ALGEBRAISCHE ZAHLENTHEORIE

1. Teilbarkeitslehre in kommutativen Ringen

Def. Sei $(R,+,\cdot)$ ein Ring (d.h. $(R,+)$ ist kommutative Gruppe, $(R,\cdot)$ ist Halbgruppe und es gelten beide Distributivgesetze).
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, sodass $a\cdot b=0$ oder $b\cdot a=0$ gilt.
Ein kommutativer Ring mit 1, der keine von 0 verschiedene Nullteiler besitzt, heißt Integritätsring oder Integritätsbereich.

Def. Sei $(R,+,\cdot)$ ein Ring. Ein Untering $I\subseteq R$ 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 I heißt maximal, falls $I\neq R$ ist und es kein Ideal J mit $I\subsetneq J\subsetneq R$ gibt.
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 $I=a\cdot R$ $(=(a))$ (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 ausführlich $a\equiv b \pmod c$.)
Die Relation $\equiv$ induziert eine Äquivalenzrelation, die mit $+$ und $\cdot$ verträglich ist (Kongruenzrelation). Sind $[a]_I$, $[b]_I$ zwei Äquivalentklassen, 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.
(Die Äquivalentklasse $[a]_I$ kann auch durch $\{a\}+I$ bzw. durch $a+I$ beschrieben werden.)

Def. 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 ein Körper ist.

(ii) Ein Ideal I ist Primideal $\Leftrightarrow$ R/I ein Integritätsring ist.

(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.

Def. Sei $(R,+,\cdot)$ ein Integritätsbereich.

d heißt größter gemeinsamer Teiler von a und b, i.Z. $d=ggT(a,b)$ $=(a,b)$, falls $d|a$ und $d|b$ und für jeden gemeinsamen Teiler $t|a$, $t|b$ auch $t|d$ gilt.

R heißt Ring mit ggT, falls alle Paare $a,b\in R$ einen ggT haben.

Man sagt, R erfüllt die Teilerkettenbedingung, falls für jede unendliche Folge $a_1,a_2,\ldots\in R$ mit $a_{i+1}|a_i$ $(i\geq 1)$ ein $n\in\mathbb{N}$ existiert, sodaß 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 $a=q_1\cdots q_r=q_1'\cdots q_s'$ immer $r=s$ gilt und für eine Permutation π auf $\{1,\ldots,r\}$ $q_i=\varepsilon_i q'_{\pi(i)}$ (mit $\varepsilon_i\in R^*$) gilt.

R heißt euklidischer Ring, wenn es eine Gradfunktion $\delta: R\setminus\{0\}\to\{0,1,2,\ldots\}$ gibt, sodaß für alle $a,b\in R$, $b\neq 0$, stets Elemente $q,r\in R$ existieren, für welche $a=bq+r$ gilt, wobei entweder $r=0$ oder $\delta(r)<\delta(b)$ ist.

Satz. Sei $(R,+,\cdot)$ ein Integritätsbereich.

(i) Ein Hauptideal (a) ist genau dann Primideal, wenn $a=0$ oder a ein Primelement ist.

(ii) Ist R ein Ring mit ggT, so ist jedes irreduzibles Element prim.

(iii) R faktoriell $\Leftrightarrow$ R ist Ring mit ggT und erfüllt die Teilerkettenbed.

(iv) Jeder euklidische Ring ist Hauptidealring.

(v) Jeder Hauptidealring ist faktoriell.

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

2. Endliche Körpererweiterungen

Def. Ein Ring $(K,+,\cdot)$ heißt **Körper**, falls $(K\setminus\{0\},\cdot)$ eine abelsche Gruppe ist.

Def. Seien K, L 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.

Diese Dimension heißt **Erweiterungsgrad** $[L:K]$.

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

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

Def. 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.

Bem. 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 obige 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.

Def. 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.

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

Bem. Jede endliche Körpererweiterung L/K ist endlich erzeugt.

Def. Ein Körper E heißt <u>algebraisch abgeschlossen</u>, 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 E heißt <u>algebraischer Abschluß</u> $\bar{K}$. Der algebraische Abschluß $\bar{K}$ ist bis auf Isomorphie eindeutig bestimmt. Sind E und E' zwei algebraisch abgeschlossene, algebraische Erweiterungen von K, so gibt es einen Isomorphismus $\sigma: E \to E'$, der K elementweise festläßt.

<u>Konstruktion von Erweiterungskörpern</u>. 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 $[L:K] = \operatorname{grad} f(x) = \operatorname{grad} m_\alpha(x)$. Normiert man $f(x)$, so erhält man das Minimalpolynom $m_\alpha(x)$. Jede Erweiterung L' mit Erweitungsgrad $[L':K] = \operatorname{grad} f(x)$, in der $f(x)$ eine Nullstelle hat, ist bis auf Isomorphie (wo K elementweise festgelassen wird) eindeutig bestimmt.

Def. Ein Erweiterungskörper L/K heißt <u>Zerfällungskörper</u> eines Polynoms $f(x) \in K[x]$ (bzw eine Familie $f_i(x) \in K[x]$, $i \in I$), falls $f(x)$ (bzw f.a. $i \in I$ $f_i(x)$) über L in Linearfaktoren zerfällt:

$$f(x) = c(x-\alpha_1)\cdots(x-\alpha_n) \qquad \left(\text{bzw } f_i(x) = c_i(x-\alpha_{1,i})\cdots(x-\alpha_{n,i})\right)$$

und $L = K(\alpha_1, \dots, \alpha_n)$ $\left(\text{bzw. } L = K\left(\bigcup_{i\in I} \{\alpha_{1i}, \dots, \alpha_{n,i}\}\right)\right)$ gilt.
L/K heißt <u>normal</u>, falls L Zerfällungskörper eines Polynoms $f(x) \in K[x]$ (bzw...) ist.

Satz. Zu jedem Polynom $f(x) \in K[x]$ (bzw 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 dann und nur dann, wenn jedes irreduzible Polynom aus $K[x]$, das in L eine Wurzel (= Nullstelle) besitzt, über L in Linearfaktoren zerfällt.

Def. 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 $w_1, \dots, w_n$ eine Basis von L über K und sei $\alpha \cdot w_i = \sum_{j=1}^{n} a_{ij} w_j$, $a_{ij} \in K$, 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 w_i unabhängig. Die Determinante von (a_{ij}) heißt die Norm $N_{L/K}(\alpha) = \det(a_{ij})$ und die Spur von (a_{ij}) heißt Spur von α $Sp_{L/K}(\alpha) = \sum_{i=1}^{n} a_{ii}$.

