Professor Dr. Jürgen Ritter
Lehrstuhl für Algebra und Zahlentheorie
Institut für Mathematik · Universität Augsburg

Protokoll zur Vorlesung Zahlentheorie 1 · Sommersemester 2007 [1]

LITERATUREMPFEHLUNGEN:

Borewics und Šafarevič, Zahlentheorie (Birkhäuser)

Fröhlich und Taylor, Algebraic number theory (Cambridge University Press)

Hasse, Number Theory (Springer Grundlehren 229)

Janusz, Algebraic Number Fields (Academc Press)

Lang, Algebraic Number Theory (Addison-Wesley)

Leutbecher, Zahlentheorie (Springer)

Neukirch, Algebraische Zahlentheorie (Springer)

Serre, Corps locaux (Hermann Paris)

1. GANZE ALGEBRAISCHE ZAHLEN

Es sei $R \subset S$ ein Paar von nullteilerfreien Ringen (mit derselben 1); insbesondere kann S also als R-Modul angesehen werden. Wir setzen $K = \mathrm{Quot}(R)$ und $L = \mathrm{Quot}(S)$. Natürlich gilt $K \subset L$.

DEFINITION. *$s \in S$ heißt ganz über R, wenn es ein normiertes Polynom $f(x) \in R[x]$ mit Nullstelle s gibt. S heißt ganz über R, falls alle $s \in S$ über R ganz sind.*

LEMMA. *$s \in S$ ist genau dann ganz über R, falls es einen endlich erzeugten R-Teilmodul $M \neq 0$ von S mit $sM \subset M$ gibt. Insbesondere ist der Begriff "ganz über R" verträglich mit $+, -, \times$.*

Beispiele von über R ganzen Elementen: Ist $s \in S$ algebraisch über K, so ist rs ganz für ein geeignetes $0 \neq r \in R$. Natürlich ist jedes $r \in R$ ganz über R.

LEMMA. 1. *Der Begriff* ganz *ist transitiv, d.h. im Falle dreier Ringe $R \subset S \subset T$ gilt: ist $t \in T$ ganz über S und S ganz über R, so ist t ganz über R.*

2. *Der Begriff* ganz *ist verträglich mit Homomorphismen: Ist S ganz über R und $f : S \to S_1$ ein Ringhomomorphismus (mit f(1)=1), so ist $f(S)$ über $f(R)$ ganz.*

3. *Im Fall, daß L/K eine endliche, separable Körpererweiterung ist, sind die Koeffizienten des irreduziblen Polynoms eines über R ganzen Elementes $s \in L$ ganz über R, insbesondere also $Sp_{L/K}(s)$ und $N_{L/K}(s)$.*

[1] Dank an Simone Schuierer und Andreas Nickel

DEFINITION UND LEMMA . *Die Menge $\tilde{R}$ aller über R ganzen Elemente von L heißt der ganze Abschluß von R in L. Dies ist ein Ring. R heißt ganz abgeschlossen in L, falls $R = \tilde{R}$ gilt.*

Insbesondere sind ZPE-Ringe in ihrem Quoptientenkörper ganz abgeschlossen.

SATZ. *R sei ein in Quot$(R) = K$ ganz abgeschlossener, noetherscher Integritätsbereich und L/K eine endliche, separable Körpererweiterung. Dann ist der ganze Abschluß $\tilde{R}$ von R in L endlich erzeugt als R-Modul (und insbesondere ein noetherscher Ring).*

Im Beweis geht wesentlich die nichtausgeartete Bilinearform $(x, y) \mapsto Sp_{L/K}(xy)$ auf L ein.

FOLGERUNG. *Ist R ein Hauptidealring, so ist $\tilde{R}$ ein freier R-Modul vom Rang $[L : K]$.*

LEMMA. *M sei eine multiplikativ abgeschlossene Teilmenge von R mit $1 \in M$. Ist S ganz über R, so ist S_M ganz über R_M. Ist $S = \tilde{R}$ in L, so gilt $S_M = \tilde{R}_M$ in L.*

Es sei $\mathfrak{p}$ ein Primideal in R und S ganz über R.

LEMMA. *$\mathfrak{p}S \neq S$; genauer: es gibt Primideale $\mathfrak{P}$ von S mit $\mathfrak{p} = \mathfrak{P} \cap R$. Des weiteren:*

$$\mathfrak{p} \text{ maximal in } R \iff \mathfrak{P} \text{ maximal in } S\,.$$

DEDEKINDRINGE :

DEFINITION. *Ein Ring $\mathfrak{o}$ heißt Dedekindring, falls $\mathfrak{o}$*

1. *nullteilerfrei,*
2. *noethersch,*
3. *ganz abgeschlossen (in $K = \mathrm{Quot}(\mathfrak{o})$)*
4. *und falls jedes Primideal $\neq 0$ in $\mathfrak{o}$ maximal ist.*

Hauptbeispiele von Dedekindringen sind (neben Hauptidealringen) die ganzen Abschlüsse von $\mathbb{Z}$ in Zahlkörpern K, also in endlichen Körpererweiterungen $K/\mathbb{Q}$.

SATZ. *In einem Dedekindring $\mathfrak{o}$ ist jedes Ideal $\neq 0$ eindeutig als Produkt von endlich vielen Primidealen $\neq 0$ darstellbar.*

Das verallgemeinert die ZPE-Eigenschsft von Hauptidealringen. – Für den Beweis (und für spätere Ausführungen) ist der Begriff eines *gebrochenen* Ideals $\mathfrak{g}$ des Dedekindringes $\mathfrak{o}$ nützlich: dies ist ein endlich erzeugter $\mathfrak{o}$-Untermodul in $K = \mathrm{Quot}(\mathfrak{o})$. Gleichbedeutend ist $\mathfrak{g} = r^{-1} \cdot \mathfrak{a}$ mit einem $0 \neq r \in \mathfrak{o}$ und einem Ideal $0 \neq \mathfrak{a}$ von $\mathfrak{o}$. Wir vereinbaren: (gebrochene) Ideale eines Dedekindringes seien ab jetzt stets $\neq 0$; wir zählen also das Nullideal extra.

Obiger Satz folgt nun im wesentlichen aus

für Primideale $\mathfrak{p}$ gilt $\mathfrak{o} \subsetneqq \mathfrak{p}^{-1} \stackrel{\text{def}}{=} \{a \in K : a\mathfrak{p} \subset \mathfrak{o}\}$.

FOLGERUNG. 1. *Zu jedem Ideal $\mathfrak{a} \subset \mathfrak{o}$ gibt es ein gebrochenes Ideal $\mathfrak{a}^{-1}$ mit $\mathfrak{a} \cdot \mathfrak{a}^{-1} = \mathfrak{o}$.*

2. *Die gebrochenen Ideale eines Dedekindringes $\mathfrak{o}$ bilden eine freie abelsche Gruppe $\mathfrak{I}_\mathfrak{o}$ mit den Primidealen als Erzeugenden.*

3. *Hat der Dedekindring $\mathfrak{o}$ nur endlich viele Primideale, so ist er schon ein Hauptidealring.*

4. *Jedes Ideal $\mathfrak{a}$ von $\mathfrak{o}$ ist von zwei Elementen erzeugt, wobei eines beliebig $\neq 0$ in $\mathfrak{a}$ vorgegeben werden darf.*

LEMMA. *Ist $\mathfrak{o}$ ein Dedekindring und $1 \in M \subset \mathfrak{o}$ eine multiplikativ abgeschlossene Menge, so ist die zugehörige Lokalisierung $\mathfrak{o}_M$ auch ein Dedekindring. Die Abbildung $\mathfrak{g} \mapsto \mathfrak{g}_M$ ist ein Gruppenepimorphismus $\mathfrak{I}_\mathfrak{o} \twoheadrightarrow \mathfrak{I}_{\mathfrak{o}_M}$ mit Kern $\{\mathfrak{g} : \mathfrak{g} \cap M \neq \emptyset\}$.*

DEFINITION. *$L \supset K$ seien endliche Körpererweiterungen von $\mathbb{Q}$. Die ganzen Abschlüsse von $\mathbb{Z}$ in L und K werden mit $\mathfrak{o}_L$ bzw. $\mathfrak{o}_K$ bezeichnet. Dies sind Dedekindringe und zugleich freie $\mathbb{Z}$-Moduln vom Rang $[L : \mathbb{Q}]$ bzw. $[K : \mathbb{Q}]$.*

Beispiel: $\mathfrak{o}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \not\equiv 1 \bmod 4 \\ \mathbb{Z}[-\frac{1}{2} + \frac{1}{2}\sqrt{d}] & d \equiv 1 \bmod 4 \end{cases}$, wobei $1 \neq d \in \mathbb{Z}$ wie üblich quadratfrei sei.

Es gilt $\mathfrak{o}_\mathbb{Q} = \mathbb{Z}$; der ganze Abschluß von $\mathfrak{o}_K$ in L ist $\mathfrak{o}_L$; $\mathfrak{o}_L$ ist ein endlich erzeugter (torsionsfreier) $\mathfrak{o}_K$-Modul. Über jedem Primideal $\mathfrak{p}$ von $\mathfrak{o}_K$ liegen nur endlich viele $\mathfrak{p}$ enthaltende Primideale $\mathfrak{P}_1, \cdots, \mathfrak{P}_g$ von $\mathfrak{o}_L$, nämlich die in der Produktzerlegung

$$\mathfrak{p}\mathfrak{o}_L = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_g^{e_g}$$

auftretenden; natürlich ist deren Anzahl $g \geq 1$ abhängig von $\mathfrak{p}$. Die Zahl e_i heißt Verzeigungsindex von $\mathfrak{P}_i$ bezüglich K; die Zahl g die Zerlegungszahl von $\mathfrak{p}$ bezüglich L.

Ist $\mathfrak{P}$ Primideal in $\mathfrak{o}_L$ und $\mathfrak{p}$ eines in $\mathfrak{o}_K$, so sagen wir $\mathfrak{P}|\mathfrak{p}$, falls $\mathfrak{P} \supset \mathfrak{p}$ (oder gleichbedeutend, falls $\mathfrak{P} \cap \mathfrak{o}_K = \mathfrak{p}$).

LEMMA. 1. *$\mathfrak{o}_K/\mathfrak{p}$ ist ein endlicher Körper. Seine Charakteristik ist die Primzahl p, die in $\mathfrak{p}$ liegt, also $\mathfrak{p}|p$.*

2. *$\mathfrak{P}|\mathfrak{p} \Longrightarrow \mathfrak{o}_L/\mathfrak{P}$ ist eine endliche Körpererweiterung von $\mathfrak{o}_K/\mathfrak{p}$ (vom Grad $f_\mathfrak{P}$, dem Restklassengrad von $\mathfrak{P}$ bezüglich K).*

3. *Ist L/K galoissch mit Gruppe $G = G_{L/K}$ und gilt $\mathfrak{P}|\mathfrak{p}$, so sind die (nicht notwendig verschiedenen) $\sigma(\mathfrak{P}) = \{\sigma(a) : a \in \mathfrak{P}\}$, für $\sigma \in G$, genau alle über $\mathfrak{p}$ liegenden Primideale. Diese haben alle den gleichen Verzweigungsindex und alle den gleichen Restklassengrad bezüglich K.*

Bemerkung: Wir werden später für Zahlkörper sehen: $\sum_{i=1}^{g} e_i f_i = [L : K]$ für jedes $\mathfrak{p}$.

DEFINITION. 1. *$\mathfrak{H}_K \overset{\text{def}}{=} \mathfrak{H}_{\mathfrak{o}_K}$ ist die von allen gebrochenen Hauptidealen erzeugte Untergruppe von $\mathfrak{I}_K \overset{\text{def}}{=} \mathfrak{I}_{\mathfrak{o}_K}$, also $\mathfrak{H}_K = \{a \cdot \mathfrak{o}_k : 0 \neq a \in K\}$.*

2. *Der Quotient $\mathrm{cl}_K = \mathfrak{I}_K/\mathfrak{H}_K$ heißt die (Ideal-) Klassengruppe von K.*

Bemerkung: Wir werden im Zahlkörperfall sehen, daß cl_K eine endliche (abelsche) Gruppe ist; ihre Ordnung k_K heißt die Klassenzahl von K. Beispiel: $h_\mathbb{Q} = 1$. Berechnen kann man h_K mit Hilfe des Residuums der Zetafunktion von K (siehe Kapitel 3).

2. Der Dirichletsche Einheitensatz

Das Rechnen in $\mathfrak{o}_K$ ist aus zwei Gründen schwerer als in $\mathbb{Z}$:

1. In $\mathfrak{o}_K$ gilt die eindeutige Primfaktorzerlegung nicht für Elemente, sondern nur für Ideale. Das erzeugt das Hindernis cl_K.

2. Einheiten in $\mathfrak{o}_K$ entgehen dem Idealbegriff. In $\mathbb{Z}$ sind dies nur ± 1.

Seien $K \supseteq k$ endliche Erweiterungen von $\mathbb{Q}$ und K/k galoissch mit Gruppe G. Den ganzen Abschluß von $\mathbb{Z}$ in K bezeichnen wir mit $\mathfrak{o}_K$, seine Einheitengruppe $\mathfrak{o}_K^\times$ mit $E = E_K$.

Wir interessieren uns für die Struktur von E als $\mathbb{Z}G$-Modul, untersuchen aber zunächst nur den $\mathbb{Z}$-Modul E.

Nach dem Satz vom primitiven Element ist $K = \mathbb{Q}(\alpha)$ für geeignetes $\alpha \in K$ und $I_{K/\mathbb{Q}} = \{\text{Isomorphismen von } K \text{ (über } \mathbb{Q}) \text{ nach } \mathbb{C}\} = \{\sigma_1, \sigma_2, \ldots, \sigma_r, \sigma_{r+1}, \overline{\sigma_{r+1}}, \ldots, \sigma_{r+s}, \overline{\sigma_{r+s}}\}$ mit $r + 2s = |I_{K/\mathbb{Q}}| = [K : \mathbb{Q}] =: n$ und

$$\begin{aligned} &\sigma_i(\alpha) \in \mathbb{R} \text{ für } i \le r, \\ &\sigma_i(\alpha) \in \mathbb{C} \setminus \mathbb{R} \text{ für } i \ge r+1 \\ &\overline{\sigma_{r+j}}(\alpha) = \overline{\sigma_{r+j}(\alpha)} \text{ für } 1 \le j \le s\,. \end{aligned}$$

Wir bezeichnen übrigens auch die σ_i für $1 \le i \le r$ sowie die Paare $\sigma_i, \overline{\sigma_i}$ für $r+1 \le i \le r+s$ mit $\mathfrak{p}_i$ (der Grund hierfür wird erst später deutlich werden.)

Die Wirkung der Galoisgruppe G auf K werde exponentiell notiert: a^σ für $a \in K, \sigma \in G$. Darüber hinaus operiert G auf $I_{K/\mathbb{Q}}$: für $\sigma_i \in I_{K/\mathbb{Q}}$ und $\sigma \in G$ setze $\sigma_i\sigma = \sigma_{i'}$ mit $a^{\sigma_{i'}} = a^{\sigma^{-1}\sigma_i}$ $(\forall\, a \in K)$. Beachte: $\sigma_i\sigma = \sigma_{i'} \Longrightarrow \overline{\sigma_i}\sigma = \overline{\sigma_{i'}}$.).

DEFINITION. *$S_\infty \overset{\text{def}}{=} \{\mathfrak{p}_1, \ldots, \mathfrak{p}_{r+s}\}$; S_∞ besitzt also eine G-Wirkung von rechts.*
$\mathbb{Z}S_\infty \overset{\text{def}}{=} \{\sum_{i=1}^{r+s} z_i\mathfrak{p}_i \ : z_i \in \mathbb{Z}\}$ ist daher ein $\mathbb{Z}G$-Rechtsmodul.
(Die Gleichheit in $\mathbb{Z}S_\infty$ ist so definiert: $\sum_{i=1}^{r+s} z_i\mathfrak{p}_i = \sum_{i=1}^{r+s} z_i'\mathfrak{p}_i \iff z_i = z_i'$ $(\forall\, i)$.)

DEFINITION. *Sei $a \in K$. Setze $|a|_i := |a^{\sigma_i}|$ für $1 \le i \le r$ und $|a|_i := |a^{\sigma_i}|^2$ für $r+1 \le i \le r+s$.*

Betrachte nun die Abbildung

$$\lambda :\ E \to \mathbb{R} \otimes_{\mathbb{Z}} \mathbb{Z}S_\infty = \{\sum_{i=1}^{r+s} r_i\mathfrak{p}_i \ : r_i \in \mathbb{R}\} = \mathbb{R}S_\infty,\ e \mapsto \sum_{i=1}^{r+s} \log|e|_i\mathfrak{p}_i\,.$$

Beobachtungen:

1. $\lambda(e_1e_2) = \lambda(e_1) + \lambda(e_2)$

2. $\lambda(E) =: \mathfrak{E} \subseteq H := \mathbb{R} \otimes_{\mathbb{Z}} \Delta S_\infty$.
   H ist eine Hyperebene in dem reellen Vektorraum $V = \mathbb{R}S_\infty$ mit Basis $\mathfrak{p}_i$, $1 \le i \le r+s =: m$; $H = \ker[\mathfrak{p}_i \mapsto 1]$. ($\mathfrak{E}$ ist insbesondere torsionsfrei.)

