Algebraische Zahlentheorie

Vorlesung Tübingen, WS 2008/2009

Die Zahlentheorie nimmt unter den mathematischen Disziplinen eine ähnliche idealisierte Stellung ein wie die Mathematik selbst unter den (anderen) Naturwissenschaften: Ihre Zielsetzungen kommen weitgehend aus ihr selbst, ihre Problemstellungen sind oft zweckfrei, ihre Resultate bizarr und überraschend.

Gegenstand dieser Vorlesung (Mo Mi 10-12; M1) ist die *algebraische* Theorie, die Untersuchung der Ringe ganzer algebraischer Zahlen (Dedekindringe). Deren Verständnis ist unabdingbar für viele klassische Fragestellungen (Fermat-Vermutung; Primzahltheorie; Galoistheorie, etc.). Ein besonderes Augenmerk liegt auf der Berechnung der Galoisgruppen von Polynomen (Zerlegungs- und Verzweigungsgruppen; Newton-Polygon). Die Verzweigungstheorie ermöglicht einen elementaren Zugang zum berühmten Satz von Kronecker–Weber: *Jeder abelsche Zahlkörper ist ein Kreiskörper.*

Vorausgesetzt werden Kenntnisse über Gruppen, Ringe und Körper, etwa im Umfang der Algebra I und II. Die Vorlesung wendet sich an Diplomanden und Staatsexamenskandidaten gleichermaßen.

Hinweis (11.02.2009): In der Vorlesung konnten (leider) nur die Paragraphen 1 bis 14 behandelt werden.

Empfohlene Literatur:

P. Samuel: Algebraic Theory of Numbers (Kershaw, 1972)

D.A. Marcus: Number Fields (Springer, 1977);

J. Neukirch: Algebraische Zahlentheorie (Springer, 1992)

Weitere Literatur (Auswahl):

P. Ribenboim: Algebraic Numbers (Wiley, 1972)

W. Narkiewics: Elementary and Analytic Theory of Algebraic Numbers (Springer, 1990)

J.-P. Serre: Corps Locaux (Hermann, 1968)

S. Lang: Algebraic Number Theory (Addison–Wesley, 1970)

J.W.S. Cassels, A. Fröhlich: Algebraic Number Theory (Academic Press, 1967)

L.C. Washington: Introduction to Cyclotomic Fields (Springer, 1997)

P. Ribenboim*: 13 Lectures on Fermat's Last Theorem (Springer, 1979)

September 2008 Peter Schmid

Inhalt

§0. Elementarteilertheorie

Wir betrachten Moduln über $\mathbb{Z}$ (der Bequemlichkeit halber). Derselbe Ansatz funktioniert für jeden euklidischen Ring.

(0.1) **Relationenmatrix.** Sei $n \in \mathbb{N}_{>0}$ und $V = (V, +)$ ein freier $\mathbb{Z}$-Modul (abelsche Gruppe) vom Range n, d.h., $V \cong \mathbb{Z}^{(n)}$ (bei komponentenweiser Addition); alternativ: V hat eine $\mathbb{Z}$-Basis $\{v_1, \cdots, v_n\}$, so dass jedes Element $v \in V$ eine *eindeutige* Darstellung $v = \sum_{j=1}^{n} a_j v_j$ mit $a_j \in \mathbb{Z}$ hat. Der Rang n ist eine Invariante von V, denn V kann in den $\mathbb{Q}$-Vektorraum $\mathbb{Q}^{(n)}$ eingebettet werden. Sei $G = (G, +)$ eine abelsche Gruppe, die durch n Elemente g_j erzeugbar ist. Dann definiert die Zuordnung $v_j \mapsto g_j$ $(1 \leq j \leq n)$ einen Epimorphimsmus (von $\mathbb{Z}$-Moduln) $\varphi : V \twoheadrightarrow G$, und nach dem Homomorphiesatz ist

$$G \cong V/U, \;\; U = \mathrm{Ker}(\varphi).$$

Die Gruppe G ist also durch die Inklusion $U \subseteq V$ bestimmt. Sei $U \neq 0$ im weiteren. Da $\mathbb{Z}$ ein Noetherscher Ring ist, ist V ein Noetherscher $\mathbb{Z}$-Modul und daher $U = \langle u_1, \cdots, u_m \rangle$ endlich erzeugbar. Es gibt eindeutig bestimmte $c_{ij} \in \mathbb{Z}$, so dass die *Relationen*

$$u_i = \sum_{j=1}^{n} c_{ij} v_i \;\; (i = 1, \cdots, m)$$

gelten. Die Matrix $C = (c_{ij}) \in M_{m \times n}(\mathbb{Z})$ ist $\neq 0$ und bestimmt $U \subseteq V$.

(0.2) **Algorithmus** (Euklid–Gauß). Zu je zwei ganzen Zahlen a, b, $b \neq 0$, gibt es eindeutig bestimmte ganze Zahlen q, r mit $a = qb + r$ und $0 \leq r < b$. Dies führt zur Berechnung von ggT(a, b) und dessen Beschreibung als Vielfachsumme in a, b (Euklid). Entsprechend führen wir auf $M_{m \times n}(\mathbb{Z})$ eine Äquivalenzrelation $\sim$ ein: $C \sim D$, falls C durch elementare Zeilen- und Spaltentransformationen in D übergeführt werden kann (Gauß). Bei diesem Prozess ändern sich (bekanntlich) die sog. *Determinantenteiler*

$$\delta_k(C) = \mathrm{ggT}(\text{k−reihige Unterdeterminanten von } C);\; k = 1, \cdots, \min(m, n)$$

nicht. Diese sind Invarianten der Matrix C. Im Falle $n = m = 1$ setzen wir $e_1 = |c_{11}|$. Andernfalls führen wir so lange elementare Umformungen durch, bis ein positiver Eintrag e_1 derart entsteht, dass die anderen von Null verschiedenen Einträge betragsmäßig nicht kleiner als e_1 gemacht werden können. Wir können e_1 in Position $(1, 1)$ bringen, und dann die übrigen Einträge in der ersten Zeile und 1. Spalte zu Null machen:

$$C \sim \begin{pmatrix} e_1 & 0 & 0 & \dots & 0 \\ 0 & c'_{22} & c'_{2,3} & \dots & c'_{2n} \\ 0 & c'_{32} & c'_{33} & \dots & c'_{2n} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & c'_{m2} & c'_{m3} & \dots & c'_{mn} \end{pmatrix} = \begin{pmatrix} e_1 & 0 \\ 0 & C' \end{pmatrix}.$$

Nach Konstruktion teilt e_1 alle Einträge in der $(m-1)\times(n-1)$-Matrix C'. Wiederhole nun diesen Prozess für C', etc.. Wir erhalten auf diese Weise ein Produkt S von elementaren $m\times m$-Matrizen und ein Produkt T von elementaren $n\times n$-Matrizen, so dass

$$SCT = \begin{pmatrix} e_1 & 0 & \dots & \dots & \dots & & 0 \\ 0 & e_2 & 0 & \dots & \dots & & 0 \\ \vdots & \ddots & \ddots & \ddots & & & \vdots \\ & & 0 & \pm e_r & 0 & & \\ & & & 0 & 0 & 0 & \\ \vdots & & & & & \ddots & \\ 0 & \dots & & & & \dots & 0 \end{pmatrix}.$$

Hierbei ist $1\le r\le \min(m,n)$ und die $e_k>0$ sind ganze Zahlen mit $e_k \mid e_{k+1}$ $(k=1,\cdots,r-1)$. Es gilt dann $\delta_k(C)=e_1\cdots e_k$ für jedes k. Folglich gilt (bis eventuell auf das Vorzeichen) $e_1=\delta_1(C)$ und $e_k=\delta_k/\delta_{k-1}$ für $k>1$, d.h., die *Elementarteiler* e_k sind durch die Matrix bestimmt. Nur der letzte Elementarteiler e_r tritt möglicherweise mit negativem Vorzeichen in der Matrix auf, aber nur dann ist dies nicht zu verhindern, wenn $n=m$ und $\det(C)<0$ ist. Für die Transformationsmatrizen gilt $\det(S)=1$, $\det(T)=1$, sie sind daher invertierbar (über $\mathbb{Z}$).

(0.3) **Satz.** *Es gibt eine $\mathbb{Z}$-Basis $\{v_1',\cdots,v_n'\}$ von V und eindeutig bestimmte ganze Zahlen $e_k>0$ mit $e_k\mid e_{k+1}$, so dass $\{e_1v_1',\cdots,e_rv_r'\}$ eine $\mathbb{Z}$-Basis von $0\neq U\subseteq V$ ist. Hierbei ist $1\le r\le n$ eindeutig bestimmt.*

Beweis. Mit obigen Bezeichnungen sei $(v_1',\dots,v_n')=T^{-1}(v_1,\dots,v_n)^t$ (Spaltenvektor). Dann ist $SCT(v_1',\dots,v_n')^t=SC(v_1,\dots,v_n)^t=S(u_1,\dots,u_m)^t$ der Spaltenvektor mit den Einträgen $u_1'=e_1v_1',\cdots,u_r'=\pm e_rv_r'$ und Nullen sonst. □

(0.4) **Folgerung.** *Die abelsche Gruppe $G\cong U/V$ hat einen eindeuting bestimmten (torsions-) freien Anteil $G_0\cong\mathbb{Z}^{(n-r)}$ und ist die direkte Summe (direktes Produkt) von G_0 mit dem direkten Produkt zyklischer Gruppen der Ordnungen $e_1,\cdots,e_r$.*

Beweis. $\mathbb{Z}v_k'/\mathbb{Z}e_kv_k'\cong\mathbb{Z}/e_k\mathbb{Z}$ ist zyklisch der Ordnung e_k. □

(0.5) **Folgerung.** *Ist $G\cong U/V$ endlich und C eine zugehörige Relationenmatrix, so ist die Ordnung $|G|=\pm\det(C)$ (gleich dem Produkt der Elementarteiler).*

Beweis. $\det(C)=\det(S)\det(C)\det(T)=\det(SCT)$. □

(0.6) **Beispiel** $(n=4,m=2)$. $C=\begin{pmatrix}3&9&-3&0\\4&2&0&2\end{pmatrix}\sim\begin{pmatrix}-1&7&-3&-2\\4&2&0&2\end{pmatrix}\sim\begin{pmatrix}1&7&-3&-2\\2&2&0&2\end{pmatrix}\sim\begin{pmatrix}1&7&-3&-2\\0&-12&6&6\end{pmatrix}\sim\begin{pmatrix}1&0&0&0\\0&-12&6&6\end{pmatrix}\sim\begin{pmatrix}1&0&0&0\\0&6&0&0\end{pmatrix}$.
Also sind 1 und 6 die Elementarteiler von C, und C definiert die abelsche Gruppe (mit 4 Erzeugenden und 2 Relationen) $G\cong\mathbb{Z}/6\mathbb{Z}\oplus\mathbb{Z}^{(2)}$.

§1. Quadratische Zahlringe

Ein *algebraischer Zahlkörper* K ist ein endlicher Erweiterungskörper von $\mathbb{Q}$.

Es ist also die Charakteristik $\mathrm{char}(K) = 0$ und der Grad (Dimension) $[K : \mathbb{Q}] = n$ endlich; $K|\mathbb{Q}$ ist separabel (und algebraisch). Nach Gauß gibt es ein primitives Element α für $K|\mathbb{Q}$ ($K = \mathbb{Q}(\alpha)$). Das Minimalpolynom $f = m_{\mathbb{Q},\alpha}$ von α über $\mathbb{Q}$ zerfällt in $\mathbb{C}$ in n verschiedene Linearfaktoren. Jede Wurzel α' von f in $\mathbb{C}$ definiert, via $\alpha \mapsto \alpha'$, einen Isomorphismus von K auf einen Teilkörper von $\mathbb{C}$. Ist r_1 die Anzahl der reellen Wurzeln von f, so gibt es genau r_1 Einbettungen in $\mathbb{R}$ und $n - r_1 = 2r_2$ ist gerade, r_2 die Anzahl der Paare konjugiert komplexer (imaginärer) Einbettungen von K in $\mathbb{C}$.

(1.1) **Definition.** K heißt ein *quadratischer Zahlkörper*, falls $[K : \mathbb{Q}] = 2$ ist. Dann ist also entweder K total reell ($r_1 = 2$) oder total imaginär ($r_1 = 0$).

Behauptung. $K = \mathbb{Q}(\sqrt{d})$ *mit einer eindeutig bestimmten quadratfreien ganzen Zahl* $d \neq 0, 1$.

Beweis. Wähle $\alpha \in K \setminus \mathbb{Q}$. Dann ist $\{1, \alpha\}$ eine $\mathbb{Q}$-Basis von K und $K = \mathbb{Q}(\alpha) = \{x + y\alpha |\ x, y \in \mathbb{Q}\}$. Es gibt eindeutig bestimmte $a, b \in \mathbb{Q}$ mit $\alpha^2 = -b - a\alpha$, d.h., $f = m_{\mathbb{Q},\alpha} = X^2 + aX + b$ ist das Minimalpolynom. Über K zerfällt $f = (X - \alpha)(X - \alpha')$, wobei $\alpha' \neq \alpha$ konjugiert zu α über $\mathbb{Q}$ und die Galoisgruppe $\mathrm{Gal}(K|\mathbb{Q})$ durch die Zuordnung $\alpha \mapsto \alpha'$ bestimmt ist. Es ist die *Spur* $\mathrm{Tr}(\alpha) = \mathrm{Tr}_{K|\mathbb{Q}}(\alpha) = \alpha + \alpha' = -a$ und die *Norm* $\mathrm{N}(\alpha) = \mathrm{N}_{K|\mathbb{Q}}(\alpha) = \alpha\alpha' = b$, und für die *Diskriminante* von f gilt

$$D = D_f = (\alpha - \alpha')^2 = (\alpha + \alpha')^2 - 4\alpha\alpha' = a^2 - 4b.$$

Wäre $\delta = \alpha - \alpha'$ $(= \sqrt{D})$ in $\mathbb{Q}$, so wäre $\delta - a = 2\alpha \in \mathbb{Q}$. Es ist also $K = \mathbb{Q}(\sqrt{D})$. Schreibe $D = \frac{r}{s} = \frac{rs}{s^2}$ mit eindeutig bestimmten teilerfremden ganzen Zahlen r, s, und setze $d = rs$.

Ist auch $K = \mathbb{Q}(\sqrt{d'})$ mit einer quadratfreien ganzen Zahl d', so gibt es $x, y \in \mathbb{Q}$ mit $d' = (x + y\sqrt{d})^2 = x^2 + dy^2 + 2xy\sqrt{d}$, und es folgt $xy = 0$, $x = 0$, $d' = d$. □

(1.2) **Satz.** *Sei* $K = \mathbb{Q}(\sqrt{d})$ *ein quadratischer Zahlkörper* ($d \in \mathbb{Z}$ *quadratfrei). Dann ist die Menge* R *aller* $\alpha \in K$*, die einer Gleichung* $\alpha^2 + a\alpha + b = 0$ *mit* $a, b \in \mathbb{Z}$ *genügen, ein Teilring von* K*;* $R = R_K$ *ist der sog. Ring der ganzen Zahlen von* K*. Es gilt*

$$R_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{falls } d \equiv 2, 3 \pmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{falls } d \equiv 1 \pmod 4 \end{cases}.$$

Beweis. $\mathbb{Z}[\sqrt{d}] \cong \mathbb{Z}[X]/(X^2 - d)$ ist jedenfalls ein Teilring von K. Ist $d \equiv 1 \pmod 4$, so ist auch $\mathbb{Z}[\frac{1+\sqrt{d}}{2}] \cong \mathbb{Z}[X]/(X^2 - X - \frac{d-1}{4})$ ein Teilring von K. Sei $\alpha = x + y\sqrt{d}$

$(x, y \in \mathbb{Q})$. Dann ist $\mathrm{Tr}(\alpha) = 2x$ und $\mathrm{N}(\alpha) = x^2 - dy^2$. Definitionsgemäß ist $\alpha \in R$ genau dann, wenn es $a, b \in \mathbb{Z}$ gibt, so dass α Wurzel von $f = X^2 + aX + b$ ist. Sei zunächst $\alpha = x \in \mathbb{Q}$. Dann ist das Minimalpolynom $m_{\mathbb{Q},\alpha} = X - x$ ein Teiler von f in $\mathbb{Q}[X]$, und das Gauß-Lemma liefert $x \in \mathbb{Z}$. Es ist also $R \cap \mathbb{Q} = \mathbb{Z}$.

Sei weiterhin $\alpha \notin \mathbb{Q}$ $(y \neq 0)$. Dann ist $f = m_{\mathbb{Q},\alpha}$ und $-a = \mathrm{Tr}(\alpha)$, $b = \mathrm{N}(\alpha)$. Genau dann ist also $\alpha \in R$, wenn es $a, b \in \mathbb{Z}$ mit

$$-a = 2x \text{ und } \mathrm{b} = \mathrm{x}^2 - \mathrm{dy}^2$$

gibt. Dies ist richtig, wenn $\alpha \in \mathbb{Z}[\sqrt{d}]$ ist, und wenn $\alpha \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ ist im Falle $d \equiv 1 \,(\mathrm{mod}\, 4)$. Seien umgekehrt obige Bedingungen erfüllt. Aus $(2x)^2 - d(2y)^2 \in \mathbb{Z}$ folgt dann $d(2y)^2 \in \mathbb{Z}$ und $2y \in \mathbb{Z}$, denn d ist quadratfrei. Setze $u = 2x$ und $v = 2y$. Es sind u, v ganze Zahlen und $\alpha = \frac{u}{2} + \frac{v}{2}\sqrt{d}$, sowie $u^2 - dv^2 \in 4\mathbb{Z}$.

1. Fall: $d \equiv 2, 3 \,(\mathrm{mod}\, 4)$

Wäre u ungerade, so wäre $u^2 \equiv 1 \,(\mathrm{mod}\, 4)$ und $v^2 \not\equiv 0 \,(\mathrm{mod}\, 4)$, daher $v^2 \equiv 1 \,(\mathrm{mod}\, 4)$ und $d \equiv v^2 d \equiv 1 \,(\mathrm{mod}\, 4)$, ein Widerspruch. Folglich ist $x = \frac{u}{2}$ ganz, und $dv^2 \equiv 0 \,(\mathrm{mod}\, 4)$, $v^2 \equiv 0 \,(\mathrm{mod}\, 4)$ und auch v gerade.

2. Fall: $d \equiv 1 \,(\mathrm{mod}\, 4)$

Ist u ungerade, so ist $u^2 \equiv 1 \,(\mathrm{mod}\, 4)$, daher auch $v^2 \equiv 1 \,(\mathrm{mod}\, 4)$ und v ungerade. Ist u gerade, so ist $u^2 \equiv 0 \,(\mathrm{mod}\, 4)$, daher auch $v^2 \equiv 0 \,(\mathrm{mod}\, 4)$ und v gerade. Mit anderen Worten: u und v haben dieselbe *Parität*, insbesondere $u - v$ gerade. Es ist

$$\alpha = \frac{1}{2}(u + v\sqrt{d}) = \frac{1}{2}(u - v) + v\frac{1 + \sqrt{d}}{2} \in \mathbb{Z}[\frac{1 + \sqrt{d}}{2}],$$

wie zu zeigen war. □

(1.3) **Satz.** *Für $d = -1, -2, -3, -7, -11$ ist $K = \mathbb{Q}(\sqrt{d})$ euklidisch, d.h., $R = R_K$ ist ein euklidischer Ring bzgl. der Norm $\mathrm{N} = \mathrm{N}_{K|\mathbb{Q}}$, insbesondere ein Hauptidealring.*

Beweis. Sei zunächst $d \in \{-1, -2\}$. Nach (1.2) ist in diesem Fall $R = \mathbb{Z}[\sqrt{d}]$. Seien $\alpha, \beta \in R$, $\beta \neq 0$. Betrachte $\frac{\alpha}{\beta} \in K$. Wir finden einen Gitterpunkt $\gamma \in R$, so dass $\frac{\alpha}{\beta} = \gamma + \delta$ mit $\delta \in \mathbb{C} = \mathbb{R}^{(2)}$ (euklidisch) und

$$\mathrm{N}(\delta) = \delta\bar{\delta} \leq \frac{1}{4}(1^2 + \sqrt{|d|}^2) = \frac{1}{4}(1 + |d|) < 1.$$

Es ist $\delta \in K$ und $\rho = \delta\beta = \alpha - \gamma\beta \in R$ mit $\mathrm{N}(\rho) = \mathrm{N}(\delta) \cdot \mathrm{N}(\beta) < \mathrm{N}(\beta)$.

Sei $d \in \{-3, -7, -11\}$. Dann $R = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ nach (1.2). Für den Radius r des Umkreises des Dreiecks $0, 1, \frac{1}{2}(1 + i\sqrt{|d|})$ gilt

$$r^2 = (\frac{1}{2}\sqrt{|d|} - r)^2 + \frac{1}{4}.$$

Es ist hier $r = \frac{1}{4}(\sqrt{|d|} + \frac{1}{\sqrt{|d|}}) < 1$. Argumentiere nun wie oben. □

(1.4) **Definition.** In diesem §1 seien weiterhin $K = \mathbb{Q}(\sqrt{d})$ und $R = R_K$ wie in (1.1), (1.2). Dann sind $\{1, \sqrt{d}\}$ bzw. $\{1, \frac{1+\sqrt{d}}{2}\}$ $\mathbb{Z}$-Basen von R. Für die Diskriminante (Algebra II oder §3) dieser Basen gilt $\det \begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix}^2 = 4d$ bzw. $\det \begin{pmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{pmatrix}^2 = d$. Jeder Basiswechsel wird durch eine Transformationsmatrix $T \in \mathrm{GL}_2(\mathbb{Z})$ mit $\det T = \pm 1$ vermittelt, so dass dies von der Wahl der *Ganzheitsbasis* von R nicht abhängt. Die ganze Zahl

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

heißt die *absolute Diskriminante* von K. Mit anderen Worten: D_K ist die Diskriminante von $X^2 - d$ im ersten Fall, und von $X^2 - X - \frac{d-1}{4}$ im zweiten Falle.

(1.5) **Lemma.** *Sei $\mathfrak{a} \neq 0$ ein Ideal von $R = R_K$, und sei $0 \neq \alpha \in \mathfrak{a}$.*

(a) *$\mathfrak{a}$ ist ein freier $\mathbb{Z}$-Modul vom Range 2 und $\mathfrak{a} \cap \mathbb{Z} \neq 0$. Insbesondere ist $\mathrm{N}\mathfrak{a} := |R/\mathfrak{a}|$ endlich, die sog. absolute Norm des Ideals.*

(b) *Ist $\mathfrak{a} = (\alpha) = \alpha R$ ein Hauptideal, so ist $\mathrm{N}\mathfrak{a} = \pm \mathrm{N}_{K|\mathbb{Q}}(\alpha)$. Genau dann ist also $\alpha \in R^*$ eine Einheit ($\mathfrak{a} = R$), wenn $\mathrm{N}_{K|\mathbb{Q}}(\alpha) = \pm 1$ ist.*

(c) *Ist $\mathfrak{a} = \mathfrak{p}$ ein Primideal, so ist $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ mit einer (positiven) Primzahl p und $\mathrm{N}\mathfrak{p} = p$ oder p^2. Der Restklassenring $k_\mathfrak{p} = R/\mathfrak{p}$ ist ein Körper (der Ordnung p oder p^2).*

Beweis. (a) Es gibt $a, b \in \mathbb{Z}$ mit $\alpha^2 + a\alpha + b = 0$. Es ist dann $b = \alpha(-\alpha - a) \in \mathfrak{a} \cap \mathbb{Z}$ (und auch $-b$). Ist $b = 0$, so ist $a = -\alpha$ (Nullteilerfreiheit). Folglich enthält $\mathfrak{a}$ eine natürliche Zahl $m > 0$. Da $R/mR = m^2$ endlich ist, ist also $R/\mathfrak{a}$ ein endlicher Ring. Den Rest liefert der Elementarteilersatz (0.3).

(b) Wir können $\alpha \notin \mathbb{Z}$ annehmen, so dass $\{1, \alpha\}$ eine $\mathbb{Q}$-Basis von K ist. Sei $m_{\mathbb{Q},\alpha} = X^2 + aX + b$. Die Multiplikation mit α ist ein Isomorphismus $\widehat{\alpha}$ von R auf αR. Außerdem ist $\mathrm{N}_{K|\mathbb{Q}}(\alpha) = \det(\widehat{\alpha})$, denn bzgl. der Basis $\{1, \alpha\}$ ist $\widehat{\alpha}$ die Matrix $\begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix}$ zugeordnet. Nach (0.3) gibt es eine $\mathbb{Z}$-Basis $\{v_1, v_2\}$ von R und Elementarteiler $e_1 \mid e_2$, so dass $\{e_1 v_1, e_2 v_2\}$ ein $\mathbb{Z}$-Basis von αR ist. Sei φ der $\mathbb{Z}$-Isomorphismus von R auf αR mit $\varphi(v_i) = e_i v_i$. Da $\widehat{\alpha}$ und φ sich nur um einen Automorphismus von αR unterscheiden, gilt

$$\det(\varphi) = e_1 e_2 = \pm \det(\widehat{\alpha}) = \pm \mathrm{N}_{K|\mathbb{Q}}(\alpha),$$

wie behauptet.

(c) Sind $x, y \in \mathbb{Z} \setminus \mathfrak{p}$, so auch xy. Also ist $\mathfrak{p} \cap \mathbb{Z}$ ein Primideal ($\neq 0$) von $\mathbb{Z}$. Diese sind alle von der behaupteten Form. Da endliche Integritätsbereiche (mit $1 \neq 0$) immer Körper sind, ist $\mathfrak{p}$ ein maximales Ideal von R. $\square$

In der Situation (c) sagen wir, das Primideal $\mathfrak{p}$ *liege über der Primzahl* p ($\mathfrak{p}|p$). Dann ist $pR \subseteq \mathfrak{p}$, und wegen $|R/pR| = p^2$ können nicht viele Primideale über p liegen. Wir schreiben $\mathbb{P} = \mathbb{P}_{\mathbb{Q}}$ für die (positiven) Primzahlen und $\mathbb{P}_K$ für die Primideale ($\neq 0$) von R_K.

(1.6) **Satz.** *Sei* $R^* = (R^*, \cdot)$ *die Einheitengruppe des Rings* $R = R_K$.

(a) *Ist* $d < 0$ *(*K *imaginär), so ist* R^* *die Gruppe der Einheitswurzeln in* K*, also* $R^* = \{\pm 1\}$ *ausgenommen die Fälle* $d = -1$ *(*$R^* = \langle i \rangle$*) und* $d = -3$ *(*$R^* = \langle e^{2\pi i/6} \rangle$*).*

(b) *Ist* $d > 0$ *(*K *reell), so gibt es eine eindeutig bestimme kleinste (Fundamental-) Einheit* $u_0 > 1$ *in* R^**, und* $R^* = \{\pm 1\} \times \langle u_0 \rangle$.

Beweis. 1. Fall: $d \equiv 2, 3 \pmod 4$

Sei $\alpha = a + b\sqrt{d} \in R$ ($a, b \in \mathbb{Z}$). Nach (1.5)(b) ist $\alpha \in R^*$ genau dann, wenn $\mathrm{N}(\alpha) = \pm 1$ ist, d.h., wenn die sog *Pellsche Gleichung* $a^2 - db^2 = \pm 1$ erfüllt ist. (Die Inverse ist dann die Konjugierte α' oder $-\alpha'$.) Ist $d < 0$ (K imaginär), so ist $\mathrm{N}(\alpha) = a^2 + |d|b^2 = +1$ nur möglich, und es folgt $a = \pm 1$ für $d \neq -1$. Ist $d > 0$ (K reell), so identifiziere $\sqrt{d}$ mit der positiven Quadratwurzel von d in $\mathbb{R}$. In diesem Fall sind ± 1 die einzigen Einheitswurzeln in K, aber es gibt eine Einheit $\alpha \neq \pm 1$ von R. Die Existenz einer solchen Einheit wird später allgemein bewiesen werden (Dirichletscher Einheitensatz, §13). Mit α sind dann auch $\pm\alpha$ und $\pm\alpha^{-1}$ Einheiten, und dies sind die vier Einheiten $\pm a \pm b\sqrt{d}$. Genau dann ist $\alpha > 1$, wenn $a > 0$ und $b > 0$ sind.

Daher gibt es $b_0 \in \mathbb{N}_{>0}$ minimal derart, dass $db_0^2 \mp 1 = a_0^2$ für eine (positive) natürliche Zahl a_0 gilt. Dann ist das Vorzeichen durch b_0 und damit auch a_0 eindeutig bestimmt, und $u_0 = a_0 + b_0\sqrt{d}$ ist eine Einheit > 1 von R (mit Norm $\mathrm{N}(u_0) = \pm 1$ entsprechend). Angenommen, es gibt eine Einheit $u_1 = a_1 + b_1\sqrt{d}$ von R mit $1 < u_1 < u_0$. Dann sind a_1, b_1 positive natürliche Zahlen mit $db_1^2 \mp 1 = a_1^2$. Nach Wahl von b_0 gilt $b_1 \geq b_0$, damit aber auch $a_1 \geq a_0$ und $u_1 \geq u_0$, ein Widerspruch. Also ist u_0 die Fundamentaleinheit von R.

Sei $u > 1$ eine weitere Einheit. Es gibt dann $n \in \mathbb{N}$ mit $u_0^n \leq u$ und $u_0^{n+1} > u$ (Archimedizität). Dann ist u/u_0^n eine Einheit mit $1 \leq u/u_0^n < u_0$. Es folgt $u = u_0^n$. Das Erzeugnis $\langle u_0 \rangle = \{u_0^m \,|\, m \in \mathbb{Z}\}$ ist natürlich eine unendliche (zyklische) Gruppe.

2. Fall: $d \equiv 1 \pmod 4$.

Sei $\alpha = \frac{a+b\sqrt{d}}{2} \in R$ ($a, b \in \mathbb{Z}$ mit gleicher Parität). Nach (1.5)(b) ist $\alpha \in R^*$ genau dann, wenn $\mathrm{N}(\alpha) = \pm 1$ ist, d.h., wenn die *Pellsche Gleichung* $a^2 - db^2 = \pm 4$ erfüllt ist. Ist $d < 0$, so ist $4\mathrm{N}(\alpha) = a^2 + |d|b^2 = +4$ nur möglich, und es folgt $a = \pm 1$ für $d \neq -3$. Sei also weiterhin $d > 0$ ($d \geq 5$), und wir verfahren wie eben. Nach dem noch zu beweisenden Einheitensatz gibt es eine Einheit $\frac{a+b\sqrt{d}}{2} > 1$ von R, und dann habe $a > 0$ und $b > 0$ automatisch dieselbe Parität.

Es gibt daher $b_0 \in \mathbb{N}_{>0}$ minimal derart, dass $db_0^2 \mp 4 = a_0^2$ für eine (positive) natürliche Zahl a_0 gilt. Dann ist das Vorzeichen durch b_0 bestimmt und damit auch a_0, es sei denn $d = 5$, wo $b_0 = 1$ und $a_0 = 1$ (minimal) zu wählen ist. Jedenfalls ist $u_0 = \frac{a_0 + b_0\sqrt{d}}{2}$ eine Einheit > 1 von R, und zwar mit Norm $\mathrm{N}(u_0) = \pm 1$ entsprechend. Sei $d > 5$ und sei angenommen, es existiere eine Einheit $u_1 = \frac{a_1 + b_1\sqrt{d}}{2}$ von R mit $1 < u_1 < u_0$. Dann sind a_1, b_1 (positive) natürliche Zahlen gleicher Parität mit $db_1^2 \mp 4 = a_1^2$. Das Vorzeichen und a_1 sind dabei durch b_1 bestimmt. Aus $u_1 < u_0$ folgt $b_1 \leq b_0$ und $a_1 \leq a_0$, damit sogar $b_1 < b_0$, ein Widerspruch. Also ist u_0 die Fundamentaleinheit von R. Der Rest ist wie im 1. Falle. $\square$

(1.7) **Beispiele.** Sei $K = \mathbb{Q}(\sqrt{d})$ mit $d > 1$ quadratfrei, und sei $R = R_K$.

1. Fall: $d \equiv 2, 3 \pmod 4$

Aufgrund des Beweises von (1.6) ist die Fundamentaleinheit $u_0 = a_0 + b_0\sqrt{d}$ wie folgt bestimmt: b_0 ist die kleinste (positive) natürliche Zahl b mit der Eigenschaft, dass $db^2 \mp 1 = a^2$ ist für eine (positive) natürliche Zahl a, und dann ist das Vorzeichen und damit auch $a_0 = a$ durch $b_0 = b$ bestimmt. Das legt auch die Norm $\mathrm{N}(u_0) = \pm 1$ fest.

$\mathbf{d = 2}$: $(2b^2 \pm 1)_{b \geq 1} = (2 \cdot 1^2 \pm 1, 2 \cdot 2^2 \pm 1, \cdots)$

Wegen $2 \cdot 1^2 - 1 = 1^2$ ist also $u_0 = 1 + \sqrt{2}$ $(\mathrm{N}(u_0) = -1)$.

$\mathbf{d = 3}$: $(3b^2 \pm 1)_{b \geq 1} = (3 \cdot 1^2 \pm 1, 3 \cdot 2^2 \pm 1, \cdots)$

Wegen $3 \cdot 1^2 + 1 = 2^2$ ist $u_0 = 2 + \sqrt{3}$ $(\mathrm{N}(u_0) = +1)$.

Entsprechend berechnet man $u_0 = 3 + \sqrt{10}$ für $d = 10$ $(\mathrm{N}(u_0) = -1)$ und $u_0 = 15 + 4\sqrt{14}$ für $d = 14$ $(\mathrm{N}(u_0) = +1)$.

2. Fall: $d \equiv 1 \pmod 4$

Aufgrund des Beweises von (1.6) ist die Fundamentaleinheit $u_0 = \frac{\alpha_0 + b_0\sqrt{d}}{2}$ wie folgt bestimmt: b_0 ist die kleinste (positive) natürliche Zahl b mit der Eigenschaft, dass $db^2 \pm 4 = a^2$ mit einer (positiven) natürlichen Zahl a ist. Ist $d \neq 5$, so ist hierbei das Vorzeichen und somit $a_0 = a$ durch $b_0 = b$ bestimmt.

$\mathbf{d = 5}$: $(5b^2 \pm 4)_{b \geq 1} = (5 \cdot 1^2 \pm 4, \cdots)$; es ist $u_0 = \frac{1}{2}(1 + \sqrt{5})$ $(\mathrm{N}(u_0) = -1)$.

$\mathbf{d = 13}$: $(13b^2 \pm 4)_{b \geq 1} = (13 \cdot 1^2 \pm 4, \cdots)$; es ist $u_0 = \frac{1}{2}(3 + \sqrt{13})$ $(\mathrm{N}(u_0) = -1)$.

(1.8) **Hauptsatz.** *Seien $K = \mathbb{Q}(\sqrt{d})$ und $R = R_K$, $D = D_K$ wie üblich. Sei $p \in \mathbb{P}$.*

(a) *Genau dann ist $pR = \mathfrak{p}^2$ mit einem eindeutig bestimmten, explizit angegebenen Primideal $\mathfrak{p}$ von R mit Norm $\mathrm{N}\mathfrak{p} = p$ (Verzeigung), wenn p ein Teiler von D ist.*

(b) *Genau dann ist $pR = \mathfrak{p}\mathfrak{p}'$ mit eindeutig bestimmten, explizit angegebenen Primidealen $\mathfrak{p} \neq \mathfrak{p}'$ mit Norm p (Zerfällung), wenn $p \nmid d$ und d ein quadratischer Rest modulo p für ungerades p und $d \equiv 1 \pmod 8$ für $p = 2$ ist.*

(c) *In allen anderen Fällen ist $pR = \mathfrak{p}$ ein Primideal von R (Trägheit).*

Notation (Legendre-Symbol): Für ungerades p schreiben wir $(\frac{d}{p}) = 0$ im Falle $p \mid d$, $(\frac{d}{p}) = 1$, falls $p \nmid d$ und d ein quadratischer Rest mod p ist, d.h., es gibt $x \in \mathbb{Z}$ mit $x^2 \equiv d \,(\mathrm{mod}\, p)$, und $(\frac{d}{p}) = -1$ sonst.

Beweis. Sei $\alpha = \sqrt{d}$ im 1. Falle und $\alpha = \frac{1+\sqrt{d}}{2}$ im 2. Falle, und entsprechend $f = X^2 - d$ bzw. $f = X^2 - X + \frac{1-d}{4}$. In jedem Fall ist α eine Wurzel von f, und nach (1.2) ist $R = \mathbb{Z}[\alpha] \cong \mathbb{Z}[X]/(f)$. Jedes Element von R hat also die Form $g(\alpha)$ für ein Polynom $g \in \mathbb{Z}[X]$, und ist $g(\alpha) = 0$, so ist g ein Teiler von f in $\mathbb{Z}[X]$ nach dem Gauß-Lemma.

Ist $\mathfrak{p}|p$ ein Primideal von R über der vorgegeben Primzahl p, so ist $\bar{\alpha} = \alpha + \mathfrak{p}$ eine Wurzel (im Körper $R/\mathfrak{p}$) der Reduktion $\bar{f} = f \mathrm{mod}\, p$ in $\mathbb{F}_p[X]$, und damit Wurzel eines (normierten) Primfaktors $\bar{f}_0$ von $\bar{f}$. Sei umgekehrt $\bar{\alpha}$ Wurzel eines solchen Primfaktors $\bar{f}_0$ von $\bar{f}$ (in einem Zerfällungskörper), und sei $f_0 \in \mathbb{Z}[X]$ ein (normiertes) Urbild. Dann definiert $g(\alpha) \mapsto \bar{g}(\bar{\alpha})$ für $g \in \mathbb{Z}[X]$ einen Epimorphismus $R \twoheadrightarrow \mathbb{F}_p(\bar{\alpha})$ (von Ringen mit 1), dessen Kern ein maximales Ideal $\mathfrak{p}$ von R über p ist. Dies ist wohldefiniert aufgrund des Gauß-Lemmas. Wir behaupten, dass

$$\mathfrak{p} = \big(p, f_0(\alpha)\big) = pR + f_0(\alpha)R$$

durch $\bar{f}_0$ bestimmt ist. Es ist klar, dass p und $f_0(\alpha)$ im Kern $\mathfrak{p}$ des obigen Epimorphismus' sind. Ist umgekehrt $g \in \mathbb{Z}[X]$ mit $g(\alpha) \in \mathfrak{p}$, so ist $\bar{g} = \bar{f}_0\bar{h}$ für ein $h \in \mathbb{Z}[X]$ und die Koeffizienten von $g - f_0h \in \mathbb{Z}[X]$ sind alle durch p teilbar. Also ist $g(\alpha) \in \big(p, f_0(\alpha)\big)$. Wir haben also eine bijektive Beziehung zwischen den Primidealen von R über p und den (normierten) Primfaktoren von $\bar{f}$ in $\mathbb{F}_p[X]$, wobei es folgende Möglichkeiten gibt:

(a) $\bar{f} = \bar{f}_0^2$ und $\mathfrak{p}^2 \subseteq pR$;

(b) $\bar{f} = \bar{f}_0\bar{f}_0'$ mit normierten Primfaktoren $\bar{f}_0 \neq \bar{f}_0'$ und $\mathfrak{p}\mathfrak{p}' \subseteq pR$;

(c) $\bar{f} = \bar{f}_0$ ist irreduzibel über $\mathbb{F}_p$ und $\mathfrak{p} = pR$ (Trägheit).

1. Fall: $d \equiv 2, 3 \,(\mathrm{mod}\, 4)$ $\quad (f = X^2 - d,\ D = 4d)$

Hier ist $\alpha = \sqrt{d}$. Sei zunächst $p = 2$. Dann gilt

$$\bar{f} = \begin{cases} X^2 & \text{falls } d \equiv 2 \,(\mathrm{mod}\, 4) \\ X^2 - \bar{1} = (X - \bar{1})^2 & \text{falls } d \equiv 3 \,(\mathrm{mod}\, 4) \end{cases}.$$

Es ist also $\mathfrak{p} = (2, \sqrt{d})$ bzw. $\mathfrak{p} = (2, \sqrt{d} - 1)$ das einzige Primideal von R oberhalb $2R$. Es gilt $\mathfrak{p}^2 = (4, 2\sqrt{d}, d) = 2R$ bzw. $= (4, 2\sqrt{d}-2, d-2\sqrt{d}+1) = (4, 2\sqrt{d}-2, d-1) = 2R$, denn es ist $(4, d) = 2$ bzw. $(4, d-1) = 2$. Es liegt also hier immer Verzweigung vor $(2 \mid D)$. Ist $p \neq 2$, so ist $\bar{f} \in \mathbb{F}_p[X]$ irreduzibel im Falle $(\frac{d}{p}) = -1$, somit $\mathfrak{p} = (p) = pR$ (Trägheit), und sonst

$$\bar{f} = \begin{cases} X^2 & \text{falls } p \mid d \\ (X + \bar{a})(X - \bar{a}) & \text{falls } (\frac{d}{p}) = 1 \end{cases}.$$

Ist $p \mid d$, so ist $\mathfrak{p} = (p, \sqrt{d})$ und $\mathfrak{p}^2 = (p^2, d, p\sqrt{d}) = pR$ (Verzweigung), denn $p^2 \nmid d$ (d ist quadratfrei) und daher $(p^2, d) = p$. Ist andererseits $a \in \mathbb{Z}$ ein Urbild von $\bar{a}$, so sind $\mathfrak{p} = (p, \sqrt{d}+a)$ und $\mathfrak{p}' = (p, \sqrt{d}-a) = (p, -\sqrt{d}+a)$ verschiedene Primideale von R über p (mit Norm p) mit $\mathfrak{p}\mathfrak{p}' \subseteq pR$. Da p kein Teiler von $2a$ ist, gilt in der Tat Zerfällung:

$$\mathfrak{p}\mathfrak{p}' = (p^2, p\sqrt{d} + pa, p\sqrt{d} - pa, d - a^2) = (p^2, 2pa, p\sqrt{d} - pa) = pR.$$

2. Fall: $d \equiv 1 \pmod 4$ $\quad (f = X^2 - X + \frac{1-d}{4},\ D = d)$

Hier ist $\alpha = \frac{1+\sqrt{d}}{2}$ und $R = \mathbb{Z}[\alpha]$. Ist $p = 2$, so ist

$$\bar{f} = \begin{cases} X^2 - X = X(X-1) & \text{falls } d \equiv 1 \pmod 8 \\ X^2 - X - 1 & \text{falls } d \equiv 5 \pmod 8 \end{cases}.$$

Das Polynom $X^2 - X - 1 = X^2 + X + 1 \in \mathbb{F}_2[X]$ ist irreduzibel (Trägheit), sonst liegt Zerfällung vor: $2R = \mathfrak{p}\mathfrak{p}'$ für $\mathfrak{p} = (2, \alpha)$ und $\mathfrak{p}' = (2, \alpha')$. Sei $p \neq 2$, und sei $S = \mathbb{Z}[\sqrt{d}]$. Es ist S ein Teilring von R mit $pR \cap S = pS$. Ferner ist $(p+1)\frac{1+\sqrt{d}}{2} \in S$ und $\frac{1+\sqrt{d}}{2} = (p+1)\frac{1+\sqrt{d}}{2} - p\frac{1+\sqrt{d}}{2}$, somit $S + pR = R$. Folglich ist $R/pR \cong S/pS$. Wir können die Primideale $\mathfrak{p}|p$ von R genau wie im 1. Falle beschreiben; man ersetze ein Primideal $\mathfrak{p}_0|p$ von S einfach durch $\mathfrak{p} = \mathfrak{p}_0 R$ (gleiche Erzeugende). $\square$

(1.9) **Anwendung.** *Sei $d < 0$. Ist $R = R_K$ ein faktorieller Ring, so ist $-d \in \{1, 2, 7\}$ oder $-d$ eine Primzahl $p \equiv 3 \pmod 8$.*

Beweis. K ist imaginär und der nichttriviale Körperautomorphismus wird von der komplexen Konjugation bewirkt; die Norm $\mathrm{N} = \mathrm{N}_{K|\mathbb{Q}}$ nimmt nur positive Werte an. Primelemente sind stets unzerlegbar, und die Umkehrung gilt immer dann, wenn der Ring faktoriell ist.

Sei $d \equiv 2, 3 \pmod 4$. Nach (1.2) ist $R = \mathbb{Z}[\sqrt{d}]$. Nach (1.8) ist $2R$ kein Primideal von R (Verzweigung), also 2 kein Primelement in R. Da R faktoriell ist, gibt es Nichteinheiten α, β in R mit $2 = \alpha\beta$. Dann ist $2^2 = (\alpha\bar{\alpha})(\beta\bar{\beta})$ und zwangsläufig $2 = \alpha\bar{\alpha}$. Schreibe $\alpha = a + b\sqrt{d}$ $(a, b \in \mathbb{Z})$. Dann $2 = \alpha\bar{\alpha} = a^2 + |d|b^2$, und dies erzwingt $a = 0$, $b = \pm 1$, $|d| = 2$ oder $a = \pm 1$, $b = \pm 1$, $|d| = 1$.

Sei $d \equiv 1 \pmod 8$. Nach (1.2) ist $R = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. Nach (1.8) ist $2R$ kein Primideal von R (Zerfällung), daher 2 kein Primelement von R. Da R faktoriell ist, gibt es eine Nichteinheit $\alpha \in R$ mit $2 = \alpha\bar{\alpha}$. Schreibe $\alpha = \frac{1}{2}(a + b\sqrt{d})$ ($a, b \in \mathbb{Z}$ mit gleicher Parität). Es folgt

$$a^2 + |d|b^2 = 8.$$

Dies erzwingt $|d| = 7$.

Sei $d \equiv 5 \,(\mathrm{mod}\, 8)$, und sei p ein Primteiler von $d = D_K$. Dann ist p ungerade. Nach (1.2) ist $R = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. Nach (1.8) ist pR kein Primideal von R (Verzweigung), also kein Primelement. Da R faktoriell ist, finden wir $a, b \in \mathbb{Z}$ mit gleicher Parität, so dass

$$a^2 + |d|b^2 = 4p$$

ist. Wegen $p \mid d$ gilt dabei $p \mid a^2$, mithin $p \mid a$. Es folgt $b = \pm 1$ und entweder $a = \pm 3$ und $|d| = 3$ oder $a = 0$ und $p = |d| \equiv 3 \,(\mathrm{mod}\, 8)$. $\square$

Anmerkung. Es gibt genau 9 imaginäre quadratische Zahlkörper $K = \mathbb{Q}(\sqrt{d})$, für welche $R = R_K$ faktoriell ist, nämlich für $-d = 1, 2, 3, 7, 11, 19, 43, 67, 163$. Dies hatte schon Gauß so vermutet, ein Beweis gelang aber erst H.M. Stark und A. Baker 1967. Offen ist noch bis heute, ob es unendlich viele reelle quadratische Zahlkörper mit dieser Eigenschaft gibt.

(1.10) **Anwendung.** *$R = R_K$ ist ein sog. Dedekindring (§5), d.h., jedes Ideal $\mathfrak{a} \neq 0$ von R lässt sich eindeutig schreiben als Produkt von Primidealen.*

Beweis. (Existenz) Angenommen, $\mathfrak{a}$ ist kein Produkt von Primidealen von R, und ist maximal gewählt mit dieser Eigenschaft (R ist freier $\mathbb{Z}$-Modul vom Range 2 und daher Noetherscher Ring). Dann $\mathfrak{a} \neq R$ $(= \mathfrak{p}^0)$ und $\mathfrak{a} \notin \mathbb{P}_K$, aber es gibt ein Primideal $\mathfrak{p}$ von R mit $\mathfrak{a} \subset \mathfrak{p}$. Es ist $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ für eine Primzahl p. Ist $\mathfrak{a} \subseteq pR$, so ist $\mathfrak{a} \subset \frac{\mathfrak{a}}{p} \subseteq R$ und das Ideal $\frac{\mathfrak{a}}{p}$ von R Produkt von Primidealen von R, nach Wahl von $\mathfrak{a}$. Wegen (1.8) gilt aber dann die Behauptung auch für $\mathfrak{a}$. Also ist $\mathfrak{a} \not\subseteq pR$, und wegen $\mathfrak{a} \subset \mathfrak{p}$ haben wir $pR = \mathfrak{pq}$ mit einem Primideal $\mathfrak{q}$ von R (Verzweigung oder Zerfällung). Es ist $\frac{\mathfrak{q}}{p} \supset R$ und

$$\mathfrak{a} \subseteq \frac{\mathfrak{aq}}{p} \subseteq \frac{\mathfrak{pq}}{p} = R.$$

Angenommen, es ist $\mathfrak{a} = \frac{\mathfrak{aq}}{p}$. Sei $\{\alpha, \beta\}$ eine $\mathbb{Z}$-Basis von $\mathfrak{a}$ (1.5). Wähle $x \in \frac{\mathfrak{q}}{p} \setminus R$. Nach Annahme ist $x\mathfrak{a} \subseteq \mathfrak{a}$. Es gibt daher $a, b, c, e \in \mathbb{Z}$ mit

$$x\alpha = a\alpha + b\beta, \quad x\beta = c\alpha + e\beta.$$

Es folgt $(x-a)\alpha = b\beta$, $(x-e)\beta = c\alpha$, somit $(x-e)(x-a)\alpha = (x-e)b\beta = bc\alpha$ und $x^2 - (a+e)x + (ae - bc = (x-e)(x-a) - bc = 0$ (Nullteilerfreiheit). Nach Definition ist aber dann $x \in R$, ein Widerspruch. Daher ist $\mathfrak{a} \subset \mathfrak{b} = \frac{\mathfrak{aq}}{p}$, und für das Ideal $\mathfrak{b}$ von R gilt die Behauptung, damit aber auch für $\mathfrak{bp} = \frac{\mathfrak{aqp}}{p} = \mathfrak{a}$.