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

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

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

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

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

Satz Sei $w_1, \dots, w_n$ eine Basis von L/K. Dann gilt

$$\det(Sp_{L/K}(w_i w_j)) \neq 0 \iff \exists \alpha \in L : Sp_{L/K}(\alpha) \neq 0.$$

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

$$\det\left(Sp_{L/K}(\alpha^{i+j-2})_{i,j=1,\dots,n}\right) = \prod_{0 \leq i < j \leq n-1} (\alpha_i - \alpha_j)^2.$$

($\alpha_0, \alpha_1, \dots, \alpha_{n-1}$ sind die Nullstellen von $m_\alpha(x)$.)

Def. Sei L/K eine endliche Erweiterung. $\alpha \in L$ heißt separabel, falls das Minimalpolynom $m_\alpha(x)$ 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 $\iff \exists \alpha \in L : Sp_{L/K}(\alpha) \neq 0$.

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

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

Def. 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 Fixpunktkörper von G ist, d.h. $K = \{a \in E \mid \sigma(a) = a \text{ für alle } \sigma \in G\}$. Überdies gilt $[E:K] = |G|$.

Def. Sei E/K eine Galoiserweiterung. Die Gruppe G aller Automorphismen σ auf E, die K elementweise festlassen heißt *Galoisgruppe* $\mathrm{Gal}_{E/K}$ der Galoiserweiterung E/K.

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

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 L/K ist einfach.

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

$$f_{\alpha}(x) = (x - \sigma_1(\alpha))(x - \sigma_2(\alpha)) \cdots (x - \sigma_n(\alpha))$$

besitzt. $\sigma_1(\alpha), \dots, \sigma_n(\alpha)$ sind die Konjugierten von α und $\sigma_i(L) = K(\sigma_i(\alpha))$ die konjugierten Körper von L. (α ist primitives Element von L).
Es gilt auch $N_{L/K}(\alpha) = \sigma_1(\alpha) \cdots \sigma_n(\alpha)$ und $\mathrm{Sp}_{L/K}(\alpha) = \sigma_1(\alpha) + \dots + \sigma_n(\alpha)$.

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

3. Endliche Körper

Def. Sei K ein Körper. Ist die additive Ordnung von 1 endlich, so ist sie die Charakteristik von K ($\mathrm{char}\, K$). Ist sie hingegen unendlich, so sei die Charakteristik von K Null.
Der Primkörper $P(K)$ ist der Durchschnitt aller Unterkörper von K.

Satz. Ist $\mathrm{char}(K) < \infty$, so ist sie eine Primzahl und der Primkörper ist isomorph zum Restklassenkörper $\mathbb{Z}/p\mathbb{Z}$. Ist hingegen $\mathrm{char}\, K = 0$, so ist der Primkörper isomorph zu $\mathbb{Q}$.

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

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 allen Nullstellen von $x^{p^n} - x$.) Man bezeichnet diesen Körper durch $\mathbb{F}_q$ oder $GF(q)$ ... Galois-Feld.

Folgerung. Über einem endlichen Körper $\mathbb{F}_q$ gibt es irreduzible Polynome beliebigen Grades.

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

$$\mathrm{Sp}_{L/K}(a) = a + a^q + \ldots + a^{q^{n-1}} \quad \text{und} \quad N_{L/K}(a) = a^{1+q+\ldots+q^{n-1}}.$$

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

4. Ganzalgebraische Zahlen

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

Def. Sei R Teilring eines Körpers K. Ein Element $\alpha \in K$ heißt **ganz (-algebraisch)** bezüglich R, wenn α Nullstelle eines normierten Polynoms mit Koeffizienten aus R ist.

Lemma. Sei $M \subseteq K$ ein endlich erzeugter R-Modul. (D.h. es gibt $w_1, \dots w_m \in K$, so daß $M = \{ a_1 w_1 + \dots + a_m w_m \mid a_1, \dots, a_m \in R \}$.) 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.

Def. 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 ganzabgeschlossene Hülle O von R in K ganzabgeschlossen in K.

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

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

Satz. Jeder faktorielle Ring ist ganzabgeschlossen.

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

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

Lemma. Sind $\alpha_1, \dots, \alpha_n$ und $\beta_1, \dots \beta_n$ Basen von L/K und $\alpha_i = \sum_{j=1}^{n} a_{ij} \beta_j$, dann gilt $\Delta(\alpha_1, \dots, \alpha_n) = \det(a_{ij})^2 \, \Delta(\beta_1, \dots, \beta_n)$.

Lemma. Sei $\alpha_1, \dots, \alpha_n \in L$ und L/K separabel. Dann ist

$$\Delta(\alpha_1, \dots, \alpha_n) = \det\left(a_i^{(j)}\right)^2,$$

wobei $\alpha_i^{(1)}, \dots, \alpha_i^{(n)}$ die Konjugierten von α_i bezeichnen.

Lemma. Seien $1, \beta, \dots, \beta^{n-1}$ l.u. in L/K und $m_\beta(x) \in K[x]$ das Minimalpolynom von β. Ist L/K separabel, dann gilt

$$\Delta(1, \beta, \dots, \beta^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{L/K}(m_\beta'(\beta)),$$

wobei $m_\beta'(x)$ die (formale) Ableitung von $m_\beta(x)$ bezeichnet.

Def. Sei $K \subseteq \mathbb{C}$ ein endlicher Erweiterungskörper von $\mathbb{Q}$. Dann heißt K <u>algebraischer Zahlkörper</u> und der ganzalgebraische Abschluß von $\mathbb{Z}$ in K heißt <u>Ring der ganzen Zahlen</u> O_K.

Lemma. Sei K alg. Zahlkörper und $\beta \in K$. Dann gibt es ein $b \in \mathbb{Z}, b \neq 0$, 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 $K/\mathbb{Q}$.

Satz. Sei K alg. Zahlkörper und I ein Ideal von O_K. Weiter sei $\alpha_1, \dots, \alpha_n \in I$ Basis von $K/\mathbb{Q}$, so daß $|\Delta(\alpha_1, \dots, \alpha_n)|$ minimal ist. Dann gilt $I = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \dots + \mathbb{Z}\alpha_n$, d.h. I ist freier endlicher $\mathbb{Z}$-Modul.

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

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 $A_1 \subseteq A_2 \subseteq \dots$ gibt es ein $N > 0$, so daß $A_m = A_{m+1}$ für alle $m \geq N$.

Folgerung. Jedes Primideal von O_K ist maximal

Bem. O_K ist i.a. nicht faktoriell. Beispielsweise sind in O_K für $K = \mathbb{Q}(\sqrt{-5})$ die Elemente $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ unzerlegbar, es gilt aber $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. Es gibt 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 $\alpha_1,\dots,\alpha_n$ und $\beta_1,\dots,\beta_n$ Basen (eines Ideals I von) $\mathcal{O}_K$, d.h. $I = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \dots + \mathbb{Z}\alpha_n = \mathbb{Z}\beta_1 + \mathbb{Z}\beta_2 + \dots + \mathbb{Z}\beta_n$, so sind die Diskriminanten gleich: $\Delta(\alpha_1,\dots,\alpha_n) = \Delta(\beta_1,\dots,\beta_n)$.