3. $\lambda(e^\sigma) = \lambda(e)^\sigma$ für $\sigma \in G$

[*zu 2.:* Betrachte $\mathbb{Z}S_\infty \to \mathbb{Z}$, $\mathfrak{p}_i \mapsto 1, \sum_{i=1}^{r+s} z_i\mathfrak{p}_i \mapsto \sum_{i=1}^{r+s} z_i$. Diese additive und G-verträgliche Abbildung heißt *Augmentation*. Ihren Kern bezeichnen wir mit ΔS_∞, also $\Delta S_\infty = \{\sum_{i=1}^{r+s} z_i\mathfrak{p}_i : \sum_{i=1}^{r+s} z_i = 0\}$. Dies ist ein $\mathbb{Z}G$-Modul und $\mathbb{R} \otimes_{\mathbb{Z}} \Delta S_\infty = H$.]

LEMMA. *Falls B eine beschränkte Teilmenge von V ist, so sind $\mathfrak{E} \cap B$ und $\lambda^{-1}(\mathfrak{E} \cap B)$ endlich.*

FOLGERUNG. *$ker(\lambda) = \{e \in E : \log|e|_i = 0 \ (\forall i)\}$ ist endlich. Als Untergruppe von $K^\times$ ist $ker(\lambda)$ somit zyklisch; genauer $ker(\lambda) = \mu_K$ = Gruppe der Einheitswurzeln in K .*

LEMMA. *$\mathfrak{E}$ ist endlich erzeugt, und zwar von reell unabhängigen Vektoren in H.*

FOLGERUNG. $E \simeq \mu_K \otimes \mathbb{Z}^d$, $d \leq m-1 = \dim H$.

SATZ. (Dirichletscher Einheitensatz) $d = m-1$, *i.e.*, $E \simeq \mu_K \oplus \mathbb{Z}^{r+s-1}$.

Die $\mathbb{Z}G$-Struktur von E ist bis heute ein Geheimnis; es gilt allerdings

FOLGERUNG. *$e \mapsto \lambda(e)$ induziert eine $\mathbb{R}G$-Isomorphie $\mathbb{R} \otimes_{\mathbb{Z}} E \underset{\mathbb{R}G}{\simeq} \mathbb{R} \otimes_{\mathbb{Z}} \Delta S_\infty$.*

Bevor wir die Beweisschritte zum Einheitensatz skizzieren, benötigen wir noch eine

DEFINITION. *Sei W ein reeller d-dimensionaler Vektorraum mit Basis $e_\nu = 1, \ldots, d$. L heißt ein volles Gitter, falls $L = \{\sum_{\mu=1}^d z_\mu l_\mu : z_\mu \in \mathbb{Z}\}$ mit über $\mathbb{R}$ linear unabhängigen l_μ gilt. $F_L := \{\sum_{\mu=1}^d r_\mu l_\mu : 0 \leq r_\mu \leq 1\}$ heißt die Fundamentalmasche des Gitters. Wir setzen $\mathrm{vol}(L) = \mathrm{vol}(F_L) = |\det(\alpha_{\mu\nu})|$, falls $l_\mu = \sum \alpha_{\mu\nu} e_\nu$. Beachte, daß $\mathrm{vol}(L)$ unabhängig von der Wahl der l_μ für L ist.*

Um den Dirichletschen Einheitensatz zu beweisen, müssen wir also zeigen, daß $\mathfrak{E} \subseteq H$ ein volles Gitter ist. Dies folgt im wesentlichen aus dem

LEMMA. *Es existieren $e_1, \ldots, e_{r+s-1} \in E$ mit $\log|e_j|_j > \sum_{i \neq j} |\log|e_j|_i| \ \forall j$.*

Somit ist also $(\log|e_j|_i) =: (\alpha_{ji})$ eine reelle $r+s-1 \times r+s-1$ - Matrix mit positiven Einträgen auf der Hauptdiagonalen und $\alpha_{jj} > \sum_{i \neq j} |\alpha_{ji}|$. Für derartige Matrizen gilt, wie aus der linearen Algebra bekannt, $\det(\alpha_{ij}) \neq 0$. Dies beweist dann den Dirichletschen Einheitensatz.

Der Beweis des Lemmas benötigt mehrere Schritte.
Zunächst betrachten wir die Abbildung

$$\Phi : \ K \to \mathbb{R}^n,\ a \mapsto (a^{\sigma_1}, \ldots, a^{\sigma_r}, \Re(a^{\sigma_{r+1}}), \Im(a^{\sigma_{r+1}}), \ldots)\,.$$

$M = \oplus_{j=1}^n \mathbb{Z} m_j$ sei ein volles Gitter in K. Die Diskriminante von M ist definiert als $d(M) = \det(m_j^{\sigma_k})^2 \in \mathbb{C}$, wobei σ_k die Isomorphismenmenge $I_{K/\mathbb{Q}}$ durchläuft (gleichwertig, aber vielleicht schöner, ist diese Definition: $d(M) = \det(\mathrm{Sp}_{K/\mathbb{Q}}(m_i m_j))_{i,j}$).

LEMMA (*). *$\Phi(M)$ ist ein volles Gitter in $\mathbb{R}^n$ vom Volumen $2^{-s}\sqrt{|d(M)|}$.*

Der Faktor 2^{-s} entsteht durch die Identifizierung $\mathbb{R}^n = \mathbb{R}^r \times \mathbb{C}^s$ über $(\Re(c), \Im(c)) \leftrightarrow (c, \overline{c})$ und der Berechnung der Determinante der reellen Matrix über $\mathbb{C}$: elementare Umformungen und das Herausziehen von i^{-s} und 2^{-s} verändert die erste Matrix in $(m_j^{\sigma_k})$.

Wähle nun für $1 \leq j \leq r+s$ Zahlen $c_j > 0$ mit $\prod_{j=1}^{r} c_j \prod_{j=r+1}^{r+s} c_j^2 \geq (\frac{2}{\pi})^s \sqrt{|d(M)|}$. Dann existiert ein $0 \neq a \in M$ mit $|a^{\sigma_j}| \leq c_j$. Denn die Menge $\{(\alpha_1, \ldots, \alpha_{r+s}) = v \in \mathbb{R}^r \times \mathbb{C}^s : |\alpha_j| \leq c_j\}$ hat das Volumen $\prod_{j=1}^{r} (2c_j) \prod_{j=r+1}^{r+s} (\pi c_j^2) \geq 2^{r+s}\sqrt{|d(M)|} = 2^n 2^{-s}\sqrt{|d(M)|}$.

Die Behauptung des vorletzten Lemmas folgt jetzt aus Lemma(*) und dem

SATZ. (Minkowski) *Sei W wie oben, L ein volles Gitter und $C \subset W$ beschränkt, konvex und symmetrisch um 0. Dann gilt:* $\mathrm{vol}(C) > 2^d \mathrm{vol}(L) \Rightarrow \exists L \ni l \neq 0$ *in* M. *Ist* C *zudem kompakt, so genügt es,* $\mathrm{vol}(M) \geq 2^d \mathrm{vol}(L)$ *zu fordern.*

Wir setzen $M = \mathfrak{o}_K$ und bezeichnen $d(M)$ mit d_K. Dann wählen wir $c \geq \sqrt{|d_K|}$, und, für festes $j, 1 \leq j \leq r+s-1$, und beliebiges $k \in \mathbb{N}$

$$\begin{cases} c_j(k) = c^{k+1} & j \leq r \\ c_j(k)^2 = c^{k+1} & j \geq r+1 \end{cases}, \; c_{r+s}(k) = c^{-k}, \; c_i(k) = 1 \; (\forall\, 1 \leq i \neq j \leq r+s-1)\,.$$

Dann ist $\prod\limits_{j=1}^{r} c_i(k) \prod\limits_{j=r+1}^{r+s} c_i(k)^2 = c \geq \sqrt{|d_K|}$.
Somit existiert also $0 \neq a_k \in \mathfrak{o}_K$ mit $|a_k^{\sigma_i}| \leq c_i(k)$, also $1 \leq |N_{K/\mathbb{Q}}(a_k)| \leq c$. Da die Hauptideale (b) in $\mathfrak{o}_K$ mit $N_{K/\mathbb{Q}}(b) = \nu$ zwischen $\nu\mathfrak{o}_K$ und $\mathfrak{o}_K$ liegen, gibt es nur endlich viele Hauptideale mit Erzeugern mit Norm $\leq c$ (eindeutige Primidealzerlegung). Und da wir unendlich viele a_k haben, gibt es also natürliche Zahlen $k, t \geq r+s$ mit $a_{k+t} = \varepsilon_j a_k, \; \varepsilon_j \in E$. Mit $|N_{K/\mathbb{Q}}(a_k)| \geq 1$ (und $e_j \overset{\text{def}}{=} 1$ oder 2, je nachdem $j \leq r$ ist oder nicht) folgt nun der Reihe nach

$$\begin{array}{l} c^{k+1} \geq |a_k^{\sigma_j}|^{e_j} = |N_{K/\mathbb{Q}}(a_k)| / \prod_{\nu \neq j} |a_k^{\sigma_\nu}|^{e_\nu} \geq c^k \\ 1 \geq |a_k^{\sigma_i}|^{e_i} = |N_{K/\mathbb{Q}}(a_k)| / \prod_{\nu \neq i} |a_k^{\sigma_\nu}|^{e_\nu} \geq c^{-1} \quad \text{für } i \neq j, r+s-1 \\ |\varepsilon_j^{\sigma_j}|^{e_j} = |a_{k+t}^{\sigma_j}|^{e_j} / |a_k^{\sigma_j}|^{e_j} \geq c^t > c^{r+s-1} \\ c \geq |\varepsilon_j^{\sigma_i}|^{e_i} \geq c^{-1} \quad \text{für } i \neq j, r+s-1 \\ \log |\varepsilon_j^{\sigma_j}|^{e_j} > (r+s-1) \log c \geq \sum_{i \neq j} |\log |\varepsilon_j^{\sigma_i}|^{e_i}| \; . \end{array}$$

Beispiel: $[K : \mathbb{Q}] = 2$, $K = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$ quadratfrei. Für $d > 0$ ist $E \simeq \langle \pm 1 \rangle \times \mathbb{Z}$, für $d < 0$ ist $E = \mu_K = \mathbb{Z}/2$, $\mathbb{Z}/6$, $\mathbb{Z}/4$, je nachdem ob $-d = 2$ oder > 4, oder $d = -3$, oder $d = -1$.
Sei nun $d > 0$, also $K \subset \mathbb{R}$, und e eine Einheit $\neq 1$. Unter allen *Grundeinheiten* (also solchen Einheiten, die den freien Bestandteil $\mathbb{Z}$ in E erzeugen) gibt es genau eine vom Betrag > 1. Berechnet werden kann sie so: Setze $e = x + y\sqrt{d}$. Jede andere Einheit > 1 ist dann $= e^n = x_n + y_n\sqrt{d}$ und es gilt

$$x_{n+1} + y_{n+1}\sqrt{d} = (xx_n + dyy_n) + (xy_n + yx_n)\sqrt{d}\,.$$

Im Fall $d \not\equiv 1 \bmod 4$ sind x und y in $\mathbb{Z}_{>0}$, und deshalb auch x_n, y_n, weshalb die Folge (x_n) streng monoton wächst. Im Fall $d \equiv 1 \bmod 4$ gilt daßelbe Argument, sofern nur $x \geq 1$ ist. Die einzige Ausnahme, $x = \frac{1}{2}$, führt zu $d = 5$ und $e = \frac{1}{2} + \frac{1}{2}\sqrt{5}$. Mit anderen Worten: $e = x + y\sqrt{d}$ hat die kleinste Komponente x unter allen Einheiten > 1. Beachte noch: $e = \frac{1}{2}(x + y\sqrt{d})$ ist Einheit, genau wenn $x^2 - dy^2 = \pm 4$ (mit $x, y \in \mathbb{Z}$) gilt.

Bemerkung. Man kann den Dirichletschen Einheitensatz leicht wie folgt verallgemeinern. Statt nur $S_\infty = \{\mathfrak{p}_1 \ldots, \mathfrak{p}_{r+s}\}$ zu betrachten, arbeite man mit einer endlichen Menge $S \supset S_\infty$, indem man noch endlich viele Primideale $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ aus $\mathfrak{o}_K$ zu S_∞ hinzunimmt und nun die sogenannte S-Einheitengruppe E_S von K betrachtet:

$E_S = \{e \in K :$ in der Primidealzerlegung des gebrochenen Hauptideals $e\mathfrak{o}_K$ kommen nur die $\mathfrak{q}_j$ vor $\}$,

E_S ist damit die Einheitengruppe des Dedekindringes $\mathfrak{o}_S \overset{\text{def}}{=} \{a \in K :$ in der Primidealzerlegung des gebrochenen Hauptideals $a\mathfrak{o}_K$ haben höchstens die $\mathfrak{q}_j$ negative Exponenten$\}$. Beachte $\mathfrak{o}_{S_\infty} = \mathfrak{o}_K$.

Das Analogon zum Dirichletschen Satz lautet nun $E_S \simeq \mu_K \times \mathbb{Z}^{|S|}$ und sein Beweis verläuft wie früher unter Verwendung der neuen Abbildung $\lambda : E_S \to \mathbb{R}^{|S|}$, $e \mapsto \sum_{1\le i\le r+s} \log|e|_{\mathfrak{p}_i} + \sum_{1\le j\le m} \log|e|_{\mathfrak{q}_j}\mathfrak{q}_j$ mit $|e|_{\mathfrak{q}_j} = q_j^{-\varepsilon_j}$, falls q_j die in $\mathfrak{q}_j$ enthaltene Primzahl und ε_j die Vielfachheit des Faktors $\mathfrak{q}_j$ in $e\mathfrak{o}_K$ ist.

Ist K/k galoissch mit Gruppe G und S stabil unter G (i.e., $\sigma(\mathfrak{q}_j) \in S$ $(\forall\, j)$) so sind E_K und E_S $\mathbb{Z}G$-Moduln und der Dirichletsche Satz liefert (zusammen mit dem Satz von Noether-Deuring aus der Darstellungstheorie endlicher Gruppen) die Existenz eines $\mathbb{Z}G$-Monomorphismus $\varphi : \Delta S \to E_S$, wobei, wie früher mit S_∞ anstelle von S,

$$\Delta S = \{\sum_{\mathfrak{p}\in S} z_{\mathfrak{p}}\mathfrak{p} : z_{\mathfrak{p}} \in \mathbb{Z}\,,\ \sum_{\mathfrak{p}\in S} z_{\mathfrak{p}} = 0\} \subset H_S \subset \mathbb{R}S \simeq \mathbb{R}^{|S|}\,.$$

Nur in wenigen Fällen kann man explizite φ tatsächlich angeben.

3. Die analytische Klassenzahlformel

Unsere Hauptinformation über die Klassengruppe cl_K beschränkt sich auf deren Ordnung.

Definition. *Die Dedekindsche Zetafunktion des Zahlkörpers K ist durch die Reihe*
$\zeta_K(x) = \sum_{\mathfrak{a}\subset\mathfrak{o}_K} \frac{1}{N(\mathfrak{a})^x}$ *erklärt. Hierbei ist* $N(\mathfrak{a}) \stackrel{\text{def}}{=} |\mathfrak{o}_K/\mathfrak{a}|$ *und* $x \in \mathbb{C}$, $\Re(x) > 1$.

Für $K = \mathbb{Q}$ ist $\zeta_{\mathbb{Q}}$ die uns bereits bekannte Riemannsche Zetafunktion $\zeta(x) = \sum_{k=1}^{\infty} \frac{1}{k^x}$. Die Konvergenz von $\zeta_K(x)$ beweist man analog zum Fall $K = \mathbb{Q}$; wie dort hat man ein Eulerprodukt $\zeta_K(x) = \prod_{\mathfrak{p}\subset\mathfrak{o}_K}(1 - N(\mathfrak{p})^{-x})^{-1}$.

Definition. *Der Regulator R_K des Zahlkörpers K ist der Betrag eines $r+s-1$-Minor der Matrix* $(\log|e_i|_j)_{\substack{1\le i\le r+s-1\\ 1\le j\le r+s}}$, *wobei die e_i Fundamentaleinheiten von K sind.*

Bemerkung. Die Definition ist sowohl unabhängig von der Wahl des Minors als auch von der der Fundamentaleinheiten. Die erstgenannte Unabhängigkeit resultiert aus $\sum_j \log|e_i|_j = 0$, die letztgenannte aus der Basiseigenschaft der e_i.

