt man für ein Primideal $P \lhd R$ die Primidealfaktorisierung seiner inversen Normabbildung

$$i_{L/K}(P) = PS = \wp_1^{e_1}\wp_2^{e_2}\dots\wp_s^{e_s}, \qquad \wp_i \lhd S$$

dann gilt mit $f_i := f_{L/K}(\wp_i)$ die Gleichung

$$e_1 f_1 + \ldots + e_s f_s = n$$

Beweis: Sei der Körper $k := R/P$. Die Einbettung $R \mapsto S$ induziert einen Homomorphismus von k nach S/PS, die eine Einbettung ist weil es sich nicht um die Nullabbildung handelt und k ja Körper ist. Diese induziert auf S/PS eine k-Vektorraumstruktur. Gleiches gilt für die Strukturen $S/\wp^{e_i}$.
Wir wollen im nächsten Schritt beweisen, dass seine k-Dimension

$$\dim_k(S/PS) = e_1 f_1 + \ldots + e_s f_s \tag{5.11}$$

gleicht. Nach Lemma 2.6 genügt es sich auf die einzelnen Faktoren zu beschränken, also

$$\dim_k(S/\wp^{e_i}) = e_i f_i, \quad 1 \le i \le s$$

Die Isomorphiesätze für Ideale auf unsere Situation angewandt liefern $(S/\wp_i^m)/(S/\wp_i^{m-1}) \cong \wp_i^{m-1}/\wp_i^m$, zusammen mit Proposition 2.1 ergibt sich

$$\dim_k(S/\wp_i^{e_i}) = e_i$$

Weiter haben wir

$$\dim_k(S/\wp^{e_i}) = (\dim_{S/\wp_i} S/\wp_i^{e_i})(\dim_k S/\wp_i) = e_i f_i,$$

nach Definiton von f_i und (5.11) folgt.
Nun sei an die Definitionen 5.4, 5.5 erinnert. Sei v der von P in K erzeugte Exponent, R' der zugehörige Exponentenring und N der R'-Modul $R'S \subset L$. Schreibe beliebiges $x \in L$ als

$$x = x_1 y_1 + \ldots + x_m y_m, \qquad x_j \in R', \quad y_j \in S$$

Nach Proposition 5.2 Punkt 1 kann man $x_j = \frac{c_j}{b}$ schreiben mit $c_j \in R$ und $b \in R \setminus P$, insbesondere $x = \frac{a}{b}$ mit $a \in S$ und obigem b. Ist $P(t)$ Minimalpolynom von a über K vom Grad r, dann ist offenbar $P(bt)b^{-r}$ Minimalpolynom von x mit Koeffizienten aus R'. Damit ist auch $Sp_{L/K} \in R'$.
Wähle ein Element w aus N, das die Erweiterung L/K erzeugt (siehe Satz vom primitiven Element) und bezeichne seine Konjugierten in $\overline{K}$ mit $w_1, \dots w_n$.
Es gilt $\det[w_j^i]_{i,j=1}^n \neq 0$ und daher ist das System

$$Sp_{L/K}(w^i v_j) = \begin{cases} 1 & \text{für } i+1 = j, \qquad i = 0, 1 \dots n-1, \quad j = 1, 2 \dots n \\ 0 & \text{für } i+1 \neq j, \qquad i = 0, 1 \dots n-1, \quad j = 1, 2 \dots n \end{cases}$$

für $v_1, \dots v_n \in L$ lösbar. Weil die v_j K-linear unabhängig sind, können wir $x \in N$ als $x = x_1 v_1 + \dots + x_n v_n$ mit $x_i \in K$ schreiben. Weil $xw^i \in N$ ist

$$Sp_{L/K}(xw^i) \in R', \quad i = 0, 1 \dots n-1 \tag{5.12}$$

aber auch

$$Sp_{L/K}(xw^i) = \sum_{j=1}^{n} x_j Sp_{L/K}(v_j w^i) = x_{i-1}, \qquad (i = 1, 2 \dots n) \tag{5.13}$$

und nach (5.12) und (5.13) gemeinsam liegen alle x_i in R'. Damit ist N Untermodul des frei von den v_j erzeugten R'-Moduls. Nach Lemma 5.1 ist R' Hauptidealring, ergo hat N höchstens n Erzeuger. Klarerweise ist N torsionsfrei, also ohne Elemente endlicher Ordnung. Ein schon zitiertes Resultat aus Algebra besagt, dass solche endlich erzeugten torsionsfreien Moduln bereits frei sind. Die Dimension des Moduls muss weiter genau n sein, weil der Modul N n K-linear unabhängige Elemente besitzt. Wir können demnach $N = \oplus_{i=1}^{n} u_i R'$ schreiben mit $u_i \in S$. Zu $a \in P \setminus P^2$ betrachte $aN = \oplus_{i=1}^{n} a u_i R'$ und die Funktion

$$\Phi : N \longmapsto (R'/aR')^n$$

$$\sum_{i=1}^{n} a_i u_i \longmapsto [a_1 \pmod{aR'}, \dots, a_n \pmod{aR'}].$$

Diese ist surjektiv und hat Kern aN. Nach dem Homomorphiesatz ist $N/aN \cong (R'/aR')^n$ als abelsche Gruppen. Nach Proposition 5.2(4) $|R'/aR'| = |k|$, also $|N/aN| = |k^n|$ und $\dim_k N/aN = n$.
Zum anderen haben wir aber oben gezeigt, dass der natürliche Isomorphismus von $S/PS \mapsto N/aN$ zur Einbettung von S in N zu $\dim_k N/aN = e_1 f_1 \dots + e_s f_s$ führt. Beide Zahlen müssen also übereinstimmen. □

Sei nun L/K *normale* Erweiterung. Lässt man ein Element g der $Gal(L/K)$ auf ein gebrochenes Ideal von $I \subset L$ wirken, so ist das Bild wieder ein gebrochenes Ideal. Solche Ideale wollen wir als *zueinander konjugiert* bezeichnen. Mit dieser Bezeichnung und der Voraussetzung einer normalen Erweiterung L/K formulieren wir eine Verbesserung obigen Satzes:

Satz 5.3. Ist L/K normal und $P \lhd R$ Primideal von R, dann sind alle Primideale $Q \lhd S$ über P zueinander konjugiert und haben die selben Verzweigungsindizes e und Trägheitsgrade f. Ist g ihre Anzahl, so gilt weiter $efg = n$.

Beweis: Wir müssen zeigen, dass alle Verzweigungsindizes und Grade übereinstimmen. Es reicht darüber hinaus aus zu zeigen, dass die Primideale über P zueinander konjugiert sind. Die Grade f_i sind dann ohnehin gleich und die Gleichheit der e_i sieht man ein, indem man

$$PS = \wp_1^{e_1} \dots \wp_s^{e_s} \tag{5.14}$$

schreibt und die Wirkung eines $g \in Gal(L/K)$ ansieht. Sind die Ideale über P konjugiert, dann werden sie einerseits durch Anwendung von g nur permutiert was $PS = g(PS)$ nach

sich zieht, wenn man $g(\wp_1) \mapsto \wp_i$ hat ergibt sich aus der eindeutigen Primidealzerlegung durch Vergleich der rechten und linken Seite der Gleichung

$$\wp_1^{e_1} \dots \wp_s^{e_s} = PS = g(PS) = g(\wp_1)^{e_1} \dots g(\wp_s)^{e_s}$$

dass $e_i = e_1$ wie gefordert.
Um zu zeigen, dass die $\wp_i$ in (5.14) konjugiert sind, bemerken wir noch einmal, dass $g \in Gal(L/K)$ als Permutation auf den $\wp_i$ wirkt. Man erkennt also, dass nur die Transitivität von $Gal(L/K)$ zu zeigen ist. Die Endlichkeit der Klassenzahl $h(S)$ von S und der kleine Fermat für Gruppen implizieren die Existenz eines $a \in S$ mit

$$\wp_1^{h(S)} = aS, \qquad a \in S \tag{5.15}$$

da das neutrale Element der Idealklassengruppe die Hauptideale sind. Offenbar $a \in \wp_1$. Seien $a_1, \dots a_n$ die Konjugierten von $a = a_1$ in K. Nach Definiton $N_{L/K}(a) = N_{L/K}(a_1) = a_1 a_2 \dots a_n \in \wp_1$, weil $a \in \wp_1$. Deswegen ist das Hauptideal $N_{L/K}(a)S \subset PS$. Insbesondere ist $a_1 a_2 \dots a_n S$ teilbar durch $\wp_i$, und weil P Primideal ist muss ein $a_j \in \wp_i$ sein, oBdA a_i. Sei $g \in Gal(L/K)$ das Element das a nach a_i schickt. (5.15) liefert

$$g(\wp_1)^{h(S)} = g(a)S = a_i S$$

wegen $a_i \in \wp_i$ aber $g(\wp_1)^{h(S)} \subset \wp_i$. Weil aber $\wp_i, g(\wp_1)$ Primideale sind und daher nach Voraussetzung maximal, folgt zunächst $g(\wp_1)^{h(S)} = \wp_i$ und aber auch $g(\wp_1) = \wp_i$, da wegen der Maximalität von $\wp_i$ die Potenzen nicht echt kleiner werden dürfen. Damit wirkt $Gal(L/K)$ transitiv. □

Definition 5.15 (Normabbildung)**.** Sei L/K Körpererweiterung, $\wp \triangleleft S$ Primideal von S und P das Primideal von R das unter $\wp$ liegt. Dann bezeichnet

$$\boldsymbol{N}_{L/K}(\wp) = P^{f_{L/K}(\wp)} \tag{5.16}$$

die *Norm* von $\wp$ und die Vorschrift

$$(I = \prod \wp^{a_\wp} \quad \Longrightarrow \quad \boldsymbol{N}_{L/K}(I) = \prod P^{a_\wp f_{L/K}(\wp)})$$

setzt die Normabbildung auf die Idealgruppe $G(I)$ fort.

Aus der Definition der Großen $e_{L/K}, f_{L/K}$ ergibt sich unmittelbar

Proposition 5.6. Sei wieder K Zerfällungskörper vom Integritätsring R und L Zerfällungskörper von S, sowie $K \subset L \subset M$ Körpererweiterungsturm, und T der ganze Abschluss von S in M. Sei weiter $P \subset \wp$, P Primideal in S und $\wp$ Primideal in T, dann gilt

$$e_{M/K}(\wp) = e_{M/L}(\wp) e_{L/K}(P), \qquad f_{M/K}(\wp) = f_{M/L}(\wp) f_{L/K}(P)$$

Korollar 5.1. Sind M/L und L/K beide unverzweigt, so auch M/K.

5.4 Weitere Vorbereitungen zu Kreisteilungskörpern

Definition 5.16. Sei R Dedekindring mit Quotientenkörper K und L/K separable, endliche Körpererweiterung, die (EN) erfüllt und die Endlichkeit der Klassenzahl gewährleistet.
Sei weiter $A \subset L$ von Null verschiedener R-Modul. Der R-Modul

$$A^* := \{x \in L : \quad Sp_{L/K}(xA) \subset R\} \tag{5.17}$$

heißt *Kodifferent von A in K.*

Die Notation obiger Definition werde nun fortgeführt.

Proposition 5.7. Sei A ein gebrochenes Ideal in L uns sei S der ganze Abschluss von R in K.

1. Dann ist der Kodifferent A^* ein gebrochenes Ideal in L
2. $$AA^* = S^*$$
3. Ist darüber hinaus $A \triangleleft S$ echtes Ideal von S, so auch $(A^*)^{-1}$.

Beweis:

1. Seien $x_1, x_2 \in A^*$, $b_1, b_2 \in S$. Die Mengeninklusion

   $$Sp_{L/K}((b_1x_1 + b_2x_2)A) \subset Sp_{L/K}(x_1A) + Sp_{L/K}(x_2A) \subset R$$

   zeigt leicht, dass A^* ein S-Modul ist. Nach der Voraussetzung an die Ringe gibt es ein $a \in S$ mit $aA \subset S$ andererseits ist jedes solche a nach Definition (5.17) in A^*. Diese Überlegungen zusammen ergeben dass $A^* \neq 0$. Bleibt also zu zeigen: Es exisitert ein $q \in S$ mit $qA^* \subset S$, in logischen Quantoren

   $$\exists q \in S : \quad qA^* \subset S \tag{5.18}$$

   Wähle dazu eine Basis $w_1, \ldots w_n \subset S$ von L über K- nach Satz 1.3 ist dies mölgich- und $0 \neq b \in A \cap R$. Setze

   $$q := b \cdot \det[Sp_{L/K}(w_iw_j)]$$

   Weil L/K separabel ist gilt $q \neq 0$. Außerdem gilt für alle $1 \leq j \leq n$, dass
   $bw_j \in S$. Nach der Wahl der w_i hat jedes $x \in L$ und damit jedes $a \in A^*$ eine Darstellung $x = c_1w_1 + \ldots + c_nw_n, \quad c_i \in K$. Die letzten beiden Bemerungen zusammen ergeben also $Sp_{L/K}(bxw_j) \in R$, da Norm (1.1) und Spur (1.2) nach Kapitel 1 im Grundkörper enthalten sind. Es gilt aber wegen $b \in A$ auch

   $$Sp_{L/K}(bxw_j) = b\sum_{k=1}^{n} c_k Sp_{L/K}(w_jw_k)$$

   und nach der Cramerschen Regel gilt $bc_k \det[Sp_{L/K}(w_iw_j)] \in R$ für alle solchen Elemente. Daraus folgt aber $qx \in S$. Wegen der Beliebigkeit von $x \in A^*$ also $qA^* \subset S$ und damit erfüllt das konstruierte q Bedingung (5.18).

2. Die weitere Behauptung $AA^* = S^*$ sieht man vermöge

$$a \in A^* \Leftrightarrow Sp_{L/K}(aA) \subset R \Leftrightarrow Sp_{L/K}(aAS) \subset R \Leftrightarrow aA \subset S^* \Leftrightarrow a \in A^{-1}S^*$$

3. Der letzte Punkt folgt aus

$$(A \subset S \Rightarrow S \subset A^*) \quad \Rightarrow \quad (A^*)^{-1} = S(A^*)^{-1} \subset A^*(A^*)^{-1} = S$$

□

Definition 5.17. Zu einem gebrochenen Ideal A von L sei das nach vorangehender Proposition gebrochene Ideal $(A^*)^{-1}$ als *Different von A über K* bezeichnet, in Zeichen $D_{L/K}(A)$. Im Falle $A = S$ heißt es der *Different der Erweiterung* L/K, in Zeichen $D_{L/K}$.

Die natürliche Selbstabbildung der Idealgruppe $G(M)$ via $A \mapsto D_{L/K}(A)$ ist im allgemeinen kein Homomorphismus, aber es gilt

Proposition 5.8. Ist $K \subset L \subset M$ ein Körpererweiterungsturm, dann gilt

$$D_{M/K} = D_{M/L} \cdot D_{L/K} \tag{5.19}$$

Beweis: Es ergibt sich die Äquivalenzkette

$$a \in D_{M/L}^{-1} \Leftrightarrow Sp_{M/L}(a) \in S \Leftrightarrow D_{L/K}^{-1} Sp_{M/L}(a) \subset D_{L/K}^{-1} \Leftrightarrow Sp_{L/K}(D_{L/K}^{-1} Sp_{M/L}(a)) \subset R$$

$$\Leftrightarrow Sp_{M/K}(aD_{L/K}^{-1}) \subset R \Leftrightarrow aD_{L/K}^{-1} \subset D_{M/K}^{-1} \Leftrightarrow a \in D_{L/K}D_{M/K}^{-1}$$

Wegen der Beliebigkeit von a also $D_{M/L}^{-1} = D_{L/K}D_{M/K}^{-1}$ und damit die Aussage des Lemmas (5.19). □

Wir erweitern nun den Begriff der Diskriminante für relative Erweiterungen L/K, L und K algebraische Zahlkörper. Diese ist nun keine Zahl, sondern ein Ideal. Dies ist notwendig, da bei solchen Erweiterungen keine Ganzheitsbasis von L über K mehr existieren muss, unsere einstige Definition also keinen Sinn mehr macht. Selbst wenn es Ganzheitsbasen gibt, ist nach der alten Definition die Eindeutigkeit nicht gegeben. Wir definieren also

Definition 5.18 (Diskriminante)**.** Die *Diskriminante* $d_{L/K}$ einer Erweiterung L/K zweier Zahlkörper K, L ist das Ideal definiert durch

$$\boldsymbol{N}_{L/K}(D_{L/K}) \tag{5.20}$$

mit der Normabbildung (5.16).