Def. Die **Diskriminante** ($\Delta(I)$) eines Ideals I von $\mathcal{O}_K$ ist die Diskriminante $\Delta(I) = \Delta(\alpha_1,\dots,\alpha_n)$ einer Basis $\alpha_1,\dots,\alpha_n$ von I.

Die **Diskriminante eines algebraischen Zahlkörpers** $K/\mathbb{Q}$ ist die Diskriminante von $\mathcal{O}_K$: $\delta_K = \Delta(\mathcal{O}_K)$.

5. Der chinesische Restsatz

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

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

Bem. 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 $I_1,\dots,I_n$ paarweise teilerfremd, so gilt $I_1\cdots I_n = I_1\cap\dots\cap I_n$.

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

$$\begin{aligned} x &\equiv a_1 \pmod{I_1} \\ &\vdots \\ x &\equiv a_n \pmod{I_n} \end{aligned}$$

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

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

6 Dedekindsche Ringe

Def. Ein kommutativer Ring mit 1 heißt **Noethersch**, wenn jede aufsteigende Kette von Idealen $I_1 \subseteq I_2 \subseteq \dots$ endlich ist, d.h. es gibt ein N, sodass für $m \geq N$ immer $I_m = I_N$ gilt.

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

Def. Ein Integritätsring R heißt **Dedekindscher Ring**, falls folgende drei Eigenschaften erfüllt sind.

(i) R ist Noethersch

(ii) Jedes Primideal $I \neq 0$ von R ist maximal

(iii) R ist ganzalgebraisch abgeschlossen.

Def. Sei R ein Integritätsring und K sein Quotientenkörper. Ein R-Modul $I \neq 0$, $I \subseteq K$, heißt **Bruchideal** (von K), wenn es ein $a \in R$, $a \neq 0$, gibt, sodass $aI \subseteq R$ gilt.

Ein Bruchideal I heißt **invertierbar**, falls für $I' = \{x \in K \mid xI \subseteq R\}$ (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 $P_1, \dots, P_r$ von R mit $P_1 \cdots P_r \subseteq I \subseteq P_1 \cap \dots \cap P_r$.

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 abelsche Gruppe, die von den Primidealen erzeugt wird.

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

Def. 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 jeden 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 $C \subseteq R$ mit $A = BC$ 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 des Dedekindschen Ringes R. Dann gilt

$$R/I = R/P_1^{a_1} \oplus \cdots \oplus R/P_k^{a_k},$$

falls I die Darstellung $I = P_1^{a_1} \cdots P_k^{a_k}$ 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 P^n/P^{n+1} isomorph.

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

(ii) Für alle $T \geq 0$ ist die Menge $\{0 \neq I \subseteq R \mid N(I) \leq T\}$ 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

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

Satz. Sei p eine Primzahl in $\mathbb{Z}$ und K ein algebraischer Zahlkörper vom Grad n. Gilt nun $(p) = p\cdot\mathcal{O}_K = P_1^{e_1} \dots P_g^{e_g}$ und bezeichnen f_i die Trägheitsindizes von P_i, so gilt:

$$\sum_{i=1}^{g} e_i f_i = n .$$

Satz Sei F eine endliche Galoserweiterung von $\mathbb{Q}$ vom Grad n und $p \in \mathbb{Z}$ eine Primzahl. Dann gilt $(p) = p\cdot\mathcal{O}_K = P_1^{e_1} \dots P_g^{e_g}$ mit $e_1 = e_2 = \dots = e_g$ und $f_1 = f_2 = \dots = f_g$. 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 $\alpha \in K$, sodass $\mathcal{O}_K = \mathbb{Z}[\alpha]$ ist. Sei $f(X) = m_\alpha(X)$ das Minimalpolynom von α. (Da α ganzalgebraisch ist, ist $m_\alpha(X)$ ganzzahlig.) Weiters sei $p \in \mathbb{Z}$ eine Primzahl und $\overline{f}(X) = \overline{G_1(X)}^{e_1} \dots \overline{G_g(X)}^{e_g}$ die Zerlegung in irreduzible Faktoren von $f(X)$ modulo p. O.Bd.A sei $\overline{G_i}(X)$ als normiert angenommen. Bezeichne $G_i(X) \in \mathbb{Z}[X]$ ein normiertes Polynom mit $G_i(X) \pmod p = \overline{G_i}(X)$. Dann sind $P_i = p\cdot\mathcal{O}_K + G_i(\alpha)\cdot\mathcal{O}_K$ Primideale von $\mathcal{O}_K$ mit

$$(p) = p\cdot\mathcal{O}_K = P_1^{e_1} \dots P_g^{e_g} .$$

e_i ist der Verzweigungsindex von P_i und $f_i = \operatorname{grad} G_i(X)$ der Trägheitsindex von P_i.

Def. 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) $h(K) = 1 \Leftrightarrow \mathcal{O}_K$ ist Hauptidealring $\Leftrightarrow \mathcal{O}_K$ 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 $x \in \mathcal{O}_K$ und ein $r \in \mathbb{N}$ mit $r \leq c$, sodaß $|N_{K/\mathbb{Q}}(ra - x)| < 1$ ist.

8. Der Dirichletsche Einheitensatz

Def. Sei K alg. Zahlkörper und $\sigma_1(K), \dots, \sigma_s(K), \sigma_{s+1}(K), \dots, \sigma_{s+t}(K), \overline{\sigma}_{s+1}(K), \dots, \overline{\sigma}_{s+t}(K)$ die konjugierten Körper von K, wobei $\sigma_1(K), \dots, \sigma_s(K) \subseteq \mathbb{R}$ und $\sigma_{s+1}(K), \dots, \sigma_{s+t}(K) \not\subseteq \mathbb{R}$ gelten ($s + 2t = n$). Dann heißt das Paar $[s,t]$ Signatur von K.

Bem. Für jedes Paar $[s,t]$ von nicht-negativen Zahlen mit $n = s + 2t \geq 1$ gibt es einen alg. Zahlkörper mit dieser Signatur.