Satz. *(Analytische Klassenzahlformel)*

$$\mathrm{res}_{x=1}\zeta_K(x) = lim_{x\searrow 1}(x-1)\zeta_K(x) = \frac{2^{r+s}\pi^s R_K h_K}{|\mu_K|\sqrt{|d_K|}},$$

mit $h_K = |cl_K|$ = Klassenzahl von K, μ_K = Einheitswurzeln in K, d_K = Diskriminante von $K \stackrel{\text{def}}{=} d(\mathfrak{o}_K)$ und R_K = Regulator von K.

Bemerkung : Hier sind zum ersten Mal analytische Daten (wie $\mathrm{res}_{x=1}\zeta_K(x)$) und arithmetische Daten (wie h_k) verknüpft.

Diskriminantenbeispiele : $d_{\mathbb{Q}(\sqrt{d})} = \begin{cases} 4d & d \not\equiv 1 \bmod 4 \\ d & d \equiv 1 \bmod 4 \end{cases}$

Hilfssatz. (vgl. Kapitel 4) *Für zwei ganze Ideale $\mathfrak{a}, \mathfrak{b} \subset \mathfrak{o}_K$ gilt:*

$$\begin{aligned} N(\mathfrak{ab}) &= N(\mathfrak{a})N(\mathfrak{b}) \\ N((a)) &= |N_{K/\mathbb{Q}}(a)| \\ d(\mathfrak{b}) &= N(\mathfrak{b})^2 d_K\,. \end{aligned}$$

LEMMA. $h_k < \infty$

Zum Beweis der analytischen Klassenzahlformel isolieren wir zunächst den Faktor h_K:

Definiere für $\tau \in cl_K$: $\zeta_{K,\tau}(x) = \sum\limits_{\mathfrak{a}\in\tau_{\text{ganz}}} \frac{1}{N(\mathfrak{a})^x}$, somit $\zeta_K(x) = \sum\limits_{\tau\in cl_K} \zeta_{K,\tau}(x)$. Wähle nun ein ganzes Ideal $\mathfrak{b} \in \tau^{-1}$. Dann gilt $\mathfrak{b} \supseteq \mathfrak{a}\mathfrak{b} = a\mathfrak{o}_K \subseteq \mathfrak{o}_K, a \in \mathfrak{b}$. Hiermit ergibt sich $\zeta_{K,\tau}(x) = N(\mathfrak{b})^x \sum_{(a)\subseteq\mathfrak{b}} N((a))^{-x} = N(\mathfrak{b})^x \sum'_{0\neq a\in\mathfrak{b}} |N_{K/\mathbb{Q}}(a)|^{-x}$, wobei die Notation $\sum'$ bedeute "summiere modulo Einheiten". – Also $\zeta_K(x) = \sum_\tau \zeta_{K,\tau}(x)$, und um den Summanden $\zeta_{K,\tau}(x)$ zu verstehen, müssen wir uns mit $\sum'$ beschäftigen.

Betrachte dazu das kommutative Diagramm

$$\begin{array}{ccc} K^\times & \xrightarrow{\Phi} & \mathbb{R}^r \times \mathbb{C}^s \simeq \mathbb{R}^n \\ & \searrow^{\Psi} & \downarrow \mathrm{L} \\ & & \mathbb{R}^{r+s} \end{array} \qquad \begin{array}{ccc} a & \xrightarrow{\Phi} & (a^{\sigma_1}, \ldots, a^{\sigma_r}, a^{\sigma_{r+1}}, \ldots, a^{\sigma_{r+s}}) \\ & \searrow^{\Psi} & \downarrow \mathrm{L} \\ & & (\log|a^{\sigma_1}|, \ldots, \log|a^{\sigma_r}|, 2\log|a^{\sigma_{r+1}}|, \ldots, 2\log|a^{\sigma_{r+s}}|) \end{array}$$

und allgemein $(y_1, \ldots, y_r, y_{r+1}, \ldots, y_{r+s}) \overset{L}{\mapsto} (\log|y_1|, \ldots, \log|y_r|, 2\log|y_{r+1}|, \ldots, 2\log|y_{r+s}|)$. Man bemerke, daß Ψ die natürliche Fortsetzung der Dirichletabbildung λ ist.

Definiere in $\mathbb{R}^{r+s}$: $1_0 = 1 = (1, \ldots, 1), 1_{r+s} = (1, \ldots, 1, 2 \ldots, 2), 1_i = \Psi(e_i)\,(\forall\, 1 \leq i \leq r+s-1)$ mit einem Satz e_i von Fundamentaleinheiten von K.

Wie im vorigen Kapitel bewiesen, sind die $1_i, 1 \leq i \leq r+s-1$, linear unabhängig und $\langle 1_i : 1 \leq i \leq r+s-1\rangle = H = 1^\perp$. Da $(1_{r+s}, 1) \neq 0$, folgt $\mathbb{R}^{r+s} = \langle 1_i : 1 \leq i \leq r+s\rangle$.
Schreibe $L(y)$, für $y \in (\mathbb{R}^r \times \mathbb{C}^s)^\times$, bezüglich dieser Basis: $L(y) = \sum_{i=1}^{r+s} \xi_i 1_i$. Die ξ_i bezeichnet man als *logarithmische Koordinaten* von y.

Beobachtung: Zu $a \in K^\times$ existiert genau ein $e \in E_K$ mit $\Phi(ae) \in \mathfrak{F}$, wobei $y \in \mathfrak{F} \subset \mathbb{R}^r \times \mathbb{C}^s$ folgendes bedeutet:

1. $L\Phi(y) = \sum_{i=1}^{r+s} \xi_i 1_i$ mit $\xi_i \in [0, 1)$ für $1 \leq i \leq r+s-1$
2. y_1 hat den Winkel in $[0, \frac{2\pi}{|\mu_K|})$, i.e., $\arg(ae)^{\sigma_1} \in [0, \frac{2\pi}{|\mu_K|})$.

Die erste Bedingung resultiert aus der Gittereigenschaft von $\Psi(E_K) = \lambda(E_K)$ in H, die zweite erreicht man durch Multiplikation mit einer geeigneten Einheitswurzel aus μ_K.
$\mathfrak{F}$ nimmt also Bezug auf die eingeschränkte Summation $\sum'$ oben. Für $\mathfrak{F}$ gilt $\alpha \cdot \mathfrak{F} \subset \mathfrak{F}$, falls $\alpha \in \mathbb{R}_{>0}$, da diese Streckung nur die logarithmische Koordinate von f bei e_{r+s} ändert.
Wir definieren noch die Normabbildung $N : (\mathbb{R}^r \times \mathbb{C}^s)^\times \to \mathbb{R}^\times,\ y \mapsto \prod\limits_{i=1}^{r} |y_i| \prod\limits_{i=r+1}^{r+s} |y_i|^2$, und bemerken $N(\Phi(a)) = |N_{K/\mathbb{Q}}(a)|$. Mittels dieser Normabbildung setze $\mathfrak{F}_1 \overset{\text{def}}{=} \{f \in \mathfrak{F} :\ N(f) \leq 1\}$, so daß also offensichtlich $\mathfrak{F} = \bigcup_{j\geq 1} \alpha_j \mathfrak{F}_1$ für jede monoton steigende unbeschränkte Folge $\alpha_j \in \mathbb{R}_{>0}$; überdies $\alpha_j \mathfrak{F}_1 \subset \alpha_{j+1}\mathfrak{F}_1$.

Wir haben damit erreicht

$$\zeta_{K,\tau}(x) = N(\mathfrak{b})^x \sum_{0\neq f\in\Phi(\mathfrak{b})\cap\mathfrak{F}} N(f)^{-x}$$

und müssen nun $\Phi(\mathfrak{b}) \cap \mathfrak{F}$ bestimmen. Dazu sei, für $t > 0$,

$$M(t) \overset{\text{def}}{=} \#\{f \in \Phi(\mathfrak{b}) \cap t^{\frac{1}{n}} \mathfrak{F}_1\} = \#\{f \in t^{-\frac{1}{n}} \Phi(\mathfrak{b}) \cap \mathfrak{F}_1\}\,.$$

Die Menge ganz rechts ist als Schnitt eines Gitters mit dem beschränkten $\mathfrak{F}_1$ endlich, weshalb wir aufgrund von $\bigcup_{t\to\infty} t^{\frac{1}{n}}\mathfrak{F}_1 = \mathfrak{F}$, die zu bestimmende Menge $\Phi(\mathfrak{b})\cap\mathfrak{F}$ als eine abzählbare Menge erkennen und dann so schreiben können

$$\Phi(\mathfrak{b})\cap\mathfrak{F} = \{f_1, f_2, \ldots\} \quad \text{mit} \quad N(f_i) =: t_i \text{ und } t_i \le t_{i+1}\,.$$

Hängen wir an jeden Gitterpunkt in $t^{-\frac{1}{n}}\Phi(\mathfrak{b})\cap\mathfrak{F}_1$ die Grundmasche des Gitters $t^{-\frac{1}{n}}\Phi(\mathfrak{b})$ an, so überdecken die entstehenden Maschen die Menge $t^{-\frac{1}{n}}\Phi(\mathfrak{b})\cap\mathfrak{F}_1$, und im Falle der Meßbarkeit von $\mathfrak{F}_1\subset\mathbb{R}^n$ erhält man

$$\mathrm{vol}(\mathfrak{F}_1) = \lim_{t\to\infty} M(t)\mathrm{vol}(t^{-\frac{1}{n}}\Phi(\mathfrak{b}))\,, \quad \text{also} \quad \frac{M(t)}{t} \to \frac{\mathrm{vol}(\mathfrak{F}_1)}{\mathrm{vol}(\Phi(\mathfrak{b}))} =: v\,.$$

Bemerkung. Zufolge von Lemma(*) aus Kapitel 1 und dem Hilfssatz weiter oben hat das Gitter $t^{-\frac{1}{n}}\Phi(\mathfrak{b})$ das Volumen

$$\frac{1}{t}2^{-s}\sqrt{|d(\mathfrak{b})|} = \frac{1}{t}2^{-s}N(\mathfrak{b})\sqrt{|d_K|}\,.$$

Und $\mathrm{vol}(\mathfrak{F}_1) = \frac{2^r\pi^s R_K}{|\mu_K|}$. Die Berechnung des Volumens des "abgeschnittenen Kegels" $\mathfrak{F}_1$ ist eine reine Volumenbestimmung im $\mathbb{R}^n$ (vgl. z.B. dazu das Buch von Fröhlich und Taylor). Der Faktor $\frac{1}{|\mu_K|}$ entsteht durch Weglassen der zweiten Eigenschaft von $\mathfrak{F}\supset\mathfrak{F}_1$; 2^r und π^s sind natürlich auftretende Volumina; R_K resultiert aus dem Wechsel zu den logarithmischen Koordinaten.
Zusammengefaßt: $v = \frac{2^{r+s}\pi^s R_K}{|\mu_K|N(\mathfrak{b})\sqrt{|d_K|}}$.

Der Definition von $M(t)$ entnimmt man ohne weiteres die Abschätzung $M(t_i-\varepsilon) < i \le M(t_{i+1})$ für unsere Normen $t_i = N(f_i)$ und für jedes $\varepsilon > 0$, also

$$\lim_{i\to\infty}\frac{M(t_i)}{t_i} = \lim_{i\to\infty}\frac{i}{t_i} = v\,,$$

und weiter [2]

$$(v-\varepsilon)^x\sum_{i>N} i^{-x} \le \sum_{i>N}\frac{1}{t_i^x} \le (v+\varepsilon)^x\sum_{i>N} i^{-x}\,.$$

Nun gilt

$$\lim_{x\to 1}(x-1)\sum_{i\ge 1}\frac{1}{i^x} = 1\,,\ \sum_{i>N}\frac{1}{t_i^x} = N(\mathfrak{b})^{-x}\zeta_{K,\tau}(x) - \sum_{i\le N}\frac{1}{t_i^x}\,,$$

somit $\lim_{x\to 1}(x-1)\zeta_{K,\tau}(x) = vN(\mathfrak{b})$.

4. Idealnormen, Zerlegung von Primidealen in endlichen Körpererweiterungen, Diskriminante und Differente

Sei $k\subset K$ eine Zahlkörpererweiterung mit $\mathfrak{o}_K =: \mathfrak{O}$ und $\mathfrak{o}_k =: \mathfrak{o}$. Wir definieren die multiplikativen Abbildungen

$$i : I(\mathfrak{o}) \to I(\mathfrak{O}),\ \mathfrak{a}\mapsto\mathfrak{a}\mathfrak{O}$$
$$N : I(\mathfrak{O}) \to I(\mathfrak{o})\,,\ \mathfrak{A} = \textstyle\prod_{i=1}^r \mathfrak{P}_i^{e_i} \mapsto \prod_{i=1}^r N(\mathfrak{P}_i)^{e_i},$$
$$\text{wobei } N(\mathfrak{P}_i) = \mathfrak{p}^{f_i},\ \text{falls } \mathfrak{p} = \mathfrak{P}\cap\mathfrak{o} \text{ und } [\mathfrak{O}/\mathfrak{P}_i : \mathfrak{o}/\mathfrak{p}] = f_i.$$

[2] wir beschränken uns hier auf reelle $x > 1$

Beobachtungen.

1. i ist injektiv.
2. Für den Spezialfall $k = \mathbb{Q}$ gilt $N(\mathfrak{A}) = |\mathfrak{O}/\mathfrak{a}| = N_{K/\mathbb{Q}}(\mathfrak{A})$.
3. Falls K/k galoissch mit Gruppe G, so gilt $iN(\mathfrak{P}) = \prod_{\sigma\in G} \mathfrak{P}^\sigma$
4. $Ni(\mathfrak{p}) = \mathfrak{p}^{[K:k]}$ für Primideale $\mathfrak{p}$ in $\mathfrak{o}$.

[*Zu 3.:* $Ni(\mathfrak{p}) = N(\prod_{i=1}^r \mathfrak{P}_i^{e_i}) = \prod_{i=1}^r N(\mathfrak{P}_i)^{e_i} = \prod_{i=1}^r \mathfrak{p}^{e_i f_i}$. Die Behauptung folgt nun aus dem nächsten Satz.]

SATZ. *Für ein Primideal $\mathfrak{p}$ von $\mathfrak{o}$ mit $\mathfrak{p}\mathfrak{O} = \prod_{i=1}^r \mathfrak{P}_i^{e_i}$ und $[\mathfrak{O} : \mathfrak{P}_i] = f_i$ gilt: $\sum_{i=1}^r e_i f_i = [K : k]$.*

Beweis des Satzes: Wir lokalsieren $\mathfrak{o}$ und $\mathfrak{O}$ nach $\mathfrak{p}$. Dann ist $\mathfrak{o}_\mathfrak{p}$ ein lokaler Dedkindring mit maximalem Ideal $\mathfrak{p}$, also insbesondere ein Hauptidealring. $\mathfrak{O}_\mathfrak{p}$ ist ein semilokaler Dedekindring und damit ebenfalls ein Hauptidealring; das Erzeugende von $\mathfrak{P}_i$ bezeichnen wir mit π_i. Ferner ist $\mathfrak{O}_\mathfrak{p}$ ein freier $\mathfrak{o}_\mathfrak{p}$-Modul mit Basis $e_1, \ldots, e_n$, $n = [K : k]$, und $\mathfrak{O}_\mathfrak{p}/\mathfrak{p}\mathfrak{O}_\mathfrak{p}$ ein $\mathfrak{o}_\mathfrak{p}/\mathfrak{p}$-Vektorraum der Dimension n. Unter Beachtung des Chinesischen Restsatzes gilt $\mathfrak{O}_\mathfrak{p}/\mathfrak{p}\mathfrak{O}_\mathfrak{p} = \oplus_{i=1}^r \mathfrak{O}_\mathfrak{p}/\mathfrak{P}_i^{e_i}$ und wir erhalten

$$n = \dim_{\mathfrak{o}_\mathfrak{p}/\mathfrak{p}} \mathfrak{O}_\mathfrak{p}/\mathfrak{p}\mathfrak{O}_\mathfrak{p} = \textstyle\sum_{i=1}^r \dim_{\mathfrak{o}_\mathfrak{p}/\mathfrak{p}}(\mathfrak{O}_\mathfrak{p}/\mathfrak{P}_i^{e_i}) = \sum_{i=1}^r e_i f_i,$$

da $[\mathfrak{O}_\mathfrak{p}/\mathfrak{P}_i : \mathfrak{o}_\mathfrak{p}/\mathfrak{p}] = f_i$ und $\mathfrak{P}_i^{j_i}/\mathfrak{P}_i^{j_i+1} \overset{\cdot\pi_i}{\cong} \mathfrak{P}_i^{j_i+1}/\mathfrak{P}_i^{j_i+2}$ $(\forall\, 0 \le j_i \le e_i)$.