Bemerkung: Im Falle $L = \mathbb{Q}$ stimmt $d_{L/\mathbb{Q}}$ mit dem von $d(L)$ erzeugten Hauptideal überein, wobei $d(L)$ die klassische Diskriminante des Körpers L aus Korollar 3.2 ist.

Korollar 5.2. Für einen Körperturm $K \subset L \subset M$ gilt

$$d(M/K) = d(L/K)^{[M:L]} \boldsymbol{N}_{L/K}(d(M/L))$$

Korollar 5.3. Sind K, L Zahlkörper mit $\mathbb{Q} \subset K \subset L$, dann gilt $d(K)^{[L:K]} | d(L)$.

Nun betrachten wir wieder den allgemeinen Fall mit zugrunde liegendem Dedekindring R, weil wir später davon Gebrauch machen müssen. Betrachte zu einem *Erzeuger* $a \in S$ *von* L/K sein Minimalpolynom

$$F(t) = t^n + a_{n-1}t^{n-1} + \ldots + a_0, \qquad a_i \in R$$

und definiere

$$\delta_{L/K}(a) := F'(a)$$

Setze δ durch $\delta(b) = 0$ für Nicht-Erzeuger b von L/K fort.

Definition 5.19.

Für einen Unterring $R \subset A \subset S$ von S sei der größte gemeinsame Teiler aller in A enthaltenen Ideale $I \lhd S$ mit $\boldsymbol{f_A}$ bezeichnet. Wir nennen ihn *Führer* von A.

Wir zielen nun auf den Beweis folgenden Satzes ab:

Satz 5.4. Der Different $D_{L/K} \lhd S$ wird von $\{\delta(a) : \quad a \in S\}$ erzeugt.

Proposition 5.9. Gilt $R \subset A \subset S$ und ist A ein Ring, dann ist

$$\boldsymbol{f_A} = \{x \in L : xA^* \subset S^*\} \quad \textit{und} \quad \boldsymbol{f_A} \subset A$$

Beweis: Sei

$$I := \{x \in L : xA^* \subset S^*\} \tag{5.21}$$

Für die eine Richtung bemerke, dass für $x \in I, y \in S$ nach Definition (5.17) von S^* die Inklusionskette

$$yxA^* \subset yS^* \subset S^*$$

gilt, demnach ist I ein S-Modul.
Außerdem zeigt die sofort aus (5.21) folgende Mengeninklusion

$$Sp_{L/K}(IA^*) \subset Sp_{L/K}(S^*) \subset R$$

unmittelbar, dass $A^* \subset I^*$ und damit $I \subset A \subset S$. Weil A Ring ist ist also insgesamt I Ideal in S und damit $\boldsymbol{f_A} | I$ nach Definition des Führers.
Sei umgekehrt $J \lhd S$ und $J \subset A$, $y \in A^*$. Zweiteres bedeutet $Sp_{L/K}(yA) \subset R$ und daher $Sp_{L/K}(JyS) \subset Sp_{L/K}(yA) \subset R$ und weiter $yJ \subset S^*$ nach (5.17). Das bedeutet wieder nach Definition des Kodifferenten (5.17) und der von I in (5.21) aber $J \subset I$. Die Beliebigkeit von J zeigt die fehlende Inklusion. □

Wir studieren nun in Hinblick auf den Beweis von Satz 5.4 Ringe der Form $R[a]$, $a \in S$, wobei a die Erweiterung L/K erzeugt. Diese haben mit $[L : K] = n$ die Form

$$R[a] = \oplus_{i=0}^{n-1} a^j R$$

wie leicht zu sehen ist.

Proposition 5.10. Sei $A = R[a]$ wie oben und $f(t)$ normiertes Minimalpolynom von a (beachte $a \in S$), dann ist ein Erzeuger des Kodifferenten A^* als R-Modul explizit gegeben als

$$A^* = B :=< \{\frac{a^j}{f'(a)} : \quad j = 0, 1, \dots n-1\} > \tag{5.22}$$

wobei die gespitzten Klammern $< . >$ das Erzeugnis andeuten.

Beweis: Die Lagrange-Polynominterpolationsformel für ein Polynom vom Grad n mit $(n+1)$ Stützstellen

$$P(x) = \sum_{j=1}^{n} l_i(x) \cdot f(x_i), \qquad l_i(x) = \prod_{j=0, j\neq i}^{n} \frac{x - x_j}{x_i - x_j}$$

angewandt auf unsere Situation für die Polynome $\{x, x^2, \dots x^{n-1}, x^n - f(x)\}$ liefert

$$\sum_{j=1}^{n} \frac{a_j^k}{f'(a_j)} \cdot \frac{f(x)}{x - a_j} = \begin{cases} x^{k+1} & \text{für } k = 0, 1 \dots n-2 \\ x^n - f(x) & \text{für } k = n-1 \end{cases} \tag{5.23}$$

wobei $a_1 = a, a_2, \dots a_n$ die Konjugierten von a sind, weil der Nennerterm der l_i in der Lagrange-Formel genau der formalen Ableitung entspricht. Setzt man $x = 0$ in (5.23) bekommt man

$$Sp_{L/K}(a^j/f'(a)) \in R \tag{5.24}$$

was per Definition $a^j/f'(a) \in A^*$ bedeutet, also $B \subset A^*$.
Für die Umkehrung sei $b \in A'$ beliebig mit Konjugierten $b_1 = b, b_2 \dots b_n$ und sei $f(t)$ gegeben als $f(t) = c_0 + c_1 t + \dots + c_n t^n$. Man erkennt, dass die Koeffizienten von

$$P(x) := \sum_{i=1}^{n} \frac{b_i f(x)}{x - a_i} = \sum_{j=1}^{n} c_j \sum_{k=0}^{j-1} x^k Sp_{L/K}(ba^{j-k-1})$$

wegen $Sp_{L/K}(bA) \subset R$ in R liegen. Wegen $bf'(a) = P(a) \in R[a]$ ist $b \in B$ was die umgekehrte Inklusion $A^* \subset B$ bestätigt. □

Korollar 5.4. $f'(a)S \subset R[a]$

Beweis: Wegen $S \subset A^*$ und der Darstellung (5.22) von A^* von oben gelangt man zu $f'(a)S \subset f'(a)A^* \subset R[a]$. □

Proposition 5.11. Sei $A = R[a]$, dann gilt

1. $$\boldsymbol{f_A} = \delta_{L/K}(a) D_{L/K}^{-1}$$

2. $$\boldsymbol{f_A} = \{x \in A : xS \subset A\} =: \widehat{A}$$

Beweis:

1. $\delta_{L/K}(a)D_{L/K}^{-1}$ ist nur eine andere Schreibweise für $f'(a)S^*$ und wegen $S^* \subset A^*$ gilt nach letzter Proposition 5.10 $f'(a)S^* \subset R[a]$. Aber nach Definiton ist $a \in S$-also ganz- und damit sind auch alle Elemente von $R[a]$ in S, weil die ganzen Elemente eine Ordnung bilden (vgl Kapitel 1 Satz 1.3). Insgesamt also

$$\delta_{L/K}(a)D_{L/K}^{-1} \subset S$$

und nach Definition des Führers $\boldsymbol{f_A}$ teilt dieser also $\delta_{L/K}(a)D_{L/K}^{-1}$. Wegen (5.24) ist
$Sp_{L/K}(A/f'(a)) \subset R$, daraus erkennt man $A/f'(a) \subset S^*$ und wegen $\boldsymbol{f_A} \subset A$ weiter

$$\boldsymbol{f_A}/f'(a) \subset S^* \tag{5.25}$$

Durch Multiplikation von (5.25) mit $f'(a)$ haben wir zusammenfassend

$$\boldsymbol{f_A} \subset f'(a)S^* = \delta_{L/K}(a)D_{L/K}^{-1}$$

erreicht. Insgesamt haben wir damit Punkt 1 nachgewiesen.

2. Für $x \in \boldsymbol{f_A}$ zeigt einerseits $xS \subset \boldsymbol{f_A}S = \boldsymbol{f_A} \subset A$, dass $\boldsymbol{f_A} \subset \widehat{A}$. Die umgekehrte Inklusion ist aber gewissenmaßen trivial, hinsichtlich der Tatsache, dass $\widehat{A} \subset A$ ein S-Ideal ist und $\boldsymbol{f_A}$ deren ggT.

□

Lemma 5.4. 1. Sei wieder $a \in S$ Erzeuger von L/K und sei $A = R[a]$. Ist $\wp \triangleleft S$ mit $\wp \nmid \boldsymbol{f_A}$, so induziert die Einbettung von A in S Isomorphismen

$$S/\wp^m \longmapsto A/(A \cap \wp^m), \quad m \geq 1$$

mit anderen Worten jede Restklasse $(\mathrm{mod}\ \wp^m)$ von S kann mit einem Element von A identifiziert werden.

2. Sei $\wp \triangleleft S$ Primideal von S und P das Primideal das Primideal von R das unter $\wp$ liegt (vgl Proposition 5.5). Schreibt man $PS = \wp^e I$ mit I relativ prim zu $\wp$, und ist $a \in I \setminus \wp$ Erzeuger von L/K und $A = R[a]$, und gilt $S/\wp^m \cong A/(A \cap \wp^m), m \geq 1$ wobei der Isomorphismus einfach durch die Einbettung von A in S gegeben ist, dann gilt

$$\wp \nmid \boldsymbol{f_A}.$$

Beweis:

1. Wähle $b \in \boldsymbol{f_A} \setminus \wp$ beliebig und $c \in S$. Proposition 5.11 Punkt 2 zeigt

$$\exists W[t] \in R[t]: \quad c = \frac{W(a)}{b}$$

Aber wählt man k mit $b^k \equiv 1\ \mathrm{mod}(\wp^m)$- aufgrund der Endlichkeit der Faktorgruppe $R/\wp^m$ und $a^{|G|} = 1$ für Gruppen ist so eine Wahl zulässig- und beachtet man

$$b = V[a], \qquad V[t] \in R[t]$$

weil $\boldsymbol{f_A} \subset A$ nach Proposition 5.9, erhält man

$$c = W(a)b^{k-1} \equiv W(a)V(a)^{k-1} \pmod{\wp^m} \tag{5.26}$$

Weil $W(a)V(a)^{k-1} \in R[a] = A$ bedeutet (5.26) gerade, dass alle Restklassen eine Entsprechung zu einem Element von A haben.

2. Wir zeigen erst: Jedes $x \in S$ hat eine Darstellung $x = P(a)/D$ mit $P(t) \in R[t]$ und $0 \neq D \in R$ unabhängig von x. Wegen $A \subset S$ gilt $S \subset S^* \subset A^*$ und wegen Proposition 5.10 gilt $S \subset R[a]/f'(a)$ (mit f Minimalpolynom von a über R). Wähle $g \in K[X]$ mit $1/f'(a) = g(a)$, so ergibt sich in der Tat eine Darstellung

$$\frac{1}{f'(a)} = \frac{V(a)}{D}, \qquad V \in R[X], D \in R$$

Sei nun m maximal mit $P^m|D$, sodass es also ein $c \in DP^{-m} \setminus P \subset R$ gibt. Dann hat nach Annahme x eine Darstellung $x = b + x_1$, $b \in A, x_1 \in \wp^{em}$. Es ergibt sich $x_1 a^m \in \wp^{em} I^m = \wp^m S \subset P^m A/D$. Man hat also $x_1 a^m \in c^{-1}A$, also $x_1 a^m = d/c$ mit $d \in A$ und weiter

$$x_1 = d/ca^m = V(a)/ca^m, \qquad V \in R[X]$$

Daher $ca^m x \in A$ was $ca^m \in \boldsymbol{f_A}$ impliziert. Weil $\wp$ Primideal ist und weder a noch c darin enthalten sind gilt $ca^m \notin \wp$, also $\boldsymbol{f_A} \nsubseteq \wp$ im Widerspruch zu $\wp|\boldsymbol{f_A}$. □

Lemma 5.5. Sei $\wp \lhd S$ Primideal von S und $I \lhd S$ Ideal von S mit $\wp \nmid I$. Dann

$$\exists a \in I: \quad \forall x \in S, \forall n \geq 0 \quad \exists y_n \in R[a]: \quad x \equiv y_n \pmod{\wp^n}$$

Beweis: Sei P das Primideal in R das unter $\wp$ liegt und $f = f_{L/K}(\wp)$ der Trägheitsgrad von $\wp$. Definiere zur kürzeren Notation $k := S/\wp$ und $k_0 := R/P$ und sei $\overline{a} \in k$ die Klasse von a unter der natürlichen Einbettung. Da k endlicher Körper ist und damit separabel- wie man durch das Nichtverschwinden der formalen Ableitung ersehen kann- kann man sich Erweiterung k/k_0 nach Satz 1.5 (Satz vom primitiven Element) durch ein einziges Element $\overline{y}$ erzeugen lassen. Sei $t^f + \overline{b_{f-1}}t^{f-1} + \ldots + \overline{b_0} \in k_0[t]$ Minimalpolnom von $\overline{y}$ in und wähle $b_i \in R$ deren Reduktion genau die $\overline{b_i}$ ergeben und definiere

$$F(t) = t^f + b_{f-1}t^{f-1} + \ldots + b_0$$

Wähle ebenso $y \in S$ mit $y \pmod{\wp} = \overline{y}$ und sodass y zusätzlich die Eigenschaft hat, dass $F(y) \notin \wp^2$. So eine Wahl ist möglich denn für ein y das lediglich der zweiten Bedingung widerspricht erfüllt $y + c$, $c \in \wp \setminus \wp^2$ offenbar beide Bedingungen. Bemühe weiters den chinesischen Restsatz um $a \in S$ zu finden mit

$$a \equiv 0 \pmod{I}, \qquad a \equiv y \pmod{\wp^2}$$

wobei die Voraussetzung der Teilerfremdheit hier eingeht. Wir zeigen: Jedes so definierte a genügt den Anforderungen.
Sei $x \in S$. Es gilt $\overline{x} = V(\overline{a})$ mit $V(t) \in k_0[t]$ und bezeichne mit $W_1(t)$ ein Polynom dessen Reduktion $\pmod P$ mit $V(t)$ übereinstimmt. Es gilt $x \equiv W_1(a) \pmod{\wp}$, was den Fall $n = 1$ des Lemmas beweist. Nun folgt eine Induktion. Sei für beliebiges $x \in S$ also $x \equiv W_n \pmod{\wp^n}$. Nach Definition von F muss das Hauptideal $F(a) \lhd S$ von $\wp$ geteilt werden, also $F(a)S = \wp J$. Weiters muss nach unserer Wahl von a gelten, dass $\wp \nmid J$. Damit existiert also ein $u \in J \setminus \wp$ und zugehöriges u' mit $uu' \equiv 1 \pmod{\wp}$. Sei weiter $Q(t) \in R[t]$ mit

$$u' \equiv Q(a) \pmod{\wp} \tag{5.27}$$

Dann ist

$$c := \frac{(x - W_n(a))u^n}{F^n(a)} \in S \tag{5.28}$$

also kann man $c \equiv T(a) \pmod{\wp}$ schreiben mit $T(t) \in R[t]$ und indem man (5.28) nach x auflöst und (5.27) berücksichtigt

$$x \equiv W_n(a) + T(a)F^n(a)Q^n(a) \pmod{\wp^{n+1}} \tag{5.29}$$

Damit ist der Induktionsschritt fertig, wie gefordert hat man zu jedem $x \in S$ ein passendes $y_{n+1} \in R[a]$ gefunden denn offenbar ist die rechte Seite von (5.29) in $R[a]$. □

Nun sind wir in der Lage den Beweis von Satz 5.4 aus den bisherigen Resultaten herzuleiten.

Beweis: Die vorangehenden beiden Lemmata 5.4,5.5 zeigen, dass es möglich ist zu festem Primideal $\wp \lhd S$ ein $a \in L$ das L/K erzeugt zu finden, das

$$\wp \nmid \boldsymbol{f_A}$$

erfüllt. Hinsichtlich Punkt 1 von Proposition 5.11

$$\delta_{L/K}(a) \subset D_{L/K}$$

und

$$\boldsymbol{f_A} D_{L/K} = \delta_{L/K}(a), \qquad A = R[a]$$

müssen alle Primideale in der Zerlegung von $D_{L/K}$ schon in gleicher Potenz im jeweils entsprechenden $\delta_{L/K}(a)$ enthalten sein, also erzeugen die $\delta_{L/K}(a)$ das Ideal $D_{L/K}$. □

Definition 5.20. Eine Erweiterung L/K heißt *Zusammensetzung* der Erweiterungen K_1/K und K_2/K, wenn L der minimale Körper ist der K_1 und K_2 enthält. Dabei werden K_1, K_2 als Körper in einem festen algebraischen Abschluss $\overline{K}$ von K betrachtet (der ja bis auf Isomorphie eindeutig ist).

