ALGEBRAISCHE ZAHLENTHEORIE

1. Teilbarkeitslehre in kommutativen Ringen

Definition: Sei $(R,+,\cdot)$ ein Ring. (d.h. $(R,+)$ ist kommutative Gruppe $(R,.)$ ist Halbgruppe und es gelten beideDistributivgesetze)

*R heißt **kommutativer Ring**, falls $(R,\cdot)$ kommutativ ist.*
*R heißt **Ring mit 1**, falls $(R,\cdot)$ ein Einselement $1\neq 0$ besitzt.*
*Ein Element $a\in R$ heißt **Nullteiler**, falls es ein $b\neq 0$ gibt, so daß $a\cdot b=0$ oder $b\cdot a=0$ gilt.*
*Ein kommutativer Ring mit 1, der keine von 0 verschiedene Nullteiler besitzt, heißt **Integritätsring** oder **Integritätsbereich**.*

*Definition: Sei $(R,+,\cdot)$ ein Ring. Ein Unterring $I\subseteq R$ heißt **Ideal**, falls für alle $a\in R$ $a\cdot I\subseteq I$ und $I\cdot a\subseteq I$ gilt.*
*Die Ideale $I=\{0\}$ und $I=R$ heißen **triviale Ideale.***
*Ein Ideal heißt **maximal**, falls $I\neq R$ ist und es kein Ideal J mit $I\subset J\subset R$ gibt.($\Leftrightarrow$ R/I Körper)*
*Ein Ideal I heißt **Primideal**, falls aus $a\cdot b\in I$ entweder $a\in I$ oder $b\in I$ folgt.*
*Ein Ideal der Form $I=aR=(a)$ (in einem kommutativen Ring) heißt **Hauptideal**.*
*Ein kommutativer Ring mit 1, der nur Hauptideale als Ideale besitzt, heißt **Hauptidealring**.*

*Zwei Elemente $a, b\in R$ heißen **kongruent modulo einem Ideal I**, i.Z. $a\equiv b \pmod I$, falls $a-b\in I$ ist. (Ist $I=(c)$ ein Hauptideal, so schreibt man auch $a\equiv b(c)$ oder $a\equiv b \pmod c$)*
*Die Relation $\equiv$ induziert eine Äquivalenzrelation, die mit + und . verträglich ist (Kongruenzrelation). Sind $[a]_I$, $[b]_I$ zwei Äquivalenzklassen, die die Elemente a bzw. b enthalten, so definiert man $[a]_I+[b]_I=[a+b]_I$ und $[a]_I\cdot[b]_I=[a\cdot b]_I$. Die entstehende Struktur $(R/I,+,\cdot)$ ist wieder ein Ring, der sogenannte **Faktorring**.*

*Definition: Sei $(R,+,\cdot)$ ein Integritätsring. Man sagt **a teilt b**, i.Z. **$a \mid b$**, falls es ein c mit $a\cdot c=b$ gibt, d.h. $b\in(a)$ oder $a\equiv 0$ (b). a heißt **Einheit**, falls $a \mid 1$.(**R^*** bezeichne die Menge der Einheiten) $a\neq 0$ heißt **irreduzibel**, falls aus $a=b\cdot c$ entweder $b\in R^*$ oder $a\in R^*$ folgt. $a\neq 0$ heißt **prim (Primelement)**, falls aus $a\mid b\cdot c$ entweder $a\mid b$ oder $a\mid c$ folgt.*

Satz: Sei $(R,+,\cdot)$ ein Integritätsbereich.
(I) Ein Ideal I ist maximal $\Leftrightarrow$ R/I ist ein Körper
(II) Ein Ideal I ist Primideal $\Leftrightarrow$ R/I ist ein Integritätsring
(III) Jedes maximale Ideal ist auch Primideal.
(IV) In einem Hauptidealring ist jedes Primideal $\neq\{0\}$ maximal.
(V) $(R^*,\cdot)$ bildet eine Gruppe, die sogenannte Einheitengruppe.
(VI) Jedes Primelement ist irreduzibel.

Definition: Sei $(R,+,\cdot)$ ein Integritätsbereich.
*d heißt **größter gemeinsamer Teiler von a und b**, i.Z. $d=ggT(a,b)=(a,b)$, falls $d \mid a$ und $d \mid b$ und für jeden gemeinsamen Teiler $t \mid a$, $t \mid b$ auch $t \mid d$ gilt.*
*R heißt **Ring mit ggT**, falls alle Paare $a, b\in R$ einen ggT haben.*

*Man sagt, R erfüllt die **endliche Teilerkettenbedingung**, falls für jede unendliche Folge $a_1, a_2, a_3, \ldots \in R$ mit $a_{i+1} \mid a_i$ $(i>0)$ ein $n\in N$ existiert, so daß für alle $k\geq n$ $a_k=\varepsilon_k a_n$ für ein $\varepsilon_k\in R^*$ gilt.*

*R heißt **faktorieller Ring** (oder **ZPE-Ring**), wenn jedes $a \in R\setminus(R^* \cup \{0\})$ als Produkt irreduzibler Elemente von R darstellbar ist und für zwei Darstellungen $a = q_1 \dots q_r = q'_1 \dots q'_s$ immer $r=s$ gibt und für eine Permutation π auf $\{1,..,r\}$ $q_i = \varepsilon_i q_{\pi(i)}$ (mit $\varepsilon_i \in R^*$) gilt. R heißt **euklidischer Ring**, wenn es eine Gradfunktion δ: $R\setminus\{0\} \to \{0,1,2,..\}$ gibt, so daß für alle $a, b \in R$, $b \neq 0$, stets Elemente $q,r \in R$ existieren, für welche $a = b \cdot q + r$ gilt, wobei entweder $r=0$ oder $\delta(r) < \delta(b)$ ist.*

Satz: Sei (R,+, ·) ein Integritätsbereich.

(I) Ein Hauptideal (a) ist Primideal ⇔ a=0 oder a ist Primelement
(II) Ist R ein Ring mit ggT, so ist jedes irreduzible Element prim.
(III) R faktoriell ⇔ R ist Ring mit ggT und erfüllt die endliche Teilerkettenbedingung.
(IV) Jeder euklidische Ring ist Hauptidealring
(V) Jeder Hauptidealring ist faktoriell.

Bemerkung: Es gibt faktorielle Ringe, die keine Hauptidealringe sind, und es gibt Hauptidealringe, die keine euklidischen Ringe sind.

2. Endliche Körpererweiterungen

*Definition: Ein Ring (K,+,·) heißt **Körper**, falls (K\{0},·) eine abelsche Gruppe ist.*
*Definition: Seien L, K zwei Körper mit $K \subseteq L$, d.h. L ist ein **Erweiterungskörper**. Dann kann L als Vektorraum über K aufgefaßt werden. Die Erweiterung L/K heißt **endlich**, falls die Dimension des Vektorraums L über K endlich ist. Die Dimension heißt **Erweiterungsgrad [L:K].***

Satz: Seien L/K und E/L endliche Körpererweiterungen. Dann ist auch E/K endlich und es gilt

$$[E:K]=[E:L].[L:K].$$

*Definition: Sei R ein kommutativer Ring. Dann bezeichnet man mit **R[x]** die Menge der Polynome $f(x)=a_n x^n + a_{n-1} x^{n-1} + \dots a_1 x + a_0$ $(a_0, a_1, \dots a_n \in R)$ in der Unbestimmten x. **(Polynomring)** Ist $a_n = 1$, so heißt f(x) **normiert**.*

Satz: Sei K ein Körper. Dann ist K[x] ein euklidischer Ring, also ein ZPE-Ring.

Bemerkung: Ist R ein ZPE-Ring, so auch R[x].
Dies folgt aus der Betrachtung des Quotientenkörpers K von R und dem Gaußschen Lemma. Für Hauptidealringe gilt diese Eigenschaft i.a. nicht: z.B. ist K[x] Hauptidealring, aber K[x, y]=K[x][y] kein Hauptidealring, da das von x.y erzeugte Ideal kein Hauptideal sein kann.

*Definition: Sei L/K eine Körpererweiterung. $\alpha \in L$ heißt **algebraisch über K**, falls es ein Polynom $f(x) \in K[x]$ mit $f(\alpha)=0$ gibt. Ist jedes $\alpha \in L$ algebraisch, so heißt die Körpererweiterung **algebraisch**. Sei α algebraisch über K. Dann heißt jenes Polynom mit minimalem Grad (von dem man o.B.d.A. annehmen kann, daß es normiert ist.), das α als Nullstelle hat, **Minimalpolynom $m_\alpha(x)$**. Dieses ist eindeutig bestimmt und irreduzibel.*

Satz: Sei α algebraisch über K und bezeichne $K(\alpha)$ den kleinsten Unterkörper von L, der α enthält. Dann gilt $K(\alpha)=K[\alpha]$ und $K(\alpha)/K$ ist endlich. Insbesondere ist der Erweiterungsgrad $[K(\alpha):K]$ gleich dem Grad des Minimalpolynoms $m_\alpha(x)$.