LEMMA. *Sei $k \subset K$ eine Zahlkörpererweiterung und $\mathfrak{B} = b\mathfrak{o}_K$ ein Hauptideal in K. Dann gilt: $N(\mathfrak{B}) = N_{K/k}(b)\mathfrak{o}_k$.*

Beweis. Sei zunächst K/k galoissch. Wende die Abbbildung i an:

$$\begin{aligned} iN(\mathfrak{B}) &= \textstyle\prod_{\sigma\in G}(b\mathfrak{o}_K)^\sigma = N_{K/k}(b)\mathfrak{o}_K \\ i(N_{K/k}(b)\mathfrak{o}_k) &= N_{K/k}(b)\mathfrak{o}_K \end{aligned}$$

Aus der Injektivität von i folgt die Behauptung.
Im allgemeinen Fall betrachte die Situation in I_H, wobei H die galoissche Hülle von K/k bezeichne, und verwende $N_{H/k} = N_{K/k}N_{H/K}$ (für Element- und Idealnorm).

DEFINITION. *Sei $k \subset K$ eine Zahlkörpererweiterung, M eine abelsche Untergruppe von K_+, A ein Ring in k mit Quot(A) $= k$ und B der ganze Abschluß von A in K. Setze*

$$M' \overset{\text{def}}{=} \{\alpha \in K : Sp_{K/k}(\alpha M) \subseteq A\}.$$

Beachte: ist M ein B-Modul, so auch M'; insbesondere ist M' mit M ein gebrochenes Ideal, da M eine k-Basis von K enthält und folgendes Lemma gilt:

LEMMA. *Ist $M = Am_1 \oplus \ldots \oplus Am_n$, $n = [K : k]$, so gilt $M' = At_1 \oplus \ldots \oplus At_n$ mit $Sp_{K/k}(t_i m_j) = \delta_{ij}$ (Dualbasis).*

LEMMA. 1. *Für ein Ideal $\mathfrak{A}$ in K gilt $\mathfrak{A}' = (\mathfrak{o}_K)'\mathfrak{A}^{-1}$*
2. *Ist $k \subseteq K \subseteq L$ eine Zahlkörpererweiterung, so gilt $\mathfrak{o}'_{L/k} = \mathfrak{o}'_{L/K}\mathfrak{o}'_{K/k}$.*

Beweis zu 2.:

$\mathrm{Sp}_{L/k}(\mathfrak{o}'_{L/K}\mathfrak{o}'_{K/k}\mathfrak{o}_L) = \mathrm{Sp}_{K/k}\mathrm{Sp}_{L/K}(\mathfrak{o}'_{L/K}\mathfrak{o}'_{K/k}\mathfrak{o}_L) = \mathrm{Sp}_{K/k}(\mathfrak{o}'_{K/k}\mathrm{Sp}_{L/K}(\mathfrak{o}'_{L/K}\mathfrak{o}_L)) \subseteq \mathfrak{o}_k$, da $\mathrm{Sp}_{L/K}(\mathfrak{o}'_{L/K}\mathfrak{o}_L) \subseteq \mathfrak{o}_K$. Es folgt $\mathfrak{o}'_{L/k} \supseteq \mathfrak{o}'_{L/K}\mathfrak{o}'_{K/k}$.

Umgekehrt, sei nun $\beta \in \mathfrak{o}'_{L/k}$. Dann gilt

$$\mathrm{Sp}_{L/k}(\beta\mathfrak{o}_L) = \mathrm{Sp}_{K/k}\mathrm{Sp}_{L/K}(\beta\mathfrak{o}_K\mathfrak{o}_L) = \mathrm{Sp}_{K/k}(\mathfrak{o}_K\mathrm{Sp}_{L/K}(\beta\mathfrak{o}_L)).$$

Aus $\mathrm{Sp}_{L/k}(\beta\mathfrak{o}_L) \subseteq \mathfrak{o}_k$ resultiert $\mathrm{Sp}_{L/K}(\beta\mathfrak{o}_L) \subseteq \mathfrak{o}'_{K/k}$. Es folgt

$$\mathfrak{o}_K \supseteq (\mathfrak{o}'_{K/k})^{-1}\mathrm{Sp}_{L/K}(\beta\mathfrak{o}_L) = \mathrm{Sp}_{L/K}((\mathfrak{o}'_{K/k})^{-1}\beta\mathfrak{o}_L),$$

und damit $\beta(\mathfrak{o}'_{K/k})^{-1} \subseteq \mathfrak{o}'_{L/K}$. Hieraus ergibt sich die Behauptung.

DEFINITION. $\mathcal{D}_{K/k} = (\mathfrak{o}'_K)^{-1}$ *wird als die Differente von* K/k *bezeichnet.*

Beobachtungen:

1. $\mathcal{D}_{L/k} = \mathcal{D}_{L/K}\mathcal{D}_{K/k}$.
2. Ist $S \subseteq \mathfrak{o}_k$ eine multiplikativ abgeschlossenen Menge, so gilt

$$\mathcal{D}_{S^{-1}\mathfrak{o}_K/S^{-1}\mathfrak{o}_k} = S^{-1}\mathcal{D}_{\mathfrak{o}_K/\mathfrak{o}_k}.$$

DEFINITION. *Sei* $n := [K : k]$, $a_1, \ldots, a_n \in K$. *Dann ist die Diskriminante der* a_i *als* $d(a_1, \ldots, a_n) = \det(a_i^{\sigma_j})^2$, $\sigma_j \in I_{K/k}$ *definiert. Sie liegt in* k.

Beobachtungen:

1. $d(a_1, \ldots, a_n) \neq 0 \iff a_1, \ldots, a_n$ bilden eine k-Basis von K.
2. $(a_1, \ldots, a_n)^T = X(b_1, \ldots, b_n)^T$, $X \in k_{n\times n} \Longrightarrow d(b_1, \ldots, b_n) = d(a_1, \ldots, a_n)(\det X)^2$.
3. Schreibe $K = k(\alpha)$. Dann ist $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ eine k-Basis von K mit $D(1, \alpha, \ldots, \alpha^{n-1}) = \prod_{1\leq i<j\leq n}(\alpha^{\sigma_j} - \alpha^{\sigma_i})^2$ (Vandermonde-Determinante).

DEFINITION. M *sei ein freies* $\mathfrak{o}_k$*-Gitter in* K. *Dann ist* $D(M) = d(a_1, \ldots, a_n)$, *falls die* $a_1, \ldots, a_n$ *eine Basis von* M *bilden* [3].
Ist $\mathfrak{A}$ *ein gebrochenes Ideal in* K, *so ist* $D(\mathfrak{A}) = \langle d(a_1, \ldots, a_n)\rangle_{\mathfrak{o}_k}$; *dies ist ein gebrochenes Ideal in* k. *Hier ist das Erzeugnis über alle* k*-Basen von* K *in* $\mathfrak{A}$ *genommen.*

Bemerkungen:

$D(M)$ ist nur modulo $(\mathfrak{o}_k^\times)^2$ bestimmt.

Sind $M_1 \subseteq M_2$ freie $\mathfrak{o}_k$-Moduln vom Rang n, so gilt $D(M_2)|D(M_1)$ und die Gleichheit der Gitter folgt aus der ihrer Diskriminanten.

Man überprüft $S^{-1}D(\mathfrak{A}) = D(S^{-1}\mathfrak{A})$ für multiplikativ abgeschlossene Mengen $S \subset \mathfrak{o}_k$.

[3] wir wechseln von d zu D, um anzuzeigen, daß wir uns nicht unbedingt im Fall $k = \mathbb{Q}$ befinden

SATZ. *Für ein gebrochenes Ideal $\mathfrak{B} \in \mathfrak{o}_K$ gilt: $D(\mathfrak{B}) = N(\mathfrak{B})^2 D_{K/k}$.*
Hier bezeichnet $D_{K/k}$ die Diskriminante von K/k und ist durch $D_{K/k} = D(\mathfrak{o}_K)$ definiert.

Beweis. 1. Fall: $\mathfrak{o}_K$ besitze eine Basis $a_1, \ldots, a_n$ über $\mathfrak{o}_k$ und es sei $\mathfrak{B} = b\mathfrak{o}_K$.
Dann ist $ba_1, \ldots, ba_n$ eine $\mathfrak{o}_k$-Basis von $\mathfrak{B}$ und es gilt

$$D_{K/k} \overset{\text{def}}{=} D(\mathfrak{o}_K) = \det(a_i^{\sigma_j})^2 \mathfrak{o}_k$$

und

$$D(\mathfrak{B}) = D(b\mathfrak{o}_K) = \det((ba_i)^{\sigma_j})^2 \mathfrak{o}_k = \det(b^{\sigma_j} a_i^{\sigma_j})^2 \mathfrak{o}_k = N(\mathfrak{B})^2 D_{K/k}.$$

Der allgemeine Fall entsteht nun aus diesem durch Lokalisieren nach den Primidealen $\mathfrak{p}$ von $\mathfrak{o}_k$, da $\mathfrak{o}_{K,\mathfrak{p}}$ ein Hauptidealring ist.

Den Zusammenhang von Differente und Diskriminante beschreibt der folgende

SATZ. $N(\mathcal{D}_{K/k}) = D_{K/k}$

Beweis. Bemerke zunächst, daß $D(\mathfrak{o}_K) D(\mathfrak{o}'_K) = 1$. Hierzu sei ohne Einschränkung

$$\mathfrak{o}_K = \oplus_{i=1}^n \mathfrak{o}_k a_i, \ \mathfrak{o}'_K = \oplus_{j=1}^n \mathfrak{o}_k b_j, \ (a_i, b_j) = \delta_{ij}$$

(sonst lokalisiere). Dann ist

$$D(\mathfrak{o}_K) = \det(a_i^{\sigma_k})^2 \mathfrak{o}_k, \ D(\mathfrak{o}'_K) = \det(b_j^{\sigma_\nu})^2 \mathfrak{o}_k,$$

und es folgt $(\det(a_i^{\sigma_k}) \det(b_j^{\sigma_\nu}))^2 = 1$.
Beachte weiter, daß nach dem letzten Satz $D(\mathfrak{o}'_K) = N(\mathcal{D}^{-1})^2 D(\mathfrak{o}_K)$ gilt. Aus diesen beiden Beziehungen erhalten wir $1 = D(\mathfrak{o}_K) D(\mathfrak{o}'_K) = N(\mathcal{D}^{-1})^2 D(\mathfrak{o}_K)^2$ und somit $N(\mathcal{D})^2 = D(\mathfrak{o}_K)^2$. Hieraus folgt die Behauptung.

Beispiele :

1. $K/\mathbb{Q}$ habe den Grad n und $a_1, \ldots, a_n$ seien über $\mathbb{Z}$ linear unabhängige ganze Elemente in K. Dann gilt
$$d(a_1, \ldots, a_n) = D_{K/\mathbb{Q}} \cdot [\mathfrak{o}_K : \langle a_1, \ldots, a_n \rangle_{\mathbb{Z}}]^2 \ .$$

2. $K = \mathbb{Q}(\sqrt{d}), 1 \neq d \in Z$, quadratfrei. Dann ist die Dualbasis von $1, \sqrt{d}$ bzw. $1, -\frac{1}{2} + \frac{1}{2}\sqrt{d}$, $\frac{1}{2}$, $\frac{1}{2\sqrt{d}}$ bzw. $\frac{1}{2} + \frac{1}{2\sqrt{d}}$, $\frac{1}{\sqrt{d}}$, also $\mathcal{D}_{K/\mathbb{Q}} = \begin{cases} 2\sqrt{d} \cdot \mathbb{Z}[\sqrt{d}] \\ \sqrt{d} \cdot \mathbb{Z}[-\frac{1}{2} + \frac{1}{2}\sqrt{d}] \ . \end{cases}$

3. Die Dualbasis von $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ im Körper $K(\alpha)$ vom Grad n über K ist $\frac{\beta_0}{f'_\alpha(\alpha)}, \ldots, \frac{\beta_{n-1}}{f'_\alpha(\alpha)}$ mit $\frac{f_\alpha(x)}{x-\alpha} = \beta_{n-1} x^{n-1} + \ldots + \beta_0$.

5. KOMPLETTIERUNGEN

Wir wollen nun den Begriff der Komplettierung einführen. Wir betrachten dazu wieder einen endlich-dimensionalen Zahlkörper K über $\mathbb{Q}$ und darin den Ring der ganzen Zahlen $\mathfrak{o} = \mathfrak{o}_K$. Sei $a \in K^\times$ beliebig. Dann kann man das von a erzeugte Ideal $\mathfrak{o}a$ eindeutig schreiben als $\prod_{i=1}^n \mathfrak{p}_i^{n_i}$ mit Primidealen $\mathfrak{p}_i$ und $n_i \in \mathbb{Z}$. Für ein Primideal $\mathfrak{p}$ in $\mathfrak{o}$ setze $w_\mathfrak{p}(a) = w(a) := n_i$, falls $\mathfrak{p} = \mathfrak{p}_i$, sonst 0. Des weiteren setze $w(0) = \infty$.

Beobachtungen:

1. $w(a) = \infty \iff a = 0$
2. $w(ab) = w(a) + w(b)$
3. $w(a+b) \geq \min(w(a), w(b))$
4. $w(a) \neq w(b) \Longrightarrow w(a+b) = \min(w(a), w(b))$
5. $w(K) = \mathbb{Z} \cup \infty$

Elemente π mit $w(\pi) = 1$ heißen Primelemente für w.

DEFINITION. *Eine Abbildung $w : K \twoheadrightarrow \mathbb{Z} \cup \infty$ mit (1), (2) und (3) heißt eine diskrete Bewertung von K.*

Über w läßt sich nun ein Betrag auf K definieren: $|a| = |a|_{\mathfrak{p}} := p^{-\frac{1}{e} w_{\mathfrak{p}}(a)}$, wobei p die ganzrationale Primzahl in $\mathfrak{p}$ und $e = e_{\mathfrak{p}/p}$ die zugehörige Verzweigungszahl ist, also $p \in \mathfrak{p}^e \setminus \mathfrak{p}^{e+1}$. Dieser Betrag erfüllt nicht nur die Dreiecksungleichung, sondern sogar $|a+b| \leq \max(|a|, |b|)$. Die ϵ-Bälle $U_\epsilon(a) = \{x \in K : |a - x| < \epsilon\}$ erzeugen eine Topologie auf K. Additiv geschrieben entsprechen diese den $U_M(a) := \{x \in K : w(a-x) > M\}$, $M \in \mathbb{N}$.

DEFINITION. *Eine Folge $(a_n)_{n \in \mathbb{N}}$ in K heißt konvergent gegen $a \in K$, in Zeichen $\lim_{n \to \infty} a_n = a$, falls*

$$\forall \epsilon > 0 \; \exists N = N(\epsilon) \in \mathbb{N} : \forall n > N : |a - a_n| < \epsilon$$

oder additiv, falls

$$\forall M \in \mathbb{N} \; \exists N = N(M) \in \mathbb{N} : \forall n > N : w(a - a_n) > M$$

Die Folge heißt eine Cauchyfolge, falls

$$\forall \epsilon > 0 \; \exists N = N(\epsilon) \in \mathbb{N} : \forall n, m > N : |a_n - a_m| < \epsilon$$

oder additiv, falls

$$\forall M \in \mathbb{N} \; \exists N = N(M) \in \mathbb{N} : \forall n, m > N : w(a_n - a_m) > M$$

Jede konvergente Folge ist natürlich eine Cauchyfolge.

DEFINITION. $\mathfrak{o}_{\mathfrak{p}} = \{x \in K : w(x) \geq 0\} = \{x \in K : |x| \leq 1\}$ *heißt der Bewertungsring zu w.*

Dies ist gleich dem alten $\mathfrak{o}_{\mathfrak{p}} = \{\frac{a}{b} : a \in \mathfrak{o}, b \in \mathfrak{o} \setminus \mathfrak{p}\}$. Im Folgenden bezeichne CF_w die Menge aller Cauchyfolgen aus K bzgl. w. Dies ist ein lokaler kommutativer Ring mit 1. Das maximale Ideal N_w sind die w-Nullfolgen.

DEFINITION. *Der Körper $K_w := CF_w / N_w$ heißt die Komplettierung von K bezüglich w.*

Da für jede Cauchyfolge, die keine Nullfolge ist, $w(a_n)$ für hinreichend großes n konstant bleibt, läßt sich w auf K_w fortsetzen. Es ist dann K_w vollständig bezüglich w. Den Bewertungsring bezeichnen wir mit $\mathfrak{o}_w = \{x \in K_w : w(x) \geq 0\}$ und sein maximales Ideal mit $\mathfrak{p}_w$. Es gilt:

$$\mathfrak{o}/\mathfrak{p} = \mathfrak{o}_\mathfrak{p}/\mathfrak{p} = \mathfrak{o}_w/\mathfrak{p}_w =: \overline{K_w}\,.$$

K_w enthält K als die Menge der konstanten Folgen.