Bemerkung: Man sieht leicht, dass L durch $K(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots \beta_m)$ entsteht, wobei die α_i Basis von K_1/K und die β_j Basis von K_2/K bilden.

Lemma 5.6. Sei K Quotientenkörper von R und L/K Zusammensetzung der Erweiterungen $K_1/K, K_2/K$ dann stimmen überein:

1. A:= Die Menge der Primideale P von R die $d(L/K)$ teilen.

2. B:= Die Menge der Primideale P die $d(K_1/K)d(K_2/K)$ teilen.

Beweis: Korollar 5.2 zeigt dass $B \subset A$. Sei $P \in B$, sodass $P \nmid d(K_1/K)$. Wir zeigen, dass P das Ideal $d(K_2/K)$ teilt und haben damit die andere Inklusion. Die Definition der Diskriminante sichert die Existenz eines Ideals $\wp$ das über P liegt und den Different $d_{L/K}$ teilt. Dieses Ideal kann nicht $D_{K_1/K}S$ teilen, denn dann wäre wegen

$$P^f = \boldsymbol{N}_{L/K}(\wp)|\boldsymbol{N}_{L/K}(D_{K_1/K}S) = \boldsymbol{N}_{K_1/K}(\boldsymbol{N}_{L/K_1}(D_{K_1/K}S))$$

$$= \boldsymbol{N}_{K_1/K}(D_{K_1/K}^{[L:K]}) = d(K_1/K)^{[L:K_1]}$$

$P|d(K_1/K)$ und damit wegen $D_{L/K} = D_{L/K_1}D_{K_1/K}$ entgegen unserer Annahme $\wp|D_{L/K}$. Sei nun $a \in O_{K_2}$ ganz über R das K_2/K erzeugt. Seien $G(t)$, $F(t)$ die Minimalpolynome von a über K_1 respective K. Wir haben $L = K_1(a)$ und $F(t) = G(t)H(t)$ mit einem $H(t) \in K_1[t]$. Aus $G(a) = 0$ leitet man $F'(a) = G'(a)H(a)$ ab. Das bedeutet aber, dass F' im von G' in S erzeugten Hauptideal liegt. Nach Satz 5.4 gilt $G'(a) \in D_{L/K} \subset \wp$, damit auch $F' \in \wp$. Wieder Satz 5.4 gibt uns $D_{K_2/K} \subset \wp$, also $P|d(K_2/K)$.

□

Korollar 5.5. Ist M/K minimale normale Erweiterung von K die L enthält, so haben $d(L/K)$ und $d(M/K)$ die selben Primidealteiler. Insbesondere ist L/K genau dann unverzweigt wenn M/K es ist.

Satz 5.5. Seien K_1/K, K_2/K Zahlkörper vom Grad n_1 respective n_2 mit relativ primen Diskriminanten $d(K_1), d(K_2)$ und bezeichne mit L ihre Zusammensetzung, sodass also $L/Q = K_1K_2/\mathbb{Q}$. Dann gilt

$$[L : \mathbb{Q}] = n_1n_2$$

$$d(L) = d(K_1)^{n_1}d(K_2)^{n_2}$$

und wenn $w_1, \dots w_{n_1}$ Ganzheitsbasis von K_1 und $v_1, \dots v_{n_2}$ Ganzheitsbasis von K_2 ist, dann ist $\{v_iw_j : \quad 1 \le i \le n_1, \quad 1 \le j \le n_2\}$ Ganzheitsbasis von L.

Beweis: Sei K minimale normale Erweiterung von $\mathbb{Q}$ mit $K_1 \subset K$. Nach dem letzten Korollar und der Voraussetzung des Satzes haben wir

$$(d(K), d(K_2)) = 1 \tag{5.30}$$

Sei nach Satz 1.5 (Satz vom primitiven Element) oBdA $K = \mathbb{Q}(a)$ und $f(t)$ sei das Minimalpolynom von a. Definieren wir $g(t)$ als Minimalpolynom von a über K_2 dann also $g(t)|f(t)$, und um die Gleichheit zu zeigen müssen wir zeigen, dass die Koeffizienten von $g(t)$ sogar rational sind. Diese Koeffiziente liegen als rationale Funktionen in manchen Konjuigerten von a über $\mathbb{Q}$ sicher in K (hier wird K normal benutzt). Wir schließen weiter, dass der Körper k der von genannten Koeffizienten erzeugt wird in $K \cap K_2$ enthalten ist. Wegen Proposition 3.5 muss $d(k)$ beide $d(K)$ und $d(K_2)$ teilen. Wegen (5.30) also $|d(k)| = 1$ und wegen Lemma 5.2 $k = \mathbb{Q}$. Also in der Tat $f(t) = g(t)$. Daher $[L : K_2] = [K_1 : K] = n_1$ und mit dem Gradsatz $[L : K] = n_1n_2$.

Die Diskriminante von $E := \{w_i v_j\}$ ist $d(K_1)^{n_1} d(K_2)^{n_2}$, also muss wegen Proposition 3.4 $d(L)$ diese Zahl teilen, denn E ist ja sicher ein Untermodul von O_L. Korollar 5.3 zeigt, dass auch $d(L)|d(K_i^{n_i})$ gilt für $i = 1, 2$, also auch das Produkt weil die Zahlen relativ prim vorausgesetzt sind. □

Jetzt können wir wesentliche algebraischen Eigenschaften von Kreisteilungskörpern fassen.

Satz 5.6 (Struktur von Kreisteilungskörpern)**.** Seien m, n positive ganze Zahlen, $K_m := \mathbb{Q}(\zeta_m)$ der Kreisteilungskörper, der durch Adjunktion einer primitven m-ten Einheitswurzel ζ_m entsteht, φ die eulersche Phi-Funkiton (also die Funktion die die Zahl der primen Restklassen modulo m zählt) sowie $(m, n) := \mathrm{ggT}(m, n)$ und $[m, n] := \mathrm{kgV}(m, n)$. Weiters bezeichne wieder $G(m)$ die Gruppe der primen Restklassen modulo m mit der Multiplikation. Dann gilt

1. $K_m K_n = K_{[m,n]}$
2. Es gilt $[K_m : \mathbb{Q}] = \varphi(m)$ sowie

$$d(K_m) = \prod_{p^a | m} d(K_{p^a})^{\varphi(mp^{-a})}$$

und $\{1, \zeta_m, \dots \zeta_m^{\varphi(m)-1}\}$ bildet eine Ganzheitsbasis. Außerdem ist $K_m/\mathbb{Q}$ normale Erweiterung mit Galoisgruppe isomorph zu $G(m)$ vermöge

$$\Theta : \qquad G(m) \longmapsto Gal(K_m/\mathbb{Q})$$

$$r \mapsto g_r, \qquad g_r(\zeta_m) := \zeta_m^r$$

Das Minimalpolynom von ζ_m über $\mathbb{Q}$ ist gegeben durch

$$F_m(x) = \prod_{1 \le j < m, (j,m)=1} (x - \zeta_m^j) = \frac{(x^m - 1)}{(x^m - 1, \prod_{j<m}(x^j - 1))}$$

3. Falls m inkongruent 2 (mod 4), so gilt $K_m \subset K_n \Leftrightarrow m|n$. Also gilt für m, n beide inkongruent zu 2 (mod 4), dass $K_m \neq K_n$.
4. Falls m inkongruent 2 (mod 4) und $m|n$, dann ist die Untergruppe von $G(n)$ die K_m über die Galoistherie entspricht

$$\{r \in G(n) : \quad r \equiv 1 \pmod m\}$$

5. $K_m \cap K_n = K_{(m,n)}$

Bemerkung: Die Forderung an m in den Punkten 3,4 ist keine echte Einschränkung wegen $K_m = K_{2m}$ für ungerades m, weil offenbar mit $-\zeta_m^{\frac{m+1}{2}}$ die primitive $2m$-te Einheitswurzel gegeben ist, also $\zeta_{2m} \in K_m$ und damit $K(\zeta_{2m}) \subset K(\zeta_m)$. Die andere Inklusion ist trivial. Beweis:

1. Ist $[m,n]=s$, dann liefert die einfache Observation
$$\zeta_m = \zeta_s^{\frac{s}{m}}, \quad \zeta_n = \zeta_s^{\frac{s}{n}}$$
dass $\zeta_m, \zeta_n \in K(s)$ (beachte $\frac{s}{m}, \frac{s}{n} \in \mathbb{Z}$) und daher $K_mK_n \subset K_s$. Für die andere Inklusion bestimme x,y als Lösungspaar der Gleichung $mx+ny=(m,n)=\frac{mn}{s}$ wie es mit dem Euklidalgorithmus stets möglich ist. Wegen $\zeta_m^y\zeta_n^x=\zeta_s$ ist $\zeta_s \in K_mK_n$ damit auch $K(\zeta_s) \in K_mK_n$.
2. Ist $m=\prod p^{a_p}$ die Primfaktorzerlegung von m, dann ist nach dem vorigen Punkt K_m die Zusammensetzung der Körper $K_{p^{a(p)}}$ und nach Satz 5.2 sind deren Diskriminanten paarweise teilerfremd. Nach dem letzten Satz 5.5 induktiv angewandt ergibt die Aussage über die Form der Diskriminante und $[K_m:\mathbb{Q}]=\varphi(m)$. Wegen Proposition 3.5 und Lemma 5.2 folgt daraus $K_{p^{a(p)}} \cap K_{\frac{m}{p^{a(p)}}} = \mathbb{Q}$ da es sonst einen nichttrivialen gemeinsamen Teiler gäbe und weiter wegen Satz 5.2 ist $K_m/\mathbb{Q}$ normal mit $Gal(K_m/\mathbb{Q}) \cong G(m)$ gelten. Die Formel für F_m erhält man, indem man feststellt dass für zu m teilerfremde j ζ_m^j zu ζ_m konjugiert sind, weil sie $(\zeta_m^j)^t=\zeta_m$ für ein t erfüllen. Die Aussage über die Galoisgruppen folgt sofort.
3. Für $m|n$ gilt klarerweise $K_m \subset K_n$. Ist d die Ordnung des aus Einheitswurzeln bestehenden Torsionsanteils aus dem dirichletschen Einheitensatz, so liefert die umgekehrte Annahme $K_m \subset K_n$ wegen $\zeta_n=\zeta_d^a$ für ein $a<d$ dass $n|d$ und also $K_n=K_d$. Wegen Punkt 2 also $\varphi(n)=\varphi(d)$. Wegen der Formel für die Phi-Funktion
$$\varphi(\prod p_i^{a(i)}) = \prod p_i^{a(i)-1}(p_i-1)$$
und $n|d$ liefert das die Fälle $d=n$ oder $d=2n$ mit n ungerade. Im ersten Fall ist ζ_m Potenz von $\zeta_d=\zeta_n$- also $m|n$- im zweiten Fall argumentiert man ebenso um $m|2n$ zu bekommen. Ungerades m führt nach obigen Überlegungen zwangsläufig zu $m|n$ und gerades m ergibt $m \equiv 2 \pmod 4$, entgegen unserer Voraussetzung.
4. Setze $q:=\frac{m}{n}$ und bezeichne H die in der Galoiskorrespondenz zu K_m gehörige Untergruppe von $G(n)$- also die Menge der Automorphismen die K_m fixiert. Diese hat offenbar die Charakterisierung, dass
$$r \in H \iff g_r(\zeta_m)=\zeta_m$$
Wegen $\zeta_m=\zeta_n^q$ ist $g_r(\zeta_m)=g_r(\zeta_n)^q=\zeta_n^{rq}$, was aber
$$r \in H \iff rq \equiv q \pmod n$$
bedeutet und also $r \equiv 1 \pmod n$ weil r in einer primen Restklasse mod n ist.
5. Setze $d:=(m,n)$, $D:=[m,n]$. Nach Punkt 1 gilt sind K_d, K_m, K_n in K_D enthalten. Bezeichne für $r|D$ mit $H_r \triangleleft G(D)$ die zu K_r gehörige Automorphismengruppe so wissen wir aus Punkt 4, dass
$$K_{mn} = fix(H_mH_n) = fix(\{s \pmod D : s=r_1r_2, r_1 \equiv 1 \pmod m, r_2 \equiv 1 \pmod n\}).$$
Nach dem Hauptsatz der Galoistheorie ist die Annahme von Punkt 5 gleichbedeutend mit $H_mH_n=H_d$. Die Inklusion $H_mH_n \subset H_d$ ist unmittelbare Folge der Definition. Für die Umkehrung wähle $s \in H_d$ beliebig und bemerke dass die Systeme
$$x \equiv s \pmod m, \qquad x \equiv 1 \pmod n$$

$$y \equiv 1 \pmod{m}, \qquad y \equiv s \pmod{n}$$

lösbar sind für x bzw y. Betrachtet man nun die Reduktionen modulo D, so stellt man fest, dass

$$x \pmod{D} \in H_n, \qquad y \pmod{D} \in H_m, \qquad xy \equiv s \pmod{D}$$

daher $s \in H_m H_n$.

□

Für uns wird im weiteren vor allem $Gal(K_m/\mathbb{Q}) \cong G(m)$ von entscheidender Bedeutung sein. Der zweite Punkt obigen Satzes impliziert sofort, dass K_m stets abelsche Zahlkörper sind. Die Erkenntnisse über Kreisteilungskörper sind deswegen so unentbehrlich weil folgender tiefliegender Satz zutrifft, den wir ohne den mehrseitigen Beweis anführen. Ein Beweis, der ohne Klassenkörpertheorie auskommt, findet sich in [Na74].

Satz 5.7 (Kronecker-Weber)**.** Jede normale Erweiterung von $\mathbb{Q}$ mit abelscher Galoisgruppe ist in einem Kreisteilungskörper $\mathbb{Q}(\zeta_m)$ enthalten.

Also sind die Kreisteilungskörper quasi die Prototypen abelscher Zahlkörper.

5.5 Kreisteilungskörper und Primideale

Zuerst benötigen wir ein Analogon von Lemma 5.4 das wir ohne Beweis anstellen

Lemma 5.7. Sei $P \triangleleft R$ Primideal von R und $a \in S$ ein Element das L/K erzeugt, $A = R[a]$ und $\boldsymbol{f_A}$ Führer von A. Dann sind äquivalent:

1. $$PS \cap A = P[a]$$
2. Die Einbettung von A in S induziert einen Isomorphismus
$$\phi : S/PS \longmapsto A/(A \cap PS)$$
jede Klasse von $S \pmod{PS}$ enthält also ein Element von A.
3. Die Einbettung von A in S induziert für alle $m \geq 1$ einen Isomorphismus
$$\phi : S/P^m S \longmapsto A/(A \cap P^m S)$$
4. $$P^m S \cap A = P^m[a]$$
5. Das Primideal P teilt nicht $\boldsymbol{N}_{L/K}(\boldsymbol{f_A})$.

Lemma 5.8. Sei ζ_m primitive m-te Einheitswurzel und K ein beliebiger Zahlkörper. Sei P Primideal von O_K mit $m \notin O_K$ und Trägheitsindex eins über $\mathbb{Q}$, also $f_{K/\mathbb{Q}}(P) = 1$. Ist f die kleinste natürliche Zahl mit $N(P)^f \equiv 1 \pmod{m}$, dann gilt in $L := K(\zeta_m)$

$$PO_L = \wp_1 \wp_2 \dots \wp_g, \qquad g = [L : K]$$

mit paarweise verschiedenen $\wp_i$ von Trägheitsgrad f.