(Eindeutigkeit) Seien $\mathfrak{p}_i$ und $\mathfrak{q}_j$ in $\mathbb{P}_K$ mit $\prod_{i=1}^n \mathfrak{p}_i = \mathfrak{a} = \prod_{j=1}^m \mathfrak{q}_j$. Wir argumentieren per Induktion nach n. Weil das Primideal $\mathfrak{p}_1 \supseteq \prod_{j=1}^m \mathfrak{q}_j$ ist, gibt es j, etwa $j = 1$, mit $\mathfrak{p}_1 \supseteq \mathfrak{q}_1$. Da $\mathfrak{q}_1$ ein maximales Ideal von R ist, folgt $\mathfrak{p}_1 = \mathfrak{q}_1$ $(= \mathfrak{p})$. Sei $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ $(p \in \mathbb{P})$. Nach (1.8) finden wir ein Primideal $\mathfrak{q}$ von R oberhalb pR mit $\frac{\mathfrak{q}}{\mathrm{N}\mathfrak{p}}\mathfrak{p} = R$. Multiplikation mit $\frac{\mathfrak{q}}{\mathrm{N}\mathfrak{p}}$ liefert $\prod_{i=2}^n \mathfrak{p}_i = \prod_{j=2}^m \mathfrak{q}_j$. Induktion! $\square$

§2. Der große Satz von Fermat

Pierre de Fermat (1608-1665); ein Porträt findet man in Ribenboim*.

Der große Satz von Fermat (Fermat's letzer Satz; die Fermatsche Vermutung) hat die Mathematik der Neuzeit so bewegt wie kein anderes Thema. Zwar hat Fermat angedeutet, er habe einen Beweis, aber niemand hat ihn gesehen. Die unzähligen Versuche über mehrere Jahrhunderte, die Fermatsche Behauptung zu beweisen, hat die Mathematik in vielen Hinsichten befruchtet und beeinflusst. Es war eine Sensation, als Andrew Wiles 1993-95 einen Beweis der Fermatschen Vermutung vorlegte. Neben Methoden der algebraischen Zahlentheorie (Klassenkörpertheorie; Iwasawa-Theorie der Klassenzahlen), die über das hinausgehen, was in dieser Vorlesung behandelt werden kann, werden zum Beweis auch Methoden aus anderen Bereichen verwendet (modulare Formen; elliptische Kurven).

Der kleine Satz von Fermat ist die (bekannte) Aussage, dass auf dem Primkörper $\mathbb{F}_p$ der Frobenius-Automorphismus identisch ist, d.h., die Primahl p teilt $a^p - a$ für jede ganze Zahl a.

(2.1) **Pythagoräische Tripel.** *Seien $a, b, c \in \mathbb{N}_{>0}$ teilerfremd. Äquivalent sind folgende Aussagen:*

(i) Es ist a ungerade und $a^2 + b^2 = c^2$.

(ii) Es ist $a = x^2 - y^2$, $b = 2xy$ und $c = x^2 + y^2$ mit teilerfremden positiven natürlichen Zahlen $x > y$, die nicht beide ungerade sind.

Beweis. $(i) \Rightarrow (ii)$: Die Rechnung mod 4 zeigt, dass c ungerade ist, daher (etwa) a ungerade, b gerade. Ferner sind a, b, c *paarweise teilerfremd.* Betrachte $\alpha = a + ib$ in $R = \mathbb{Z}[i]$ ($i^2 = -1$). Nach (1.3) ist R faktoriell. Sei π ein Primteiler von α in R. Angenommen, $\pi \mid \alpha' = a - ib$ in R. Dann ist π ein Teiler von $\alpha + \alpha' = 2a$ und von $c^2 = \alpha\alpha'$, somit $\pi \mid c$. Da $2a$ und c teilerfremde ganze Zahlen sind, folgt $\pi \mid 1$ und $\pi \in R^* = \langle i \rangle$, ein Widerspruch. Wegen $\alpha\alpha' = c^2$ geht also π in α mit geradem Exponenten auf. Folglich ist $a + ib = \alpha = u\beta^2$ mit $u \in R^* = \langle i \rangle$ und $\beta = x + iy \in R$ ($x, y \in \mathbb{Z}$). Es ist $u = \pm 1$. Wegen $a > 0$ können wir $u = 1$ und $x > y > 0$ annehmen. Es sind x, y teilerfremd und nicht beide ungerade, denn $a = x^2 - y^2$ ist ungerade. Es ist $b = 2xy$ und $c = x^2 + y^2$.

$(ii) \Rightarrow (i)$: Verifikation ! $\square$

(2.2) **Satz** (Fermat). *Es gibt keine positiven ganzen Zahlen a, b, c mit $a^4 + b^4 = c^4$.*

Beweis. Wir zeigen, dass es nicht einmal solche Zahlen gibt mit $a^4 + b^4 = c^2$ (!). Andernfalls wählen wir diese Zahlen so, dass c möglichst klein ist. Die Idee ist,

eine positive Lösung (a', b', c') von $X^4 + Y^4 = Z^2$ zu konstruieren, für welche $c' < c$ ist (*Fermats unendlicher Abstieg*). Aufgrund der Wahl von c sind a, b, c paarweise teilerfremd (!). Sei etwa a ungerade. Nach (2.1) ist $a^2 = x^2 - y^2$, $b^2 = 2xy$, $c = x^2 + y^2$ mit positiven teilerfremden ganzen Zahlen x, y. Aus $b^2 = 2xy$ folgt, dass genau eine der Zahlen x, y gerade ist. Wäre x gerade, so wäre $x^2 \equiv 0 \,(\mathrm{mod}\, 4)$, $y^2 \equiv 1 \,(\mathrm{mod}\, 4)$, somit $a^2 = x^2 - y^2 \equiv -1 \,(\mathrm{mod}\, 4)$, was nicht möglich ist. Daher ist x ungerade, $y = 2y'$ gerade. Da $b^2 = 4xy'$ und x und y' teilerfremd sind, gilt $x = c'^2$, $y' = t^2$ mit positiven ganzen Zahlen c', t. Nun ist $a^2 + y^2 = x^2$, also (a, y, x) ein Pythagoräisches Tripel. Nach (2.1) gilt

$$a = m^2 - n^2,\ y = 2mn,\ x = m^2 + n^2$$

mit teilerfremden natürlichen Zahlen m, n. Aus $y = 2y' = 2t^2$ erhalten wir $m = a'^2$, $n = b'^2$ mit teilerfremden natürlichen Zahlen a', b'. Damit gilt

$$a'^4 + b'^4 = x = c'^2.$$

Hierbei gilt $c = x^2 + y^2 = c'^4 + 4t^4 > c'^4$, also $c > c'$, entgegen der Wahl von c. □

(2.3) **Ternäre Tripel.** *Es gibt keine von* 0 *verschiedenen ganzen Zahlen* a, b, c *mit* $a^3 + b^3 = c^3$.

Beweis (Fall 1. Angenommen, es gibt solche Zahlen. Dann können wir a, b, c als teilerfremd voraussetzen, und dann sind sie paarweise teilerfremd. Es gibt die beiden folgenden (Fermat-) Fälle.

Fall 1: $3 \nmid abc$.

Wir rechnen modulo 9. Es gilt $a^3, b^3, c^3 \equiv \pm 1 \,(\mathrm{mod}\, 9)$. Andererseits ist $c^3 = a^3 + b^3 \equiv 0, \pm 2 \,(\mathrm{mod}\, 9)$. Widerspruch!

Fall 2: 3 teilt genau eine der Zahlen a, b, c.

Auch dieser Fall führt zu einem Widerspruch, aber dies liegt tiefer und wurde zuerst von Euler bewiesen. Gauß hat einen eleganten Beweis angegeben, der verwendet, dass der Ring $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ der ganzen Zahlen des 3-ten Kreisteilungskörpers faktoriell ist (vgl. Übung (14) und Ribenboim*, p. 42-45).

(2.4) **Theorem** (A. Wiles). *Für* $n \geq 3$ *gibt es keine von* 0 *verschiedenen ganzen Zahlen* a, b, c *mit* $a^n + b^n = c^n$.

Wir können hier nur einen Spezialfall behandeln. Nach (2.2) und (2.3) genügt es, das Theorem für jede Primzahl $n = p > 3$ nachzuweisen. (Ist $n = mp$, so $X^n = (X^m)^p$; ist n durch keine ungerade Primzahl teilbar, so ist $n = m \cdot 4$ ein 2-Potenz und $X^n = (X^m)^4$.) Wir halten im Folgenden ein solches p fest und betrachten den

p-ten Kreisteilungskörper $L = \mathbb{Q}(\varepsilon)$, etwa $\varepsilon = e^{2\pi i/p}$. Sei $S = \mathbb{Z}[\varepsilon]$. Bekanntlich ist $\Phi_p = \frac{X^p-1}{X-1} = X^{p-1} + X^{p-2} + \cdots + X + 1$ das Minimalpolynom von ε über $\mathbb{Q}$, denn

$$\Phi_p(X+1) = X^{p-1} + pX^{p-2} + \binom{p}{2}X^{p-3} + \cdots + \binom{p}{p-2}X + p$$

ist ein Eisenstein-Polynom bzgl. p. Es gilt $X^p - 1 = (X-1)(X-\varepsilon)(X-\varepsilon^2)\cdots(X-\varepsilon^{p-1})$. Ferner ist $\mathbb{Z}[X]/(\Phi_p) \cong S$ via $X \mapsto \varepsilon$, und S ist ein freier $\mathbb{Z}$-Modul vom Range $p-1$ mit Basis $\{1, \varepsilon, \varepsilon^2, \cdots, \varepsilon^{p-2}\}$.

Sei $G = \mathrm{Gal}(L|\mathbb{Q})$. Jedes $\sigma \in G$ ist festgelegt (und festlegbar) durch $\varepsilon \mapsto \varepsilon^j$, $j = 1, \cdots, p-1$. Also ist $G \cong (\mathbb{Z}/p\mathbb{Z})^*$ zyklisch (der Ordnung $p-1$). Sei $\mathrm{Tr} = \mathrm{Tr}_{L|\mathbb{Q}}$ die *Spurabbildung* $\alpha \mapsto \sum_{\sigma\in G} \alpha^\sigma$ und $\mathrm{N} = \mathrm{N}_{L|\mathbb{Q}}$ die *Norm* $\alpha \mapsto \prod_{\sigma\in G} \alpha^\sigma$ $(\alpha \in L)$. Aus der Kenntnis von $\Phi_p = m_{\mathbb{Q},\varepsilon}$ folgt $\mathrm{Tr}(\varepsilon) = \mathrm{Tr}(\varepsilon^j) = -1$, $\mathrm{N}(\varepsilon) = \mathrm{N}(\varepsilon^j) = 1$ für $j = 1, \ldots, p-1 (p-1$ ist gerade), sowie $\mathrm{Tr}(\varepsilon - 1) = -p$. Wegen $\Phi_p(X+1) = m_{\mathbb{Q},\varepsilon-1}$ ist

$$p = \mathrm{N}(\varepsilon - 1) = (\varepsilon - 1)(\varepsilon^2 - 1)\cdots(\varepsilon^{p-1} - 1).$$

(2.5) **Lemma.** *Für das Hauptideal $\mathfrak{p} = (\varepsilon - 1)S$ von $S = \mathbb{Z}[\varepsilon]$ gilt $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, $S/\mathfrak{p} \cong \mathbb{F}_p$ und $pS = \mathfrak{p}^{p-1}$ (totale Verzweigung).*

Beweis. Wir zeigen zunächst, dass die $\frac{\varepsilon^j-1}{\varepsilon-1}$ Einheiten in S sind $(j = 2, \cdots, p-1)$. Es ist $\frac{\varepsilon^j-1}{\varepsilon-1} = 1 + \varepsilon + \cdots + \varepsilon^{j-1} \in S$. Ist $t \in \mathbb{Z}$ mit $jt \equiv 1 \,(\mathrm{mod}\, p)$, so ist andererseits auch

$$\frac{\varepsilon - 1}{\varepsilon^j - 1} = \frac{(\varepsilon^j)^t - 1}{\varepsilon^j - 1} = 1 + \varepsilon^j + \cdots + \varepsilon^{j(t-1)} \in S.$$

Aus obiger Identität folgt damit $pS = \mathfrak{p}^{p-1}$. Wegen $|S/pS| = p^{p-1}$ folgt $\mathfrak{p} \subset S$ und $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Für $\alpha = a_0 + a_1\varepsilon + a_2\varepsilon^2 + \cdots + a_{p-2}\varepsilon^{p-2}$ in S $(a_i \in \mathbb{Z})$ gilt

$$\alpha \equiv a_0 + a_1 + \cdots + a_{p-2} \,(\mathrm{mod}\, \mathfrak{p}).$$

Folglich ist $S = \mathbb{Z} + \mathfrak{p}$, und $S/\mathfrak{p} \cong \mathbb{Z}/(\mathfrak{p} \cap \mathbb{Z}) = \mathbb{Z}/p\mathbb{Z}$. $\square$

(2.6) **Satz.** *$S = \mathbb{Z}[\varepsilon]$ ist der Ring R_L der ganzen Zahlen von $L = \mathbb{Q}(\varepsilon)$.*

Beweis. Wir nennen hier (vorläufig) ein Element $\alpha \in L$ ganz, wenn das Minimalpolynom $m_{\mathbb{Q},\alpha} \in \mathbb{Z}[X]$ ist (siehe §3). Ist $\alpha \in S$, so ist α ganz in diesem Sinne. Sei dazu A_n der $\mathbb{Z}$-Aufspann von $1, \alpha, \alpha^2, \cdots, \alpha^n$ $(n \in \mathbb{N})$. Dann $A_n \subseteq A_{n+} \subseteq S$. Da $S = \mathbb{Z}[\varepsilon]$ ein Noetherscher $\mathbb{Z}$-Modul ist, gibt es n derart, dass $\alpha^{n+1} \in A_n$ ist. Aber dann ist α^{n+1} Wurzel eines *normierten* Polynoms $f \in \mathbb{Z}[X]$ (vom Grade $n+1$), und das Gauß-Lemma liefert $\alpha \in R_L$. Es ist also $S \subseteq R_L$. Entsprechend zeigt man, dass R_L ein Teilring von L ist (vgl. (3.3)), und zwar mit $R_L \cap \mathbb{Q} = \mathbb{Z}$ (Gauß-Lemma).

Sei $\alpha \in R_L$. Dann sind die Konjugierten von α über $\mathbb{Q}$ in R_L, somit die Norm $\mathrm{N}(\alpha)$ und die Spur $\mathrm{Tr}(\alpha)$ in $R_L \cap \mathbb{Q} = \mathbb{Z}$ (vgl. (3.7)). Schreibe (eindeutig) $\alpha = x_0 + x_1\varepsilon + x_2\varepsilon^2 + \cdots + x_{p-2}\varepsilon^{p-2}$ ($x_i \in \mathbb{Q}$). Dann ist

$$\alpha(\varepsilon - 1) = x_0(\varepsilon - 1) + x_1(\varepsilon^2 - \varepsilon) + \ldots + x_{p-2}(\varepsilon^{p-1} - \varepsilon^{p-2}) \in R_L.$$

Wegen $\mathrm{Tr}(\varepsilon^{j+1} - \varepsilon^j) = 0$ für $j = 1, \ldots, p-2$ folgt $\mathrm{Tr}(\alpha(\varepsilon - 1)) = x_0\mathrm{Tr}(\varepsilon - 1) = -x_0 p$. Andererseits ist $\mathrm{Tr}(\alpha(\varepsilon - 1)) \in R_L \cap \mathbb{Q} = \mathbb{Z}$. Wegen $\mathrm{N}(\varepsilon - 1) = p$ ist $\varepsilon - 1$ keine Einheit von R_L, denn aus $u(\varepsilon - 1) = 1$ für $u \in R_L$ folgte $\mathrm{N}(u) \in \mathbb{Z}$ und $\mathrm{N}(u)\mathrm{N}(\varepsilon - 1) = 1$. Da $\mathrm{Tr}(\alpha(\varepsilon - 1))$ die Summe der G-konjugierten Elemente $\alpha_j(\varepsilon^j - 1)$ von $\alpha(\varepsilon - 1)$ ist, die alle in $\mathfrak{p}R_L = (\varepsilon - 1)R_L$ liegen, gilt nach (2.5) sogar $\mathrm{Tr}(\alpha(\varepsilon - 1)) \in p\mathbb{Z}$. Folglich ist $x_0 \in \mathbb{Z}$. Damit ist, wie eben,

$$(\alpha - x_0)\varepsilon^{p-1} = (\alpha - x_0)\varepsilon^{-1} = x_1 + x_2\varepsilon + \cdots + x_{p-2}\varepsilon^{p-3}$$

ein ganzes Element in R_L. Dasselbe Argument liefert nun $x_1 \in \mathbb{Z}$; Induktion! $\square$

$L = \mathbb{Q}(\varepsilon)$ ist total imaginär ($r_1 = 0$ und $r_2 = (p-1)/2$). Die komplexe Konjugation definiert ein Element in G, das durch $\varepsilon \mapsto \varepsilon^{-1} = \bar{\varepsilon}$ bestimmt ist. Sei $L^+ = \mathbb{Q}(\varepsilon + \varepsilon^{-1}) = \mathbb{Q}(\cos\frac{2\pi}{p})$ der maximale total reelle Teilkörper von L ($r_1^+ = (p-1)/2$ und $r_2^+ = 0$).

(2.7) **Lemma** (Kummer). *Sei $u \in S^*$ eine Einheit in $S = \mathbb{Z}[\varepsilon]$. Dann gibt es $t \in \mathbb{Z}$ und $u^+ \in L^+$, so dass $u = \varepsilon^t u^+$ ist.*

Beweis. Betrachte $\alpha = u/\bar{u}$ und $m = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. Mit u ist auch $\bar{u}$ eine Einheit und daher $\alpha \in S = R_L$. Für den komplexen Betrag gilt $|\alpha|^2 = \alpha\bar{\alpha} = 1$, also $|\alpha| = 1$. Da G abelsch ist, gilt analog $|\alpha^\sigma| = |u^\sigma/\overline{u^\sigma}| = 1$. Entsprechendes gilt für jede Potenz α^k ($k \in \mathbb{N}$). Sei $f_k = m_{\mathbb{Q},\alpha^k} = \sum_i a_i^{(k)} X^i$. Es gilt $\mathrm{grd}(\mathrm{f_k}) = [\mathbb{Q}(\alpha^\mathrm{k}) : \mathbb{Q}] \leq \mathrm{m}$, und die $a_i^{(k)}$ sind die elementarsymmetrischen Funktionen der Wurzeln von f_k. Daher ist $a_i^{(k)} \in R_L \cap \mathbb{Q} = \mathbb{Z}$ und $|a_i^{(k)}| \leq \binom{m}{i} \leq 2^m$. Es gibt also höchstens $m2^{m+1}$ solche Polynome f_k. Daher gibt es $k < \ell$ mit $\alpha^k = \alpha^\ell$, somit $\alpha^{\ell-k} = 1$, und α ist eine Einheitswurzel.

Die Gruppe der Einheitswurzeln in L hat die Ordnung $2p$ und wird durch $-\varepsilon$ erzeugt (Eulersche φ-Funktion !). Es ist also $\alpha = \pm e^j$ für geeignetes Vorzeichen und $1 \leq j \leq p-1$. Angenommen, es ist $\alpha = -\varepsilon^j$. Schreibe $u = a_0 + a_1\varepsilon + \cdots + a_{p-2}\varepsilon^{p-2}$ ($a_i \in \mathbb{Z}$). Dann ist $\bar{u} = a_0 + a_1\varepsilon^{-1} + \cdots$, und für $a = a_0 + \cdots + a_{p-2}$ gilt

$$\bar{u} \equiv a \equiv u \equiv -e^j\bar{u} \equiv -\bar{u} \,(\mathrm{mod}\,\mathfrak{p}).$$

Daher ist $2\bar{u} \in \mathfrak{p} = (\varepsilon - 1)S$. Wegen $p \neq 2$ folgt $\bar{u} \in \mathfrak{p}$. Aber dann ist $\bar{u}$ sicher keine Einheit in S.

Folglich ist $u/\bar{u} = +\varepsilon^j$. Wähle $t \in \mathbb{Z}$ mit $2t \equiv j \,(\mathrm{mod}\, p)$ und setze $u^+ = \varepsilon^t\bar{u}$. Dann ist $u = \varepsilon^t u^+$ und $\overline{u^+} = \varepsilon^{-t}u = \varepsilon^{-t}\varepsilon^j\bar{u} = \varepsilon^t\bar{u} = u^+$, also $u^+ \in L^+$. $\square$

(2.8) **Satz.** *Sei $S = \mathbb{Z}[\varepsilon]$ als faktorieller Ring vorausgesetzt. Dann gibt es keine ganzen Zahlen a, b, c mit $p \nmid abc$ und $a^p + b^p = c^p$.*

Beweis. Andernfalls finden wir solche Zahlen a, b, c, die teilerfremd sind, und dann automatisch paarweise teilerfremd. Wir können oBdA annehmen, dass $a \not\equiv b \,(\mathrm{mod}\, p)$ ist. Ist nämlich $a \not\equiv -c \,(\mathrm{mod}\, p)$, so vertausche man b und $-c$ und betrachte $a^p + (-c)^p = (-b)^p$. Ist $a \equiv b \equiv -c \,(\mathrm{mod}\, p)$, so ist (kleiner Fermat) $-2c^p \equiv a^p + b^p \equiv c^p \,(\mathrm{mod}\, p)$ und somit $p \mid 3c$. Das ist nicht möglich, da wir $p > 3$ vorausgesetzt haben.

Die Substitution $X \mapsto \frac{-a}{b}$ in $X^p - 1 = (X-1)(X-\varepsilon)(X-\varepsilon^2)\cdots(X-\varepsilon^{p-1})$ liefert die Identität

$$(a+b)(a+\varepsilon b)\cdots(a+\varepsilon^{p-1}b) = a^p + b^p = c^p.$$

Wir behaupten, dass die Elemente $a+\varepsilon^i b$ von S für $i = 0, \cdots, p-1$ paarweise teilerfremd sind. Sei $\pi \in S$ ein Primelement. Angenommen, es gibt $i < j$, so dass π sowohl $a + \varepsilon^i b$ als auch $a + \varepsilon^j b$ teilt. Dann ist π ein Teiler von $\varepsilon^i b - \varepsilon^j b = u(\varepsilon - 1)b$, wobei $u \in S^*$ ist, somit $\pi \mid \varepsilon - 1$ oder $\pi \mid b$ (S faktoriell). Analog ist π ein Teiler von $\varepsilon^j(a + \varepsilon^i b) - \varepsilon^i(a + \varepsilon^j b) = v(\varepsilon - 1)a$ für ein $v \in S^*$, daher $\pi \mid \varepsilon - 1$ oder $\pi \mid b$. Wegen $(a, b) = 1$ folgt $\pi \mid \varepsilon - 1$, somit $(\pi) = \mathfrak{p}$ nach (2.5). Es folgt $a + b \equiv a + \varepsilon^i b \equiv 0 \,(\mathrm{mod}\, \pi)$ und, wegen $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, $a + b \equiv 0 \,(\mathrm{mod}\, p)$. Aber dann ist $c^p \equiv a^p + b^p \equiv a + b \equiv 0 \,(\mathrm{mod}\, p)$ und somit $p \mid c$ (S faktoriell). Dies ist ein Widerspruch zur Voraussetzung.

Wir folgern, dass $a + \varepsilon b = u\alpha^p$ für geeignete $u \in S^*$ und $\alpha \in S$ ist. (Analoges für die anderen Faktoren in obiger Identität.) Nach (2.7) ist $u = \varepsilon^t u^+$ für geeignete $t \in \mathbb{Z}$ und $u^+ \in L^+$. Schreibe $\alpha = x_0 + x_1\varepsilon + \cdots + x_{p-2}\varepsilon^{p-2}$ mit $x_i \in \mathbb{Z}$ und setze $x = \sum_i x_i$. Dann gilt (binomischer Lehrsatz)

$$\alpha^p \equiv x_0^p + x_1^p\varepsilon^p + \cdots + x_{p-2}^p\varepsilon^{(p-2)p} \equiv x \,(\mathrm{mod}\, pS).$$

Daher ist $a + \varepsilon b = \varepsilon^t u^+ \alpha^p \equiv \varepsilon^t u^+ x \,(\mathrm{mod}\, pS)$. Ebenso ist $a + \bar{\varepsilon} b = \varepsilon^{-t} u^+ \bar{\alpha}^p \equiv \varepsilon^{-t} u^+ x \,(\mathrm{mod}\, pS)$ (wegen $\bar{x} = x$ und $\bar{S} = S$). Wir erhalten $\varepsilon^{-t}(a + \varepsilon b) \equiv \varepsilon^t(a + \varepsilon^{-1} b) \,(\mathrm{mod}\, pS)$ und

$$a + \varepsilon b - \varepsilon^{2t} a - \varepsilon^{2t-1} b \equiv 0 \,(\mathrm{mod}\, pS).$$

Jede Teilmenge von $\{1, \varepsilon, \varepsilon^2, \cdots, \varepsilon^{p-1}\}$ aus $p-1$ Elementen ist eine $\mathbb{Z}$-Basis von $S = \mathbb{Z}[\varepsilon]$ ($\sum_{i=0}^{p-1} \varepsilon^i = 0$) und die Restklassen mod pS bilden eine $\mathbb{F}_p$-Basis von S/pS. Sind also $1, \varepsilon, \varepsilon^{2t}, \varepsilon^{2t-1}$ verschieden, so gilt $p \mid a$ und $p \mid b$, entgegen unserer Voraussetzung. Daher sind sie nicht verschieden. Wegen $1 \neq \varepsilon$ und $\varepsilon^{2t} \neq \varepsilon^{2t-1}$ bleiben folgende Möglichkeiten:

$1 = \varepsilon^{2t}$: Dann ist $a + \varepsilon b - a - \varepsilon^{-1} b \equiv 0 \,(\mathrm{mod}\, pS)$, also $\varepsilon b - \varepsilon^{p-1} b \equiv 0 \,(\mathrm{mod}\, pS)$ und $p \mid b$, ein Widerspruch.

$1 = \varepsilon^{2t-1}$: Dann ist $\varepsilon = \varepsilon^{2t}$, und wir erhalten $(a - b) - (a - b)\varepsilon \equiv 0 \,(\mathrm{mod}\, pS)$ und damit $p \mid a - b$. Dies widerspricht unserer Bedingung $a \not\equiv b \,(\mathrm{mod}\, p)$.

$\varepsilon = \varepsilon^{2t-1}$: Dann ist $a - \varepsilon^2 a \equiv 0 \,(\mathrm{mod}\, pS)$, somit $p \mid a$, ein Widerspruch. $\square$

(2.9) **Anmerkungen.** Sei $S = \mathbb{Z}[\varepsilon] = \mathbb{Z}[\varepsilon_p]$ für die Primzahl $p > 3$.

(a) Leider ist S in der Regel *nicht* faktoriell. Genau dann ist S faktoriell, wenn $p \leq 19$ ist. (Den Fall $p = 23$ werden wir uns in einer Übung vornehmen.)

(b) Wir werden sehen, dass S ein Dedekindring ist (§5). Genau dann ist S faktoriell, wenn S ein Hauptidealring ist (5.9). Ferner gibt es eine natürliche Zahl $h = h_p \geq 1$ mit der Eigenschaft, dass die h-te Potenz jedes Ideals von S ein Hauptideal ist (*Klassenzahl*; siehe §12). Genau dann ist S faktoriell, wenn $h_p = 1$ ist. (Zum Beispiel ist $h_{23} = 3$.)

(c) Die Primzahl p heißt *regulär*, wenn p kein Teiler von h_p ist. Der Beweis von (2.8) überträgt sich sofort auf den Fall, dass p eine reguläre Primzahl ist. Man braucht nur zu überlegen, dass die Hauptideale $(a + \varepsilon^i b)S$ paarweise teilerfremd sind. Aus der eindeutigen Primidealzerlegung folgt dann

$$(a + \varepsilon b)S = \mathfrak{a}^p$$

für ein Ideal $\mathfrak{a} \neq 0$ von S. Da p regulär ist, erzwingt dies, dass $\mathfrak{a}$ selbst ein Hauptideal ist. Nun verfährt man wie oben.

Auch der 2. Fall der Fermatschen Vermutung (p teilt genau eine der Zahlen a, b, c) lässt sich (mit etwas mehr Mühe) für reguläres p beweisen (siehe Ribenboim*, p. 82-90, und Washington, p. 167-182). Der Beweisansatz geht im wesentlichen auf Kummer (ca. 1840) zurück, auch wenn der in diesem frühen Stadium noch glaubte, alle diese Ringe seien faktoriell (E. Kummer, 1810-1893).

(d) Leider gibt es unendlich viele irreguläre Primzahlen (siehe Washington, p. 62). Die kleinste irreguläre Primzahl ist $p = 37$.

§3. Ganzheit

Durchweg seien $R \subseteq S$ Integritätsbereiche (mit $1 \neq 0$) und $K \subseteq L$ die zugehörigen Quotientenkörper.

(3.1) **Definition.** Ein Element $\alpha \in S$ heißt *ganz* über R, falls α Wurzel eines *normierten* Polynoms $f \in R[X]$ (mit Grad grd(f) ≥ 1) ist. Die Ringerweiterung $S|R$ heißt ganz, falls jedes Element von S ganz über R ist. Die Menge

$$R_{S|R} = \{\alpha \in S |\ \alpha \text{ ganz über } R\}$$

heißt der *ganze Abschluss* von R in S.

Spezialfall: Im Falle $R = \mathbb{Z}$ nennt man die über $\mathbb{Z}$ ganzen Elemente auch *ganz-algebraisch*. Ist L ein algebraischer Zahlkörper, so bezeichnet $R_L = R_{L|\mathbb{Z}}$ die Menge der ganz-algebraischen Zahlen in L. Wegen des Gauß-Lemmas ($\mathbb{Z}$ faktoriell) ist ein Element $\alpha \in L$ genau dann ganz-algebraisch, wenn das Minimalpolynom $m_{\mathbb{Q},\alpha} \in \mathbb{Z}[X]$ ist.

Bemerkung. Die Körpererweiterung $L|K$ ist genau dann ganz, wenn sie algebraisch ist. Genauer gilt: Ist $S|R$ ganz, so gilt

$$R = K \iff S = L.$$

Ist nämlich $R = K$ und $0 \neq \beta \in B$ ganz (algebraisch), so ist $K[\beta] = K(\beta) \cong K[X]/(m_{K,\beta})$ ein endlicher Erweiterungskörper von K, und es existiert $\beta^{-1} \in K(\beta) \subseteq S$. Ist $S = L$ ein Körper und $0 \neq \alpha \in R$, so existiert $\alpha^{-1} \in S$ und ist daher ganz über R. Es gibt also eine Relation

$$\alpha^{-n} + a_{n-1}\alpha^{-n+1} + \cdots + a_1\alpha^{-1} + a_0 = 0$$

mit Koeffizienten $a_i \in R$. Multiplikation mit α^{n-1} zeigt, dass das Element $\alpha^{-1} = -(a_{n-1} + \cdots + a_1\alpha^{n-2} + a_0\alpha^{n-1})$ in R ist.

(3.2) **Hauptsatz.** *Für $\alpha \in S$ sind folgende Aussagen äquivalent:*

(i) $\alpha \in R_{S|R}$ ist ganz über R.

(ii) Der Ring $R[\alpha]$ (erzeugt von r und α) ist ein endlich erzeugter R-Modul.

(iii) Es gibt einen endlich erzeugten R-Modul $0 \neq V \subseteq L$ mit $\alpha V \subseteq V$.

Beweis. $(i) \Rightarrow (ii)$: Es gibt eine R-Relation $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$ ($n \in \mathbb{N}_{>0}$, $a_i \in R$), und dann ist α^n R-Linearkombination in $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$. Foglich ist der Ring $R[\alpha]$ als R-Modul erzeugt durch $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$.

$(ii) \Rightarrow (iii)$: Setze $V = \mathbb{Z}[\alpha]$.

$(iii) \Rightarrow (i)$: Sei V als R-Modul erzeugt durch $v_1, \cdots, v_n$. Dann gilt $\alpha v_i = a_{i1}v_1 + \cdots + a_{in}v_n$ mit Koeffizienten $a_{ij} \in R$ $(1 \leq i \leq n)$. Sei $A = (a_{ij}) \in M_n(R)$. Es ist $(\alpha I_n - A)(v_1, \ldots, v_n)^t = 0$ und daher die Matrix $\alpha I_n - A$ singulär $(V \neq 0)$. Folglich ist deren Determinante 0, d.h., α ist Wurzel des charakteristischen Polynoms $\det(XI_n - A)$, welches ein normiertes Polynom in $R[X]$ ist. $\square$

(3.3) **Folgerung.** *Sind $\alpha_1, \ldots, \alpha_n$ endlich viele über R ganze Elemente von S, so ist der Ring $R[\alpha_1, \ldots, \alpha_n]$ ganz über R und ein endlich erzeugter R-Modul. Insbesondere ist $R_{S|R}$ ein Teilring (Integritätsbereich) von S, der R enthält.*

Beweis. Nach (3.2) ist $R[\alpha_1]$ ein endlich erzeugter R-Modul. Offenbar ist α_2 ganz über $R[\alpha_1]$, daher $R[\alpha_1, \alpha_2] = R[\alpha_1][\alpha_2]$ ein endlich erzeugter $R[\alpha_1]$-Modul. Ist $\{u_i\}_i$ ein R-Erzeugensystem von $R[\alpha_1]$ und $\{v_j\}_j$ ein $R[\alpha_1]$-Erzeugendensystem von $R[\alpha_1, \alpha_2]$, so ist $\{u_i v_j\}_{i,j}$ ein R-Erzeugendensystem für $V = R[\alpha_1, \alpha_2]$. Nach (3.2) ist jedes Element von $R[\alpha_1, \alpha_2]$ ganz über R, insbesondere $\alpha_\pm \alpha_2$ und $\alpha_1 \cdot \alpha_2$. Dies zeigt, dass $R_{S|R}$ ein Ring $(\supseteq R)$ ist. Der Rest folgt durch Induktion. $\square$

(3.4) **Satz.** *Sei $R \subseteq S' \subseteq S$, S' ein Integritätsbereich. Ist S ganz über S' und S' ganz über R, so ist S ganz über R ("Transitivität").*

Beweis. Sei $\beta \in S$. Es gibt $a_i \in S'$ und $n \in \mathbb{N}_{>0}$ mit $\beta^n + a_{n-1}\beta^{n-1} + \cdots + a_0 = 0$ (β ganz über S'). Da die a_i ganz über R sind, ist nach (3.3) $S'' = R[a_0, \cdots, a_{n-1}]$ ganz über R ist. Nun ist β ganz über S'', daher $V = S''[\beta]$ ein endlich erzeugter S''-Modul. Folglich ist V ein endlich erzeugter R-Modul, mit $\beta V \subseteq V$. Nach (3.2) ist β ganz über R. $\square$

(3.5) **Definition.** Der Ring R heißt *ganz-abgeschlossen*, falls $R_{K|R} = R$ ist, d.h., falls jedes über R ganze Element des Quotientenkörpers K schon in R liegt.

Beispiele: (a) Ist R ein faktorieller Ring, so ist R ganz-abgeschlossen. Dies folgt aus dem Gauß-Lemma, denn ist $\alpha \in K$ ganz über R, so gibt es ein normiertes Polynom $f \in R[X]$ mit Wurzel α, und $X - \alpha$ ist ein Teiler von f in $R[X]$. Man kann dies auch direkt einsehen: Sei etwa

$$f(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0 \ (a_i \in R).$$

Schreibe $\alpha = \frac{a}{b}$ mit *teilerfremden* $a, b \in R$. Multiplikation mit b^n liefert die Identität $a^n = -b(a_{n-1}a^{n-1} + \cdots + a_1 ab^{n-2} + a_0 b^{n-1})$, so dass b ein Teiler von a^n ist. Da R faktoriell ist, folgt $b \mid a$ und $b \in R^*$.

(b) Der ganze Abschluss $S' = R_{L|R}$ von R in L ist ganz-abgeschlossen. Es ist nämlich $S' \supseteq R$ ein Integritätbereich nach (3.3), der nach (3.4) ganz-abgeschlossen ist (in L und damit im Quotientenkörper von S').

(3.6) **Lemma.** *Sei $S|R$ ganz und $\sigma : S \to S'$ ein Homomorphismus von Integritätsbereichen (die 1 erhaltend). Ist $\alpha \in S$ ganz über R, so ist $\alpha^\sigma = \sigma(\alpha)$ ganz über $R^\sigma = \sigma(R)$.*

Beweis. Sei $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$ ($a_i \in R$). Es folgt

$$(\alpha^\sigma)^n + a_{n-1}(\alpha^\sigma)^{n-1} + \cdots + a_0^\sigma = 0^\sigma = 0.$$

Also ist α^σ ganz über R^σ. $\square$

Konvention: Weiterhin in §3 sei $L|K$ eine Körpererweiterung endlichen Grades $[L : K] = n$ (und damit algebraisch). Für $\alpha \in L$ sei $\widehat{\alpha} : x \mapsto \alpha x$ ($x \in L$); dies ist ein K-Endomorphismus von L (und invertierbar für $\alpha \neq 0$). Es gilt (Algebra II, SS 2008, (10.3), oder Samuel. p. 36):

$$\det(XI_n - \widehat{\alpha}) = m_{K,\alpha}^{[L:K(\alpha)]}.$$

Definiere die *Spur* $\mathrm{Tr}_{L|K}(\alpha) = \mathrm{Spur}(\widehat{\alpha})$ und die *Norm* $\mathrm{N}_{L|K}(\alpha) = \det(\widehat{\alpha})$. Es ist $\mathrm{Tr}_{L|K} : L \to K$ eine K-Linearform und $\mathrm{N}_{L|K} : L^* \to K^*$ ein Gruppenhomomorphismus. Ist $m_{K,\alpha} = \prod_{i=1}^m (X - \alpha_i)$ die Faktorisierung in einem algebraischen Abschluss $\bar{K} \supseteq L$ von K, so ist

$$\mathrm{Tr}_{L|K}(\alpha) = [L : K(\alpha)] \sum_{i=1}^m \alpha_i, \;\; \mathrm{N}_{L|K}(\alpha) = \big((-1)^m \prod_{i=1}^m \alpha_i\big)^{[L:K(\alpha)]}.$$

(3.7) **Lemma.** *Genau dann ist $\mathrm{Tr}_{L|K} \neq 0$, wenn $L|K$ separabel ist. Ist R ganzabgeschlossen und $\alpha \in L$ ganz über R, so ist $m_{K,\alpha} \in R[X]$. In diesem Fall sind also $\mathrm{Tr}_{L|K}(\alpha)$ und $\mathrm{N}_{L|K}(\alpha)$ in R.*

Beweis. Sei zunächst $L|K$ separabel. Es gibt dann genau $n = [L : K]$ verschiedene K-Einbettungen $\sigma_1, \ldots, \sigma_n$ von L in $\bar{K}$. Die Wurzeln α_i von $m_{K,\alpha}$ sind gerade die α^{σ_j}, wobei jede Wurzel genau $[L : K(\alpha)]$ oft vorkommt. Es ist also $\mathrm{Tr}_{L|K}(\alpha) = \sum_{j=1}^n \alpha^{\sigma_j}$. Nach dem Lemma von Dedekind–Artin [Algebra II, (10.1)] sind die σ_j linear unabhängig im $\bar{K}$-Vektorraum aller Abbildungen $L^* \to \bar{K}$. Es ist also $\sigma_1 + \ldots + \sigma_n \neq 0$ in diesem Vektorraum, daher $\mathrm{Tr}_{L|K}(\beta) = \beta^{\sigma_1} + \ldots + \beta^{\sigma_n} \neq 0$ für ein $\beta \in L$.

Sei $L|K$ inseparabel. Dann ist $\mathrm{char}(K) = p$ eine Primzahl. Ist K_0 der separable Abschluss von K in L, so ist $L|K_0$ total inseparabel und $[L : K_0] = p^s$ für ein $s \geq 1$. Ist $\alpha \in L$ inseparabel über K, so ist $m_{K,\alpha} = g(X^{p^t})$ mit $g \in K[X]$ (irreduzibel) und maximalem $t \geq 1$, und jede Wurzel von $m_{K,\alpha}$ hat die Vielfachheit p^t. Daher ist $\mathrm{Tr}_{L|K}(\alpha) = 0$ in diesem Falle. Ist $\alpha \in L$ separabel über K, so ist $\alpha \in K_0$ und $[L : K(\alpha)]$ durch p teilbar, und wieder folgt $\mathrm{Tr}_{L|K}(\alpha) = 0$.

Sei nun R ganz-abgeschlossen und $\alpha \in R_{L|R}$. Nach (3.6) sind dann alle Wurzeln $\alpha_i = \alpha^{\sigma_i}$ von $f = m_{K,\alpha}$ ganz über $R = R^\sigma$. Nach (3.3) sind dann auch die Koeffizienten von f, die elementarsymmetrischen Funktionen der α_i, ganz über R. Damit folgt die Behauptung. $\square$

(3.8) **Satz.** *Sei $L|K$ separabel, R ganz-abgeschlossen und $S = R_{L|R}$ der ganze Abschluss von R in L. Zu jeder K-Basis $\{v_1, \cdots, v_n\}$ gibt es dann von Null verschiedene Elemente $a, b \in R$, so dass gilt:*

$$R(av_1) \oplus \ldots \oplus R(av_n) \subseteq S \subseteq R(\frac{v_1}{b}) \oplus \ldots \oplus R(\frac{v_n}{b}).$$

Ist insbesondere R ein Noetherscher Ring, so ist S ein Noetherscher R-Modul, somit selbst ein Noetherscher Ring.

Beweis. Wir können $a_i \neq 0$ in R so finden, dass $a_i v_i$ ganz über R ist (Multiplikation einer K-Relation für v_i mit einer geeigneten Potenz des Produktes der Nenner der Koeffizienten). Setze $a = a_1 \ldots a_n$. Dann $av_i \in S$ für alle i (ganz über R). Dies beweist den linken Teil der Aussage des Satzes.

Nach Voraussetzung und (3.7) ist die K-Bilinearform $(x, y) \mapsto \mathrm{Tr}_{L|K}(xy)$ auf $L^{(2)}$ nichtausgeartet. Daher existiert die *duale Basis* $\{v_i^*\}$ zu $\{v_i\}$ bzgl. dieser Form, für welche also gilt:

$$\mathrm{Tr}_{L|K}(v_i v_j^*) = \delta_{ij} = \begin{cases} 1 & \text{falls } i = j \\ 0 & \text{sonst} \end{cases}.$$

Wie eben gibt es $b \neq 0$ in R, so dass $bv_j^* \in S$ für alle j ist. Sei $\beta = \sum_{i=1}^n x_i v_i$ ein Element von S ($x_i \in K$). Da R ganz-abgeschlossen ist, liefert (3.7)

$$R \ni \mathrm{Tr}_{L|K}(\beta b v_j^*) = b\mathrm{Tr}_{L|K}\Big(\sum_{i=1}^n x_i v_i v_j^*\Big) = b\sum_{i=1}^n x_i \mathrm{Tr}_{L|K}(v_i v_j^*) = bx_j$$

für $j = 1, \ldots, n$. Folglich ist $x_j \in R(\frac{1}{b})$ und $\beta \in R(\frac{v_1}{b}) \oplus \ldots \oplus R(\frac{v_n}{b})$. $\square$

(3.9) **Diskriminanten.** Sei $L|K$ separabel (vom Grade n), R ganz-abgeschlossen und $S = R_{L|R}$ der ganze Abschluss von R in L. Für ein n-Tupel $(v_i) = (v_1, \ldots, v_n)$ in $L^{(n)}$ definiere die *Diskriminante*

$$D_{L|K}(v_1, \ldots, v_n) = \det\big(\mathrm{Tr}(v_i v_j)_{i,j}\big)$$

als die Gramsche Determinante der nach (3.7) nichtausgearteten symmetrischen K-Bilinearform $(x, y) \mapsto \mathrm{Tr}_{L|K}(xy)$ auf L. Es ist also $D_{L|K}(v_1, \ldots, v_n) \neq 0$ (in K) genau dann, wenn (v_i) eine (geordnete) K-Basis von L ist. Nach (3.8) gibt es eine solche K-Basis mit $v_i \in S$ für alle i, und dann ist $D_{L|K}(v_1, \ldots, v_n) \in R$ nach (3.7). Wir definieren die *relative Diskriminante* $D_{S|R}$ als das Ideal ($\neq 0$) von R erzeugt durch all diese Elemente.

Lemma. *Seien $\sigma_1, \dots, \sigma_n$ die verschiedenen K-Einbettungen von L in einen algebraischen Abschluss $\bar{K}$ von K.*

(a) *Ist $(u_1, \dots, u_n)^t = T(v_1, \dots, v_n)^t$ für eine K-Basis (v_i) von L und $T \in \mathrm{GL}_n(K)$, so ist $D_{L|K}(u_1, \dots, u_n) = \det(T)^2 D_{L|K}(v_1, \dots, v_n)$.*

(b) $D_{L|K}(v_1, \dots, v_n) = \det(v_i^{\sigma_k})^2$.

(c) *Ist $\alpha \in L$ primitiv für $L|K$ (Gauß), so ist $D_{L|K}(1, \alpha, \dots, \alpha^{n-1}) = D_f$ die Diskriminante von $f = m_{K,\alpha}$.*

Beweis. (a) Sei $T = (t_{ij})$. Dann ist $\mathrm{Tr}_{L|K}(u_k u_\ell) = \sum_{i,j} t_{ki} t_{\ell j} \mathrm{Tr}_{L|K}(v_i v_j)$ und somit $\big(\mathrm{Tr}_{L|K}(u_k u_l)\big) = T\big(\mathrm{Tr}_{L|K}(v_i v_j)\big)T^t$.

(b) $\mathrm{Tr}_{L|K}(v_i v_j) = \sum_k v_i^{\sigma_k} v_i^{\sigma_k}$, also $\big(\mathrm{Tr}_{L|K}(v_i v_j)\big) = (v_i^{\sigma_k})(v_j^{\sigma_k})^t$.

(c) Hier ist $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ eine K-Basis von L, und die $\alpha_k = \alpha^{\sigma_k}$ sind die verschiedenen Wurzeln von $f = m_{K,\alpha}$. Es ist

$$D_{L|K}(1, \alpha, \alpha^2, \dots, \alpha^{n-1}) = \begin{vmatrix} 1 & \alpha_1 & \dots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \dots & \alpha_2^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \dots & \alpha_n^{n-1} \end{vmatrix}^2 = \prod_{i<j} (\alpha_i - \alpha_j)^2$$

(Vandermonde). Dies ist definitionsgemäß die Diskriminante D_f des Polynoms f. □

Anmerkung: Ist f' die (formale) Ableitung von f, so gilt $D_f = (-1)^{\binom{n}{2}} \mathrm{N}_{L|K}(f'(\alpha))$.

(3.10) **Zahlkörperfall:** Sei $R = \mathbb{Z}$, $K = \mathbb{Q}$, L ein algebraischer Zahlkörper und $S = R_L$. Nach (3.8) und (0.3) ist dann S ein freier $\mathbb{Z}$-Modul vom Range $n = [L : \mathbb{Q}]$; eine $\mathbb{Z}$-Basis von R_L heißt auch *Ganzheitsbasis* von L. Ist (v_i) eine solche Ganzheitsbasis, so ist die *absolute Diskriminante* von L wohldefiniert durch

$$D_L = D_{L|\mathbb{Q}}(v_1, \dots, v_n),$$

denn nach (3.9)(a) ist dies unabhängig von der Wahl der Ganzheitsbasis ($\det(T)^2 = 1$ für $T \in \mathrm{GL}_n(\mathbb{Z})$). Es ist $D_L \neq 0$ eine ganze Zahl und $D_{S|\mathbb{Z}} = D_L\mathbb{Z}$. Die Diskriminante D_L ist eine wichtige Invariante für L.