Sei nun $\pi \in K$ ein Primelement für w und $x \in K_w^\times$ mit $w(x) = n$. Dann läßt sich x als Laurentreihe in π mit Koeffizienten α_i aus einem fest gewählten Vertretersystem von $\overline{K_w}$ in $\mathfrak{o}_w$ schreiben

$$x = \pi^n\alpha_0 + \pi^{n+1}\alpha_1 + \pi^{n+2}\alpha_2 + \dots\,.$$

Die Potenzreihen entsprechen also den Elementen von $\mathfrak{o}_w$. Man beachte, daß $\mathfrak{o}_w$ kompakt und K_w lokalkompakt ist.

Lemma. $\sum_{i=0}^{\infty} a_i$, $a_i \in K_w$, *konvergiert* $\iff$ $a_i \to 0$.

Lemma. *Zwei Bewertungen w_1 und w_2 bestimmen genau dann die gleiche Topologie auf K, wenn es ein $0 \neq \alpha \in \mathbb{Q}$ mit $w_1(x) = \alpha w_2(x)$ $(\forall\, x \in K)$ gibt.*

Das liegt an der Tatsache, daß $\{x \in K : x^n \to 0\} = \{x \in K : w(x) > 0\}$.

Insbesondere trägt jede endliche Erweiterung L von K_w eine eindeutige Topologie, die w fortsetzt und somit enthält der ganze Abschluß von o_w in L nur ein einziges Primideal $\neq 0$.

Lemma. *Sei K ein Zahlkörper über $\mathbb{Q}$. Dann gilt:* $K \otimes_\mathbb{Q} \mathbb{Q}_p = \bigoplus_{\mathfrak{p}|p} K_\mathfrak{p}$.

Beweisskizze. Wähle zunächst ein primitives Element $\alpha \in K$ mit Minimalpolynom $f(x) \in \mathbb{Q}[x]$. Es sei $f(x) = \prod_{i=1}^d f_i(x)$ mit über $\mathbb{Q}_p$ irreduziblen Polynomen $f_i \in \mathbb{Q}_p[x]$; also $K \otimes_\mathbb{Q} \mathbb{Q}_p = \bigoplus_{i=1}^d K_i$ mit $K_i = \mathbb{Q}_p[x]/f_i(x)$. Jedes solche K_i ist dann die Komplettierung von K bzgl. einer Bewertung $w_{\mathfrak{p}_i}$. Sei $n = [K \otimes_\mathbb{Q} \mathbb{Q}_p : \mathbb{Q}_p]$. Dann ist einerseits $n = [K : \mathbb{Q}] = \sum_j e_j f_j$ (mit den üblichen Bezeichnungen) und andererseits $n = [\bigoplus_i K_i : \mathbb{Q}_p] = \sum_i [K_i : \mathbb{Q}_p] = \sum_i e_i f_i$. Es darf also kein $K_\mathfrak{p}$ fehlen. Analog zeigt man für jede Zahlkörpererweiterung K/k, daß $K \otimes_k k_\mathfrak{p} = \bigoplus_{\mathfrak{q}|\mathfrak{p}} K_\mathfrak{q}$ gilt.

Ein Analogon zum Newtonverfahren im Reellen ist der folgende

Satz (Hensels Lemma). *Sei K komplett, $f(x) \in \mathfrak{o}[x]$ und $\pi \in \mathfrak{o}$ ein Primelement. Es gebe ein $\alpha_0 \in \mathfrak{o}$ mit $w(f'(\alpha_0)) = w \geq 0$ und $w(f(\alpha_0)) \geq v > 2w$.*

Dann gibt es ein $\alpha_1 \in \mathfrak{o}$ mit $\alpha_1 \equiv \alpha_0 \bmod \pi^{v-w}$, $w(f(\alpha_1)) \geq v+1$ und $w(f'(\alpha_1)) = w$.

Interpretation: Falls α_0 eine Nullstelle von $f \bmod \pi$ ist, so können wir sukzessive weitere Nullstellen $\alpha_1, \alpha_2, \dots$ von $f \bmod \pi$ konstruieren, die bzgl. der Bewertung w von K gegen eine Nullstelle α von f konvergieren. Der Beweis ist konstruktiv: Setze zunächst $\alpha_1 = \alpha_0 + \pi^{v-w}\beta$ mit $\beta \in \mathfrak{o}$. Schreibe $f(\alpha_0) = \pi^v\gamma$ und $f'(\alpha_0) = \pi^w u$ mit $w(\gamma) \geq 0$ und $w(u) = 0$. Dann ist β die Lösung der Kongruenz $\gamma \equiv -u\beta \bmod \pi$.

Lemma (Krasners Lemma). *Sei K komplett, $\alpha, \beta \in K^c$, $L = K(\beta, \sigma(\alpha) : \sigma \in I_{K(\alpha)/K})$. L erbt von K eine Bewertung w. Es gelte $w(\beta - \alpha) > w(\sigma(\alpha) - \alpha)$ für alle $1 \neq \sigma \in I_{K(\alpha)/K}$. Dann ist $K(\alpha) \subset K(\beta)$.*

Beweis. Sei $\tau \in I_{K(\beta,\alpha)/K(\beta)}$. Wir wollen $\tau = 1$ zeigen. Weil es nur eine einzige Bewertung auf $K(\beta,\alpha)$ gibt, gilt $w\tau = w$. Falls $\tau \neq 1$, so gilt also $w(\tau(\alpha)-\alpha) < w(\beta-\alpha) = w(\beta-\tau(\alpha))$. Der Vergleich der Bewertungen auf der rechten und linken Seite von $\tau(\alpha)-\alpha = \tau(\alpha)-\beta+\beta-\alpha$ liefert den Widerspruch.

Konsequenzen aus den vorangegangen beiden Lemmata sind folgende

Beobachtungen: Sei K komplett, $f(x) \in K[x]$ separabel, $n = \deg(f)$.

Ist $g(x) \in K[x]$ vom selben Grad n und koeffizientenweise nahe bei f, so liegen auch die Wurzeln von f und g nahe beieinander.

Ist dabei f irreduzibel, so auch g.

Ist $L/\mathbb{Q}_p$ eine endliche Erweiterung, so ist $L = K_\mathfrak{p}$ für eine geeignete endliche Erweiterung $K/\mathbb{Q}$.

FOLGERUNG. *Bis auf Isomorphie hat K nur endlich viele Erweiterungen von gegebenem Grad.*

An dieser Stelle wenden wir uns für einen Moment zurück ins "Globale" :

1. Sei $\alpha \in K^\times$, K ein Zahlkörper. Wir definieren

$$\| \alpha \|_\mathfrak{p} \overset{\text{def}}{=} \begin{cases} p^{-w_\mathfrak{p}(\alpha) f_{\mathfrak{p}|p}} & \text{wenn } \mathfrak{p} \subset \mathfrak{o}_K \\ |\sigma_\mathfrak{p}(\alpha)|^{1 \text{ oder } 2} & \text{wenn } \mathfrak{p}|\infty \ \& \ \ \mathfrak{p} \leftrightarrow \{\sigma_\mathfrak{p}, \overline{\sigma}_\mathfrak{p}\} \subset I_{K/\mathbb{Q}}\,,\ \sigma_\mathfrak{p}(K) \subset \mathbb{R} \text{ bzw. } \sigma_\mathfrak{p}(K) \not\subseteq \mathbb{R}\ . \end{cases}$$

   Damit gilt die

   PRODUKTFORMEL. $\prod_\mathfrak{p} \| \alpha \|_\mathfrak{p} = 1$.

   Der Beweis benutzt die Äquivalenz

   > Ist L/K galoissch, so gilt die Produktformel für $\lambda \in L$ genau dann, wenn sie für $N_{L/K}(\lambda) \in K$ gilt.

   Damit reicht es, sie für $\alpha \in \mathbb{Q}$ nachzuweisen und hier wiederum, nur Primzahlen $q = \alpha$ zu betrachten.

2. Sei K/k eine galoissch-endliche Erweiterung von Zahlkörpern mit Gruppe $G := G_{K/k}$, $\mathfrak{p} \subset k$ prim, $K = k(\alpha)$, $f_\alpha(x) \in k[x]$. Wie bereits bekannt, gilt

$$K \otimes_k k_\mathfrak{p} \cong \bigoplus_{\mathfrak{P}|\mathfrak{p}} K_\mathfrak{P},\ f_\alpha(x) = \prod_\mathfrak{P} f_\mathfrak{P}(x),\ k_\mathfrak{P} = k_\mathfrak{p}(\alpha_\mathfrak{P}),$$

   wobei $\alpha_\mathfrak{P}$ Nullstelle von $f_\mathfrak{P}(x)$ ist. In dieser Situation wird die Zerlegungsgruppe im Globalen die Galoisgruppe im Lokalen:

   SATZ. *$K_\mathfrak{P}/k_\mathfrak{p}$ ist galoissch mit Gruppe $G_\mathfrak{P} = \{\sigma \in G : \sigma(\mathfrak{P}) = \mathfrak{P}\}$.*

Beweis: Sei α_1 eine Wurzel von $f_{\mathfrak{P}_0}(x)$, also auch von $f_\alpha(x)$. Da K/k galoissch, liegt α_1 in K. Die Abbildung $0 \neq h : K_{\mathfrak{P}_0} \to \bigoplus_{\mathfrak{P}|\mathfrak{p}} K_{\mathfrak{P}}$, $\alpha_{\mathfrak{P}_0} \mapsto \alpha_1$, zusammen mit den Projektionen in die einzelnen Komponenten liefert Homomorphismen von $K_{\mathfrak{P}_0}$ nach $K_{\mathfrak{P}}$. Diese sind entweder gleich der Nullabbildung oder injektiv. Letzteres ist jedoch aufgrund der Eindeutigkeit der Bewertung nur für $\mathfrak{P} = \mathfrak{P}_0$ der Fall. Somit ist $\alpha_1 \in K_{\mathfrak{P}_0}$ und $K_{\mathfrak{P}_0}/k_{\mathfrak{p}}$ galoissch.

Sei nun $\sigma \in G_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}$. Dann ist $\sigma|_K \in G_{\mathfrak{P}}$: Auf K haben wir die Bewertungen $w_{\mathfrak{P}}$ und $w_{\mathfrak{P}} \circ \sigma$. Da $\sigma \in G_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}$, stimmen diese überein, und es folgt $\sigma(\mathfrak{P}) = \mathfrak{P}$. Wir erhalten also eine Abbildung $G_{K_{\mathfrak{P}}/k_{\mathfrak{p}}} \to G_{\mathfrak{P}}$, $\sigma \mapsto \sigma|_K$; diese ist injektiv. Da beide Gruppen gleiche Mächtigkeit haben (Schluß wie bei der Produktformel) folgt die Isomorphie.

Zurück ins Lokale:

SATZ. *Seien $\mathfrak{O}$ bzw. $\mathfrak{o}$ die Bewertungsringe von K bzw. k. Es gibt ein $\alpha \in \mathfrak{O}$ mit $\mathfrak{O} = \mathfrak{o}[\alpha]$.*

Beweis: Wähle ein Primelement $\Pi \in K$ und ein $\gamma \in K$, so daß $\overline{K} = \overline{k}(\overline{\gamma})$. Dann wird $\mathfrak{O}$ von den Elementen $\Pi^i\gamma^j$ mit $0 \leq i < e$ und $0 \leq j < f$ über $\mathfrak{o}$ erzeugt: nach Nakajama genügt es nämlich, hierzu die Situation modulo $\mathfrak{p}$ zu betrachten, wobei $\mathfrak{p}$ das maximale Ideal in $\mathfrak{o}$ bezeichnet. Man kann nun γ so wählen, daß ein Polynom $g(x)$ existiert, so daß $g(\gamma)$ ein Primelement ist: setze jetzt $\alpha = \gamma$. Zur Konstruktion von γ: Wähle zunächst γ als Vertreter von $\overline{\gamma}$ und $g(x)$ mit $\overline{g}(x) = f_{\overline{\gamma}}(x)$, also $w(g(\gamma)) \geq 1$. Bei Gleichheit sind wir fertig. Ansonsten wählen wir ein weiteres Primelement $\tilde{\Pi} \in \mathfrak{O}$ und ersetzen γ durch $\gamma + \tilde{\Pi}$. Dieses neue γ besitzt die gewünschte Eigenschaft.

DEFINITION. *Sei $K/\mathbb{Q}_p$ endlich, $\mathfrak{p}$ das maximale Ideal in $\mathfrak{o}$ und $U := \mathfrak{o}^\times$. Dann heißen die Gruppen $U^{(n)} := \{1 + x : w(x) \geq n\} = 1 + \mathfrak{p}^n$ die 1- Einheiten n-ter Stufe.*

Die Abbildung $U \to \overline{K}^\times$, $x \mapsto \overline{x}$ induziert eine natürliche Isomorphie $U/U^{(1)} \simeq \overline{K}^\times$. Für alle $i \geq 1$ liefert $1 + \pi^i x \mapsto \overline{x}$ eine Isomorphie $U^{(i)}/U^{(i+1)} \simeq (\overline{K}^+ = \mathfrak{o}/\mathfrak{p}, +)$, die allerdings von der Wahl des Primelementes π abhängt.

SATZ. *Sei K wie oben, mit Bewertung w. Dann gilt: $[U : U^m] = [U^{(1)} : U^{(2)}]^s|\mu_m|$, wobei $w(m) = s$.*

Beweisskizze: $\mathfrak{o} := \mathfrak{o}_w, \mathfrak{p} := \mathfrak{p}_w, \pi\mathfrak{o} = \mathfrak{p}, w(m) = s$. Wähle $r \geq s + 1$.
Wir zeigen zunächst $(U^{(r)})^m = U^{(r+s)}$.
Sei hierzu $1 + x\pi^r \in U^{(r)}, x \in \mathfrak{o}$. Aus $(1 + x\pi^r)^m \equiv 1 + mx\pi^r (\bmod \pi^{s+r+1})$ folgt "$\subseteq$".
Betrachte nun den Homomorphismus $f : U^{(r)} \to (U^{(r)})^m$, $x \mapsto x^m$. Dieser ist surjektiv: Sei dazu $U^{(r+s)} \ni \alpha = 1 + t\pi^{r+s}$. Die Gleichung $x^m = \alpha = 1 + t\pi^{r+s}$ besitzt $\bmod \pi^{r+s}$ die Lösung $x = 1$. Da $w(mx^{m-1}|_{x=1}) = w(m) = s$, $r + s > 2s$, können wir Hensels Lemma anwenden und erhalten eine Lösung $x = 1 + \gamma$, $\gamma \in U^{(r)}$, mit $(1 + \gamma)^m = \alpha$. Hiermit folgt $(U^{(r)})^m = U^{(r+s)}$.
Beobachtung: Sei G eine (abelsche) Gruppe, $V \leq G$ und $f : G \to H$ ein Homomorphismus. Aus den Isomorphiesätzen folgt unmittelbar

$$[G : V] = [f(G) : f(V)][\ker(f) : \ker(f|_V)].$$

Für $U^{(r)} \leq U$ und f wie oben übersetzt sich dies in

$$[U : U^{(r)}] = [U^m : U^{(r+s)}][\mu_m : 1] = \frac{[U : U^{(r+s)}]}{[U : U^m]}|\mu_m|,$$

falls r so groß gewählt wird, daß $U^{(r)}$ keine m-ten Einheitswurzeln enthält. Somit erhalten wir

$$[U : U^m] = \frac{[U : U^{(r+s)}]}{[U : U^{(r)}]}|\mu_m| = [U^{(r)} : U^{(r+s)}]|\mu_m| = [U^{(1)} : U^{(2)}]^s|\mu_m|.$$

FOLGERUNG. *Wegen $K^\times = \langle\pi\rangle \times U$ und $(K^\times)^m = \langle\pi^m\rangle \times U^m$ gilt also $[K^\times : (K^\times)^m] = m[U^{(1)} : U^{(2)}]^s|\mu_m|$, wobei $w(m) = s$.*

Sei nun K/k eine endliche galoissche Erweiterung kompletter Körper. Die Restklassenkörpererweiterung $\overline{K}/\overline{k}$ ist eine Erweiterung endlicher Körper und damit galoissch zyklisch: $G_{\overline{K}/\overline{k}} = \langle\phi\rangle$, ϕ der Frobeniusautomorphismus.