Satz: Jede endliche Körpererweiterung L/K ist algebraisch.

Definition: Eine Körpererweiterung L/K heißt ***endlich erzeugt****, falls es* $\alpha_1, \ldots \alpha_m \in L$ *mit* $K(\alpha_1, \ldots \alpha_m)=L$ *gibt. Sie heißt* ***einfach****, falls es ein* $\alpha \in L$ *mit* $K(\alpha)=L$ *gibt. So ein* α *heißt auch* ***primitives Element****.*

Bemerkung: Jede endliche Körpererweiterung L/K ist endlich erzeugt.

Definition: Ein Körper E heißt ***algebraisch abgeschlossen****, falls jedes Polynom* $f(x) \in E[x]$ *eine Nullstelle* $\alpha \in E$ *besitzt.*

Satz: Jeder Körper K besitzt einen algebraisch abgeschlossenen Erweiterungskörper E, der algebraisch über K ist. So ein Körper heißt **algebraischer Abschluß** $\overline{K}$. Der algebraische Abschluß ist bis auf Isomorphie eindeutig bestimmt. Sind E und E′ zwei algebraisch abgeschlossen algebraische Erweiterungen von K, so gibt es einen Isomorphismus $\sigma: E \to E'$, der K elementweise fest läßt.

Konstruktion von Erweiterungskörpern

Sei $f(x) \in K[x]$ irreduzibel über K. Dann ist das Hauptideal (f(x)) prim und daher maximal. (K[x] ist Hauptidealring.) Demnach ist $L=K[x]/(f(x))=K[x]/f(x)$ ein Körper. K kann durch $a \mapsto a+(f(x))$ in L eingebettet werden und wird dadurch zu einem Erweiterungskörper von K. Interpretiert man nun f(x) als Polynom über L und setzt man $\alpha=x+f(x)$, so gilt in L: $f(\alpha)=0$. Weiters gilt $L=K(\alpha)=K[\alpha]$ und $[L:K]=\text{grad } f(x)=\text{grad } m_\alpha(x)$. Normiert man f(x), so erhält man das Minimlpolynom $m_\alpha(x)$. Jede Erweiterung L′ mit Erweiterungsgrad $[L':K]=\text{grad } f(x)$, in der f(x) eine Nullstelle hat, ist bis auf Isomorphie (wo K elementweise fest gelassen wird) eindeutig bestimmt.

Definition: Ein Erweiterungskörper L/K heißt ***Zerfällungskörper eines Polynoms*** $f(x) \in K[x]$ *(b.z.w.* ***einer Familie*** $f_i(x) \in K[x], i \in I$*), falls f(x) (b.z.w. für alle* $i \in I$ $f_i(x)$*) über L in Linearfaktoren zerfällt :* $f(x)=c(x-\alpha_1)\ldots(x-\alpha_n)$ *(b.z.w.* $f_i(x)=c_i\,(x-\alpha_{1i})\ldots(x-\alpha_{ni})$ *) und* $L=K(\alpha_1,\ldots\alpha_n)$ *(b.z.w.* $L=K(\bigcup_{i\in I}\{\alpha_{1i},\ldots,\alpha_{ni}\})$*) gilt.*

L/K heißt ***normal****, falls L Zerfällungskörper eines Polynoms* $f(x) \in K[x]$ *(b.z.w. einer Familie* $f_i(x) \in K[x], i \in I$*) ist.*

Satz: Zu jedem Polynom $f(x) \in K[x]$ (b.z.w, System von Polynomen $f_i(x) \in K[x], i \in I$) gibt es einen Zerfällungskörper, der bis auf Isomorphie (wo K elementweise festgehalten wird) eindeutig bestimmt ist.

Satz: L/K ist normal $\Leftrightarrow$ jedes irreduzible Polynom aus K[x], das eine Wurzel (= Nullstelle) (in L) besitzt, zerfällt über L in Linearfaktoren.

Definition: Sei L/K eine endliche Erweiterung. Für jedes $\alpha \in L$ *ist die Abbildung* $a \mapsto \alpha \cdot a$ *eine lineare Abbildung auf L. Sei* $\omega_1,\ldots,\omega_n$ *eine Basis von L über K und sei* $\alpha \cdot \omega_i = \sum_{j=1}^{n} a_{ij}\omega_j$,

$a_{ij} \in K$*, dann bezeichne* $f_\alpha(x)=\det(x \cdot I-(a_{ij}))$ *das* ***charakteristische Polynom von*** α*. Dieses ist natürlich von der speziellen Wahl der Basis* ω_i *unabhängig.*

Determinante

Die ~~Diskriminante~~ von (a_{ij}) heißt die ***Norm*** $N_{L/K}(\alpha)=\det(a_{ij})$ *und die Spur von* (a_{ij}) *heißt* ***Spur von*** α $Sp_{L/K}(\alpha)=\sum_{j=1}^{n} a_{ii}$.

Satz: Es gilt $f_\alpha(x)= m_\alpha(x)^s$ für ein $s\geq 1$.

Satz: $a\in K \Rightarrow Sp_{L/K}(a)=[L:K]\cdot a,\ N_{L/K}(a)=a^{[L:K]}$

$Sp_{L/K}(\alpha+\beta)=Sp_{L/K}(\alpha)+Sp_{L/K}(\beta)$

$N_{L/K}(\alpha\cdot\beta)=N_{L/K}(\alpha)\cdot N_{L/K}(\beta)$

$K\subseteq L\subseteq E \Rightarrow Sp_{E/K}(\alpha)=Sp_{L/K}(Sp_{E/L}(\alpha)),\quad N_{E/K}(\alpha)=N_{L/K}(N_{E/L}(\alpha))$

Satz: Sei $\omega_1,\ldots,\omega_n$ eine Basis von L/K. Dann gilt

$\det(Sp_{L/K}(\omega_i\,\omega_j))\neq 0 \Leftrightarrow \exists\alpha\in L: Sp_{L/K}(\alpha)\neq 0$

Satz: Sei α algebraisch über K und $L=K(\alpha)$, $n=[L:K]$. Dann ist

$\det(Sp_{L/K}(\alpha^{i+j-2})_{i,j=1,\ldots,n})=\prod_{0\leq i<j\leq n-1}(\alpha_i-\alpha_j)^2$ $\quad(\alpha_0,\ldots,\alpha_{n-1}$ sind die Nullstellen von $m_\alpha(x)$.)

Definition: Sei L/K eine endliche Erweiterung $\alpha\in L$ heißt ***separabel****, falls das Minimlpolynom $m_\alpha(x)$ keine mehrfachen Nullstellen hat.($f(x)$ hat genau dann keine mehrfachen Nullstellen, wenn $f(x)$ und $f(x)'$ teilerfremd sind. Ist $f(x)$ irreduzibel, so ist das genau dann der Fall, wenn $f(x)'$ nicht das Nullpolynom ist.) Die Erweiterung L/K heißt* ***separabel****, wenn jedes $\alpha\in L$ separabel ist. Ein Polynom $f(x)\in K[x]$ heißt* ***separabel****, wenn es keine mehrfachen Nullstellen hat.*

Satz: L/K separabel $\Leftrightarrow \exists\alpha\in L: Sp_{L/K}(\alpha)\neq 0$

Satz: $\alpha_1,\ldots,\alpha_m$ separabel über K $\Rightarrow$ $K(\alpha_1,\ldots,\alpha_m)/K$ separabel

Satz: Sei $K\subseteq L\subseteq E$ und L/K als auch E/L separabel. Dann ist auch E/K separabel.

Definition: Eine endliche Erweiterung E/K heißt ***galoisch****, falls E Zerfällungskörper eines separablen Polynoms ist.*

Satz: Sei L/K separabel. Dann gibt es ein $E\supseteq L$, so daß E/K galoisch ist.

Satz: E/K ist genau dann galoisch, wenn es eine endliche Gruppe G von Automorphismen auf E gibt, so daß K der Fixkörper von G ist. D.h. $K=\{a\in E \mid \sigma(a)=a$ für alle $\sigma\in G\}$ Überdies gilt $[E:K]=|G|$.

Definition: Sei E/K eine Galoischerweiterung . Die Gruppe G der Automorphismen σ auf E, die K elementweise festlassen, heißt ***Galoisgruppe*** $Gal_{E/K}$ *der Galoiserweiterung E/K*

Fundamentalsatz der Galoistheorie: Sei E/K eine Galoiserweiterung und $G= Gal_{E/K}$. Ordnet man jede Untergruppe $U\subseteq G$ dem entsprechenden Fixpunktkörper $L=\{a\in E \mid \sigma(a)=a$ für alle $\sigma\in U\}$ zu, so ist dadurch eine bijektive Zuordnung zwischen Untergruppen und Zwischenkörpern gegeben. Diese Zuordnung kehrt die Enthaltenssein-relation um. Es gilt $[E:K]=|U|$, $[L:K]=\text{ind}(U)=[G:U]$. Weiters ist L/K genau dann galoisch, wenn U Normalteiler von G ist. In diesem Fall gilt $Gal_{E/K}\cong G/U$.