Es gibt immer $\alpha \in S = R_L$ mit $L = \mathbb{Q}(\alpha)$, und dann ist der Ring $\mathbb{Z}[\alpha]$ ein freier $\mathbb{Z}$-Teilmodul von S mit demselben Rang n. Daher ist der Index $|S : \mathbb{Z}[\alpha]| = m$ endlich nach (0.3). Es gibt eine $\mathbb{Z}$-Basis (v_i) von S und Elementarteiler $e_i \mid e_{i+1}$, so dass $(e_i v_i)$ eine $\mathbb{Z}$-Basis von $\mathbb{Z}[\alpha]$ ist. Die Diagonalmatrix $T = \mathit{diag}(e_1, \dots, e_n)$ beschreibt dann einen $\mathbb{Z}$-Isomorphismus von S auf $\mathbb{Z}[\alpha]$, und es ist $\det(T) = e_1 \cdots e_n = m$. Nach (3.9) ist also

$$D_f = [R_L : \mathbb{Z}[\alpha]]^2 D_L$$

für $f = m_{\mathbb{Q},\alpha}$. Ist also D_f/D_L quadratfrei, so ist $D_f = D_L$ und $R_L = \mathbb{Z}[\alpha]$ ein sog. *monogener* Ring über $\mathbb{Z}$.

§4. Primideale

Es sei R (zunächst) ein Integritätsbereich mit Quotientenkörper K. Eine *multiplikative Teilmenge* M von R ist eine solche mit $1 \in M$, $0 \notin M$ und der Eigenschaft, dass mit $x, y \in M$ auch $xy \in M$ ist. Ein Primideal $\mathfrak{p}$ von R ist ein (echtes) Ideal, für welches der Restklassenring $R/\mathfrak{p}$ ein Integritätsbereich ist, d.h., für welches $M_\mathfrak{p} = R \setminus \mathfrak{p}$ eine multiplikative Teilmenge von R ist. Formal ist hier das Nullideal auch ein Primideal, aber dies schließen wir (meist) aus. Mit $\mathbb{P}_R$ wird die Menge der Primideale $\mathfrak{p} \neq 0$ von R bezeichnet (Primstellen).

(4.1) **Definition.** Sei M eine multiplikative Teilmenge von R. Dann heißt die Teilmenge

$$R_M = \{\frac{a}{b} \mid a \in R, b \in M\}$$

von K die *Lokalisierung* von R durch M. Es ist klar, dass dies ein Teilring von K ist, der R enthält. Ist $M = M_\mathfrak{p} = R \setminus \mathfrak{p}$ für ein Primideal $\mathfrak{p}$ ($\neq 0$) von R, so schreiben wir $R_\mathfrak{p} = R_{M_\mathfrak{p}}$ (Lokalisierung bei $\mathfrak{p}$).

Ist V ein (unitärer) R-Modul, der in einem Erweiterungskörper von K liegt, so ist entsprechend $V_M = \{\frac{v}{b} \mid v \in V, b \in M\}$, und dies ist ein R_M-Modul in kanonischer Weise (Bruchrechnen).

(4.2) **Satz.** *Ist $\mathfrak{p}$ ein Primideal ($\neq 0$) von R, so ist $R_\mathfrak{p}$ ein "lokaler Ring", d.h., $R_\mathfrak{p}$ hat genau ein maximales Ideal $\mathfrak{m} = \{\frac{a}{b} \mid a \in \mathfrak{p}, b \in R \setminus \mathfrak{p}\}$. Es ist $R \cap \mathfrak{m} = \mathfrak{p}$. Ist $\mathfrak{p}$ ein maximales Ideal von R, so gilt zudem $R + \mathfrak{m} = R_\mathfrak{p}$. In diesem Fall definiert also $a \mapsto a + \mathfrak{m}$ einen natürlichen Epimorphismus (von Ringen mit 1) von R auf den "Restklassenkörper" $k_\mathfrak{p} = R_\mathfrak{p}/\mathfrak{m}$ von $R_\mathfrak{p}$ mit Kern $\mathfrak{p}$: $R/\mathfrak{p} \cong k_\mathfrak{p}$.*

Beweis. Sind $a, b \in R \setminus \mathfrak{p}$, so existiert $(\frac{a}{b})^{-1} = \frac{b}{a}$ in $R_\mathfrak{p}$. Es ist also $R_\mathfrak{p}^* = R_\mathfrak{p} \setminus \mathfrak{m}$ und $\mathfrak{m}$ als Menge der Nichteinheiten von $R_\mathfrak{p}$ das einzige maximale Ideal. Ist $x = \frac{a}{b}$ ein Element von $R \cap \mathfrak{m}$ ($a \in \mathfrak{p}$, $b \in R \setminus \mathfrak{p}$), so ist $a = bx \in \mathfrak{p}$ und $b \notin \mathfrak{p}$, somit $x \in \mathfrak{p}$. Folglich ist $R \cap \mathfrak{m} \subseteq \mathfrak{p}$; die umgekehrte Inklusion ist trivial.

Sei $\mathfrak{p}$ ein maximales Ideal von R. Sei $x = \frac{a}{b}$ ein Element von $R_\mathfrak{p}$ ($a \in R$, $b \in R \setminus \mathfrak{p}$). Dann ist das Summenideal (ggT) $(\mathfrak{p}, b) = \mathfrak{p} + bR = R$. Es gibt also $y \in \mathfrak{p}$ und $r \in R$ mit $1 = y + br$. Folglich ist

$$x = a\frac{y}{b} + ar \in \mathfrak{m} + R.$$

Dies beweist auch die letzte Aussage. □

Ist beispielsweise $R = \mathbb{Z}$ und $p \in \mathbb{P}$ eine Primzahl, dann ist $(p) = p\mathbb{Z}$ ein maximales Ideal von $\mathbb{Z}$. In diesem Falle ist der lokale Ring $\mathbb{Z}_{(p)}$, ebenso wie $\mathbb{Z}$, ein Hauptidealring. Bis auf Einheiten ist p das einzige Primelement von $\mathbb{Z}_{(p)}$. Es ist $p\mathbb{Z}_{(p)}$ das maximale Ideal von $\mathbb{Z}_{(p)}$, mit Restklassenkörper $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

(4.3) **Lemma.** *Sei M eine multiplikative Teilmenge von R und $L|K$ eine Körpererweiterung. Ist $S = R_{L|R}$, so ist $S_M = R_{L|S_M}$.*

Beweis. Sei $a \in S$ und $b \in M$. Ist $V \neq 0$ ein endlich erzeugter R-Modul mit $aV \subseteq V$, so ist V_M ein endlich erzeugter R_M-Modul mit $\frac{a}{b}V_M \subseteq V_M$. Nach (3.2) ist $\frac{a}{b}$ ganz über R_M. Ist $y \in L$ ganz über R_M, etwa

$$y^n + \frac{a_{n-1}}{b_{n-1}}y^{n-1} + \ldots + \frac{a_0}{b_0} = 0$$

mit $a_i \in R$ und $b_i \in M$, so ist by ganz über R für $b = (b_0 \ldots b_{n-1})^n \in M$. Also liegt by in $S = R_{L|R}$ und $y \in S_M$. $\square$

(4.4) **Lemma.** *Seien U und V R-Moduln (in einem Erweiterungskörper von R). Gilt $U_\mathfrak{p} \subseteq V_\mathfrak{p}$ für alle maximalen Ideale $\mathfrak{p}$ von R, so ist $U \subseteq V$.*

Beweis. Sei $u \in U$. Nach Voraussetzung gibt es zu jedem maximalen Ideal $\mathfrak{p}$ von R Elemente $a_\mathfrak{p} \in R \setminus \mathfrak{p}$ und $v_\mathfrak{p} \in V$ mit $u = \frac{v_\mathfrak{p}}{a_\mathfrak{p}}$. Sei $\mathfrak{a}$ das Ideal von R erzeugt durch die $a_\mathfrak{p}$. Nach Konstruktion liegt es in keinem maximalen Ideal von R. Da jedes echte Ideal von R in einem maximalen Ideal liegt (Lemma von Zorn), ist $\mathfrak{a} = R$. Folglich gibt es eine *endliche* Darstellung

$$1 = \sum_\mathfrak{p} x_\mathfrak{p} a_\mathfrak{p}$$

mit gewissen $x_\mathfrak{p} \in R$. Aber dann ist $u = \sum x_\mathfrak{p} a_\mathfrak{p} u = \sum x_\mathfrak{p} v_\mathfrak{p}$ in V. $\square$

(4.5) **Satz.** *Sei M eine multiplikative Teilmenge von R. Die Zuordnung $\mathfrak{p} \mapsto \mathfrak{p}_M$ ist eine Bijektion von den Primidealen $\mathfrak{p}$ von R mit $\mathfrak{p} \cap M = \varnothing$ auf die Primideale von R_M.*

Beweis. Gilt $\mathfrak{p} \cap M = \varnothing$, so ist $\mathfrak{p}_M = \mathfrak{p}R_M$ ein Primideal von R_M und $R \cap \mathfrak{p}_M = \mathfrak{p}$. (Ist $x = \frac{p}{b}$ in $R \cap \mathfrak{p}_M$, mit $p \in \mathfrak{p}$, $b \in M$, so ist mit $p = bx$ auch $x \in \mathfrak{p}$, denn $b \notin \mathfrak{p}$.) Ist umgekehrt $\mathfrak{p}'$ ein Primideal von R_M, so ist $\mathfrak{p} = R \cap \mathfrak{p}'$ ein Primideal von R ($x, y \in R \setminus \mathfrak{p}'$ impliziert $xy \in R \setminus \mathfrak{p}'$), und es gilt $\mathfrak{p} \cap M = \varnothing$, da sonst $1 \in \mathfrak{p}'$ wäre). Es gilt $\mathfrak{p}_M = \mathfrak{p}'$, denn ist $\frac{a}{b} \in \mathfrak{p}'$ mit $a \in R$, $b \in M$, so ist $a = \frac{a}{b} \cdot b \in R \cap \mathfrak{p}' = \mathfrak{p}$ und daher $\frac{a}{b} = \frac{1}{b}a \in \mathfrak{p}_M$. $\square$

Zusatz. Für Ideale $\mathfrak{a}$, $\mathfrak{b}$ von R ist das Produktideal $\mathfrak{ab}$ die Menge aller endlichen Summen $\sum ab$ ($a \in \mathfrak{a}$, $b \in \mathfrak{b}$). Es ist $(\mathfrak{ab})_M = \mathfrak{a}_M \cdot \mathfrak{b}_M$. Die Zuordnung $\mathfrak{a} \mapsto \mathfrak{a}_M$ ist ein Epimorphismus (von Halbgruppen) der Ideale von R auf die von R_M, dessen Kern aus den Idealen $\mathfrak{a}$ besteht mit $\mathfrak{a} \cap M \neq \varnothing$.

Weiterhin sei R ein kommutativer Ring (mit $1 \neq 0$), nicht notwendig nullteilerfrei. Ein R-Modul V heißt *Noethersch*, falls jede nichtleere Menge von Teilmoduln von V ein

maximales Element (bzgl. Inklusion) besitzt. Dies ist gleichwertig mit: Jeder Teilmodul von V ist endlich erzeugt, oder: Jede aufsteigende Kette von Teilmoduln wird nach endlich vielen Schritten konstant (vgl. Samuel, p. 20). R ist ein *Noetherscher Ring*, falls R als Modul über sich selbst Noethersch ist. Dann sind endlich erzeugte R-Moduln automatisch Noethersch.

(4.6) **Satz.** *Sei R ein Noetherscher Ring (kommutativ mit $1 \neq 0$).*

(a) *Jedes Ideal $\mathfrak{a} \neq 0$ von R enthält ein (endliches) Produkt von Primidealen $\neq 0$.*

(b) *Der Durchschnitt der Primideale von R ist die Menge der nilpotenten Elemente von R (Nilradikal).*

Beweis. (a) Angenommen, dies ist falsch. Sei dann $\mathfrak{a}$ maximal gewählt (bzgl. Inklusion) ohne die behauptete Eigenschaft (R Noethersch). Dann ist $\mathfrak{a} \neq R$ und natürlich auch kein Primideal von R. Daher gibt es $x, y \in R \setminus \mathfrak{a}$ mit $xy \in \mathfrak{a}$. Betrachte die Summenideale $\mathfrak{a}_x = \mathfrak{a} + xR$ und $\mathfrak{a}_y = \mathfrak{a} + yR$. Da beide $\mathfrak{a}$ echt enthalten, gibt es nach Wahl von $\mathfrak{a}$ Primideale $\mathfrak{p}_i$ und $\mathfrak{q}_j$ mit

$$\mathfrak{a}_x \supseteq \mathfrak{p}_1 \dots \mathfrak{p}_r, \;\; \mathfrak{a}_y \supseteq \mathfrak{q}_1 \dots \mathfrak{q}_s.$$

Wegen $xy \in \mathfrak{a}$ ist dann aber $\mathfrak{a} \supseteq \mathfrak{a}_x \mathfrak{a}_y \supseteq \mathfrak{p}_1 \dots \mathfrak{p}_r \mathfrak{q}_1 \dots \mathfrak{q}_s$, entgegen unserer Annahme.

(b) Die Aussage gilt allgemein (ohne "Noethersch"); dann hat man das Lemma von Zorn heranzuziehen. Ist $a \in R$ nilpotent, d.h, $a^n = 0$ für ein $n \in \mathbb{N}$, so liegt a in jedem Primideal von R. Diese Elemente bilden auch ein Ideal des (kommutativen) Rings R. Sei $u \in R$ nicht nilpotent. Wir haben ein Primideal $\mathfrak{p}$ von R zu finden mit $u \notin \mathfrak{p}$. Betrachte die Menge der Ideale von R, die keine Potenz von u enthalten. Diese Menge enthält das Nullideal. Sei $\mathfrak{p}$ ein maximales Element in dieser Menge. (Als Übung zeige man, dass diese Menge induktiv geordnet ist.) Dann ist $u^n \notin \mathfrak{p}$ für alle n. Seien $x, y \in R \setminus \mathfrak{p}$. Dann ist $\mathfrak{p} + xR \supset \mathfrak{p}$, also $u^r \in \mathfrak{p} + xR$ für ein r. Analog ist $u^s \in \mathfrak{p} + yR$ für ein s. Damit ist aber

$$u^{r+s} \in (\mathfrak{p} + xR)(\mathfrak{p} + yR) \subseteq \mathfrak{p} + xyR.$$

Wegen $u^{r+s} \notin \mathfrak{p}$ folgt $xy \notin \mathfrak{p}$. Daher ist $\mathfrak{p}$ ein Primideal von R. $\square$

Der Durchschnitt der maximalen Ideale von R heißt das *Jacobson-Radikal* $J(R)$. Unter gewissen Endlichkeitsforderungen ist $J(R)$ identisch mit dem Nilradikal (etwa wenn alle Primideale $\neq 0$ maximale Ideale sind).

(4.7) **Lemma** (Nakayama). *Sei $\mathfrak{a}$ ein Ideal von R mit $\mathfrak{a} \subseteq J(R)$. Ist V ein endlich erzeugter R-Modul mit $\mathfrak{a}V = V$, so ist $V = 0$.*

Beweis. Angenommen, es ist $V \neq 0$. Nach Voraussetzung ist V als R-Modul endlich erzeugbar. Ist r die *minimale* Erzeugendenzahl und V erzeugt durch $v_1, \dots v_r$, so gibt es wegen $\mathfrak{a}V = V$ eine Darstellung

$$v_1 = a_1 v_1 + \ldots + a_r v_r$$

mit $a_i \in \mathfrak{a}$. Daher ist $(1-a_1)v_1 = a_2 v_2 + \ldots + a_r v_r$. Es ist $1 - a_1$ eine Einheit in R, denn sonst wäre $1 - a_1$ in einem maximalen Ideal $\mathfrak{p}$ von R (Lemma von Zorn), und wegen $a_1 \in \mathfrak{a} \subseteq \mathfrak{p}$ wäre $1 \in \mathfrak{p}$. Daher ist V durch $v_2, \dots, v_r$ erzeugbar, ein Widerspruch. □

Meist wird (4.7) so angewandt: Ist V ein endlich erzeugter R-Modul und U ein Teilmodul mit $\mathfrak{a}V + U = V$, so ist $U = V$ ($\mathfrak{a} \subseteq J(R)$). Dann ist nämlich V/U ein endlich erzeugter R-Modul mit $\mathfrak{a}(V/U) = V/U$.

Seien $\mathfrak{a}_1, \dots, \mathfrak{a}_r$ endlich viele paarweise teilerfremde (echte) Ideale von R, d.h., $\mathfrak{a}_i + \mathfrak{a}_j = R$ für $i \neq j$ ($r \geq 2$). Dann ist $\mathfrak{a}_i \cap \mathfrak{a}_j = \mathfrak{a}_i\mathfrak{a}_j$ für $i \neq j$, denn es gibt $a_i \in \mathfrak{a}_i$ und $a_j \in \mathfrak{a}_j$ mit $a_i + a_j = 1$, und für jedes $x \in \mathfrak{a}_i \cap \mathfrak{a}_j$ ist $x = xa_i + xa_j \in \mathfrak{a}_i\mathfrak{a}_j$. Die Umkehrung ist trivial. Sind x, y beliebige Elemente von R, so ist $a = xa_i + ya_j$ ein Element in R mit

$$a \equiv ya_j \equiv y(1 - a_i) \equiv y - ya_i \equiv y \,(\mathrm{mod}\, \mathfrak{a}_i).$$

Analog ist $a \equiv x \,(\mathrm{mod}\, \mathfrak{a}_j)$. Wir haben die Kongruenzen *simultan* gelöst.

(4.8) **Satz** (Chinesischer Restesatz). *Unter obigen Vorausetzungen ist der natürliche Homomorphismus $a \mapsto (a+\mathfrak{a}_1, \dots, a+\mathfrak{a}_r)$ ein Epimorphismus von R auf das direkte Produkt $R/\mathfrak{a}_1 \times \ldots \times R/\mathfrak{a}_r$ der Restklassenringe $R/\mathfrak{a}_i$ (komponentenweise Addition und Multiplikation) mit Kern $\bigcap_{i=1}^r \mathfrak{a}_i = \prod_{i=1}^r \mathfrak{a}_i$.*

Beweis. Den Fall $r = 2$ haben wir schon erledigt. Sei $r > 2$ und $\mathfrak{b} = \mathfrak{a}_2 \dots \mathfrak{a}_r$. Induktiv gilt $R/\mathfrak{b} \cong R/\mathfrak{a}_2 \times \ldots \times R/\mathfrak{a}_r$. Für jedes $i \geq 2$ gibt es Elemente $z_i \in \mathfrak{a}_1$ und $a_i \in \mathfrak{a}_i$ mit $z_i + a_i = 1$ und daher ist ist

$$1 = \prod_{i=2}^{r} (z_i + a_i) = c + a_2 \dots a_r,$$

wobei c eine Summe von Termen mit Faktoren z_i ist und daher in $\mathfrak{a}_1$ liegt. Wegen $a_2 \dots a_r \in \mathfrak{b}$ ist also $\mathfrak{a}_1 + \mathfrak{b} = R$. Nach dem schon erledigten Fall ist $R/\mathfrak{a}_1\mathfrak{b} \cong R/\mathfrak{a}_1 \times R/\mathfrak{b}$, und der Satz bewiesen. □

Der Isomorphismus $R/\mathfrak{a}_1 \dots \mathfrak{a}_r \cong R/\mathfrak{a}_1 \times \ldots \times R/\mathfrak{a}_r$ induziert einen Isomorphismus der Einheitengruppen.

(4.9) **Beispiel.** Sei $n = p_1^{e_1} \dots p_r^{e_r}$ die Primfaktorzerlegung der natürlichen Zahl $n \geq 2$. Dann ist die *prime Restklassengruppe*

$$(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/p_1^{e_1}\mathbb{Z})^* \times \ldots \times (\mathbb{Z}/p_r^{e_r}\mathbb{Z})^*.$$

Für die Eulersche φ-Funktion gilt also $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*| = \varphi(p_1^{e_1}) \dots \varphi(p_r^{e_r})$.

§5. Dedekindringe

Die Ringe ganzer Zahlen algebraischer Zahlkörper sind sog. Dedekindringe (R. Dedekind, 1831-1916). Die Untersuchung ihrer Idealtheorie ist ein zentrales Thema der Algebraischen Zahlentheorie.

(5.1) **Definition.** Sei R ein Integritätsbereich (mit $1 \neq 0$). R heißt ein *Dedekindring*, falls gilt:

(D1) R ist Noethersch;

(D2) R ist ganz-abgeschlossen (in seinem Quotientenkörper K);

(D3) Jedes Primideal $\mathfrak{p} \neq 0$ von R ist ein maximales Ideal.

Wir vereinbart bezeichnen wir mit $\mathbb{P}_R$ die Menge der Primideale $\neq 0$ von R. Diese Menge ist genau dann leer, wenn R ein Körper ist. Wir wollen dies in Zukunft ausschließen. Ist R ein Dedekindring und $\mathfrak{p} \in \mathbb{P}_R$, so heißt $k_\mathfrak{p} = R/\mathfrak{p}$ der *Restklassenkörper* von $\mathfrak{p}$ (D3).

(5.2) **Satz.** *Ist K ein algebraischer Zahlkörper, so ist $R = R_K$ ein Dedekindring; genauer: R ist ein freier $\mathbb{Z}$-Modul vom (endlichen) Range $n = [K : \mathbb{Q}]$, und für jedes $\mathfrak{p} \in \mathbb{P}_R = \mathbb{P}_K$ ist der Restklassenkörper $k_\mathfrak{p} = R/\mathfrak{p}$ endlich.*

Beweis. Nach (3.10) ist R ein freier $\mathbb{Z}$-Modul vom Range n. Sei $\mathfrak{a} \neq 0$ ein Ideal von R. Aus der Ganzheit von $\mathfrak{a}$ über $\mathbb{Z}$ folgt, dass $\mathfrak{a} \cap \mathbb{Z} \neq 0$ ist. (Vergleiche mit (1.5); jedes $0 \neq \alpha \in \mathfrak{a}$ genügt einer Relation $\alpha^m + c_{m-1}\alpha^{m-1} + \cdots + c_0 = 0$ mit $c_i \in \mathbb{Z}$, $c_0 \neq 0$, und $c_0 \in \mathfrak{a}$.) Daher enthält $\mathfrak{a}$ eine positive ganze Zahl m, und die *absolute Norm*

$$\mathrm{N}\mathfrak{a} = |R/\mathfrak{a}|$$

ist als Teiler von $|R/mR| = m^n$ endlich. Insbesondere sind die Restklassenringe nach Primidealen $\neq 0$ endliche Intergritätsbereiche und damit Körper. Übrigens ist nach (0.3) auch $\mathfrak{a}$ ein freier $\mathbb{Z}$-Modul vom Range n. $\square$

(5.3) **Satz.** *Sei R ein Dedekindring mit Quotientenkörper K. Sei $L|K$ eine endliche separable Körpererweiterung und $S = R_{L|R}$ der ganze Abschluss von R in L. Dann ist S ein Dedekindring.*

Beweis. (D1) folgt aus (3.9) und (D2) aus (3.5). Wir haben (D3) noch nachzuweisen. Sei $\mathfrak{P} \neq 0$ ein Primideal von S. Dann ist $\mathfrak{p} = \mathfrak{P} \cap R$ ein Primideal von R ($x, y \in R \setminus \mathfrak{P} \Rightarrow xy \in R \setminus \mathfrak{P}$). Ferner ist $\mathfrak{p} \neq 0$, denn jedes $0 \neq \beta \in \mathfrak{P}$ ist ganz über R, genügt also einer Relation $\beta^n + a_{n-1}\beta^{n-1} + \ldots + a_0 = 0$ mit $a_i \in R$, wobei wir $a_0 \neq 0$ annehmen dürfen (siehe oben). Es ist $a_0 \in \mathfrak{P} \cap R = \mathfrak{p}$. Da R ein Dedekindring ist, ist $\mathfrak{p}$ ein maximales Ideal von R, also $k_\mathfrak{p} = R/\mathfrak{p}$ ein Körper.

Sei $\sigma : y \mapsto y + \mathfrak{P}$ der kanonische (Ring-) Epimorphismus von S auf $k_\mathfrak{P} = S/\mathfrak{P}$. Es ist $\mathrm{Ker}(\sigma) = \mathfrak{p}$. Nach (3.6) ist $k_\mathfrak{P}|k_\mathfrak{p}$ ganz. Da $k_\mathfrak{p}$ ein Körper ist, ist damit nach (3.1) auch $k_\mathfrak{P}$ ein Körper. $\square$

(5.4) **Definition.** Weiterhin in diesem §5 sei R ein Dedekindring mit Quotientenkörper K. Ein R-Teilmodul $\mathfrak{b} \neq 0$ von K heißt *gebrochenes Ideal* von R, falls es $0 \neq b \in R$ gibt mit $b\mathfrak{b} \subseteq R$, d.h., $\mathfrak{a} = b\mathfrak{b}$ ist ein gewöhnliches (*ganzes*) Ideal von R. Ist schon $\mathfrak{b} \subseteq R$, so ist $\mathfrak{b}$ ein (ganzes) Ideal. Ein gebrochenes Hauptideal ist von der Form $R\frac{a}{b}$ mit Elementen a, b $(\neq 0)$ von R. Für die gebrochenen Ideale sind Summe, Produkt wie für Ideale erklärt; es gibt immer gemeinsame Nenner! Wir definieren noch für jedes gebrochene Ideal $\mathfrak{b}$ von R:

$$\mathfrak{b}^{-1} = \{x \in K |\ x\mathfrak{b} \subseteq R\}.$$

(5.5) **Lemma.** *Die gebrochenen Ideale von R sind genau die von 0 verschiedenen endlich erzeugten R-Teilmoduln von K. Sie bilden bzgl. Multiplikation eine kommutative Halbgruppe I_R mit Neutralelement R. Ist $\mathfrak{a} \in I_R$ ein ganzes Ideal, so ist $\mathfrak{a}^{-1}$ ein gebrochenes Ideal von R mit $R \subseteq \mathfrak{a}^{-1}$ und $\mathfrak{a}\mathfrak{a}^{-1} \subseteq R$.*

Beweis. Jeder endlich erzeugte R-Teilmodul $\neq 0$ von K is ein gebrochenes Ideal, da es zu endlich vielen Elementen $\frac{a_i}{b_i}$ in K $(a_i, b_i \in R)$ den gemeinsamen Nenner $b = \prod b_i$ gibt. Da R Noethersch ist (D1), sind alle Ideale, und damit auch alle gebrochenen Ideale, endlich erzeugt über R.

Sei $\mathfrak{a} \neq 0$ ein ganzes Ideal von R. Dann ist $R \subseteq \mathfrak{a}^{-1}$. Ferner ist $\mathfrak{a}^{-1}$ ein R-Teilmodul von K mit $b\mathfrak{a}^{-1} \subseteq R$ für jedes $0 \neq b \in \mathfrak{a}$, daher ein gebrochenes Ideal von R. Somit ist auch $\mathfrak{a}\mathfrak{a}^{-1} \subseteq R$. $\square$

(5.6) **Lemma.** *Für jedes Primideal $\mathfrak{p} \neq 0$ von R gilt $\mathfrak{p}\mathfrak{p}^{-1} = R$.*

Beweis. Angenommen, dies ist falsch. Nach (5.5) ist $\mathfrak{p} = R\mathfrak{p} \subseteq \mathfrak{p}^{-1}\mathfrak{p} \subseteq R$. Da $\mathfrak{p}$ ein maximales Ideal von R ist (D3), gilt nach Annahme also $\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}$. Wir wissen auch, dass $\mathfrak{p}^{-1} \supseteq R$ ist. Für jedes $x \in \mathfrak{p}^{-1}$ gilt nun $x\mathfrak{p} \subseteq \mathfrak{p}$, und $\mathfrak{p}$ ist ein endlich erzeugter R-Modul. Nach (3.2) ist daher jedes Element von $\mathfrak{p}^{-1}$ ganz über R. Da R ganz abgeschlosen ist (D2), folgt $\mathfrak{p}^{-1} = R$.

Um dies zu einem Widerspruch zu führen, "konstruieren" wir ein Element $\frac{a}{b}$ in $K \setminus R$ mit $\frac{a}{b}\mathfrak{p} \subseteq R$. Sei dazu $b \neq 0$ ein beliebiges Element von $\mathfrak{p}$. Nach (4.6) gibt es eine kleinste Nummer r, so dass $(b) = Rb$ das Produkt von r Primidealen $\mathfrak{p}_i$ von R enthält. Da $\mathfrak{p}$ ein Primideal von R mit

$$\mathfrak{p} \supseteq Rb \supseteq \mathfrak{p}_1 \ldots \mathfrak{p}_r$$

ist, liegt mindestens eines der Primideale, etwa $\mathfrak{p}_1$, in $\mathfrak{p}$. Da $\mathfrak{p}_1$ ein maximales Ideal von R ist (D3), folgt $\mathfrak{p}_1 = \mathfrak{p}$. Setze $\mathfrak{a} = \mathfrak{p}_2 \dots \mathfrak{p}_r$. Es ist $Rb \supseteq \mathfrak{p}\mathfrak{a}$ aber $Rb \not\supseteq \mathfrak{a}$, da r minimal gewählt war. Es gibt daher $a \in \mathfrak{a}$ mit $a \notin Rb$. Aus $\mathfrak{p}\mathfrak{a} \subseteq Rb$ folgt $\frac{a}{b}\mathfrak{p} \subseteq R$ und $\frac{a}{b} \in \mathfrak{p}^{-1}$. Wegen $a \notin Rb$ ist $\frac{a}{b} \notin R$. $\square$

(5.7) **Hauptsatz.** *Das Monoid I_R der gebrochenen Ideale des Dedekindrings R ist eine freie abelsche Gruppe mit $\mathbb{Z}$-Basis $\mathbb{P}_R$. Jedes gebrochene Ideal $\mathfrak{a}$ von R hat eine eindeutige Darstellung der Form*

$$\mathfrak{a} = \prod_{\mathfrak{p} \in \mathbb{P}_R} \mathfrak{p}^{n_\mathfrak{p}(\mathfrak{a})}$$

mit ganzen Zahlen $n_\mathfrak{p}(\mathfrak{a})$, der Ordnung von $\mathfrak{a}$ bei $\mathfrak{p}$ ($n_\mathfrak{p}(\mathfrak{b}) = 0$ fast immer).

Bemerkung. Sei H_R die *Gruppe* der gebrochenen Hauptideale von R. Die Faktorgruppe $\mathrm{C}\ell_R = I_R/H_R$ heißt die *Idealklassengruppe* von R. Genau dann ist R ein Hauptidealring, wenn $\mathrm{C}\ell_R$ trivial ist ($I_R = H_R$).

Beweis. (Existenz) Es genügt zu zeigen, dass jedes ganze Ideal ($\neq 0$) Produkt von Primidealen von R ist. Angenommen, dies ist falsch und $\mathfrak{a}$ sei entsprechend maximal (bzgl. Inklusion) gewählt (R Noethersch). Dann ist $\mathfrak{a} \subset R$ (R = leeres Produkt), liegt daher (echt) in einem Primideal (maximalen) Ideal $\mathfrak{p}$ von R. Nach (5.6) ist

$$\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} = R.$$

Wäre $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$, so wäre jedes Element von $\mathfrak{p}^{-1}$ ganz über R nach (3.2), und es folgte der Widerspruch $\mathfrak{p}^{-1} = R$ (5.6). (Dieses Argument hatten wir eben schon.) Daher ist $\mathfrak{a} \subset \mathfrak{a}\mathfrak{p}^{-1}$, somit $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_1 \dots \mathfrak{p}_r$ mit Primidealen $\mathfrak{p}_i$ von R, nach Wahl von $\mathfrak{a}$. Aber dann ist $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r\mathfrak{p}$.

(Eindeutigkeit) Sei $\prod_{\mathfrak{p} \in \mathbb{P}_R} \mathfrak{p}^{n_\mathfrak{p}} = \prod_{\mathfrak{p} \in \mathbb{P}_R} \mathfrak{p}^{m_\mathfrak{p}}$ mit ganzen Zahlen $n_\mathfrak{p}$, $m_\mathfrak{p}$, die für fast alle $\mathfrak{p}$ Null sind. Wäre $n_\mathfrak{p} - m_\mathfrak{p} \neq 0$ für ein $\mathfrak{p}$, so können wir wegen (5.6) die positiven und negativen Exponenten separieren und erhielten eine Darstellung;

$$\mathfrak{p}_1^{n_1} \dots \mathfrak{p}_r^{n_r} = \mathfrak{q}_1^{m_1} \dots \mathfrak{q}_s^{m_s}$$

mit paarweise verschiedenen Primidealen $\mathfrak{p}_i$, $\mathfrak{q}_j$ und $n_i > 0$, $m_j > 0$. Dann ist das Primideal $\mathfrak{p}_1 \supseteq \mathfrak{q}_1^{m_1} \dots \mathfrak{q}_s^{m_s}$, enthält damit eines der Primideale $\mathfrak{q}_j$, etwa $\mathfrak{q}_1$. Da $\mathfrak{q}_1$ ein maximales Ideal von R ist, folgt $\mathfrak{p}_1 = \mathfrak{q}_1$, ein Widerspruch.

Das Inverse von $\mathfrak{b} = \prod_{\mathfrak{p} \in \mathbb{P}_R} \mathfrak{p}^{n_\mathfrak{p}(\mathfrak{b})}$ ist $\mathfrak{b}^{-1} = \prod_{\mathfrak{p} \in \mathbb{P}_R} \mathfrak{p}^{-n_\mathfrak{p}(\mathfrak{b})}$. Daher ist I_R eine Gruppe. $\square$

(5.8) **Lemma.** *Für $\mathfrak{p} \in \mathbb{P}_R$ sei $n_\mathfrak{p} : I_R \to \mathbb{Z}$ die Ordnungsfunktion gemäß (5.7). Es gilt für $\mathfrak{a}$, $\mathfrak{b}$ in I_R:*

(i) $n_\mathfrak{p}(\mathfrak{ab}) = n_\mathfrak{p}(\mathfrak{a}) + n_\mathfrak{p}(\mathfrak{b})$;

(ii) $n_\mathfrak{p}(\mathfrak{a} + \mathfrak{b}) = \min(n_\mathfrak{p}(\mathfrak{a}), n_\mathfrak{p}(\mathfrak{b}))$;

(iii) $\mathfrak{a} \subseteq \mathfrak{b} \iff n_\mathfrak{p}(\mathfrak{a}) \geq n_\mathfrak{p}(\mathfrak{b})$ *für alle* $\mathfrak{p} \in \mathbb{P}_R$.

Beweis. (i) ist klar. Ferner ist $\mathfrak{a} \subseteq R \iff n_\mathfrak{p}(\mathfrak{a}) \geq 0$ für alle $\mathfrak{p}$, und $\mathfrak{a} \subseteq \mathfrak{b} \iff \mathfrak{a}\mathfrak{b}^{-1} \subseteq R$. Dies liefert (iii), und daraus folgt (ii), da $\mathfrak{a} + \mathfrak{b}$ der ggT der beiden gebrochenen Ideale ist. □

(5.9) **Satz.** *Der Dedekindring R ist ein Hauptidealring unter jeder der folgenden Voraussetzungen:*

(a) *R ist faktoriell.*

(b) *R hat nur endlich viele Primideale.*

Beweis. (a) Wegen (5.7) genügt es zu zeigen, dass jedes Primideal $\mathfrak{p} \neq 0$ von R Hauptideal ist. Wähle $0 \neq x \in \mathfrak{p}$ und schreibe eindeutig $x = \prod_i p_i$ als Produkt von Primelementen p_i in R. Da R ein faktorieller Dedekindring ist, ist $(p_i) = Rp_i$ ein maximales Ideal von R für jedes i. Wegen $x \in \mathfrak{p}$ ist $p_i \in \mathfrak{p}$ für mindestens ein i, und es folgt $\mathfrak{p} = (p_i)$.

(b) Seien $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ die sämtlichen verschiedenen Primideale ($\neq 0$) von R. Dann gilt $\mathfrak{p}_i^{e_i} + \mathfrak{p}_j^{e_j} = R$ für $i \neq j$ und alle natürlichen Zahlen e_i, e_j (5.7), (5.8). Sei $\mathfrak{a} = \prod_{i=1}^r \mathfrak{p}_i^{n_i}$ ein Ideal ($\neq 0$) von R. Für jedes i wähle ein Element $\pi_i \in \mathfrak{p}_i \setminus \mathfrak{p}_i^2$. Nach dem Chinesischen Restesatz (4.8) gibt es ein Element $a \in R$, so dass

$$a \equiv \pi_i^{n_i} \pmod{\mathfrak{p}_i^{n_i+1}}$$

für alle $i = 1, \ldots, r$ ist. Es gilt dann $n_{\mathfrak{p}_i}(aR) = n_i$ für alle i. Daher ist $\mathfrak{a} = (a)$ ein Hauptideal. □

§6. Diskrete Bewertungsringe

Parallel zur Idealtheorie der Dedekindringe verläuft die Bewertungstheorie. Jedes Primideal $\mathfrak{p}$ ($\neq 0$) eines Dedekindrings R definiert eine $\mathfrak{p}$-adische Bewertung des Quotientenkörpers von R und einen Bewertungsring $R_\mathfrak{p}$. Die Struktur von $R_\mathfrak{p}$ ist viel einfacher als die von R; es ist ein *lokaler Hauptidealring*, mit genau einem maximalen Ideal, ein sog. "diskreter Bewertungsring". Viele Gesetzmäßigkeiten für R lassen sich in der *Lokalisierung* $R_\mathfrak{p}$ studieren, vielleicht noch eleganter durch Übergang zu der *Komplettierung*. Der bewertungstheoretischen Ansatz hat den Vorteil, dass auch die *archimedischen* Bewertungen in völliger Analogie mitbetrachtet werden können. Im Zahlkörperfall sind dies die durch die Einbettungen in $\mathbb{C}$ (bzw. $\mathbb{R}$) gegebenen Betragsfunktionen.

(6.1) **Definition.** Sei R ein Dedekindring mit Quotientenkörper K, und sei $\mathfrak{p} \in \mathbb{P}_R$. Sei ∞ ein Symbol, das größer als alle ganzen (reellen) Zahlen z ist (mit $z+\infty = \infty+s = \infty$). Definiere dann die $\mathfrak{p}$-adische Bewertung $v_\mathfrak{p} : K \to \mathbb{Z} \cup \{\infty\}$ durch

$$v_\mathfrak{p}(x) = \begin{cases} n_\mathfrak{p}(xR) & \text{für } x \neq 0 \\ \infty & \text{sonst} \end{cases}.$$

Dabei ist $n_\mathfrak{p}$ erklärt wie in (5.7), (5.8). Es gelten demnach folgende Rechenregeln:

(i) $v_\mathfrak{p} : K^* \to \mathbb{Z}$ ist ein Gruppenepimorphismus; vgl. (5.8)(i).

(ii) $v_\mathfrak{p}(x+y) \geq \min\{(v_\mathfrak{p}(x), v_\mathfrak{p}(y)\}$; vgl. (5.8)(ii).

Abbildungen $v = v_\mathfrak{p}$ (auf Körpern) mit diesen beiden Eigenschaften nennt man (additive) *diskrete Bewertungen*. Aus (i), (ii) folgt $v(1) = v(1 \cdot 1) = v(1) + v(1) = 0 = v(-1)$, also $v(-x) = v(x)$. Für $0 \neq x \in K$ ist $v(x^{-1}) = -v(x)$. Wir können ferner (ii) ergänzen durch

(ii)* $v_\mathfrak{p}(x+y) = v_\mathfrak{p}(x)$ falls $v_\mathfrak{p}(x) < v_\mathfrak{p}(y)$ ist.

Es ist dann nämlich $v(x) = v(x+y-y) \geq \min\big(v(x+y), v(-y)\big) \geq \min\big(v(x), v(y)\big) = v(x)$. Wir definieren noch (vorübergehend)

$$R_{v_\mathfrak{p}} = \{x \in K |\ v_\mathfrak{p}(x) \geq 0\}.$$

(6.2) **Satz.** *$R_{v_\mathfrak{p}} = R_\mathfrak{p}$ ist ein lokaler Hauptidealring mit Restklassenklassenkörper $k_\mathfrak{p} \cong R/\mathfrak{p}$, und ein (echter) maximaler Teilring von K.*

Beweis. Sei $R_v = R_{v_\mathfrak{p}}$. Nach Definition ist $0 \in R_v$, und R_v ist ein Teilring von K wegen (i), (ii) in (6.1). Offenbar ist $R_v^* = \{x \in K \,|\, v_\mathfrak{p}(x) = 0\}$ und

$$\mathfrak{m} = \{x \in K |\ v_\mathfrak{p}(x) \geq 1\}$$

das einzige maximale Ideal von R. Wähle $\pi \in K$ mit $v_\mathfrak{p}(\pi) = 1$ (etwa $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$). Ist $y \in \mathfrak{m}$ und $v_\mathfrak{p}(y) = r \in \mathbb{N}_{>0}$, so ist $v_\mathfrak{p}(y^{-1}\pi^r) = 0$, also $y = u\pi^r$ mit einer Einheit

$u \in R_v^*$. Folglich ist $\mathfrak{m} = (\pi)$ ein Hauptideal, und alle Ideale von R_v sind Potenzen $(\pi)^r = (\pi^r)$ davon. R_v ist ein lokaler Hauptidealring. Jedes Element von K^* hat eine eindeutige Darstellung der Form $x = u\pi^r$ mit $u \in R_v^*$ und $r \in \mathbb{Z}$, und $x \in R_v$ genau dann, wenn $r \geq 0$ ist. Wegen $\pi^{-1} \notin R_v$ ist R_v ein echter maximaler Teilring von K.

Definitionsgemäß ist $R_\mathfrak{p} \subseteq R_v$. Nach (4.2) ist $R_\mathfrak{p}$ ein lokaler Ring mit maximalem Ideal $\mathfrak{m}_\mathfrak{p} = \mathfrak{p}R_\mathfrak{p}$, wobei $\mathfrak{m}_\mathfrak{p} \cap R = \mathfrak{p}$ und $R_\mathfrak{p}/\mathfrak{m}_\mathfrak{p} \cong R/\mathfrak{p}$ ein Körper ist. Nach (4.3) ist $R_\mathfrak{p}$ ganz-abgeschlossen (D2), und aus (4.5) folgt, dass $R_\mathfrak{p}$ Noethersch (D1) und dass $\mathfrak{p}R_\mathfrak{p}$ das einzige Primideal $\neq 0$ von $R_\mathfrak{p}$ ist (D3). Also ist $R_\mathfrak{p}$ ein lokaler Dedekindring, nach (5.9)(b) damit ein lokaler Hauptidealring. Wie eben erkennt man, dass $R_\mathfrak{p}$ ein maximaler Teilring von K ist. Daher gilt $R_\mathfrak{p} = R_v$. $\square$

(6.3) **Bemerkungen.** Wähle eine reelle Zahl c mit $0 < c < 1$ und definiere die multiplikative $\mathfrak{p}$-adische Bewertung von K durch

$$|x|_\mathfrak{p} = c^{v_\mathfrak{p}(x)},$$

mit der Konvention $c^\infty = 0$. Es gilt dann:

(i) $|xy|_\mathfrak{p} = |x|_\mathfrak{p}|y|_\mathfrak{p}$ (und $|x|_\mathfrak{p} = 0 \iff x = 0$),

(ii) $|x + y|_\mathfrak{p} \leq \max\{|x|_\mathfrak{p}, |y|_\mathfrak{p}\}$ (Ultrametrik).

Änderung der Konstanten c liefert äquivalente Metriken (gleiche Toplogie). Der so bewertete Körper K kann in der üblichen Weise komplettiert werden (Ring der Cauchyfolgen modulo Ideal der Nullfolgen). In der jetzigen Situation erhält man die Komplettierung von R, oder $R_\mathfrak{p}$, auch als *projektiven Limes*

$$\varprojlim_n R/\mathfrak{p}^n.$$

Die Quotientenkörper sind die sog. $\mathfrak{p}$-adischen Körper. Ist K ein Zahlkörper und $\mathfrak{p} \in \mathbb{P}_K$, so normiert man meistens $c = \frac{1}{\mathrm{N}\mathfrak{p}}$.

Beispiel. Sei $R = \mathbb{Z}$, $K = \mathbb{Q}$ und p eine Primzahl. Dann ist $|x|_p = (\frac{1}{p})^{v_p(x)}$, wobei $v_p(x) = r$ ist für $0 \neq x = up^r$ mit $u \in \mathbb{Z}_{(p)}^*$. Die Komplettierung liefert den Körper $\mathbb{Q}_p$ der p-adischen Zahlen. Diese p-adischen Körper sind völlig gleichrangig dem Körper $\mathbb{R} = \mathbb{Q}_\infty$ der reellen Zahlen, den man durch die Komplettierung von $\mathbb{Q}$ bzgl. der Betragsbewertung $|\cdot| = |\cdot|_\infty$ erhält. (Bis auf Äquivalenz sind dies auch die einzigen Bewertungen von $\mathbb{Q}$; Satz von Ostrowski, vgl. Neukirch, S. 124 und S. 130.)

(6.4) **Satz** (Krull). *Für jeden Integrittsbaereich R ist $R = \bigcap_\mathfrak{p} R_\mathfrak{p}$, wobei $\mathfrak{p}$ über die maximalen Ideal von R läuft.*

Beweis. Offenbar ist R enthalten in dem Ring $S = \bigcap_{\mathfrak{p} \in \mathbb{P}_R} R_\mathfrak{p}$. Für den R-Modul S gilt andererseits $S_\mathfrak{p} = R_\mathfrak{p}$ für alle $\mathfrak{p}$. Daher ist $R = S$ nach (4.4). $\square$

(6.5) **Satz.** *Sei R ein Noetherscher Integritätsbereich. Genau dann ist R ein Dedekindring, wenn $R_\mathfrak{p}$ ein diskreter Bewertungsring ist für alle maximalen Ideale $\mathfrak{p}$ von R*

Beweis. Sind die $R_\mathfrak{p}$ diskrete Bewertungsringe, so sind sie faktoriell und daher ganz-abgeschlossen, und dasselbe gilt für ihren Durchschnitt R (6.4). Aus (4.5) folgt, dass die Primideale ($\neq 0$) von R maximal sind (ebenso wie die der $R_\mathfrak{p}$). Die andere Richtung haben wir in (6.2) gezeigt. □

(6.6) **Satz.** *Sei $R = R_\mathfrak{p}$ ein diskreter Bewertungsring mit Qutientenkörper K, Bewertung $v = v_\mathfrak{p}$, maximalem Ideal $\mathfrak{p} = (\pi)$ und Restklassenkörper $k_\mathfrak{p}$. Setze $U^{(0)} = R^* = R \setminus \mathfrak{p}$ und*

$$U^{(n)} = 1 + \mathfrak{p}^n = \{x \in K^* \mid v(x-1) \geq n\}$$

für $n \geq 0$. Dies ist eine mit wachsendem n absteigende Kette von Untergruppen von R^* (höhere Einseinheitengruppen) mit $U^{(0)}/U^{(1)} \cong k_\mathfrak{p}^*$ und $U^{(n)}/U^{(n+1)} \cong k_\mathfrak{p}^+$ für $n \geq 1$.

Beweis. Für $x, y \in \mathfrak{p}^n$ ist $(1+x)(1+y) = 1 + x + y + xy \in 1 + \mathfrak{p}^n$ ($n \geq 1$). Wegen $v(x) \geq n > 0$ ist $v(1+x) = v(0) = 0$, also $u = 1 + x$ in R^*, und

$$v(u^{-1} - 1) = v(\frac{1}{u}(1-u)) = -v(u) + v(1-u) = v(u-1).$$

Also ist $U^{(n)}$ eine Gruppe. Die erste Isomorphie ergibt sich aus der Zuordnung $u \mapsto u + \mathfrak{p} = u(1+\mathfrak{p})$. Für $n > 0$ betrachtet man die Zuordnung $1 + a\pi^n \mapsto a + \mathfrak{p} : U^{(n)} \to k_\mathfrak{p}^+$, die ein Epimorphismus mit Kern $U^{(n+1)}$ ist. □

(6.7) **Satz.** *Sei R ein Dedekindring mit Quotientenkörper K und $L|K$ eine endliche separable Erweiterung. Sei $S = R_{L|R}$ und $\mathfrak{p} \in \mathbb{P}_R$. Dann ist $S_\mathfrak{p}$ ein Hauptidealring und ein freier $R_\mathfrak{p}$-Modul vom Range $[L : K]$.*

Beweis. Nach (5.3) ist S ein Dedekindring. Nach (4.3) ist $S_\mathfrak{p}$ der ganze Abschluss von $R_\mathfrak{p}$ in L. Nach (4.5) und dessen Zusatz übertragen sich auch (D1), (D3) von S auf $S_\mathfrak{p}$. Folglich ist $S_\mathfrak{p}$ ein Dedekindring. Aber alle Primstellen von $S_\mathfrak{p}$ liegen über dem einzigen maximalen Ideal von $R_\mathfrak{p}$. Nach (5.7) hat $S_\mathfrak{p}$ daher nur endlich viele Primideale, ist somit nach (5.9) ein Hauptidealring.