Beweis: Wegen Lemma 5.3 ist lediglich zu zeigen, dass der Grad k eines Primideals $\wp \triangleleft O_L$ das über P liegt f gleicht. Wir zeigen zunächst: Der Führer $\boldsymbol{f_A}$ des Ringes $O_K[\zeta_m]$ teilt das Ideal mO_L.
Sei $g(x)$ Minimalpolynom von ζ_m über K, dann gilt $f(x)g(x) = x^m - 1$ mit einem $g(x) \in O_K[x]$, denn natürlich gilt $f(x)|(x^m-1)$ und alle Koeffizienten von g sind augenscheinlich ganz. Das heißt aber

$$\delta_{L/K}(\zeta_m)g(\zeta_m) = m \cdot \zeta_m^{m-1}$$

und weil ζ_m Einheit ist $\delta_{L/K}(\zeta_m)O_L | mO_L$ und wegen Proposition 5.11 auch $\boldsymbol{f_A}|mO_L$. Nach Definition der Normabbildung also $\boldsymbol{N}_{L/K}(\boldsymbol{f_A})|m^{[L:K]}O_K$. Nun wenden wir obiges Lemma an. Das Resultat eben zeigt, dass der Punkt 5 erfüllt ist, also auch die übrigen und man kann zu jedem $x \in O_L$ ein $F(x) \in O_K[x]$ finden mit

$$x \equiv F(\zeta_m) \pmod{PO_L}$$

indem man a mit ζ_m identifiziert und unter Ausnutzung, dass die Ganzheitsringe O_K, O_L ganzabgeschlossen sind, also zu S korrespondieren aus obigem Lemma.
Die Defintion von f und Satz 3.6 erkennt man

$$x^{N(P)^f} \equiv F(\zeta_m)^{N(P)^f} \equiv F(\zeta_m^{N(P)^f}) \equiv F(\zeta_m) \pmod{PO_L}$$

und damit auch (mod$\wp$). Satz 3.6 zeigt aber, dass $N(\wp) = N(P)^k$ (Multiplikativität der Norm) die kleinste Zahl r ist sodass $x^r \equiv x \bmod(\wp)$ für alle $x \in O_L$ gültig ist, folglich $k \leq f$.
Wäre $N(P)^k \neq 1 \pmod m$ so wäre $\zeta^{N(P)^t}$ eine von ζ_m verschiedene m-te Einheitswurzel, also wäre die Differenz

$$\zeta_m^{N(P)^t} - \zeta_m \in PO_L \Rightarrow \zeta_m^{N(P)^t} - \zeta_m \in \wp$$

Mit $K_m = \mathbb{Q}(\zeta_m)$ heißt das aber, dass die Diskriminante $d_{K_m/\mathbb{Q}}(\zeta_m) \in \wp$. Diese ist aber ganz, also $\zeta_m^{N(P)^t} - \zeta_m \in \wp \cap Z$ das nach Voraussetzung an m von einer Primzahl $p \nmid m$ erzeugt wird, im Widerspruch zu unserer Charakterisierung von Kreisteilungskörpern in Satz 5.6. Es muss daher $N(P)^k \equiv 1 \pmod m$ gelten und daraus folgt die andere Ungleichung $f \leq t$. □

Satz 5.8. Sei $K = \mathbb{Q}(\zeta_m)$ der m-te Kreisteilungskörper. Sei weiters $p \nmid m$ Primzahl und f die kleinste Zahl mit $p^f \equiv 1 \pmod m$, dann gilt

$$pO_K = \wp_1\wp_2 \dots \wp_g, \qquad g = \frac{\varphi(m)}{f}$$

mit paarweise verschiedenen $\wp_i$ vom Trägheitsgrad f.
Ist andererseits $p|m$, also $p = m^a m_1$ mit $p \nmid m_1$ mit $a \geq 1$, und f kleinstmöglich mit $p^f \equiv 1 \pmod{m_1}$, dann

$$pO_K = (\wp_1\wp_2 \dots \wp_g)^e, \quad e = \varphi(p^a), \quad g = \frac{\varphi(m_1)}{f}$$

mit paarweise verschiedenen $\wp_i$ vom Trägheitsgrad f.

Beweis: Der erste Teil folgt unmittelbar aus dem vorangehenden Lemma hinsichtlich Satz 5.6 Punkt 2 für $[K_m : \mathbb{Q}] = \varphi(m)$. Im Fall $p|m$ gilt mit $K_1 := K(\zeta_{m_1})$ wieder $[K : \mathbb{Q}] = \varphi(m)$ und $[K_1 : \mathbb{Q}] = \varphi(m_1)$ und daher

$$[K : K_1] = \frac{\varphi(m)}{\varphi(m_1)} = \varphi(p^a) = [\mathbb{Q}(\zeta_{p^a}) : \mathbb{Q}]$$

Aufgrund dieser Gleichheit muss das p^a-te Kreisteilungspolynom irreduzibel sein (da $[K : K_1]$ sonst nicht den volle Erweiterungsgrad $[K : K_1]$ hätte sondern einen echten Teiler davon). Wendet man den ersten Punkt vermöge $p \nmid m_1$ auf den Körper K_1 an erhält man

$$pO_{K_1} = P_1 \dots P_g, \qquad g = \frac{\varphi(m)}{f}$$

Nach Satz 5.3 sind in der nach Satz 5.6 normalen Erweiterung $[K : \mathbb{Q}]$ alle Verzeigungsindizes gleich also hat man

$$pR_K = (\wp_1 \wp_2 \dots \wp_r)^e \tag{5.31}$$

wobei es unsere Aufgabe ist r, e zu bestimmen. Für die $\wp_i$ von oben sagt Satz 5.3

$$ref_{K/\mathbb{Q}}(\wp_i) = [K : \mathbb{Q}] = \varphi(m_1) \tag{5.32}$$

und weil p unverzweigt ist in K_1/Q, muss $(e, [K_1 : \mathbb{Q}]) = 1$ gelten und wegen (5.32) daher

$$e|[K : K_1] = \varphi(p^a)$$

Beachte nun, dass p wegen $N_{K_m/\mathbb{Q}}(p) = p$ und der Multiplikativität der Norm höchstens $\varphi(p^a)$ Nichteinheiten als Teiler in einer beliebigen Faktorisierung haben kann (die dann alle Konjugierte mit Norm jeweils p sind). Diese Tatsache angewandt auf die konkrete Faktorisierung

$$p = F_{p^a}(1) = \prod_{k, p\nmid k} (1 - \zeta_{p^a}^k) = (1 - \zeta_{p^a})^{\varphi(p^a)} \cdot \prod_{k, p\nmid k} (1 + \zeta_{p^a} + \ldots + \zeta_{p^a}^{k-1})$$

zeigt, dass der letzte Produktterm eine Einheit ϵ sein muss, da $(1 - \zeta_{p^a})$ offensichtlich nicht Norm 1 hat und damit keine ist. Diese Erkenntnis bedeutet also zusammengefasst

$$p = \epsilon \cdot (1 - \zeta_{p^a})^{\varphi(p^a)}$$

Zusammen mit (5.31) also

$$pO_K = (1 - \zeta_{p^a})^{\varphi(p^a)} O_K = (\wp_1 \dots \wp_r)^e$$

und weil $e|\varphi(p^a)$ muss $e = \varphi(p^a)$ gelten.
Für r kann man nach Defintion von f, g mittels Satz 1.7 sofort auf $r \geq g$ schließen. Für die andere Ungleichung ergibt $e = \varphi(p^a)$

$$r\varphi(p^a) f_{K/\mathbb{Q}}(\wp_i) = \varphi(m) = \varphi(m_1)\varphi(p^a) \Longrightarrow r f_{K/Q}(\wp_i) = \varphi(m_1)$$

Nach Definiton ist aber auch $fg = \varphi(m_1)$ und aber auch $f_{K/Q}(\wp_i) = f_{K/K_1}(\wp_i) f$. Kombination dieser 3 Gleichungen ergibt

$$r f_{K/K_1}(\wp_i) = g \Longrightarrow g \geq r$$

□

5.6 P-adische Körper

Am Anfang sei an Abschnitt 5.1 verwiesen, dessen Notation wieder verwendet wird. In diesem und dem folgenden Unterkapitel werden eine Reihe von Sätzen und Lemmata aufgrund des Umfangs nur mit groben Beweisskizzen angeführt. Lediglich Sätze, in denen auf mehrere vorangehende Feststellungen zurückgegriffen wird, werden exakt bewiesen um den logischen Aufbau möglichst lückenlos zu illustrieren. Man findet die fehlenden Beweise sämtlich in [Na74].

Satz 5.9 (Vervollständigung)**.** Sei K Körper mit Bewertung v. Dann existiert ein bis auf Isomorphie eindeutiger Körper (dh alle Bewertungen sind gleich) $L \supset K$ mit Bewertung w derart, dass

1. L ist vollständig bezüglich w
2. die Bewertung w stimmt auf K mit v überein, dh $w(x) = v(x)\ \forall x \in K$.
3. K liegt dicht in L

Darüber hinaus ist w diskret, falls v es ist. Ist v eine zum Primideal P assoziierte Bewertung, gilt $v(K) = v(L)$. Der Ring $R_w := \{x \in L : w(x) \leq 1\}$ ist der Abschluss von $R_v := \{x \in K : v(x) \leq 1\}$ und das Primideal $P_w = \{x \in L : w(x) < 1\}$ ist der Abschluss von $P_v := \{x \in K : v(x) < 1\}$.

Beweis: (Skizze)
Man konstruiert zu einem vollständigen metrischen Raum der die Bedingungen erfüllt (enthält K dicht und die Mterik stimmt mit der Bewertung überein) zuerst eine Ringstruktur, indem man $x+y$ als $\lim x_n + y_n$ für gegen x bzw y konvergente Folgen x_n respective y_n definiert und zeigt, dass dies wohldefiniert ist. Daraus ergibt sich auch unmittelbar der letzte Teil der Aussage über die Abschlüsse. Es stellt sich heraus, dass dies sogar eine Körperstruktur induziert. Die Fortsetzung ist wegen Stetigkeitsgründen wieder eine Bewertung. □

Definition 5.21. Sei v eine diskrete Bewertung *zum Primideal* $P \triangleleft O_K$. In diesem Fall bezeichne K_P oder K_v die Vervollständigung L von K bezüglich der Topologie von v aus dem obigen Satz und diese heißt *P-adischer Körper*. Zugehöriges R_P wie oben nennen wir den *Ganzheitsring von K_P*.

Man beachte, dass für die Ganzheitsringe von nicht P-adischen Körpern der Ganzheitsring mit dem Buchstaben O statt R bezeichnet wird. Dies soll zur leichteren Unterscheidung dienen.

Korollar 5.6. Ist v diskrete Bewertung von K und L dessen Vervollständigung mit Metrik w und gilt $|R_v/P_v| < \infty$, dann ist die von der Einbettung von K in L induzierte Abbildung

$$R_v/P_v \longmapsto R_w/P_w$$

ein Isomorphismus.

Beweis: Zweifellos ist die Abbildung ein Homomorphismus. Wegen der letzten Aussage von Satz 5.9 ist das Bild dicht, wegen der geforderten Endlichkeitsbedingung muss die Abbildung also bijektiv sein. □

Dieser Satz 5.9- insbesondere die Übereinstimmung der Bildbereiche $v(K) = v(K_P)$ wie aus der Beweisskizze ersichtlich wird- ermöglicht im Fall einer von einem Primideal erzeugten Bewertung eine Ausweitung des Begriff des Exponenten auf K_P durch

$$n_P(x) := \log_a v(x), \qquad x \in K_P$$

mit $a \in (0,1)$ derart, dass $v(x) = a^{n_P(x)}$ erfüllt ist.

Tatsächlich sind alle diskreten Bewertungen von diesem Typ, wie folgender Satz zeigt.

Satz 5.10. Sei K Zahlkörper. Alle Bewertungen von K sind archimedisch oder diskret. Ist v *diskrete* Bewertung von K, dann exisitert ein Primideal $P \triangleleft O_K$ mit

$$v(x) = a^{n(x)}, \qquad a \leq 1$$

wobei n der Exponent zu P ist. Ist v *archimedische* Bewertung von K, so ist

$$v(x) = |\sigma(x)|$$

mit einem Monomorphismus $\sigma : K \mapsto \mathbb{C}$.
Umgekehrt erzeugt jedes Primideal $P \triangleleft O_K$ eine diskrete Bewertung von K und jede Einbettung $K \mapsto \mathbb{C}$ eine archimedische Bewertung. Bewertungen zu verschiedenen Primidealen sind nicht äquivalent und Bewertungen die von Einbettungen herrühren sind genau im Falle äquivalent, dass sie komplex konjugiert zueinander sind.

Beweis: (Skizze)
Erst beweist man für den Fall $K = \mathbb{Q}$, dass jede nichttriviale Bewertung entweder äquvalent zur Betragsfunktion $|x|$ ist oder äquivalent zur von einer Primzahl inuduzierten p-adischen Bewertung, wobei man den archimedischen und diskreten Fall separat behandelt. Im diskreten Fall kann man durch geschickte Wahl eine Ungleichung

$$v(M) \leq \max(1, v(n)^{\log M / \log n}), \qquad M, n \in \mathbb{Z}$$

herleiten, und das ausnutzen um weiter zu zeigen, dass $\frac{\log v(n)}{\log n}$ konstant ist, was gerade bedeutet, dass $v(x) = |x|^c, c \in \mathbb{R}$ äquivalent zur Betragsbewertung ist. Im archimedischen Fall behilft man sich mit der Menge

$$A := \{n \in \mathbb{Z} : v(n) < 1\}$$

und zeigt, dass dies ein Ideal $A \triangleleft \mathbb{Z}$ ist um schließlich zu zeigen, dass die Bewertung wie gefordert äquivalent zu einer p-adischen ist.
Im Fall $[K : \mathbb{Q}] \geq 2$ unterscheidet man wieder zwischen diskreten und archimedischen Bewertungen. Im diskreten Fall schhreibt man für jedes $x \in K$ $v(x) = c^{n(x)}$ und zeigt letztendlich, dass dieses c nicht von x abhängt, wobei ein wesentlicher Schritt ist zu zeigen, dass die Einschränkung $m(x)$ von $n(x)$ auf $\mathbb{Q}$ nicht die Nullabbildung ist und

deshalb weiter wegen obigem $K = \mathbb{Q}$-Fall $m(x)/e$ eine von einer Primzahl induzierten Bewertung ist, wobei e der kleinste in $\mathbb{Q}$ angenommene Wert von $n(x)$ in $\mathbb{Q}$ ist. Der archimedische Fall ist überaus technisch, und es sei wieder auf [Na74] verwiesen. □

Uns interessiert die Aussage obigen Satzes im diskreten Fall. Bald werden wir folgende etwas aus obigem Zusammmenhang fallende topologische Proposition benötigen.

Proposition 5.12. Sei $K \subset \mathbb{C}$ komplexer Körper mit einer Bewertung v und sei E endlichdimensionaler Vektrorraum über K. Hat E eine von der Norm induzierte Topologie in der Addition und skalare Multiplikation (mit Elementen von K) *stetig* sind, und induziert diese Normtopologie darüber hinaus auf eindimensionalen Unterräumen $\{ax : a \in K\}$ die Topologie von K, dann stimmt die Normtopologie mit der Produkttopologie überein, also ist

$$f: \quad K^n \longmapsto E$$

$$[x_1, x_2, \ldots x_n] \longmapsto \sum_{j=1}^{n} x_j a_j$$

ein topologischer Isomorphismus.

Beweis: (Skizze)
Aus der Definition ist leicht ersichtlich, dass f stetiger Isomorphismus ist. Die Bijektivität folgt beispielsweise etwa weil die a_i voraussetzungsgemäß eine K-Basis von E bilden. Um zu zeigen, dass es sich um einen *topologischen* Isomorphismus handelt, beweist man die Beziehung

$$v(x_i) \leq C \cdot \|x_1 a_1 + \ldots + x_n a_n\|, \qquad 1 \leq i \leq n, x_i \in K$$

Dies geschieht durch einen technischen Induktionsbeweis. Man betrachtet die Mengen E_j, die aus den Elementen des Bildbereichs E bestehen, von denen maximal j Stück der x_i in der Darstellung von Null verschieden sind. Der Induktionsanfang ist in den Voraussetzungen bereits vorhanden, sollte es für E_j stimmen aber nicht für E_{j+1}, so kann man durch geschickte Koordinatenwahlen die Existenz eines Elements ableiten, das gegen 0 konvergiert und gleichzeitig nicht gegen 0 konvergieren kann, was den notwendigen Widerspruch bedeutet. □

Proposition 5.13. 1. Der Ring R_P ist Dedekindring mit trivialer (einelementiger) Idealklassengruppe. $\wp := \{x \in K_P : v(x) \leq 1\}$ mit der zu P gehörigen Bewertung v (wie oben) ist das eindeutige von Null verschiedene Primideal von R_P und es gilt der Körperisomorphismus

$$R_P/\wp \cong O_K/P$$

2. Der Ring R_P ist der topologische Abschluss von O_K in K_P, also

$$\overline{O_K} = R_P$$

und außerdem

$$\overline{P^m} = \wp^m, \qquad \wp^m \cap O_K = P^m$$

3. Bezeichne mit $U(K_P)$ die Gruppe der invertierbaren Elemente von K_P. Dann gilt

$$U(K_P) = R_P \setminus \wp$$

und zu jedem festen $\zeta \in \wp \setminus \wp^2$ hat jedes $y \in K_P$ eine eindeutige Darstellung

$$y = a \cdot \zeta^{n_P(x)}$$

Beweis:

1. Folgt aus Lemma 5.1, Proposition 5.2 und Korollar 5.6.
2. Für beliebiges $x =\in K$ sei $n_P(x) = m$. Das bedeutet, dass man $x = \frac{a}{b}$ schreiben kann mit $a \in P^m, b \notin P$. Wähle vermöge Satz 2.3 (chinesischer Restsatz) für jedes $n \in \mathbb{N}$ ein $z_n \in \wp^n$ mit
$$a - bz_n \equiv 0 \pmod{\wp^n}$$
Nach Konstruktion konvergiert die Folge z_n gegen $\frac{a}{b} = x$. Weil ebenfalls nach Konstruktion alle $z_n \in \wp^m \cap K$ haben wir also
$$\wp^m \cap K \subset \overline{P^m} \quad \Longrightarrow \quad \wp^m \subset \overline{P^m}$$
Weil $\wp^m$ abgeschlossen ist und $\wp^m$ dicht in P^m ist gilt sogar Gleichheit in rechter Inklusion und Punkt 2 folgt.
3. Wegen Lemma 2.5 besteht in einem Ring mit eindeutigem Primideal selbiges genau aus den Nichteinheiten. Hinsichtlich des ersten Punktes ist die Aussage klar.