Folgerung: Jede separable Erweiterung L/K besitzt nur endlich viele Zwischenkörper.

Satz: Eine endliche Erweiterung L/K ist genau dann einfach, wenn es nur endlich viele Zwischenkörper gibt.

Satz vom primitiven Element: Jede endliche separable Erweiterung ist einfach.

Satz: Sei L/K eine endliche separable Erweiterung vom Grade [L:K]=n. Dann gibt es in einem passenden Erweiterungskörper E/K n Isomorphismen $\sigma_1,\ldots,\sigma_n$, die K elementweise fest lassen, so daß das charakteristische Polynom die Zerlegung

$$f_\alpha(x)=(x-\sigma_1(\alpha))(x-\sigma_2(\alpha))\ldots(x-\sigma_n(\alpha))$$

besitzt. $\sigma_1(\alpha),\ldots,\sigma_n(\alpha)$ sind die Konjugierten von α und $\sigma_i(L)=K(\sigma_i(\vartheta))$ die konjugierten Körper von L. (ϑ ist primitives Element von L).

Satz: Für jede endliche Erweiterung der rationalen Zahlen gibt es genau n Isomorphismen in den Körper der Komplexen Zahlen.

3. Endliche Körper

Definition: Sei K ein Körper. Ist die additive Ordnung von 1 endlich, so ist sie die ***Charakteristik*** *von K (charK) . Ist sie hingegen unendlich, so sei die Charakteristik von K Null. Der* ***Primkörper*** *P(K) ist der Durchschnitt aller Unterkörper von K.*

Satz: Ist char(K)$\neq 0$, so ist sie eine Primzahl und der Primkörper ist isomorph zum Restklassenkörper $\mathbf{Z}/p\mathbf{Z}$. Ist hingegen charK=0, so ist der Primkörper isomorph zu $\mathbf{Q}$.

Satz: Ist K endlich und p=char(K), so gilt $|K|=p^n$ für ein $n\in\mathbf{N}$.

Satz: Die multiplikative Gruppe eines endlichen Körpers ist zyklisch.

Satz: Für eine Primzahl p und eine natürliche Zahl n gibt es bis auf Isomorphie genau einen Körper mit $q=p^n$ Elementen, nämlich den Zerfällungskörper des Polynoms $x^{p^n}-x$. (Genau genommen besteht dieser Körper aus den Nullstellen von $x^{p^n}-x$.) Man bezeichnet diesen Körper durch $\mathbf{F}_q$ oder GF(q)...Galoisfeld.

Folgerung: Über einem endlichem Körper $\mathbf{F}_q$ gibt es irreduzible Polynome beliebigen Grades.

Satz: Jede endliche Erweiterung L eines endlichen Körpers $K=\mathbf{F}_q$ ist eine Galoiserweiterung. Sei [L:K]=n. Dann besteht die Galoisgruppe $G=Gal_{L/K}$ aus den Automorphismen $\sigma_i(a)=a^{q^i}$ (i=0,1,..,n-1). Dementsprechend berechnet man Spur und Norm durch

$$Sp_{L/K}(a)=a+a^q+\ldots+a^{q^{n-1}} \qquad \text{und} \qquad N_{L/K}(a)=a^{1+q+\ldots+q^{n-1}}$$

Bemerkung: Die Galoisgruppe endlicher Erweiterungen endlicher Körper ist zyklisch, also insbesondere abelsch.

4. Ganzalgebraische Zahlen

Definition: Sei R ein Integritätsbereich. auf den (formalen) Quotienten $\frac{a}{b}$ *(a, b∈**R**, b≠0) wird durch* $\frac{a}{b}+\frac{c}{d}=\frac{a\cdot d+b\cdot c}{b\cdot d}$ *und* $\frac{a}{b}\cdot\frac{c}{d}=\frac{a\cdot c}{b\cdot d}$ *eine Addition und eine Multiplikation definiert. Zwei Quotienten* $\frac{a}{b}$, $\frac{c}{d}$ *heißen gleich (oder äquivalent), falls a·d=b·c gilt. Diese (Äquivalenz-)Relation ist mit den Operationen +, · verträglich. Faktorisiert man nach dieser (Kongruenz-)Relation, so erhält man den* ***Quotientenkörper*** *von R. R läßt sich in seinen Quotientenkörper einbetten, indem man a∈**R** mit jener Äquivalenzklasse identifiziert, die den Quotienten* $\frac{a}{1}$ *enthält.*

Definition: Sei R ein Teilring eines Körpers K. Ein Element α∈K heißt ***ganz(-algebraisch)*** *bezüglich R, wenn α Nullstelle eines normierten Polynoms mit Koeffizienten aus R ist.*

Lemma: Sei M⊆K ein endlich erzeugter R-Modul. (D.h. Es gibt $\omega_1,\ldots,\omega_n \in K$, so daß $M = \{a_1\omega_1+\ldots+a_n\omega_n | a_1,\ldots,a_n \in R\}$.) Ist M auch ein Teilring von K (D.h. er ist bezüglich der Multiplikation abgeschlossen.), dann sind alle Elemente aus M ganz bezüglich R.

Satz: Die Gesamtheit O aller bezüglich R ganzen Elemente bildet einen Ring.

Definition: Sei R Teilring eines Körpers K. Die Gesamtheit O der bezüglich R ganzen Elemente von K wird als ***ganzalgebraische Hülle*** *von R in K bezeichnet. Ein Teilring eines Körpers K heißt* ***ganzabgeschlossen in K*** *, wenn er gleich seiner ganzalgebraischen Hülle in K ist. Ein Integritätsbereich heißt* ***ganzabgeschlossen****, wenn er in seinem Quotientenkörper ganzabgeschlossen ist.*

Satz: Sei R Teilring eines Körpers K. Dann ist die ganzalgebraische Hülle O von R in K ganzabgeschlossen in K.

Lemma: Sei R ganzabgeschlossen (in seinem Quotientenkörper Q) und sei f(x)∈R[x] normiert. Weiters sei φ(x)∈Q[x] ein normierter Teiler von f(x). Dann ist φ(x)∈R[x].

Satz: Sei R ganzabgeschlossen (in seinem Quotientenkörper Q) und sei K/Q eine algebraische Erweiterung von Q. Dann ist α∈K nur dann ganz bezüglich R, wenn sein Minimalpolynom $m_\alpha(x) \in R[x]$.

Satz: Jeder faktorielle Ring ist ganzabgeschlossen.

Definition: Sei L/K endliche Körpererweiterung vom Grad [L:K]=n. Die ***Diskriminante*** $\Delta(\alpha_1,\ldots,\alpha_n)$ *von* $\alpha_1,\ldots,\alpha_n \in L$ *ist die* $\det\left(Sp_{L/K}(\alpha_i\alpha_j)\right)$.

Lemma: Ist $\Delta(\alpha_1,\ldots,\alpha_n) \neq 0$, dann ist $\alpha_1,\ldots,\alpha_n$ Basis der separablen Körpererweiterung L/K. Ist umgekehrt L/K separabel und $\alpha_1,\ldots,\alpha_n$ Basis von L/K, dann gilt $\Delta(\alpha_1,\ldots,\alpha_n) \neq 0$.

Lemma: Sind $\alpha_1,\ldots,\alpha_n$ und $\beta_1,\ldots,\beta_n$ Basen von L/K und $\alpha_i = \sum_{j=1}^{n}\alpha_{ij}\beta_j$, dann gilt

$$\Delta(\alpha_1,\ldots,\alpha_n) = \det(\alpha_{ij})^2\,\Delta(\beta_1,\ldots,\beta_n).$$

Lemma: Sei $\alpha_1,\ldots,\alpha_n \in L$ und L/K separabel. Dann ist $\Delta(\alpha_1,\ldots\alpha_n) = \det\left(\alpha_i^{(j)}\right)^2$, wobei $\alpha_i^{(1)},\ldots,\alpha_i^{(n)}$ die Konjugierten von α_i bezeichnen.

Lemma: Seien $1,\beta,\beta^2,\ldots,\beta^{n-1}$ l.u. in L/K und $m_\beta(x) \in K[x]$ das Minimalpolynom von β. Ist L/K separabel, dann gilt $\Delta\left(1,\beta,..,\beta^{n-1}\right) = (-1)^{\frac{n(n-1)}{2}} N_{L/K}\left(m_\beta'(\beta)\right)$, wobei $m_\beta'(\beta)$ die (formale) Ableitung von $m_\beta(x)$ bezeichnet.

*Definition: Sei $K \subseteq C$ ein endlicher Erweiterungskörper von **Q**. Dann heißt K **algebraischer Zahlkörper** und der ganzalgebraische Abschluß von **Z** in K heißt **Ring der ganzen Zahlen** O_K.*

Lemma: Sei K alg. Zahlkörper und $\beta \in K$. Dann gibt es ein $b \in \mathbf{Z}$, $b \neq 0$, so daß $b\cdot\beta \in O_K$.