Nach (3.8) ist $S_\mathfrak{p}$ ein Noetherscher $R_\mathfrak{p}$-Modul, eingezwängt zwischen zwei freie $R_\mathfrak{p}$-Moduln des Ranges $n = [L : K]$. Der Elementarteilersatz (0.3) gilt für $R_\mathfrak{p}$ (vgl. Übung 3). Das liefert die letzte Behauptung. □

§7. Erweiterungen von Dedekindringen

Durchweg sei R ein Dedekindring mit Quotientenkörper K und $L|K$ eine endliche separable Körpererweiterung vom Grade $[L : K] = n$. Es sei $S = R_{L|R}$ der ganze Abschluss von R in L. Nach (5.3) ist auch S ein Dedekindring.

(7.1) **Zerlegungshomomorphismus.** Ist $\mathfrak{a} \in I_R$, so ist nach (5.5) der von $\mathfrak{a}$ erzeugte S-Modul $\mathfrak{a}S$ in I_S ($\neq 0$ und endlich erzeugt). Die Zuordnung $\mathfrak{a} \mapsto \mathfrak{a}S$ ist ein Homomorphismus $i_{L|K} : I_R \to I_S$ der Gruppen der gebrochenen Ideale (wegen $(\mathfrak{a}S)(\mathfrak{b}S) = (\mathfrak{a}\mathfrak{b})S$). Dabei wird H_R in H_S abgebildet, also ein Homomorphismus $i^*_{L|K} : \mathrm{C}\ell_R \to \mathrm{C}\ell_S$ induziert.

Lemma. *$i_{L|K}$ ist injektiv (aber $i^*_{L|K}$ i.a. nicht).*

Beweis. Sei $i_{L|K}(\mathfrak{a}) = \mathfrak{a}S = S = S^{-1}$. Dann ist auch $\mathfrak{a}^{-1}S = S$, also $\mathfrak{a}$ und $\mathfrak{a}^{-1}$ in S und damit ganz über R. Es folgt $\mathfrak{a} \subseteq R$ und $\mathfrak{a}^{-1} \subseteq R$, wegen (D2). Nach (5.7), (5.8) erzwingt dies $\mathfrak{a} = R$. $\square$

Nach (5.7) ist $i_{L|K}$ bestimmt auf der $\mathbb{Z}$-Basis $\mathbb{P}_R$. Sei $\mathfrak{p} \in \mathbb{P}_R$. Es gibt eindeutig bestimmte positive ganze Zahlen $r = r_{\mathfrak{p}}(L)$ ("Zerlegungszahl") und $e_i = e(\mathfrak{P}_i|\mathfrak{p})$ ("Verzweigungsindex"), so dass

$$\mathfrak{p}S = i_{L|K}(\mathfrak{p}) = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$$

mit paarweise verschiedenen Primidealen $\mathfrak{P}_i$ von S ist ("Zerlegung von $\mathfrak{p}$ in L"). Für jedes i ist der Restklassenkörper $k_{\mathfrak{P}_i} = S/\mathfrak{P}_i$ eine Erweiterung von $k_{\mathfrak{p}} = R/\mathfrak{p}$ endlichen Grades $f_i = f(\mathfrak{P}_i|\mathfrak{p})$. Ist nämlich $\varphi_i : S \twoheadrightarrow S/\mathfrak{P}_i$ der kanonische Epimorphismus, so ist $\mathrm{Ker}(\varphi_i|R) = \mathfrak{p}$. Also wird R auf einen Teilkörper von $k_{\mathfrak{P}_i}$ abgebildet, den wir mit $k_{\mathfrak{p}} = R/\mathfrak{p}$ identifizieren können. Da S als R-Modul nach (3.8) endlich erzeugt ist, ist der *Restklassengrad* $f_i = [k_{\mathfrak{P}_i} : k_{\mathfrak{p}}]$ endlich. Wir zeigen in (7.5):

$$\sum_{i=1}^{r} e_i f_i = n = [L : K].$$

Sprechweisen:

- $\mathfrak{p}$ ist träge (prim) in L, falls $r = 1 = e_1$ gilt ($\mathfrak{p}S \in \mathbb{P}_S$; $f_1 = n$).
- $\mathfrak{p}$ ist unverzweigt in L, falls $e_i = 1$ für alle i ist.
- $\mathfrak{p}$ ist total verzweigt in L, falls $r = 1 = f_1$ ist ($\iff e_1 = n$).
- $\mathfrak{p}$ zerfällt total in L, falls $e_i = 1 = f_i$ für alle i ($\iff r = n$).

(7.2) **Norm.** Die Norm $\mathrm{N}_{L|K} : L^* \to K^*$ ist ein Gruppenhomomorphismus. Sei $\mathfrak{b} \in I_S$. Unter der *Norm* $\mathrm{N}_{L|K}(\mathfrak{b})$ versteht man das gebrochene Ideal von R, das durch

alle $\mathrm{N}_{L|K}(\beta)$ mit $\beta \in \mathfrak{b}$ erzeugt wird (ein endlich erzeugter R-Modul $\neq 0$). Wir haben einen Gruppenhomomorphismus $\mathrm{N}_{L|K} : I_S \to I_R$. Ist $\mathfrak{b} = \beta S$ in H_S, so ist $\mathrm{N}_{L|K}(\mathfrak{b}) = \mathrm{N}_{L|K}(\beta)R$ in H_R, so wieder ein induzierter Homomorphismus $\mathrm{N}^*_{L|K} : \mathrm{C}\ell_S \to \mathrm{C}\ell_R$.

Für $\mathfrak{a} \in I_R$ gilt $\mathrm{N}_{L|K}(\mathfrak{a}S) = \mathfrak{a}^n$. Daher ist auch $\mathrm{N}^*_{L|K} \circ \iota^*_{L|K}$ die Potenzierung mit n auf $\mathrm{C}\ell_R$. Zur Untersuchung der Norm können wir uns nach (5.7) wieder auf Primideale (von S) konzentrieren:

(7.3) **Lemma.** *Sei $\mathfrak{P} \in \mathbb{P}_S$. Dann ist $\mathfrak{P} \cap R = \mathfrak{p}$ in $\mathbb{P}_R$; $\mathfrak{P}$ liegt über $\mathfrak{p}$ ($\mathfrak{P}|\mathfrak{p}$), und $\mathfrak{P}$ kommt in der Zerlegung von $\mathfrak{p}$ in L vor.*

(a) *Sei $L'|L$ endlich separabel, $S' = R_{L'|K} = R_{L'|L}$ und $\mathfrak{P}'|\mathfrak{P}$ in $\mathbb{P}_{S'}$. Es gilt $e(\mathfrak{P}'|\mathfrak{p}) = e(\mathfrak{P}'|\mathfrak{P}) \cdot e(\mathfrak{P}|\mathfrak{p})$ und $f(\mathfrak{P}'|\mathfrak{p}) = f(\mathfrak{P}'|\mathfrak{P}) \cdot f(\mathfrak{P}|\mathfrak{p})$.*

(b) $\mathrm{N}_{L|K}(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}|\mathfrak{p})}$.

Beweis. Im Beweis von (5.3) haben wir schon gesehen, dass $\mathfrak{p} = \mathfrak{P} \cap R \neq 0$ ein Primideal (maximales Ideal) von R ist. Es liegt $\mathfrak{P}$ über $\mathfrak{p}$, und die Primideale von S, die in der Zerlegung von $\mathfrak{p}$ vorkommen, sind genau die, die $\mathfrak{p}$ enthalten (5.8). Die erste Identität in (a) folgt aus der eindeutigen Primidealzerlegung, die zweite ist die Dimensionsformel für Körpererweiterungen.

Zum Beweis von (b) sei L' die Galoishülle von $L|K$. Es gilt die *Transitivität* $\mathrm{N}_{L'|K} = \mathrm{N}_{L|K} \circ \mathrm{N}_{L'|L}$. Setze $f = f(\mathfrak{P}|\mathfrak{p})$ und $f' = f(\mathfrak{P}'|\mathfrak{P})$. Gilt die behauptete Normbeziehung für Galoiserweiterungen, so ist also $\mathrm{N}_{L'|L}(\mathfrak{P}') = \mathfrak{P}^{f'}$ und $\mathrm{N}_{L'|K}(\mathfrak{P}') = \mathfrak{p}^{ff'}$, und es folgt

$$\mathfrak{p}^{ff'} = \mathrm{N}_{L|K}(\mathfrak{P}^{f'}) = \mathrm{N}_{L|K}(\mathfrak{P})^{f'}$$

und daher die Behauptung wegen (5.7). Wir können daher $L = L'$ als Galoiserweiterung von K voraussetzen. Ist dann $G = \mathrm{Gal}(L|K)$, so gilt

$$\mathrm{N}_{L|K}(\mathfrak{P})S = \prod_{\sigma \in G} \mathfrak{P}^\sigma.$$

Wir werden in (8.1) zeigen, dass G transitiv auf den Primidealen von L über $\mathfrak{p}$ operiert und dass all diese Primideale denselben Verzweigungsindex e und Restklassengrad f über $\mathfrak{p}$ haben. Nach (7.5) unten bedeutet dies $|G| = ref$ und $\prod_{\sigma \in G} \mathfrak{P}^\sigma = (\mathfrak{p}^f)S = (\mathfrak{p}S)^f$. Man benutze noch, dass $i_{L|K}$ nach (7.1) eine Injektion ist. □

(7.4) **Zahlkörperfall:** Sei $R = \mathbb{Z}$ und $S = R_L$ (L Zahlkörper). Sei $\mathfrak{a} \neq 0$ ein ganzes Ideal von S, $\mathrm{N}\mathfrak{a} = |S/\mathfrak{a}|$ die absolute Norm (3.10). Es gilt

$$\mathrm{N}_{L|\mathbb{Q}}(\mathfrak{a}) = (\mathrm{N}\mathfrak{a})\mathbb{Z}.$$

Zum Beweis können wir aufgrund des Chinesischen Restesatzes $\mathfrak{a} = \mathfrak{P}^e$ für ein Primideal $\mathfrak{P}$ von S und $e \geq 1$ annehmen. Sei $\mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$ und $f = f(\mathfrak{P}|\mathfrak{p}\mathbb{Z})$. Dann ist $|S/\mathfrak{P}| = p^f$ und daher $|S/\mathfrak{b}| = p^{fe}$, denn für $y_\nu \in \mathfrak{P}^\nu \setminus \mathfrak{P}^{\nu+1}$ ist $\mathfrak{P}^\nu = \mathfrak{P}^{\nu+1} + Ry_\nu$ und daher $y \mapsto yy_\nu + \mathfrak{P}^{\nu+1}$ ein R-Epimorphismus von R auf $\mathfrak{P}^\nu/\mathfrak{P}^{\nu+1}$ mit Kern $\mathfrak{P}$ ($\nu \in \mathbb{N}$). (Alternativ: $\mathfrak{P}^\nu/\mathfrak{P}^{\nu+1}$ ist nach (5.7) ein irreduzibler S-Modul, der von $\mathfrak{P}$ annulliert wird, daher ein 1-dimensionaler $k_\mathfrak{P}$-Vektorraum.) Wegen $\mathrm{N}_{L|\mathbb{Q}}(\mathfrak{P}) = p^f\mathbb{Z}$ folgt die Behauptung.

Ist auch $\mathfrak{b} \neq 0$ ein ganzes Ideal, so gilt also $\mathrm{N}(\mathfrak{a}\mathfrak{b}) = \mathrm{N}\mathfrak{a} \cdot \mathrm{N}\mathfrak{b}$, denn $\mathrm{N}_{L|\mathbb{Q}} : I_S \to I_\mathbb{Z}$ ist ein Homomorphismus. Ist $\mathfrak{a} = \alpha S$ ein Hauptideal, so ist $\mathrm{N}\mathfrak{a} = \pm\mathrm{N}_{L|\mathbb{Q}}(\alpha)$ und genau dann $\alpha \in S^*$ eine Einheit, wenn $\mathrm{N}_{L|\mathbb{Q}}(\alpha) = \pm 1$ ist (vgl. mit (1.5)).

(7.5) **Haupsatz.** *Sei $\mathfrak{p}S = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$ die Zerlegung von $\mathfrak{p} \in \mathbb{P}_R$ in L, und sei $f_i = f(\mathfrak{P}_i|\mathfrak{p})$. Dann ist $A = S/\mathfrak{p}S$ eine (kommutative) $k_\mathfrak{p}$-Algebra mit $\dim_{k_\mathfrak{p}} \mathrm{A} = \mathrm{n}$, und das Radikal $J(A) = \mathfrak{P}_1 \dots \mathfrak{P}_r/\mathfrak{p}S$ ist ein nilpotentes Ideal von A. Es gilt ferner:*

(a) *$A \cong S/\mathfrak{P}_1^{e_1} \times \dots \times S/\mathfrak{P}_r^{e_r}$ und $A/J(A) \cong k_{\mathfrak{P}_1} \times \dots \times k_{\mathfrak{P}_r}$.*

(b) *$\sum_{i=1}^r e_i f_i = \dim_{k_\mathfrak{p}} \mathrm{A} = \mathrm{n}$ (= [L : K]).*

Beweis. Setze $k = k_\mathfrak{p}$. Da die $\mathfrak{P}_i^{e_i}$ paarweise teilerfremde Ideale von R sind, ist nach dem Chinesischen Restesatz (4.8) die Zuordnung $\beta \mapsto (\beta + \mathfrak{P}_1^{e_1}, \dots, \beta + \mathfrak{P}_r^{e_r})$ ein Ringepimorphismus von R auf das direkte Produkt $S/\mathfrak{P}_1^{e_1} \times \dots \times S/\mathfrak{P}_r^{e_r}$ mit Kern $\prod_{i=1}^r \mathfrak{P}_i^{e_i} = \mathfrak{p}S$. Dies ist natürlich auch R-linear, so dass A in natürlicher Weise eine k-Algebra ist. Es bleibt zu zeigen:

(i) $\dim_k \mathrm{A} = \mathrm{n}$ und

(ii) $\dim_k \mathrm{S}/\mathfrak{P}^\mathrm{e} = \mathrm{ef}$ für $\mathfrak{P} = \mathfrak{P}_i$, $e = e_i$, $f = f_i$.

Ad (i): Beim Lokalisieren bei $\mathfrak{p}$ bleiben nach (4.2), (4.5) alle Zerlegungsinvarianten erhalten. Insbesondere ist $A \cong S_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}$ als k-Algebra. Wir können daher $R = R_\mathfrak{p}$ als diskreten Bewertungsring annehmen. Dann ist $S = S_\mathfrak{p}$ nach (6.7) ein freier R-Modul vom Range n. Ist $\{v_i\}$ eine R-Basis von S, so ist $\{v_i + \mathfrak{p}S\}$ eine k-Basis von A.

Ad (ii): Betrachte die Kette von k-Vektorräumen $S/\mathfrak{P}^e \supseteq \mathfrak{P}/\mathfrak{P}^e \supseteq \dots \supseteq \mathfrak{P}^{e-1}/\mathfrak{P}^e$. Die Quotienten $\mathfrak{P}^\nu/\mathfrak{P}^{\nu+1}$ in dieser Kette sind alle isomorph zu $S/\mathfrak{P}$. Das Argument ist genau wie eben in (7.4). Also ist $\dim_k \mathrm{R}/\mathfrak{P}^\mathrm{e} = \mathrm{ef}$. □

(7.6) **Satz** (Kummer–Dedekind). *Sei $L = K(\alpha)$ mit einem primitiven $\alpha \in S$ und $S' = R[\alpha]$ (existiert immer nach Gauß). Sei $f = m_{K,\alpha}$ das Minimalpolynom, also $f \in R[X]$. Sei $\mathfrak{p} \in \mathbb{P}_R$ und $\bar{f} = f \bmod \mathfrak{p}$ die Reduktion mod $\mathfrak{p}$. Es gelte die Primfaktorzerlegung*

$$\bar{f} = \bar{f}_1^{e_1} \dots \bar{f}_r^{e_r}$$

mit paarweise verschiedenen normierten Polynomen $\bar{f}_i \in k_\mathfrak{p}[X]$ ($e_i > 0$). Seien f_i in $R[X]$ normierte Urbilder der $\bar{f}_i$. Dann gilt:

(a) *Die $\mathfrak{P}_i = \mathfrak{p}S' + f_i(\alpha)S' = \big(\mathfrak{p}, f_i(a)\big)_{S'}$ für $i = 1, \dots, r$ sind die verschiedenen Primideale (maximalen Ideale) von S' über $\mathfrak{p}$, mit Restklassengrad $f(\mathfrak{P}_i|\mathfrak{p}) = \mathrm{grd}(\bar{\mathrm{f}}_\mathrm{i})$.*

(b) *Es gilt $\mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r} \subseteq \mathfrak{p}S'\sigma$; ist $S = S' = R[\alpha]$ (monogen), so ist $\mathfrak{p}S = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$ die Zerlegung von $\mathfrak{p}$ in L.*

Beweis. $S' \subseteq S$ ist ein freier (Noetherscher) R-Modul (mit Basis $\{1, \alpha, \dots, \alpha^{n-1}\}$). Nach Voraussetzung ist $S'/\mathfrak{p}S' \cong k_\mathfrak{p}[X]/(\bar{f}) = A$. Nach Definition ist $\mathfrak{P}_i$ das Urbild in $S' = R[\alpha]$ des Ideals $\bar{\mathfrak{P}}_i$ in A erzeugt durch das Bild von $\bar{f}_i$ (und f_i). Es ist also $S'/\mathfrak{P}_i \cong k_\mathfrak{p}[X]/(\bar{f}_i)$ eine Körpererweiterung von $k_\mathfrak{p}$ vom Grade $d_i = \mathrm{grd}(\bar{\mathrm{f}}_\mathrm{i})$. Offenbar sind dies auch alle Primideale (maximalen Ideale) von S' oberhalb $\mathfrak{p}$, und sie sind paarweise verschieden. Man beachte, dass $k_\mathfrak{p}[X]$ ein Hauptidealring ist. Wegen $f(\alpha) = 0$ und $f - f_1^{e_1} \dots f_r^{e_r} \in \mathfrak{p}[X]$ ist $f_1(\alpha)^{e_1} \dots f_r(\alpha)^{e_r} \in \mathfrak{p}S'$. Wegen $\mathfrak{P}_i^{e_i} \subseteq \mathfrak{p}S' + f_i(\alpha)^{e_i}S'$ erhalten wir

$$\mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r} \subseteq \mathfrak{p}S' + f_1(\alpha)^{e_1} \dots f_r(\alpha)^{e_r} \subseteq \mathfrak{p}S'.$$

Sei nun $S = S'$ monogen. Setzen wir $e_i' = e(\mathfrak{P}_i|\mathfrak{p})$, so ist $\mathfrak{p}S = \mathfrak{P}_1^{e_1'} \dots \mathfrak{P}_r^{e_r'}$ die Zerlegung von $\mathfrak{p}$ in L, und es gilt $e_i \geq e_i'$ für alle i nach (5.7), (5.8). Nach (7.5) gilt $\sum_{i=1}^r e_i' d_i = n$. Wegen $\sum_{i=1}^r e_i d_i = \mathrm{grd(f)} = \mathrm{n}$ muss $e_i' = e_i$ gelten. □

(7.7) **Zusatz.** *Ist in (7.6) $S_\mathfrak{p} = R_\mathfrak{p}[\alpha]$ und $\mathfrak{P}_i = (\mathfrak{p}, f_i(\alpha))_{S_\mathfrak{p}} \cap S$, so ist $\mathfrak{p}S = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ die Zerlegung von $\mathfrak{p}$ in L (und $f(\mathfrak{P}_i|\mathfrak{p}) = \mathrm{grd}(\bar{\mathrm{f}}_\mathrm{i})$).*

Beweis. Nach (4.2), (4.5) können wir die Zerlegung von $\mathfrak{p}$ in L nach Lokalisierung bei $\mathfrak{p}$ studieren; alle Invarianten bleiben erhalten. □

Bemerkung. Wir haben (7.6) im Falle quadratischer Zahlringe schon in §1 bewiesen, wo die Ringe immer monogen sind. Dies ist nicht immer so; ist etwa $R = \mathbb{Z}$ und L ein kubischer Zahlkörper ($[L : \mathbb{Q}] = 3$), in welchem 2 total zerfällt, so ist $S = R_L$ (und ebensowenig $S_{(2)}$) nicht monogen, denn nach (7.6) müsste es sonst 3 verschiedene lineare Polynome über $\mathbb{F}_2$ geben. (Ein solches Beispiel ist $L = \mathbb{Q}(\alpha)$, wo α Wurzel von $X^3 + X^2 - 2X + 8$ ist.)

(7.8) **Satz** (Unverzweigtheit). *Sei $\alpha \in S$ mit $L = K(\alpha)$ und $f = m_{K,\alpha}$. Ist $\mathfrak{p} \in \mathbb{P}_R$ kein Teiler von D_f, d.h., $f \bmod \mathfrak{p}$ separabel, so ist $S_\mathfrak{p} = R_\mathfrak{p}[\alpha]$ und $\mathfrak{p}$ unverzweigt in L.*

Beweis. oBdA: $R = R_\mathfrak{p}$ (ein diskreter Bewertungsring, mit maximalem Ideal $\mathfrak{p} = \pi R$). Nach (6.7) ist dann $S = S_\mathfrak{p}$ ein freier R-Modul vom Range $n = [L : K]$. Ist (v_i) eine R-Basis von S, so ist nach (3.9)

$$D_f = D_{L|K}(1, \alpha, \dots, \alpha^{n-1}) = c^2 D_{L|K}(v_1, \dots, v_n)$$

mit einem Element $0 \neq c \in R$. Nach Voraussetzung ist aber $D_f \in R^* = R \setminus \mathfrak{p}$ eine Einheit in R. Also ist auch $c \in R^*$ und $\{1, \alpha, \ldots, \alpha^{n-1}\}$ eine R-Basis von S, d.h., $S = R[\alpha]$. Da $f \bmod \mathfrak{p}$ separabel ist (alle Primfaktoren mit erster Potenz $e_i = 1$), ist $\mathfrak{p}$ unverzweigt in L nach (7.6). $\square$

(7.9) **Satz** (Totale Verzweigung). *Sei $\mathfrak{p} \in R$ und $\pi \in L$ eine Wurzel von $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in R_\mathfrak{p}[X]$.*

(a) *Ist f ein Eisenstein-Polynom bzgl. $\mathfrak{p}R_\mathfrak{p}$, so ist $S_\mathfrak{p} = R_\mathfrak{p}[\pi]$ und $\mathfrak{p}$ total verzweigt in L.*

(b) *Ist $\mathfrak{p}$ total verzweigt in L, $\mathfrak{P} = \mathfrak{p}S$ und $v_\mathfrak{P}(\pi) = 1$, so ist $f = m_{K,\pi}$ ein Eisenstein-Polynom bzgl. $\mathfrak{p}R_\mathfrak{p}$ und $S_\mathfrak{p} = R_\mathfrak{p}[\pi]$.*

Beweis. oBdA: $R = R_\mathfrak{p}$. Setze noch $a_n = 1$.

(a) Sei f ein Eisenstein-Polynom bzgl. $\mathfrak{p}$, d.h., alle Koeffizienten $a_i \in \mathfrak{p}$ und $a_0 \notin \mathfrak{p}^2$. Es ist dann $\mathfrak{p} = a_0 R$. Bekanntlich ist f irreduzibel über K, also $f = m_{K,\pi}$. Ferner ist $f \bmod \mathfrak{p} = X^n$, und nach (7.6) ist $\mathfrak{P} = (\mathfrak{p}, \pi) = (a_0, \pi)$ das einzige maximale Ideal von $S' = R[\pi]$ über $\mathfrak{p}$. Wegen

$$a_0 = \pi(-\pi^{n-1} - a_{n-1}\pi^{n-2} - \ldots - a_1)$$

ist $\mathfrak{P} = \pi S'$ ein Hauptideal. Da $S'|R$ ganz ist, liegt jedes Primideal $\neq 0$ von S' über $\mathfrak{p}$, also S' ein lokaler Ring. Da S' Noethersch ist, gibt es zu jedem $0 \neq y \in S'$ nach (4.6) eine kleinste Nummer m mit $yS' \supseteq \pi^m S'$. Also ist $\bigcap_m \pi^m S' = 0$ (aber π nicht nilpotent). Wir können (eindeutig) schreiben $y = u\pi^m$ mit $u \in (S')^* = S' \setminus \mathfrak{P}$. Daher ist $S' = R[\pi]$ ein diskreter Bewertungsring, mithin ganz-abgeschlossen, und $S' = S$. Nach (7.6) ist $\mathfrak{p}$ total verzweigt in L.

(b) Sei $\mathfrak{p}S = \mathfrak{P}^n$ (totale Verzweigung) und $v_\mathfrak{P}(\pi) = 1$. Wegen (a) genügt es zu zeigen, dass dann f ein Eisenstein-Polynom bzgl. $\mathfrak{p}$ ist. Es ist die Einschränkung $v_\mathfrak{P}|K = n \cdot v_\mathfrak{p}$. Wegen

$$a_n\pi^n + a_{n-1}\pi^{n-1} + \ldots + a_0 = 0$$

und der Identität (ii)* in (6.1) gibt es Indizes $0 \leq i < j \leq n$, so dass $v_\mathfrak{P}(a_i\pi^i) = v_\mathfrak{P}(a_i\pi^j)$ der minimale $v_\mathfrak{P}$-Wert aller Summanden ist. Es ist $v_\mathfrak{P}(a_i) \equiv v_\mathfrak{P}(a_j) \equiv 0 \,(\mathrm{mod}\, n)$. Wegen $v_\mathfrak{P}(\pi^i) = i$, $v_\mathfrak{P}(\pi^j) = j$ erhalten wir die Kongruenz $i \equiv j \,(\mathrm{mod}\, n)$. Aber dies erzwingt $i = 0$ und $j = n$. Folglich ist $v_\mathfrak{p}(a_0) = \frac{1}{n} v_\mathfrak{P}(a_0) = \frac{1}{n} v_\mathfrak{P}(\pi^n) = 1$, und $v_\mathfrak{P}(a_s) + s = v_\mathfrak{P}(a_s\pi^s) > n$ für $0 < s < n$. Für die übrigen Koeffizienten gilt also

$$v_\mathfrak{p}(a_s) = \frac{1}{n} v_\mathfrak{P}(a_s) > \frac{1}{n}(n - s)$$

und somit $v_\mathfrak{p}(a_s) \geq 1$ $(0 < s < n)$. Daher ist f ein Eisenstein-Polynom bzgl. $\mathfrak{p}$. $\square$

§8. Galoiserweiterungen

Durchweg sei R ein Dedekindring mit Quotientenkörper K und $L|K$ eine endliche Galoiserweiterung mit Gruppe $G = \mathrm{Gal}(L|K)$ der Ordnung $|G| = n = [L : K]$. Ferner sei $S = R_{L|R}$ der ganze Abschluss von R in L; S ist ein Dedekindring, der unter G invarant ist. Ferner betrachten wir feste Primstellen $\mathfrak{P}|\mathfrak{p}$ von $S|R$ (Verzweigungsindex e, Trägheitsgrad f). Die Theorie geht im wesentlichen auf D. Hilbert (1862-1943) zurück.

(8.1) **Satz.** *G operiert transitiv auf den Primidealen von S über $\mathfrak{p}$. Für jedes $\sigma \in G$ gilt $e(\mathfrak{P}^\sigma|\mathfrak{p}) = e(\mathfrak{P}|\mathfrak{p}) = e$ und $f(\mathfrak{P}^\sigma|\mathfrak{p}) = f(\mathfrak{P}|\mathfrak{p}) = f$. Folglich ist die Zerlegungszahl $r_\mathfrak{p}(L) = r = \frac{n}{ef}$, und sind die $\mathfrak{P}_i = \mathfrak{P}^{\sigma_i}$ die verschiedenen Bilder von $\mathfrak{P}$ unter G, so ist $\mathfrak{p}S = (\mathfrak{P}_1 \dots \mathfrak{P}_r)^e$ die Zerlegung von $\mathfrak{p}$ in L.*

Beweis. Es ist $\mathfrak{P}^\sigma \cap R = (\mathfrak{P} \cap R)^\sigma = \mathfrak{p}^\sigma = \mathfrak{p}$ und $\beta + \mathfrak{P} \mapsto \beta^\sigma + \mathfrak{P}^\sigma$ ein Isomorphimus von von S-Moduln und $k_\mathfrak{p}$-Algebren. Ferner ist $\mathfrak{P}^e \supseteq \mathfrak{p} \iff (\mathfrak{P}^\sigma)^e = (\mathfrak{P}^e)^\sigma \supseteq \mathfrak{p}$. Es ist daher nur noch die Transitivität zu zeigen.

Angenommen, es gibt ein Primideal $\mathfrak{P}'$ über $\mathfrak{p}$, für welches $\mathfrak{P}^\sigma \neq \mathfrak{P}'$ ist für alle $\sigma \in G$. Nach dem Chinesischen Restesatz (4.8) gibt es dann $x \in S$ mit

$$\left.\begin{array}{l} x \equiv 0 \,(\mathrm{mod}\, \mathfrak{P}'), \\ x \equiv 1 \,(\mathrm{mod}\, \mathfrak{P}^\sigma) \end{array}\right\}$$

für alle $\sigma \in G$. Dann ist $\mathrm{N}_{L|K}(x) \in \mathfrak{P}' \cap R = \mathfrak{p}$ nach (3.7) und $x^\sigma \notin \mathfrak{P}$ für alle $\sigma \in G$. Aus letzterem folgt aber $\mathrm{N}_{L|K}(x) = \prod_{\sigma \in G} x^\sigma \notin \mathfrak{P}$, denn $\mathfrak{P}$ ist ein Primideal, somit doch $\mathrm{N}_{L|K}(x) \notin \mathfrak{p}$. $\square$

(8.2) **Definition.** Der Stabilisator $G_\mathfrak{P} = \{\sigma \in G \mid \mathfrak{P}^\sigma = \mathfrak{P}\}$ von $\mathfrak{P}$ in G heißt die *Zerlegungsgruppe* von $\mathfrak{P}$. Dies ist eine Untergruppe von G. Nach (8.1) ist der Index $|G : G_\mathfrak{P}| = r$ die Zerlegungszahl von $\mathfrak{p}$ in L, also $|G_\mathfrak{P}| = ef$. Ist $\{\sigma_i\}$ ein Repräsentantensytem für die Rechtsnebenklassen von $G_\mathfrak{P}$ in G, so sind die $\mathfrak{P}^{\sigma_i}$ gerade die verschiedenen Primideale von S über $\mathfrak{p}$. Für jedes $\sigma \in G$ ist

$$G_{\mathfrak{P}^\sigma} = \sigma^{-1} G_\mathfrak{P} \sigma = (G_\mathfrak{P})^\sigma$$

eine konjugierte Untergruppe.

Jedes $\sigma \in G_\mathfrak{P}$ induziert ein Element $\bar{\sigma} \in \mathrm{Gal}(k_\mathfrak{P}|k_\mathfrak{p})$ durch

$$(x + \mathfrak{P})^{\bar{\sigma}} = x^\sigma + \mathfrak{P} \quad (x \in S).$$

Die Zuordnung $\sigma \mapsto \bar{\sigma} : G_\mathfrak{P} \to \mathrm{Gal}(k_\mathfrak{P}|k_\mathfrak{p})$ ist ein Gruppenhomomorphismus, dessen Kern

$$T_\mathfrak{P} = G_\mathfrak{P}^{(0)} = \{\sigma \in G_\mathfrak{P} \mid x^\sigma \equiv x \,(\mathrm{mod}\, \mathfrak{P}) \text{ für alle } x \in S\}$$

die *Trägheitsgruppe* von $\mathfrak{P}$ heißt. Es ist $T_\mathfrak{P}$ ein Normalteiler von $G_\mathfrak{P}$.

Die Fixkörper $L_{G_\mathfrak{P}}$ und $L_{T_\mathfrak{P}}$ dieser Gruppen heißen *Zerlegungskörper* bzw. *Trägheitskörper* von $\mathfrak{P}$. $L_{G_\mathfrak{P}}|L_{T_\mathfrak{P}}$ ist also eine Galoiserweiterung mit Gruppe $G_\mathfrak{P}/T_\mathfrak{P}$.

(8.3) **Satz.** *Die Restklassenerweiterung $k_\mathfrak{P}|k_\mathfrak{p}$ ist stets normal und $G_\mathfrak{P}/T_\mathfrak{P} \cong \mathrm{Gal}(k_\mathfrak{P}|k_\mathfrak{p})$. Ist also $k_\mathfrak{P}|k_\mathfrak{p}$ separabel, so ist $|T_\mathfrak{P}| = e$ der Verzweigungsindex. Ist $T_\mathfrak{P} = 1$, dann ist immer $e = 1$ und $k_\mathfrak{P}|k_\mathfrak{p}$ galoissch.*

Beweis. In jedem Falle ist $G_\mathfrak{P}/T_\mathfrak{P}$ isomorph zu einer Untergruppe von $\mathrm{Gal}(k_\mathfrak{P}|k_\mathfrak{p})$, und die Ordnung dieser Galoisgruppe ist ein Teiler von f und genau dann gleich f, wenn $k_\mathfrak{P}|k_\mathfrak{p}$ eine Galoiserweiterung ist. Ist also $T_\mathfrak{P} = 1$, so muss $|G_\mathfrak{P}| = f$, $e = 1$ und die Erweiterung galoissch sein.

Sei $\bar{\alpha}$ ein Element in $k_\mathfrak{P}$. Sei $\alpha' \in S$ ein Urbild. Nach dem Chinesischen Restesatz gibt es $\alpha \in S$ mit

$$\left.\begin{array}{l} \alpha \equiv \alpha' \,(\mathrm{mod}\,\mathfrak{P}), \\ \alpha \equiv 0 \,(\mathrm{mod}\,\mathfrak{P}^\sigma) \end{array}\right\}$$

für alle $\sigma \in G \setminus G_\mathfrak{P}$. Betrachte das Polynom $h(X) = \prod_{\sigma\in G}(X - \alpha^\sigma)$ in $L[X]$. Die Koeffizienten von h sind die elementarsymmetrischen Polynome in den Konjugierten $\alpha^\sigma \in S$. Daher ist $h \in R[X]$ $(R = S \cap K)$, und die Reduktion

$$\bar{h} = h \,mod\, \mathfrak{p} = X^{n-ef} \prod_{\sigma\in G_\mathfrak{P}} (X - \bar{\alpha}^{\bar{\sigma}})$$

ist ein Polynom in $k_\mathfrak{p}[X]$. Da $\bar{\alpha}$ eine Wurzel von $\bar{h}$ ist und $G_\mathfrak{P}$ auf den Wurzeln von $\bar{h}$ transitiv operiert, zerfällt $m_{k_\mathfrak{p},\bar{\alpha}}$ in $k_\mathfrak{P}$. Folglich ist $k_\mathfrak{P}|k_\mathfrak{p}$ normal. Wählt man $\bar{\alpha}$ als primitives Element für den separablen Abschluss von $k_\mathfrak{p}$ in $k_\mathfrak{P}$ (Gauß), so liefert dieses Argument den behaupteten Epimorphismus von $G_\mathfrak{P}$ auf $\mathrm{Gal}(k_\mathfrak{P}|k_\mathfrak{p})$. $\square$

(8.4) **Satz.** *Sei $k_\mathfrak{P}|k_\mathfrak{p}$ als separabel vorausgesetzt (somit galoissch). Seien $L_z = L_{G_\mathfrak{P}}$ und $L_t = L_{T_\mathfrak{P}}$ der Zerlegungskörper bzw. Trägheitskörper von $\mathfrak{P}$. Wir setzen $\mathfrak{P}_z = \mathfrak{P} \cap L_z$ und $\mathfrak{P}_t = \mathfrak{P} \cap L_t$; ist F ein Zwischenkörper von $L|K$, so sei $\mathfrak{P}_F = \mathfrak{P} \cap F$.*

(a) *L_z ist der größte Zwischenkörper F, für welchen $e(\mathfrak{P}_F|\mathfrak{p}) = 1 = f(\mathfrak{P}_F|\mathfrak{p})$ gilt. Es ist L_z auch der kleinste Zwischenkörper F, für welchen $r_{\mathfrak{P}_F}(L) = 1$ gilt.*

(b) *L_t ist der größte Zwischenkörper F, für welchen $e(\mathfrak{P}_F|\mathfrak{p}) = 1$ ist. Es ist L_t auch der kleinste Zwischenkörper F, für welchen $e(\mathfrak{P}|\mathfrak{P}_F) = e$ gilt.*

Beweis. Sei F ein Zwischenkörper von $L|K$ und $H = \mathrm{Gal}(L|F)$. Es ist $H_\mathfrak{P} = H \cap G_\mathfrak{P}$ und $H^{(0)}_\mathfrak{P} = H \cap G^{(0)}_\mathfrak{P}$.

(a) $G_\mathfrak{P} = \mathrm{Gal}(L|L_z)$ ist nach (8.1) transitiv auf den Primidealen von S über $\mathfrak{P}_z$ (und lässt $\mathfrak{P}$ fest). Also ist $r_{\mathfrak{P}_z}(L) = 1$, $e(\mathfrak{P}|\mathfrak{P}_z) = e$ und $f(\mathfrak{P}|\mathfrak{P}_z) = f$. Nach (7.3) folgt

$e(\mathfrak{P}_z|\mathfrak{p}) = 1 = f(\mathfrak{P}_z|\mathfrak{p})$. Gilt $e(\mathfrak{P}_F|\mathfrak{p}) = 1 = f(\mathfrak{P}_F|\mathfrak{p})$, so ist entsprechend $e(\mathfrak{P}|\mathfrak{P}_F) = e$ und $f(\mathfrak{P}|\mathfrak{P}_F) = f$, daher $|H_\mathfrak{P}| = ef$ nach (8.3). Also ist $H \supseteq H_\mathfrak{P} = G_\mathfrak{P}$ und $F \subseteq L_z$ in diesem Falle. Gilt $r_{\mathfrak{P}_F}(L) = 1$, so ist $H = H_\mathfrak{P} \subseteq G_\mathfrak{P}$ und $F \supseteq L_z$ (Hauptsatz der Galoistheorie).

(b) Es ist $r_{\mathfrak{P}_t}(L) = 1 = f(\mathfrak{P}|\mathfrak{P}_t)$ und $e(\mathfrak{P}|\mathfrak{P}_t) = e$. Folglich ist $e(\mathfrak{P}_t|\mathfrak{p}) = 1$ und $f(\mathfrak{P}_t|\mathfrak{p}) = f$ nach (7.3). Gilt $e(\mathfrak{P}_F|\mathfrak{p}) = 1$, so ist entsprechend $e(\mathfrak{P}|\mathfrak{P}_F) = e$ und $|H^{(0)}_\mathfrak{P}| = e$ nach (8.3), mithin $H \supseteq H^{(0)}_\mathfrak{P} = G^{(0)}_\mathfrak{P}$ und $F \subseteq L_t$. □

(8.5) **Folgerung.** *Sei wieder $k_\mathfrak{P}|k_\mathfrak{p}$ separabel, und sei $L|K$ die Galoishülle von $F|K$. Ist $\mathfrak{p}$ unverzweigt (bzw. total zerfallend) in F, so auch in L.*

Beweis. Es gilt Entsprechendes auch bzgl. jeder Konjugierten F^σ ($\sigma \in G$). Nach (8.4) gilt $F^\sigma \subseteq L_t$ (bzw. $L^\sigma \subseteq L_z$). □

(8.6) **Hauptsatz** (Dedekind–Bauer). *Sei L der Zerfällungskörper des normierten Polynoms $h \in R[X]$, und sei $\mathfrak{p}$ kein Teiler der Diskriminante D_h, d.h., $\bar{h} = h \bmod \mathfrak{p}$ (und damit auch h) ist separabel (vgl. mit 7.8). Dann ist $\mathfrak{p}$ unverzweigt in L und $k_\mathfrak{P}|k_\mathfrak{p}$ galoissch ($T_\mathfrak{P} = 1$), und $G_\mathfrak{P} \cong \mathrm{Gal}_{k_\mathfrak{p}}(\bar{h})$ als Permutationsgruppe der Wurzeln von $\bar{h}$.*

Beweis. Sei $h\prod_{i=1}^m (X - \alpha_i)$ über L, und sei $\bar{\alpha}_i = \alpha_i + \mathfrak{P}$. Nach (8.2) gibt es einen Homomorphismus $\sigma \mapsto \bar{\sigma}$ von $G_\mathfrak{P}$ in $\mathrm{Gal}(k_\mathfrak{P}|k_\mathfrak{p})$ mit Kern $T_\mathfrak{P}$ (zunächst nicht notwendig surjektiv). Sei $\sigma \in T_\mathfrak{P}$. Dann gilt $\bar{\alpha}_i^{\bar{\sigma}} = \bar{\alpha}_i$ für alle i. Da σ die Wurzeln von h permutiert und die $\bar{\alpha}_i$ nach Voraussetzung paarweise verschieden sind, folgt $\alpha_i^\sigma = \alpha_i$ für alle i. Aber dann ist $\sigma = 1$ auf $L = K(\alpha_1, \ldots, \alpha_m)$. Damit ist $T_\mathfrak{P} = 1$, und die Behauptung folgt aus dem Zusatz in (8.3). □

(8.7) **Beispiel.** Sei L der Zerfällungskörper des Polynoms $h = X^5 - X + 1 \in \mathbb{Z}[X]$. Dies ist ein Artin–Schreier Polynom mod 5, daher $h \bmod 5$ irreduzibel über $\mathbb{F}_5$. (Es gibt keine Wurzel in $\mathbb{F}_5$, und ist $\bar{a}$ eine Wurzel in einem Zerfällungskörper, so ist $W_h = \{\bar{\alpha} + j \mid j \in \mathbb{F}_5\}$ die Wurzelmenge und $\sum_{j\in M}(\bar{\alpha} + j) \notin \mathbb{F}_5$ für jede Teilmenge $\varnothing \neq M \subset \mathbb{F}_5$.) Nach (8.6) enthält $G = \mathrm{Gal}_\mathbb{Q}(h)$ daher einen 5-Zykel auf W_h. Es ist

$$h \bmod 2 = (X^2 + X + 1)(X^3 + X^2 + 1)$$

die Primfaktorzerlegung über $\mathbb{F}_2$. Also enthält G nach (8.6) ein disjunktes (vertauschbares) Produkt einer Transposition und eines 3-Zykels auf W_h, daher eine Transposition. Es ist $G \cong S_5$, denn eine transitive Permutationsgruppe vom Primzahlgrad, die eine Transposition enthält, ist die volle symmetrische Gruppe:

Anmerkung (C. Jordan, 1871). Sei G eine transitive Untergruppe von S_m, die eine Transposition enthält; es sei G *primitiv*, d.h., es gibt *keine* Teilmenge (Block) $B \subset \{1, 2, \ldots, m\}$ mit $1 < |B| < m$, für welche $B^g = B$ oder $B^g \cap B = \varnothing$ für alle

$g \in G$ ist. (G ist genau dann primitiv, wenn ein Punktstabilisator eine maximale Untergruppe ist, also etwa wenn m eine Primzahl ist oder G 2-fach transitiv.) Nenne zwei Ziffern äquivalent (unter G), falls sie durch Produkte disjunkter Transpositionen aus G ineinander übergeführt werden können. Die Äquivalenzklassen bilden einen (trivialen) G-Block, der die ganze Ziffernmenge sein muss. Seien nun $r \neq s$ Ziffern. Dann gibt es Transpositionen $(r, t_1), (t_1, t_2), \ldots, (t_l, r)$ in G, etwa alle Ziffern $t_i \neq r, s$, deren Produkt r in s überführt. Aber dann ist $(r, s) = \Big(\big((r, t_1)^{(t_1, t_2)}\big)^{\cdots}\Big)^{(t_l, s)}$ eine Transposition in G. Es folgt $G = S_m$, da S_m durch die Transpositionen erzeugt wird.

(8.8) **Beispiel.** Sei $m \in \mathbb{N}_{\geq 3}$. Wir konstruieren ein normiertes Polynom $h \in \mathbb{Z}[X]$ vom Grade m mit $\mathrm{Gal}_{\mathbb{Q}}(h) \cong S_m$. Sei dazu $h_i \in \mathbb{Z}[X]$ normiert vom Grade m mit:

- $h_1 \bmod 2$ ist irreduzibel über $\mathbb{F}_2$.
- $h_2 \bmod 3$ hat einen normierten Primfaktor vom Grade $m-1$ über $\mathbb{F}_3$.
- $h_3 \bmod 5$ hat über $\mathbb{F}_5$ einen Primfaktor vom Grade 2 (m ungerade) oder zwei normierte Primfaktoren ungeraden Grades (m gerade).

Solche h_i existieren. Setze $h = -15h_1 + 10h_2 + 6h_3$. Dann ist h normiert vom Grade m, und $h \equiv h_1 \,(\mathrm{mod}\, 2)$, $h \equiv h_2 \,(\mathrm{mod}\, 3)$, $h \equiv h_3 \,(\mathrm{mod}\, 5)$. Nach (8.6) enthält $G = \mathrm{Gal}_{\mathbb{Q}}(f)$ einen m-Zykel auf W_h, einen $(m-1)$-Zykel, ist also 2-fach transitiv, und eine Transposition. Es ist $G \cong S_m$.

(8.9) **Satz.** *Sei $K = \mathbb{Q}$ (L Zahlkörper) und sei auch $F|\mathbb{Q}$ endlich galoissch, L, F etwa Teilkörper von $\mathbb{C}$ (so dass das Kompositum LF erklärt ist). Ist* $\mathrm{ggT}(\mathrm{D_L}, \mathrm{D_F}) = 1$ und $L \cap F = \mathbb{Q}$, *so ist $R_{LF} = R_L R_F$*

Beweis. Das Kompositum LF ist galoissch über $\mathbb{Q}$ und $\mathrm{Gal}(LF|F) = \{\sigma_k | k = 1, \ldots, n\} \cong G$. Sei $\{\alpha_i\}_{1 \leq i \leq n}$ eine Ganzheitsbasis von L und $\{\beta_j\}_{1 \leq j \leq m}$ eine solche von F. Dann ist $\{\alpha_i \beta_i\}_{i,j}$ eine $\mathbb{Q}$-Basis von LF und eine $\mathbb{Z}$-Basis von $R_L R_F$. Sei $y \in R_{LF}$. Es gibt $r \in \mathbb{N}_{>0}$ und $c_{ij} \in \mathbb{Z}$, r teilerfremd zu $\mathrm{ggT}(\mathrm{c_{ij}} : \mathrm{i, j})$ mit $y = \sum_{i,j} \frac{c_{ij}}{r} \alpha_i \beta_j$. Wir zeigen $r \mid D_L$; analog gilt $r \mid D_F$, somit $r = 1$.

Setze $y_i = \sum_{j=1}^{m} \frac{c_{ij}}{r} \beta_j$ $(1 \leq i \leq n)$. Wir erhalten durch Anwendung der σ_k auf y die n Gleichungen

$$\sum_{i=1}^{n} \alpha_i^{\sigma_k} y_i = y^{\sigma_k} \quad (k = 1, \ldots, n).$$

Sei $d = \det(\alpha_i^{\sigma_k})$ und d_k die Determinante der Matrix, die man aus $(\alpha_i^{\sigma_k})$ durch Ersetzen der k-ten Spalte durch den Spaltenvektor $(y^{\sigma_k})^t$ erhält. Dann sind d, d_i ganz-algebraisch, und $D_L = d^2$. Nach der Cramerschen Regel ist $y_i = d_i/d$, daher $D_L y_i = d d_i$ ganz-algebraisch. Damit ist $\sum_{j=1}^{m} \frac{D_L c_{ij}}{r} \beta_j = D_L y_i \in R_{LF} \cap F = R_F$. Da $\{\beta_j\}$ eine Ganzheitsbasis von F ist, und r teilerfremd zu $\mathrm{ggT}(\mathrm{c_{ij}})$, folgt $r \mid D_L$. $\square$

§9. Verzweigung und Diskriminante

Wie in §7 sei R ein Dedekindring mit Quotientenkörper K und $L|K$ eine endliche separable Körpererweiterung vom Grade $[L : K] = n$. Es sei $S = R_{L|R}$ der ganze Abschluss von R in L.

(9.1) **Definition.** Die (relative) *Diskriminante* $D_{S|R}$ ist definiert als der R-Modul erzeugt durch alle $D_{L|K}(v_1, \ldots, v_n)$ mit Einträgen $v_i \in S$. Man hat nur solche n-Tupel zu betrachten, die eine K-Basis von L bilden. Nach (3.7), (3.9) ist $D_{S|R} \neq 0$ ein (ganzes) Ideal von R. Es gibt also nur endlich viele Primideale von R, die $D_{S|R}$ enthalten.

Bemerkung. Ist $R = \mathbb{Z}$ und L ein algebraischer Zahlkörper, so ist $D_{S|R} = D_L\mathbb{Z}$. Entsprechend einfach ist die Situation, wenn man zur Lokalisierung $R_\mathfrak{p}$ bei einem Primideal $\mathfrak{p}$ übergeht. In diesem Fall ist $S_\mathfrak{p}$ nach (6.7) ein Hauptidealring und freier $R_\mathfrak{p}$-Modul vom Range n, daher

$$D_{S_\mathfrak{p}|R_\mathfrak{p}} = (D_{S|R})_\mathfrak{p} = D_{L|K}(v_1, \ldots, v_n)S_\mathfrak{p}$$

für jede $R_\mathfrak{p}$-Basis $\{v_1, \ldots, v_n\}$ von $S_\mathfrak{p}$.