□

Satz 5.11. Sei K Zahlkörper, und $0 \neq P \triangleleft O_K$ Primideal mit Vervollständigung K_P. Sei weiter L/K endliche Erweiterung von K und $\wp \triangleleft O_L$ ein Primideal das über P liegt mit Vervollständigung $L_\wp$. Weiters bezeichne wie üblich mit R_P,$R_\wp$ die Ganzheitsringe in K_P,$L_\wp$ respective. Dann gilt:

1. $[L_\wp : K_P] = e_{L/K}(\wp) f_{L/K}(\wp)$
2. $L_\wp = K_P L$ ($L_\wp$ wird also von K_P und L erzeugt)
3. $R_\wp$ ist der ganze Abschluss von R_P in $L_\wp$
4. Sind $P_1 \triangleleft R_P$, $\wp_1 \triangleleft R_\wp$ Primideale, dann liegt $\wp_1$ über P_1 und ist das einzige solche Primideal von $R_\wp$ und
$$e_{L_{\wp_1}/K_{P_1}}(\wp_1) = e_{L/K}(\wp), \qquad f_{L_{\wp_1}/K_{P_1}}(\wp_1) = f_{L/K}(\wp)$$

Beweis: Der Abschluss von K in $L_\wp$ ist vollständig und kann vermöge Satz 5.9 mit K_P identifiziert werden. Bezeichne mit $a_1, a_2 \ldots a_n$ eine Basis des K-Vektorraums L und setze

$$H := a_1 K_P + a_2 K_P + \ldots + a_n K_P$$

Offenbar ist H K_P-Vektorraum und $L \subset H \subset L_\wp$ sowie $\dim_{K_P} H \leq n$. Nach Proposition 5.12 trägt H die Produkttopologie von K_P^n. Bezüglich der Produkttopologie ist K_P^n aber abgeschlossen, also muss bereits $H = L_\wp$ gelten. Weil H aber nach Definiton von K_P und L erzeugt wird, folgt Punkt 2. Proposition 5.13 zeigt, dass $\wp_1$ einziges Primideal von

$R_{\wp_1}$ ist. Es liegt also wie gefordert über P_1. Wir befinden uns in einem Dedekindring, also können wir Lemma 5.3 anwenden um

$$[L_\wp : K_P] = e_{L_\wp/K_P}(\wp_1) f_{L_\wp/K_P}(\wp_1)$$

zu erhalten. Hinsichtlich Punkt 1 von Proposition 5.13 gilt $f_{L_\wp/K_P}(\wp_1) = f_{L/K}(\wp)$. Zur Vereinfachung führen wir folgende Notation ein:

$$e := e_{L_\wp/K_P}(\wp_1), \qquad e_1 := e_{L/K}(\wp)$$

Nach der Definition des Verzeigungsindex also $PO_L = \wp^{e_1} Q$ mit $\wp \nmid Q$. Bildet man auf beiden Seiten die Abschlüsse und bezeichnet man den Abschluss von Q mit Q_1, dann haben wir $PR_\wp = \wp_1^{e_1} Q_1$. Weil $\wp \nmid Q$ und Teilbarkeit umgekehrte Inklusion bedeutet gibt es ein $y \in Q \setminus \wp$ das Einheit in $R_\wp$ ist, also $Q_1 = R_\wp$ und letztlich

$$\wp_1^e = P_1 R_\wp = \wp_1^{e_1} \Longrightarrow e = e_1$$

Also haben wir Punkt 4 und in trivialer Folge aus Lemma 5.3 auch Punkt 1 bewiesen. Für Punkt 3 sei $a \in R_\wp$. Nach Proposition 5.13 Punkt 2 und der Definition des Abschlusses gibt es eine Folge $x_1, x_2, \ldots$ in O_L vom vollen Grad $n = [L : K] = [O_L : O_K]$ (wobei zweiter als Modulgrad zu verstehen ist) die gegen a konvergiert. Seien die Minimalpolynome der ganzalgebraischen Elemente x_i gegeben durch

$$F_i(t) = t^n + c_{n-1}^i t^{n-1} + \ldots + c_0^i, \qquad c_j^l \in O_K$$

Halte nun denn unteren Index fest und wähle eine konvergente Teilfolge mit $c_j := \lim_{i\to\infty} c_j^i$. Das Polynom $F(t) = t^n + c_{n-1}t^{n-1} + \ldots c_0$ hat a als Nullstelle wegen der Stetigkeit, also ist a im Ganzheitsring von R_P, denn die c_j sind natürlich in R_P. Wegen der Belieibigkeit von $a \in R_\wp$ ist also $R_\wp$ im ganzen Abschluss von R_P in L enthalten. $R_\wp$ ist aber ganzabgeschlossen und es gilt $R_P \subset R_\wp$. Daraus folgt die ausständige dritte Behauptung.

□

Seien nun im folgenden K ein P-adischer Körper(!) Zum Studium algebraischer Zahlkörper sind normale Erweiterungen solcher P-adischer Körper nützlich. Sei also L/K normal mit Galoisgruppe $G(L/K)$. Sei R Ganzheitsring von K und S Ganzheitsring von S. Nach dem vorangehenden Unterkapitel haben R und S je genau ein Primideal P respective $\wp$, und die entsprechenden Restklassenkörper seien mit k_K und k_L bezeichnet. Da k_L/k_K eine Körpererweiterung zweier endlicher Körper ist, ist es eine Galoiserweiterung, die Galoisgruppe heiße $G(k_L/k_K)$. Wir führen nun eine Abbildung ein.

$$\Lambda : G(L/K) \longmapsto G(k_L/k_K)$$

$$g \longmapsto \Lambda(g)$$

wobei für $a \in S$ gelte

$$\Lambda(g)(a) = g(a) \pmod{k_L}$$

Da diese Abbildung nur von der Klasse von $a \pmod{k_K}$ abhängt ist die Zielmenge tatsächlich $G(k_L/k_K)$. Der Grund hiefür ist: Gilt $a \equiv b \pmod{k_K}$, so ist die Differenz durch das Primideal teilbar, was $n_L(a-b) \geq 1$ nach sich zieht. Darum auch $n_L(g(a) - g(b)) \geq 1$ und dasselbe Argument wie eben in die andere Richtung gelesen ergibt $g(a) \equiv g(b) \pmod{k)_L}$. Schränkt man Λ also von S auf den Restklassenkörper k_L ein, so bleibt k_K fixiert. Weiter kann man von Λ nachprüfen, dass es ein Homomorphismus ist, *dessen Kern wir mit G_0 bezeichnen und Trägheitsgruppe von L/K* nennen. Es gilt (ohne Beweis)

$$G_0 = \{g \in G : \forall y \in S \quad g(y) \equiv y \pmod{\wp}\}$$

Wir erinnern für nächste Definition an die Einheitengruppe U_K aus Proposition 5.13. Wir definieren U_i als Teilmenge der Einheiten von U der Form $1 + \wp^i$.

Definition 5.22. Für $i = 1, \ldots$ und der Trägheitsgruppe G_0 einer Erweiterung L/K seien durch

$$G_i = \{g \in G_0 : \frac{g(x)}{x} \in U_i(L) \quad \forall x \in S \setminus \{0\}\}$$

die *Verzweigungsgruppen* definiert.

Es handelt sich in der tat um Gruppen: Für $g_1, g_2 \in G_i$ und $x \neq 0$ gilt

$$\frac{(g_1 g_2)(x)}{x} = \frac{g_1(g_2(x))}{g_2(x)} \cdot \frac{g_2(x)}{x} \in U_i(L)$$

denn im ersten Bruch spielt $g_2(x)$ die Rolle des x aus der Definition und das Produkt invertierbarer Elemente ist wieder invertierbar. Das zeigt, dass G_i abgeschlossen bezüglich Gruppenoperation ist, und wegen der Endlichkeit muss das Inverse nicht überprüft werden um es als Gruppe auszuweisen.
Wegen $g(x)x^{-1} \in 1 + \wp^i$ für alle $x \in S$ und hinreichend großen Index i nur für die Identität gelten kann- da es für ein von Null verschiedenes Element eine maximale $\wp$-Potenz gibt die diese teilt- sind ab einem gewissen Index alle Verzweigungsgruppen trivial.

Satz 5.12. Sei L/K normale Erweiterung eines P-adischen Körpers K und $G = G(L/K)$. Dann gilt:

1. Die maximale unverzweigte Erweiterung L_0/K mit $L_0 \subset L$ hat die Trägheitsgruppe G_0 als Galoisgruppe
$$G(L/L_0) = G_0$$
Es gilt $G_0 \triangleleft G$ (also G_0 ist Normalteiler) mit $|G/G_0| = e(L/K)$ mit zyklischer Faktorgruppe der Ordnung $f(L/K)$. Identifiziert man $G(L/L_0) = G_0$, so stimmen die Verzweigungsgruppen von L/K und L/L_0 überein.
2. Die maximale schwach verzweigte Erweiterung L_1/K von K die in L enthalten ist (also $L_1 \subset L$) hat die erste Verzweigungsgruppe G_1 als vom Hauptsatz der Galoistheorie induzierte Galoisgruppe und es gilt wieder $G_1 \triangleleft G$. Ist p die Charakterisitk von k_K, dann ist G_1 ist eine p-Gruppe und G_0/G_1 ist zyklisch mit $p \nmid |G_0/G_1|$ und es existiert eine Einbettung
$$\Delta : G_0/G_1(k_L, \cdot)$$
in die multiplikative Gruppe von k_L.

3. Für $i \leq t$ mit t so, dass G_t ist die letzte nichttriviale Verzweigungsgruppe ist gilt $G_i \triangleleft G$ und ein isomorphes Bild von G_i/G_{i+1} kann in U_i/U_{i+1} eingebettet werden. Die Isomorphismen sind dabei induziert durch die wohldefinierten Homomorphismen

$$f_i : G_i \longmapsto U_i/U_{i+1}$$

$$f_i(g) = g(\Pi)\Pi^{-1}, \qquad \Pi \in k_L^*$$

Beweis: (Skizze)

1. Sei $g \in G(L/L_0)$- der L_0 entsprechenden Untergruppe von L/K im Sinne der Galoistheorie. Beachte, dass $k_{L_0} = k_L$. Assoziiere gemäß dieser Beziehung jedem Element von k_L ein Element von L_0. Dieses ist linksinvariant unter g, was gerade $g \in G_0$ bedeutet. Man zeigt weiter unter anderem über den Isomorphismus $G(L_0/K) \cong G/G(L/L_0)$, dass $|G_0| = |G(L/L_0)|$, und zusammen mit der erwähnten Inklusion bleibt den Gruppen nichts anderes über als übereinzustimmen. Die letzten Aussagen vonPunkt 1 folgen über den Sachverhalt, dass bei einer unverzweigten P-adischen Erweiterung die Galosigruppe stets zyklisch ist. Hiefür sei auf Theorem 5.8 und Corollary 2 davon in [Na74] verwiesen.

2. Man bedient sich der Abbildung

$$\varpi : G_0 \longmapsto k_L^*$$

$$\varpi(g) \equiv g(\Pi)\Pi^{-1} \pmod{\wp}$$

die nicht von der Wahl von Π abhängt, zeigt dass sie Homomorphismus mit Kern G_1 ist. Wegen $G_1 \subset G_0$ enthält der zu G_1 gehörige Fixpunktkörper $M := FIX(G_1)$ den Körper L_0, die maximale unverzweigte Erweiterung von K in L. Genauer zeigt man

$$K \subset L_0 \subset M \subset L_1 \subset L$$

mit $[L : L_1] = p^k$. Man erhält dass $G(L/L_1)$ die maximale p-Untergruppe von $G(L/M)$ und folglich normal ist. Damit ist L_1/M schwach verzeigt und voll verzweigt (das heißt $f = 1$). Mithilfe eines Satzes zur Charakterisierung solcher voll und schwach verzweigten Erweiterungen p-adischer Körper (siehe Theorem 5.11 [Na74]) zeigt man letztlich $M = L_1$. Da der Homomorphismus *varpi* eine Einbettung von G_0/G_1 in die zyklische Gruppe k_L^* induziert (bemerke: endliche Untergruppen eines Körpers sind stets zyklisch) muss der Faktor G_0/G_1 selbst zyklisch sein.

3. Man weist nach, dass die f_i von Π unabhängige Homomorphismen sind. Es gilt $\ker f_i = G_{i+1}$ und die Normalteielreeigenschaft folgt, weil G_i die maximale Untergruppe von G ist die trivial auf S/P^{i+1} wirkt und für $g \in G$ und ein h das trivial auf S/P^{i+1} wirkt, muss auch ghg^{-1} trivial auf S/P^{i+1} wirken.

□

Zum Abschluss der Vollständigkeit halber noch ein Lemma und ein Korollar mit skizzenhaften Beweisen, das wir im Beweis von Proposition 5.14 brauchen werden.

Lemma 5.9. Die Erweiterung L/K zweier P-adischer Körper K, L ist unverzweigt $\Longleftrightarrow$ $\exists a \in S : L = K(a)$ und das Bild von a in k_L ist einfache Nullstelle eines Polynoms $\varphi(x) \in k_K[x]$, wobei $\varphi(x)$ aus einem Polynom $F \in R[x]$ mit $F(a) = 0$ durch Reduktion der Koeffizienten $\pmod P$ entsteht.

Beweis: (Skizze) Aus der Unverzweigtheit von L/K folgt $n = f = [k_L/k_K]$. Sei $\overline{a}$ Erzeuger der separablen weil endlichdimensionalen Erweiterung k_L/k_K und $\varphi(x)$ sein Minimalpolynom. Bezeichne weiter mit $F(x) \in R[x]$ ein monisches Polynom vom Grad n dessen Reduktion $\pmod P$ mit $\varphi(x)$ übereinstimmt. Nach Corollary 1 zu Theorem 5.3 in [Na74] hat F eine Nullstelle in $a \in L$. Man erkennt durch

$$[L : K] = [k_L : k_K] = [K(a) : K]$$

dass F irreduzibel über K ist sowie $K(a) = L$. Nach Konstruktion ist $a \in S$, und die eine Richtung ist gezeigt.
Für die andere Richtung sei oBdA $F(x)$ irreduzible über K. Corollary 4 zu selbigem hier unbewiesenen Theorem 5.3 aus [Na74] zeigt, dass φ Potenz eines irreduziblen Polynoms sein muss. Weil es eine einfache Nullstelle besitzt muss es selbst irreduzibel sein. Man erzielt also das Ergebnis

$$n = \deg F = \deg\varphi = [k_L : k_K] \leq n$$

Also $f(L/K) = [k_L : k_K] = n$. Daher ist L/K unverzweigt. □

Korollar 5.7. Sind für P-adische Körper K, L beide L/K und M/K unverzweigt, so auch LM/K.