Lemma: Sei K alg. Zahlkörper. Dann enthält jedes Ideal $I \neq \{0\}$ von O_K eine Basis von K/**Q**.

Satz: Sei K alg. Zahlkörper und I ein Ideal von O_K. Weiters sei $\alpha_1,\ldots,\alpha_n \in I$ Basis von K/**Q**, so daß $|\Delta(\alpha_1,\ldots,\alpha_n)|$ minimal ist. Dann gilt $I = \mathbf{Z}\alpha_1 + \mathbf{Z}\alpha_2 + \ldots + \mathbf{Z}\alpha_n$, d.h. I ist frei erzeugter **Z**-Modul.

Lemma: Sei I ein Ideal von O_K. Dann gilt $I \cap \mathbf{Z} \neq \{0\}$.

Satz: Für jedes Ideal I von O_K ist der Faktorring O_K/I endlich .

Satz: O_K ist ein **Noetherscher Ring**, d.h. für jede aufsteigende Folge von Idealen $A_1 \subseteq A_2 \subseteq \ldots$ gibt es ein $N>0$, so daß $A_m = A_{m+1}$ für $m \geq N$.

Folgerung: Jedes Primideal von O_K ist maximal.

Bemerkung: O_K ist i.a. nicht faktoriell. Beispielsweise wird in O_K für $K=\mathbf{Q}(\sqrt{-5})$ die Elemente 2, 3, $1+\sqrt{-5}$, $1-\sqrt{-5}$ irreduzibel, es gilt aber $2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. Es gilt allerdings eine schwächere Bedingung, nämlich daß jedes Ideal eindeutig in ein Produkt von Primidealen zerlegt werden kann. O_K ist ein **Dedekindscher Ring** .

Lemma: Sind $\alpha_1,\ldots,\alpha_n$ und $\beta_1,\ldots,\beta_n$ Basen eines Ideals I von O_K, d.h. $I = \mathbf{Z}\alpha_1 + \mathbf{Z}\alpha_2 + \ldots + \mathbf{Z}\alpha_n = \mathbf{Z}\beta_1 + \mathbf{Z}\beta_2 + \ldots + \mathbf{Z}\beta_n$, so sind die Diskriminanten gleich:

$$\Delta(\alpha_1,\ldots,\alpha_n) = \Delta(\beta_1,\ldots,\beta_n).$$

*Definition: Die **Diskriminante $\Delta(I)$** eines Ideals I von O_K ist die Diskriminante $\Delta(I) = \Delta(\alpha_1,\ldots,\alpha_n)$ einer Basis $\alpha_1,\ldots,\alpha_n$ von I. Die **Diskriminante** eines algebraischen Zahlkörpers K/**Q** ist die Diskriminante von O_K: $\delta_K = \Delta(O_K)$.*

5. Der chinesische Restsatz

Definition: Seien I, J Ideale eines kommutativen Ringes R mit 1. Unter der ***Summe I+J*** *versteht man die Menge* $\{a+b|a\in I, b\in J\}$ *und unter dem* ***Produkt I·J*** *die Menge* $\{a_1b_1+\ldots+a_kb_k|a_i\in I, b_i\in J, k\geq 1\}$. *I+J und I·J sind dann wieder Ideale von R..*

Definition: Zwei Ideale I, J eines kommutativen Ringes R mit 1 heißen ***teilerfremd****, wenn I+J=R gilt.*

Bemerkung: In Hauptidealringen gilt,daß a und b genau dann teilerfremd sind, wenn (a)+(b)=R gilt.

Lemma: Ist I teilerfremd zu J_1 und zu J_2 in R, dann ist es auch zu $J_1\cdot J_2$ und $J_1\cap J_2$ teilerfremd.

Lemma: Sind $I_1,\ldots,I_n$ paarweise teilerfremd, so gilt $I_1\cdot\ldots\cdot I_n=I_1\cap\ldots\cap I_n$.

Satz: Sind $I_1,\ldots,I_n$ paarweise teilerfremde Ideale eines kommutativen Ringes R mit 1, dann ist für beliebige $a_1,\ldots,a_n\in R$ das System von Kongruenzen

$$x\equiv a_1 \pmod{I_1}$$
$$\ldots$$
$$x\equiv a_n \pmod{I_n}$$

lösbar. Ist u eine Lösung, so ist die Gesamtheit aller Lösungen des Kongruenzsystems durch die x mit $x\equiv u \pmod{I_1\cdot\ldots\cdot I_n}$ gegeben.

Satz: Sind $I_1,\ldots,I_n$ paarweise teilerfremde Ideale eines kommutativen Ringes R mit 1, dann ist $R/I_1\cdot\ldots\cdot I_n$ isomorph zur direkten Summe $R/A_1\oplus\ldots\oplus A_n$, und die Einheitengruppe von $R/I_1\cdot\ldots\cdot I_n$ ist isomorph zum direkten Produkt der Einheitengruppen der R/A_i (i=1,...,n).

6. Dedekindsche Ringe

Definition: Ein kommutativer Ring mit 1 heißt ***Noethersch****, wenn jede aufsteigende Kette von Idealen* $I_1\subseteq I_2\subseteq\ldots$ *endlich ist, d. h. es gibt ein N, so daß für* $m\geq N$ *immer* $I_{m+1}=I_m$ *gilt.*

Satz: Ein kommutativer Ring mit 1 ist nur dann Noethersch, falls jedes Ideal endlich erzeugt ist.

Definition: Ein Integritätsring R heißt ***Dedekindscher Ring****, falls folgende drei Eigenschaften erfüllt sind: (I) R ist Noethersch.*
(II) Jedes Primideal I≠0 von R ist maximal.
(III) R ist ganzalgebraisch abgeschlossen.

Definition: Sei R ein Integritätsring und K sein Quotientenkörper. Ein R-Modul I≠0, $I\subseteq K$ *heißt* ***Bruchideal*** *(von K), wenn es ein* $a\in R$, $a\neq 0$ *gibt, so daß* $a\cdot I\subseteq R$ *gilt.*
Ein Bruchideal I heißt ***invertierbar****, falls für* $I'=\{x\in K|x\cdot I\subseteq R\}$ *(nicht nur* $I\cdot I'\subseteq R$, *sondern auch)* $I\cdot I'=R$ *gilt, i.Z.* $I'=I^{-1}$.

Lemma: Die Menge der Bruchideale bildet ein kommutatives Monoid.
Die Menge der invertierbaren Bruchideale bildet eine kommutative Gruppe.
Die Menge der **Hauptbruchideale** (d. h. Ideale der Form $I=a\cdot R$, $a\in K$) bildet eine Untergruppe der Gruppe der invertierbaren Bruchideale.

Satz: Ein Integritätsring R ist nur dann Dedekindscher Ring, wenn jedes Bruchideal (im Quotientenkörper von R) invertierbar ist.

Lemma: Sei R ein Noetherscher Ring und $0\neq I\neq R$ ein Ideal von R. Dann gibt es Primideale $P_1,\ldots,P_r$ von R mit $P_1\cdot\ldots\cdot P_r\subseteq I\subseteq P_1\cap\ldots\cap P_r$.

Lemma: In einem Dedekindschen Ring R ist jedes Primideal $P\neq 0$ invertierbar.

Lemma: In einem Dedekindschen Ring R kann jedes Ideal $0\neq I\neq R$ als Produkt von Primidealen dargestellt werden.

Satz: In einem Dedekindschen Ring R kann jedes Ideal $0\neq I\neq R$ (bis auf die Reihenfolge) eindeutig als Produkt von Primidealen dargestellt werden.

Folgerung: Die Gruppe der Bruchideale eines Dedekindschen Ringes ist eine frei erzeugte Gruppe, die von den Primidealen erzeugt wird.

Folgerung: Ein Ideal $I\neq 0$ kann nur durch endlich viele verschiedene Ideale geteilt werden.

*Definition: Ein Ideal **B teilt A**, falls es ein Ideal C mit $A=B\cdot C$ gibt. Der **größte gemeinsame Teiler (A, B)** zweier Ideale A,B ist ein Ideal, das sowohl A als auch B teilt, und jeder gemeinsame Teiler von A und B teilt (A,B).*

Satz: Sei R ein Dedekindscher Ring. Dann gilt:

(I) $A=\prod P^{a(P)}$, $B=\prod P^{b(P)} \Rightarrow (A,B)=\prod P^{\min(a(P),b(P))}$

(II) Sind A, B zwei Bruchideale (vom Quotientenkörper K), dann gilt $A\subseteq B$ nur dann, wenn es ein Ideal $C\lhd R$ mit $A=B\cdot C$ gibt. Insbesondere gilt für Ideale $A, B\subseteq R$: A ist teilbar durch B $\Leftrightarrow A\subseteq B$

(III) $(A, B)=A+B$

(IV) Sind $A, B\subseteq R$ teilerfremd (d.h. $(A, B)=R$), dann gilt $A\cdot B=A\cap B$

Satz: Sei $0\neq I\neq R$ ein Ideal eines Dedekindschen Ringes R. Dann gilt
$R/I=R/P_1^{a_1}\oplus\ldots\oplus R/P_k^{a_k}$, falls I die Darstellung $I=P_1^{a_1}\cdot\ldots\cdot P_k^{a_k}$ hat.