Satz (Dirichlet). Sei K alg. Zahlkörper mit Signatur $[s,t]$. Dann gibt es $r = s + t - 1$ Einheiten $\varepsilon_1, \dots, \varepsilon_r \in \mathcal{O}_K$, sodaß sich jede Einheit $\varepsilon \in \mathcal{O}_K$ eindeutig in der Form

$$\varepsilon = \zeta \varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r}$$

darstellen läßt, wobei $a_1, \dots, a_r$ ganze Zahlen sind und ζ eine in $\mathcal{O}_K$ enthaltene Einheitswurzel ist. Die Einheitswurzeln in $\mathcal{O}_K$ bilden eine zyklische Gruppe gerader Ordnung. Demnach ist die Einheitengruppe von $\mathcal{O}_K$ direktes Produkt einer endlichen zyklischen Gruppe gerader Ordnung und $r = s + t - 1$ zyklischer Gruppen unendlicher Ordnung. Die erzeugenden Einheiten $\varepsilon_1, \dots, \varepsilon_r$ heißen Grundeinheiten.

Def. Seien $a_1, \dots, a_m \in \mathbb{R}^n$ m l.u. Vektoren über $\mathbb{R}$. Dann heißt die davon erzeugte freie abelsche Gruppe $G = G(a_1, \dots, a_m) = \left\{ \sum_{i=1}^{m} k_i a_i \mid k_i \in \mathbb{Z} \right\}$ m-dimensionales Gitter des $\mathbb{R}^n$. Ist $m = n$, so spricht man auch von einem (vollständigen) Gitter. Die Menge

$$P = \left\{ \sum_{i=1}^{n} x_i a_i \mid 0 \leq x_i < 1 \right\}$$

heißt Fundamentalparallelepiped der Gitterbasis $a_1, \dots, a_m$ und das Volumen von P

$$\operatorname{Vol} P = |\det(a_1, \dots, a_n)| = d(G)$$

Gitterkonstante von G. (Die Gitterkonstante ist von der Wahl der Gitterbasis unabhängig.)

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

Def. Sei K alg. Zahlkörper mit Signatur $[s,t]$. Bezeichnen $\sigma_1,\dots,\sigma_s$ die reellen und $\sigma_{s+1}, \overline{\sigma_{s+1}}, \dots, \sigma_{s+t}, \overline{\sigma_{s+t}}$ die komplexen Einbettungen von K in $\mathbb{C}$, so kann jedem $\alpha \in K$ ein

$$x(\alpha) = (\sigma_1(\alpha),\dots,\sigma_s(\alpha),\sigma_{s+1}(\alpha),\dots,\sigma_{s+t}(\alpha)) \in \mathbb{R}^s \times \mathbb{C}^t \cong \mathbb{R}^{s+2t} = \mathbb{R}^n$$

zugeordnet werden. Das ist die geometrische Darstellung des Körpers K im $\mathbb{R}^n$.

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

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

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

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

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

Lemma (i) $\varepsilon \in \mathcal{O}_K$ ist Einheit $\Leftrightarrow |N_{K/\mathbb{Q}}(\varepsilon)| = 1$

(ii) Die Einheiten ε von $\mathcal{O}_K$ mit $l(\varepsilon) = 0$ bilden eine zyklische Gruppe gerader Ordnung und sind genau die Einheitswurzeln in $\mathcal{O}_K$.

(iii) Die Gesamtheit der Bilder $l(\varepsilon)$ von Einheiten von $\mathcal{O}_K$ bilden ein Gitter der Dimension $\leq s+t-1$.

Satz von Blichfeld. Zu jedem Gitter G und jeder nichtleeren, beschränkten, integrierbaren Menge $M \subseteq \mathbb{R}^n$ kann man einen Punkt P angeben, sodaß die Anzahl der Gitterpunkte des von P ausgehenden Punktgitters $P+G$ innerhalb der Menge M mindestens $\geq \mathrm{Vol}(M)/d(G)$ beträgt.

Gitterpunktsatz von Minkowski. Sei K eine um 0 symmetrische, beschränkte und konvexe Menge im $\mathbb{R}^n$ 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 $\mathbb{R}^n \cong \mathbb{R}^s \times \mathbb{C}^t$ $(n = s+2t)$ und gelte für $c_1,\dots,c_{s+t} > 0$ die Ungleichung $c_1 c_2 \cdots c_{s+t} > (4/\pi)^t \cdot d(G)$, so gibt es in G einen von 0 verschiedenen Punkt $(x_1,\dots,x_{s+t}) \in \mathbb{R}^s \times \mathbb{C}^t$ mit $|x_i| < c_i$.

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

9. Quadratische Zahlkörper

Def. Ein alg. Zahlkörper K mit $[K:\mathbb{Q}]=2$ heißt quadratisch

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

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

$$\mathcal{O}_K=\mathbb{Z}+\mathbb{Z}\sqrt{d},\quad \delta_K=4d \quad \text{für } d\equiv 2,3 \pmod 4 \text{ und}$$

$$\mathcal{O}_K=\mathbb{Z}+\mathbb{Z}\left(\frac{-1+\sqrt{d}}{2}\right),\quad \delta_K=d \quad \text{für } d\equiv 1 \pmod 4.$$

Satz. Jede quadratische Körpererweiterung von $\mathbb{Q}$ ist Galois.

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

(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) $p\mid \delta_K \Rightarrow (p)=P^2$.

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) $2\mid \delta_K$, $\Rightarrow (2)=P^2$.

Def. Ein Polynom der Form $f(x,y)=ax^2+bxy+cy^2$ mit $a,b,c\in\mathbb{Z}$ heißt quadratische Form. $\delta(f)=b^2-4ac$ ist ihre Diskriminante. $f(x,y)$ heißt primitiv, falls $\operatorname{ggT}(a,b,c)=1$ ist. 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 $\delta(f_1)=\delta(f_2)$.

Def. Sei $d\in\mathbb{Z}$, $d\neq 0$. 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 $d < 0$

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

Satz. Sei $d < 0$ Diskriminante eines imaginär quadratischen Körpers $K = \mathbb{Q}(\sqrt{-d})$. Für jedes Ideal $I \trianglelefteq \mathcal{O}_K$, dargestellt in der Form $I = \mathbb{Z}a_1 \oplus \mathbb{Z}a_2$, wobei man o.B.d.A annehmen kann, daß $\operatorname{Im}(a_1\bar{a}_2 - \bar{a}_1 a_2) > 0$ ist, stelle man eine quadratische Form

$$f_{a_1 a_2}(x,y) = \frac{1}{N(I)} N_{K/\mathbb{Q}}(a_1 x + a_2 y)$$

auf. Für diese gilt:

(i) $f_{a_1 a_2}(x,y)$ ist eine primitive, positiv definite, quadratische Form mit ganzzahligen Koeffizienten und Diskriminante d.

(ii) Zwei Ideale $I = \mathbb{Z}a_1 \oplus \mathbb{Z}a_2$, $J = \mathbb{Z}b_1 \oplus \mathbb{Z}b_2$ sind genau dann in derselben Idealklasse, wenn die quadratischen Formen $f_{a_1 a_2}(x,y)$, $f_{b_1 b_2}(x,y)$ äquivalent sind.