Aufschluß über den Zusammenhang von $G_{K/k}$ und $G_{\overline{K}/\overline{k}}$ gibt der folgende

SATZ. *Sei K/k eine galoissch-endliche Erweiterung kompletter Körper. Dann existiert ein kanonischer surjektiver Homomorphismus $G_{K/k} \twoheadrightarrow G_{\overline{K}/\overline{k}}$. Der Kern dieser Abbildung heißt Verzweigungsgruppe.*

Beweis. Sei $\sigma \in G_{K/k}$. Da σ sowohl $\mathfrak{o}_k$ als auch $\mathfrak{P}$ festläßt, liefert $\overline{\sigma} : \mathfrak{o}_K/\mathfrak{P} \to \mathfrak{o}_K/\mathfrak{P}$ ein Element aus $G_{\overline{K}/\overline{k}}$. Zur Surjektivität: Schreibe $\overline{K} = \overline{k}(\overline{\alpha}), \alpha \in \mathfrak{o}_K$. Sei $\tau \in G_{\overline{K}/\overline{k}}$. $\tau(\alpha)$ ist Wurzel von $f_{\overline{\alpha}}(x)$, und damit wegen $f_{\overline{\alpha}}|\overline{f_\alpha}$ auch von $\overline{f_\alpha}$. Da K/k galoissch, zerfällt f_α vollständig über K: $f_\alpha(x) = \prod(x - \alpha_i)$, $\alpha_1 = \alpha$, also $\overline{f_\alpha}(x) = \prod(x - \overline{\alpha_i})$ und $\tau(\overline{\alpha}) = \overline{\alpha_i}$ für ein gewisses i. Indem wir nun die Abbildung $k(\alpha) \to K, \alpha \mapsto \alpha_i$, zu einem Isomorphismus $\sigma \in G$ liften, erhalten wir das gesuchte Urbild.

UNVERZWEIGTE ERWEITERUNGEN KOMPLETTER KÖRPER:

DEFINITION. *Sei K/k eine endliche Erweiterung kompletter Körper. Diese heißt unverzweigt, wenn $e_{\mathfrak{P}/\mathfrak{p}} = 1$.*

Bemerkung: Äquivalente Definitionen sind:

$$\begin{aligned} K/k \text{ ist unverzweigt} &\iff [\pi \text{ ist Primelement in } k \Rightarrow \pi \text{ ist Primelement in } K] \\ &\iff [\overline{K} : \overline{k}] = [K : k] \end{aligned}$$

LEMMA. *Sei K/k eine unverzweigte Erweiterung kompletter Körper. Dann gilt:*

1. *$\overline{K} = \overline{k}(\overline{\alpha}) \Rightarrow K = k(\alpha)$ mit einer Hochhebung $\alpha \in \mathfrak{o}_K$ von $\overline{\alpha}$.*
2. *K/k ist zyklisch: $G_{K/k} = \langle\phi\rangle$ mit $\phi(x) \equiv x^q (\bmod \mathfrak{P})$ $(\forall x \in \mathfrak{o}_K)$. ϕ ist hierdurch eindeutig bestimmt und heißt wieder Frobeniusautomorphismus.*

Beweis: *zu 1.:* Es gilt $f_{\overline{\alpha}}|\overline{f_\alpha}$. Damit ist $\deg(f_{\overline{\alpha}}) = [\overline{K} : \overline{k}] \le \deg(\overline{f_\alpha}) = \deg(f_\alpha) \le [K : k]$. Da K/k unverzweigt, folgt also $\deg(f_\alpha) = [K : k]$.
zu 2.: Da $\overline{f_\alpha} = f_{\overline{\alpha}}$, zerfällt $\overline{f_\alpha}$ vollständig in $\overline{K}$. Hebe diese Nullstellen hoch nach $\mathfrak{o}_K$ und verfeinere gemäß Hensels Lemma zu echten Nullstellen von f_α: Sei β Hochhebung einer Nullstelle von $\overline{f_\alpha}$. Dann ist $w(f_\alpha(\beta)) > 0$ und $w(f'_\alpha(\beta)) = 0$, da $f_{\overline{\alpha}}$ separabel. Somit sind die Voraussetzungen für Hensels Lemma erfüllt.

LEMMA. *Sei K/k eine endliche Erweiterung kompletter Körper, $K = k(\alpha), \alpha \in \mathfrak{o}, \overline{f_\alpha}$ doppelwurzelfrei. Dann ist K/k unverzweigt und $\overline{K} = \overline{k}(\overline{\alpha})$.*

Beweis. Sei L der Zerfällungskörper von f_α: $f_\alpha(x) = \prod_{i=1}^{n}(x-\alpha_i) \in L[x]$. Nach einem obigem Satz gilt $\phi : G_{L/k} \twoheadrightarrow G_{\overline{L}/\overline{k}}$. Dies ist sogar eine Injektion: Sei dazu $\phi(\sigma) = \overline{\sigma} = 1$. Dann ist $\overline{\alpha_i} = \overline{\sigma}(\overline{\alpha_i}) = \overline{\sigma(\alpha_i)}$ $(\forall i)$. Da $\overline{f_\alpha}$ doppelwurzelfrei ist, folgt $\sigma(\alpha_i) = \alpha_i$ $(\forall i)$, also $\sigma = 1$. L/k ist also unverzweigt und damit zyklisch. Inbesondere ist K/k galoissch, und somit $L = K$. Aus $\overline{f_\alpha}(x) = \prod_{\sigma \in G_{K/k}} (x - \overline{\sigma(\alpha)}) = \prod_{\overline{\sigma} \in G_{\overline{K}/\overline{k}}} (x - \overline{\sigma}(\overline{\alpha})) = f_{\overline{\alpha}}(x)$ resultiert $\overline{K} = \overline{k}(\overline{\alpha})$.

FOLGERUNG. *Sei k komplett. Dann existiert zu vorgegebenem Grad n genau eine unverzweigte Erweiterung K/k.*

Beweisskizze: Zur Existenz: Wähle ein normiertes irreduzibles Polynom $\overline{f}(x) \in \overline{k}[x]$ vom Grad n und setze $\overline{K} = \overline{k}[x]/\overline{f}(x)$. Hebe $\overline{f}(x)$ hoch zu einem Polynom $f(x)$in $\mathfrak{o}_k[x]$. Dieses ist ebenfalls normiert, irreduzibel und hat Grad n. Setze $K = k[x]/f(x)$.

LEMMA. 1. *Sei $k \subset K \subset L$ eine Erweiterung kompletter Körper. Dann gilt: L/k unverzweigt $\iff$ L/K und K/k unverzweigt.*

2. *Seien K/k und L/k Erweiterungen kompletter Körper und K/k unverzweigt. Dann ist auch KL/L unverzweigt.*

Beweis: *zu 1.:* Dies folgt aus der Multiplikativität der Verzweigungsindizes.
zu 2.: Sei $K = k(\alpha)$, $\overline{f_{\alpha,k}}$ doppelwurzelfrei. Bezeichnen wir mit $f_{\alpha,L}$ das Minimalpolynom von α über L, so ist dieses wegen $f_{\alpha,L} | f_{\alpha,k}$ ebenfalls doppelwurzelfrei und somit KL/L unverzweigt.

SATZ. *Sei K/k eine unverzweigte Erweiterung kompletter Körper, π ein Primelement in k und $n = [K:k]$. Dann gilt*

$$N_{K/k}(K^\times) = \langle \pi^n \rangle \times U_k.$$

Beweis. Da K/k unverzweigt, ist π auch Primelement in K. Sei nun $K^\times \ni \alpha = \pi\epsilon$, $w_K(\epsilon) = 0$. Wegen $N_{K/k}(\alpha) = N_{K/k}(\pi)N_{K/k}(\epsilon) = \pi^n N_{K/k}(\epsilon)$ genügt es, $N_{K/k}(U_K) = U_k$ zu zeigen. Hierfür erinnern wir uns daran, daß $\overline{N}_{\overline{K}/\overline{k}} : \overline{K}^\times \to \overline{k}^\times$ und $\overline{Sp}_{\overline{K}/\overline{k}} : \overline{K}^+ \to \overline{k}^+$ surjektiv sind (vgl. Algebra I). Sei nun $u \in U_k$. Es existiert also ein $\overline{\epsilon_o} \in \overline{K}^\times$ mit $\overline{N}_{\overline{K}/\overline{k}}(\epsilon_o) = \overline{u}$, was wegen der Unverzweigtheit von K/k äquivalent zu $N_{K/k}(\epsilon_o) \equiv u \pmod{\mathfrak{P}}$ ist. Es folgt $N_{K/k}(\epsilon_o^{-1})u = 1 + x_1\pi$, x_1 ganz. Wähle nun ein $\overline{y_1} \in \overline{K}$ mit $\overline{Sp}_{\overline{K}/\overline{k}}(\overline{y_1}) = \overline{x_1}$ und setze $\epsilon_1 = 1 + y_1\pi$, y_1 eine Hochhebung von $\overline{y_1}$. Dann ist $N_{K/k}(\epsilon_1) \equiv 1 + Sp_{K/k}(y_1)\pi \pmod{\pi^2}$, und es resultiert $N_{K/k}(\epsilon_o^{-1})u \equiv N_{K/k}(\epsilon_1) \pmod{\pi^2}$. Führen wir dieses Verfahren sukzessive fort, erhalten wir $U_K \ni \prod \epsilon_i$, $\epsilon_i \in U_K^{(i)}$, mit $N_{K/k}(\prod \epsilon_i) = u$. Das Produkt $\prod \epsilon_i$ konvergiert, weil $\epsilon_i \in U_K^{(i)}$.

Bemerkungen:

1. Wie im Fall einer endlichen Körpererweiterung über $\mathbb{Q}$ gilt *Ist $K/\mathbb{Q}_p$ endlich, so enthält K nur endlich viele Einheitswurzeln: $|\mu_K| < \infty$.*

   Beweis: Sei $\zeta \in K$ eine Einheitswurzel. Dann zerlege $\zeta = \zeta_1\zeta_2$, wobei ζ_1 p-Potenzordnung und ζ_2 eine zu p prime Ordnung hat. Ist $\zeta_2 \neq 1$, dann ist $\zeta_2 \notin U^{(1)}$, da dies eine pro-p-Gruppe ist. Deshalb bleiben für ζ_2 nur $|\overline{K}^\times|$, also endlich viele Möglichkeiten. Für $\zeta_1 = \zeta_{p^n}$ löst $\zeta_{p^n} - 1$ ein Eisenstein-Polynom in $\mathbb{Z}_p$ vom Grad $p^{n-1}(p-1)$. Also gilt: $[\mathbb{Q}_p(\zeta_{p^n}) : \mathbb{Q}_p] \to \infty$ für $n \to \infty$.

2. Jede komplette Erweiterung K/k besitzt einen eindeutig bestimmten Teilkörper K_{nr}, so daß K_{nr}/k unverzweigt und K/K_{nr} rein verzweigt ist.

REIN- UND ZAHM-VERZWEIGTE ERWEITERUNGEN KOMPLETTER KÖRPER:

Im Folgenden sei stets K/k eine endliche Erweiterung kompletter Körper, $n = [K : k] = ef$.

DEFINITION. *K/k heißt rein (oder total) verzweigt, falls $f = 1$ (also $e = n$).*

SATZ. *K/k rein verzweigt $\iff$ $K = k(\alpha)$ und $f_\alpha(x)$ ist ein Eisenstein-Polynom.*

In diesem Fall ist α ein Primelement in K.

Beweisskizze: Sei K/k rein verzweigt und $\Pi \in K$ ein Primelement. Dann ist $K = k(\Pi)$, da K aus Laurentreihen in Π mit Koeffizienten aus einem Vertretersystem von $\overline{K} = \overline{k}$ in K besteht. Sei W die Bewertung auf K. Für die Eisenstein-Eigenschaft von $f_\Pi(x) = \sum_{i=0}^{n} a_i x^i$ rechnet man (mit Hilfe der elementar-symmetrischen Funktionen) nach, daß $W(a_i) \geq 1$ und $W(a_0) = e = W(\pi)$ gilt, wobei π ein Primelement in k ist. Umgekehrt ist $e = W(a_0) = W(\prod_\sigma \alpha^\sigma) = [K : k]W(\alpha) = efW(\alpha)$. Also $f = 1 = W(\alpha)$.

Anwendung: $\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p$ ist eine rein verzweigte Erweiterung vom Grad $(p-1)p^{n-1}$.

ACHTUNG: Das Kompositum zweier rein verzweigter Körper kann ein unverzweigtes Teilstück enthalten! Dazu wähle K_0 als die unverzweigte Erweiterung von $\mathbb{Q}_p$ vom Grad p und K_1 als den Teilkörper von $\mathbb{Q}_p(\zeta_{p^2})$ vom Grad p über $\mathbb{Q}_p$. L sei das Kompositum; es enthält $p+1$ Teilkörper vom Grad p über $\mathbb{Q}_p$, von denen je zwei L erzeugen und p rein verzweigt über $\mathbb{Q}_p$ sind.

DEFINITION. *Sei $p = char(\overline{k})$. Dann heißt K/k zahm verzweigt, falls $p \nmid e$, ansonsten wild verzweigt.*

Offenbar gilt: *Sei L/K ebenfalls endlich. Dann gilt: L/k zahm $\iff$ L/K und K/k zahm.* Um auch ein Verschiebngsargument zu erhalten, brauchen wir zuerst den

SATZ. *K/k ist genau dann rein und zahm verzweigt, falls es Primelemente $\Pi \in K$ und $\pi \in k$ gibt mit $K = k(\Pi)$ und $\Pi^e = \pi$, $p \nmid e$.*

Für den Beweis wählt man sich zunächst zwei beliebige Primelemente und konstruiert sich dann über Hensels Lemma Primelemente mit den gewünschten Eigenschaften: $\Pi_1^e = \pi_1\varepsilon$, $\varepsilon \in U_K$, $\varepsilon \equiv \varepsilon_1 \bmod \Pi_1$ mit $\varepsilon_1 \in U_k$, $\varepsilon\varepsilon_1^{-1}$ ist e-te Potenz.

LEMMA. *Ist K/k zahm und L/k endlich, so ist auch KL/L zahm.*

Zum Beweis vergrößert man zuerst K zu der galoisschen Erweiterung $H = K_{\mathrm{nr}}(\sqrt[e]{\varepsilon}, \sqrt[e]{\pi_k}, \zeta_e)$ von k (mit $K = K_{\mathrm{nr}}(\sqrt[e]{\pi_k\varepsilon})$, $\varepsilon \in U_{K_{\mathrm{nr}}}$). Dann betrachtet man die unverzweigte Erweiterung LH_{nr}/L und die *galoissche* Erweiterung LH/LH_{nr}, deren Grad ein Teiler von e und die somit zahm ist. Sie enthält LK.

SATZ. *Sei K/k galoissch mit Gruppe G, $\sigma \in G$. Dann sind folgende Aussagen äquivalent:*

1. $w(\sigma(\alpha) - \alpha) \geq i + 1$ $(\forall \alpha \in \mathfrak{O}_K)$

2. *σ wirkt trivial auf $\mathfrak{O}_K/\mathfrak{P}^{i+1}$*

3. *$w(\sigma(\alpha)-\alpha) \geq i+1$, falls $\mathfrak{O}_K = \mathfrak{o}_k[\alpha]$*

DEFINITION. *$G_i := \{\sigma \in G : w(\sigma(\alpha)-\alpha) \geq i+1 \ (\forall \alpha \in \mathfrak{O}_K)\}$ heißt die i-te Verzweigungsgruppe von K/k.*

Es gilt: $G_{-1} = G$, und G_0 ist die uns bereits bekannte Verzweigungsuntergruppe. Des weiteren ist $G_i \supseteq G_{i+1}$ und $G_i \lhd G$ für alle i. Schließlich wird $G_i = 1$ für genügend großes i. Es interessieren besonders die Stellen, an denen $G_i \neq G_{i+1}$ gilt (diese "Sprünge" sind bis heute nicht vollständig verstanden).

LEMMA. *Sei $\Pi \in \mathfrak{O}_K$ ein Primelement, $i \geq 0$, und $\sigma \in G_0$. Dann gilt:*

$$\sigma \in G_i \iff \sigma(\Pi)/\Pi \equiv 1 \bmod \mathfrak{P}^i$$

Beobachtung: $G/G_0 \simeq G_{\overline{K}/\overline{k}}$ ist zyklisch. Die Abbildung

$$\begin{array}{ccc} G_i/G_{i+1} & \to & U_K^{(i)}/U_K^{(i+1)} \\ \sigma & \mapsto & \sigma(\Pi)/\Pi \end{array}$$

ist nach obigem Lemma wohldefiniert und insbesondere ein injektiver Homomorphismus. Also sind alle Quotienten G_i/G_{i+1} p-elementar abelsch. Deshalb:

G_1 ist eine p-Gruppe (mit $p \in \mathfrak{p}$). Im Lokalen gibt es nur auflösbare Galoisgruppen.