Satz: Jedes Ideal $I\neq 0$ eines Dedekindschen Ringes R hat die Darstellung $I=xR+yR$.

Satz: Ist $P\neq 0$ ein Primideal eines Dedekindschen Ringes R und $n\geq 1$. Dann sind die additiven Gruppen von R/P und R^n/P^n isomorph.

*Definition: Ein Dedekindscher Ring R erfüllt die **endliche Normbedingung**, falls für alle Ideale $I\neq 0$ der Faktorring R/I endlich ist. In diesem Fall heißt die Mächtigkeit $N(I)=|R/I|$ die **Norm des Ideals I**.*

Satz: R erfülle die endliche Normbedingung. Dann gilt:

(I) $N(I\cdot J)=N(I)\cdot N(J)$

(II) Für alle $T\geq 0$ ist die Menge $\{0\neq I\lhd R \mid N(I)\leq T\}$ endlich.

(III) Die Ordnung der Einheitengruppe von R/I ist gegeben durch

$$\varphi(I)=N(I)\prod_{P\mid I}\left(1-\frac{1}{N(P)}\right).$$

7. Faktorisieren im Ring der ganzen Zahlen

*Definition: Sei K ein algebraischer Zahlkörper und $P\neq 0$ ein Primideal von O_K. Dann ist $P\cap\mathbf{Z}$ ein Primideal von **Z**, d.h. $P\cap\mathbf{Z}=p\cdot\mathbf{Z}$ für eine Primzahl $p\in\mathbf{Z}$. Zerlegt man das Ideal $I=p\cdot O_K=P_1^{e_1}P_2^{e_2}\ldots P_g^{e_g}$ in seine Primidealfaktoren (o.B.d.A. kann man $P_1=P$ wählen, da $I=p\cdot O_K\subseteq P$ gilt), so heißt die natürliche Zahl $e\geq 1$ der **Verzweigungsindex von P**, i.Z. $e=e(P)$. Wegen $P\cap\mathbf{Z}=p\cdot\mathbf{Z}$ ist p die Charakteristik des endlichen Körpers O_K/P, d.h. $|O_K/P|=p^f$ für eine natürliche Zahl $f\geq 1$. Diese Zahl heißt **Trägheitsindex von P**, i.Z. $f=f(P)$.*

Satz: Sei p eine Primzahl in **Z** und K ein algebraischer Zahlkörper vom Grad n. Gilt nun $(p)=p\cdot O_K=P_1^{e_1}\ldots P_g^{e_g}$ und bezeichne f_i die Trägheitsindizes von P_i, so gilt: $\sum_{i=1}^{g}e_if_i=n$.

Satz: Sei F eine endliche Galoiserweiterung von **Q** vom Grad n und $p\in\mathbf{Z}$ eine Primzahl. Dann gilt $(p)=p\cdot O_K=P_1^{e_1}\ldots P_g^{e_g}$ mit $e_1=e_2=\ldots=e_g=:e$ und $f_1=f_2=\ldots=f_g=:f$. Bezeichnet man diese gemeinsamen Werte mit e bzw. mit f, dann gilt auch $e\cdot f\cdot g=n$.

Satz: Sei K ein algebraischer Zahlkörper und es gebe ein $\alpha\in K$, so daß $O_K=\mathbf{Z}[\alpha]$ ist. Sei $f(x)=m_\alpha(x)$ das Minimalpolynom von α. (Da α ganzalgebraisch ist, ist $m_\alpha(x)$ ganzzahlig.) Weiters sei $p\in\mathbf{Z}$ eine Primzahl und $\bar{f}(x)=\bar{G}_1(x)^{e_1}\ldots\bar{G}_g(x)^{e_g}$ die Zerlegung in irreduzible Faktoren von f(x) modulo p. O.B.d.A. sei $\bar{G}_i(x)$ als normiert angenommen. Bezeichne $G_i(x)\in\mathbf{Z}$ ein normiertes Polynom mit $G_i(x)\pmod p=\bar{G}_i(x)$. Dann sind $P_i=p\cdot O_K+G_i(\alpha)\cdot O_K$ Primideale von O_K mit $(p)=p\cdot O_K=P_1^{e_1}\ldots P_g^{e_g}$. e_i ist der Verzweigungsindex von P_i und $f_i=\mathrm{grad}\,G_i(x)$ der Trägheitsindex von P_i.

*Definition: Sei K algebraischer Zahlkörper. Bezeichne G(K) die Gruppe der Bruchideale in K und P(K) die Untergruppe der Hauptbruchideale. $H(K)=G(K)/P(K)$ ist die **Idealklassengruppe** von K und $h(K)=|H(K)|$ die **Klassenzahl** von K.*

***Satz**: (I) Die Klassenzahl h(K) ist für jeden algebraischen Zahlkörper endlich.*
(II) $h(K)=1 \Leftrightarrow O_K$ ist Haupidealring $\Leftrightarrow O_K$ ist faktorieller Ring.

Satz: Sei K algebraischer Zahlkörper. Dann gibt es eine Konstante C=C(K) mit der folgenden Eigenschaft: Für alle $a\in K$ gibt es ein $x\in O_K$ und ein $r\in\mathbf{N}$ mit $r\leq C$, so daß $|N_{K/Q}(ra-x)|<1$ ist.

8. Der Dirichletsche Einheitensatz

Definition: Sei K algebraischer Zahlkörper und $\sigma_1(K),\ldots,\sigma_s(K),\sigma_{s+1}(K),\ldots,\sigma_{s+t}(K),\overline{\sigma}_{s+1}(K),\ldots,\overline{\sigma}_{s+t}(K)$ *die konjugierten Körper von K, wobei* $\sigma_1(K),\ldots,\sigma_s(K)\subseteq\boldsymbol{R}$ *und* $\sigma_{s+1}(K),\ldots,\sigma_{s+t}(K)\not\subseteq\boldsymbol{R}$ *gelten (s+2t=n). Dann heißt das Paar*

[s,t] ***Signatur*** *von K.*

Bemerkung: Für jedes Paar [s,t] von nicht-negativen Zahlen mit n=s+2t>0 gibt es einen algebraischen Zahlkörper mit dieser Signatur.

Satz (Dirichlet):

Sei K algebraischer Zahlkörper mit Signatur [s,t]. Dann gibt es r=s+t-1 Einheiten $\varepsilon_1,\ldots,\varepsilon_r\in O_K$, so daß sich jede Einheit $\varepsilon\in O_K$ eindeutig in der Form $\varepsilon=\zeta\varepsilon_1^{a_1},\ldots,\varepsilon_r^{a_r}$ darstellen läßt, wobei $a_1,\ldots,a_r$ ganze Zahlen sind und ζ eine in O_K enthaltene Einheitswurzel ist. Die Einheitswurzeln in O_K bilden eine zyklische Gruppe gerader Ordnung. Demnach ist die Einheitengruppe von O_K direktes Produkt einer endlichen zyklischen Gruppe gerader Ordnung und r=s+t-1 zyklischer Gruppen unendlicher Ordnung. Die erzeugenden Einheiten $\varepsilon_1,\ldots,\varepsilon_r$ heißen **Grundeinheiten**.

Definition: Seien $a_1,\ldots,a_m\in\boldsymbol{R}^n$ *m l.u. Vektoren über* $\boldsymbol{R}$. *Dann heißt die davon erzeugte freie abelsche Gruppe* $G=G(a_1,\ldots,a_m)=\{\sum_{i=1}^{m}k_ia_i\,|\,k_i\in\boldsymbol{Z}\}$ ***m-dimensionales Gitter des*** R^n.

Ist m=n, so spricht man auch von einem (vollständigen) ***Gitter****. Die Menge* $P=\{\sum_{i=1}^{n}x_ia_i\,|\,o\le x_i<1\}$ *heißt* ***Fundamentalparallelepiped*** *der* ***Gitterbasis*** $a_1,\ldots,a_m\in\boldsymbol{R}^n$ *und das Volumen von P* $Vol\,P=|det(a_1,..,a_m)|=d(G)$ ***Gitterkonstante*** *von G.*
(Die Gitterkonstante ist von der Wahl der Gitterbasis unabhängig.)

Satz: Die m-dimensionalen Gitter ($1\le m\le n$) des $\mathbf{R}^n$ sind genau die diskreten Untergruppen von $\langle\mathbf{R}^n,+\rangle$. (Diskret heißt, daß in jeder beschränkten Menge des $\mathbf{R}^n$ nur endlich viele Punkte aus G liegen.)