(9.2) **Hauptsatz.** *Sei $\mathfrak{p} \in \mathbb{P}_R$. Genau dann gilt $\mathfrak{p} \supseteq D_{S|R}$, wenn $\mathfrak{p}$ in L verzweigt oder es ein Primideal $\mathfrak{P}|\mathfrak{p}$ in S gibt mit inseparabler Erweiterung $k_\mathfrak{P}|k_\mathfrak{p}$. Insbesondere gibt es nur endliche viele Primideale von R, die in L verzweigen.*

Beweis. Sei $A = S/\mathfrak{p}S$ und $k = k_\mathfrak{p}$. Nach (7.5) ist $\dim_{\mathrm{k}}\mathrm{A} = \mathrm{n}$. Sei $\{\bar{a}_i\}$ eine k-Basis von A, und sei $a_i \in S$ jeweils ein Urbild von a_i. Seien τ und $\bar{\tau}$ die Bilinearformen auf $S^{(2)}$ bzw. $A^{(2)}$ gegeben durch $\tau(x, y) = Spur(a \mapsto xay)$ bzw. $Spur(\bar{a} \mapsto x\bar{a}y)$. Es ist $\det\big(\bar{\tau}(\bar{a}_i, \bar{a}_j)_{i,j}\big)$ nach (3.7), (3.10) das natürliche Bild von

$$D_{L|K}(a_1, \ldots, a_n) = \det\big(\tau(a_i, a_j)_{i,j}\big)$$

in A. Nach Definition wird $D_{S|R}$ als R-Modul von solchen Diskriminanten erzeugt. Es ist $\det\big(\bar{\tau}(\bar{a}_i, \bar{a}_j)_{i,j}\big) \neq 0$ (in k) genau dann, wenn $\bar{\tau}$ nichtausgeartet ist.

Sei $J(A) \neq 0$, also $\mathfrak{p}$ verzweigt in L nach (7.5). Dann wähle die k-Basis von A so, dass $\bar{a}_1 \in J(A)$ ist. Dann sind alle $\bar{a}_1\bar{a}_i$ nilpotent, alle k-Endomorphismen $x \mapsto \bar{a}_1 x \bar{a}_i$ von A nilpotent und daher $\bar{\tau}(\bar{a}_1, \bar{a}_i) = 0$ für alle i. Die Gramsche Matrix von $\bar{\tau}$ bzgl. $\{\bar{a}_i\}$ hat also in der 1. Spalte nur Nullen; $\bar{\tau}$ ist ausgeartet. Folglich ist $D_{S|R} \subseteq \mathfrak{p}$.

Sei $J(A) = 0$, also $\mathfrak{p}$ unverzeigt in L nach (7.5), und $A \cong k_{\mathfrak{P}_1} \times \ldots \times k_{\mathfrak{P}_r}$ für die Primideale $\mathfrak{P}_i$ in S über $\mathfrak{p}$. Da sich die Ideale $k_i = k_{\mathfrak{P}_i}$ im direkten Produkt gegenseitig annullieren, ist $\bar{\tau} = \bar{\tau}_1 \times \ldots \times \bar{\tau}_r$, wobei $\bar{\tau}_i$ die Einschränkung von $\bar{\tau}$ auf $k_i^{(2)}$ ist. Nach (3.7) ist $\bar{\tau}_i$ die Spurform $(x, y) \mapsto \mathrm{Tr}_{k_i|k}(xy)$, und diese ist nichtausgeartet, wenn $k_i|k$ separabel ist, und die Nullform andernfalls. Es ist also $\bar{\tau}$ genau dann von Null verschieden, wenn alle $k_i|k$ separabel sind. Dies beweist den Satz. □

(9.3) **Folgerung.** *Sei $R = \mathbb{Z}$ und L ein algebraischer Zahlkörper. Genau die Primzahlen verzweigen in L, die D_L teilen.*

Beweis. Man hat nur zu beachten, dass Erweiterungen endlicher Körper immer separabel (sogar zyklisch) sind. □

Wir kommen nun nochmals zurück auf die explizite Beschreibung der Zerlegung in Sinne von Kummer–Dedekind (7.6).

(9.4) **Satz.** *Sei $L = K(\alpha)$ mit $\alpha \in S$ und $f = m_{K,\alpha}$. Ist $\mathfrak{p} \in \mathbb{P}_R$ kein Teiler von $D_f D_{S|R}^{-1}$, so ist $S_\mathfrak{p} = R_\mathfrak{p}[\alpha]$ und daher kann die Zerlegung von $\mathfrak{p}$ in L aus der Reduktion von f mod $\mathfrak{p}$ abgelesen werden (im Sinne von (7.6)).*

Beweis. Nach (6.2) ist $R_\mathfrak{p}$ ein diskreter Bewertungsring mit Restklassenkörper $k_\mathfrak{p} \cong R/\mathfrak{p}$. Nach (6.7) ist $S_\mathfrak{p}$ ein freier $R_\mathfrak{p}$-Modul vom Range $[L : K] = n$. Sei $\{v_1, \ldots, v_n\}$ eine K-Basis von L mit $v_i \in S$ und S-Aufspann $\langle v_1, \ldots, v_n\rangle_S \supseteq \langle 1, \alpha, \ldots, \alpha^{n-1}\rangle_S$. Nach (3.10) ist

$$D_f = D_{L|K}(1, \alpha, \ldots, \alpha^{n-1}) = c^2 D_{L|K}(v_1, \ldots, v_n),$$

wobei $c \in S$ die Determinante einer Übergangsmatrix ist. $D_{S|R}$ wird von all diesen $D_{L|K}(v_1, \ldots, v_n)$ als R-Modul erzeugt. Die Voraussetzung besagt also gerade, dass $\mathfrak{p}$ kein Teiler dieser $c = c(v_1, \ldots, v_n)$ ist. Mit anderen Worten, c ist eine Einheit in $R_\mathfrak{p}$. Folglich ist $R_\mathfrak{p}[\alpha] = S_\mathfrak{p}$. □

(9.5) **Beispiel.** Sei $R = \mathbb{Z}$, $K = \mathbb{Q}$ und $L = \mathbb{Q}(\alpha)$ für die reelle Wurzel α von $f = X^3 - 2$ ($[K : \mathbb{Q}] = n = 3$). Wir behaupten, dass $S = \mathbb{Z}[\alpha]$ der Ring der ganzen Zahlen in L ist. Nach (4.4) ist $\mathbb{Z}[\alpha] = S$ genau dann , wenn $\mathbb{Z}_{(p)}[\alpha] = S_{(p)}$ für alle Primzahlen p gilt.

Es ist $f'(\alpha) = 3\alpha^2$ und daher $D_f = (-1)^{n(n-1)/2}\mathrm{N}_{L|\mathbb{Q}}(f'(\alpha)) = -2^2 \cdot 3^3$. Folglich ist $D_L \in \{-2^2 \cdot 3^3, -3^3, -2^2 \cdot 3, -3\}$. Jedenfalls verzweigen nach (9.3) nur die Primzahlen 2 und 3 in L, und 3 verzweigt sicher. Für $p \geq 5$ gilt also $\mathbb{Z}_{(p)}[\alpha] = S_{(p)}$ nach (7.8) oder (9.4). Dies gilt ebenfalls für $p = 2$ nach (7.9), denn f ist ein Eisenstein-Polynom bzgl. $p = 2$ (und wir haben totale Verzweigtheit). Da $f(X - 1) = (X - 1)^3 - 2 = X^3 - 3X^2 + 3X - 3$ Eisensteinsch bzgl. $p = 3$ ist, und $\mathbb{Z}[\alpha+1] = \mathbb{Z}[\alpha]$, gilt Entsprechendes auch für $p = 3$.

Sei E der Zerfällungskörper von f (in $\mathbb{C}$); dieser enthält den 3-ten Kreisteilungskörper $F = \mathbb{Q}(\sqrt{-3})$, und es ist $E = FL$ das Kompositum. Es ist $G = \mathrm{Gal}(E|\mathbb{Q}) \cong S_3$. Sei $\mathfrak{P}|p$ ein Primideal von E. Sei $p = 2$. Nach (1.8) ist dann 2 träge (prim) in F. Mit (7.3) folgt $f(\mathfrak{P}|2) = 2$, und ebenso $e(\mathfrak{P}|2) = 3$. In diesem Falle ist also $G_\mathfrak{P} = G$ nach (8.3) und E der Trägheitskörper von $\mathfrak{P}$ nach (8.4). Sei $p = 3$. Nach (1.8) verzweigt 3

(total) in F. Mit (7.3) erhalten wir $G = T_{\mathfrak{P}}$ (totale Verzweigung) in diesem Falle. Ist $p \geq 5$, so ist p unverzweigt in E nach (8.6). Sei speziell $p = 5$. Aus $S = \mathbb{Z}[\alpha]$ und der Primfaktorzerlegung $f \bmod 5 = (X+2)(X^2+3X+4)$ über $\mathbb{F}_5$ folgt $5S = \mathfrak{P}_1\mathfrak{P}_2$, wo $\mathfrak{P}_1 = (5, \alpha+2)$ den Restklassengrad 1 und $\mathfrak{P}_2 = (5, \alpha^2+3\alpha+4)$ den Grad 2 hat. Nach (8.6) ist hier also $|G_{\mathfrak{P}}| = 2$ und daher $r_5(E) = 3$.

Anhang (Dedekind-Kriterium). *Sei $R = R_{\mathfrak{p}}$ ein diskreter Bewertungsring und $\alpha \in S = S_{\mathfrak{p}}$ mit $L = K(\alpha)$. Sei $f = m_{K,\alpha}$, und sei $\bar{f} = f \bmod \mathfrak{p}$ die Reduktion. Seien $1 \leq e_1 < e_2 < \ldots < e_s$ die Multiplizitäten der Primfaktoren von $\bar{f}$ in $k_{\mathfrak{p}}[X]$. Es gibt also Produkte $\bar{f}_i$ von paarweise teilerfremden irreduziblen, normierten Polynomen in $k_{\mathfrak{p}}[X]$, so dass*

$$\bar{f} = \bar{f}_1^{e_1} \cdots \bar{f}_s^{e_s}$$

ist. Sei $f_i \in R[X]$ ein normiertes Urbild von $\bar{f}_i$ $(1 \leq i \leq s)$, und setze

$$h = \tfrac{1}{\pi}\big(f_1^{e_1} \cdots f_s^{e_s} - f\big) \in R[X].$$

Genau dann ist $S = R[\alpha]$, wenn die Reduktion $\bar{h} = h \bmod \mathfrak{p}$ teilerfremd ist zu allen $\bar{f}_2, \ldots, \bar{f}_s$ und zu $\bar{f}_1$ im Falle $e_1 > 1$.

Beweis. Setze $k = k_{\mathfrak{p}}$, $\mathfrak{p} = \pi R$ und $A = R[\alpha] \cong R[X]/(f)$. Es ist $\pi A \subseteq J(A)$ nach (7.7). Setzen wir $g = f_1 \cdots f_s$, so ist das Jacobson-Radikal

$$J = J(A) = (\pi, g(\alpha)).$$

Ferner ist $J^e \subseteq \pi A$ für $e = \max\big(e_1, \ldots, e_s\big)$. Sei zunächst $A = S$, also ein Hauptidealring nach (6.7). Ist $e_1 > 1$, so ist dann $J^2 \supseteq \pi A$ und daher $J = \pi A + g(\alpha)A = J^2 + g(\alpha)A$. Aus dem Lemma von Nakayama (4.7) folgt $J = (g(\alpha))$. In diesem Fall ist

$$\pi A = \big(f_1(\alpha)^{e_1} \cdots f_s(\alpha)^{e_s}\big) = \pi h(\alpha) A$$

und somit $h(\alpha)$ eine Einheit in A. Analog ist für $b = f_2(\alpha)^{e_2} \cdots f_s(\alpha)^{e_s}$ das Ideal $(\pi, b) = bA$ (wegen $e_j > 1$ für $j \geq 2$). Ist $e_1 = 1$ und $s > 1$, so ist nach dem Chinesischen Restesatz $\pi A = \big(\pi, f_1(\alpha)\big) \cdot bA = (\pi b, f_1(\alpha) \cdots f_s(a)^{e_s}) = \big(\pi b, \pi h(\alpha)\big)$ und daher $h(\alpha)$ teilerfremd zu b in A.

Zum Beweis der Rückrichtung betrachten wir die Menge

$$\widehat{A} = \{x \in L \,|\, xJ \subseteq J\}.$$

Offenbar ist $\widehat{A}$ ein Ring mit $\widehat{A} \supseteq A$. Da $J = J(A)$ eine endlich erzeugter (Noetherscher) R-Modul ist, ist ferner $\widehat{A}|R$ ganz nach (3.2) (und Definition). Also ist $A \subseteq \widehat{A} \subseteq S = R_{L|R}$. Sei $A = \widehat{A}$ vorausgesetzt. Wir behaupten, dass dann $A = S$ ist. Angenommen, es

gibt ein $y \in S \setminus A$. Dann ist $yJ \not\subseteq J$ (wegen $A = \widehat{A}$). Der Ring $B = A[y]$ ist ganz über R und ein freier R-Modul vom Range $n = [L : K]$. Es gibt eine natürliche Zahl s, so dass $\pi^s B \subseteq J$ ist. Da $J/\pi^s B$ das Jacobson-Radikal (Nilradikal) der endlichdmensionalen k-Algebra $A/\pi^s B$ ist (4.6), gibt es also eine kleinste natürliche Zahl t mit $J^t B \subseteq J$. Hierbei ist $t \geq 2$. Wähle ein Element $z \in J^{t-1}B \setminus J$. Dann ist $zJ \subseteq J^t B \subseteq J$ und daher $z \in \widehat{A} = A$. Andererseits ist

$$z^2 \in (J^{t-1}B)^2 \subseteq J^{2t-2}B \subseteq J^t B \subseteq J.$$

Da A/J ein direktes Produkt von Körpern ist, folgt der Widerspruch $z \in J$.

Zum Beweis von $A = S$ genügt es also nachzuweisen, dass $\widehat{A} = A$ ist. Sei also $y \in \widehat{A}$. Setze noch $g_e = g$ im Falle $e_1 > 1$ und $g_e = f_2 \cdots f_s$ sonst. Nach Voraussetzung ist $\bar{h} = h \bmod p$ teilerfremd zu $\bar{g}_e = g_e \bmod \pi$. Wegen $A/\pi A \cong k[X]/(\bar{f})$ gibt es daher a, b, c in A mit $1 = a\pi + bh(\alpha) + cg_e(\alpha)$. Es gilt also

$$y = a\pi y + bh(\alpha)y + cg_e(\alpha)y.$$

Wir zeigen, dass alle drei Summanden in A liegen. Wir wissen, dass $\pi A \subseteq J$ ist. Daher ist $y\pi \in J$, etwa $y\pi = a_0\pi + b_0 g(\alpha)$ mit $a_0, b_0 \in A$. Durch Ersetzung von y durch $y - a_0$ können wir $y\pi = b_0 g(\alpha)$ annehmen (und die obige Gleichung für y gilt weiterhin).

Es ist klar, dass $ay\pi \in A$ ist. Ferner ist $g(\alpha)y \in J$, somit

$$\pi h(\alpha)y = f_1(\alpha)^{e_1} \dots f_s(\alpha)^{e_s} y = f_1(\alpha)^{e_1 - 1} \dots f_s(\alpha)^{e_s - 1} g(\alpha)y \in \pi A.$$

Folglich ist auch $bh(\alpha)y \in A$, und es bleibt zu zeigen, dass $g_e(\alpha)y \in A$ ist. Dies ist klar im Falle $g_e = g$. Sei also weiterhin $e_1 = 1$.

Ist $s = 1$, so ist $g = f_1 \equiv f \,(\mathrm{mod}\, \pi A[X])$ und daher $g(\alpha) \in \pi A$ und $y = \frac{1}{\pi} b_0 g(\alpha) \in A$. Sei also $s > 1$. Da $b_0 g(\alpha)^2 = g(\alpha)y \in \pi J \subseteq \pi A$ ist, ist $b_0 \bmod \pi$ ein Vielfaches von $f_2(\alpha)^{e_2 - 2} \dots f_s(\alpha)^{e_s - 2}$. Mit anderen Worten, es ist

$$b_0 = a_1\pi + b_1 f_2(\alpha)^{e_2 - 2} \dots f_s(\alpha)^{e_s - 2}$$

für gewisse a_1, b_1 in A. Es folgt

$$(y - a_1 g(\alpha))g_e(\alpha) = (p^{-1}b_0 - a_1)g(\alpha)g_e(\alpha) = b_1 h(\alpha) \in A.$$

Es ist nämlich $(p^{-1}b_0 - a_1)g(\alpha)g_e(\alpha) = \pi^{-1} b_1 g(\alpha) g_e(\alpha) \prod_{j=2}^{s} f_j(\alpha)^{e_j - 2}$, und dies ist gleich $\pi^{-1} b_1 f_1(\alpha) f_2(\alpha)^{e_2} \dots f_s(\alpha)^{e_s} = b_1 h(\alpha)$. Da $a_1 g(\alpha) g_e(\alpha) \in A$ ist, folgt damit $y g_e(\alpha) \in A$, wie gefordert. $\square$

§10. Frobenius-Automorphismen

In diesem Abschnitt sei $L|K$ eine Galoiserweiterung algebraischer Zahlkörper mit Gruppe $G = \mathrm{Gal}(L|K)$. Ferner sei $R = R_K$, $S = R_L$, und $\mathfrak{P}|\mathfrak{p}$ seien Primideale in $S|R$ über der Primzahl p.

(10.1) **Definition.** Sei vorausgesetzt, dass $e(\mathfrak{P}|\mathfrak{p}) = 1$ ist (Unverzweigtheit). Dann gibt es genau ein Element $\sigma = (\mathfrak{P}, L|K)$ in G mit

$$x^\sigma \equiv x^{\mathrm{N}\mathfrak{p}} \,(\mathrm{mod}\,\mathfrak{P})$$

für alle $x \in S$. Dieses σ heißt der *Frobenius-Automorphismus* von $\mathfrak{P}$; σ erzeugt die Zerlegungsgruppe $G_\mathfrak{P}$ von $\mathfrak{P}$, hat also die Ordnung $f(\mathfrak{P}|\mathfrak{p})$.

Bemerkung. Für $\tau \in G$ gilt nach (8.2) $\tau^{-1}(\mathfrak{P}, L|K)\tau = (\mathfrak{P}^\tau, L|K)$. Die Frobenius-Automorphismen bilden also eine *Konjugiertenklasse* in G, die durch $\mathfrak{p}$ bestimmt ist, und wir schreiben $(\mathfrak{p}, L|K)$ für diese Klasse. Ist G *abelsch*, so schreiben wir einfach $(\mathfrak{p}, L|K)$ für den Automorphismus und nennen den Fixkörper auch den Zerlegungskörper von $\mathfrak{p}$.

(10.2) **Lemma.** *Sei $e(\mathfrak{P}|\mathfrak{p}) = 1$ und sei F ein Zwischenkörper von $L|K$. Nach (7.3) ist dann $\mathfrak{P}$ unverzwegit über $\mathfrak{P}_F = F \cap \mathfrak{P}$ und $\mathfrak{P}_F$ unverzweigt über $\mathfrak{p}$. Es gilt:*

(a) $(\mathfrak{P}, L|F) = (\mathfrak{P}, L|K)^{f(\mathfrak{P}_F|\mathfrak{p})}$.

(b) *Ist $F|K$ galoissch, so ist $(\mathfrak{P}_F, F|K) = (\mathfrak{P}, L|K)|F$ die Einschränkung.*

Beweis. Setze $\sigma = (\mathfrak{P}, L|K)$ und $f_0 = (\mathfrak{P}_F|\mathfrak{p})$.

(a) Nach (7.3) ist $\mathrm{N}\mathfrak{P}_F = (\mathrm{N}\mathfrak{p})^{f_0}$ die Ordnung des Körpers $k_{\mathfrak{P}_F}$. Die Zerlegungsgruppe von $\mathfrak{P}$ über F ist der Durchschnitt von $G_\mathfrak{P}$ mit $\mathrm{Gal}(L|F)$ und hat die Ordnung $f(\mathfrak{P}|\mathfrak{P}_F) = |G_\mathfrak{P}|/f_0$. Es ist also $\sigma^{f_0} = (\mathfrak{P}, L|F)$.

(b) Sei $\sigma_0 = \sigma|F$. Da σ das Primideal $\mathfrak{P}_F = \mathfrak{P} \cap F$ invariant lässt, ist σ_0 ein Element der Zerlegungsgruppe von $\mathfrak{P}_F$. Wegen

$$y^{\sigma_0} \equiv y^{\mathrm{N}\mathfrak{p}} \,(\mathrm{mod}\,\mathfrak{P}_F)$$

für alle $y \in S \cap F$ folgt die Behauptung. □

(10.3) **Hauptsatz.** *Sei $K = \mathbb{Q}$ und $L = \mathbb{Q}(\varepsilon)$ der m-te Kreisteilungskörper, $\varepsilon = \varepsilon_m$ eine primitive m-te Einheitswurzel ($m \geq 3$ und $m \not\equiv 2 \,(\mathrm{mod}\,4)$). Genau dann verzweigt eine Primzahl p in L, wenn p ein Teiler von m. (Ist $m = 2u$ mit u ungerade, so ist L der u-te Kreisteilungskörper und 2 verzweigt nicht in L.) Es gelten folgende genauere Aussagen:*

(a) *Ist p eine Primzahl mit $p \nmid m$, so ist der Frobenius $\sigma_p = (p, L|\mathbb{Q})$ festgelegt durch $\varepsilon^{\sigma_p} = \varepsilon^p$, hat also die Ordnung $f = o(p \bmod m)$ in der primen Restklassengruppe $(\mathbb{Z}/m\mathbb{Z})^*$. Die Galoisgruppe $G = \mathrm{Gal}(L|Q)$ wird erzeugt durch diese σ_p, ist also isomorph zu $(\mathbb{Z}/m\mathbb{Z})^*$.*

(b) *Ist p eine Primzahl mit $p \mid m$, etwa $m = p^a r$ mit $p \nmid r$, so ist $\mathbb{Q}(\varepsilon^{p^a}) = \mathbb{Q}(\varepsilon_r)$ der Trägheitskörper von p in L, also $\varphi(p^a) = p^{q-1}(p-1)$ der Verzweigungsindex in L.*

(c) *$R_L = \mathbb{Z}[\varepsilon]$ ist der Ring der ganzen Zahlen in L.*

Beweis. Natürlich ist $\varepsilon = \varepsilon_m$ ganz-algebraisch, und eine Wurzel des m-ten Kreisteilungspolynoms $\Phi_m \in \mathbb{Z}[X]$, dessen Grad $\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^*|$ ist.

(a) Sei p eine Primzahl mit $p \nmid m$. Dann ist $X^m - 1$ separabel mod p, denn die Ableitung mX^{m-1} ist teilerfremd zu $X^m - 1 \bmod p$. Also verzweigt p nicht in L nach (7.8) oder (9.3). Jedes Element $\sigma \in G$ ist festgelegt durch $\varepsilon^\sigma = \varepsilon^j$ für eine Nummer $j = j(\sigma)$ ($1 \le j \le m$ und j teilerfremd zu m). Insbesondere ist G abelsch. Sei $\sigma_p = (p, L|\mathbb{Q})$ der Frobenius zu p. Da ε^{σ_p} Wurzel von $m_{\mathbb{Q},\varepsilon}|\Phi_m$ und $\varepsilon^{\sigma_p} \equiv \varepsilon \pmod{\mathfrak{P}}$ ist, erzwingt die Separabilität mod p, wie in (8.6), die Behauptung $\varepsilon^{\sigma_p} = \varepsilon^p$ und $o(\sigma) = o(p \bmod m) = f = f(\mathfrak{P}|p)$. Nach (7.3) ist übrigens $\mathrm{N}_{L|\mathbb{Q}}(\mathfrak{P}) = (p^f)$ und $(p^f, L|\mathbb{Q}) := \sigma_p^f = 1$.

Dies gilt für alle Primzahlen p, die nicht in m aufgehen. Daher induziert G alle möglichen Automorphismen der zyklischen Gruppe $\langle\varepsilon\rangle$. Es ist $G \cong (\mathbb{Z}/m\mathbb{Z})^*$ und $|G| = \varphi(m) = [L : \mathbb{Q}]$, und $\Phi_m = m_{\mathbb{Q},\varepsilon}$.

(b) Sei p eine Primzahl mit $p \mid m$, und $m = p^a r$ mit $p \nmid r$. Ist p ungerade, so verzweigt p im p-ten Kreisteilungskörper nach (2.5) und daher in L. Ist m gerade, so ist $a \ge 2$ (nach Vereinbarung), und 2 verzweigt in $\mathbb{Q}(i)$ nach (1.8) und damit in L. Wir zeigen, dass p total verzweigt in $F = \mathbb{Q}(\varepsilon^r) = \mathbb{Q}(\varepsilon_{p^a})$. Es ist $\Phi_{p^a}(X) = \frac{X^{p^a}-1}{X^{p^{a-1}}-1} = \Phi_p(X^{p^{a-1}})$ und $\Phi_{p^a}(1) = p$. Setze $\pi = \varepsilon_{p^a} - 1$. Nach (a) ist $m_{\mathbb{Q},\pi}(X) = \Phi_{p^a}(X+1)$. Es ist $m_{\mathbb{Q},\pi}(0) = p$ und daher $\mathrm{N}_{L|\mathbb{Q}}(\pi) = \pm p$. Nach (7.4) ist $\mathfrak{P}_F = \pi R_F$ ein Primideal über p mit $\mathbb{F}_p$ als Restklassenkörper (vgl. mit 2.5). Die (binomische) Berechnung von $m_{\mathbb{Q},\pi} \bmod p$ zeigt, dass das Polynom Eisensteinsch bzgl. p ist. Wende (7.9) an.

Sei $E = \mathbb{Q}(\varepsilon_r)$. Es ist $L = FE$. Nach (a) ist p unverzweigt in E. Da p in $F \cap E$ sowohl unverzweigt wie auch total verzweigt ist, ist $F \cap E = \mathbb{Q}$. (Dies liefert auch die Galoistheorie direkt.) Nach (8.4) ist E der Trägheitskörper von p (oder $\mathfrak{P}$).

(c) Ist $m = p^a$ eine Primzahlpotenz, so verzweigt p nach (b) total in L und ist nach (a) auch die einzige verzweigende Primzahl. Nach (9.3) ist dann $\pm D_L$ eine p-Potenz, und die Behauptung folgt aus (7.9), (7.8) und (4.4), denn dann stimmt die Aussage lokal überall. Der allgemeine Fall folgt mit (8.9) durch Induktion nach der Anzahl der Primteiler von n. □

(10.4) **Definition.** Sei $G = \mathrm{Gal}(L|K)$ abelsch und $I_K^{(u)}$ die freie abelsche Gruppe

der gebrochenen Ideale von $R = R_K$ auf den Primstellen $\mathfrak{p}$, die in L nicht verzweigen (vgl. (5.7) und (9.2)). Durch die Zuordnung $\mathfrak{p} \mapsto (\mathfrak{p}, L|K)$ wird damit ein Homomorphismus $\phi_{L|K} : I_K^{(u)} \to G$ definiert, der sog. idealtheoretische *Artin-Homomorphismus.*

Theorem. *$\phi_{L|K}$ ist surjektiv.*

Der Beweis dieses Theorems beruht auf der 1. Ungleichung der *Klassenkörpertheorie* (siehe Anhang). Diese Theorie beschreibt alle abelschen Galoiserweiterungen eines Zahlkörpers K durch die *innere Struktur* des Körpers. Wir können in dieser Vorlesung nur den Spezialfall $K = \mathbb{Q}$ behandeln; wir werden (in §17) zeigen, dass alle abelschen Erweiterungen von $\mathbb{Q}$ "Kreiskörper" sind, d.h., Teilkörper von Kreisteilungskörpern (Kronecker–Weber).

Spezialfall. *Sei $K = \mathbb{Q}$ und $L = \mathbb{Q}(\varepsilon_m)$ wie in (10.3); sei $m = p_1^{e_1} \cdots p_r^{e_r}$ die Primfaktorzerlegung. Es ist $I_{\mathbb{Q}}^{(u)} = I_{\mathbb{Q}}^{(m)}$ die Gruppe der gebrochenen Ideale (x) von $\mathbb{Q}$, die teilerfremd zu m (Zähler und Nenner) sind, $\phi_{L|\mathbb{Q}} : I_{\mathbb{Q}}^{(m)} \to G$ ist surjektiv und $\mathrm{Ker}(\phi_{L|\mathbb{Q}}) = H_{\mathbb{Q}}^{(mp_\infty)}$ besteht aus allen solchen (x), für welche $x > 0$ ist (entsprechend der archimedischen Betragsbewertung $|\cdot| = p_\infty$ von $\mathbb{Q}$) und $x \equiv 1 \,(\mathrm{mod}\, m)$ ist, d.h., $v_{p_i}(x-1) \geq e_i$ für alle $i = 1, \ldots, r$.*

Beweis. Nach (10.3) ist nur die letzte Aussage zu beweisen. Der Artin-Homomorphismus $\phi_{L|\mathbb{Q}} : I_{\mathbb{Q}}^{(m)} \to G \cong (\mathbb{Z}/m\mathbb{Z})^*$ ist erklärt durch $(p) = (-p) \mapsto p + m\mathbb{Z}$ ($p \in \mathbb{P}$, $p \nmid m$). Sei $x = \frac{a}{b}$ und $(x) = (-x)$ in $\mathrm{Ker}(\phi_{L|\mathbb{Q}})$ ($a, b \in \mathbb{Z}$ teilerfremd, $b > 0$). Dann ist $|a| \equiv b \,(\mathrm{mod}\, m)$. Für den *positiven* Erzeuger von $(x) = x\mathbb{Z}$ gilt also die Kongruenz $1 \,(\mathrm{mod}\, m)$ (für den negativen nicht wegen $m > 2$). □

Notation. Unter 2^* verstehen wir im Folgenden eine der Zahlen $-4, \pm 8$, und unter $\mathbb{Q}(\sqrt{2^*})$ entsprechend einen der drei quadratischen Zahlkörper. Ferner sei

$$p^* = \Big(\frac{-1}{p}\Big)p = \begin{cases} +p & \text{falls } p \equiv 1 \,(\mathrm{mod}\, 4) \\ -p & \text{falls } p \equiv 3 \,(\mathrm{mod}\, 4) \end{cases}.$$

für eine ungerade Primzahl p. Die beiden *Ergänzungsgesetze* haben wir schon in den Übungen diskutiert: $\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \,(\mathrm{mod}\, 4)$; $\left(\frac{2}{p}\right) = 1 \iff p \equiv \pm 1 \,(\mathrm{mod}\, 8)$.

(10.5) **Lemma.** *Sei $m = p^a$ für eine Primzahl p ($a \geq 1$, und $a \geq 3$ im Falle $p = 2$). Sei $L = \mathbb{Q}(\varepsilon_m)$.*

(a) *Ist $p \neq 2$, so ist $\mathbb{Q}(\sqrt{p^*}$ der einzige quadratische Zahlkörper der in L liegt.*

(b) *Ist $p = 2$, so sind die drei Körper $\mathbb{Q}(\sqrt{2^*})$ die quadratischen Zahlkörper in L, und $\mathbb{Q}(\sqrt{2})$ ist der einzige quadratische Zahlkörper, der im maximalen total reellen Teilkörper L^+ liegt. Insbesondere ist $L^+|\mathbb{Q}$ zyklisch (und $(\mathbb{Z}/2^a\mathbb{Z})^* \cong \mathbb{Z}/2^{a-2}\mathbb{Z} \times \{\pm 1\}$).*

Beweis. Nach (10.3) verzweigt die Primzahl p total in L, und sonst keine. Ist $p \neq 2$, so ist nach (1.8) $\mathbb{Q}(\sqrt{p^*})$ der einzige quadratische Zahlkörper, in welchem p verzweigt und sonst keine andere Primzahl. In allen drei Körpern $\mathbb{Q}(\sqrt{2^*})$ verzweigt 2 und sonst keine andere Primzahl, und $\mathbb{Q}(\sqrt{2})$ ist der einzige reelle Körper unter diesen. Im Falle $p = 2$ hat $\mathrm{Gal}(L^+|\mathbb{Q})$ daher nur eine maximale Untergruppe, ist also zyklisch (von 2-Potenzordnung). □

Bemerkung. Sei $p \neq 2$ in (10.5). Die Anwendung von (0.4) zeigt, dass L einen eindeutig bestimmten Teilkörper K besitzt mit $[K : \mathbb{Q}] = p^{a-1}$ ($L = K \cdot \mathbb{Q}(\varepsilon_p)$). In (17.6) werden wir zeigen: Ist $K'|\mathbb{Q}$ galoissch vom Grade p^{a-1}, und verzweigt nur die Primzahl p in K', so ist $K'|\mathbb{Q}$ zyklisch und $K' = K$ ist. Dies ist ein wesentlicher Schritt zum Beweis von Kronecker–Weber. Dass $(\mathbb{Z}/p^a\mathbb{Z})^* \cong \mathbb{Z}/p^{a-1}\mathbb{Z} \times \mathbb{F}_p^*$ zyklisch ist, kann man direkt aus der Kongruenz $(1+p)^{p^{a-2}} \equiv 1 + p^{a-1} \pmod{p^a}$ ablesen.

(10.6) **Folgerung.** *Jeder quadratische Zahlkörper ist ein Kreiskörper.*

Beweis. Nach (1.1) hat ein solcher Körper die Form $K = \mathbb{Q}(\sqrt{d})$ mit einer eindeutig bestimmten quadratfreien ganzen Zahl $d \neq 0, 1$. Ist $d \equiv 1 \pmod 4$, so ist $D_K = d = p_1^* \dots p_s^*$ mit paarweise verschiedenen ungeraden Primzahlen p_i. Ist $d \equiv 2, 3 \pmod 4$, so ist $D_K = 4d = 2^* p_1^* \dots p_s^*$, wobei $2^* \in \{-4, \pm 8\}$ und die übrigen p_i wieder ungerade Primzahlen sind. In jedem Falle liegt K im $|D_K|$-ten Kreisteilungskörper über $\mathbb{Q}$. □

(10.7) **Satz** (Quadratisches Reziprozitätsgesetz; C.F. Gauß, 1777-1855). *Für ungerade Primzahlen $p \neq q$ gilt*

$$\left(\tfrac{q}{p}\right) = \left(\tfrac{p}{q}\right) \iff p \equiv 1 \pmod 4 \text{ oder } q \equiv 1 \pmod 4.$$

Beweis. Sei $L = \mathbb{Q}(\varepsilon)$ der p-te Kreisteilungskörper. Nach (10.5) ist $K = \mathbb{Q}(\sqrt{p^*})$ der in L liegende quadratische Zahlkörper. Sei $H = \mathrm{Gal}(L|K)$. Nach (10.3) ist q unverzweigt in L, somit $\sigma = \sigma_q = (q, L|\mathbb{Q}) : \varepsilon \mapsto \varepsilon^q$ erklärt. Nach (10.2) ist die Einschränkung $\sigma|K = (q, K|\mathbb{Q})$, daher $\sigma \in H \iff (q, K|\mathbb{Q}) = 1$, und dies tritt genau dann ein, wenn q in K total zerfällt. Dies ist nach (1.8) genau dann der Fall, wenn $\left(\frac{p^*}{q}\right) = 1$ ist. Andererseits ist $\sigma \in H$ genau dann, wenn $o(\sigma) = o(q \bmod p)$ ein Teiler von $(p-1)/2$ ist, und dies ist genau dann der Fall, wenn die Restklasse von q ein Quadrat in $\mathbb{F}_p^*$ ist, d.h., wenn $\left(\frac{q}{p}\right) = 1$ ist. Es ist also

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right).$$

Man beachte noch, dass $\left(\frac{p^*}{q}\right) = \left(\frac{p}{q}\right)\left(\frac{(-1)^{(p-1)/2}}{q}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ ist. □

(10.8) **Satz.** *Sei $m \geq 3$. Es gibt unendlich viele Primzahlen $p \equiv 1 \,(\mathrm{mod}\, m)$.*

Beweis. Nach (10.3) zerfällt eine Primzahlen p genau in $L = \mathbb{Q}(\varepsilon_m)$ total, wenn $p \nmid m$ und $(p, L|\mathbb{Q}) = 1$ ist. Das bedeutet gerade, dass $p \equiv 1 \,(\mathrm{mod}\, m)$ ist. Es ist also zu zeigen, das es unendlich viele Primzahlen p gibt, die in L zerfallen. (Eine entsprechende Aussage gilt für jeden Zahlkörper, mit ähnlicher Beweisführung durch Übergang zur Galoishülle.) Ist p eine Primzahl, für welche $\Phi_m \bmod p$ eine Wurzel in $\mathbb{F}_p$ hat, so zerfällt die Reduktion nach (8.5) über $\mathbb{F}_p$ in Linearfaktoren und daher ist $(p, L|\mathbb{Q}) = 1$. Es ist $\Phi_m(0) = \pm 1$, somit $\Phi_m(n!) \equiv \pm 1 \,(\mathrm{mod}\, n!)$ für jede positive ganze Zahl n. Eine Primzahl $p \leq n$ kann daher kein Teiler von $\Phi_m(n!)$ sein. Es gibt aber eine Primzahl p, die $\Phi_m(n!)$ teilt. Zu jeder natürlichen Zahl n gibt es also eine Primzahl $p > n$ mit $(p, L|\mathbb{Q}) = 1$. $\square$

(10.9) **Anmerkungen.** Sei $L = \mathbb{Q}(\varepsilon_m)$ wie eben. Zu jedem vorgegebenen Element $\sigma : \varepsilon_m \mapsto \varepsilon_m^a$ von $\mathrm{Gal}(L|\mathbb{Q})$ gibt es unendlich viele Primzahlen p, so dass $(p, L|\mathbb{Q}) = \sigma$ ist. Mit anderen Worten: Zu jeder zu m teilerfremden ganzen Zahl a gibt es unendlich viele Primzahlen p mit $p \equiv a \,(\mathrm{mod}\, m)$. Dies ist der *Dirichletsche Primzahlsatz*, dessen Beweis analytische Methoden benutzt (Neukirch, S. 490). In (10.3), (10.4) bedeutet dies, dass der Artin-Homomorphismus surjektiv bleibt auf kleineren Idealgruppen.

Auch hier gibt es eine Verallgemeinerung auf beliebige Galoiserweiterungen $L|K$ von Zahlkörpern, die auf *Frobenius* und *Chebotarev* zurückgeht: Zu jeder Konjugiertenklasse c in $G = \mathrm{Gal}(L|K)$ gibt es unendlich viele $\mathfrak{p}$ in K mit $c = \left(\mathfrak{p}, L|K\right)$ (Neukirch, S. 569 oder Narkiewics, p. 382).

§11. Geometrie der Zahlen

Es sei K ein algebraischer Zahlkörper vom Grade $[K:\mathbb{Q}] = n$ und $R = R_K$. Sei ferner $\mathbb{R}^{(n)}$ der reelle euklidische Vektorraum (mit Lebesgueschem Maß) der Dimension n. Wie in (1.1) sei $n = r_1 + 2r_2$, wobei $\sigma_1, \ldots, \sigma_{r_1}$ die verschiedenen Einbettungen von K in $\mathbb{R}$ sind und $\sigma_{r_1+j} \neq \overline{\sigma_{r_1+j}}$ für $1 \leq j \leq r_2$ die Paare konjugiert komplexer (imaginärer) Einbettungen.

(11.1) **Definition.** Der (Ring-) Monomorphismus $\sigma : K \to \mathbb{R}^{(n)}$ mit

$$x^\sigma = \Big(x^{\sigma_1}, \ldots, x^{\sigma_{r_1}}, \mathrm{Re}(\mathrm{x}^{\sigma_{r_1+1}}), \mathrm{Im}(\mathrm{x}^{\sigma_{r_1+1}}), \ldots, \mathrm{Re}(\mathrm{x}^{\sigma_{r_1+r_2}}), \mathrm{Im}(\mathrm{y}^{\sigma_{r_1+r_2}})\Big)$$

heißt die *Minkowski-Einbettung* von K (H. Minkowski, 1864-1909). Unter dieser Abbildung wird der Ring $R = R_K$, der ein freier $\mathbb{Z}$-Modul vom Range n ist, offenbar auf eine *diskrete Untergruppe* von $\mathbb{R}^{(n)}$ abgebildet. Eine additive Untergruppe H von $\mathbb{R}^{(n)}$ heißt dabei diskret, falls in jeder beschränkten (kompakten) Teilmenge des $\mathbb{R}^{(n)}$ nur endlich viele Punkte von H liegen. Erzeugt H den ganzen reellen Vektorraum $\mathbb{R}^{(n)}$, so nennen wir H ein *Gitter* im $\mathbb{R}^{(n)}$. (Beispiele für $n = 2$ findet man in §1.)

(11.2) **Lemma.** *Ist H eine diskrete Untergruppe von $\mathbb{R}^{(n)}$, so gibt es $\mathbb{R}$-linear unabhängige Vektoren $v_1, \ldots, v_r$, so dass H der freie $\mathbb{Z}$-Modul mit $\{v_1, \ldots, v_r\}$ als Basis ist.*

Beweis. Sei r maximal, so dass es $\mathbb{R}$-linear unabhängige Vektoren $u_1, \ldots, u_r$ in H gibt. Wir können $r > 0$ und induktiv die u_i so annehmen, dass jeder Vektor in der Untergruppe $H_0 = H \cap \langle u_1, \ldots, u_{r-1}\rangle_{\mathbb{R}}$ eine $\mathbb{Z}$-Linearkombination in $u_1, \ldots, u_{r-1}$ ist. Jeder Vektor in H ist eine $\mathbb{R}$-Linearkombination in den $u_1, \ldots, u_r$.

Sei T die Menge aller $x \in H$ der Form $x = \sum_{i=1}^{r} a_i u_i$ mit $a_i \in \mathbb{R}$ und $0 \leq a_i < 1$ für $i = 1, \ldots, r-1$, $0 \leq a_r \leq 1$. Es ist $u_r \in T$, und T ist beschränkt, also endlich. Sei $v \in T$ ein Element mit kleinstem Koeffizienten $a_r = b_r > 0$ bei u_r, etwa

$$v = v_r = b_1 u_1 + \cdots + b_r u_r.$$

Zu vorgegebem $h = \sum_i c_i u_i$ in H ($c_i \in \mathbb{R}$) findet man dann $z_i \in \mathbb{Z}$ derart, dass

$$h' = h - z_r v - z_1 u_1 - \cdots - z_{r-1} u_{r-1} \in T$$

und dass für den Koeffizienten $c'_r = c_r - z_r b_r$ von h' bei u_r gilt $0 \leq c'_r < b_r$. (Wähle z_r so, dass $z_r b_r \leq c_r < (z_r + 1) b_r$ ist.) Dann ist $c'_r = 0$ und $h' \in H_0$, also eine $\mathbb{Z}$-Linearkombination in $u_1, \ldots, u_{r-1}$ nach Induktionsvoraussetzung. Damit ist h eine $\mathbb{Z}$-Linearkombination in $u_1, \cdots, u_{r-1}, v_r$. Setze noch $v_i = u_i$ für $i = 1, \ldots, r-1$. Offenbar sind $v_1, \ldots, v_r$ linear unabhängig über $\mathbb{R}$ und bilden eine $\mathbb{Z}$-Basis von H. $\square$

(11.3) **Definition.** Sei $H \subseteq \mathbb{R}^{(n)}$ ein Gitter. Es gibt eine $\mathbb{R}$-Basis $\{w_1, \ldots, w_n\}$ von $\mathbb{R}^{(n)}$, die H als $\mathbb{Z}$-Modul erzeugt. Wir nennen dann

$$P = \{c_1 w_1 + \ldots + c_n w_n | \, c_i \in \mathbb{R}, \; 0 \leq c_i < 1\}$$

den zugehörigen Fundamentalbereich (Grundmasche) von H. Das *Maß* von H wird dann erklärt durch das Volumen von P, d.h.,

$$\mu(H) = \mathrm{vol(P)} = |\det(\mathrm{w_1}, \ldots, \mathrm{w_n})|.$$

Bemerkung. Ein Basiswechsel wird durch eine Transfomationsmatrix $T \in \mathrm{GL}_n(\mathbb{Z})$ bewerkstelligt. Wegen $\det(T) = \pm 1$ ist das Maß von H also wohldefiniert. Übrigens gibt es zu jedem $y \in \mathbb{R}^{(n)}$ genau ein $x \in P$ mit $y \equiv x \,(\mathrm{mod}\, H)$, und $\mathbb{R}^{(n)}/H$ ist ein n-dimensionaler *Torus*. Ist $H' \subseteq H$ eine additive Untergruppe mit endlichem Index, so ist H' nach (0.3) ein Teilgitter von H mit Maß $\mu(H') = \mu(H)|H : H'|$.

(11.4) **Hauptsatz** (Minkowski). *Sei $H \subseteq \mathbb{R}^{(n)}$ ein Gitter. Sei $T \subseteq \mathbb{R}^{(n)}$ eine kompakte, konvexe Teilmenge, die symmetrisch zu 0 liegt. Ist dann* $\mathrm{vol(T)} \geq 2^{\mathrm{n}} \mu(\mathrm{H})$*, so gibt es einen Gitterpunkt $0 \neq h_0 \in H \cap T$.*

Beweis. T konvex bedeutet, dass mit $x, y \in T$ auch die Verbindungsstrecke $\{tx + (1-t)y | \, 0 \leq t \leq 1\}$ in T liegt. T symmetrsich zu 0 meint, dass mit $x \in T$ auch $-x \in T$ ist. Kompakte Teilmengen von $\mathbb{R}^{(n)}$ haben bekanntlich ein Lebeguessches Maß (hier mit vol bezeichnet), und dieses Maß ist σ-additiv (abzählbar additiv) und translationsinvariant. Sei P ein Fundamentalbereich zu H, also $\mu(H) = \mathrm{vol(P)}$.

1. Fall: $\mathrm{vol(T)} > 2^{\mathrm{n}}\mathrm{vol(P)}$

Setze $T' = \frac{1}{2}T = \{\frac{1}{2}y \,|\, y \in T\}$. Es ist dann $\mathrm{vol(T')} = (\frac{1}{2})^{\mathrm{n}}\mathrm{vol(T)}$, daher $\mathrm{vol(T')} > \mathrm{vol(P)}$. Ferner gilt

$$T' = \biguplus_{h \in H} \Big(T' \cap (P + h) \Big).$$

Daraus folgt $\mathrm{vol(T')} = \sum_{\mathrm{h} \in \mathrm{H}} \mathrm{vol}\big(\mathrm{T'} \cap \mathrm{P} + \mathrm{h})\big)$. Wegen der Translationsinvarianz ist $\mathrm{vol}\big(\mathrm{T'} \cap \mathrm{P} + \mathrm{h})\big) = \mathrm{vol}\big((-\mathrm{h} + \mathrm{T'}) \cap \mathrm{P}\big)$. Die Mengen $(-h + T') \cap P$, $h \in H$, können nicht paarweise disjunkt sein. Daher gibt es $x \neq y$ in T mit $\frac{x}{2} \equiv \frac{y}{2} \,(\mathrm{mod}\, H)$. Da T symmetrisch bzgl. 0 ist, ist auch $-y \in T$; da T konvex ist, ist damit auch $\frac{1}{2}(x - y) \in T$. Folglich ist $h_0 = \frac{1}{2}(x - y)$ ein von Null verschiedenes Element in $H \cap T$.