Wir wollen nun einen Zusammenhang zwischen Verzweigung und der Differente herstellen. Dafür sei zunächst daran erinnert, daß das Inverse der Differente $\mathcal{D} = \mathcal{D}_{K/k}$ das zu $\mathfrak{O}$ duale Gitter bezüglich der Bilinearform $(x,y) = Sp_{K/k}(xy)$ ist. Im kompletten Fall gilt $\mathfrak{O} = \mathfrak{o}[\alpha]$ für ein $\alpha \in \mathfrak{O}$, also bildet $1, \alpha, \ldots, \alpha^{n-1}$ eine Basis von $\mathfrak{O}$ über $\mathfrak{o}$. Die Dualbasis sei $d_0, \ldots d_{n-1}$. Diese läßt sich aus dem Minimalpolynom von α berechnen: ist $f_\alpha(x) = (x-\alpha)(b_{n-1}x^{n-1} + \ldots b_1 x + b_0)$, so gilt $d_j = \frac{b_j}{f'_\alpha(\alpha)}$. Damit

LEMMA. *a) $\mathfrak{O}' = \mathfrak{O}\frac{1}{f'_\alpha(\alpha)}$, also $\mathcal{D} = (f'_\alpha(\alpha))$*

b) Ist K/k zusätzlich galoissch, so gilt $w(\mathcal{D}) = \sum_{i\geq 0}(|G_i|-1)$

Dies folgt aus dem offensichtlichen Zusammenhang zwischen den Koeffizienten von f_α und den b_j, woraus $\mathfrak{O} = \mathfrak{o}_k[\alpha] = \mathfrak{o}_k b_0 + \ldots + \mathfrak{o}_k b_{n-1}$ resultiert, und der Berechnung von $w_K(f'_\alpha(\alpha)) = w_K(\prod_\sigma(\alpha - \sigma(\alpha)))$.

Den Zusammenhang zwischen der Verzweigung und der Differente (im kompletten Fall) liefert nun der folgende

SATZ. *a) K/k ist unverzweigt $\iff \mathcal{D} = 1$*

b) K/k ist zahm verzweigt $\iff \mathcal{D} = \mathfrak{P}^{e-1}$. Dabei ist $\mathfrak{P}$ das maximale Ideal in $\mathfrak{O}$ und e die Verzweigungszahl.

c) Ist K/k wild verzweigt, so ist $\mathfrak{D} = \mathfrak{P}^d$ mit $d \geq e$.

Wir kehren nun zur *globalen* Situation zurück, i.e. K/k ist jetzt eine endliche Erweiterung von Zahlkörpern. Da die Differente mit Lokalisierungen verträglich ist, betrachten wir nur ein festes Primideal $\mathfrak{p} \in \mathfrak{o}_k$ und bezeichnen mit $\mathfrak{o}$ bzw. $\mathfrak{O}$ die Komplettierungen von $\mathfrak{o}_k$ bzw.

$\mathfrak{O}_K$ nach $\mathfrak{p}$. Wir wissen bereits $K \otimes_k k_\mathfrak{p} = \bigoplus_{\mathfrak{P}|\mathfrak{p}} K_\mathfrak{P}$. Analog gilt nun für die Ganzheitsringe $\mathfrak{O} \otimes_\mathfrak{o} \mathfrak{o}_\mathfrak{p} = \bigoplus_{\mathfrak{P}|\mathfrak{p}} \mathfrak{O}_\mathfrak{P}$, wobei die Gleichheit aus der natürlichen Abbildung resultiert, die $x \otimes y$ auf xy in jeder Komponente abbildet: die Surjektivität dieser Abbildung testet man am besten modulo $\mathfrak{p}$ (Nakayama); ihre Injektivität folgt dann aus der Torsionsfreiheit des freien $\mathfrak{o}_\mathfrak{p}$-Moduls $\mathfrak{O} \otimes_\mathfrak{o} \mathfrak{o}_\mathfrak{p}$. Aus $K \otimes_k k_\mathfrak{p} = \bigoplus_{\mathfrak{P}|\mathfrak{p}} K_\mathfrak{P}$ ergibt sich die Zerlegung $\mathrm{Sp}_{K/k} = \sum \mathrm{Sp}_{\mathfrak{P}/\mathfrak{p}}$ der globalen Spur in die lokalen Spuren und daraus weiter, zuerst, $\mathfrak{O}' \otimes_\mathfrak{o} \mathfrak{o}_\mathfrak{p} = \bigoplus_{\mathfrak{P}|\mathfrak{p}} \mathfrak{O}'_\mathfrak{P}$, und dann, daß $\mathcal{D}_{K_\mathfrak{P}/k_\mathfrak{p}}$ genau die Potenz von $\mathfrak{P}$ ist, mit der $\mathfrak{P}$ in $\mathcal{D}_{K/k}$ vorkommt.

FOLGERUNG. *Im Globalen gilt:* K/k *unverzweigt* $\iff \mathcal{D}_{K/k} = 1$

Beispiele :

1. *Kreiskörer* – Es sei $n = p^r m$, $p \nmid m$. Dann gilt
   (a) p ist in $\mathbb{Q}(\zeta_n)$ unverzweigt $\iff p \nmid n$ (i.e. $r = 0$)
   (b) $f_p = \mathrm{ord}_{(\mathbb{Z}/m)^\times}(p \bmod m)$, $e_p = \varphi(p^r)$
   (c) $\mathfrak{o}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$
2. Die Galoisgruppe der Artin-Schreier Gleichung $x^p - x - 1 \in \mathbb{Z}[x]$ ist die S_p.

   Denn diese Gleichung ist modulo p irreduzibel und deshalb unverzweigt bei p; weil aber der Betrag ihrer Differente > 1 ist, gibt es eine Primzahl q, die verzweigt. Ist L der Zerfällungskörper, so existiert also ein $1 \neq \sigma \in G_{\mathfrak{q},0}$ (mit $\mathfrak{q}|q$ in L). Weiter muß $f(x) = x^p - x - 1 \bmod q$ eine doppelte Wurzel besitzen, und $xf'(x) - pf(x) = (p-1)x + p$ zeigt, daß es genau $p-1$ verschiedene Wurzeln gibt. Davon läßt σ $p-2$ fest und vertauscht die beiden anderen, ist also eine Transposition.

IDÈLE UND IDÈLEKLASSEN :

Wir betrachten weiter die globale Situation, i.e. K ist ein Zahlkörper über $\mathbb{Q}$.

DEFINITION. $J_K = \{(\ldots, x_\mathfrak{p}, \ldots)_{\mathfrak{p}\subset K} \mid x_\mathfrak{p} \in K_\mathfrak{p}^\times$, *fast immer* $x_\mathfrak{p} \in U_\mathfrak{p}\}$ *heißt die Idèlegruppe von* K, $C_K = J_K/K^\times$ *die Idèleklassengruppe von* K.

Dabei laufen die $\mathfrak{p} \in K$ auch über die archimedischen Stellen. $K^\times$ liegt auf natürliche Weise in J_K. J_K wird zu einer hausdorffschen topologischen Gruppe, indem wir eine Umgebungsbasis der 1 auszeichnen: diese bestehe aus den kartesischen Produkten $\prod_{\mathfrak{p}\in K} V_\mathfrak{p}$, wobei fast immer $V_\mathfrak{p} = U_\mathfrak{p}$ und sonst $V_\mathfrak{p} = U_\mathfrak{p}^{(m)}$ gilt (bzw., bei den archimedischen Stellen, $V_\mathfrak{p}$ ein offenes Intervall um 1 ist). Damit ist $K^\times$ diskret und abgeschlossen in J_K. C_K ist mit J_K dann eine hausdorffsche lokal kompakte topologische Gruppe.
Wir betrachten zwei Abbildungen:

$$\begin{array}{ccc} J_K & \twoheadrightarrow & I_K \\ (\ldots, x_\mathfrak{p}, \ldots) & \mapsto & \prod_{\mathfrak{p}\subset K, \text{ endl.}} \mathfrak{p}^{w_\mathfrak{p}(x_\mathfrak{p})} \end{array}$$

$$\begin{array}{ccc} J_K & \to & \mathbb{R}_{>0} \\ (\ldots, x_\mathfrak{p}, \ldots) & \mapsto & \prod_{\mathfrak{p}\subset K} ||x_\mathfrak{p}||_\mathfrak{p} \end{array}$$

Bei der ersten Abbildung geht $K^\times$ surjektiv auf die Hauptidealgruppe P_K, so daß wir eine induzierte Abbildung $C_K \twoheadrightarrow cl_K$ erhalten. Bei der zweiten läuft das Produkt wieder über

alle $\mathfrak{p}$, den Kern bezeichnen wir mit J_K^0. Wegen der Produktformel enthält dieser $K^\times$. Dies induziert also Abbildungen $C_K^0 \rightarrowtail C_K \twoheadrightarrow \mathbb{R}_{>0}$, wobei $C_K^0 = J_K^0/K^\times$.

Sei nun S eine endliche Stellenmenge von $\mathfrak{p} \subset K$. Setze

$$J_S = J_{K,S} = \prod_{\mathfrak{p}\notin S} U_\mathfrak{p} \times \prod_{\mathfrak{p}\in S} K_\mathfrak{p}^\times .$$

Sind insbesondere S_∞ die archimedischen Stellen, so schreiben wir abkürzend J_∞ für J_{S_∞}. Es gilt für $S \supset S_\infty$: $K^\times \cap J_S = E_S = \{\alpha \in K : w_\mathfrak{p}(\alpha) = 0\ (\forall \mathfrak{p} \notin S)\}$; E_S sind die S-Einheiten von K. Wir erhalten folgendes kommutatives Diagramm mit exakten Zeilen und Spalten:

$$\begin{array}{ccccc} E_\infty & \rightarrowtail & K^\times & \twoheadrightarrow & P_K \\ \downarrow & & \downarrow & & \downarrow \\ J_K^0 \cap J_\infty & \rightarrowtail & J_K^0 & \twoheadrightarrow & I_K \\ \downarrow & & \downarrow & & \downarrow \\ (J_K^0 \cap J_\infty)/E_\infty & \rightarrowtail & C_K^0 & \twoheadrightarrow & cl_K \end{array}$$

Die Endlichkeit der Klassengruppe cl_K und der Dirichletsche Einheitensatz liefern nun folgenden

SATZ. *C_K^0 ist kompakt.*

Wählt man $S \supset S_\infty$ endlich, aber so groß, daß die $\mathfrak{p} \in S \setminus S_\infty$ die Klassengruppe erzeugen, so gilt $(J_\infty K^\times \cap J_S)/E_S \simeq J_\infty/E_\infty$, also insbesondere die

FOLGERUNG. *$C_K \simeq J_S/E_S$ für S hinreichend groß.*

Sei nun K/k eine endliche Erweiterung von Zahlkörpern.
Beobachtungen:

1. $J_k \subset J_K$, indem man $x_\mathfrak{P} = x_\mathfrak{p}$ für $K \supset \mathfrak{P}|\mathfrak{p}$ setzt.
2. Ist K/k zusätzlich galoissch mit Gruppe G, so wird J_K (und damit C_K) zum G-Modul: Ist $x = (\ldots, x_\mathfrak{P}, \ldots) \in J_K$ und $\sigma \in G$, so schreibe $x_\mathfrak{P} = \lim_\mathfrak{P} x_n$, wobei $\lim_\mathfrak{P}$ den Limes bezüglich $||\cdot||_\mathfrak{P}$ bezeichnet. Setze dann $\sigma(x) = (\ldots, \lim_{\sigma(\mathfrak{P})} \sigma(x_n), \ldots)$ mit dem entsprechenden Eintrag an der Stelle $\sigma(\mathfrak{P})$.
3. Sei $S \supset S_\infty$ endlich und G-stabil. Dann ist auch J_S ein G-Modul.
4. $J_K^G = J_k$; deshalb $C_k \subset C_K$.
5. Auch ohne die Voraussetzung galoissch gilt: $C_k \subset C_K$.

Etwas aufwendiger zu beweisen ist der folgende

SATZ. *Ist K/k endlich galoissch mit Gruppe G, so gilt: $C_K^G = C_k$.*

Dazu betrachte den linksexakten Funktor $F(M) = M^G$, i.e. jede kurze exakte Sequenz $M_1 \rightarrowtail M_2 \twoheadrightarrow M_3$ liefert eine Sequenz $M_1^G \rightarrowtail M_2^G \to M_3^G$. Die Surjektivität geht i.A. verloren. Wenden wir diesen Funktor auf die Sequenz $K^\times \rightarrowtail J_K \twoheadrightarrow C_K$ an, erhalten wir also $k^\times \rightarrowtail J_k \to C_K^G$. Daß hier die Surjektivität dennoch gilt, ist eine Folgerung aus Hilberts Satz 90.

Wir konzentrieren uns zunächst auf den Funktor $(\_)^G$, der einem $\mathbb{Z}G$-Modul M die abelsche Gruppe $M^G = \{m \in M : xm = m \ (\forall\, x \in G)\}$ und einer $\mathbb{Z}G$-linearen Abbildung $\varphi : M_1 \to M_2$ deren Einschränkung auf die Fixpunkte, also $\varphi : M_1^G \to M_2^G$ zuordnet. Sind weiterhin M_1 und M_2 $\mathbb{Z}G$-Linksmoduln und ist $\phi \in \mathrm{Hom}(M_1, M_2)$ nur ein Homomorphimus von abelschen Gruppen, so wird $\mathrm{Hom}(M_1, M_2)$ über $(x\phi)(m_1) = x(\phi(x^{-1}m_1))$ zum G-Modul. Die Menge aller mit G verträglichen Homomorphismen bezeichnen wir mit $\mathrm{Hom}_G(M_1, M_2)$; offenbar ist dies $\mathrm{Hom}(M_1, M_2)^G$. Insbesondere gilt für $\mathbb{Z}$ mit der trivialen G-Wirkung: $\mathrm{Hom}_G(\mathbb{Z}, M) = M^G$.

Beobachtung: Aus einer kurzen exkten Sequenz $M' \rightarrowtail M \twoheadrightarrow M''$ von $\mathbb{Z}G$-Moduln (also $\ker(M \twoheadrightarrow M'') = \mathrm{im}\,(M' \rightarrowtail M)$) wird die exakte Sequenz $(M')^G \rightarrowtail M^G \to (M'')^G$; man verliert i.a. die Surjektivität rechts.

DEFINITION. *Moduln der Form* $\mathrm{Hom}(\mathbb{Z}G, A)$*, wobei* A *eine beliebige abelsche Gruppe ist, heißen koinduzierte Moduln.*

SATZ. *Es gibt genau ein System von Funktoren* $H^q(G, M)$*,* $q \in \mathbb{N}_0$ *mit*

$H^0(G, M) = M^G$

Für jede kurze exakte Sequenz von G*-Moduln* $M' \rightarrowtail M \twoheadrightarrow M''$ *gibt es Verbindungshomomorphismen* $H^q(G, M'') \to H^{q+1}(G, M')$ *mit*

$$\ldots \to H^q(G, M') \to H^q(G, M) \to H^q(G, M'') \to H^{q+1}(G, M') \to \ldots$$

ist exakt.

$H^q(G, C) = 0$ *für* $q \geq 1$ *und alle koinduzierten* C*.*

Beweisskizze: Wähle eine $\mathbb{Z}G$-projektive Auflösung von $\mathbb{Z}$: $\ldots \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{d_0} \mathbb{Z} \to 0$, überall exakt (d.h. $\mathrm{im}\, d_q = \ker d_{q-1}$), mit projektiven $\mathbb{Z}G$-Moduln P_i; $\mathbb{Z}$ ist hier wieder der $\mathbb{Z}G$-Modul mit trivialer G-Wirkung. (Also z.B. $P_0 = \mathbb{Z}G$, $d_0 = \mathrm{augm}$; $P_1 =$ der $\mathbb{Z}G$-freie Modul mit $|G| - 1$ Erzeugenden, die auf die Erzeugenden $x - 1$ von $\Delta(G) = \ker d_0$ abgebildet werden, usw.). Dann ist auch $\mathrm{Hom}(\mathbb{Z}, M) \rightarrowtail \mathrm{Hom}(P_0, M) \to \mathrm{Hom}(P_1, M) \to \ldots$ exakt, weil der Kern der Abbildung $P_i \to P_{i-1}$ ein $\mathbb{Z}$-direkter Summand des $\mathbb{Z}$-torsionsfreien Moduls P_i ist. Allerdings erfüllt die Sequenz

$$0 \xrightarrow{0} \mathrm{Hom}_G(P_0, M) \xrightarrow{d_1} \mathrm{Hom}_G(P_1, M) \xrightarrow{d_2} \ldots$$

nur noch $d_{i+1}d_i = 0$, d.h. nur $\mathrm{im}\,(d_i)$ (=Koränder) $\subset \ker(d_{i+1})$ (=Kozkeln). Setze

$$H^q(G, M) := \ker(d_{q+1})/\mathrm{im}\,(d_q)$$

Die gewünschten Eigenschaften sind leicht, wenn auch mühsam, zu überprüfen.

Die Wohldefiniertheit folgt aus der letzten Aussage des Satzes und der behaupteten langen Kohomologiesequenz.