Beweis: Sei $a \in S$ wie in vorangehendem Lemma 5.9 derart, dass insbesondere also $L = K(a)$. Dann ist $LM = KM(a)$ und das Bild von a in k_{LM} ist einfache Nullstelle des Minimalpolynomes φ aus Lemma 5.9 (also das Minimalpolnom $\varphi \in k_K[x]$ in k_L). Die Aussage folgt nun aus der Äquivalenz aus Lemma 5.9. □

Weiters gilt obiges Korollar, falls man *unverzweigt* durch *schwach verzweigt* ersetzt. Dies werden wir im Beweis von Proposition 5.15 ebenfalls verwenden. Der Beweis unterscheidet sich stark von dem von Lemma 5.9 und sei hier ebenfalls ausgelassen.

5.7 Anwendung P-adischer Körper auf algebraische Zahlkörper

Wir wollen nun die Resultate von eben auf normale Erweiterungen L/K mit algebraischen Zahlkörpern K, L heben. Das Konzept von Trägheits-und Verzweigungsgruppen lässt sich hinsichtlich des folgenden Satzes übernehmen.

Satz 5.13. Sei L/K normale Erweiterung mit Galoisgruppe $G = G(L/K)$. Sei $P \triangleleft O_K$ Primideal von O_K und $\wp \triangleleft O_L$ ein Primideal über P. Dann gilt:
Die Erweiterung $L_\wp/K_P$ von P-adischen Körpern ist normal und es gibt eine kanonische Einbettung

$$\Gamma : G(L_\wp/K_P) \longmapsto G$$

und vermöge der induzierten Identifikation von $L_\wp/K_P$ mit $\Gamma(L_\wp/K_P)$ gilt weiter

$$|G/G(L_\wp/K_P)| = \sharp\{\wp \triangleleft O_L : \wp \quad prim, \quad liegt \quad über \quad P \quad in \quad L\}$$

Beweis: (Skizze) Erst muss man zeigen, dass für einen Erzeuger $a \in L$ von L/K gilt $L_\wp = K_P(a)$. Weil die Konjugierten von a in K_P alle auch Konjugierte von a in K sind, liegen sie sämtlich in $L \subset L_\wp$. Weil dies für alle Konjugierten gilt, ist also $L_\wp/K_P$ normale Erweiterung. Des weiteren muss die Einschränkung eines Automorphismus $s \in G(L_\wp/K_P)$ auf L in $G = G(L/K)$ liegt, und diese Einschränkung ist injektiv, denn wenn die EInschränkung die Identität auf L ist muss $s(a) = a$ gelten und daher weil a wie festgehalten Erzeuger von $L_\wp$ bezüglich K_P ist, muss in diesem Fall die ganze Abbildung die Identität sein. Aus Punkt 1 von Satz 5.11 sowie Satz 5.3 gewinnt man schlielich die Anzahlformel. □

Definition 5.23. Das Bild $\Gamma(G(L_\wp/K_P)) \subset G(L/K)$ heißt *Zerlegungsgruppe des Ideals* $\wp$. Identifziert man wieder $G(L_\wp/K_P)$ mit $\Gamma(G(L_\wp/K_P))$, so sind auch die zugehörigen Trägheits- und Verzweigungsgruppen von $L_\wp/K_P$ Untergruppen von $G(L/K)$, $G_i(L_\wp/K_P) \subset G(L/K)$ bzw $\Gamma(G_i(L_\wp/K_P)) \subset G(L/K)$. Diese heißen *Trägheitsgruppe und Verzweigungsgruppen des Primideals* $\wp$ *über* K.

Man kann zeigen: definiert man in einer normalen Erweiterung L/K mit Primideal $\wp \triangleleft O_L$

$$G_{-1}(\wp) = \{g \in G : g(\wp) = \wp\}$$

$$G_i(\wp) = \{g \in G : \quad \forall a \in O_L : g(a) - a \in \wp^{1+i}\}, \qquad i \geq 0$$

so ist G_{-1} die Zerlegungsgruppe gemäß obiger Definition, G_0 die Trägheitsgruppe und die G_i zu positivem Index stimmen mit den Verzweigungsgruppen überein.

Nach dem Hauptsatz der Galoistheorie entsprechen jeder dieser Untergruppen zum Primideal $\wp$ je ein Zwischenkörper der Erweiterung L/K. Genauer definieren wir:

Definition 5.24. Sei mit $K_{-1}(\wp)$ der über Galoistheorie der Zerlegungsgruppe von $\wp$ entsprechende Zwischenkörper von L/K bezeichnet. Wir nennen ihn *Zerlegungskörper zu* $\wp$. Ebenso sei mit $K_0(\wp)$ der zur Trägheitsgruppe G_0 gehörige Zwischenkörper *Trägheitskörper zu* $\wp$ bezeichnet und der zur i-ten Verzweigungsgruppe G_i gehörige Zwischenkörper sei K_i und *i-ter Verzweigungskörper zu* $\wp$ genannt.

In der Herleitung der Klassenzahlformel für abelsche Zahlkörper wird das kommende Resultat benötigt, das gewissermaßen das Ziel dieses Unterkapitels darstellt.

Lemma 5.10. Sei wieder $\wp$ Primideal in O_L und bezeichne mit $\wp_i \triangleleft R_{K_i}$ das eindeutige Primideal von R_{K_i} das unter $\wp$ liegt und mit $P \triangleleft O_K$ das Primideal von K das unter $\wp$ liegt. Dann git:

$$P \cdot O_{K_{-1}} = \wp_{-1} \cdot Q, \qquad \wp_{-1} \nmid Q, \qquad f_{K_{-1}/K}(\wp_{-1}) = 1$$

Außerdem ist K_{-1} der maximale Teilkörper von L mit diesen Eigenschaften.
In K_0 gilt

$$P \cdot O_{K_0} = \wp_0 \cdot Q_0, \qquad \wp_0 \nmid Q_0, \qquad f_{K_0/K}(\wp_0) = f_{L/K}(\wp)$$

und K_0 der maximale Teilkörper von L mit diesen Eigenschaften.
Ähnlich gilt in K_1

$$P \cdot O_{K_1} = \wp_1^{e_0} \cdot Q_1, \qquad \wp_0 \nmid Q_1, \qquad f_{K_1/K}(\wp_1) = f_{L/K}(\wp)$$

und K_0 der maximale Teilkörper von L mit diesen Eigenschaften, wobei e_0 gegeben ist als $e(L/K) = e_0 p^m$, $p \nmid e_0$ wo p die Chararkterisitk von $O_L/\wp$ ist.
Schließlich ist K_0/K_{-1} zyklisch (bestitzt also eine zyklische Galoisgruppe) vom Grad

$$|K_0/K_{-1}| = f_{L/K}(\wp)$$

K_1/K_0 ist zyklisch vom Grad

$$|K_1/K_0| = e_0,$$

und L/K_1 ist p-Erweiterung vom Grad

$$|L/K_1| = \frac{e}{e_0}.$$

Beweis: Wegen $K \subset K_{-1} \subset L$ und $\wp_{-1}$ über P liegt erkennt man, dass
$K_P \subset (K_{-1})_{\wp_{-1}} \subset L_\wp$. Die Galoisgruppe $\mathrm{Gal}(L_\wp/K_P)$ fixiert nach Definition K_{-1}, aus Stetigkeitsgründen auch die Vervollständigung $(K_{-1})_{\wp_{-1}}$. Wegen der 1:1 Korrespondenz aus dem Hauptsatz der Galoistheorie folgt unmittelbar $K_P = (K_{-1})_{\wp_{-1}}$. Zusammen mit Satz 5.11 also

$$e_{K_{-1}/K}(\wp_{-1}) = f_{K_{-1}/K}(\wp_{-1}) = 1$$

Das bedeutet aber gerade $P \cdot O_{K_{-1}} = \wp_{-1} Q$, $\wp_{-1} \nmid Q$. Ist umgekehrt $K \subset M \subset L$ und $\wp_M \triangleleft O_M$ das unter $\wp$ liegt, so folgt $e_{M/K}(\wp_M) = f_{M/K}(\wp_M) = 1$ also $M_{\wp_M} = K_P$, also wird M von G_{-1} fixiert und ist daher in K_{-1} enthalten, wegen der 1:1 Korrespondenz also $M = K_{-1}$. Daraus folgt die geforderte Maximalität. Die übrigen Behauptungen sind Fogerungen aus Satz 5.11 und Satz 5.12 angewandt auf die Gruppen G_i. □

Die Gruppen G_i ermöglichen vermöge vorangehenden Lemmas uns nun auch die Struktur der Zerlegung von Primidealen die unter einem vorgegebenen Primideal liegen, sowie jene von Zwischenkörpern. Dies ist im nächsten Korollar festgehalten.

Korollar 5.8. Sei L/K normale Erweiterung eines Zahlkörpers K.

1. Sei $\wp \triangleleft O_L$ Primideal und P das eindeutige Primideal das unter $\wp$ liegt. Dann steht der Verzweigungsindex und der Trägheitsindex zu den Gruppen $G_i(\wp)$ in Verbindung durch

   $$e_{L/K}(\wp) = |G_0(\wp)|, \qquad f_{L/K}(\wp) e_{L/K}(\wp) = |G_{-1}(\wp)|$$

   Aus vorangehendem Lemma folgt unmittelbar weiter, dass $P \cdot O_L$ Produkt von $r := \frac{[L:K]}{|G_{-1}(\wp)|}$ Primidealen $P_1, \dots P_r \triangleleft O_L$ ist.
2. Ist $K \subset M \subset L$ Zwischenkörper, dann ist die Gruppe $G_i^*(\wp) \subset G(L/M)$- definiert als die Gruppe G_i gebildet bezüglich der Erweiterung L/M mit entsprechender Galoisgruppe $G(L/M)$- gleich dem Schnitt der Gruppe $G_i(\wp)$ bezüglich der Erweiterung L/K mit $G(L/M)$, also

   $$G_i^*(\wp) = G_i(\wp) \cap G(L/M)$$

Zum Abschluss des Unterkapitels wieder eine technische Proposition mit Korollar, das wir für den Beweis von Proposition 5.15 brauchen werden.

Proposition 5.14. Ist L/K Erweiterung zweier Zahlkörper dann gilt

$$D_{L/K} = \prod_{\wp} (D_{L_\wp/K_P} \cap R_L)$$

wobei man das Produkt über alle Primideale $\wp \lhd O_L$ erstreckt und jeweils $P \lhd O_K$ das unter $\wp$ liegende Primideal bezeichnet.

Ein Beweis findet sich auf Seite 267 in [Na74].

Korollar 5.9. Ein Primideal $\wp \lhd O_L$ ist unverzweigt bzw schwach verzweigt in L/K genau dann wenn die zugehörige P-adische Erweiterung unverzweigt bzw schwach verzeigt ist. Dabei ist $P \lhd O_K$ das Primideal unter $\wp$.

Der Beweis hierzu folgt noch nicht trivial aus Proposition 5.14 und erfordert noch eine technische Aussage über den Differenten, siehe Theorem 4.8 und Corollary 1 dazu auf Seite 166 in [Na74].

5.8 Klassenzahlformel für abelsche Zahlkörper

Grundlage für die spezielle Klassenzahlformel für abelsche Zahlkörper bildet der Satz von Kronecker-Weber. Für einen abelschen Zahlkörper K sei $\tau = \tau(K)$ die kleinste natürliche Zahl, sodass $K \subset K_\tau$ gilt, wobei $K_\tau = \mathbb{Q}(\zeta_\tau)$ der τ-te Kreisteilungskörper ist. Wir nennen dieses $\tau(K)$ den *Führer* von K. Wesentliche Eigenschaften von $\tau(K)$ sind aufgelistet in

Proposition 5.15. Seien K und L abelsche Zahlkörper. Dann gilt:

1. $K \subset K_m \iff \tau(K) | m$
2. $\tau(K \cap L) | (\tau(K), \tau(L))$
3. $\tau(K \cdot L) = [\tau(K), \tau(L)]$
4. eine Primzahl $p \in \mathbb{Z}$ ist verzweigt in $K/\mathbb{Q} \iff p | \tau(K)$
5. eine Primzahl p ist schwach verzweigt in $K/\mathbb{Q} \iff p | \tau(K) \wedge p^2 \nmid \tau(K)$

Dabei bezeichnet $(,)$ den ggT, $[,]$ das kgV, $K \cdot L$ ist die Zusammensetzung der Körper K, L und eine Primzahl p wird mit $p \cdot O_K$ identifiziert.

Beweis:

1. Setzt man $K \subset K_m$ voraus liefert Satz 5.6 Punkt 5

   $$K \subset K_m \cap K_\tau = K_{(m,\tau)}$$

   Weil τ minimal gewählt war gilt $(m, \tau) \geq \tau$. Die umgekehrte Ungleichung ist trivial, also $(m, \tau) = \tau$ und damit $\tau(K) | m$. Die Umkehrung folgt trivial aus $\mathbb{Q}_N \subset \mathbb{Q}_{kN}$ für natürliche Zahlen k, N.

2. Wieder hinsichtlich Punkt 5 Satz 5.6

   $$K \cap L \subset K_{\tau(K)} \cap K_{\tau(L)} = K_{(\tau(K),\tau(L))}$$

   Nach dem eben bewiesenen Punkt 1 folgt Punkt 2.

3. Sei $\tau_0 := \tau(K \cdot L)$. Wegen $K \subset KL$, $L \subset KL$ und $KL \subset K_{\tau_0}$ liefert wieder Punkt 1 dass $[\tau(K), \tau(L)]|\tau_0$. Andererseits haben wir $KL \subset K_{\tau(K)}K_{\tau(L)} = K_{[\tau(K),\tau(L)]}$ und erneute Anwendung von Punkt 1 ergibt $\tau_0|[\tau(K), \tau(L)]$. Die wechselseitige Teilbarkeit zeigt die Gleichheit.

4. Falls $p \nmid \tau = \tau(K)$ dann ist p unverzweigt in $K_\tau/\mathbb{Q}$ nach Satz 5.8 Punkt 1, da die explizite Foreml zeigt, dass jedes Primideal einzeln vorkommt. Insbesondere ist es wegen $K \subset K_\tau$ auch in $K/\mathbb{Q}$ unverzweigt. Im Falle $p|\tau$ ergibt im Fall von unverzweigtem p eine Kombination der Aussagen aus Korollar 5.9 und Satz 5.8 über die Struktur von (p) in $K_m/\mathbb{Q}$, dass p unverzweigt in $K/\mathbb{Q}$ und $K_m/\mathbb{Q}$ ist und nach Korollar 5.7 ebenso in $KK_m/\mathbb{Q}$ ist, mit m so dass $\tau = p^a m$ und $p \nmid m$. Diese Erkenntnis und erneute Anwendung von der Strukturformel aus Satz 5.8 liefert

$$\varphi(p^a) = e_{K_\tau/\mathbb{Q}}(P) = e_{K_\tau/KK_m}(P) \leq [K_\tau : KK_m]$$

$$= \frac{[K_\tau : K_m]}{N} = \frac{\varphi(\tau)}{\varphi(m)N} = \frac{\varphi(p^a)}{N}, \qquad P \lhd K_\tau$$

mit beliebigem Primideal P über p. Folglich $N = 1$. Die Tatsache, dass die Vektorraumdimension $[KK_m : K] = 1$ ist bedeutet aber $K \subset K_m$ aber $\tau = p^a m > m$ ist per Definition die kleinste Zahl die das leistet. Widerspruch.

5. Schreibe wieder $\tau = \tau(K) = p^a m, \nmid m$ und liege $P \lhd K_\tau$ über p.
   $\Longrightarrow$ Nach Punkt 4 gilt $a \geq 1$ und ähnlich wie oben schließt man aus der Bemerkung nach Korollar 5.7, Korollar 5.9 und Satz 5.8, dass p schwach verzweigt in $KK_{pm}/\mathbb{Q}$ ist. Satz 5.8 ergibt

$$e_{K_\tau/\mathbb{Q}}(P) = \varphi(p^a) = p^{a-1}(p-1) \Longrightarrow p^{a-1}|e_{K_\tau/\mathbb{Q}}(P)$$

   Beide Erkenntnisse zusammen ergeben $p^{a-1}|e_{K_\tau/KK_{pm}}(P)$. Weiter

$$p^{a-1}| \quad e_{K_\tau/KK_{pm}}(P)| \quad [K_\tau : KK_{pm}] = \frac{[K_\tau : K_{pm}]}{[KK_{pm} : K_{pm}]}$$

$$= \frac{\varphi(\tau)}{[KK_{pm} : K_{pm}]\varphi(pm)} = \frac{p^{a-1}}{[KK_{pm} : K_{pm}]}$$

   also $[KK_{pm} : K_{pm}] = 1$ ud $K \subset K_{pm}$ und also $\tau|pm$ und wegen $p \nmid m$ auch $p^2 \nmid \tau$ wie gefordert.
   $\Longleftarrow$ Die Formel $e = \varphi(p^a)$ aus Satz 5.8 impliziert $p \nmid e_{K_\tau/\mathbb{Q}}(P)$. Damit ist p unverzweigt in $K_\tau/\mathbb{Q}$ und erst recht in $K/\mathbb{Q}$.