2. Fall: $\mathrm{vol(T)} = 2^{\mathrm{n}}\mathrm{vol(P)}$

Für jedes $\varepsilon > 0$ setze $T_\varepsilon = (1 + \varepsilon)T$. Dies ist eine kompakte Menge mit $\mathrm{vol}(\mathrm{T}_\varepsilon) = (1 + \varepsilon)^{\mathrm{n}}\mathrm{vol(T)} > \mathrm{vol(T)}$. Nach Fall 1 ist also $T_\varepsilon \cap (H \setminus \{0\}) \neq \varnothing$. Nach (11.2) ist diese Menge endlich (nämlich kompakt und diskret). Da der Durchschnitt einer Kette nichtleerer kompakter Mengen nichtleer ist, folgt die Behauptung auch in diesem Fall. □

(11.5) **Beispiel.** Sei $T = B_n(r)$ die kompakte Einheitskugel im $\mathbb{R}^{(n)}$ um 0 mit Radius $r > 0$. Dann ist $\mathrm{vol(T)} = \omega_\mathrm{n} \mathrm{r}^\mathrm{n}$ mit einer Konstanten ω_n. Es ist $\omega_1 = 2$, $\omega_2 = \pi$, $\omega_3 = \frac{4}{3}\pi$, etc.. Für $n > 2$ gilt nach dem Satz von Fubini und dem Transformationssatz induktiv (Einführung von Polarkoordianten)

$$\omega_n = \int_0^{2\pi} \int_0^1 \omega_{n-2}(\sqrt{1-\rho^2})^{n-2}\rho \;\, d\rho \, d\theta = 2\pi\omega_{n-2}/n.$$

Für gerades n ist also $\omega_n = \pi^{n/2}/(n/2)!$ (und im allgemeinen $\omega_n = \pi^{n/2}/\Gamma(1+\frac{n}{2})$). Sei $\mathbb{Z}^{(n)}$ das kanonische Gitter im $\mathbb{R}^{(n)}$ (mit Maß 1) und $H \subseteq \mathbb{Z}^{(n)}$ eine Untergruppe mit endlichem Index m. Dann ist H ein Gitter im $\mathbb{R}^{(n)}$ mit Maß $\mu(H) = m$. Ist $\mathrm{vol(B_n(r))} = 2^\mathrm{n}\mu\mathrm{(H)}$, d.h. $r^n = 2^n\mu(H)/\omega_n$, so gibt es also nach (11.4) ganze Zahlen x_i, nicht alle gleich 0, so dass $(x_1, \ldots, x_n) \in H \cap B_n(r)$ ist. Dann ist also

$$0 < x_1^2 + \cdots + x_n^2 \leq \frac{4}{(\omega_n)^{2/n}}\mu(H)^{2/n}.$$

Für $n \leq 4$ ist $\frac{4}{(\omega_n)^{2/n}} < 2$.

(11.6) **Anwendung** (Lagrange). *Jede natürliche Zahl m ist Summe von 4 Quadraten ganzer Zahlen.*

Beweis. Für $\alpha = a + ib$ und $\beta = c + id$ mit $a, b, c, d \in \mathbb{Z}$ (und $i^2 = -1$) ist $\det \begin{pmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{pmatrix} = a^2 + b^2 + c^2 + d^2$. Da det multiplikativ ist, sind also Produkte von Summen von 4 Quadraten wieder Summen von 4 Quadraten. Es genügt also den Satz für Primzahlen $m = p$ zu beweisen. Wir können $p \neq 2$ annehmen (und $p \equiv 3 \,(\mathrm{mod}\, 4)$ nach Übung (5)). Es gibt ganze Zahlen u, v mit $u^2 + v^2 \equiv -1 \,(\mathrm{mod}\, p)$, denn es gibt $(p+1)/2$ Quadrate $\bar{u}^2$ in $\mathbb{F}_p$ (inklusive 0) und $(p+1)/2$ Elemente der Form $-1 - \bar{v}^2$ (Schubfachprinzip). Für diese u, v sei

$$H = \{(a, b, c, d) \in \mathbb{Z}^{(4)} \mid c \equiv ua + vb \,(\mathrm{mod}\, p),\ d \equiv -va + ub \,(\mathrm{mod}\, p)\}.$$

H ist eine Untergruppe von $\mathbb{Z}^{(4)}$ mit Index p^2, und ein Gitter in $\mathbb{R}^{(4)}$ mit Maß $\mu(H) = p^2$. (Eine Transfromationsmatrix von $\mathbb{Z}^{(4)}$ auf H ist gegeben durch $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ u & v & p & 0 \\ -v & u & 0 & p \end{pmatrix}$.)

Nach (11.5) gibt es $(a, b, c, d) \in H$ mit

$$0 < a^2 + b^2 + c^2 + d^2 < 2\mu(H)^{1/2} = 2p.$$

Rechnen mod p liefert $a^2 + b^2 + c^2 + d^2 \equiv a^2 + b^2 + (ua + vb)^2 - (ub - va)^2 \,(\mathrm{mod}\, p)$, und die rechte Seite ist gleich $(u^2 + v^2 + 1)a^2 + (u^2 + v^2 + 1)b^2 \equiv 0 \,(\mathrm{mod}\, p)$. Folglich ist $p = a^2 + b^2 + c^2 + d^2$. $\square$

(11.7) **Satz.** *R^σ ist ein Gitter in $\mathbb{R}^{(n)}$ mit Maß $\mu(R^\sigma) = 2^{-r_2}|D_K|^{1/2}$.*

Beweis. Sei $\{v_1, \dots, v_n\}$ eine Ganzheitsbasis von R. Nach (3.10) ist die Diskriminante $D_K = D_{K|\mathbb{Q}}(w_1, \dots, w_n)$ gegeben durch die Determinante (im Quadrat)

$$D_K = \begin{vmatrix} w_1^{\sigma_1} & \dots & w_n^{\sigma_1} \\ \vdots & & \vdots \\ w_1^{\sigma_{r_1+1}} & \dots & w_n^{\sigma_{r_1+1}} \\ \vdots & & \vdots \\ w_1^{\bar\sigma_{r_1+1}} & \dots & w_n^{\bar\sigma_{r_1+1}} \\ \vdots & & \vdots \end{vmatrix}^2 .$$

Benützt man, dass $\bar{+}z = 2\mathrm{Re(z)}$ und $-\mathrm{Re(z)} + \bar{\mathrm{z}} = -\mathrm{i\ Im(z)}$ ist für $z \in \mathbb{C}$, so erhält man durch Addition von r_2 Zeilen und anschließende Subtraktion von r_2 Zeilen $D_K = \Big(2^{r_2}(-i)^{r_2} \det(w_1^\sigma, \dots, w_n^\sigma)\Big)^2$. Wegen $D_K \neq 0$ sind also die Vektoren $w_1^\sigma, \dots, w_n^\sigma$ $\mathbb{R}$-linear unabhängig. Folglich ist R^σ ein Gitter in $\mathbb{R}^{(n)}$, und zwar mit Maß $\mu(R^\sigma) = |\det(w_1^\sigma, \dots, w_n^\sigma)| = 2^{-r_2}|D_K|^{1/2}$. $\square$

(11.8) **Folgerung.** *Ist $\mathfrak{a} \neq 0$ ein Ideal von $R = R_K$, so ist $\mathfrak{a}^\sigma$ ein Gitter in $\mathbb{R}^{(n)}$ mit Maß $\mu(\mathfrak{a}^\sigma) = 2^{-r_2}|D_K|^{1/2}\mathrm{N}\mathfrak{a}$.*

Beweis. Es ist $\mathfrak{a}^\sigma$ eine Untergruppe von R^σ mit endlichem Index $|R^\sigma : \mathfrak{a}^\sigma| = |R/\mathfrak{a}| = \mathrm{N}\mathfrak{a}$. $\square$

(11.9)) **Archimedische Bewertungen.** Sei $x \in K$. Für jede reelle Einbettung $\sigma_i : K \to \mathbb{R}$ definiere die zugehörige reelle Bewertung durch den reellen Betrag

$$|x|_i = |x^{\sigma_i}| \quad (1 \leq i \leq r_1).$$

Für jedes Paar imaginärer Einbettungen $\sigma_{r_1+j} \neq \bar\sigma_{r_1+j}$ definiere die zugehörige komplexe Bewertung durch

$$|x|_{r_1+j} = x^{\sigma_{r_1+j}}\overline{x^{\sigma_{1+j}}} = x^{\bar\sigma_{r_1+j}}\overline{x^{\bar\sigma_{r_1+j}}} = |x^{\sigma_{r_1+j}}|^2 \quad (1 \leq j \leq r_2)$$

(komplexer Betrag quadratisch). Diese $r = r_1 + r_2$ *archimedischen Bewertungen* sind bis auf Äquivalenz neben den $\mathfrak{p}$-adischen Bewertungen ($\mathfrak{p} \in \mathbb{P}_R$) die einzigen Bewertungen von K (Ostrowski). Sie beschreiben Homomorphismen von K^* in $\mathbb{R}^*$ (plus Dreiecksungleichung). Für $x \in K^*$ gilt

$$|\mathrm{N}_{K|\mathbb{Q}}(x)| = \prod_{j=1}^{r} |x|_j.$$

§12. Die Klassenzahl

Voraussetzungen und Bezeichnungen wie in §11 ($[K:\mathbb{Q}] = n = r_1 + 2r_2$, σ etc.). Nach (5.2), (5.7) ist die Idealklassengruppe $\mathrm{C}\ell_K = \mathrm{C}\ell_R = \{[\mathfrak{a}] = \mathfrak{a}H_R : \mathfrak{a} \in I_R\}$ des Dedekindrings $R = R_K$ erklärt. Wir zeigen, dass diese Gruppe endliche Ordnung besitzt; $h_K = |\mathrm{C}\ell_K|$ heißt die *Klassenzahl* von K. Ihre Größe misst die Abweichung von R von der Eigenschaft, Hauptidealring zu sein.

(12.1) **Definition.** $M_K = M(r_1, r_2) = (\frac{4}{\pi})^{r_2} \frac{n!}{n^n}$ heißt die *Minkowski-Konstante* von K. Es ist also $M_{\mathbb{Q}} = M(1,0) = 1$ (zu $n = 1$). Ferner gilt:

Zu $n = 2$: $M(2,0) = 0,5$ und $M(0,1) \approx 0,63661$.

Zu $n = 3$: $M(3,0) \approx 0,22222$ und $M(1,1) \approx 0,28299$.

Zu $n = 4$: $M(4,0) = 0,09375$ und $M(2,1) \approx 0,11937$ und $M(0,2) \approx 0,12198$.

Zu $n = 5$: $M(5,0) = 0,0384$ und $M(3,1) \approx 0,04889$ und $M(1,2) \approx 0,06225$.

(12.2) **Satz.** *In jeder Idealklasse von K (d.i. von $R = R_K$) liegt ein Ideal $\mathfrak{a}$ mit Norm $\mathrm{N}\mathfrak{a} \leq M_K |D_K|^{1/2}$.*

Beweis. (a) Sei $c \in \mathrm{C}\ell_K$. Es gibt ein *ganzes* Ideal $\mathfrak{b}$ mit Klasse $[\mathfrak{b}] \in c^{-1}$. (Multipliziere sonst mit einem geeigneten Element $\neq 0$ von R.) Nach (11.8) ist $\mathfrak{b}^\sigma$ ein Gitter in $\mathbb{R}^{(n)}$ mit Maß$\mu(\mathfrak{b}^\sigma) = 2^{-r_2}|D_K|^{1/2}\mathrm{N}\mathfrak{b}$. Wir suchen ein Element $0 \neq x \in \mathfrak{b}$ mit $|N_{K|\mathbb{Q}}(x)| \leq M_K |D_K|^{1/2}\mathrm{N}\mathfrak{b}$. Nach (5.8) ist dann $\mathfrak{a} = x\mathfrak{b}^{-1}$ ein ganzes Ideal von R, mit $[\mathfrak{a}])c$, und nach (7.4) gilt $\mathrm{N}\mathfrak{a} = \mathrm{N}_{K|\mathbb{Q}}(x)/\mathrm{N}\mathfrak{b} \leq M_K |D_K|^{1/2}$, wie gewünscht. Man beachte, dass nach der arithmetisch-geometrischen Ungleichung für den Betrag der Norm gilt

$$|\mathrm{N}_{K|\mathbb{Q}}(x)| = \prod_{i=1}^{r_1} |x^{\sigma_i}| \prod_{j=1}^{r_2} |x^{\sigma_{r_1+j}}|^2 \leq \Big(\frac{1}{n}\big(\sum_{i=1}^{r_1} |x^{\sigma_i}| + 2\sum_{j=1}^{r_2} |x^{\sigma_{r_1+j}}|\big)\Big)^n.$$

(b) Für eine reelle Zahl $a > 0$ betrachte die Teilmenge T_a von $\mathbb{R}^{(n)} = \mathbb{R}^{(r_1)} \times \mathbb{C}^{(r_2)} = \mathbb{R}^{(n)}$ der Tupel $(y_1, \ldots, y_{r_1}; z_1, \ldots, z_{r_2})$ mit

$$\sum_{i=1}^{r_1} |y_i| + 2\sum_{j=1}^{r_2} |z_j| \leq a.$$

Diese Menge T_a ist kompakt, konvex und symmetrisch bzgl. 0. Für ihr Volumen gilt $\mathrm{vol}(\mathrm{T_a}) = 2^{\mathrm{r_1}}\Big(\frac{\pi}{2}\Big)^{\mathrm{r_2}} \frac{\mathrm{a^n}}{\mathrm{n!}}$ (siehe Anhang), und dies hängt stetig von a ab (monoton wachsend). Wähle a so, dass $\mathrm{vol}(\mathrm{T_a}) = 2^{\mathrm{n}}\mu(\mathfrak{b}^\sigma) = 2^{\mathrm{r_1}+2\mathrm{r_2}}\mu(\mathfrak{b}^\sigma)$ ist. Es gilt dann

$$\Big(\frac{\pi}{2}\Big)^{r_2} \frac{a^n}{n!} = 2^{r_2}|D_K|^{1/2}\mathrm{N}\mathfrak{b}.$$

Nach (11.4) gibt es $0 \neq x \in \mathfrak{b}$ mit $x^\sigma \in T_a$. Gemäß (a) erhalten wir, wie gewünscht, $|\mathrm{N}_{K\mathbb{Q}}(x)| \leq \frac{a^n}{n^n} = M_K |D_K|^{1/2}\mathrm{N}\mathfrak{b}$. $\square$

(12.3) **Hauptsatz** (Dirichlet). *$\mathrm{C}\ell_K$ ist eine endliche Gruppe, also die Klassenzahl $h_K = |\mathrm{C}\ell_K|$ endlich.*

Beweis. Sei $m_0 \in \mathbb{N}$ mit $m_0 \geq M_K |D_K|^{1/2}$. Nach (12.2) ist

$$\mathrm{C}\ell_K = \{[\mathfrak{a}] \mid \mathfrak{a} \text{ ganzes Ideal von } R \text{ mit } \mathrm{N}\mathfrak{a} \leq m_0\}.$$

Ist $\mathfrak{a}$ ein Ideal mit $\mathrm{N}\mathfrak{a} = m \leq m_0$, so ist $mR \subseteq \mathfrak{a}$ (nach dem gruppentheoretischen Satz von Lagrange). Nach (5.7) gibt es nur endliche viele Ideale von R oberhalb mR. Folglich ist $\mathrm{C}\ell_K$ endlich. $\square$

(12.4) **Folgerung** (Hermite–Minkowski). *Ist $K \neq \mathbb{Q}$ ($n > 1$), so ist $D_K \neq \pm 1$. Insbesondere gibt es nach (9.3) eine Primzahl, die in K verzweigt.*

Beweis. Nach (12.2) ist $M_K |D_K|^{1/2} \geq \mathrm{N}\mathfrak{a} \geq 1$ für ein ganzes Ideal $\mathfrak{a}$ (was keine Rolle mehr spielen wird). Also ist $|D_K| \geq \left(\frac{1}{M_K}\right)^2 = \left(\frac{\pi}{4}\right)^{2r_2} \frac{n^{2n}}{(n!)^2} \geq \left(\frac{\pi}{4}\right)^n \cdot \frac{n^n}{(n!)^2}$ (wegen $2r_2 \leq n$ und $\frac{\pi}{4} < 1$). Setze $a_n = \left(\frac{\pi}{4}\right)^n \cdot \frac{n^{2n}}{(n!)^2}$ ($n \geq 2$). Es ist $a_2 = \frac{\pi^2}{4} > 1$ und

$$\frac{a_{n+1}}{a_n} = \frac{\pi}{4}(1 + \frac{1}{n})^{2n} = \frac{\pi}{4}(1 + 2 + \cdots) \geq \frac{3\pi}{4} > 1.$$

Folglich ist $|D_K| \geq \frac{\pi^2}{4}\left(\frac{3\pi}{4}\right)^{n-2} > 1$. $\square$

Mit den beschriebenen Methoden kann man zeigen, dass es nur endlich viele Zahlkörper gibt mit vorgegebener Diskriminante (Hermite). Wir wollen an zwei Beispielen illustrieren, wie man mit (12.2) die Klassenzahl nach oben abschätzen kann.

(12.5) **Beispiel.** Sei α eine Wurzel von $f = X^5 - X + 1$ und $K = \mathbb{Q}(\alpha)$. In (8.6) haben wir gezeigt, dass $\mathrm{Gal}_{\mathbb{Q}}(f) \cong S_5$ ist. Es ist $D_f = 19 \cdot 151$ quadratfrei (Übung 26), daher $R = \mathbb{Z}[\alpha]$ der Ring der ganzen Zahlen von K und $D_K = D_f$ (3.10). Hier ist $n = 5$ und $r_1 = 1$, wie man aus dem reellen Graph der *Parabel* $x \mapsto f(x)$ entnimmt (oder wegen $D_K > 0$). Also ist $r_2 = 2$ und $M_K \approx 0,0625$. Es ist $M_K |D_K|^{1/2} \approx 3,3477$, daher nach (12.2)

$$\mathrm{C}\ell_K = \{[\mathfrak{a}] \mid \mathfrak{a} \text{ ganzes Ideal von } R \text{ mit } \mathrm{N}\mathfrak{a} < 4\}.$$

Solche Ideale $\mathfrak{a} \neq R$ sind allenfalls Primideale $\mathfrak{p}$ mit $\mathrm{N}\mathfrak{p} = 2$ oder 3.

1. Fall: $\mathrm{N}\mathfrak{p} = 2$

Dann ist $R/\mathfrak{p} \cong \mathbb{F}_2$ und $\mathfrak{p} \cap \mathbb{Z} = 2\mathbb{Z}$. Wegen $R = \mathbb{Z}[\alpha]$ müsste $f \bmod 2$ eine Wurzel in $\mathbb{F}_2$ haben. Das ist aber nicht der Fall; ein solches Primideal gibt es also nicht.

2. Fall: $\mathrm{N}\mathfrak{p} = 3$

Dann müsste entsprechend $f \bmod 3$ eine Wurzel in $\mathbb{F}_3$ haben, aber auch dies ist nicht der Fall. Folglich ist $h_K = 1$.

(12.6) **Beispiel.** *Für $K = \mathbb{Q}(\sqrt{-5})$ gilt $h_K = 5$.*

Beweis. Hier ist $n = 2, r_1 = 0, r_2 = 1$, also $M_K \approx 0,63661$. Nach (1.3), (1.4) ist ferner $R = R_K = \mathbb{Z}[\frac{1+\sqrt{-47}}{2}]$ und $D_K = -47$. Wir haben die Abschätzung $M_K|D_K|^{1/2} < 5$. Entsprechend (12.2) sind nur die Ideale von R zu untersuchen mit Norm $2, 3$ oder 4. Nach (1.8) zerfallen die Primzahlen 2 und 3 in K. Es gibt also Primideale $\mathfrak{p}$ mit $\mathrm{N}\mathfrak{p} = 2$ sowie $\mathfrak{q}$ mit $\mathrm{N}\mathfrak{q} = 3$. Die Galois-konjugierten Primideale $\mathfrak{p}'$ und $\mathfrak{q}'$ repräsentieren die inversen Klassen von $\mathfrak{p}$ bzw. $\mathfrak{q}$. Nach (1.10) oder (5.7) sind $\mathfrak{p}^2$, $(\mathfrak{p}')^2$ und $2R = \mathfrak{p}\mathfrak{p}'$ die einzigen Ideale von R mit Norm 4. Es ist daher

$$\mathrm{C}\ell_K = \{1\} \cup \{[\mathfrak{p}], [\mathfrak{p}]^{-1}, [\mathfrak{p}]^2, [\mathfrak{p}]^{-2}, [\mathfrak{q}], [\mathfrak{q}]^{-1}\}.$$

Es ist also $h_K \leq 7$. Wir zeigen, dass $[\mathfrak{p}]$ die Ordnung 5 in $\mathrm{C}\ell_K$ hat. Daraus folgt dann die Behauptung (nach Lagrange).

Sei $x = \frac{a+b\sqrt{-47}}{2}$ ein Element von R ($a, b \in \mathbb{Z}$ mit gleicher Parität). Dann ist $\mathrm{N}_{K|\mathbb{Q}}(x) = \frac{a^2+47b2}{4}$, und wir haben die Normen 0 ($a = b = 0$), 1 ($a = 2, b = 0$), 4 ($a = 4, b = 0$), 9 ($a = 6, b = 0$), 12 ($a = b = 1$), 14 ($a = 3, b = 1$), 16 ($a = 8, b = 0$), 18 ($a = 5, b = 1$), 24 ($a = 7, b = 1$), 32 ($a = 9, b = 1$). Daher ist $\mathfrak{p}$ kein Hauptideal und auch $[\mathfrak{p}]^2 \neq 1$, denn $2R$ ist das einzige Ideal von R mit Norm 4, und $\mathfrak{p} \neq \mathfrak{p}'$. Ferner ist $[\mathfrak{p}]^3 \neq 1$, denn es gibt kein Ideal mit Norm 8, und es ist $[\mathfrak{p}]^4 \neq 1$, da $4R$ das einzige Ideal mit Norm 16 ist. Für

$$\alpha = \frac{3+\sqrt{-47}}{2}$$

gilt $\mathrm{N}_{K|\mathbb{Q}}(\alpha) = 32$. Nach (5.7) ist also $\alpha R = \mathfrak{p}^r(\mathfrak{p}')^s$ mit eindeutig bestimmten natürlichen Zahlen r, s, für welche $r + s = 5$ gilt. Es ist daher $[\alpha R] = [\mathfrak{p}]^{r-s}$ und, wie wir gesehen haben, $|r - s| \geq 5$. Folglich hat $[\mathfrak{p}]$ die Ordnung 5. $\square$

Anhang (Volumenberechnung): Sei $a \in \mathbb{R}_{>0}$ und T_a die (kompakte) Menge aller $(y_i; z_j) \in \mathbb{R}^{(r_1)} \times \mathbb{C}^{(r_2)} = \mathbb{R}^{(n)}$ mit $\sum_{i=1}^{r_1} |y_i| + 2\sum_{j=1}^{r_2} |z_j| \leq a$. Es gilt

$$\mathrm{vol}(\mathrm{T_a}) = \mathrm{V}(\mathrm{r_1}, \mathrm{r_2}; \mathrm{a})) = 2^{\mathrm{r_1}} \left(\tfrac{\pi}{2}\right)^{\mathrm{r_2}} \tfrac{\mathrm{a^n}}{\mathrm{n!}}.$$

Wir führen den Beweis durch Induktion nach r_1 und nach r_2, bei Anwendung von Fubini plus Transformationsformel (Polarkoordinaten). Es ist $V(1, 0; a) = 2a$ und $V(0, 1; a) = \pi\left(\frac{a}{2}\right)^2$. Wir berechnen

$$V(r_1 + 1, r_2; a) = \int_{-a}^{a} V(r_1, r_2; a - |y|)dy = 2\int_0^a 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2} \frac{(a-y)^n}{n!} dy$$

und

$$V(r_1, r_2 + 1; a) = \int_{|z| \leq \frac{a}{2}} V(r_1, r_2; a - 2|z|)dz = \int_0^{2\pi} \int_0^{a/2} V(r_1, r_2; a - 2\rho)\rho \, d\theta \, d\rho.$$

Man verifiziert die Behauptung.

13. Der Dirichletsche Einheitensatz

Voraussetzungen und Bezeichnungen wie in §11, §12 ($[K : \mathbb{Q}] = n = r_1 + 2r_2$, $R = R_K$ etc.). E_K sei die Gruppe der Einheitswurzeln in K, und mit $r = r_1 + r_2$ wird die Anzahl der archimedischen Bewertungen $|\cdot|_i$ von K bezeichnet (11.9).

(13.1) **Definition.** Die *logarithmische Einbettung* $\mathrm{Log} : \mathrm{K}^* \to \mathbb{R}^{(\mathrm{r})}$ wird erklärt durch

$$\mathrm{Log(x)} = \Big(\log|\mathrm{x}|_1, \ldots, \log|\mathrm{x}|_\mathrm{r}\Big).$$

Da $|xy|_i = |x|_i|y|_i$ für alle x, y und alle i gilt, und da der natürliche Logarithmus $\log = \ln : \mathbb{R}^*_{>0} \to \mathbb{R}^+$ ein Homomorphismus ist, ist Log ein Homomorphismus in die additive Gruppe von $\mathbb{R}^{(r)}$. (Log ist nicht injektiv, aber es stellt sich heraus, dass der Kern von $\mathrm{Log}|\mathrm{R}^*$ endlich und gleich E_K ist.)

(13.2) **Lemma.** *Für jede beschränkte Teilmenge T von $\mathbb{R}^{(r)}$ ist die Menge der $x \in R^*$ mit* $\mathrm{Log(x)} \in \mathrm{T}$ *endlich, daher* $\mathrm{Log(R^*)}$ *eine diskrete Untergruppe von $\mathbb{R}^{(r)}$.*

Beweis. Es gibt eine reelle Zahl $c > 1$, so dass $-\ln c \le t_i \le \ln c$ für alle $(t_1, \ldots, t_r) \in T$. Sei $x \in R^*$ mit $\mathrm{Log(x)} \in \mathrm{T}$. Dann gilt

$$\frac{1}{c} \le |x|_i \le c$$

für $i = 1, \ldots, r$. Da x ganz-algebraisch ist, ist $f = m_{\mathbb{Q},x}$ in $\mathbb{Z}[X]$ nach dem Gauß-Lemma. Die Koeffizienten von f sind die elementarsymmetrischen Funktionen in den Konjugierten x^{σ_i}; sie sind daher betragsmäßig beschränkt (gemäß 11.9). Da dies ganze Zahlen sind, haben sie nur endlich viele möglichen Werte. Es gibt also nur endlich viele Minimalpolynome über $\mathbb{Q}$, für welche $x \in R^*$ mit $\mathrm{Log(x)} \in \mathrm{T}$ ist (vgl. mit 2.7). Dies beweist das Lemma. □

(13.3) **Lemma.** $\mathrm{Log(R^*)}$ *liegt in der Hyperebene W von $\mathbb{R}^{(r)}$ aller r-Tupel (y_i) mit $\sum_{i=1}^r y_i = 0$. Der Kern von* $\mathrm{Log}|\mathrm{R}^*$ *ist gerade die (endliche, zyklische) Gruppe E_K der Einheitswurzeln in K, die Torsionsgruppe von R^* (bestehend aus allen Elementen endlicher Ordnung).*

Beweis. Für $x \in R^*$ ist $\prod_{1=1}^r |x|_i = |\mathrm{N}_{K|\mathbb{Q}}(x)| = 1$ nach (7.4), (11.9). Folglich ist $\sum_{i=1}^r \log|x|_i = \log 1 = 0$ und $\mathrm{Log(x)} \in \mathrm{W}$. Nach (13.2) ist der Kern von $\mathrm{Log}|\mathrm{R}^*$ eine *endliche* Untergruppe E von R^*, also zyklisch. (Nach (0.4) gibt es ein Element in E mit einer Ordnung d derart, dass die Ordnung jedes Elements von E ein Teiler von d ist. Das Polynom $X^d - 1$ hat aber höchstens d Wurzeln in K.) Es ist $E = E_K$, denn ist ε eine Einheitswurzel in K, so ist $\varepsilon \in R^*$ und $|\varepsilon|_i = 1$ für alle $i = 1, \ldots, r$. □

Nach (0.3) und (13.2), (13.3) ist damit $R^* \cong E_K \times \mathbb{Z}^{(r'-1)}$ für ein $r' \leq r$, wobei $r' = r$ genau dann gilt, wenn $\mathrm{Log}(\mathrm{R}^*)$ ein Gitter in der Hyperebene W ist. Das ist genau die Aussage des Dirichletschen Einheitensatzes (L. Dirichlet, 1805-1859); vgl. den Spezialfall quadratische Zahlkörper in (1.6).

(13.4) **Hauptsatz** (Dirichlet). *R^* ist modulo E_K eine freie abelsche Gruppe vom Range $r - 1 = r_1 + r_2 - 1$.*

Beweis. Wir haben zu zeigen, dass $\mathrm{Log}(\mathrm{R}^*)$ eine $\mathbb{R}$-Basis von W enthält. Sei $\{w_1, \ldots, w_{r-1}\}$ eine $\mathbb{R}$-Basis von W und $w_r \in \mathbb{R}^{(r)} \setminus W$. Sei $\lambda \neq 0$ eine Linearform mit $w_i^\lambda = l_i w_i$ für reelle Zahlen l_i, wobei $l_r = 0$ sei. Wir beschreiben Log bzgl. dieser $\mathbb{R}$-Basis, d.h., die Werte als r-Tupel bzgl. $\{w_i\}$. Wir haben $u \in R^*$ zu finden mit $\mathrm{Log(u)}^\lambda \neq 0$. Die Idee ist, von 0 verschiedene Elemente $x_k \neq x_{k'}$ in R mit gleicher Norm (bis auf das Vorzeichen) derart zu finden, dass dies für $u = x_k x_{k'}^{-1}$ gilt.

Setze $a = \left(\frac{2}{\pi}\right)^{r_2} |D_K|^{1/2}$ und $b = 1 + \log a \sum_{i=1}^r |l_i|$. (Es wird sich zeigen dass $a \geq 1$ und daher $b > 0$ ist.) Für $k \in \mathbb{N}_{>0}$ wähle ein r-Tupel $t_k = (t_{k1}, \ldots, t_{kr})$ aus positiven reellen Zahlen $t_{ki} > 0$, so dass gilt:

$$\sum_{i=1}^r l_i \log t_{ki} = 2kb \quad \textit{und} \quad \prod_{i=1}^r t_{ki} = a.$$

Dies ist möglich wegen $l_r = 0$. Betrachte nun die Menge

$$T_k = T(a, t_k) = \{(y_i; z_j) \in \mathbb{R}^{(r_1)} \times \mathbb{C}^{(r_2)} \ : \ |y_i| \leq t_{ki} \ ; \ |z_j| \leq \sqrt{t_{k,r_1+j}} \ \}.$$

Dies ist eine kompakte, konvexe Teilmenge von $\mathbb{R}^{(n)} = \mathbb{R}^{(r_1)} \times \mathbb{C}^{(r_2)}$, die symmetrisch bzgl. Null ist, und es ist

$$\mathrm{vol(T_k)} = \prod_{\mathrm{i=1}}^{\mathrm{r_1}} (2\mathrm{t_{ki}}) \prod_{\mathrm{j=r_1+1}}^{\mathrm{r_2}} (\pi \mathrm{t_{kj}}) = 2^{\mathrm{r_1}} \pi^{\mathrm{r_2}} \mathrm{a} = 2^{\mathrm{r}} |\mathrm{D_K}|^{1/2}.$$

Nach (11.7) ist R^σ ein Gitter in $\mathbb{R}^{(n)}$ mit $\mu(R^\sigma) = 2^{-r_2} |D_K|^{1/2}$, somit

$$\mathrm{vol(T_k)} = 2^{\mathrm{n}} \mu(\mathrm{R}^\sigma).$$

Nach (11.4) gibt es daher $0 \neq x_k \in R$ mit $(x_k)^\sigma \in T_k$, also $1 \leq |x_k|_i \leq t_{ki}$ für alle i ($|x|_i \in \mathbb{N}$). Folglich haben wir

$$1 \leq |\mathrm{N}_{K|\mathbb{Q}}(x_k)| = \prod_{i=1}^r |x_k|_i \leq \prod_{i=1}^r t_{ki} = a.$$

Insbesondere ist $a \geq 1$ (und somit $|D_K| \geq \left(\frac{\pi}{2}\right)^{2r_2}$; vgl. mit (12.4)). Für $j = 1, \ldots, r$ gilt weiter

$$a^{-1} t_{kj} = \prod_{i \neq j} t_{ki}^{-1} \leq \prod_{i \neq j} |x_k|_i^{-1} |\mathrm{N}_{K|\mathbb{Q}}(x_k)| = |x_k|_j$$

und somit $0 \leq \log t_{kj} - \log |x_k|_j \leq \log a$. Aufsummieren liefert

$$\left| \sum_{j=1}^{r} l_j \log t_{kj} - \sum_{j=1}^{r} l_j \log |x_k|_j \right| \leq \sum_{j=1}^{r} |l_j| \big(\log t_{kj} - \log |x_k|_j \big) \leq \log a \sum_{j=1}^{r} |l_j|.$$

Nach Definition der Konstanten b ist die rechte Seite dieser Ungleichung $< b$, und auf der linken Seite steht $|2kb - \mathrm{Log}(\mathrm{x_k})^\lambda|$. Für jede natürliche Zahl k haben wir also $x_k \in R$ gefunden mit $1 \leq |\mathrm{N}_{K|\mathbb{Q}}(x_k)| \leq a$ und

$$(2k-1)b < \mathrm{Log}(\mathrm{x_k})^\lambda < (2\mathrm{k}+1)\mathrm{b}.$$

Da die Norm eine ganze Zahl ist, gibt es also $k \neq k'$ mit $|\mathrm{N}(x_k)| = |\mathrm{N}(x_{k'})|$, also $x_k R = x_{k'} R$ und $x_k = u x_{k'}$ mit $u \in R^*$. Es ist $\mathrm{Log}(\mathrm{u})^\lambda = \mathrm{Log}(\mathrm{x_k})^\lambda - \mathrm{Log}(\mathrm{x_{k'}})^\lambda \neq 0$. Damit ist der Satz bewiesen. □

(13.5) **Beispiel.** Sei $L = \mathbb{Q}(\varepsilon_p)$ der p-te Kreisteilungskörper für eine ungerade Primzahl p. Wir haben schon zu (2.7) angemerkt, dass hier $r_1 = 0$ und $n = 2r_2 = p - 1$ ist. In diesem Fall ist $E_L = \langle -\varepsilon_p \rangle$ zyklisch der Ordnung $2p$ und R_L^*/E_L eine freie abelsche Gruppe vom Range $(p-3)/2$.

Für den maximalen total reellen Teilkörper $K = L^+ = \mathbb{Q}(\cos \frac{2\pi}{p})$ gilt $n^+ = r_1^+ = (p-1)/2$ ($r_2^+ = 0$). Hier ist $E_K = \{\pm 1\}$ und R_K^*/E_K frei abelsch von demselben Range $(p-3)/2$. In (2.7) haben wir sogar (Kummer folgend) gezeigt, dass

$$R_L^* = E_L \cdot R_K^* = \langle \varepsilon_p \rangle \cdot R_K^*$$

gilt.

Anmerkung. Ist C die multiplikative Untergruppe von L^* erzeugt durch $-\varepsilon_p$ und den $\varepsilon_p^j - 1$ für $j = 1, \ldots, p-1$, so nennt man $C_L = C \cap R_L^*$ bzw. $C_K = C \cap R_K^*$ die Gruppen der *Kreiseinheiten* in L bzw. K. Schon Kummer hat gesehen, dass die Klassenzahl

$$h_p^+ = h_K = |R_K^* : C_K|$$

ist (Washington, p. 145). Es ist h_p^+ ein Teiler der Klassenzahl $h_p = h_L$ (Washington, p. 40); $h_p^- = h_p / h_p^+$ heißt auch der erste Faktor der Klassenzahl h_p.

§14. Das Newton-Polygon

Sei R ein Dedekindring mit Quotientenkörper K, $\mathrm{char}(K) = 0$, und sei $f \in K[X]$ ein normiertes Polynom vom Grade n mit $f(0) \neq 0$. Aus technischen Gründen (elementarsymmetrische Funktionen) schreiben wir

$$f = a_0 X^n - a_1 X^{n-1} + - \cdots + (-1)^n a_n.$$

Dabei ist also $a_0 = 1$ und $a_n \neq 0$. Sei L *der* Zerfällungskörper von f, $S = R_{L|R}$ und $G = \mathrm{Gal}(L|K)$. Seien $\mathfrak{P}|\mathfrak{p}$ feste Primstellen in $S|R$. Wir setzen voraus, dass $k_\mathfrak{p}$ ein endlicher Körper der Charakteristik p ist. Nach (8.3) hat dann die Trägheitsgruppe $T_\mathfrak{P}$ die Ordnung $e = e(\mathfrak{P}|\mathfrak{p})$. Mit $F = L_{G_\mathfrak{P}}$ wird der Zerlegungskörper von $\mathfrak{P}$ bezeichnet, so dass also $G_\mathfrak{P} = \mathrm{Gal}(L|F)$ ist. Für die Bewertungen schreiben wir $v = v_\mathfrak{p}$ und $w = v_\mathfrak{P}$. Für $x \in K^*$ gilt dann

$$w(x) = e \cdot v(x).$$

Über L sei $f = \prod_{i=1}^n (X - \alpha_i)$, und $W_f = \{\alpha_1, \ldots, \alpha_n\}$ die Wurzelmenge; wir setzen nicht voraus, dass f separabel ist. Für eine rationale Zahl m sei schließlich

$$W_{f,m} = \{\alpha \in W_f \mid w(\alpha) = e \cdot m\}.$$

(14.1) **Definition.** Ordne jedem Monom $\pm a_i X^{n-i} \neq 0$ in f den Punkt $\big(i, v(a_i)\big)$ im euklidischen $\mathbb{R}^{(2)}$ zu. Die untere konvexe Hülle dieser Punkte heißt das *Newton-Polygon* von f bzgl. $v = v_\mathfrak{p}$. Es besteht aus geradlinigen *Seiten* L_m der Längen $\ell > 0$ und Höhen h, deren Steigungen $m = \frac{h}{\ell}$ streng monoton wachsen.

(14.2) **Beispiel.** Sei $K = \mathbb{Q}$ und $\mathfrak{p} = p\mathbb{Z}$, und sei $f = X^5 - \frac{4}{5}X^3 + \frac{10}{3}X + 10$. Interessant sind hier nur die Primzahlen $p = 2, 3, 5$, wo Seiten mit von Null verschiedenen Steigungen auftreten. (Manchmal hilft auch eine geeignete Substitution weiter; man denke an das p-te Kreisteilungspolynom oder an das Polynom $X^3 - 2$ in (9.5).)

p=2: Eine Seite L_m mit Länge $\ell = 5$ und Steigung $m = 1/5$.

p=3: Zwei Seiten: L_{m_1} mit $\ell_1 = 4$ und $m_1 = -1/4$; L_{m_2} mit $\ell_2 = 1$ und $m_2 = 1$.

p=5: Zwei Seiten: L_{m_1} mit $\ell_1 = 2$, $m_1 = -1/2$; L_{m_2} mit $\ell_2 = 3$, $m_2 = \frac{2}{3}$.

(14.3) **Lemma.** *Sei L_m eine Seite des Newton-Polygons von f mit Länge ℓ und Steigung m. Dann hat f genau ℓ Wurzeln $\alpha_{r+1}, \ldots, \alpha_{r+\ell}$ (gezählt mit Vielfachheiten) mit $w(\alpha_{r+j}) = em$, und das Polynom*

$$f_m = \prod_{j=1}^{\ell} (X - \alpha_{r+j})$$

hat die Koeffizienten in $F = L_{G_\mathfrak{P}}$. Ist die rationale Zahl m nicht Steigung einer Seite des Polygons, so ist $W_{f,m} = \varnothing$.

Beweis. Nummeriere die Wurzeln $\alpha_1, \ldots, \alpha_n$ von f so, dass $w(\alpha_i) \leq w(\alpha_j)$ für $i < j$ ist. Nach Vieta gilt für $i = 1, \ldots, n$:

$$a_i = \sum_{1 \leq k_1 < k_2 < \ldots < k_i \leq n} \alpha_{k_1} \alpha_{k_2} \cdots \alpha_{k_i}.$$

Aufgrund der Ultrametrik (6.1) gilt $w(a_i) \geq \min_{1 \leq k_1 < k_2 < \ldots < k_i \leq n} w(\alpha_{k_1} \alpha_{k_2} \cdots \alpha_{k_i}) = w(\alpha_1 \cdots \alpha_i) = w(\alpha_1) + \cdots + w(\alpha_i)$, und es gilt Gleichheit im Falle $w(\alpha_i) < w(\alpha_{i+1})$. Sind also $\alpha_{r+1}, \ldots, \alpha_s$ die sämtlichen Wurzeln von f mit konstantem (ganzzahligen) w-Wert em (etwa), so gilt $w(a_r) = \sum_{i=1}^{r} w(\alpha_i)$ und $w(a_s) = \sum_{i=1}^{s} w(\alpha_i) = w(a_r) + (s-r)em$. Nehmen wir, aufgrund von $w(a_0) = 0$, induktiv $w(a_r) \neq \infty$ an, so ist auch $w(a_s) \neq \infty$ ($a_r a_s \neq 0$). Ist $k \geq r$ mit $a_k \neq 0$, so ist $w(a_k) - w(a_r) \geq w(\alpha_{r+1}) + \cdots + w(\alpha_k) \geq (k-r)em$, und echt größer für $k > s$. Ist $k < r$ mit $a_k \neq 0$, so ist $w(a_r) - w(a_k) \leq w(\alpha_{k+1}) + \cdots + w(\alpha_r) < (r-k)em$, und $(k, v(a_k))$ liegt echt oberhalb der Graden durch $(r, v(a_r))$ und $(s, v(a_s))$. Die Verbindungsstrecke ist also eine Seite des Newton-Polygons mit Länge $\ell = s - r$ und Steigung

$$m = \frac{v(a_s) - v(a_r)}{s - r} = \frac{1}{e} \frac{w(a_s) - w(a_r)}{s - r}.$$

Für jedes $\sigma \in G$ und jedes $y \in L^*$ gilt $v_{\mathfrak{P}^\sigma}(y^\sigma) = v_{\mathfrak{P}}(y)$. Für $\sigma \in G_{\mathfrak{P}}$ gilt also $w(y^\sigma) = w(y)$. Die Wurzeln der Primfaktoren von f_m, damit von f_m selbst, werden also von $G_{\mathfrak{P}}$ permutiert. Ihre Koeffizienten sind daher einzeln fest unter der Zerlegungsgruppe $G_{\mathfrak{P}}$ und liegen daher in dessen Fixkörper F. $\square$

(14.4) **Hauptsatz.** *Sind $m_1 < \cdots < m_t$ die Steigungen der verschiedenen Seiten des Newton-Polygons von f bzgl. $\mathfrak{p}$, so ist $W_f = \biguplus_{i=1}^{t} W_{f,m_i}$ eine Zerlegung in nichtleere $G_{\mathfrak{P}}$-invariante Teilmengen. Sei $m = m_i$ für ein i, und sei L_m die Seite mit Steigung $m = \frac{h}{\ell} = \frac{h_m}{e_m}$, wobei ℓ die Länge von L_m und h_m, e_m teilerfremde ganze Zahlen sind, $e_m > 0$. Sei ferner $\mathfrak{P}_F = \mathfrak{P} \cap F$ und $\alpha \in W_{f,m}$ eine Wurzel von f_m (siehe 14.3).*

(a) *Der Verzweigungsindex von $\mathfrak{P} \cap F(\alpha)$ über $\mathfrak{P}_F$ ist durch e_m teilbar; insbesondere ist $|T_{\mathfrak{P}}| = e$ durch e_m teilbar.*

(b) *Ist $\ell = e_m$, d.h., $\mathrm{ggT}(\ell, \mathrm{h}) = 1$, so ist f_m irreduzibel über F (und damit separabel) vom Grade e_m, daher $\mathfrak{P}_F$ total verzweigt in $F(\alpha)$.*

Beweis. Das Polynom f_m hat die Koeffizienten in $F = L_{G_{\mathfrak{P}}}$ nach (14.3). Damit ist W_{f_m} invariant unter $G_{\mathfrak{P}}$, und die ersten Aussagen folgen. Setze $\mathfrak{q} = \mathfrak{P} \cap F(\alpha)$. Nach (8.4) ist $e(\mathfrak{P}_F|\mathfrak{p}) = 1$. Daher ist nach (7.3) $e = e(\mathfrak{P}|\mathfrak{q}) \cdot e(\mathfrak{q}|\mathfrak{P}_F)$ und

$$v_{\mathfrak{q}}(\alpha) = \frac{1}{e(\mathfrak{P}|\mathfrak{q})} w(\alpha) = \frac{em}{e(\mathfrak{P}|\mathfrak{q})} = e(\mathfrak{q}|\mathfrak{P}_F) \cdot m = \frac{e(\mathfrak{q}|\mathfrak{P}_F)}{e_m} h_m.$$

Da $v_{\mathfrak{q}}(\alpha)$ eine ganze Zahl ist, ist e_m ein Teiler von $e(\mathfrak{q}|\mathfrak{P}_F)$, und dies wiederum ist ein Teiler von e.

Sei nun $\ell = e_m$ vorausgesetzt. Nach Konstruktion, und wegen $e(\mathfrak{P}_F|\mathfrak{p}) = 1$, besteht das Newton-Polygon von f_m bzgl. $v_{\mathfrak{P}_F}$ aus einer Seite der Länge $\ell = \mathrm{grd}(\mathrm{f_m})$ und Steigung m. Für jeden (normierten) Primfaktor g von f_m über F haben wir entsprechend ein Newton-Polygon mit einer Seite der Länge grd(g) und derselben Steigung m. Da ℓ teilerfremd zur Höhe h ist, folgt $\mathrm{grd(g)} = \mathrm{grd(f_m)}$ und $f_m = g$. Damit ist $\ell = \mathrm{grd(f_m)} = [\mathrm{F}(\alpha) : \mathrm{F}]$. Nach (7.5) ist sicherlich $e(\mathfrak{q}|\mathfrak{P}_F) \leq [F(\alpha) : F]$. Da $\frac{e(\mathfrak{q}|\mathfrak{P}_F)}{\ell} h_m$ eine ganze Zahl ist, und ℓ teilerfremd zu $h_m = h$, ist $e(\mathfrak{q}|\mathfrak{P}_F) = [F(\alpha) : F]$. $\square$

(14.5) **Beispiel.** Sei $v(a_i) \geq 1$ für $i = 1, \ldots, n$ aber $v(a_n) = 1$, d.h., $f \in R_{\mathfrak{p}}[X]$ ist ein Eisenstein-Polynom bzgl. $\mathfrak{p}$ (oder $\mathfrak{p}R_{\mathfrak{p}}$). Das Newton-Polygon besteht dann aus einer Seite der Länge n und Höhe 1, also mit Steigung $m = 1/n$. Nach (14.4) ist daher $f = f_m$ irreduzibel über K (sogar über dem Trägheitskörper von $\mathfrak{P}$). Es verzweigt $\mathfrak{p}$ total in $K(\alpha)$ für jeds $\alpha \in W_f$ (vgl. 8.9).

Wie könnte eine Verallgemeinerung des Eisensteinschen Irreduzibilitätskriterium Kriteriums aussehen ?

(14.6) **Beispiel.** Sei $K = \mathbb{Q}$ und $f = X^5 - \frac{4}{5}X^3 + \frac{10}{3}X + 10$; vgl. (15.2). Hier ist $n = 5$ und f ein Eisenstein-Polynom bzgl. $p = 2$. Insbesondere ist f irreduzibel über $\mathbb{Q}$ und daher $G = \mathrm{Gal}_{\mathbb{Q}}(f)$ transitiv auf W_f.

Im Falle $p = 3$ hat die erste Seite des Newton-Polygons die Länge 4 und Steigung $m = -1/4$. Nach (14.4) ist $|T_{\mathfrak{P}}|$ daher durch 4 teilbar. (Eine genauere Betrachtung zeigt, dass $T_{\mathfrak{P}}$ zyklisch der Ordnung 4 und $G_{\mathfrak{P}}$ eine Diedergruppe der Ordnung 8 ist; siehe §15.)

Sei $p = 5$. Nach (14.2) hat das Newton-Polygon von f zwei Seiten. Die erste Seite hat die Länge 2 und Steigung $-1/2$, die zweite die Länge 3 und Steigung $2/3$. Nach (14.4) operiert $T_{\mathfrak{P}}$ auf den 5 Wurzeln von f daher in zwei Bahnen der Längen 2 und 3. (Hier kann man mit den Resultaten aus §15 zeigen, dass $T_{\mathfrak{P}}$ zyklisch der Ordnung 6 und $G_{\mathfrak{P}} \cong S_2 \times S_3$ ist.)

In jedem Falle ist G transitiv auf W_f und enthält eine Transposition. Nach Jordan (8.7) ist $G \cong S_5$.

Problem: Sei p eine Primzahl und a eine ganze Zahl, die durch p aber nicht p^2 teilbar ist. Sei $f = X^p + aX + a$ und $G = \mathrm{Gal}_{\mathbb{Q}}(f)$. Man sieht sofort, dass für $p = 2, 3$ dieses Eisenstein-Polynom bzgl. p die Gruppe $G \cong S_p$ hat. Die (noch unbewiesene) Vermutung ist, dass dies immer so ist. Für $p = 5$ hat dies Ludwig Gauckler in seiner Diplomarbeit gezeigt (siehe *Arch. Math.* **90** (2008), 136-139). Viele Spezialfälle (etwa wenn $a \leq p$ oder $a \equiv 2 \pmod 3$) konnten von Michael Kölle in seiner Doktorarbeit behandelt werden (siehe *Acta Arithm.* **115** (2004), 71-84). Das Newton-Polygon spielt jeweils eine wichtige Rolle bei diesen Untersuchungen.