Definition: Sei K alg. Zahlkörper mit Signatur [s,t]. Bezeichnen $\sigma_1,\ldots,\sigma_s$ *die reellen und* $\sigma_{s+1}(K),\overline{\sigma}_{s+1}(K),\ldots,\sigma_{s+t}(K),\overline{\sigma}_{s+t}(K)$ *die komplexen Einbettungen von K in C, so kann jedem* $\alpha\in K$ *ein* $x(\alpha)=\left(\sigma_1(\alpha),..,\sigma_s(\alpha),\sigma_{s+1}(\alpha),\ldots,\sigma_{s+t}(\alpha)\right)\in\boldsymbol{R}^s\times\boldsymbol{C}^t\cong\boldsymbol{R}^{s+2t}=\boldsymbol{R}^n$ *zugeordnet werden. Das ist die* ***geometrische Darstellung*** *des Körpers K im* $\boldsymbol{R}^n$.

Lemma: Ist $\alpha_1,\ldots,\alpha_n$ eine Basis von K/**Q**, so sind die Vektoren $x(\alpha_1),\ldots,x(\alpha_n)\in\mathbf{R}^n$ l.u. über **R**.

Lemma: Die geometrische Darstellung von O_K bildet ein (vollständiges) Gitter mit Gitterkonstante $2^{-t}\sqrt{|\delta_K|}$, wobei δ_K die Diskriminante von K bezeichnet.

Definition: Sei K wie oben. Jedem $\alpha \neq 0$ kann durch

$$l(\alpha) = \left(\log|\sigma_1(\alpha)|,\ldots,\log|\sigma_s(\alpha)|,2\log|\sigma_{s+1}(\alpha)|,\ldots,2\log|\sigma_{s+t}(\alpha)|\right) \in \boldsymbol{R}^{s+t}$$

*zugeordnet werden. Dies ist die **logarithmische Darstellung** von $K\setminus\{0\}$ im sogenannten **Logarithmenraum**. Die Abbildung $\alpha \to l(\alpha)$ ist ein Homomorphismus der multiplikativen Gruppe von K in die additive Gruppe von $\boldsymbol{R}^{s+t}$.*

Lemma:(I) $\varepsilon \in O_K$ ist Einheit $\Leftrightarrow$ $|N_{K/Q}(\varepsilon)|=1$

(II) Die Einheiten ε von O_K mit $l(\varepsilon)=0$ bilden eine zyklische Gruppe gerader Ordnung und sind genau die Einheitswurzeln in O_K.

(III) Die Gesamtheit der Bilder $l(\varepsilon)$ von Einheiten von O_K bilden ein Gitter der Dimension $\leq s+t-1$

Satz vom Blickfeld: Zu jedem Gitter G und jeder nicht leeren, beschränkten, integrierbaren Menge $M \subseteq \mathbf{R}^n$ kann man einen Punkt P angeben, so daß die Anzahl der Gitterpunkte des von P ausgehenden Punktgitters PG innerhalb der Menge M mindestens $\geq \mathrm{Vol}(N)/d(G)$ beträgt.

Gitterpunktsatz von Minkowski: Sei K eine symmetrische, beschränkte und konvexe Menge im $\mathbf{R}^n$ und G ein Gitter mit $\mathrm{Vol}(K) > 2^n \cdot d(G)$. Dann enthält K mindestens einen von 0 verschiedenen Gitterpunkt aus G.

Folgerung: Sei G ein Gitter im $\mathbf{R}^s \times \mathbf{C}^t \cong \mathbf{R}^n$ $(n=s+2t)$ und gelte für $c_1,\ldots,c_{s+t} > 0$ die Ungleichung $c_1 \cdot \ldots \cdot c_{s+t} > \left(\frac{4}{\pi}\right)^t \cdot d(G)$, so gibt es in G einen von 0 verschiedenen Punkt $(x_1,\ldots,x_{s+t}) \in \mathbf{R}^s \times \mathbf{C}^t \cong \mathbf{R}^n$ mit $|x_i| < c_i$.

Lemma:Ein Gitter G ist dann und nur dann vollständig, wenn es ein beschränkte Menge U mit $\bigcup_{x \in G}(x + U) = \mathbf{R}^n$ gibt.

9. Quadratische Zahlkörper

*Definition: Ein algebraischer Zahlkörper K mit $[K:\mathbf{Q}]=2$ heißt **quadratisch**.*

Lemma: Sei K quadratischer Zahlkörper. Dann gibt es eine eindeutig bestimmte quadratfreie ganze Zahl $d \neq 1$ mit $K=\mathbf{Q}(\sqrt{d})$.

Satz: Sei $d \neq 1$ quadratfrei und $K=\mathbf{Q}(\sqrt{d})$. Dann gilt:

$O_K=\mathbf{Z}+\mathbf{Z}\sqrt{d}$, $\quad \delta_K=4d$ für $d \equiv 2,3 \pmod 4$ und

$O_K=\mathbf{Z}+\mathbf{Z}\cdot\frac{-1+\sqrt{d}}{2}$, $\delta_K=d$ für $d \equiv 1 \pmod 4$.

Satz: Jede quadratische Körpererweiterung von Q ist Galoisch.

Satz: Sei p eine ungerade (rationale) Primzahl. Dann gilt für $K=\mathbf{Q}(\sqrt{d})$

(I) $p\nmid\delta_K$, $x^2 \equiv d \pmod p$ ist lösbar $\Rightarrow$ $(p) = P \cdot P'$, $P \neq P'$

(II) $p\nmid\delta_K$, $x^2 \equiv d \pmod p$ ist unlösbar $\Rightarrow$ $(p)=P$

(III) $p|\delta_K \Rightarrow (p)=P^2$

Hingegen gilt für p=2

(I) $2\nmid\delta_K$, $d\equiv 1\ (8) \Rightarrow (p) = P \cdot P'$, $P \neq P'$

(II) $2\nmid\delta_K$, $d\equiv 5\ (8) \Rightarrow (2)=P$

(III) $2|\delta_K \Rightarrow (2)=P^2$.

Definition: Ein Polynom der Form $f(x,y)= ax^2 + bxy + cy^2$ mit $a,b,c \in \mathbf{Z}$, heißt ***quadratische Form****. $\delta(f) = b^2-4ac$ ist ihre* ***Diskriminante****. $f(x,y)$ heißt* ***primitiv****, falls $ggT(a,b,c)=1$. Sie ist* ***positiv definit*** *(d.h. $f(x,y)>0$ für $(x,y)\neq(0,0)$), falls $a>0$ und $\delta(f)<0$ sind. Zwei quadratische Formen $f_1(x,y)$, $f_2(x,y)$ heißen* ***äquivalent****, falls es eine ganzzahlige Matrix* $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ *mit $AD-BC=\pm 1$ gibt, sodaß $f_1(Ax+By, Cx+Dy) = f_2(x,y)$ gilt. In diesem Fall gilt auch $\delta(f_1) = \delta(f_2)$.*

Definition: Sei $d \in \mathbf{Z}$, $d\neq 0$. Dann heißt die Anzahl der Äquivalenzklassen von quadratischen Formen mit $\delta(f)=d$ ***Klassenzahl*** *$h(d)$.*

Lemma: (I) Jede primitive positiv definite quadratische Form ist äquivalent zu einer Form $g(x,y)=ax^2 + bxy + cy^2$ mit $|b|\leq a\leq c$

(II) Jede primitive indefinite quadratische Form mit nicht quadratischer Diskriminante ist äquivalent zu einer Form $g(x,y)=ax^2 + bxy + cy^2$ mit $|b|\leq|a|$, $|b|\leq|c|$.

Folgerung: $h(d)$ ist für alle $d\neq 0$ endlich:

$h(d) \leq \frac{2}{3}(-d)$ für $d<0$

$h(d) \leq \frac{2}{5}d + d(\alpha)$ für $d>0$, d keine Quadratzahl.

Satz: Sei $d<0$ Diskriminante eines imaginär quadratischen Körpers $K=\mathbf{Q}(\sqrt{-d})$. Für jedes Ideal $I\subseteq O_K$, dargestellt in der Form $I=\mathbf{Z}a_1 \oplus \mathbf{Z}a_2$, wobei man o.B.d.A. annehmen kann, daß $\mathrm{Im}(a_1\bar{a}_2 - \bar{a}_1 a_2) > 0$ ist, stelle man eine quadratische Form $f_{a_1a_2}(x,y)=\frac{1}{N(I)}N_{K/Q}(a_1x + a_2y)$ auf. Für diese gilt:

(I) $f_{a_1a_2}(x,y)$ ist eine primitive, positiv definite, quadratische Form mit ganzzahligen Koeffizienten und Diskriminante d.

(II) Zwei Ideale $I=\mathbf{Z}a_1 \oplus \mathbf{Z}a_2$, $J=\mathbf{Z}b_1 \oplus \mathbf{Z}b_2$ sind genau dann in der selben Idealklasse, wenn die quadratischen Formen $f_{a_1a_2}(x,y)$, $f_{b_1b_2}(x,y)$ äquivalent sind.