(iii) Die Zuordnung $f_{a_1 a_2} \longmapsto$ (Klasse von $I = \mathbb{Z}a_1 \oplus \mathbb{Z}a_2$) induziert eine Bijektion zwischen der Menge aller Klassen primitiver, positiv definiter, quadratischer Formen mit Diskriminante d und der Idealklassengruppe $H(K)$

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

$$\{ f_{a_1 a_2}(x,y) \mid x,y \in \mathbb{Z} \} = \{ N(J) \mid J \in X^{-1} \}$$

und

$$\left| \{ J \in X^{-1} \mid N(J) = m \} \right| = \frac{1}{\varepsilon(d)} \sum_{\substack{x,y \\ f_{a_1 a_2}(x,y) = m}} 1 ,$$

wobei

$$\varepsilon(d) = \begin{cases} 6 & \text{für } d = -3 \\ 4 & \text{für } d = -4 \\ 2 & \text{für } d \neq -3, -4 \end{cases}$$

(bzl. ($\varepsilon(d)$ ist die Anzahl der Einheitswurzeln in K)

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

Satz Sei $d < 0$ Diskriminante eines imaginär quadratischen Körpers. Dann gilt

$$h(\mathbb{Q}(\sqrt{d})) = h(d) .$$

Def. 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) $d = \varepsilon p_1 \cdots p_r \equiv 1\,(4)$, $\varepsilon = \pm 1$, $r \geq 1$, p_i ungerade Primz.

(b) $d = 4\varepsilon p_1 \cdots p_r$, $\varepsilon p_1 \cdots p_r \equiv 3\,(4)$, $r \geq 0$ —u—

(c) $d = 8\varepsilon p_1 \cdots p_r$, $r \geq 0$, 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 Falle (b) $\left(\frac{d}{n}\right) = \begin{cases} \eta \cdot \prod_{i=1}^{r} \left(\frac{n}{p_i}\right), & \text{wobei } \eta = \begin{cases} 1 & \text{für } n \equiv 1\,(4) \\ -1 & \text{für } n \equiv -1\,(4) \end{cases} \\ 0 & \text{f. } n \equiv 0\,(2) \end{cases}$

und im Falle (c)

$$\left(\frac{d}{n}\right) = \begin{cases} (-1)^{(n^2-1)/8} \prod_{i=1}^{r} \left(\frac{n}{p_i}\right), & \text{falls } \operatorname{sgn}(d) = \prod_{i=1}^{r} \left(\frac{-1}{p_i}\right) \\ \eta \cdot (-1)^{(n-1)/8} \prod_{i=1}^{r} \left(\frac{n}{p_i}\right), & \text{falls nicht.} \\ 0 \quad \text{f. } n \equiv 0\,(2) \end{cases} \Bigg\} \; n \equiv 1\,(2)$$

Für jedes diese d betrachte man weiters die **L-Reihe**

$$L_d(s) = \sum_{n=1}^{\infty} \frac{\left(\frac{d}{n}\right)}{n^s} \qquad (\operatorname{Re} s > 0).$$

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

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

Satz. Für $d < 0$ gilt $\lim_{d \to -\infty} \log h(\mathbb{Q}(\sqrt{d})) / \log |d|^{1/2} = 1$. ($d$ Diskrim.)

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

Satz. Für $d > 0$ gilt $\lim_{d \to \infty} \log h(\mathbb{Q}(\sqrt{d})) / \log |d|^{1/2} = 1$. ($d$ Diskrim.)

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

Satz. Sei K alg. Zahlkörper. Dann gibt es eine Konstante $C = C(K)$ mit der folgenden Eigenschaft: Für alle $a \in K$ gibt es ein $x \in \mathcal{O}_K$ und ein $r \in \mathbb{N}$ mit $r \le C$, sodass $|N_{K/\mathbb{Q}}(r \cdot a - x)| < 1$ ist.

Beweis. $\omega_1, \dots, \omega_n \in \mathcal{O}_K$ Basis von $K/\mathbb{Q}$ $(n = [K:\mathbb{Q}])$

$$C_1 = \max \{ |N_{K/\mathbb{Q}}(a_1\omega_1 + \dots + a_n\omega_n)| : |a_i| \le 1, i = 1, \dots, n \}$$

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

$a \in K$, $r = 0, 1, 2, \dots, C^n$: $r \cdot a = \sum_{i=1}^{n} b_{i,r}\omega_i = \sum_{i=1}^{n} \{b_{i,r}\}\omega_i + \underbrace{\sum_{i=1}^{n} [b_{i,r}]\omega_i}_{b_r \in \mathcal{O}_K}$

$$\Rightarrow r \cdot a - b_r = \sum_{i=1}^{n} a_{i,r}\omega_i \text{ mit } b_r \in \mathcal{O}_K,\ 0 \le a_{i,r} < 1$$

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

$r := r_1 - r_2 \Rightarrow 0 < r \le C$; $x := b_{r_1} - b_{r_2} \in \mathcal{O}_K$

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

□

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

Beweis. $C = C(K)$, $S = \{ \mathfrak{J} \trianglelefteq \mathcal{O}_K : \mathfrak{J} \mid C! \cdot \mathcal{O}_K \} \Rightarrow |S| < \infty$

Beh. $\forall\, 0 \ne \mathfrak{I} \trianglelefteq \mathcal{O}_K\ \exists\, \mathfrak{J} \in S : \mathfrak{I} \cong \mathfrak{J}$ (d.h. $\mathfrak{I}\mathfrak{J}^{-1}$ ist H.I.)

Beweis. $\exists\, a \in \mathfrak{I}, a \ne 0 : |N(a)| = \min \{ |N(b)| : b \in \mathfrak{I}, b \ne 0 \}$.

$$\forall b \in \mathfrak{I}\ \exists r \le C\ \exists c \in \mathcal{O}_K : |N(r \cdot b - c \cdot a)| < |N(a)|$$

$r \cdot b - c \cdot a \in \mathfrak{I} \Rightarrow rb - ca = 0 \Rightarrow a \mid a \cdot b \Rightarrow a \mid C! \cdot b$

$\Rightarrow a \cdot \mathcal{O}_K \mid C! \cdot \mathfrak{I} \Rightarrow \exists\, \mathfrak{J} \trianglelefteq \mathcal{O}_K : C! \cdot \mathfrak{I} = a \cdot \mathfrak{J}$ $\left(\Rightarrow \mathfrak{I} \cong \mathfrak{J} \right)$

$a \in \mathfrak{I} \Rightarrow C! \cdot a \in a \cdot \mathfrak{J} \Rightarrow C! \in \mathfrak{J} \Rightarrow \mathfrak{J} \mid C! \cdot \mathcal{O}_K$ □

Satz $H \leq \mathbb{Z}^n \Rightarrow H \cong \mathbb{Z}^m$, $m \leq n$.