§15. Verzweigungsgruppen

Wie in §8 sei R ein Dedekindring mit Quotientenkörper K und $L|K$ eine endliche Galoiserweiterung mit Gruppe $G = \mathrm{Gal}(L|K)$. Ferner seien $S = R_{L|R}$ der ganze Abschluss von R in L und $\mathfrak{P}|\mathfrak{p}$ feste Primstellen (Verzweigungsindex e). Wir setzen voraus, das $k_\mathfrak{P}|k_\mathfrak{p}$ separabel ist (etwa $k_\mathfrak{p}$ endlich). Nach (8.3) hat dann die Trägheitsgruppe $T_\mathfrak{P}$ die Ordnung e. Ferner ist $G_\mathfrak{P}/T_\mathfrak{P} \cong \mathrm{Gal}(k_\mathfrak{P}|k_\mathfrak{p})$.

(15.1) **Definition.** Für jede natürliche Zahl s definiere die s-te *Verzweigungsgruppe* von $\mathfrak{P}$ durch

$$G_\mathfrak{P}^{(s)} = \{\sigma \in G_\mathfrak{P} |\ x^\sigma \equiv x \,(\mathrm{mod}\, \mathfrak{P}^{s+1}) \text{ für alle } x \in S\}.$$

$G_\mathfrak{P}^{(s)}$ ist der Kern der Operation von $G_\mathfrak{P}$ auf $S/\mathfrak{P}^{s+1}$ und daher ein Normalteiler von $G_\mathfrak{P}$. Offenbar ist $G_\mathfrak{P}^{(0)} = T_\mathfrak{P}$ die Trägheitsgruppe.

(15.2) **Hauptsatz** (Hilbert). *$G_\mathfrak{P}^{(0)}/G_\mathfrak{P}^{(1)} = \langle \tau\ G_\mathfrak{P}^{(1)} \rangle$ ist zyklisch, nämlich isomorph zu einer Untergruppe von $k_\mathfrak{P}^*$. Ferner gilt:*

(a) *Ist* $\mathrm{char}(k_\mathfrak{p})$ *kein Teiler von e ("zahme Verzweigung"), so ist $G_\mathfrak{P}^{(1)} = 1$ und, falls $k_\mathfrak{p}$ ein endlicher Körper ist , $G_\mathfrak{P} = \langle \sigma, \tau \rangle$ eine metazyklische Gruppe mit $\sigma^{-1}\tau\sigma = \tau^{\mathrm{N}\mathfrak{p}}$.*

(b) *Ist* $\mathrm{char}(k_\mathfrak{p})$ *ein Teiler von e, also* $\mathrm{char}(k_\mathfrak{p}) = p$ *eine Primzahl mit $p \mid e$ ("wilde Verzweigung"), so ist $G_\mathfrak{P}^{(0)}/G_\mathfrak{P}^{(1)}$ eine zyklische p'-Gruppe und $G_\mathfrak{P}^{(1)} \neq 1$ eine p-Gruppe. Für jedes $s \geq 1$ ist $G_\mathfrak{P}^{(s)}/G_\mathfrak{P}^{(s+1)}$ isomorph zu einer Untergruppe von $k_\mathfrak{P}^+$, und es gibt eine Nummer t, für welche $G_\mathfrak{P}^{(t)} = 1$ ist.*

Beweis. Die Aussagen das Satzes betreffen (vordergründig) nur die Struktur der Trägheitsgruppe. Durch Übergang von K zum Trägheitskörper von $\mathfrak{P}$ können wir also nach (8.4) annehmen, dass $\mathfrak{p}$ in L total verzweigt ($G = T_\mathfrak{P} = G_\mathfrak{P}^{(0)}$). Ferner können wir zur Lokalisierung bei $\mathfrak{p}$ übergehen; die Struktur der Verzweigungsgruppen wird dadurch nicht berührt. Sei also auch $R = R_\mathfrak{p}$ und $S = S_\mathfrak{p}$. Dann ist nach (7.9) $S = R[\pi]$ monogen. Daher liegt ein Element $\sigma \in G$ genau dann in $G^{(s)}$, wenn

$$v_\mathfrak{P}(\pi^\sigma - \pi) \geq s + 1$$

ist. Für $t \geq \max_{1 \neq \sigma \in G}\big(v_\mathfrak{P}(\pi^\sigma - \pi)\big)$ ist also $G^{(t)} = 1$. Wir können die obige Relation auch beschreiben durch $\frac{\pi^\sigma}{\pi} \equiv 1 \,(\mathrm{mod}\, \pi^s)$. Mit anderen Worten, setzt man wie in (6.6) $U^{(0)} = S^*$ und $U^{(s)} = 1 + \pi^s S$ für $s > 0$ (Einseinheitengruppe), so ist $\sigma \in G^{(s)}$ genau dann, wenn $\frac{\pi^\sigma}{\pi} \in U^{(s)}$ ist ($s \geq 0$). Ist $u\pi$ ein anderes Primelement von S ($u \in U^{(0)}$), so ist $u^\sigma \equiv u \,(\mathrm{mod}\, \pi^{s+1})$ und daher

$$\frac{u^\sigma \pi^\sigma}{u\pi} \equiv \frac{\pi^s}{\pi} \,(\mathrm{mod}\, U^{(s+1)}).$$

Die Zuordnung $\sigma \mapsto \frac{\pi^\sigma}{\pi} \bmod U^{(s+1)}$ ist also, unabhängig von der Wahl des Primelements, eine Abbildung $\lambda_s : G^{(s)} \to U^{(s)}/U^{(s+1)}$. Wir zeigen, dass λ_s ein Homomorphismus von Gruppen ist. Für $\sigma, \tau \in G^{(s)}$, und $u = \frac{\pi^\tau}{\pi} \in U^{(s)}$, gilt

$$\frac{\pi^{\sigma\tau}}{\pi} = \frac{\pi^\sigma}{\pi}\frac{\pi^\tau}{\pi}\frac{u^\tau}{u} \equiv \frac{\pi^\sigma}{\pi}\frac{\pi^\tau}{\pi} \,(\bmod U^{(s+1)}).$$

Also ist λ_s ein Homomorphismus, mit Kern $G^{(s+1)}$. Nach (6.6) ist $U^{(0)}/U^{(1)} \cong k_\mathfrak{P}^*$ und $U^{(s)}/U^{(s+1)} \cong k_\mathfrak{P}^+$ für $s \geq 1$.

Damit ergeben sich alle Aussagen des Satzes bis auf die Zusatzbehauptung in (a). Sei also $G_\mathfrak{P}^{(1)} = 1$ und $k_\mathfrak{p}$ ein endlicher Körper, etwa der Charakteristik p. Dann wird $\mathrm{Gal}(k_\mathfrak{P}|k_\mathfrak{p})$ erzeugt durch den Frobenius-Automorphismus (Potenzierung mit $\mathrm{N}\mathfrak{p} = |k_\mathfrak{p}|$). Sei $\sigma \in G_\mathfrak{P}$ ein Urbild dieses Automorphismus'. Die Trägheitsgruppe $G_\mathfrak{P}^{(0)} = \langle\tau\rangle$ ist eine zyklische p'-Gruppe (isomorph zu einer Untergruppe von $k_\mathfrak{P}^*$) und ein Normalteiler der Zerlegungsgruppe. Die Konjugierte $\tau^\sigma = \sigma^{-1}\tau\sigma$ liegt also in $G_\mathfrak{P}^{(0)}$. Wir benutzen nun, dass $\lambda_0 : G^{(0)} \to U^{(0)}/U^{(1)} \cong k_\mathfrak{P}^*$ ein injektiver Gruppenhomorphismus ist, der nicht von der Wahl des Primelements π abhängt, und dass σ auf $k_\mathfrak{P}^*$ die Potenzierung mit $\mathrm{N}\mathfrak{p}$ induziert. Da auch $\pi^{\sigma^{-1}}$ ein Primelement ist, erhalten wir

$$\lambda_0(\tau^\sigma) \equiv \Big(\frac{(\pi^{\sigma^{-1}})^\tau}{\pi^{\sigma^{-1}}}\Big)^\sigma \equiv \Big(\frac{\pi^\tau}{\pi}\Big)^\sigma \equiv \lambda_0(\tau)^\sigma \,(\bmod U^{(1)}).$$

Also gilt $\tau^\sigma = \tau^{\mathrm{N}\mathfrak{p}}$, wie behauptet. □

(15.3) **Folgerung.** *Ist $k_\mathfrak{p}$ ein endlicher Körper, so ist $G_\mathfrak{P}$ auflösbar.*

Beweis. In diesem Fall sind $G_\mathfrak{P}/T_\mathfrak{P}$ und $T_\mathfrak{P}/G_\mathfrak{P}^{(1)}$ zyklisch. Ferner ist $G_\mathfrak{P}^{(1)}$ eine normale p-Sylowgruppe von $G_\mathfrak{P}$, wobei $\mathrm{char}(k_\mathfrak{p}) = p$ ist. □

(15.4) **Satz.** *Sei F ein Zwischenkörper von $L|K$ und $H = \mathrm{Gal}(L|F)$. Dann ist $H_\mathfrak{P}^{(s)} = H \cap G_\mathfrak{P}^{(s)}$ für alle s. Ist $F|K$ normal, so werden die Verzweigungsgruppen von $\mathfrak{P}$ auf die von $\mathfrak{p} = \mathfrak{P} \cap F$ abgebildet, doch die Nummerierung ändert sich.*

Beweis. Dies folgt direkt aus der Definition. □

Für die Beschreibung der Verzweigungsgruppen $(G/H)_\mathfrak{p}^{(t)}$ in Relation zu $G_\mathfrak{P}^{(s)}$ vergleiche man Neukirch (S. 189) oder Serre (p. 81).

(15.5) **Galoishülle.** Wir nehmen nun an, dass L der Zerfällungskörper eines irreduziblen und separablen Polynoms $f \in K[X]$ ist. Wir setzen ferner voraus, dass die Charakteristik $\mathrm{char}(k_\mathfrak{p}) = p$ eine Primzahl ist. Mit W_f wird die Menge der Wurzeln von f (in L) bezeichnet. Für festes (aber beliebiges) $\alpha \in W_f$ sei $F = K(\alpha)$, $A = F \cap S$ und

$$\mathfrak{p}A = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$$

die Zerlegung von $\mathfrak{p}$ in F; setze noch (ausnahmsweise) $d_i = f(\mathfrak{q}_i|\mathfrak{p})$. Das Primideal $\mathfrak{q}_i$ heißt *zahm* verzweigt über $\mathfrak{p}$, falls $p \nmid e_i$ gilt (sonst *wild*). Gilt $p \nmid e_i$ für alle $i = 1, \ldots, r$, so heißt $\mathfrak{p}$ zahm verzweigt in F.

(15.6) **Hauptsatz** (van der Waerden). *Sei L die Galoishülle der separablen Erweiterung $F|K$. Mit obigen Bezeichnungen gilt:*

(a) *$G_\mathfrak{P}$ hat auf W_f genau r Bahnen W_i, und $|W_i| = e_i d_i$ $(1 \le i \le r)$.*

(b) *$T_\mathfrak{P}$ hat auf W_i genau d_i Bahnen, jede von der Länge e_i $(1 \le i \le r)$.*

(c) *$G_\mathfrak{P}^{(1)}$ hat auf W_i lauter Bahnen der gleichen Länge $(e_i)_p = p^{v_p(e_i)}$ $(1 \le i \le r)$.*

Beweis. Da f irreduzibel über K ist, ist G transitiv auf W_f und daher diese Wirkung isomorph zu der von G auf der Menge der Rechtsnebenklassen nach dem Punktstabilisator $G_\alpha = \mathrm{Gal}(L|F)$. Nach (8.1) operiert G auch transitiv auf den Primidealen von S über $\mathfrak{p}$. Für jedes $\sigma \in G$ ist $\mathfrak{P}^\sigma \cap F$ eines der Primideale $\mathfrak{q}_i$ (über $\mathfrak{p} = \mathfrak{p}^\sigma$). Wähle $\sigma_i \in G$ derart, dass $\mathfrak{P}^{\sigma_i^{-1}}|\mathfrak{q}_i$ ist $(1 \le i \le r)$.

Die $G_\mathfrak{P}$-Bahnen W_i entsprechen den verschiedenen (paarweise disjunkten) Doppelnebenklassen $G_\alpha \sigma_i G_\mathfrak{P}$, d.h., es ist $W_i = \{\alpha^{\sigma_i \tau} \mid \tau \in G_\mathfrak{P}\}$. Der Bahn W_i korrespondiert die G_α-Bahn $(G_\mathfrak{P}^{\sigma_i^{-1}})^{G_\alpha}$ der Primideale von S über $\mathfrak{q}_i$. (Invertiere die Doppelnebenklasse.) Es ist

$$\big((G_\mathfrak{P})_{\alpha^{\sigma_i}}\big)^{\sigma_i^{-1}} = \big(G_\alpha\big)_{\mathfrak{P}^{\sigma_i^{-1}}}.$$

Nach (8.3) ist $|G_\mathfrak{P}| = ed$, wobei (ausnahmsweise) $d = f(\mathfrak{P}|\mathfrak{p})$ gesetzt ist, und ebenso $|(G_\alpha)_{\mathfrak{P}^{\sigma_i^{-1}}}| = e_i' d_i'$, wobei $e_i' = e(\mathfrak{P}^{\sigma_i^{-1}}|\mathfrak{q}_i)$ und $d_i' = f(\mathfrak{P}^{\sigma_i^{-1}}|\mathfrak{q}_i)$ ist. Nach der Bahnformel ist also

$$|W_i| = |G_\mathfrak{P} : (G_\mathfrak{P})_{\alpha^{\sigma_i}}| = \frac{|G_\mathfrak{P}|}{|(G_\mathfrak{P})_{a^{\sigma_i}}|} = \frac{ed}{e_i' d_i'} = e_i f_i,$$

denn es ist $e = e_i e_i'$ und $d = d_i d_i'$ (Transitivität).

Da $T_\mathfrak{P}$ ein Normalteiler von $G_\mathfrak{P}$ ist, haben alle $T_\mathfrak{P}$-Bahnen auf W_i dieselbe Länge, und eine analoge Rechnung zeigt, dass diese Länge $|T_\mathfrak{P} : (T_\mathfrak{P})_{\alpha^{\sigma_i}}| = \frac{e}{e_i'} = e_i$ ist. Nach (15.2) ist $G_\mathfrak{P}^{(1)}$ ein Normalteiler von $G_\mathfrak{P}$ und eine (normale) p-Sylowgruppe von $T_\mathfrak{P}$, hat daher auf W_i lauter Bahnen gleicher Länge, und zwar gleich der größten p-Potenz, die in e_i aufgeht. $\square$

(15.7) **Folgerung.** *Ist $\mathfrak{p}$ unverzweigt (zahm verzweigt; total zerfallend) in F, so auch in L.*

Beweis. Ist $\mathfrak{p}$ unverzweigt in F, so sind alle $e_i = 1$ and daher $T_{\mathfrak{P}}$ trivial auf W_f und somit $T_{\mathfrak{P}} = 1$. Ist $\mathfrak{p}$ zahm verzweigt in F, so ist $G_{\mathfrak{P}}^{(1)}$ trivial auf W_f und daher $G_{\mathfrak{P}}^{(1)} = 1$. Gilt schließlich $e_i f_i = 1$ für alle i, so ist $G_{\mathfrak{P}} = 1$. $\square$

(15.8) **Folgerung.** *Sei $F = L_{G_{\mathfrak{P}}}$ der Zerlegungskörper von $\mathfrak{P}$ und $\mathfrak{P}_F = \mathfrak{P} \cap F$. Sei $\{\alpha_i = \alpha^{\sigma_i}\}_{1 \le i \le r}$ ein Repräsentantensystem für die $G_{\mathfrak{P}}$-Bahnen auf W_f, und sei $F_i = F(\alpha_i)$ und $\mathfrak{q}_i' = \mathfrak{P} \cap F_i$. Dann ist $F_i|F$ eine Erweiterung vom Grade $e_i d_i$, in welcher $e(\mathfrak{q}_i'|\mathfrak{P}_F) = e_i$ und $f(\mathfrak{q}_i'|\mathfrak{P}_F) = d_i$ ist ($1 \le i \le r$). Ist $k_{\mathfrak{P}}|k_{\mathfrak{p}}$ abelsch (zyklisch, etwa wenn $k_{\mathfrak{p}}$ endlich), so gibt es einen eindeutig bestimmte größten Zwischenkörper E_i, in welchem $\mathfrak{P}_F$ unverzweigt ist; dieser ist normal (abelsch; zyklisch) über F vom Grade d_i.*

Beweis. Sei $E = L_{T_{\mathfrak{P}}}$ der Trägheitskörper von $\mathfrak{P}$. Die Wurzeln von m_{F,α_i} in L bilden gerade die $G_{\mathfrak{P}}$-Bahn, die α_i enthält. Ist $G_{\mathfrak{P}}/T_{\mathfrak{P}}$ abelsch (zyklisch), d.h., $E|F$ abelsch (zyklisch), so ist $E_i = F_i \cap E$ normal über F mit abelscher (zyklischer) Gruppe. Es ist $[F_i : E_i] = e_i$, denn die Wurzeln von m_{E,α_i} bilden eine $T_{\mathfrak{P}}$-Bahn auf W_f. $\square$

Wir können also (theoretisch) die Zerlegung von $\mathfrak{p}$ in F studieren durch Übergang zu den einzelnen Erweiterungen $F_i|F$, wo die Zerlegungszahl 1 ist. Ist insbesondere $k_{\mathfrak{p}}$ endlich, so können wir den Verzweigungsindex e_i jedes Primideals $\mathfrak{q}_i$ in einer total verzweigten Erweiterung $F_i|E_i$ berechnen. (Dies entspricht dem Übergang zum lokalen $\mathfrak{p}$-adischen Körper.)

(15.9) **Beispiel.** Sei $R = \mathbb{Z}$ und $F = \mathbb{Q}(\alpha)$, wo α Wurzel des Polynoms $f = X^3 - 2$ ist. Sei L der Zerfällungskörper von f. Hier ist $G \cong S_3$. Nach (9.5) verzweigen die Primzahlen 2 und 3 total in F. (In der Notation von (15.5) also $r = 1$, $e_1 = 3$, $d_1 = 1$.) Nach (15.6) ist die Trägheitsgruppe $T_{\mathfrak{P}}$ transitiv auf W_f für $\mathfrak{P}$ in L über 2 oder 3.

Für $p = 2$ ist $G_{\mathfrak{P}}^{(1)} = 1$ und daher $T_{\mathfrak{P}} \cong A_3$ nach (15.2). Der Fixkörper der Trägheitsgruppe ist der 3-te Kreisteilungskörper $\mathbb{Q}(\sqrt{-3})$, in welchem 2 nach (1.8) träge ist. Also ist $G_{\mathfrak{P}} = G$.

Für $p = 3$ ist $G_{\mathfrak{P}}^{(1)} \cong A_3$ nach (15.6) und (15.2) (transitive 3-Gruppe). Es verzweigt 3 in $\mathbb{Q}(\sqrt{-3})$ (Verzweigungsindex 2). Also ist in diesem Falle $e = 3 \cdot 2 = 6$ und $T_{\mathfrak{P}} = G$.

§16. Differente und Hilbertformel

Sei R ein Dedekindring mit Quotientenkörper K und $L|K$ eine endliche separable Erweiterung vom Grade n, $S = R_{L|R}$ der ganze Abschluss. Wir halten ferner Primstellen $\mathfrak{P}|\mathfrak{p}$ in $S|R$ fest. Es sei $k_\mathfrak{p} = R/\mathfrak{p}$ ein endlicher Körper der Charakteristik p.

(16.1) **Definition.** $\widehat{S} = \{x \in L \mid \mathrm{Tr}_{L|K}(xS) \subseteq R\}$ heißt der *Komplementärmodul* zu $S|R$. Nach (3.7) ist $\widehat{S} \supseteq S$, und nach (3.8) ist $\widehat{S}$ ein S-Modul, der zwischen zwei freie R-Moduln vom Range n *eingeklemmt* werden kann. Es ist also sicherlich $\widehat{B}$ ein gebrochenes Ideal von B. Das dazu inverse *ganze* Ideal

$$\Delta_{S|R} = \widehat{S}^{-1}$$

heißt die *Differente* von $S|R$. Natürlich ist $\Delta_{S|R}^{-1} = \widehat{S}$.

(16.2) **Lemma** (Transitivität). *Ist F ein Zwischenkörper von $L|K$ und $A = F \cap S$, so ist $\Delta_{S|R} = \big(\Delta_{A|R}S\big)\Delta_{S|A} = \Delta_{A|R}\Delta_{S|A}$.*

Beweis. Für ein gebrochenes Ideal $\mathfrak{b}$ von S gilt

$$\mathfrak{b} \subseteq \Delta_{S|A}^{-1} \iff \mathrm{Tr}_{L|F}(\mathfrak{b}) \subseteq A \iff \Delta_{A|R}^{-1} \cdot \mathrm{Tr}_{L|F}(\mathfrak{b}) \subseteq \Delta_{A|R}^{-1}.$$

Dies ist wiederum äquivalent zu $\mathrm{Tr}_{F|K}\big(\Delta_{A|R}^{-1}\mathrm{Tr}_{L|F}(\mathfrak{b})\big) \subseteq R$, und dies können wir schreiben:

$$\mathrm{Tr}_{F|K}\big(\mathrm{Tr}_{L|F}(\Delta_{A|R}^{-1}\mathfrak{b})\big) = \mathrm{Tr}_{L|K}(\Delta_{A|R}^{-1}\mathfrak{b}) \subseteq R.$$

Dies ist gleichwertig mit $\Delta_{A|R}^{-1}\mathfrak{b} \subseteq \Delta_{S|R}^{-1} \iff \mathfrak{b} \subseteq \Delta_{A|R}\Delta_{S|R}^{-1}$. □

(16.3) **Lemma.** $(\Delta_{S|R})_\mathfrak{p} = \Delta_{S_\mathfrak{p}|R_\mathfrak{p}}$.

Beweis. Dies ist trivial. □

(16.4) **Satz.** *Ist $S = R[\pi]$ ein monogener Ring und $f = m_{K,\pi}$, so ist $\Delta_{S|R} = f'(\pi)S$.*

Beweis. Sei $\{z_j\}_{j=0}^{n-1}$ die K-Basis von L dual zu $\{1, \pi, \ldots, \pi^{n-1}\}$ bzgl. der Spurform $\mathrm{Tr} = \mathrm{Tr}_{L|K}$. Es ist $\mathrm{Tr}(Rz_jS) = R\mathrm{Tr}(z_j\pi^j) = R$, daher $z_jR \subseteq \widehat{S}$ für alle j. Ist umgekehrt $y \in \widehat{S}$, etwa $y = c_0z_0 + c_1z_1 + \ldots + c_{n-1}z_{n-1}$ ($c_j \in K$), so ist $c_i = \mathrm{Tr}(y \cdot \pi^i) \in R$ für alle i. Damit ist $\widehat{S} = Rz_0 \oplus \ldots \oplus Rz_{n-1}$ gezeigt.

Wir berechnen nun die z_j und zeigen $z_j = \frac{b_j}{f'(\pi)}$ für gewisse $b_j \in S$. Sei $f = X^n + a_{n-1}X^{n-1} + \ldots + a_0$, und seien $\pi = \pi_1, \pi_2, \ldots, \pi_n$ die Wurzeln von f (in einem Zerfällungskörper). Wir bestimmen die b_j durch Division in $S[X]$:

$$\frac{f(X)}{X - \pi} = b_{n-1}X^{n-1} + b_{n-2}X^{n-2} + \ldots + b_0.$$

Es ist dann $b_{n-1} = 1$, $b_{n-2} - \pi b_{n-1} = a_{n-1}$, $b_{n-3} - \pi b_{n-2} = a_{n-2}$, ..., $\pi b_0 = a_0$. Folglich bilden die so (rekursiv) bestimmten b_j ebenso wie die Potenzen π^j eine R-Basis von S. Wir haben $\mathrm{Tr}(b_j \frac{\pi^i}{f'(\pi)}) = \delta_{ij}$ nachzuweisen.

Für jedes $0 \le r \le n-1$ gilt

$$\sum_{i=1}^{n} \frac{f(X)}{X - \pi_i} \cdot \frac{\pi_i^r}{f'(\pi_i)} = X^r,$$

denn die Differenz der Polynome auf den beiden Seiten hat wegen $f'(\pi_i) = \prod_{j \neq i}(\pi_i - \pi_j)$ die n Wurzeln $\pi_1, \ldots, \pi_n$ aber höchstens den Grad $n-1$. Definiert man nun die Spur eines Polynoms durch Anwendung auf die Koeffizienten, so gilt also

$$\mathrm{Tr}\Big(\frac{f(X)}{X - \pi} \cdot \frac{X^r}{f'(\pi)}\Big) = X^r \quad (0 \le r \le n-1).$$

Durch Betrachten des Koeffizienten von X^r erhält man die Behauptung. □

(16.5) **Satz.** $\mathrm{N}_{L|K}(\Delta_{S|R}) = D_{S|R}$.

Beweis. Nach (5.7), (16.3) können wir lokalisieren und $R = R_{\mathfrak{p}}$, $S = S_{\mathfrak{p}}$ annehmen. Nach (6.7) sind dann R und S Hauptidealringe, und es gibt eine R-Basis $\{v_i\}$ von S. Sei $\widehat{S} = \beta S$. Die duale Basis $\{v_i^*\}$ bzgl. der Spur $\mathrm{Tr} = \mathrm{Tr}_{L|K}$ ist eine R-Basis von $\widehat{S}$, und es gilt $D_{L|K}(v_1^*, \ldots, v_n^*) = D_{L|K}(v_1, \ldots, v_n)^{-1} = D_{S|R}^{-1}$. Daher folgt

$$D_{S|R}^{-1} = D_{L|K}(\beta v_1, \ldots, \beta v_n) = \mathrm{N}_{L|K}(\beta)^2 D_{S|R}.$$

Damit ist $\mathrm{N}_{L|K}(\Delta_{S|R})^2 = \mathrm{N}_{L|K}(\widehat{S})^{-2} = \mathrm{N}_{L|K}(\beta)^{-2} R = D_{S|R}^2$, und die Behauptung folgt aus (7.5). □

(16.6) **Satz.** *Das Primideal $\mathfrak{P}$ von S ist genau dann verzweigt über R (d.h., über $\mathfrak{p} = \mathfrak{P} \cap R$), wenn $\mathfrak{P} \supseteq \Delta_{S|R}$ ist. Ist $e = e(\mathfrak{P}|\mathfrak{p})$ und $s = n_{\mathfrak{P}}(\Delta_{S|R})$ die Ordnung von $\Delta_{S|R}$ bei $\mathfrak{P}$, so gilt $s = e-1$ bei zahmer Verzweigung und $e \le s \le e(v_{\mathfrak{p}}(e)+1)-1$ sonst.*

Beweis. Wieder können wir $R = R_{\mathfrak{p}}$ annehmen. Nach (15.8) können wir überdies annehmen, dass $\mathfrak{p}$ in L total verzweigt (Übergang zur Galoishülle und zum Trägheitskörper). Nach (7.9) ist dann $S = R[\pi]$ monogen und $f = m_{K,\pi}$ ist ein Eisenstein-Polynom bzgl. $\mathfrak{p}$, etwa

$$f = X^n + a_{n-1}X^{n-1} + \ldots + a_0.$$

Es ist also $n = e$, $v_{\mathfrak{P}}(\pi) = 1$ und $e \mid v_{\mathfrak{P}}(a_i)$ für $i \le e-1$. Ferner ist nach (16.4) $s = v_{\mathfrak{P}}(f'(\pi))$. Für $i = 0, \ldots, e-1$ ist

$$v_{\mathfrak{P}}((e-i)a_i\pi^{e-i-1}) \equiv v_{\mathfrak{P}}(e-i) + e - i - 1 \equiv -i - 1 \,(\mathrm{mod}\, n).$$

Daher haben die einzelnen Summanden in $f'(\pi)$ verschiedene $v_{\mathfrak{P}}$-Werte. Somit gilt

$$s = v_{\mathfrak{P}}(f'(\pi)) = \min_{0 \le i < e} \big(v_{\mathfrak{P}}(e-i) a_i \pi^{e-i-1}\big).$$

Bei zahmer Verzweigung ($v_{\mathfrak{p}}(e) = 0$) ist $e-1$ dieses Minimum, und ist $v_{\mathfrak{p}}(e) \ge 1$, so gilt die Abschätzung $e \le s \le v_{\mathfrak{P}}(e) + e - 1 = e(v_{\mathfrak{p}}(e)+1) - 1$. $\square$

(16.7) **Folgerung.** *Sei $\mathfrak{p}S = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ die Zerlegung von $\mathfrak{p}$ in L und $f_i = f(\mathfrak{P}_i|\mathfrak{p})$. Dann ist $n_{\mathfrak{p}}(D_{S|R}) \ge \sum_{i=1}^{r}(e_i - 1)f_i$, und es gilt nur dann Gleichheit, wenn $\mathfrak{p}$ zahm verzweigt in L.*

Beweis. Nach (7.3) ist $\mathrm{N}_{L|K}(\mathfrak{P}_i) = \mathfrak{p}^{f_i}$. Wende (16.6) und (16.5) an. $\square$

(16.8) **Beispiel.** Sei $R = \mathbb{Z}$, $\mathfrak{p} = p\mathbb{Z}$ und $L = \mathbb{Q}(a)$, wobei $f = m_{\mathbb{Q},\alpha} \in \mathbb{Z}[X]$ sei (α ganz-algebraisch). Ist $v_p(D_f) = 1$, so ist auch $v_p(D_L) = 1$ und $\mathrm{Gal}_{\mathbb{Q}}(f)$ enthält eine Transposition. Die erste Aussage ist klar, da $D_f = c^2 D_L$ mit $c \in \mathbb{N}_{>0}$ ist. Ist $pR_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ die Zerlegung von p in L, und ist $f_i = f(\mathfrak{P}_i|p)$, so ist nach (7.5), (16.7) daher

$$\sum_{i=1}^{r}(e_i - 1)f_i \le 1.$$

Nach (9.3) ist also genau ein $e_i = 2$ und die übrigen gleich 1, alle $f_i = 1$, und p ist zahm verzweigt in L. Insbesondere ist $p \ne 2$. Aus (15.6) folgt, dass die Trägheitsgruppe $T_{\mathfrak{P}}$ eines Primideals $\mathfrak{P}$ über p im Zerfällungskörper von f von einer Transposition auf der Wurzelmenge W_f erzeugt wird. Es ist also beispielweise $\mathrm{Gal}_{\mathbb{Q}}(f) \cong S_n$, falls n eine Primzahl ist (Jordan).

(16.9) **Hauptsatz** (Hilbert). *Sei $L|K$ galoissch mit Gruppe G. Es gilt*

$$n_{\mathfrak{P}}(\Delta_{S|R}) = \sum_{s \ge 0}(|G_{\mathfrak{P}}^{(s)}| - 1).$$

Beweis. Nach (15.2) ist $G_{\mathfrak{P}}^{(t)} = 1$ für eine Nummer t. Wie im Beweis von (16.6) genügt es die Situation zu betrachten, wo $R = R_{\mathfrak{p}}$ und $\mathfrak{p}$ in L total verzweigt. Dann ist also $e = n = [L:K]$ der Verzweigungsindex von $\mathfrak{P}$ über $\mathfrak{p}$ und $S = R[\pi]$ monogen. Ferner ist $\Delta_{S|R} = f'(\pi)S$ für das Eisenstein-Polynom $f = m_{K,\pi}$ (16.4). Über $L = K(\pi)$ zerfällt f in Linearfaktoren: $f = \prod_{\sigma \in G}(X - \pi^\sigma)$, also $f'(\pi) = \prod_{1 \ne \sigma \in G}(\pi - \pi^\sigma)$. Für $\sigma \in G_{\mathfrak{P}}^{(s)} \setminus G_{\mathfrak{P}}^{(s+1)}$ ist $v_{\mathfrak{P}}(\pi^\sigma - \pi) = s + 1$ (vgl. den Beweis von (15.2)). Daher ist

$$n_{\mathfrak{P}}(\Delta_{S|R}) = v_{\mathfrak{P}}(f'(\pi)) = \sum_{s=0}^{t}\big(|G_{\mathfrak{P}}^{(s)}| - |G_{\mathfrak{P}}^{(s+1)}|\big)(s+1).$$

Setzt man $k_s = |G_{\mathfrak{P}}^{(s)}|$, so ist dies gleich $(k_0 - k_1) + 2(k_1 - k_0) + \ldots + t(k_{t-1} - 1) = \sum_{s=0}^{t}(k_s - 1)$. $\square$

§17. Der Satz von Kronecker–Weber

(17.1) **Hauptsatz** (Kronecker–Weber).

Jeder abelsche Zahlkörper ist ein Kreiskörper.

Zur Terminologie (nochmals): L ist ein abelscher Zahlkörper, falls L eine über $\mathbb{Q}$ endliche Galoiserweiterung mit abelscher Gruppe ist. Unter einem Kreiskörper verstehen wir einen Teilkörper eines Kreisteilungskörpers über $\mathbb{Q}$. Teilkörper und Komposita von abelschen Zahlkörpern sind abelsch; Teilkörper und Komposita von Kreiskörpern sind Kreiskörper.

Alle Zahlkörper werden als eingebettet in $\mathbb{C}$ betrachtet. Für einen algebraischen Zahlkörper K definieren wir

$$\delta(K) = \{p \in \mathbb{P} \mid p \mid D_K\}.$$

Nach (9.3) ist $\delta(K)$ gerade die Menge der Primzahlen, die in K verzweigen.

(17.2) **Lemma.** *Für algebraische Zahlkörper K, F gilt:*

(a) *Ist $K \subseteq F$, so ist $\delta(K) \subseteq \delta(L)$.*

(b) $\delta(KF) = \delta(K) \cap \delta(F)$.

(c) *Ist $\delta(K) = \varnothing$, so ist $K = \mathbb{Q}$.*

Beweis. (a) Transitivität des Verzweigungsindex' (7.3).

(b) Nach (15.7) gilt $\delta(K) = \delta(K')$, wenn K' die Galoishülle von $K|\mathbb{Q}$ ist. Wir können also K und F als galoissch über $\mathbb{Q}$ annehmen. Dann ist $\sigma \mapsto (\sigma|K, \sigma|F)$ ein Monomorphismus von $\mathrm{Gal}(KF|\mathbb{Q})$ in das direkte Produkt $\mathrm{Gal}(K|\mathbb{Q}) \times \mathrm{Gal}(F|\mathbb{Q})$, wobei Trägheitsgruppen in Trägheitsgruppen abgebildet werden. Ist also p eine Primzahl, die weder in K noch in F verzweigt, und ist $\mathfrak{P}$ ein Primideal von KF über p, so ist $T_{\mathfrak{P}} = 1$ und daher p unverzweigt in KF. Die Umkehrung folgt aus (a).

(c) Dies ist (12.4). □

(17.3) **Argumentation.** Sei L ein abelscher Zahlkörper. Um zu zeigen dass L ein Kreiskörper ist, bietet sich die Induktion nach dem Grad $[L : \mathbb{Q}]$ an. Dies reduziert auf die Situation, wo $L|\mathbb{Q}$ zyklisch vom Primzahlpotenzgrad ist. Dann sind nämlich alle echten Teilkörper von L Kreiskörper, und man ist fertig, es sei denn, es gibt nur einen maximalen Teilkörper. Im letzteren Falle ist $L|\mathbb{Q}$ wie behauptet, denn endliche abelsche Gruppen mit nur einer minimalen Untergruppe sind nach (0.4) zyklisch von Primzahlpotenzordnung. Für unsere Zwecke reicht es, per Induktion nach der Anzahl der Primteiler von $[L : \mathbb{Q}]$ zu argumentieren. Dies führt zumindest auf die Situation, dass $[L : \mathbb{Q}]$ eine Primzahlpotenz ist.

(17.4) **Satz.** *Sei L ein abelscher Zahlkörper und $p \in \delta(L)$ ein Primzahl, die nicht in $[L:\mathbb{Q}]$ aufgeht. Dann gibt es einen abelschen Zahlkörper K mit $\delta(K) = \delta(L) \setminus \{p\}$ und einen Kreiskörper $F \subseteq \mathbb{Q}(\varepsilon_p)$, so dass $L \subseteq KF$ gilt. Es ist $[K:\mathbb{Q}]$ überdies ein Teiler von $[L:\mathbb{Q}]$.*

Beweis. Sei $G = \mathrm{Gal}(L|\mathbb{Q})$ und $\mathfrak{p}|p$ in L. Wegen $p \nmid |G|$ ist p *zahm* verzweigt in L (15.2). Nach (14.2)(a) ist $G_\mathfrak{p} = \langle \sigma, \tau \rangle$, wobei die Trägheitsgruppe $T_\mathfrak{p} = \langle t \rangle$ und $\sigma^{-1}\tau\sigma = \tau^p$ ist. Da $G_\mathfrak{p}$ abelsch ist, folgt $\tau^{p-1} = 1$. Daher ist $|T_\mathfrak{p}| = e = e(\mathfrak{p}|p)$ ein Teiler von $p-1$ ist. Insbesondere ist p ungerade ($e > 1$). Sei F *der* Teilkörper von $\mathbb{Q}(\varepsilon_p)$ mit $[F:\mathbb{Q}] = e$. Nach (10.3) ist $F|\mathbb{Q}$ zyklisch mit $\delta(F) = \{p\}$, und p verzweigt total in F. Setze $E = LF$ und $H = \mathrm{Gal}(E|\mathbb{Q})$. Es ist E wieder ein abelscher Zahlkörper, und zwar mit $\delta(E) = \delta(L)$ nach (17.2)(b), in welchem p zahm verzweigt.

Sei $\mathfrak{P}$ ein Primideal von E über $\mathfrak{p}$ und $K = E_{H^{(0)}_\mathfrak{P}}$ der Trägheitskörper. Nach (8.4) ist p unverzweigt in K, daher $\delta(K) \subseteq \delta(E) \setminus \{p\}$. Nach (17.2)(c) ist $K \cap F = \mathbb{Q}$. Wir behaupten, dass $KF = E = LF$ ist. Dies beweist dann den Satz.

Die Einschränkung $\sigma \mapsto (\sigma|L, \sigma|F)$ ist ein Monomorphismus von H in das direkte Produkt $G \times \mathrm{Gal}(F|\mathbb{Q})$. Dabei wird die zyklische Gruppe $H^{(0)}_\mathfrak{P}$ in das direkte Produkt der entsprechenden Trägheitsgruppen abgebildet, die beide zyklisch der Ordnung e sind. Da der Verzweigungsindex von p in E ein Vielfaches von e ist, ist also $H^{(0)}_\mathfrak{P}$ zyklisch der Ordnung $e = [F:\mathbb{Q}] = [E:K]$. Da $K \cap F = \mathbb{Q}$ ist, ergibt sich wie behauptet $E = KF$. Ferner ist $[K:\mathbb{Q}] = [E:F] = [LF:F] = [L:L\cap F]$ ein Teiler von $[L:\mathbb{Q}]$. □

Nach (17.3), (17.4) hat man für den Beweis von Kronecker–Weber Galoiserweiterungen $L|\mathbb{Q}$ vom Grade $[L:\mathbb{Q}] = p^a$ für eine Primzahl p zu betrachten ($a \geq 1$), in welchen nur die Primzahl p verzweigt ($\delta(L) = \{p\}$). Wir werden die Abelschheit von L durch die Forderung erzwingen, dass L (total) reell ist.

(17.5) **Satz.** *Sei $L|\mathbb{Q}$ galoissch und $G = \mathrm{Gal}(L|\mathbb{Q})$ eine 2-Gruppe. Ist $\delta(L) = \{2\}$ und L (total) reell, so ist $L|\mathbb{Q}$ zyklisch und L ein Kreiskörper.*

Beweis. Wir können $G \neq 1$ und $\delta(L) = \{2\}$ annehmen (17.2)(c). Da L reell ist, ist $\mathbb{Q}(\sqrt{2})$ der einzige quadratische Zahlkörper in L. Das bedeutet, dass G nur eine maximale Untergruppe hat und daher zyklisch ist. Sei $[L:\mathbb{Q}] = 2^a$ und L' der maximale reelle Teilkörper von $\mathbb{Q}(\varepsilon_{2^{a+2}})$. Nach (10.3) ist $\delta(L') = \{2\}$. Für das Kompositum LL' gelten alle Voraussetzungen des Satzes. Daher ist $LL'|\mathbb{Q}$ zyklisch und $L = L'$. □

Ist in (17.5) L nicht reell aber L ein abelscher Zahlkörper, so ist $L_0 = L(\sqrt{-1}) \cap \mathbb{R}$ ein (total) reeller Körper (normal über $\mathbb{Q}$), und ist $[L_0:\mathbb{Q}] = 2^a$ und L' wie eben, so ist $L_0 = L'$ und

$$L \subseteq L(\sqrt{-1}) = L_0(\sqrt{-1}) \subseteq \mathbb{Q}(\varepsilon_{2^{a+2}}).$$

Wir haben also nur noch die (17.5) entsprechende Situation für *ungerade* Primzahlen zu betrachten. Übrigens hat der Zerfällungskörper von $X^4 - 2$ über $\mathbb{Q}$ als Galoisgruppe eine Diedergruppe der Ordnung 8 und nur die Primzahl 2 verzweigt in ihm.

(17.6) **Satz.** *Sei $L|\mathbb{Q}$ galoissch und $\mathrm{Gal}(L|\mathbb{Q})$ eine p-Gruppe für eine ungerade Primzahl p. Ist $\delta(L) = \{p\}$, so ist $L|\mathbb{Q}$ zyklisch und (daher) L ein Kreiskörper.*

Beweis. Hier ist L automatisch (total) reell. Es genügt zu zeigen, dass $L|\mathbb{Q}$ zyklisch ist. Ist dann etwa $[L : \mathbb{Q}] = p^a$ und L' der Teilkörper von $\mathbb{Q}(\varepsilon_{p^{a+1}})$ mit Grad $[L' : \mathbb{Q}] = p^a$, so ist nach (10.3), (17.2)(b) $\delta(LL') = \{p\}$ und daher mit demselben Argument $\mathrm{Gal}(LL'|\mathbb{Q})$ ein zyklische p-Gruppe und somit $L = L'$.

Angenommen, $L|\mathbb{Q}$ ist nicht zyklisch. Dann hat $\mathrm{Gal}(L|\mathbb{Q})$ eine nichtzyklische Faktorgruppe der Ordnung p^2 und daher L einen Teilkörper F, der über $\mathbb{Q}$ galoissch ist mit nichtzyklischer Gruppe $G = \mathrm{Gal}(K|\mathbb{Q})$ der Ordnung p^2. Nach (17.2) gilt $\delta(K) = \{p\}$.

Sei $\mathfrak{P}|p$ ein Primideal in K. Wäre die Trägheitsgruppe $T_{\mathfrak{P}}$ eine echte Untergruppe von G, so wäre der Fixkörper eine echte Erweiterung von $\mathbb{Q}$, in welcher keine Primzahl verzweigt. Das geht nicht nach (17.2)(c). Nach (15.2) ist $G = G_{\mathfrak{P}}^{(0)} = G_{\mathfrak{P}}^{(1)}$, also p total und wild verzweigt in K. Nach (16.6) ist $\Delta_{R_K|\mathbb{Z}}$ eine Potenz von $\mathfrak{P}$. Wir behaupten, dass

$$\big(\Delta_{R_F|\mathbb{Z}}\big) R_K = \mathfrak{P}^{2p(p-1)}$$

für jeden Teilkörper F von K mit $[F : \mathbb{Q}] = p$ ist. Sei $\bar{G} = \mathrm{Gal}(F|\mathbb{Q})$ und $\mathfrak{p} = \mathfrak{P} \cap F$. Sei t minimal derart, dass $\bar{G}_{\mathfrak{p}}^{(t)} = 1$ ist. Nach der Hilbertformel (16.9) gilt dann $n_{\mathfrak{p}}(\Delta_{R_F|\mathbb{Z}}) = t(p-1)$. Wegen $e(\mathfrak{p}|p) = p$ gilt nach (16.6) andererseits die Abschätzung $p \le n_{\mathfrak{P}}(\Delta_{R_F|\mathbb{Z}}) \le p \cdot v_p(p) + p - 1 = 2p - 1$. Es folgt $t = 2$ (wegen $p > 2$) und die Behauptung (wegen $e(\mathfrak{P}|\mathfrak{p}) = p$). (Warum ist $D_F = +p^{2(p-1)}$?)

Sei nun s minimal mit der Eigenschaft, dass $G_{\mathfrak{P}}^{(s)} \neq G$ ist. Nach (15.2) ist dann

$$G/G_{\mathfrak{P}}^{(s)} = G_{\mathfrak{P}}^{(s-1)}/G_{\mathfrak{P}}^{(s)} \cong k_{\mathfrak{P}}^{+} = \mathbb{F}_p^{+}.$$

Also ist $F = K_{G_{\mathfrak{P}}^{(s)}}$ vom Grad p über $\mathbb{Q}$. Existierte $F' \neq F$ in K mit Grade p über $\mathbb{Q}$, so wäre nach (15.4) $\mathrm{Gal}(L|F')_{\mathfrak{P}}^{(s)} = \mathrm{Gal}(L|F') \cap G_{\mathfrak{P}}^{(s)} = 1$ und daher

$$n_{\mathfrak{P}}(\Delta_{R_K|R_{F'}}) < n_{\mathfrak{P}}(\Delta_{R_K|R_F})$$

nach (16.9). Wir erhielten einen Widerspruch aus der Transitivität (16.2) der Differenten $\Delta_{R_K|\mathbb{Z}}$ (bzgl. F bzw. F'). Also ist F einzig, und $G = \mathrm{Gal}(K|\mathbb{Q})$ und $\mathrm{Gal}(L|\mathbb{Q})$ sind zyklisch . $\square$

Der Satz von Kronecker–Weber (17.1) folgt per Induktion nach der Anzahl der Primteiler von $[L : \mathbb{Q}]$ aus (17.4), (17.5), (17.6).

Anhang

Klassenkörpertheorie

Sei K ein algebraischer Zahlkörper. Unter einem *Modul* (Zykel, Divisor) $\mathfrak{m}$ von K verstehen wir ein formales Produkt $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, wobei $\mathfrak{m}_0 = \prod_{\mathfrak{p}\in\mathbb{P}_K} \mathfrak{p}^{m_\mathfrak{p}}$ ein (ganzes) Ideal von K (d.i., von R_K) und $\mathfrak{m}_\infty$ ein Produkt von paarweise verschiedenen archimedischen Bewertungen von K ist (leeres Produkt = 1). Mit $I_K^{(\mathfrak{m})} = I_K^{(\mathfrak{m}_0)}$ wird die freie abelsche Gruppe der Ideale von K teilerfremd zu (allen Primstellen in) $\mathfrak{m}_0$ bezeichnet (5.7). $H_K^{(\mathfrak{m})}$ ist die Gruppe der gebrochenen Hauptideale (x) von K, für welche gilt:

(i) $v_\mathfrak{p}(x-1) \geq m_\mathfrak{p}$ für alle $\mathfrak{p} \mid \mathfrak{m}_0$ $(m_\mathfrak{p} > 0)$;

(ii) $x > 0$ bzgl. jeder *reellen* Bewertung $|\cdot|_\mathfrak{p}$ in $\mathfrak{m}_\infty$.

Eine archimedische Bewertung (unendliche Primstelle) $|\cdot|_\mathfrak{p}$ von K verzweige in einem Erweiterungskörper L, falls sie reell aber eine Fortsetzung auf L imaginär ist. Mit $I_L^{(\mathfrak{m})}$ wird die Gruppe der Ideale von L bezeichnet, die teilerfremd zu den Primidealen von L über denen in $\mathfrak{m}_0$ sind.

Artin-Reziprozität. *Für jede endliche abelsche Erweiterung $L|K$ existiert der kleinste Modul $\mathfrak{f} = \mathfrak{f}_{L|K}$ ("Führer") in K mit folgenden Eigenschaften:*

(i) $\mathfrak{f}$ *ist genau durch die in L verzweigenden Primstellen teilbar.*

(ii) *Ist $\mathfrak{m}$ ein Modul in K mit $\mathfrak{f} \mid \mathfrak{m}$, so ist nach (i) und (10.4) der Artin-Homomorphismus $\phi_{L|K} : I_K^{(\mathfrak{m})} \to \mathrm{Gal}(L|K)$ erklärt. Dieser induziert einen Isomorphismus*

$$I_K^{(\mathfrak{m})}/H_K^{(\mathfrak{m})}\mathrm{N}_{L|K}(I_L^{(\mathfrak{m})}) \cong \mathrm{Gal}(L|K).$$

Für einen Beweis vgl. man Neukirch, Kap. 6, §7. Den Artin-Homomorphismus schreibt man meist $\phi_{L|K} = \left(\frac{L|K}{}\right)$. Ist $K = \mathbb{Q}$ und $L = \mathbb{Q}(\varepsilon_m)$ der m-te Kreisteilungskörper ($m \geq 3$ ungerade oder durch 4 teilbar), so ist nach (10.3), (10.4)

$$\mathrm{N}_{L|\mathbb{Q}}(I_L^{(m)}) \subseteq \mathrm{Ker}(\phi_{L|\mathbb{Q}}) = H_\mathbb{Q}^{(mp_\infty)}.$$

Daher ist $\mathfrak{f}_{L|\mathbb{Q}} = mp_\infty$. Zu $L^+ = \mathbb{Q}(\varepsilon_m + \varepsilon_m^{-1})$ gehört der Führer $\mathfrak{f}_{L^+|\mathbb{Q}} = m$.