(III) Die Zuordnung $f_{a_1a_2} \mapsto$ (Klasse von $I=\mathbf{Z}a_1 \oplus \mathbf{Z}a_2$) induziert eine Bijektion zwischen der Menge aller Klassen primitiver, positiv definiter, quadratischen Formen mit Diskriminante d und der Idealklassengruppe H(K).

(IV) Sei $I=\mathbf{Z}a_1 \oplus \mathbf{Z}a_2$ und X die Idealklasse von H(K), die I enthält. Dann gilt

$$\{ f_{a_1a_2}(x,y) | x,y \in \mathbf{Z}\} = \{N(J) | J \in X^{-1}\} \text{ und } \left|\{J \in X^{-1} | N(J) = m\}\right| = \frac{1}{\varepsilon(d)} \sum_{\substack{x,y \\ f_{a_1a_2}(x,y)=m}} 1$$

wobei $\varepsilon(d) = \begin{cases} 6 \text{ für } d = -3 \\ 4 \text{ für } d = -4 \\ 2 \text{ für } d \neq -3,-4 \end{cases}$ ist. ($\varepsilon(d)$ ist die Anzahl der Einheitswurzeln in K.)

Bemerkung: Für d>0 gibt es ein ähnliche Beziehung zwischen Formen und Idealklassen. Nur erhält man hier eine Bijektion zwischen den Äquivalenzklassen von Formen und Diskriminante d und $H^*(K)$. $H^*(K)$ wird dadurch erzeugt, daß zwei Ideale I, J äquivalent heißen, wenn es $a,b \in O_K$ mit aI=bJ gibt, so daß a,b>0 als auch ihre Konjugierten >0 sind.

Satz: Sei d<0 Diskriminante eines imaginär quadratischen Körpers. Dann gilt $h(\mathbf{Q}(\sqrt{-d}))=h(d)$.

Definition: Sei p eine Primzahl.

Dann ist das ***Legendresymbol*** $\left(\frac{n}{p}\right)$ *durch* $\left(\frac{n}{p}\right) = \begin{cases} +1, \text{ falls } x^2 \equiv n\ (p) \text{ lösbar und } p \nmid n \\ -1, \text{ falls } x^2 \equiv n\ (p) \text{ unlösbar und } p \nmid n \\ 0, \text{ falls } p \mid n \end{cases}$

definiert. Weiters sei das ***Kroneckersymbol*** $\left(\frac{d}{n}\right)$ *für folgende ganze Zahlen d definiert:*

(a) $d = \varepsilon \cdot p_1 \cdot \ldots \cdot p_r \equiv 1\ (4)$, $\varepsilon = \pm 1$, $r \geq 1$, p_i *ungerade Primzahlen*
(b) $d = 4\varepsilon \cdot p_1 \cdot \ldots \cdot p_r$, $\varepsilon \cdot p_1 \cdot \ldots \cdot p_r \equiv 3\ (4)$, $r \geq 0$, p_i *ungerade Primzahlen*
(c) $d = 8\varepsilon \cdot p_1 \cdot \ldots \cdot p_r$ $r \geq 0$, p_i *ungerade Primzahlen.*

Dann sei im Fall (a) $\left(\frac{d}{n}\right) = \prod_{i=1}^{r} \left(\frac{n}{p_i}\right)$,

im Fall (b) $\left(\frac{d}{n}\right) = \begin{cases} \eta \cdot \prod_{i=1}^{r} \left(\frac{n}{p_i}\right), \text{ wobei } \eta = \begin{cases} 1 \text{ für } n \equiv 1\ (4) \\ -1 \text{ für } n \equiv -1\ (4) \end{cases} \text{ und} \\ 0 \text{ für } n \equiv 0\ (2) \end{cases}$

im Fall (c) $\left(\frac{d}{n}\right) = \left.\begin{cases} (-1)^{\frac{(x^2-1)}{8}} \prod_{i=1}^{r} \left(\frac{n}{p_i}\right), \text{ falls } sgn(d) = \prod_{i=1}^{r} \left(\frac{-1}{p_i}\right) \\ \eta \cdot (-1)^{\frac{(x^2-1)}{8}} \prod_{i=1}^{r} \left(\frac{n}{p_i}\right), \text{ falls nicht} \\ 0 \qquad \text{für } n \equiv 0\ (2) \end{cases}\right\} n \equiv 1\ (2)$

Für jedes dieser d betrachte man weiters die ***L-Reihe*** $L_d(s) = \sum_{n=1}^{\infty} \frac{\left(\frac{d}{n}\right)}{n^s}$ *(Res>0).*

Satz (Dirichletsche Klassenzahlformel)

Sei K quadratischer Zahlkörper mit Diskriminante d,ε(d) die Anzahl der Einheitswurzeln in K, h(d) die Klassenzahl und im Fall d>0 sei ε>1 die Grundeinheit in K. Dann gilt

$$h(d)=\begin{cases}\dfrac{\varepsilon(d)|d|^{1/2}}{2\pi}L_d(1)=\dfrac{\varepsilon(d)}{2d}\displaystyle\sum_{n=1}^{|d|}\left(\frac{d}{n}\right)n & \text{für } d<o\\ \dfrac{d^{1/2}}{2\log\varepsilon}L_d(1)=\dfrac{-1}{\log\varepsilon}\displaystyle\sum_{0<n<\frac{d}{2}}\left(\frac{d}{n}\right)\log\left(\sin\frac{\pi n}{d}\right) & \text{für } d>0\end{cases}$$

Satz: Für d<0 gilt $\lim\limits_{d\to-\infty}\dfrac{\log h\left(Q\left(\sqrt{d}\right)\right)}{\log|d|^{1/2}}=1$. (d Diskriminante)

Nur für d=-1,-2,-3,-7,-11,-19,-43,-67 und -163 ist h(d)=1.

Satz: Für d>0 gilt $\overline{\lim\limits_{d\to\infty}}\dfrac{\log h\left(Q\left(\sqrt{d}\right)\right)}{\log|d|^{1/2}}=1$. (d Diskriminante)

Bemerkung: Es ist ein ungelöstes Problem, ob es unendlich viele reell-quadratische Körper mit Klassenzahl 1 gibt.

10. Kreisteilungskörper

Definition: Sei $m\in N$ und $\zeta_m=e^{2\pi i/m}$. $L=Q(\zeta_m)$ heißt dann ***m-ter Kreisteilungskörper****. Wegen* $x^m-1=(x-1)(x-\zeta_m)(x-\zeta_m^{\,2})\ldots(x-\zeta_m^{\,m-1})$ *ist L Zerfällungskörper von x^m-1 und daher auch Galois.*

Definition: Die Einheitswurzeln $\zeta_m^{\,a}$ mit (a,m)=1 (1≤a<m) heißen ***primitive m-te Einheitswurzeln****.*

$\Phi_m(x)=\prod\limits_{\substack{(a,m)=1\\1\le a<m}}(x-)$ *ist dann das* ***m-te Kreisteilungspolynom****. Sein Grad ist φ(m)*

Satz: $x^m-1=\prod\limits_{d|m}\Phi_d(x)$

Lemma: $\Phi_m(x)\in\mathbf{Z}[x]$

Satz: $\Phi_m(x)$ ist irreduzibel über **Q**.

Folgerung: $[\mathbf{Q}(\zeta_m):\mathbf{Q}]=\varphi(m)$. Weiters ist die Galoisgruppe isomorph zur Einheitengruppe $E(\mathbf{Z}/m\mathbf{Z})$. [(a,m)=1: $\sigma_a(\zeta)=\zeta^a$]

Satz: Für $L=\mathbf{Q}(\zeta_m)$ gilt $O_L=\mathbf{Z}[\zeta_m]$

Bemerkung: Da dieser Satz in voller Allgemeinheit sehr umständlich zu beweisen ist, beschränken wir uns auf den Fall einer Primzahl m bzw. auf eine viel schwächere Version für allgemeine m.

Lemma: Sei K/**Q** algebraischer Zahlkörper vom Grad n, $\alpha_1,\ldots,\alpha_n$ eine Basis von K/**Q** und $\Delta = \Delta(\alpha_1,\ldots\alpha_n)$. Dann gilt $\Delta \cdot O_K \subseteq \mathbf{Z}\alpha_1+\ldots+\mathbf{Z}\alpha_n$.

Lemma: $\Delta(1,\zeta_m,\ldots,\zeta_m^{\varphi(m)-1}) \mid m^{\varphi(m)}$

Satz: Sei $p\in\mathbf{Z}$ eine Primzahl mit $p \nmid m$ und $w\in O_{Q(\zeta_m)}$. Dann gibt es ein $v\in\mathbf{Z}[\zeta_m]$ mit $w\equiv v$ (p).