Bew. $n=1$: $H \leq \mathbb{Z}$

1. Fall: $H = \{0\} \Rightarrow H \cong \mathbb{Z}^0$

2. Fall: $\exists\ k := \min\{l \in H \mid l > 0\}$

·) $H \supseteq k\cdot\mathbb{Z}$ (offensichtlich)

·) $H \subseteq k\mathbb{Z}$: $x \in H \Rightarrow \exists q, r \in \mathbb{Z}: x = q\cdot k + r$, $0 \leq r < k$

$r = -q\cdot k + x \in H \Rightarrow r = 0 \Rightarrow x = q\cdot k$

$\Rightarrow x \in k\cdot\mathbb{Z}$

$\Rightarrow H = k\mathbb{Z} \cong \mathbb{Z}^1$.

$n-1 \to n$: $H \leq \mathbb{Z}^n$

$$U_1 := \{l \in \mathbb{Z} \mid \exists\, l_2, \dots, l_n \in \mathbb{Z}: (l, l_2, \dots, l_n) \in H\}$$

$$U_2 := \{(0, l_2, \dots, l_n) \in \mathbb{Z}^n \mid \exists\, l \in \mathbb{Z}: (l, l_2, \dots, l_n) \in H\}$$

$U_1 \leq \mathbb{Z}$, $U_2 \leq \{0\} \times \mathbb{Z}^{n-1} \cong \mathbb{Z}^{n-1} \Rightarrow U_2 \cong \mathbb{Z}^{m'}$, $m' \leq n-1$

1. Fall $U_1 = \{0\} \Rightarrow U_2 = H \cong \mathbb{Z}^{m'}$, $m' \leq n-1 < n$.

2. Fall $U_1 = k\mathbb{Z}$, $k > 0$

$k \in U_1 \Rightarrow \exists\, (\bar{l}_2, \dots, \bar{l}_n): (k, \bar{l}_2, \dots, \bar{l}_n) \in H$

$U_1 := (k, \bar{l}_2, \dots, \bar{l}_n)\cdot\mathbb{Z} \leq \mathbb{Z}^n$

·) $U_1 \cap U_2 = \{0\}$: $x = (l_1, \dots, l_n) \in U_1 \cap U_2$

$\Rightarrow l_1 = 0 \wedge \exists q \in \mathbb{Z}: (l_1, \dots, l_n) = q\cdot(k, \bar{l}_2, \dots, \bar{l}_n)$

$\Rightarrow q = 0 \Rightarrow x = (0, \dots, 0)$

·) $U_1 + U_2 = H^n$: $x = (l_1, \dots, l_n) \in H^n \Rightarrow \exists q \in \mathbb{Z}: l_1 = q\cdot k$

$\Rightarrow x - q\cdot(k, \bar{l}_2, \dots, \bar{l}_n) = (0, l_2 - q\bar{l}_2, \dots, l_n - q\bar{l}_n) \in U_2 \Rightarrow x \in U_1 + U_2$

$\Rightarrow H \subseteq U_1 \times U_2 \cong \mathbb{Z} \times \mathbb{Z}^{m'} \cong \mathbb{Z}^{m'+1}$, $m'+1 \leq n-1+1 = n$. ■

ALGEBRAISCHE ZAHLENTHEORIE ÜBUNGEN

1) Man zeige: Sei R ein Integritätsbereich und $I \subsetneq R$ ein Ideal. Dann ist R/I ein Körper dann und nur dann, wenn I maximal ist.

2) Man zeige: ~~Sei R ein ZPE-Ring. Dann ist dort~~ Ein Hauptideal (a) ist prim genau dann, wenn $a=0$ ist oder a prim ist.

3) Man zeige: Ist R ein ZPE-Ring, so auch $R[x]$.
(Aul: Man betrachte den Quotientenkörper)

4) Man beweise für $K \subseteq L \subseteq E$

$$Sp_{E|K}(\alpha) = Sp_{L|K}(Sp_{E|L}(\alpha)) \text{ und } N_{E|K}(\alpha) = N_{L|K}(N_{E|L}(\alpha)).$$

5) Man zeige: $f(x) \in K[x]$ hat genau dann keine mehrfachen Nullstellen, wenn $f(x)$ und $f'(x)$ teilerfremd sind. $\left(f(x) = \sum_{k=0}^{n} a_k x^k, f'(x) = \sum_{k=1}^{n} k a_k x^{k-1} \right)$.
Ist $f(x)$ irreduzibel, so ist dies genau dann der Fall, wenn $f'(x)$ nicht das Nullpolynom ist.

6) Man bestimme ein primitives Element ϑ des Zahlkörpers $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ und drücke $\sqrt{2}$ und $\sqrt{3}$ durch ϑ aus.

7) Sei L der Zerfällungskörper von $f(x) = x^2 - 2$ über $K = \mathbb{Q}$. Man bestimme die Galoissche Gruppe von L/K und ihre Untergruppen

8) Sei K ein Körper mit $\operatorname{char} K \neq 0$. Man zeige, daß das Polynom $f(x) = x^p - x - a$ $(a \in K)$ entweder in K vollständig in Linearfaktoren zerfällt oder irreduzibel ist. Im zweiten Fall zeige man, daß $f(x)$ separabel ist.

9) Man zeige: Sei E/K eine endliche Galoiserweiterung und L ein Zwischenkörper. Dann ist nur dann L/K eine Galoiserweiterung, wenn die zu L korrespondierende Untergruppe U von der Galoisgruppe $G = \mathrm{Gal}_{E/K}$ ein Normalteiler von G ist. Weiter gilt $\mathrm{Gal}_{L/K} \cong G/U$.

10) Man zeige mit Hilfe einer geeigneten Galoisgruppe, daß es keine $x, y, u, v \in \mathbb{Q}$ mit

$$(x + y\sqrt{2})^4 + (u + v\sqrt{2})^4 = 1 + \sqrt{2}$$

geben kann.

11) Sei K ein Körper der Charakteristik $\mathrm{cha}(K) = 0$ und α algebraisch über K. Dann bezeichne

$$R(\alpha) = \frac{Sp_{K(\alpha)/K}(\alpha)}{[K(\alpha):K]}$$

den Rationalteil von α. Man zeige, daß R K-linear ist, d.h. es gilt $R(\lambda_1\alpha + \lambda_2\beta) = \lambda_1 R(\alpha) + \lambda_2 R(\beta)$ für $\lambda_1, \lambda_2 \in K$ und α, β algebraisch über K.