Beispiel. Sei $K = \mathbb{Q}$ und $L = \mathbb{Q}(\sqrt{d})$ ein quadratischer Zahlkörper (1.1). Für eine zu D_L teilerfremde ungerade natürliche Zahl $r > 0$ definiere das *Jacobi-Symbol* durch

$$(\sqrt{d})^{\phi_{L|\mathbb{Q}}(r)} = \left(\frac{d}{r}\right)\sqrt{d}.$$

Aus der Artin-Reziprozität folgt $\left(\frac{d}{r}\right) = \left(\frac{d}{s}\right)$ für $r \equiv s \,(\mathrm{mod}\, 8d_0)$, d_0 der ungerade Anteil an d. In dieser Weise kann das Quadratische Reziprozitätsgesetz (für das Jacobi-Symbol) abgeleitet werden.

Existenzsatz. *Sei $\mathfrak{m}$ ein Modul von K und C eine Untergruppe von $I_K^{(\mathfrak{m})}$, die $H_K^{(\mathfrak{m})}$ enthält. Dann gibt es (in festem algebraischen Abschluss) genau eine abelsche Erweiterung $L|K$, für welche $C = H_K^{(\mathfrak{m})} \mathrm{N}_{L|K}(I_L^{(\mathfrak{m})})$ und $I_K^{(\mathfrak{m})}/C \cong \mathrm{Gal}(L|K)$ via Artin-Homomorphismus ist. L ist der "Klassenkörper" zur Idealklassengruppe $C/H_K^{(\mathfrak{m})}$.*

Für einen Beweis vgl. man Neukirch, Kap. 6, §6. Zu abelschen Erweiterungen L, L' von K findet man immer einen (zulässigen) Modul $\mathfrak{m}$ von K, der durch beide Führer teilbar ist, und dann gilt $L \subseteq L' \iff C \supseteq C'$ für die entsprechenden Idealgruppen. Jedem abelschen Zahlkörper L können wir daher einen zulässigen Modul $\mathfrak{m} = mp_\infty$ von $\mathbb{Q}$ mit einer Nummer $m \geq 3$ (nicht zweimal ungerade) und eine Idealgruppe $C \supseteq H_{\mathbb{Q}}^{(mp_\infty)}$ zuordnen. Folglich ist $L \subseteq \mathbb{Q}(\varepsilon_m)$ (Kronecker–Weber).

Definition. Der Klassenkörper L zum Modul $\mathfrak{f} = 1$ von K und zur Untergruppe $C = H_K$ heißt der *Hilbertsche Klassenkörper* $\mathrm{Hil(K)}$ von K. Dies ist der größte über K abelsche Körper, in welchem keine (endliche oder unendliche) Primstelle verzweigt (Existenzsatz). Es gilt also $\mathrm{Gal(Hil(K)|K)} \cong \mathrm{I_K/H_K} = \mathrm{C}\ell_\mathrm{K}$ via Artin-Reziprozität.

Nach (12.4) ist zum Beispiel $\mathrm{Hil}(\mathbb{Q}) = \mathbb{Q}$. Wie schon von Hilbert vermutet (Hilberts Satz 94), wird jedes Ideal von K Hauptideal in $\mathrm{Hil(K)}$ (Neukirch, S. 429). Nach Konstruktion ist $\mathrm{Hil^2(K)} = \mathrm{Hil}\big(\mathrm{Hil(K)}\big)$ galoissch über K; allerdings bricht der *Klassenkörperturm* $\mathrm{Hil^n(K)}$ i.a. nicht ab (Cassels–Fröhlich, Chap. 9).

Beispiel. Sei $K = \mathbb{Q}(\sqrt{d})$ ein imaginärer quadratischer Zahlkörper und $D = D_K = p_1^* \cdots p_s^*$, wobei $2^* \in \{-4, \pm 8\}$ und $p^* = \big(\frac{-1}{p}\big)p$ für ungerade Primzahlen p gesetzt ist (§10). Es ist $L = \mathbb{Q}\big(\sqrt{p_1^*}, \ldots, \sqrt{p_s^*}\big) \subseteq \mathbb{Q}(\varepsilon_{|D|})$ (10.6). Keine (endliche oder unendliche) Primstelle von K verzweigt in L (!). Daher ist $L \subseteq \mathrm{Hil(K)}$, somit $2^{s-1} \mid h_K$.

Satz. *Sei $K|\mathbb{Q}$ eine Galoiserweiterung mit Gruppe G. Ist G eine p-Gruppe für eine Primzahl p und verzweigt nur eine Primzahl in K, so ist p kein Teiler von h_K.*

Beweis. Angenommen, $p \mid h_K$. Sei L der Hilbertsche p-Klassenkörper von K, d.h., $L \subseteq \mathrm{Hil(K)}$ und Grad $[L : K]$ gleich dem p-Anteil von h_K. $L|\mathbb{Q}$ ist galoissch und $H = \mathrm{Gal}(L|\mathbb{Q})$ eine p-Gruppe. Die Trägheitsgruppe eines über der in K verzweigenden Primzahl liegenden Primideals von L ist eine echte Untergruppe von H, liegt also in einer maximalen Untergruppe N. Da N normal in H ist, ist der Fixkörper $F = L_N$ galoissch über $\mathbb{Q}$ (vom Grade p). Keine Primzahl verzweigt in F nach Voraussetzung (und Konstruktion). Aber dies widerspricht (12.4). $\square$

Sei K_a der Teilkörper von $\mathbb{Q}(\varepsilon_{p^{a+1}})$ mit Grad $[K_a : \mathbb{Q}] = p^a$ ($p \in \mathbb{P}_{>2}$, $a \geq 1$). Nach (10.3) verzweigt nur die Primzahl p in K_a, und nach (17.6) ist $\mathrm{Gal}(K_a|\mathbb{Q}) \cong \mathbb{Z}/p^a\mathbb{Z}$. Die Vereinigung $\widetilde{K} = \bigcup_{a \geq 1} K_a$ heißt die *Iwasawa-Kreiserweiterung* von $\mathbb{Q}$ zur Primzahl p. Nach obigem Satz gilt $p \nmid h_{K_a}$ für alle a. Das ist eine der Ideen, die dem Beweis der Fermat-Vermutung nach Wiles zugrundeliegen.

Übungsaufgaben

Blatt 1 (15.10.2008)

(1) Man berechne die Elementarteiler der ganzzahligen Matrix

$$C = \begin{pmatrix} 0 & 9 & -18 & 12 \\ -6 & -12 & 0 & 24 \end{pmatrix}.$$

Welche abelsche Gruppe mit 4 Erzeugenden und 2 Relationen wird dadurch beschrieben ?

(2) Seien $a > 0$ und $b > 0$ teilerfremde natürliche Zahlen. Man zeige, dass durch elementare Zeilen- und Spaltentransformationen folgende Äquivalenzen gelten:

$$\begin{pmatrix} -a & 0 \\ 0 & -b \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & ab \end{pmatrix} \sim \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}.$$

Interpretation: Die abelsche Gruppe $\mathbb{Z}/a\mathbb{Z} \oplus \mathbb{Z}/b\mathbb{Z}$ ist die zyklische Gruppe $\mathbb{Z}/ab\mathbb{Z}$. Warum ist $\begin{pmatrix} -a & 0 \\ 0 & -b \end{pmatrix} \not\sim \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$?

(3) Sei R ein Integritätsbereich (mit $1 \neq 0$). Man zeige:
(a) Hat R nur endlich viele Elemente, so ist R ein Körper.
(b) Ist R ein Hauptidealring mit nur einem maximalen Ideal $\mathfrak{p} = \pi R \neq 0$, so ist jedes von Null verschiedene Ideal von R eine Potenz $\mathfrak{p}^n = \pi^n R$, und es gilt der Elementarteilersatz für R.

(4) Sei p eine Primzahl, und sei A ein assoziativer Ring mit $1 \neq 0$ und Ordnung $|A| = p^2$. Man zeige:
(a) A ist kommutativ. (Das Zentrum $Z(A) = \{z \in A |\, zx = xz \text{ für alle } x \in A\}$ ist ein Teilring von A.)
(b) Die Menge $J = J(A) = \{a \in A |\, a^n = 0 \text{ für ein } n \in \mathbb{N}\}$ der nilpotenten Elemente ist ein Ideal von A.
(c) Ist $J \neq 0$, so ist J das einzige maximale Ideal von A (Ordnung p) und $A^* = A \setminus J$ die Einheitengruppe.
(d) Ist $J = 0$, so ist entweder A ein Körper oder A hat nichttriviale Primideale $\mathfrak{p} \neq \mathfrak{p}'$ (der Ordnung p) mit $\mathfrak{p}\mathfrak{p}' = \mathfrak{p} \cap \mathfrak{p}' = 0$.
Zusatz. Welche Isomorphietypen gibt es für A ?

Blatt 2 (20.10.2008)

(5) Sei $R = \mathbb{Z}[i]$ der Ring der ganzen Gaußschen Zahlen ($i^2 = -1$).
(a) Man zeige, dass $\mathfrak{p} = (1+i)R$ ein maximales Ideal von R und $2R = \mathfrak{p}^2$ ist.
(b) Ist p eine ungerade Primzahl und $p = a^2 + b^2$ mit $a, b \in \mathbb{Z}$, so ist $p \equiv 1 \pmod 4$ und $pR = \mathfrak{p}\mathfrak{p}'$ mit Primidealen $\mathfrak{p} \neq \mathfrak{p}'$.
(c) Ist p eine Primzahl mit $p \equiv 1 \pmod 4$, so gibt es eine ganze Zahl x mit $p \mid x^2+1$, denn $\mathbb{F}_p^*$ ist zyklisch der Ordnung $p-1$ und enthält wegen $4 \mid p-1$ ein Element $\bar{x}$ der Ordnung 4. Warum ist $\bar{x}^2 = -1$?
(d) Ist p eine Primzahl mit $p \equiv 1 \pmod 4$, so ist p Summe von 2 Quadraten in $\mathbb{Z}$ (Fermat).

(6) Man zeige, dass der Ring $R = \mathbb{Z}[\sqrt{2}]$ der ganzen Zahlen in $K = \mathbb{Q}(\sqrt{2})$ euklidisch bzgl. des Betrags der Norm $\mathrm{N} = \mathrm{N}_{K|\mathbb{Q}}$ ist. (Man überlege, dass es zu $x, y \in \mathbb{Q}$ immer ganze Zahlen a, b gibt mit $|(x-a)^2 - 2(y-b)^2| < 1$.)

(7) Man berechne die Einheiten des Rings $R = R_K$ der ganzen Zahlen für die reellen quadratischen Zahlkörper $K = \mathbb{Q}(\sqrt{d})$ mit $d = 6, 7, 17$. Man gebe jeweils die Norm der Fundamentaleinheit an.

(8) Sei $R = \mathbb{Z}[\sqrt{-3}]$. Man zeige, dass R (im Gegensatz zu $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$) Ideale $\mathfrak{a}$ hat, die keine Hauptideale sind. (Vorschlag: $\mathfrak{a} = (2, 1+\sqrt{-3})$.) Man zeige ferner, dass es Ideale $\mathfrak{b} \neq 0$ von R gibt, die nicht Produkte von Primidealen sind. (Vorschlag: $\mathfrak{b} = 2R$.)

Blatt 3 (27.10.2008)

(9) Sei $K = \mathbb{Q}(\sqrt{-5})$ und $R = R_K$. Nach (1.9) der Vorlesung ist R kein faktorieller Ring, also auch kein Hauptidealring. Man zeige, dass $\mathfrak{p} = (3, 1+\sqrt{-5})$ ein Primideal von R ist aber kein Hauptideal. Man zeige ferner, dass $\mathfrak{p}^2$ ein Hauptideal von R ist.

(10) Man gebe die Zerlegung der Primzahlen $p = 2, 3, 5$ im Körper $K = \mathbb{Q}(\sqrt{-5})$ an, d.h., man schreibe pR_K (eindeutig) als Produkt von Primidealen von R_K. Welche der auftretenden Primideale sind Hauptideale ?

(11) Sei p eine ungerade Primzahl und ε eine primitive 8-te Einheitswurzel über $\mathbb{F}_p$. Man zeige:
(a) 8 ist ein Teiler von $p^2 - 1 = (p-1)(p+1)$ und daher $[\mathbb{F}_p(\varepsilon) : \mathbb{F}_p] = 1$ oder 2.
(b) Für $x = \varepsilon + \varepsilon^{-1}$ gilt $x^2 = 2$ und $x^p = \varepsilon^p + \varepsilon^{-p}$.
(c) Genau dann ist $x \in \mathbb{F}_p^*$, wenn $p \equiv \pm 1 \,(\mathrm{mod}\, 8)$ ist.

(12) Das Legendre-Symbol $\left(\frac{\cdot}{p}\right)$ für eine ungerade Primzahl p wurde in (1.8) der Vorlesung eingeführt. Man zeige: Ist n eine ganze Zahl mit $p \nmid n$, so gilt $\left(\frac{-n}{p}\right) = 1$ genau dann, wenn es teilerfremde ganze Zahlen x, y gibt, so dass p ein Teiler von $x^2 + ny^2$ ist. Für $n = 1, 2, 3$ impliziert diese Teilbarkeitsbeziehung die Existenz ganzer Zahlen a, b mit $p = a^2 + nb^2$.
Anmerkung. Wir kennen schon die beiden *Gesetze* $\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \,(\mathrm{mod}\, 4)$ und $\left(\frac{2}{p}\right) = 1 \iff p \equiv \pm 1 \,(\mathrm{mod}\, 8)$ (Übungen (5) und (11)). Hinzu kommt also jetzt $\left(\frac{3}{p}\right) = 1 \iff p \equiv \pm 1 \,(\mathrm{mod}\, 12)$. (Warum ?)

Zum Legendre-Symbol

Sei p eine ungerade Primzahl. Für eine ganze Zahl a ist $(\frac{a}{p}) = 0, \pm 1$ wie in (1.8) der Vorlesung definiert. Dies hängt nur von der Restklasse von a mod p ab und definiert einen Charakter (Gruppenhomomorphismus) $\mathbb{F}_p^* \to (\{\pm 1\}, \cdot)$. Ist $x = a + p\mathbb{Z}$ mit $p \nmid a$, so ist $(\frac{x}{p}) = x^{(p-1)/2}$ in $\mathbb{F}_p^*$ und $x \in \mathbb{F}_p^{*2}$ ein Quadrat in $\mathbb{F}_p^*$ genau dann, wenn x im Kern des Endomorphismus' $x \mapsto x^{(p-1)/2}$ von $\mathbb{F}_p^*$ ist. Nun zu einigen Übungen:

(5) Nach (1.3) der Vorlesung ist der Ring $R = \mathbb{Z}[i]$ der ganzen Gaußschen Zahlen ein Hauptidealring. Nach (1.8) gilt $(\frac{-1}{p}) = 1$ genau dann, wenn $pR = \mathfrak{p}\mathfrak{p}'$ ist mit Primidealen $\mathfrak{p} \neq \mathfrak{p}'$ von R der Norm p. Es ist dann $\mathfrak{p} = (a + ib)R$ mit $a, b \in \mathbb{Z}$ und

$p = \mathrm{N}(a+ib) = a^2+b^2$ gemäß (1.5). Da p ungerade ist, ist etwa a ungerade und b gerade, daher $p \equiv 1 \pmod 4$. Ist umgekehrt $4 \mid p-1$, so enthält die (zyklische) Gruppe $\mathbb{F}_p^*$ (der Ordnung $p-1$) ein Element der Ordnung 4, dessen Quadrat -1 in $\mathbb{F}_p^*$ ist. Folglich ist $(\frac{-1}{p}) = 1$ in diesem Falle. *Ergebnis*: $(\frac{-1}{p}) = (-1)^{(p-1)/2}$, und dies ist genau dann $+1$, wenn $p = a^2 + b^2$ mit $a, b \in \mathbb{Z}$ ist.

(11) Sei ε eine primitive 8-te Einheitswurzel über $\mathbb{F}_p$. Da $p^2 - 1 = (p+1)(p-1)$ durch 8 teilbar und $\mathbb{F}_{p^2}^*$ zyklisch der Ordnung $p^2 - 1$ ist, gilt $[\mathbb{F}_p(\varepsilon) : \mathbb{F}_p] = 1$ oder 2. Setze $x = \varepsilon + \varepsilon^{-1}$. Wegen $\varepsilon^4 = -1$ gilt $\varepsilon^2 = -\varepsilon^{-2}$ und daher $x^2 = 2$. Wegen $x^p = \varepsilon^p + \varepsilon^{-p}$ gilt $x^p = x$ für $p \equiv \pm 1 \pmod 8$ und $x^p = \varepsilon^5 + \varepsilon^{-5} = -(\varepsilon + \varepsilon^{-1}) = -x$ für $p \equiv \pm 5 \pmod 8$. Also ist $x \in \mathbb{F}_p$ (und damit 2 ein Quadrat in $\mathbb{F}_p$) genau dann, wenn $p \equiv \pm 1 \pmod 8$ ist. *Ergebnis.* $(\frac{2}{p}) = (-1)^{(p^2-1)/8}$.

(12) Sei n eine ganze Zahl mit $p \nmid n$. Ist $\left(\frac{-n}{p}\right) = 1$, so gibt es ganze Zahlen x, y mit $p \nmid xy$ und $x^2 \equiv -ny^2 \pmod p$, d.h., mit $p \mid x^2 + ny^2$. Wir können annehmen, dass x und y teilerfremd sind. Ist umgekehrt $p \mid x^2 + ny^2$ mit ganzen, nicht durch p teilbaren Zahlen x, y, so ist $\left(\frac{-n}{p}\right) = 1$. Sei nun $n \in \{1, 2, 3\}$ und $s \in \mathbb{Z}$ mit $s^2 \equiv -n \pmod p$. Sei $M = [-\sqrt{p}/2, \sqrt{p}/2] \cap \mathbb{Z}$. Da $|M \times M| \geq p+1$ ist, gibt es $(x, y) \neq (x', y')$ in $M \times M$ mit $x \equiv sy \pmod p$ und $x' \equiv sy' \pmod p$. Setze $a = x - x'$ und $b = y - y'$ bzw. $= y + y'$, je nachdem ob y und y' dasselbe Vorzeichen haben oder nicht. Dann ist $a \equiv \pm sb \pmod p$, also $a^2 \equiv -nb^2 \pmod p$, und $a^2 \leq p$, $b^2 \leq p/4$. Wäre $a = 0 = b$, so wäre $x = x'$, $y = -y'$ und p ein Teiler von $x - sy$ und von $x + sy$, mithin von $2x$. Dies ist nicht möglich, da p ungerade und $|x| < p$ ist. Da p ein Teiler von $(0 <)\ a^2 + nb^2\ (\leq 7p/4 < 2p)$ ist, folgt $p = a^2 + nb^2$.

Anmerkung. Der Fall $n = 3$ (und $p \geq 5$) ist interessant. Es ist $(\frac{-3}{p}) = 1$ genau dann, wenn $\mathbb{F}_p$ eine primitive 3-te Einheitswurzel $\varepsilon = \frac{-1+\sqrt{-3}}{2}$ enthält, also genau dann, wenn $3 \mid p-1$ gilt. Wegen $(\frac{-1}{3}) = -1$ gilt also $(\frac{-3}{p}) = 1 \iff p \equiv 1 \pmod 3 \iff (\frac{p}{3}) = 1$. Mit (5) erhalten wir (durch Betrachten von $(\mathbb{Z}/12\mathbb{Z})^*$) das neue *Gesetz*:

$$\left(\frac{3}{p}\right) = 1 \iff p \equiv \pm 1 \pmod{12}.$$

Blatt 4 (3.11.2008)

(13) Man gebe mindestens 4 Tripel paarweise teilerfremder natürlicher Zahlen a, b, c an, wobei a ungerade ist und $a^2 + b^2 = c^2$ gilt.

(14) Sei $\varepsilon = \frac{-1+\sqrt{-3}}{2}$ eine primitive 3-te Einheitswurzel über $\mathbb{Q}$. Warum ist $-\varepsilon^2 = \frac{1+\sqrt{-3}}{2}$ eine primitive 6-te Einheitswurzel ? Warum ist $\pi = \varepsilon - 1$ ein Primelement in dem Hauptidealring $R = \mathbb{Z}[\varepsilon]$? Man zeige:
(a) Sind α, β Elemente von R mit $\alpha \equiv \beta \pmod{\pi}$, so gilt $\alpha^3 \equiv \beta^3 \pmod{\pi^3}$.
(b) Ist $\alpha \in R$ mit $\pi \nmid \alpha$ ($\alpha \notin \pi R$), so ist $\alpha^3 \equiv \pm 1 \pmod{\pi^3}$.
(c) Sei angenommen, es gebe paarweise teilerfremde Elemente α, β, γ in R mit $\alpha^3 + \beta^3 = \gamma^3$. Dann kann etwa $\pi \nmid \alpha\beta$ angenommen werden. Man zeige, dass dann π ein Teiler von γ ist. (Auch dies konnte Gauß ausschließen.)

(15) Sei K ein algebraischer Zahlkörper und α ein primitives Element für $K|\mathbb{Q}$, also $K = \mathbb{Q}(\alpha)$. Das Minimalpolynom $f = m_{\mathbb{Q},\alpha}$ von α zerfalle über $\mathbb{C}$ als Produkt $f = \prod_{i=1}^{n}(X - \alpha_i)$ (etwa $\alpha = \alpha_1$). Warum ist f separabel, d.h., die Diskriminante $D_f = \prod_{i<j}(\alpha_i - \alpha_j)^2 \neq 0$? Die Norm $\mathrm{N}(\alpha) = \mathrm{N}_{K|\mathbb{Q}}(\alpha)$ ist das Produkt der *Konjugierten* α_i von α. Jedes $\beta \in K$ ist von der Form $\beta = g(\alpha)$ für ein rationales Polynom g, und dann ist $\mathrm{N}(\beta) = \prod_{i=1}^{n} g(\alpha_i)$. Man zeige, dass dies wohldefiniert ist. Ferner zeige man, dass

$$D_f = (-1)^{n(n-1)/2}\mathrm{N}(f'(\alpha))$$

gilt. Hier bezeichnet f' die (formale) Ableitung von f.

(16) Sei p eine ungerade Primzahl, $\varepsilon = \varepsilon_p$ eine primitive p-te Einheitswurzel und $L = \mathbb{Q}(\varepsilon)$. Definiere die Diskriminante $D_L = D_{\Phi_p}$ durch das p-te Kreisteilungspolynom Φ_p. (Dies ist begündet durch die Tatsache, das nach (2.6) der Vorlesung $R_L = \mathbb{Z}[\varepsilon] \cong \mathbb{Z}[X]/(\Phi_p)$ der Ring der ganzen Zahlen von L ist.) Unter Verwendung von (15) zeige man

$$D_L = (-1)^{(p-1)/2}p^{p-2}.$$

(Hinweis: Durch Differentiation von $(X-1)\Phi_p(X) = X^p - 1$ erhält man die Gleichung $(\varepsilon - 1)\Phi_p'(\varepsilon) = p\varepsilon^{p-1}$.)

Blatt 5 (10.11.2008)

(17) Welche der folgenden komplexen Zahlen sind ganz-algebraisch ?
$(1+\sqrt{3})/2$; $(1+\sqrt{-3})/2$; $\sin\frac{\pi}{7}$; $e^{\pi i/9}$; $(1+i)/\sqrt{2}$.

(18) Seien $R \subseteq S$ Integritätsbereiche mit Quotientenkörpern $K \subseteq L$. Man zeige:
(a) Ist $S|R$ ganz, so ist $L|K$ algebraisch.
(b) Ist $S = R_{L|R}$ der ganze Abschluss von R in L, so ist

$$L = \{\tfrac{\beta}{a} |\ \beta \in S,\, 0 \neq a \in R\}.$$

(19) Seien $R \subseteq S$ Integritätsbereiche (automatisch mit derselben 1). Ist $u \in S^*$ eine Einheit, so ist der Ring $R[u] \cap R[u^{-1}]$ ganz über R. (Zu $x \in R[u] \cap R[u^{-1}]$ finde man $n \in \mathbb{N}$ derart, dass für $M = R + Ru + Ru^2 + \ldots + Ru^n$ gilt $xM \subseteq M$.)

(20) Sei K ein quadratischer Zahlkörper und $R = R_K$. Man zeige, dass es immer eine Primzahl p gibt, die in K verzweigt. Dann ist also $pR = \mathfrak{p}^2$ mit einem Primideal $\mathfrak{p}$ von R der Norm p. Man zeige, dass R/pR isomorph zum Ring aller oberen Dreiecksmatrizen der Form $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$ über $\mathbb{F}_p$ ist (vgl. Übung (4)). Warum gibt es nur endlich viele in K verzweigende Primzahlen ?

Blatt 6 (17.11.2008)

Durchweg seien $d_1 \neq d_2$ quadratfreie ganze Zahlen $\neq 0, 1$ und $d_3 = d_1 d_2 / \mathrm{ggT}(\mathrm{d}_1, \mathrm{d}_2)^2$. Dann sind die $K_i = \mathbb{Q}(\sqrt{d_i})$ für $i = 1, 2, 3$ die drei quadratischen Zahlkörper in dem *biquadratischen* Körper $L = K_1K_2 = K_1K_3 = K_2K_3$. Die Ringe der ganzen Zahlen in den K_i sind nach (1.2) der Vorlesung bekannt. Seien $\mathrm{N}_i = \mathrm{N}_{L|K_i}$ und $\mathrm{Tr}_i = \mathrm{Tr}_{L|K_i}$ die *relativen* Normen und Spuren.

(21) Sei $i \in \{1, 2, 3\}$ und $\alpha \in L$. Man zeige, dass $\alpha \in R_L$ genau dann ganz-algebraisch ist, wenn $\mathrm{N}_i(\alpha)$ und $\mathrm{Tr}_i(\alpha)$ ganz-algebraisch sind.

(22) Sei $d_1 \equiv 3 \,(\mathrm{mod}\, 4)$ und $d_2 \equiv d_3 \equiv 2 \,(\mathrm{mod}\, 4)$. Durch Berechnen von $\mathrm{Tr}_i(\alpha)$ für $i = 1, 2, 3$ zeige man, dass jedes $\alpha \in R_L$ die Form $\frac{1}{2}(a + b\sqrt{d_1} + c\sqrt{d_2} + d\sqrt{d_3})$ hat mit $a, b, c, d \in \mathbb{Z}$. Durch Betrachten von $\mathrm{N}_1(\alpha)$ zeige man, dass a und b gerade und $c \equiv d \,(\mathrm{mod}\, 2)$ sein muss. (*Hinweis:* $\sqrt{d_2}\sqrt{d_3} = \pm d_2'\sqrt{d_1}$ mit geradem $d_2' = d_2/\mathrm{ggT}(\mathrm{d}_1, \mathrm{d}_2)$.) Man folgere, dass $\{1, \sqrt{d_1}, \sqrt{d_2}, \frac{\sqrt{d_2}+\sqrt{d_3}}{2}\}$ eine Ganzheitsbasis von L ist.

(23) Sei $d_1 \equiv 1 \,(\mathrm{mod}\, 4)$ und $d_2 \equiv d_3 \equiv 2$ oder $3 \bmod 4$. Wieder hat jedes $\alpha \in R_L$ die Form $\frac{1}{2}(a + b\sqrt{d_1} + c\sqrt{d_2} + d\sqrt{d_3})$ mit $a, b, c, d \in \mathbb{Z}$. In diesem Fall erhält man $a \equiv b \,(\mathrm{mod}\, 2)$ und $c \equiv d \,(\mathrm{mod}\, 2)$. Man folgere, dass $\{1, \frac{1+\sqrt{d_1}}{2}, \sqrt{d_2}, \frac{\sqrt{d_2}+\sqrt{d_3}}{2}\}$ eine Ganzheitsbasis von L ist.

(24) Man berechne die absolute Diskriminante D_L in den beiden in (22), (23) behandelten Fällen.

Anmerkung: Ist $d_1 \equiv d_2 \equiv d_3 \equiv 1 \,(\mathrm{mod}\, 4)$, so ist

$$\{1, \frac{1+\sqrt{d_1}}{2}, \frac{1+\sqrt{d_2}}{2}, (\frac{1+\sqrt{d_1}}{2})(\frac{1+\sqrt{d_3}}{2})\}$$

eine Ganzheitsbasis von L. Damit sind dann, bei eventueller Vertauschung der d_i, alle möglichen Fälle behandelt.

Blatt 7 (24.11.2008)

(25) Sei $p \geq 5$ eine Primzahl und $L = \mathbb{Q}(\varepsilon)$ für eine primitive p-te Einheitswurzel $\varepsilon = \varepsilon_p$. Sei $\alpha = \varepsilon + \varepsilon^{-1}$ und $K = \mathbb{Q}(\alpha)$ der maximale total reelle Teilkörper von L. Man zeige (unter Verwendung von (2.6) der Vorlesung), dass $R_K = \mathbb{Z}[\alpha]$ ist. Man folgere, dass $\sin(\frac{\pi}{p})$ und $\sin(\frac{2\pi}{p})$ keine ganz-algebraischen Zahlen sind.

(26) Das Polynom $f = X^5 - X + 1$ ist irreduzibel mod 5 (Beweis!) und daher über $\mathbb{Q}$. Sei $\alpha \in \mathbb{C}$ eine Wurzel von f in $\mathbb{C}$ und $K = \mathbb{Q}(\alpha)$. Warum ist $\alpha \in R = R_K$? Warum ist die Diskriminante $D_f = \mathrm{N}_{K|\mathbb{Q}}(f'(\alpha))$? Man berechne:
(a) $\mathrm{Tr}_{K|\mathbb{Q}}(\alpha) = 0$, $\mathrm{N}_{K|\mathbb{Q}}(\alpha) = -1$.
(b) Es ist $\beta = f'(\alpha) = \frac{-5}{\alpha} + 4$ und daher $f(\frac{5}{4-\beta}) = 0$. Man berechne das Minimalpolynom $m_{\mathbb{Q},\beta}$ und damit D_f.
(c) Aus dem Ergebnis für D_f leite man ab, dass $D_f = D_K$ und $R = \mathbb{Z}[\alpha]$ ist.

(27) Sei K ein algebraischer Zahlkörper. Man zeige, dass die absolute Diskriminante D_K genau dann positiv ist, wenn die Anzahl r_2 der Paare konjugiert komplexer imaginärer Einbettungen von K in $\mathbb{C}$ gerade ist.

(28) Für die Diskriminante eines algebraischen Zahlkörpers K gilt $D_K \equiv 0 \,(\mathrm{mod}\, 4)$ oder $D_K \equiv 1 \,(\mathrm{mod}\, 4)$. (*Hinweis:* Sei $\{a_i\}$ eine Ganzheitsbasis von K und $\det\big((\alpha_i)_{ij}^{\sigma_j}\big) = P - N$, wobei die σ_j die verschiedenen Einbettungen von K in $\mathbb{C}$ sind und P in der Leibniz-Formel der Anteil der geraden Permutationen ist, N der der ungeraden. Dann ist $D_K = (P-N)^2 = (P+N)^2 - 4PN$. Man verwende, dass $P+N$ und PN ganz-algebraisch sind und invariant unter allen σ_j.)

Blatt 8 (1.12.2008)

(29) Es seien $U \subseteq V$ freie $\mathbb{Z}$-Moduln des gleichen endlichen Ranges $n \geq 1$. Man zeige:
(a) Der Index $|V : U|$ ist endlich.
(b) Ist p eine Primzahl mit $p \nmid |V : U|$, so gilt $U_{(p)} = V_{(p)}$ für die Lokalisierungen bei $(p) = p\mathbb{Z}$.

(30) Man beantworte folgende Fragen, jeweils mit Begründung:
- Ist der Polynomring $\mathbb{Z}[X]$ ein Dedekindring ?
- Ist der Polynomring $\mathbb{Q}[X]$ein Dedekindring ?
- Ist der Polynomring $\mathbb{Q}[X, Y]$ in den Unbestimmten X, Y ein Dedekindring ?

(31) Sei R ein Dedekindring und seien $\mathfrak{a}$ und $\mathfrak{b}$ gebrochene Ideale von R.
(a) Genau dann haben $\mathfrak{a}$ und $\mathfrak{b}$ dieselbe Klasse $[\mathfrak{a}] = [\mathfrak{b}]$ in $\mathrm{C}\ell_R$, wenn es von Null verschiedene Elemente x, y in R gibt mit $x\mathfrak{a} = y\mathfrak{b}$.
(b) Genau dann gilt $[\mathfrak{a}] = [\mathfrak{b}]$, wenn $\mathfrak{a}$ und $\mathfrak{b}$ als R-Moduln isomorph sind.

(32) Sei R ein Dedekindring und $\mathfrak{a} \neq 0$ ein Ideal von R. Man zeige:
(a) Jedes Ideal von $R/\mathfrak{a}$ ist durch ein Element erzeugbar. (Man kann $\mathfrak{a} \subset R$ annehmen. Es gibt nur endlich viele Primideale von R oberhalb $\mathfrak{a}$. Man argumentiere wie in (5.9) der Vorlesung unter Anwendung des Chinesischen Restesatzes.)
(b) $\mathfrak{a}$ ist (als R-Modul) durch 2 Elemente erzeugbar.

Blatt 9 (8.12.2008)

Unter einer (multiplikativen) Bewertung des Körpers K versteht man einen Gruppenhomomorphismus $|\cdot| : K^* \to (\mathbb{R}_{>0}, \cdot)$ mit $|x+y| \leq |x| + |y|$, wobei man noch $|0| = 0$ setzt. Die Bewertung heißt nichtarchimedisch, falls stets $|x+y| \leq \max\{|x|, |y|\}$ gilt.

(33) Ist K ein algebraischer Zahlkörper und $\sigma : K \to \mathbb{C}$ eine Körpereinbettung, so definiert $|x|_\sigma = |x^\sigma|$ eine (archimedische) Bewertung von K ($|\cdot|$ der komplexe Betrag). Es gibt genau $r_1 + r_2$ solche Bewertungen von K, wobei r_1 die Anzahl der reellen und r_2 die der Paare konjugiert komplexer (nichtreeller) Einbettungen von K ist.

(34) Für jede Primzahl p wird durch $|x|_p = (\frac{1}{p})^{v_p(x)}$ eine nichtarchimedische (diskrete) Bewertung von $\mathbb{Q}$ erklärt, wobei für $x \neq 0$ mit $v_p(x) = r$ die Ordnung von x bei $p\mathbb{Z}$ bezeichnet wird ($x = p^r \frac{a}{b}$ mit nicht durch p teilbaren ganzen Zahlen a, b). Für $x \in \mathbb{Q}^*$ ist $|x|_p = 1$ fast immer und $\prod_{p \in \mathbb{P}} |x|_p = 1/|x|$, wobei $|\cdot| = |\cdot|_\infty$ der gewöhnliche Betrag auf $\mathbb{Q}$ ist.

(35) Sei $K = k(X)$ der Quotientenkörper des Polynomrings über dem Körper k. Sei $0 < c < 1$. Für jedes irreduzible normierte Polynom $p \in k[X]$ wird durch $|f|_p = c^r$ eine nichtarchimedische (diskrete) Bewertung erklärt, wobei $r \in \mathbb{Z}$ für $f \neq 0$ durch $f = p^r \frac{g}{h}$ mit nicht durch p teilbaren Polynomen g, h bestimmt wird. Für $f = \frac{g}{h}$ wird ferner durch $|f|_\infty = c^{\mathrm{grd(h)} - \mathrm{grd(g)}}$ eine weitere Bewertung auf K definiert. Es gilt $\prod_p |f|_p = 1/|f|_\infty$.

(36) Ist $|\cdot|$ eine nichtarchimedische Bewertung von K, so ist $R = \{x \in K : |x| \leq 1\}$ ein Teilring von K und $\mathfrak{m} = \{x \in K : |x| < 1\}$ das einzige maximale Ideal von R.

Blatt 10 (15.12.2008)

(*Weihnachtsaufgabe*)

Sei $L = k(t)$ der Quotientenkörper des Polynomrings $S = k[t]$ über dem Körper k (in der Unbestimmten t) und K ($\subseteq L$) der Quotientenkörper des Teilrings $R = k[t^2]$. Man bearbeite bis zum 12.01.2009 *vier* der folgenden Aufgaben.

(37) R und S sind (isomorphe) euklidische Ringe, somit Hauptidealringe, und Dedekindringe.

(38) $S = R_{L|R}$ ist der ganze Abschluss von R in L.

(39) Es ist der Grad $[L : K] = 2$, und $L|K$ ist genau dann separabel, wenn $\mathrm{char}(k) \neq 2$ ist.

(40) $S' = k[t^2, t^3] = R[t^3]$ ist ein Noetherscher Teilring von S mit Quotientenkörper L, und jedes Primideal $\neq 0$ von S' ist maximal. Dennoch ist S' kein Dedekindring.

(41) Sei $\mathrm{char}(k) \neq 2$. Es ist $\{1, t\}$ eine R-Basis von S und die relative Diskriminante $D_{S|R} = (t^2)$ das von t^2 erzeugte (maximale) Ideal von R. Man folgere (oder zeige direkt), dass $(t^2) = t^2R$ das einzige Primideal $\neq 0$ von R ist, das in L verzweigt.

(42) Sei $\mathrm{char}(k) \neq 2$ und $0 \neq a \in k$. Das Primideal $\mathfrak{p} = (t^2 - a)R$ von R zerfällt genau dann in L (total), wenn $a \in k^{*2}$ ein Quadrat in k ist.

(43) Der Bewertungsring von $L = k(t)$ bezüglich der Gradbewertung v_∞ (Grad Nenner - Grad Zähler) ist die Lokalisierung des Rings $k[\frac{1}{t}]$ bei dem Primideal $\mathfrak{p} = \frac{1}{t}k[\frac{1}{t}]$.

(44) Ist $k = \mathbb{C}$, so zerfallen alle Primideale $\neq 0$, t^2R von R (total) in L. Ist $k = \mathbb{R}$, so zerfallen alle Primideale $\mathfrak{p} \neq 0$ von R mit Grad $\dim_{\mathrm{k}} \mathrm{R}/\mathfrak{p} \geq 2$ (total) in L.

Blatt 11 (12.01.2009)

(45) Aus der Tatsache, dass die Primzahl $p = 23$ in $L = \mathbb{Q}(e^{2\pi i/23})$ total verzweigt, aber jede andere Primzahl in L unverzweigt ist, folgere man, dass $K = \mathbb{Q}(\sqrt{-23})$ der (einzige) quadratische Zahlkörper in L ist.

(46) Seien $K \subseteq L$ wie in (45). Man zeige, dass $\mathfrak{p} = (2, \frac{1+\sqrt{-23}}{2})$ kein Hauptideal aber $\mathfrak{p}^3$ ein Hauptideal von R_K ist.

(47) Aus (46) folgere man, dass der 23-te Kreisteilungsring über $\mathbb{Z}$ kein Hauptidealring ist.

(48) Sei α eine reelle Wurzel von $f = X^3 - 3X + 1$ und $K = \mathbb{Q}(\alpha)$. Man zeige, dass f irreduzibel über $\mathbb{Q}$ und $K|\mathbb{Q}$ galoissch ist. (*Hinweis:* Auch $\alpha^2 - 2$ ist eine Wurzel von f; alternativ: K ist Teilkörper von $\mathbb{Q}(e^{2\pi i/9})$.) Aus dem zweiten Hinweis leite man $R_K = \mathbb{Z}[\alpha]$ ab und zeige, dass 2 in K träge ist und 19 in K total zerfällt.

Blatt 12 (19.01.2009)

Man bearbeite bis Montag, 26.01.2009, vier der folgenden Aufgaben schriftlich und möglichst viele bis Montag, 02.02.2009, mündlich.

(49) Seien $K \subseteq L$ algebraische Zahlkörper und p eine Primzahl. Verzweigt p total in L, so auch in K. Ist p unverzweigt in L, so auch in K.

(50) Sei M eine multiplikative Teilmenge und $\mathfrak{p}$ ein maximales Ideal des Integritätsbereichs R mit $M \cap \mathfrak{p} = \varnothing$. Man zeige $R + \mathfrak{p}_M = R_M$ und $R/\mathfrak{p} \cong R_M/\mathfrak{p}_M$.

(51) Man bestimme die Fundamentaleinheit des Rings der ganzen Zahlen von $\mathbb{Q}(\sqrt{14})$.

(52) Sei $\varepsilon_8 = e^{2\pi i/8}$ und $L = \mathbb{Q}(\varepsilon_8)$. Man zeige, dass $p = 2$ in L total verzweigt und dass sonst keine Primzahl dort verzweigt.

(53) Sei $L = \mathbb{Q}(\varepsilon_8)$ wie in (52). Man zeige, dass die Diskriminante D_L eine positive 2-Potenz und dass $\mathbb{Z}[\varepsilon_8]$ der Ring der ganzen Zahlen in L ist.

(54) Man gebe alle (drei) quadratischen Zahlkörper an, die in $L = \mathbb{Q}(\varepsilon_8)$ liegen.

(55) Man zeige, dass eine (ungerade) Primzahl p genau dann in $L = \mathbb{Q}(\varepsilon_8)$ total zerfällt, wenn $p \equiv 1 \pmod 8$ ist.

(56) Sei $\varepsilon_5 = e^{2\pi i/5}$ und $L = \mathbb{Q}(\varepsilon_5)$. Man zeige, dass in $\mathbb{Q}(\sqrt{5})$ ebenso wie in L nur die Primzahl $p = 5$ verzweigt und folgere $\mathbb{Q}(\sqrt{5}) = L^+ \subseteq L$.

(57) Man gebe alle Einheiten des Ring $\mathbb{Z}[\varepsilon_5]$ an.

(58) Sei $\varepsilon = e^{2\pi i/31}$, $L = \mathbb{Q}(\varepsilon)$ und $\mathfrak{P}$ ein Primideal von R_L über $p = 2$. Man zeige, dass der Zerlegungskörper K von $\mathfrak{P}$ der (einzige) Teilkörper von L mit $[K : \mathbb{Q}] = 6$ ist.

(59) Sei K wie in (58). Warum zerfällt $p = 2$ total in K ? Man zeige, dass R_K nicht monogen über $\mathbb{Z}$ ist, d.h., es gibt *kein* Element α mit $R_K = \mathbb{Z}[\alpha]$.

(60) Sei $L|\mathbb{Q}$ endlich galoissch. Gibt es eine Primzahl, die in L träge (prim) ist, so ist $\mathrm{Gal}(L|\mathbb{Q})$ zyklisch.

Blatt 13 (9.02.2009)

(61) Das Polynom $f = X^3+X^2-2X+8$ hat keine Wurzel in $\mathbb{Z}$ und ist daher irreduzibel über $\mathbb{Q}$. Sei α eine Wurzel von f in $\mathbb{C}$ und $K = \mathbb{Q}(\alpha)$, $R = R_K$. Man zeige:
(a) $D_f = D_{K|\mathbb{Q}}(1, \alpha, \alpha^2) = 4p$, wobei $p = 503$ eine Primzahl ist.
(b) $\beta = 4/\alpha$ ist eine Wurzel von $X^3 - X^2 + 2X + 8$.
(c) $D_{K|\mathbb{Q}}(1, \alpha, \beta) = p$, und es gilt $\alpha^2 = 2 - \alpha - 2\beta$ und $\beta^2 = -2 - 2\alpha + \beta$.
(d) Es gilt $2R = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ mit paarweise verschiedenen Primidealen $\mathfrak{p}_i$ von R.
Warum ist der Ring R nicht monogen ?

(62) Das Polynom $g = X^3 - X + 1$ ist irreduzibel über $\mathbb{Q}$ (Begründung!) und hat genau eine reelle Wurzel α. Sei $L = \mathbb{Q}(\alpha)$. Man zeige, dass $D_g = -23$ und (daher) $R_K = \mathbb{Z}[\alpha]$ ist, und die Klassenzahl $h_K = 1$. Ferner ist $L = K(\sqrt{-23})$ der Zerfällungskörper von f und $\mathrm{Gal}(L|\mathbb{Q}) \cong S_3$.

(63) Sei $h = X^4 - 8X + 12 \in \mathbb{Q}[X]$ und $G = \mathrm{Gal}_{\mathbb{Q}}(h)$. Man zeige:
(a) $h \bmod 5 = X^4+2X+2 = (X-1)(X^3+X^2+X+3)$ ist die Primfaktorzerlegung über $\mathbb{F}_5$.
(b) h hat keine Wurzel $x \in \mathbb{Z}$ und daher auch keine in $\mathbb{Q}$ (nach Gauß). (Es müsste $x \equiv 1 \,(\mathrm{mod}\, 5)$ nach (a) sein sowie x ein Teiler von $h(0) = 12$.)
(c) h ist irreduzibel über $\mathbb{Q}$ und $|G|$ durch 12 teilbar.
(d) Für die Diskriminante von h gilt $D_h = 2^{12} \cdot 3^4$. Man folgere $G \cong A_4$.
Zusatz. Wie kann man aus (d) die Existenz eines Zahlkörpers K mit $[K : \mathbb{Q}] = 4$ folgern, dessen einzige Teilkörper K und $\mathbb{Q}$ sind ?

(64) Sei $L = \mathbb{Q}(\sqrt{5}, \sqrt{-1})$, $S = R_L$ und $G = \mathrm{Gal}(L|\mathbb{Q})$.
(a) Man zeige $S = \mathbb{Z}[\frac{1+\sqrt{5}}{2}, \sqrt{-1}]$. Man berechne D_L und zeige, dass 2 und 5 die einzigen in L verzweigenden Primzahlen sind.
(b) Man berechne die Zerlegungsgruppen in G für 2 und 5 und den Frobenius $(p, L|\mathbb{Q})$ für alle übrigen Primzahlen p.
(c) Man zeige, dass kein Primideal von $K = \mathbb{Q}(\sqrt{-5})$ in L verzweigt. (L ist der sog. Hilbertsche Klassenkörper von K.)

(65) Bekanntlich (Vorlesung 9.5) ist $\mathbb{Z}[\sqrt[3]{2}]$ der Ring der ganzen Zahlen des (reellen) Zahlkörpers $K = \mathbb{Q}(\sqrt[3]{2})$. Man zeige, dass die Klassenzahl $h_K = 1$ ist.

(66) Man zeige, dass $K = \mathbb{Q}(\sqrt{-23})$ die Klassenzahl 3 hat.

(67) Man zeige, dass die Galoisgruppe des rationalen Polynoms $X^5 + \frac{6}{5}X^2 + 3$ die symmetrische Gruppe S_5 ist.

Test (2.02.2009)

(1) Welche der folgenden komplexen Zahlen sind ganz über $\mathbb{Z}$? - $\frac{3+\sqrt{5}}{2}$, $\frac{3+i\sqrt{5}}{2}$, $2\cos\frac{2\pi}{7}$.

(2) Man zeige, dass $\mathfrak{p} = (2, 1+\sqrt{-5})$ kein Haupideal von $\mathbb{Z}[\sqrt{-5}]$ ist, dass aber $\mathfrak{p}^2$ ein Hauptideal ist.

(3) Man bestimme die Fundamentaleinheit des Rings der ganzen Zahlen von $\mathbb{Q}(\sqrt{21})$.

(4) Sei α die positive reelle Wurzel von $X^4 - 2$ und $K = \mathbb{Q}(\alpha)$. Man zeige, dass 2 in K total verzweigt.

(5) Sei $K = \mathbb{Q}(\alpha)$ wie in (4). Man zeige, dass keine ungerade Primzahl in K verzweigt und dass $R_K = \mathbb{Z}[\alpha]$ ist.

(6) Sei $K = \mathbb{Q}(\alpha)$ wie in (4), (5). Man gebe explizit die Primideale $\mathfrak{p} \neq \mathfrak{p}'$ von R_K über der Primzahl 3 an ($3R_K = \mathfrak{p}\mathfrak{p}'$).

(7) Sei $K = \mathbb{Q}(\alpha)$ wie in (4), (5), (6). Sei $L|\mathbb{Q}$ die Galoishülle von $K|\mathbb{Q}$, d.h., der Zerfällungskörper von X^4-2 (etwa in $\mathbb{C}$). Man zeige, dass keine ungerade Primzahl in L verzweigt und (daher) $\pm D_L$ eine 2-Potenz ist.

(8) Sei L wie in (7). Man zeige, dass $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$ und $\mathbb{Q}(\sqrt{-2})$ die einzigen quadratischen Zahlkörper in L sind.

(9) Sei L wie in (7), (8). Man zeige, dass der Trägheitskörper eines Primideals $\mathfrak{P}|2$ von R_L entweder $\mathbb{Q}$ oder ein quadratischer Zahlkörper ist. Man schließe das Letztere aus und zeige damit, dass 2 in L total verzweigt.

(10) Sei L wie in (7), (8), (9). Man zeige, dass keine Primzahl in L träge (prim) ist.