□

Lemma 5.11. Sei K abelscher Zahlkörper, also $K/\mathbb{Q}$ abelsch und K_m ein beliebiger Kreisteilungskörper mit $K \subset K_m$ und $p \in \mathbb{Z}$ Primzahl. Schreibe $m = p^\alpha m_1$ mit $p \nmid m_1$. Sei weiters $\wp \lhd O_{K_m}$ Primideal in K_m das über $p\mathbb{Z}$ liegt.

1. Dann besteht die Zerlegungsgruppe $G_{-1}(\wp)$ genau aus den Restklassen $\pmod m$, die reduziert $\pmod{m_1}$ in der von p erzeugten zyklischen Gruppe liegen.

2. Für die Gruppe Trägheitsgruppe $G_0(\wp)$ haben wir

$$x \in G_0(\wp) \Longleftrightarrow x \equiv 1 \pmod{m_1}$$

3. und $G_1(\wp)$ ist die maximale p-Untergruppe von $G_0(\wp)$.

Beachte dass nach dem Struktursatz für Kreisteilungskörper die Galoisgruppe von K_m isomorph zu $G(m)$, der primen Restklassengruppe modulo m ist und obiges Lemma hinsichtlich dieses Isomorphismus wohldefiniert ist.
Beweis:

1. Der Beweis des ersten Teils ist technisch und erfordert Fallunterscheidungen.
Sei zunächst $\alpha = 0$. Sei f die multiplikative Ordnung von $p \pmod m$ in $G(m)$. Satz 5.8 impliziert, dass $p(= pO_{K_m})$ unverzweigt ist und $f_{K_m/K} = f$. Wir wenden Lemma 5.10 an um

$$|G_{-1}(\wp)| = f, \qquad G_{-1} \cong (\mathbb{Z}/f\mathbb{Z}, +)$$

zu erhalten. Wir zeigen, dass der Automorphismus g_p der

$$g_p : \zeta_m \longmapsto \zeta_m^p$$

erfüllt in G_{-1} ist. Weil in unserem Fall $m = m_1$ und g_p Ordnung f hat, ist dann gemäß unseres Isomorphismus $G(K_m/K) \cong G(m)$ die Aussage bezüglich G_{-1} bewiesen. Wir verwenden

$$x = P(\zeta_m) \equiv 0 \pmod{\wp}, \quad (P(t) \in \mathbb{Z}[t]) \quad \Longrightarrow 0 \equiv P(\zeta_m)^p \equiv P(\zeta_m^p) \pmod{\wp}$$

um

$$g_p(x) = P(\zeta_m^p) \in \wp \Longrightarrow \quad g_p \in G_{-1}$$

zu erhalten. Weil man jedes $x \in \wp$ als $P(\zeta_m), P(t) \in \mathbb{Z}[t]$ darstellen kann, ist wird also das Primideal $\wp$ von g_p festgehalten, wie in der Definition von G_{-1} gefordert.
Als nächsten Spezialfall sei $m = p^\alpha$. Nach Satz 5.8 gilt

$$e_{K_m/\mathbb{Q}}(\wp) = \varphi(p^\alpha) = [K_m : \mathbb{Q}], \qquad f_{K_m/\mathbb{Q}}(\wp) = 1 \tag{5.33}$$

Aus dem Beweis von Satz 5.3 $|G_{-1}| = e_{K_m/\mathbb{Q}}(\wp)$, zusammen mit (5.33) also $|G_{-1}| = [K_m : \mathbb{Q}]$. Es muss sich also um die volle Galoisgruppe handeln.
Wir führen den allgemeinen Fall auf die bereits behandelten zurück, indem wir K_m als Zusammensetzung $K_m = K_{p^\alpha} K_{m_1}$ schreiben. Zur vereinfachten Schreibweise sei $M := K_{p^\alpha}, L := K_{m_1}$. Man kann nach dem Struktursatz für Kreisteilungskörper

$$G(K_m/\mathbb{Q}) = G(L/\mathbb{Q}) \oplus G(M/\mathbb{Q}) \Longleftrightarrow G(m) = G(m_1) \oplus G(p^\alpha)$$

schreiben. Wir betten nun die direkten Summanden in K_m ein, indem wir $G(L/\mathbb{Q})$ als die Untergruppe von $G(m)$ identifizieren, die M festhält und umgekehrt. Um G_{-1} zu bestimmen, seien $P_1 \triangleleft O_K$ und $P_2 \triangleleft O_L$ die Primideale die unter $\wp$ liegen. Sei weiter $g \in G_{-1}(\wp)$ beliebig. Bezeichne zu diesem g mit g_1, g_2 die Einschränkungen auf $G(L/\mathbb{Q})$ wobei M trivial abgebildet (fixiert) wird wieder zurückgehoben

auf einen Automorphismus von K_m, sowie auf $G(M/\mathbb{Q})$ wobei L trivial abgebildet (fixiert) wird wieder zurückgehoben auf einen Automorphismus von K_m respective, sodass also g praktisch von $g_1 \in G(L/\mathbb{Q}), g_2 \in G(M/\mathbb{Q})$ durch Hintereinanaderausführung erzeugt wird. $g_i(P_i)$ sind nach Konstruktion konjugiert zum Primideal P_i und wegen $g_i(P_i)O_{K_m} \subset g(\wp) = \wp$ mit letzterer Gleichheit weil $g \in G_{-1}(\wp)$ folgt

$$g(P_i) = P_i \Longrightarrow g_i \in G_{-1}(P_i)$$

Damit haben wir $G_{-1}(\wp) \subset G_{-1}(P_1) \oplus G_{-1}(P_2)$ nachgerechnet.
Sind umgekehrt $g_i \in G_{-1}(P_i)$ muss für die Hintereinanderausführung g von g_1, g_2 einmal $g(\wp) = \wp$ sein, andernfalls würde $g(\wp) = Q \neq \wp$ zu $g_1(P_1) = g(P_1) \subset Q$ führen da $P_1 \subset \wp$, dies wiederum heißt $\wp \cdot Q | P_1 O_{K_m}$ im Sinne eines echten Teilers. Das widerspricht Satz 5.8, da in der Zerlegung von pO_K niemals Primideale mit Vielfachheit größer eins auftreten. Insgesamt haben wir

$$G_{-1}(\wp) = G_{-1}(P_1) \oplus G_{-1}(P_2) = G_{-1}(P_1) \oplus G(M/\mathbb{Q}).$$

Dieses Ergebnis ist aber nur eine Umformulierung der Aussage über G_{-1} wie sie in der Formulierung des Lemmas steht.

2. Für Punkt 2 sei wieder an die Aussage aus Lemma 5.10 erinnert, dass der zu G_0 korrespondierende Körper $FIX(G_0)$ der maximale Teilkörper von K_m mit unverzweigtem p ist. Das ist aber andererseits unser $K_{m_1} = L$. Aus Satz 5.8 folgt außerdem, dass p unverzweigt in $L/\mathbb{Q}$ ist sowie

$$[K_m : L] = \varphi(p^\alpha) = e_{K_m/L}(\wp)$$

und wegen der Standardidentität von Lemma 5.3 gewinnen wir $f_{K_m/L}(\wp) = 1$. Also verzweigt p in jedem $\mathbb{Q} \subset L \subset K_m$, woraus wir erschließen, dass G_0 die Galoisgruppe $Gal(K_m/L)$ ist. Diese kann mit

$$\{r : g_r(\zeta_{m_1}) = \zeta_{m_1}\}$$

identifiziert werden. Wegen der Identität $\zeta_{m_1} = \zeta_m^p$ und weil g_r Homomorphismus ist gilt demnach $g_r(\zeta_{m_1}) = \zeta_m^{rp}$. Damit ζ_{m_1} von g_r fixiert wird wie wir es wollen, muss in Folge $rp \equiv p \pmod{m}$ gelten, woraus man leicht $r \equiv 1 \pmod{m_1}$ ersieht. Ein Blick auf die Definition von G_0 zeigt, dass der zweite Punkt damit ebenfalls bewiesen ist.

3. Die Aussage über G_1 ist unmittelbar aus Lemma 5.10 ersichtlich. □

Sei im kommenden Satz $H = fix(K) \subset G(K_m/\mathbb{Q}) \cong G(m)$ die Automorphismenuntergruppe die $K \subset K_m$ fixiert, wobei $G(m)$ wieder die prime Restklassengruppe modulo m mit Multiplikation ist.

Satz 5.14. Sei K abelscher Zahlkörper vom Grad $[K/\mathbb{Q}] = n$ und $K_m \supset K$ beliebiger Kreisteilungskörper der K enthält. Dann gilt für Primzahlen $p \in \mathbb{Z}$

$$p \cdot O_K = (\wp_1 \wp_2 \dots \wp_g)^e, \qquad f_{K/\mathbb{Q}}(\wp_i) = f$$

mit

1. Falls $p \nmid m \quad \Longrightarrow \quad e = 1$, f... Ordnung von p in $G(m)/H$, $g = \frac{n}{ef}$
2. Falls $p = p^a m_1$, $p \nmid m_1 \quad \Longrightarrow \quad e = \frac{\varphi(p^a)}{N}, \quad f = FNN_1, \quad g = \frac{n}{ef}$
   mit
   $N = \sharp\{x \pmod m \in H : \quad x \equiv 1 \pmod{m_1}\}$
   N_1... Zahl der Restklassen $x \pmod m \in H$ für die $x \pmod{m_1}$ in der zyklischen von $p \pmod{m_1}$ erzeugten Untergruppe von $G(m_1)$ liegt und
   F... Ordnung von $p \pmod{m_1}$ in $G(m_1)$.

Beweis: Vorangehendes Lemma beschreibt die Gruppen G_i für den Fall eines Kreisteilungskörpers K_m/Q. Die entsprechende Aussage für unsere Situation einer beliebigen abelschen Erweiterung $K/\mathbb{Q}$ mit $\mathbb{Q} \subset K \subset K_m$ ist nun einfach die Anwendung von Korollar 5.8, Punkt 2 indem man diverse naheliegende Identifikationen vornimmt, etwa dass die $\wp_i$ genau die Primideale sind die über p liegen. □

Sei weiterhin K abelscher Zahlkörper mit $\mathbb{Q} \subset K \subset K_m$ und $H = fix(K) \subset G(m)$ und sei weiters $X(K) \subset 2^{G(m)}$ die Gruppe der Dirichletcharaktere, die auf H konstant den Wert 1 annehmen. Indem man ein Element aus $X(K)$ zu einem Dirichletcharakter auf $G(m)$ fortsetzt kann man wie im Kapitel 5.1 Bewertungen und L-Reihen ausgeführt den induzierten primitiven Dirchletcharakter betrachten, wir wollen ihn mit χ' bezeichnen. Weiters erinnern wir an die Definition des Führers eines Dirchletcharakters, wir werden ihn im kommenden Satz mit $f(\chi)$ bezeichnen.
Im Beweis des folgenden Satzes, der endgültig die Brücke von der Zetafunktion zu den L-Reihen darstellt und die Klassenzahlformel für abelsche Zahlkörper impliziert, werden wir die Tatsache verwenden, dass für zwei Teilkörper K,L eines Kreisteilungskörpers K_m die Beziehung

$$X(K) \cap X(L) = X(K \cap L) \tag{5.34}$$

zutreffend ist. Dies ist unmittelbare Folge des Hauptsatzes der Galoistheorie, der die Untergruppen der Charaktergruppe von $Gal(K_m/\mathbb{Q}) \cong G(m)$ und die Zwischenkörper $\mathbb{Q} \subset K \subset K_m$ in eine 1:1 Beziehung setzt.

Satz 5.15. Für einen abelschen Zahlkörper gilt

$$\zeta_K(s) = \prod_{\chi \in X(K)} L(s, \chi') \tag{5.35}$$

Beweis: Wegen des Identitätssatzes aus der Funktionentheorie ist es hinreichend, die Gleichheit auf der Halbebene $\mathrm{Re}(s) > 1$ nachzurechnen. Dort haben wir für die Zetafunktion die Produktdarstellung zur Verfügung, die man offensichtlich aufspalten kann in der Form

$$\zeta_K(s) = \prod_p \prod_{P_p} (1 - N(P)^{-s})^{-1}$$

wobei die Schreibweise P_p die Primideale P bezeichnet die unter p liegen.
Ähnlich haben wir auf $\mathrm{Re}(s) > 1$ auf der linken Seite

$$L(s, \chi') = \prod_p (1 - \chi'(p) p^{-s})^{-1}$$

wobei χ' durch $\chi'(p) = 0$ für $p|f(\chi)$ fortgesetzt wird. Könnte man nun

$$\prod_{P_p}(1 - N(P)^{-s}) = \prod_{\chi}(1 - \chi'(p)p^{-s}) \tag{5.36}$$

für alle Primzahlen $p \in \mathbb{Z}$ beweisen, so folgt (5.35) einfach durch vertauschen der Produktreihenfolge

$$\prod_{\chi \in X(K)} L(s, \chi') = \prod_{p}\prod_{\chi}(1 - \chi'(p)p^{-s}) = \prod_{\chi}\prod_{p}(1 - \chi'(p)p^{-s})$$

was wegen der absoluten Konvergenz gerechtfertigt ist. Es bleibt (5.36) zu zeigen. Schreibt man

$$p \cdot O_K = (\wp_1\wp_2 \dots \wp_g)^e, \qquad f = f_{K/\mathbb{Q}}(\wp_i) \qquad \forall i = 1, 2, \dots, n$$

so kann man die linke Seite von (5.36) durch $(1 - p^{-fs})^{-g}$ ausdrücken. Wir wollen die rechte Seite in selbigen Ausdruck überführen um den Satz zu beweisen. Sei vorerst $p \nmid m$ und in Folge $e = 1$, wobei zur Erinnerung m durch $K \subset K_m$ bestimmt ist. Satz 5.14 ermöglicht für $\chi \in X(K)$ wegen $\chi' = 1$ auf H den Schluss

$$\chi'(p)^f = \chi'(p^f) = \chi'(1) = 1 \quad \Longrightarrow \quad \chi'(p) = \zeta_f^{K(p)}, \quad 0 \neq K(p) \in \mathbb{N}$$

mit $\zeta_f = e^{\frac{2\pi i}{f}}$ wie immer. Eine entscheidende Beobachtung ist nun: Für die Charaktere auf $G(m)/H$ die identisch eins auf der von $p \pmod m$ erzeugten Klasse sind- bezeichne sie mit T- ist die Teilmenge, die bei p eine *vorgegebene* f-te Einheitswurzel annimmt eine Nebenklasse von T in der Menge aller Charaktere von G/H. Da diese Nebenklassen alle gleichmächtig sind haben sie jeweils $\frac{|G/H|}{f} = g$ Elemente und es gilt die Identität

$$1 - \chi'(p)p^{-s} = \prod_{j=0}^{f}(1 - \zeta_f^j \cdot p^{-s})^g.$$

Indem wir die einfach nachzurechnende Identiität

$$\prod_{j=0}^{f}(1 - \zeta_f^j x) = 1 - x^f$$

für $x = p^{-s}$ verwenden ergibt sich

$$\prod_{j=0}^{f}(1 - \zeta_f^j p^{-s}) = 1 - p^{-fs}$$

und schließlich mit

$$\prod_{\chi}(1 - \chi'(p)p^{-s}) = (1 - p^{-fs})^g$$

das Gewüschte. Im anderen Fall $p|m$ schreibe wie in Lemma 5.11 $m = p^\alpha m_1, p \nmid m_1$. Nach Proposition 5.15 ist $L = K \cap K_{m_1}$ der größte Unterkörper von K in dem p unverzweigt ist und mit Lemma 5.10 gilt weiter für alle $P \triangleleft O_L$ über p, dass

$$f_{L/\mathbb{Q}}(P) = f, \quad g_{L/\mathbb{Q}}(P) = g \tag{5.37}$$

Nach Definition impliziert $p|f(\chi)$ dass $\chi'(p) = 0$, weshalb man auf der linken Seite von (5.36) viele Faktoren streichen kann. Sie wird zu

$$\prod_{\chi \in X(K)} (1 - \chi'(p)p^{-s}) = \prod_{\chi \in X(K), f(\chi)|m_1} (1 - \chi'(p)p^{-s}) \tag{5.38}$$