12) Seien $k_1, \dots, k_\ell \geq 2$ natürliche Zahlen und a_i $(i = 1, \dots, \ell)$ natürliche Zahlen, die keine k_i-ten Potenzen in $\mathbb{Z}$ sind. Dann gilt

$$\sqrt[k_1]{a_1} + \dots + \sqrt[k_\ell]{a_\ell} \notin \mathbb{Q}.$$

(Hinweis: Man berechne den Rationalteil)

13) Sei $\mathbb{F}_q$ endlicher Körper und bezeichne $\psi(n)$ die Anzahl der verschiedenen (normierten) irreduziblen Polynome vom Grade n über $\mathbb{F}_q$. Dann gilt

$$\sum_{d \mid n} d \cdot \psi(d) = q^n \qquad \left(\text{bzw. } \psi(n) = \frac{1}{n} \sum_{d \mid n} \mu(d)\, q^{\frac{n}{d}} \right)$$

(Hinweis: Man zerlege $x^{q^n} - x$ in irreduzible Faktoren.)

14) Sei $q = p^n$ und $\mathbb{F}_q$ endlicher Körper. Man zeige, daß es genau $\varphi(q-1)$ erzeugende Elemente der multiplikativen Gruppe gibt. Man folgere daraus, daß immer $n \mid \varphi(p^n - 1)$ gilt.

($\varphi(m)$ ist die Eulersche φ-Funktion. Sie bezeichnet die Anzahl der zu m teilerfremden Zahlen zwischen 1 und m. $\varphi(m) = m \cdot \prod_{p \mid m} (1 - \frac{1}{p})$.)

15) Man zeige: Seien $1, \beta, \dots, \beta^{n-1}$ l.u. in L/K und $m_\beta(x) \in K[x]$ das Minimalpolynom von β. Ist L/K separabel, dann gilt

$$\Delta(1, \beta, \dots, \beta^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{L/K}(m'_\beta(\beta)),$$

wobei $m'_\beta(x)$ die (formale) Ableitung von $m_\beta(x)$ bezeichnet.

16) Man bestimme eine Ganzheitsbasis (d.h. eine Basis des Ringes der ganzalg. Zahlen) und die Diskriminante des Körpers $K = \mathbb{Q}(\rho)$, wobei ρ eine Wurzel der Gleichung $x^3 - x - 1 = 0$ ist.

17) Man zeige, daß $1, \theta, \frac{\theta + \theta^2}{2}$ eine Ganzheitsbasis des kubischen Körpers $\mathbb{Q}(\theta)$, $\theta^3 - \theta - 4 = 0$ ist.

18) Seien a und b teilerfremde quadratfreie natürliche Zahlen, sodaß $a^2 \equiv b^2 \pmod 8$ gilt. Man zeige, daß die Diskriminante von $\mathbb{Q}(\sqrt[3]{ab^2})$ gleich $\delta = -3a^2b^2$ ist.

19) Man zeige, im Körper $K = \mathbb{Q}(\sqrt[3]{2})$ jede Einheit (von O_K) die Form $\pm(1 + \sqrt[3]{2})^k$ hat.

20) Man zeige, daß im kubischen Körper $K = \mathbb{Q}(\sqrt[3]{6})$ keine Zahl α der Form $\alpha = x + y\sqrt[3]{6} \neq 0$ mit teilerfremden ganzen x, y existiert, für die $N_{K/\mathbb{Q}}(\alpha) = 10z^3$ mit $z \in \mathbb{Z}$ gilt. Daraus folgere man, daß die Gleichung $x^3 + 6y^3 = 10z^3$ (und daher die Gleichung $3x^3 + 4y^3 + 5z^3 = 0$) keine nichttriviale Lösung in ganzen Zahlen hat.

21) Sei $d \neq 1$ eine quadratfreie ganze Zahl. Man zeige, daß für die quadratischen Zahlkörper $K = \mathbb{Q}(\sqrt{d})$

$$O_K = \begin{cases} \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\} & \text{für } d \equiv 2, 3 \pmod 4 \\ \left\{\frac{a + b\sqrt{d}}{2} \mid a, b \in \mathbb{Z}\right\} & \text{für } d \equiv 1 \pmod 4 \end{cases}$$

gilt.

22) Man zeige: Sei R kommutativer Ring. Dann lässt sich jedes symmetrische Polynom $f(x_1,\dots,x_n) \in R[x_1,\dots,x_n]$ eindeutig als Polynom $f(x_1,\dots,x_n) = g(s_1,\dots,s_n)$ in den elementar-symmetrischen Polynomen

$$s_1(x_1,\dots,x_n) = x_1 + x_2 + \cdots + x_n$$
$$s_2(x_1,\dots,x_n) = x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n = \sum_{1\le i<j\le n} x_i x_j$$
$$\vdots$$
$$s_k(x_1,\dots,x_n) = \sum_{1\le i_1<i_2<\cdots<i_k\le n} x_{i_1}x_{i_2}\cdots x_{i_k}$$
$$\vdots$$
$$s_n(x_1,\dots,x_n) = x_1x_2\cdots x_n$$

darstellen, wobei $g(y_1,\dots,y_n) \in R[y_1,\dots,y_n]$ ist. (Ein Polynom heißt symmetrisch, wenn für alle Permutationen $\pi \in S_n$

$$f(x_{\pi(1)},\dots,x_{\pi(n)}) = f(x_1,\dots,x_n)$$

gilt.)

Hinweis: (i) Zurückführen des Problems auf homogene Polynome

(ii) Man ordne die Summanden eines homogenen symmetrischen Polynoms lexikographisch. Der größte Summand sei $a\cdot x_1^{m_1}x_2^{m_2}\cdots x_n^{m_n}$ $(m_1 \ge m_2 \ge \dots \ge m_n)$. Man subtrahiere $a\cdot s_1^{m_2-m_1}\cdot s_2^{m_3-m_2}\cdots s_n^{m_n}$ und iteriere dieses Verfahren.

23) Sei $K = \mathbb{Q}(\sqrt[3]{2})$. Man faktorisiere das Ideal $I = 5\cdot O_K$ vollständig in Primideale von O_K.

24) Sei R ein Dedekindscher Ring und K sein Quotientenkörper. Man zeige, dass dann der ganzalgebraische Abschluss von R in einer endlichen separablen Erweiterung L von K wieder ein Dedekindscher Ring ist. Gilt überdies, dass für jedes Ideal $I \neq 0$ von R der Faktorring R/I endlich ist, so gilt diese Eigenschaft auch für den ganzalgebraischen Abschluss von R in L.

25) Man beweise: Sei G eine Gruppe und $K \subseteq H$ zwei Normalteiler von G. Dann gilt

$$G/K \Big/ H/K \cong G/H.$$

26) Man beweise: Gibt es in einem Dedekindschen Ring R nur endlich viele Primideale, dann ist R Hauptidealring.
(Hinweis: sei $I = P_1^{r_1} \cdots P_s^{r_s}$ und $x_i \in P_i^{r_i} \setminus P_i^{r_i+1}$. Man betrachte $x \in R$, das $x \equiv x_i \, (P_i^{r_i+1})$ erfüllt und zeige $I = xR$.)