Folgerung: Sei $p\in\mathbf{Z}$ prim, $p \nmid m$, $n>0$, $p^n \equiv 1$ (m), $w\in O_{Q(\zeta_m)} \Rightarrow w^{p^n} \equiv w$ (p).

Satz: Sei $p\in\mathbf{Z}$ prim, $p \nmid m$, $P|(p) \Rightarrow e(P)=1$.

Lemma: Sei $p\in\mathbf{Z}$ prim, $p \nmid m$, $\sigma_p(\zeta) = \zeta^p$, $w\in O_{Q(\zeta_m)} \Rightarrow \sigma_p(w) \equiv w^p$ (p).

Folgerung: Sei $p\in\mathbf{Z}$ prim, $p \nmid m$, $P|(p) \Rightarrow \sigma_p(P) = P$.

Satz: Sei $p\in\mathbf{Z}$ prim, $p \nmid m$, f sei kleinste natürliche Zahl mit $p^f \equiv 1$ (m).
Dann gilt $(p) = P_1\cdot\ldots\cdot P_g$ mit $f(P_i)=f$ und $g=\varphi(m)/f$.

Folgerung: $P|(p)$, $G(P)=\{\sigma\in Gal: \sigma(P)=P\} \Rightarrow G(P)=\langle\sigma_p\rangle$.

Satz: Sei $l\in\mathbf{Z}$ prim, $L=(1-\zeta_l)\subseteq O_{Q(\zeta_l)} \Rightarrow (l) = L^{l-1}$, $f(L) = 1$,
(wobei L natürlich ein Primideal ist).

Satz: Sei P ein Primideal in $\mathbf{Q}(\zeta_m)$ und $P\cap\mathbf{Z}=p\mathbf{Z}$. Dann gilt

$$e(P) > 1 \Leftrightarrow \begin{cases} p|m \text{ für ungerade } p \\ 4|p \text{ für } p = 2 \end{cases}$$

Satz: Sei $l\in\mathbf{Z}$ prim $\Rightarrow O_{Q(\zeta_l)} = \mathbf{Z}[\zeta_l]$.

*Definition: Eine Primzahl $l\in\mathbf{Z}$ heißt **regulär**, falls $l \nmid h(\mathbf{Q}(\zeta_l))$.*

Satz: Sei l eine reguläre Primzahl. Dann hat die Diophantische Gleichung $x^l + y^l = z^l$ keine Lösung $x,y,z\in\mathbf{Z}$ mit $l \nmid xyz$.

Bemerkung: Es ist unbekannt, ob es unendlich viele reguläre Primzahlen gibt. Allerdings gibt es unendlich viele nicht reguläre Primzahlen.

Lemma: Sei $l\in\mathbf{Z}$ prim. Dann sind die einzigen Einheitswurzeln in $\mathbf{Q}(\zeta_l)$ die Zahlen $\pm\zeta_l^i$, i=1,2,..,l. (Dieses Lemma gilt auch für allgemeine m.)

Lemma:Sei K algebraischer Zahlkörper vom Grad n.
Gilt für ein $\alpha\in K$ $|\sigma_1(\alpha)|\le 1,\ldots,|\sigma_n(\alpha)|\le 1$. Dann ist α Einheitswurzel.

Lemma: Sei u eine Einheit in $\mathbf{Z}[\zeta_l]$ ($l\in\mathbf{Z}$ prim). Dann ist $\zeta_l^s u$ reell für ein $s\in\mathbf{Z}$.

Lemma: Seien $x,y \in \mathbf{Z}$ $l \nmid x \cdot y$ mit $(x,y)=1$ und $l \in \mathbf{Z}$ prim, so daß $x^l + y^l + z^l = 0$ für ein z mit $l \nmid z$. Dann sind die Hauptideale $(x+\zeta^i y)$, $(x+\zeta^j y)$, $i \not\equiv j$ (l), teilerfremd in $\mathbf{Z}[\zeta_l]$.

Lemma: Seien $x,y \in \mathbf{Z}$ mit $(x,y,z)=1$ und $l \in \mathbf{Z}$ prim $l \nmid h$. Dann gibt es $u,\beta \in \mathbf{Z}[\zeta_l]$, u reelle Einheit in $\mathbf{Z}[\zeta_l]$, so daß $x+\zeta y = \zeta^s u\beta$ für ein $s \in \mathbf{z}$ und $\beta \equiv n$ (l) für ein $n \in \mathbf{Z}$ gelten.

Lemma: Mit der obigen Notation gilt $x+\zeta y - \zeta^{2s}x - \zeta^{2s-1}y \in l \cdot \mathbf{Z}[\zeta_l]$.

Bemerkung: Für Kreisteilungskörper gibt es wieder eine Klassenzahlformel:

$$h = \frac{w\sqrt{|\delta|}}{2^{s+t}\pi^t R} F(1) \prod_{\chi \neq \chi_0} L(1,\chi),$$

wobei w die Anzahl der Einheitswurzeln in $\mathbf{Q}(\zeta_m)$ bezeichnet, δ die Diskriminante, R den Regulator, $F(s) = \prod_{p|m}\left(1-\frac{1}{N(P)^s}\right)^{-1} \cdot \prod_{p|m}\left(1-\frac{1}{p^s}\right)$ und $L(s,\chi) = \sum_{n \geq 1} \frac{\chi(n)}{n^s}$ bezeichnet.

Dabei sind $\chi(n)$ die Dirichletschen Charaktere modulo m.

Ist χ gerade, d.h. $\chi(-n)=\chi(n)$, dann ist $L(1,\chi) = -\frac{\tau(\chi)}{m} \sum_{(k,m)=1} \overline{\chi}(k) \log\left(\sin\frac{\pi k}{m}\right)$

und für ungerade χ $L(1,\chi) = -\frac{\pi i \tau(\chi)}{m^2} \sum_{(k,m)=1} \overline{\chi}(k)k$ und $\tau(\chi) = \sum_{(k,m)=1} \chi(k)\zeta_m^{\,k}$.

Satz: Sei K algebraischer Zahlkörper. Dann gibt es eine Konstante C=C(K) mit der folgenden Eigenschaft: Für alle $a \in K$ gibt es ein $x \in O_K$ und ein $r \in \mathbf{N}$ mit $r \leq C$, so daß $\left|N_{K/Q}(r \cdot a - x)\right| < 1$ ist.

Bew: $\omega_1,\ldots,\omega_n \in O_K$ Basis von K/Q (n=[K:Q])

$$C_1 = \max\left\{\left|N_{K/Q}(a_1\omega_1+\ldots+a_n\omega_n)\right|: |a_i| \leq 1,\ i=1,\ldots,n\right\}$$

$$C := [C_1^{1/n} + 2] \quad \left(\Rightarrow \frac{C_1}{C^n} < 1\right)$$

$$a \in K,\ r=0,1,2,\ldots,C^n: r \cdot a = \sum_{i=1}^n b_{i,r}\omega_i = \sum_{i=1}^n \{b_{i,r}\}\omega_i + \sum_{i=1}^n [b_{i,r}]\omega_i$$

$$\Rightarrow r \cdot a - b_r = \sum_{i=1}^n a_{i,r}\omega_i \text{ mit } b_r \in O_K,\ 0 \leq a_{i,r}$$

$$\Rightarrow \exists r_1,r_2: \left|a_{i,r_1} - a_{i,r_2}\right| \leq \frac{1}{C},\ i=1,\ldots,n \quad (\text{o.B.d.A. } r_1 > r_2)$$

$$r := r_1 - r_2 \Rightarrow 0 < r \leq C;\ x := b_{r_1} - b_{r_2} \in O_K$$

$$\Rightarrow |N(r \cdot a - x)| = |N((r_1-r_2)a - (b_{r_1} - b_{r_2}))| = |N(\sum_{i=1}^n (a_{i,r_1} - a_{i,r_2})\omega_i)| < \frac{C_1}{C^n} < 1$$

□

Satz: $|H(K)| < \infty$

Bew: $C=C(K)$, $S=\{J \subseteq O_K: J \mid C! \cdot O_K\} \Rightarrow |S| < \infty$

Beh: $\forall \neq I \subseteq O_K: \exists J \in S: I \cong J$ (d. h. $I \cdot J^{-1}$ ist HI.)

Bew: $\exists a \in I, a \neq 0: |N(a)| = \min\{|N(b)|: b \in I, b \neq 0\}\}$.

$\forall b \in I \; \exists r \leq C \; \exists c \in O_K: |N(r \cdot b - c \cdot a)| < |N(a)|$

$r \cdot b - c \cdot a \in I \Rightarrow r \cdot b - c \cdot a = 0 \Rightarrow a \mid r \cdot b \Rightarrow a \mid c! \cdot b$

$\Rightarrow a \cdot O_K \mid c! \cdot I \Rightarrow \exists J \subseteq O_K: c! \cdot I = a \cdot J \; (\Rightarrow I \cong J)$

$a \in I \Rightarrow c! \cdot a \in a \cdot J \Rightarrow c! \in J \Rightarrow J \mid c! \cdot O_K$

□