Eine andere Interpretation von $f(\chi)|m_1$ ist

$$f(\chi)|m_1 \Longleftrightarrow \chi \in X(K_{m_1})$$

also wird auf der rechten Seite von (5.38) wegen (5.34) genau über $\chi \in X(L)$ das Produkt erstreckt. Folglich

$$\prod_{\chi \in X(K)} (1 - \chi'(p)p^{-s}) = \prod_{\chi \in X(L)} (1 - \chi'(p)p^{-s})$$

Wegen $p \nmid m_1$ können wir die Ergebnisse des Falls $p \nmid m$ hier für L anwenden um

$$\prod_{\chi \in X(K)} (1 - \chi'(p)p^{-s}) = (1 - p^{-f's})^{g'}, \qquad f' := f_{L/\mathbb{Q}}(P), g' := g_{L/\mathbb{Q}}(P)$$

zu erhalten. Die Behauptung folgt aus (5.37). □

Jetzt können wir die Klassenzahlformel für abelsche Zahlkörper anschreiben als

Satz 5.16.

$$h(K) = \frac{\sqrt{|d(K)|}\omega(K)}{2^s(2\pi)^t R_K} \cdot \prod_{\chi \in X(K), \chi \neq 1} L(1, \chi') \tag{5.39}$$

Beweis: Formt man die Gleichung (4.1) aus Satz 4.1 nach $h(K)$ um und verwendet die Formel (5.35), so reicht es $L(s, \chi'_0) = \zeta(s)$ für den Hauptcharakter χ_0 über den das Produkt nicht erstreckt wird zu bemerken, da die riemannsche Zetafunktion einen Pol mit Residuum 1 an der Stelle $s = 1$ besitzt. □

Wir geben nun noch einige Varianten für Spezifizierungen an:

Satz 5.17. Für reelle Zahlkörper $K \subset \mathbb{R}$ vom Grad n gilt

$$h(K) = \frac{\sqrt{|d(K)|}}{2^{n-1} R_K} \prod_{\chi \in X(K), \chi \neq 1} L(1, \chi') \tag{5.40}$$

Beweis: Abelsche Klassenzahlformel (5.39) für die Signatur $(s, t) = (n, 0)$ unter Berücksichtigung, dass die Einheitswurzelgruppe im reellen Fall nur aus $\{1, -1\}$ besteht und daher $\omega(K) = 2$ gilt. □

Ganz ähnlich folgt

Satz 5.18. Für imaginäre Zahlkörper K vom Grad n mit Sigantur (s,t) gilt

$$h(K) = \frac{\sqrt{|d(K)|}\omega(K)}{(2\pi)^t R_K} \prod_{\chi \in X(K), \chi \neq 1} L(1, \chi')$$

Beachte, dass im Falle quadratischer Zahlkörper- also bei $n = [K : \mathbb{Q}] = 2$- einer der beiden obigen Fälle auftritt.
Ein Hauptproblem ist offenbar die Auswertung der L-Reihen an der Stelle $s = 1$. Wie man dabei vorgehen kann sei abschließend noch angedeutet.

5.9 Auswertung der L-Reihen

Bezeichne hier $f = f(K)$ den Führer eines Zahlkörpers K aus Beginn des Abschnitts 5.8 und im weiteren $\zeta = \zeta_f = e^{\frac{2\pi i}{f}}$. Weiter sei als

$$\sum_{x \bmod f}$$

die *Summe über ein primes Restklassensystem* $x \pmod f$ zu verstehen, das bedeutet es wird über alle zu f teilerfremden Restklassen x summiert. Aufgrund der Periodizizät der L-Reihen in denen diese Summen auftreten wird diese Schreibweise wo verwendet wohldefiniert sein.
Zunächst gilt für $\mathrm{Re}(s) > 1$:

$$L(s,\chi) = \sum_{m=1}^{\infty} \frac{\chi(m)}{m^s} = \sum_{z \bmod f} \chi(z) \sum_{n \equiv z \bmod f, n \geq 1} \frac{1}{n^s} =$$

$$\sum_{z \bmod f} \chi(z) \sum_{n=1}^{\infty} \frac{1}{n^s} \frac{1}{f} \sum_{x \bmod f} \zeta^{(z-n)x} = \frac{1}{f} \sum_{x \bmod f} \sum_{z \bmod f} \chi(z) \zeta^{zx} \sum_{n=1}^{\infty} \frac{\zeta^{-nx}}{n^s}$$

Mit dem abelschen Stetigkeitssatz für Dirichletsche Reihen kann man auf $s = 1$ übergehen und mithilfe der Potenzreihe des Logarithmus:

$$L(1,\chi) = -\frac{1}{f} \sum_{x \bmod f} \tau_x(\chi) \cdot \log(1 - \zeta^{-x}) = -\frac{\tau(\chi)}{f} \sum_{x \bmod f} \overline{\chi}(x) \cdot \log(1 - \zeta^{-x}) \quad (5.41)$$

wobei

$$\tau_x(\chi) := \sum_{z \bmod f} \chi(z) \zeta^{zx}$$

sowie

$$\tau(\chi) := \sum_{x \bmod f(\chi)} \chi(x) \zeta_{f(\chi)}^{x}$$

und der elementare Zusammenhang $\tau_x(\chi) = \overline{\chi}(x)\tau(\chi)$ in der letzten Identität von (5.41) verwendet wurde.
Die Summe auf der rechten Seite von (5.41) nennen wir $S(\chi)$ und zielen darauf ab sie zu berechnen. Zunächst bearbeiten wir sie weiter zu

$$S(\chi) = \sum_{x \bmod f} \chi(x) \cdot \log(1-\zeta^x) = \frac{1}{2} \sum_{x \bmod f} \chi(x) \cdot [\log(1-\zeta^{-x}) + \chi(-1) \cdot \log(1-\zeta^x)]$$

Wir betrachten nun die Fälle $\chi(-1) = 1$ und $\chi(-1) = -1$ separat. (Beachte, dass wegen $\chi(-1)^2 = \chi((-1)^2) = \chi(1) = 1$ damit alle Fälle abgedeckt sind.)

1. $\chi(-1) = 1$

$$S(\chi) = \frac{1}{2} \sum_{x \bmod f} \chi(x)[\log(1-\zeta^{-x}) + \log(1-\zeta^x)] = \frac{1}{2} \sum_{x \bmod f} \chi(x) \cdot \log|1-\zeta^x|^2$$

$$= \sum_{x \bmod f} \chi(x) \cdot \log|1-\zeta^x| = 2 \sum_{\pm x \bmod f} \chi(x) \cdot \log|1-\zeta^x|$$

wobei

$$\sum_{\pm x \bmod f}$$

die *Summe über ein Halbsystem der primen Restklassen* $(\bmod f)$ andeutet, also derart, dass die Menge $\{\pm x \pmod f\}$ alle primen Restklassen $(\bmod f)$ abdeckt. Also

$$S(\chi) = 2 \sum_{\pm x \bmod f} \chi(x) \cdot \log|1-\zeta^x| \tag{5.42}$$

Nach erneutem kurzem Blick auf (5.41) zusammen mit der Formel für $S(\chi)$ aus (5.42) vermerken wir als Resultat für den ersten Fall

$$L(1,\chi) = 2\frac{\tau(\chi)}{f(\chi)} \sum_{\pm x \bmod f} (-\chi(x) \cdot \log|1-\zeta_{f(\chi)}^x|) \tag{5.43}$$

2. $\chi(-1) = -1$
Man berechnet

$$1-\zeta^x = 1-e^{\frac{2\pi i x}{f}} = (e^{-\frac{\pi i x}{f}} - e^{\frac{\pi i x}{f}})e^{\frac{\pi i x}{f}} = -2i \cdot \sin\frac{\pi x}{f} \cdot e^{\frac{\pi i x}{f}}$$

$$= 2\sin\frac{\pi x}{f} \cdot e^{\pi i(\frac{x}{f}-\frac{1}{2})},$$

$$1-\zeta^{-x} = 1-e^{-\frac{2\pi i x}{f}} = (e^{\frac{\pi i x}{f}} - e^{-\frac{\pi i x}{f}})e^{-\frac{\pi i x}{f}} = 2i \cdot \sin\frac{\pi x}{f} \cdot e^{-\frac{\pi i x}{f}}$$

$$= 2\sin\frac{\pi x}{f} \cdot e^{-\pi i(\frac{x}{f}-\frac{1}{2})}$$

Fixiert man nun das *kleinste positive Restsystem* $(\mathrm{mod}\ f)$, also genau die zu f teilerfremden ganzen Zahlen $0 < x < f$ und bezeichnet es mit

$$\sum_{x \bmod f}^{+}$$

dann gilt

$$2\sin\frac{\pi x}{f} > 0, \qquad |\frac{x}{f} - \frac{1}{2}| < \frac{1}{2}$$

sodass also $2\sin\frac{\pi x}{f} = |\log(1-\zeta^{\pm x})|$ sowie die Imaginärteile $\pm\pi i(\frac{x}{f} - \frac{1}{2})$ im Bereich $[-\pi i, \pi i]$ liegen. In diesem Fall kann man die Darstellung

$$S(\chi) = \frac{1}{2}\sum_{x \bmod f} \chi(x)[\log(1-\zeta^{-x}) - \log(1-\zeta^{x})] = -\pi i \sum_{x \bmod f}^{+} \chi(x)(\frac{x}{f} - \frac{1}{2})$$

$$= \frac{\pi}{i}\frac{1}{f}\sum_{x \bmod f}^{+} \chi(x)x,$$

ableiten, und in Folge von (5.41) vermerken wir

$$L(1,\chi) = \frac{\pi}{i}\cdot\frac{\tau(\chi)}{f(\chi)}\cdot\frac{1}{f(\chi)}\sum_{x \bmod f(\chi)}^{+}(-\overline{\chi}(x)x) \tag{5.44}$$

als Ergebnis für den zweiten Fall.

Über die Funktionalgleichungen der Zetafunktionen ζ_K und L-Reihen, welche hier nur erwähnt seien, kann man relativ einfach

$$\prod_{\chi} f(\chi) = d \tag{5.45}$$

$$\prod_{\chi}\tau(\chi) = \sqrt{\prod_{\chi} f(\chi)} = \sqrt{d}, \qquad K \subset \mathbb{R} \tag{5.46}$$

$$\prod_{\chi}\tau(\chi) = i^t\sqrt{\prod_{\chi} f(\chi)} = i^t\sqrt{d}, \qquad K \subset \mathbb{C} \tag{5.47}$$

erhalten, siehe [Ha1]. Wir fügen dieses Wissen zu den Gleichungen (5.43), (5.44):

$$h(K) = \frac{\prod_{\chi\neq 1}\sum_{\pm x \bmod f(\chi)}(-\chi(x)\cdot\log|1-\zeta^{x}_{f(\chi)}|)}{R_K}, \qquad K \subset \mathbb{R} \tag{5.48}$$

ergibt sich aus (5.39) von Satz 5.16 und den Gleichungen (5.43), (5.45), (5.46) für reelle Zahlkörper $K \subset \mathbb{R}$, sowie

$$h(K) = \frac{\prod_{\chi_0 \neq 1} \sum_{\pm x \bmod f(\chi_0)} (-\chi_0(x) \cdot \log|1 - \zeta_{f(\chi_0)}^x|) \cdot \frac{\omega}{2} \prod_{\chi_1} \frac{1}{f(\chi_1)} \sum_{x \bmod f(\chi_1)}^{+} (-\chi_1(x)x)}{R_K}, \tag{5.49}$$

$$K \subset \mathbb{C}$$

für imaginäres K über (5.40) aus Satz 5.17 und den Gleichungen (5.44), (5.45), (5.47), wobei mit χ_0 die Charaktere mit $\chi_0(-1) = 1$ und mit χ_1 jene mit $\chi_1(-1) = -1$ gemeint sind.
Dabei folgt (5.48) auch direkt aus (5.49) indem man $\omega(K) = 2$ setzt und erkennt, dass das zweite Produkt auf der rechten Seite von (5.49) das leere Produkt, also eins ist.

Sei nun weiter K_0 definiert als *der größte reelle Teilkörper* $\mathbb{Q} \subset K_0 \subset K$ von K. Man beachte, dass aus dem Satz von Kronecker-Weber folgt, dass $[K : K_0] = 2$, denn K_0 ist der Fixpunktkörper unter der komplexen Konjugation $\zeta_f \mapsto \overline{\zeta_f}$. Der Einheitenrang aus dem Dirichletschen Einheitensatz Satz 1.7 ist für beide Körper K, K_0 gleich $(t-1)$, und über die Definition des Regulators folgt relativ leicht, dass

$$Q := \frac{2^{t-1} R_{K_0}}{R_K} \in \mathbb{Z}$$

der Index der Untergruppe der Einheiten aus K_0 und ihrer Produkte mit Einheitswurzeln aus K- also das Erzeugnis von $E(K_0) \cup T$ mit T der Einheitswurzelgruppe von K und $E(K_0)$ der Einheitengruppe in K_0- in der Einheitengruppe von K ist. Q heißt auch *Einheitenindex* von K/K_0. Der reine Einheitenindex von K_0 in K wäre im übrigen $Q \cdot \frac{\omega}{2}$.
(5.49) wird durch diese Feststellungen zu

$$h(K) = \frac{\prod_{\chi \neq 1} \sum_{\pm x \bmod f(\chi_0)} (-\chi_0(x) \log|1 - \zeta_{f(\chi_0)}|)}{R_{K_0}} \cdot Q\omega \prod_{\chi_1} \frac{1}{2f(\chi_1)} \sum_{\pm x \bmod f(\chi_1)}^{+} (-\chi_1(x)x)$$

Dabei bezeichnet

χ ... die Charaktere von K, aufgefasst als Charaktere nach der K zugeordneten Kongruenzgruppe H vom Führer f,
χ_0 ... die Charaktere des größten reellen Teilkörpers K_0 von K $\quad (\chi_0(-1) = 1)$,
χ_1 ... die Charaktere von K/K_0 $\quad (\chi_1(-1) = -1)$,
f(χ) ... ihre Führer,
$\sum_{\pm x \bmod f(\chi)}$ ... die Summation über ein primes Halbsystem mod $f(\chi)$,
$\sum_{x \bmod f(\chi)}^{+}$ ... Summation über das kleinste positive Restsystem mod $f(\chi)$,
$\zeta_{f(\chi)} = e^{\frac{2\pi i}{f(\chi)}}$,
R_{K_0} ... den Regulator von K_0,
Q ... den Einheitenindex von K/K_0,
$\omega(K)$ ... die Anzahl der Einheitswurzeln von K

Literaturverzeichnis

[Hu1] Thomas W. Hungerford: *Algebra*. Seattle, Washington: Springer (1980).

[Fi1] Gerd Fischer: *Lehrbuch der Algebra*. München: Vieweg (2008).

[Mi1] J.S. Milne: *Algebraic Number Theory*. www.jmilne.org/math/ (2009).

[Ste05] W.A. Stein: *Introduction to algebraic number theory*. www.sheffield.ac.uk/ pm1afj/courses/zeta/zeta_k1.ps (2005).

[Si05] Gary Sivek: *The analytic class number formula*. http://modular.fas.harvard.edu/129-05/final_papers/Gary_Sivek.pdf (2005).

[Art32a] Emil Artin: *Über die Bewertungen algebraischer Zahlkörper*. Journal für die reine und angewandte Mathematik, 167:157159, (1932) de Gruyter Verlag.

[Na74] Wladyslav Narkiewicz: *Elementary and analytic theory of algebraic numbers*. Warschau, Springer (1974)

[BS66] Borevich, Shafarevich: *Number Theory*. New York : Academic Press, [1966].

[Ahl79] L.V. Ahlfors: *Complex Analysis*. McGraw-Hill, Inc., (1979).

[Za1] Don B. Zagier: *Zetafunktionen und quadratische Zahlkörper*. Berlin [u.a.], Springer (1981)

[Co91] Cohn P.M.: *Algebraic numbers and algebraic functions*. London [u.a.], Chapman Hall/CRC Mathematics Series (1991).

[Ha1] Helmut Hasse: *Über die Klassenzahl abelscher Zahlkörper*. Berlin, Akademie-Verlag Berlin (1952)

[Ge08] Ernst-Ulrich Gekeler: Algebraische Zahlentheorie. http://www.math.uni-sb.de/ag/gekeler/LEHRE/AZT0809/algZ_Kapitel01.pdf, Saarland (2008)