27) Man beweise: In einem Dedekindschen Ring R wird jedes Ideal I von höchstens zwei Elementen erzeugt, d.h. $\exists\, x, y$ mit $R = xI + yI$. (Hinweis: Seien I und x_i wie oben und J ein zu I teilerfremdes Ideal, $x \equiv x_i \, (P_i^{r_i+1})$, $x \equiv 1 \, (J)$, $xR = I \cdot I_2$, und $y \equiv x_i \, (P_i^{r_i+1})$, $y \equiv 1 \, (I_2)$.)

28) Man zeige: Sei R Dedekindscher Ring und sei $N(I) < \infty$ für alle $I \neq 0$. Dann ist die Ordnung der Einheitengruppe von R/I durch

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

gegeben. (Hinweis: Man verwende den Chinesischen Restsatz und die Eigenschaft $\varphi(P^n) = N(P^n) - N(P^n)/N(P) = N(P^n) - N(P^{n-1})$.)

29) Man zeige: Für jedes Paar $[s,t]$ von nicht-negativen Zahlen mit $n = s + 2t \geq 1$ gibt es einen algebraischen Zahlkörper mit der Signatur $[s,t]$.

30) Sei $K = \mathbb{Q}(\theta)$, $\theta^3 = 6$. Man zeige, daß $\varepsilon = 1 - 6\theta + 3\theta^2$ Grundeinheit in K ist.

31) Sei K alg. Zahlkörper mit Signatur $[s,t]$ und Grad $n = s + 2t$. Man zeige, daß es Einheiten $\eta_1, \ldots, \eta_r$ ($r = s + t - 1$) Einheiten in $\mathcal{O}_K$ gibt, sodaß sich alle $a \in \mathcal{O}_K$ mit Norm $N_{K/\mathbb{Q}}(a) = \pm 1$ eindeutig in der Form

$$a = \zeta \eta_1^{a_1} \cdots \eta_r^{a_r}$$

darstellen lassen, wobei $a_i \in \mathbb{Z}$ und ζ Einheitswurzel in $\mathcal{O}_K$ ist.

32) Sei K alg. Zahlkörper und $F(m) = |\{0 \neq I \trianglelefteq \mathcal{O}_K : N(I) = m\}|$.
Man zeige, daß für teilerfremde m, n $F(mn) = F(m) \cdot F(n)$ gilt.

$f(x,y) = ax^2 + bxy + cy^2$ mit $a, b, c \in \mathbb{Z}$ heißt quadratische Form, sie heißt primitiv, wenn $ggT(a,b,c) = 1$ ist und $d(f) = b^2 - 4ac$ ist ihre Diskriminante. $f_1(x,y) = a_1x^2 + b_1xy + c_1y^2$ und $f_2(x,y) = a_2x^2 + b_2xy + c_2y^2$ heißen equivalent, wenn es eine Matrix $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ mit $AD - BC = \pm 1$ $(A, B, C, D \in \mathbb{Z})$ gibt, sodaß $f_1(Ax + By, Cx + Dy) = f_2(x,y)$ gilt. $(\Rightarrow d(f_1) = d(f_2))$

Man zeige: 33) Jede primitive, positiv definite quadratische Form ist zu einer Form $g(x,y) = ax^2 + bxy + cy^2$ mit

$$|b| \leq a \leq c$$

äquivalent.

34) Jede primitive, indefinite quadratische Form mit einer nichtquadratischen Diskriminante ist zu einer Form $g(x,y) = ax^2 + bxy + cy^2$ mit

$$|b| \leq |a|, \quad |b| \leq |c|$$

äquivalent.

35) Jede primitive, indefinite quadratische Form mit quadratischer Diskriminante $d = D^2 \neq 0$ ist zu einer Form $g(x,y) = ax^2 + Dxy$ mit $0 \leq a \leq D-1$ equivalent.

Die quadratischen Formen der Beispiele 33, 34, 35, heißen reduziert.

36) Sei $f(x,y) = ax^2 + bxy + cy^2$ eine positiv definite, primitive, reduzierte Form. Dann ist $a = f(1,0)$ der kleinste positive Wert, der angenommen werden kann, $c = f(0,1)$ der kleinste Wert für $y \neq 0$ und $a - |b| + c$ der kleinste Wert mit $x \neq 0$ und $y \neq 0$. $(x, y \in \mathbb{Z})$.

37) Ist $f(x,y)$ eine reduzierte quadratische Form mit $b \equiv 0(2)$ und äquivalent zu $x^2 - Dy^2$ mit $D<0$, dann ist bereits $f(x,y) = x^2 - Dy^2$.

38) Sei K alg. Zahlkörper mit Signatur $[s,t]$. Man zeige, daß es dann ein $a \in \mathcal{O}_K, a \neq 0$, mit

$$|N_{K/\mathbb{Q}}(a)| \leq \left(\frac{4}{\pi}\right)^t n! \, n^{-n} \, |\delta_K|^{1/2}$$

gibt. (Anl: Gitterpunktsatz von Minkowski).
Man folgere daraus

$$|\delta_K| > \left(\frac{\pi}{4}\right)^{2t} \left(\frac{n^n}{n!}\right)^2 > 1 .$$

39) Man zeige, daß es nur endlich viele algebraische Zahlkörper mit derselben Diskriminante gibt.
(Man zeige mit Hilfe des Minkowskischen Gitterpunktsatzes, daß es für α mit $K = \mathbb{Q}(\alpha)$ nur endlich viele Möglichkeiten gibt.)

40) Sei K alg. Zahlkörper mit Signatur $[s,t]$. Man zeige, daß es dann in jeder Idealklasse von $H(K)$ ein Ideal I, $0 \neq I \subseteq \mathcal{O}_K$, mit

$$N(I) \leq \left(\frac{4}{\pi}\right)^t n! \, n^{-n} \, |\delta_K|^{1/2}$$

gibt. Man folgere daraus, daß es nur endlich viele Idealklassen gibt, d.h. $h(K) = |H(K)| < \infty$.

41) Sei K alg. Zahlkörper und $a \in \mathcal{O}_K, a \neq 0$.
Dann gilt

$$N(a\mathcal{O}_K) = |N_{K/\mathbb{Q}}(a)| .$$

42) Sei $d \neq 1$ eine quadratfreie ganze Zahl.
Man zeige für $K = \mathbb{Q}(\sqrt{d})$

$$\delta_K = \begin{cases} 4d & \text{für } d \equiv 2,3 \pmod 4 \\ d & \text{für } d \equiv 1 \pmod 4 \end{cases}$$