Diese behauptete lange exakte Sequenz ihrerseits beruht nur auf ein genaues Hinschauen auf Diagramme der Gestalt

$$\begin{array}{ccccc}
\mathrm{Hom}_G(P_{q-1}, M') & \to & \mathrm{Hom}_G(P_q, M') & \to & \mathrm{Hom}_G(P_{q+1}, M') \\
\downarrow & & \downarrow & & \downarrow \\
\mathrm{Hom}_G(P_{q-1}, M) & \to & \mathrm{Hom}_G(P_q, M) & \to & \mathrm{Hom}_G(P_{q+1}, M) \\
\downarrow & & \downarrow & & \downarrow \\
\mathrm{Hom}_G(P_{q-1}, M'') & \to & \mathrm{Hom}_G(P_q, M'') & \to & \mathrm{Hom}_G(P_{q+1}, M'')
\end{array}$$

mit exakten Spalten (weil die P_q projektiv sind).

Und die letzte Aussage im Satz für $\mathrm{Hom}(\mathbb{Z}G, A)$ und einen beliebigen $\mathbb{Z}G$-Modul N ist eine Konsequenz des Isomorphismus

$$\begin{aligned}&\mathrm{Hom}_G(N, \mathrm{Hom}(\mathbb{Z}G, A)) \to \mathrm{Hom}(N, A)\\ &\phi \mapsto [n \mapsto (\phi(n))(1)]\,, \text{ und umgekehrt } h \mapsto [n \to \phi_n \text{ mit } \phi_n(g) = h(g^{-1}n)]\,.\end{aligned}$$

Die Eindeutigkeit der $H^q(G, M)$ resultiert schließlich aus der langen Kohomologiesequenz zu $M' \overset{\varphi}{\rightarrowtail} \mathrm{Hom}(\mathbb{Z}G, M') \twoheadrightarrow \mathrm{coker}\,\varphi$ mit $\varphi(m') = [g \mapsto m']$.

Wir geben eine spezielle projektive Auflösung, die Standardauflösung, von $\mathbb{Z}$ an: Setze $P_q = \mathbb{Z}[\underbrace{G \times \ldots \times G}_{q+1}]$. Das ist ein freier G-Modul mit Basis $(g_0, g_1, \ldots, g_q)$ und Wirkung

$$g(g_0, g_1, \ldots, g_q) = (gg_0, gg_1, \ldots, gg_q)\,.$$

Definiere für $q > 0$

$$\begin{array}{rcl} P_q & \overset{d}{\to} & P_{q-1} \\ (g_0, \ldots, g_q) & \mapsto & \sum\limits_{i=0}^{q} (-1)^i (g_0, \ldots, g_{i-1}, g_{i+1}, \ldots, g_q) \end{array}$$

$P_0 = \mathbb{Z}G \to \mathbb{Z}$ sei die Augmentation. Dann ist

$$\ldots \overset{d}{\to} P_1 \overset{d}{\to} P_0 \overset{aug}{\to} \mathbb{Z} \to 0$$

exakt.

Mittels der Standardauflösung bestimmen wir die ersten Kozykel und Koränder. Sei dazu $f \in \mathrm{Hom}_G(P_q, M)$. Da f eine G-verträgliche Abbildung ist, können wir ebenso $f \in \mathrm{Hom}(\underbrace{G \times \ldots \times G}_{q}, M)$ auffassen. Schreibt man f in der Form $f(1, g_1, g_1g_2, \ldots, g_1g_2 \cdots g_q) = \varphi(g_1, g_2, \ldots, g_q))$ so liefert eine direkte Rechnung, daß die 1-Kozykeln (i.e. $q = 1,\ d_1(\varphi) = 0$) von der Form $\varphi : G \to M$ mit $\varphi(g_1g_2) = g_1\varphi(g_2) + \varphi(g_1)$ und die 1-Koränder (i.e. $\varphi \in \mathrm{im}\,(d_0)$) die $\varphi : G \to M$ mit $\varphi(g) = gm - m$ für ein $m \in M$ sind. Hat M triviale G-Wirkung, so gilt also $H^1(G, M) = \mathrm{Hom}(G, M)$, insbesondere ist $H^1(G, \mathbb{Z}) = 0$ für endliches G. Entsprechend erhält man für die 2-Kozykeln die Bedingung $g_1\varphi(g_2, g_3) - \varphi(g_1g_2, g_3) + \varphi(g_1, g_2g_3) = \varphi(g_1, g_2)$. Die 2-Koränder erfüllen $\varphi(g_1, g_2) = g_1\phi(g_2) - \phi(g_1g_2) + \phi(g_1)$ für ein $\phi : G \to M$.

Beispiel 1. $H^1(G, K^\times) = 1$ (und damit $C_K^G = C_k$). Dazu rechnet man nach, daß sich jeder 1-Kozykel f als $\tau \mapsto c/c^\tau$ mit einem $c = \sum_{\sigma \in G} f(\sigma) d^\sigma \in K^\times$ schreiben läßt, wobei d eine Normalbasis von K/k erzeuge.

Beispiel 2. Betrachte kurze exakte Gruppensequenzen der Form $M \rightarrowtail E \twoheadrightarrow G$ mit abelscher (endlicher) Gruppe M, also $M \lhd E$ und $E/M \simeq G$. Es wirke G so auf M: Wähle zu $g \in G$ ein Urbild $e \in E$ und setze $gm = e^{-1}me \in M$. Dies ist unabhängig von der Wahl des Urbilds. Eine Abbildung $s : G \to E$ mit $s(g) \bmod M = g$ heiße Schnitt. Es ist dann $E = \{m \cdot s(g) : m \in M,\ g \in G\}$ und die Gleichung

$$m_1 s(g_1) m_2 s(g_2) = m_1 s(g_1) m_2 s(g_1)^{-1} s(g_1) s(g_2) = m_1 m_2^{g_1^{-1}} f(g_1, g_2) s(g_1 g_2)$$

definiert eine Funktion $f : G \times G \to M$, den sogenannten Faktorzykel. Die Assoziativität in E liefert für f genau die obige Bedingung eines 2-Kozykels. Ist nun s' ein weiterer Schnitt, der

analog eine Funktion f' definiert, so unterscheidet sich diese von f um einen 2-Korand. Es folgt, daß $H^2(G,M)$ die Gruppenerweiterungen $M \rightarrowtail E \twoheadrightarrow G$ klassifiziert (mit der Gleichheit

$$\begin{array}{ccccc} M & \rightarrowtail & E_1 & \twoheadrightarrow & G \\ \| & & \downarrow & & \| \\ M & \rightarrowtail & E_2 & \twoheadrightarrow & G \end{array}$$

resultierend aus) . Ist überdies die Erweiterung $M_1 \rightarrowtail E_1 \twoheadrightarrow G$ zentral, d.h. $M_1 \leq Z(E_1)$ oder: G wirkt trivial auf M_1, so wird eine G-Abbildung $M_1 \xrightarrow{\beta} M_2$ von der induzierten Abbildung $H^2(G,M_1) \to H^2(G,M_2)$ in das kommutative *push-out*-Diagramm

$$\begin{array}{ccccc} M_1 & \overset{\alpha}{\rightarrowtail} & E_1 & \overset{\varepsilon}{\twoheadrightarrow} & G \\ \beta\downarrow & & \gamma\downarrow & & \| \\ M_2 & \overset{\alpha'}{\rightarrowtail} & E_2 & \overset{\delta}{\twoheadrightarrow} & G \end{array}$$

übersetzt, in dem $E_2 = E_1 \times M_2 / \{(\alpha(m_1), -\beta(m_1))\}$ und $\alpha'(m_2) = \overline{(m_2, 1)}$ sowie $\delta(\overline{(e_1, m_2)}) = \varepsilon(m_1)$ gilt.

Als nächstes leiten wir eine zur Kohomologietheorie analoge Theorie für den Funktor $M \rightsquigarrow M_G$ her, wobei $M_G \overset{\text{def}}{=} M/\Delta(G)M$ mit $\Delta(G) = \langle g-1 : g \in G\rangle_{\mathbb{Z}}$ gilt, so daß also M_G der größte G-invariante Faktormodul von M ist. Dazu betrachten wir zunächst Tensorprodukte von G-Moduln M und N. Über $g(m \otimes n) = gm \otimes gn$ $(\forall m \in M, n \in N)$ wird $M \otimes_{\mathbb{Z}} N$ zu einem G-Modul. Setze $mg := g^{-1}m$. Damit gilt das

LEMMA. *Für alle G-Moduln M und N gilt*

1. $M \otimes_{\mathbb{Z}G} N = (M \otimes_{\mathbb{Z}} N)_G$
2. $(\mathbb{Z} \otimes_{\mathbb{Z}} M)_G = M_G$
3. *Ist $M' \rightarrowtail M \twoheadrightarrow M''$ exakt, so auch $M'_G \to M_G \twoheadrightarrow M''_G$ (die Injektivität bleibt nicht unbedingt erhalten).*

DEFINITION. *Moduln der Form $\mathbb{Z}G \otimes A$ heißen induzierte Moduln. Dabei ist A wieder eine beliebige abelsche Gruppe, auf der G trivial wirkt.*

Für endliches G sind dies die alten koinduzierten Moduln aufgrund von

$$\mathrm{Hom}(\mathbb{Z}G, A) \simeq \mathrm{Hom}(\mathrm{Hom}(\mathbb{Z}G, \mathbb{Z}), A) \simeq \mathrm{Hom}(\hat{\mathbb{Z}}, A) \simeq \mathbb{Z}G \otimes A$$

(vgl. auch das folgende Lemma).

Entsprechend zu früher gilt der

SATZ. *Es gibt genau ein System von Funktoren $H_q(G,M)$, $q \in \mathbb{N}_0$ mit*

$H_0(G,M) = M_G$

Für jede kurze exakte Sequenz von G-Moduln $M' \rightarrowtail M \twoheadrightarrow M''$ gibt es Verbindungshomomorphismen $H_{q+1}(G,M'') \to H_q(G,M')$ mit

$$\ldots \to H_q(G,M') \to H_q(G,M) \to H_q(G,M'') \to H_{q-1}(G,M') \to \ldots$$

ist exakt.

$H_q(G,C) = 0$ *für $q \geq 1$ und alle induzierten C.*

Zum Beweis benutzt man dieselbe projektive Auflösung von $\mathbb{Z}$ wie in der Kohomologie. Wählt man den Standardkomplex und benutzt

$$\mathbb{Z}[G^{q+1}] \otimes_{\mathbb{Z}G} M = \mathbb{Z}[G^q] \otimes M = \{\sum_{G^q}(g_1, \ldots, g_q) \otimes f(g_1, \ldots, g_q)\},$$

so erhält man die 1-Zykel als die Abbildungen $f : G \to M$ mit $\sum_{g\in G}(g^{-1} - 1)f(g) = 0$.

Wenden wir $(\_)_G$ auf die Sequenz $\Delta G \rightarrowtail \mathbb{Z}G \twoheadrightarrow \mathbb{Z}$ an, so erhalten wir bei trivialer Wirkung von G auf $\mathbb{Z}$

$$H_1(G, \mathbb{Z}) = \Delta(G)/\Delta(G)^2 = G/G', \quad g - 1 \bmod \Delta(G)^2 \leftrightarrow g \bmod G'.$$

LEMMA. *Sei* $P^* := \mathrm{Hom}(P, \mathbb{Z})$, *P* $\mathbb{Z}G$*-projektiv, M ein G- Modul. Dann ist* $\mathrm{Hom}(P^*, M) = P \otimes M$.

Den Isomorphismus stiftet die Abbildung $p \otimes m \mapsto \Phi : [\phi \mapsto \phi(p)m]$. Für die Umkehrabbildung wähle eine $\mathbb{Z}$-Dualbasis φ_j einer Basis p_i von P und bilde den Homomorphismus f auf $\sum_i a_i \otimes f(b_i)$ ab.

Betrachte nun die Abbildung

$$\begin{array}{rccc} N_G : & M & \to & M \\ & m & \mapsto & \sum\limits_{g\in G} gm \end{array}$$

Beachte: $\mathrm{im}\,(N_G) \subset M^G$ und $\Delta(G)\cdot M \subset \ker(N_G)$, also faktorisiert N_G über M_G. Sei $\ldots P_1 \to P_0 \to \mathbb{Z} \to 0$ wieder eine projektive Auflösung von $\mathbb{Z}$. In dem Diagramm

$$\begin{array}{ccccccccc} 0 & \to & M^G & \to & \mathrm{Hom}_G(P_0, M) & \stackrel{d_1}{\to} & \mathrm{Hom}_G(P_1, M) & \to \ldots \\ & & N_G \uparrow & & d_0 \uparrow & & & \\ 0 & \leftarrow & M_G & \leftarrow & \mathrm{Hom}_G(P_0^*, M) & \stackrel{d_{-1}}{\leftarrow} & \mathrm{Hom}_G(P_1^*, M) & \leftarrow \ldots \end{array}$$

liefert dann die obere Zeile $H^q(G, M)$ und die untere $H_q(G, M)$ [4]. Außerdem ist $d_i d_{i-1} = 0$ für alle i.

DEFINITION (Tatesche Kohomologie). $\hat{H}^q(G, M) = H^q(G, M)$ *für* $q \geq 1$, $\hat{H}^{-q}(G, M) = H_{q-1}(G, M)$ *für* $q \geq 2$, $\hat{H}^0(G, M) = M^G/N_G(M)$ *und* $\hat{H}^{-1}(G, M) = ker(N_G)/\Delta GM$.

Es gilt offensichtlich: $\hat{H}^{-1}(G, M) = \ker(d_0)/\mathrm{im}\,(d_{-1})$ und $\hat{H}^0(G, M) = \ker(d_1)/\mathrm{im}\,(d_0)$.

SATZ (Tate). *Aus der kurzen exakte Sequenz* $M' \rightarrowtail M \twoheadrightarrow M''$ *von G-Moduln resultiert die lange exakte Sequenz*

$$\ldots \to \hat{H}^q(G, M') \to \hat{H}^q(G, M) \to \hat{H}^q(G, M'') \to \hat{H}^{q+1}(G, M') \to \ldots$$

für alle $q \in \mathbb{Z}$. *Des weiteren:* $\hat{H}^q(G, M) = 0$ *für induzierte (oder koinduzierte) Moduln.*

[4] statt der $\mathrm{Hom}_G(P_q^*, M)$ kann man natürlich genausogut $P_q \otimes_G M$ schreiben

Zu betrachten ist nur das Stück, an dem die lange Homologie- mit der langen Kohomologie-Sequenz zusammengesetzt wird. Man rechnet nach, daß das Diagramm

$$\begin{array}{ccccccccccc} & & \hat{H}^{-2}(G,M'') & & M'_G & & M_G & & M''_G & & \\ & & \| & & \| & & \| & & \| & & \\ \ldots \to & & H_1(G,M'') & \to & H_0(G,M') & \to & H_0(G,M) & \to & H_0(G,M'') & \to & 0 \\ & & \downarrow & & N_G \downarrow & & N_G \downarrow & & N_G \downarrow & & \downarrow \\ & & 0 & \to & H^0(G,M') & \to & H^0(G,M) & \to & H^0(G,M'') & \to & H^1(G,M') \to \ldots \end{array}$$

kommutiert. Da $\hat{H}^{-1}(G,M) \subset M_G$ induziert das Diagramm die Abbildungen

$$\hat{H}^{-2}(G,M'') \to \hat{H}^{-1}(G,M') \to \hat{H}^{-1}(G,M) \to \hat{H}^{-1}(G,M'')\,.$$

Und indem man obiges Diagramm für $N = M', M, M''$ um die exakten Spalten $\hat{H}^{-1}(G,N) \rightarrowtail H_0(G,N) \overset{N_G}{\to} H^0(G,N) \twoheadrightarrow \hat{H}^0(G,N)$ erweitert, gewinnt man aus dem *Schlangenlemma* die restlichen Abbildungen. Letzteres besagt folgendes: Ist

$$\begin{array}{ccccc} A & \overset{\alpha}{\to} & B & \twoheadrightarrow & C \\ i \downarrow & & j \downarrow & & k \downarrow \\ A' & \rightarrowtail & B' & \overset{\sigma}{\to} & C' \end{array}$$

ein kommutatives Diagram mit exakten Zeilen wie gezeigt, so resultiert eine exakte Sequenz $\ker i \overset{\alpha}{\to} ker j \to \ker k \to \operatorname{coker} i \to \operatorname{coker} j \overset{\sigma}{\to} \operatorname{coker} k$ und die linke (rechte) Abbildung ist injektiv (surjektiv), falls α injektiv (σ surjektiv) ist.

Beispiel: Sei $G = \langle g \rangle$ zyklisch. Dann ist $\Delta G = \mathbb{Z}G(g-1)$ (geometrische Reihe!), des weiteren haben wir die kurze exakte Sequenz $\mathbb{Z} \rightarrowtail \mathbb{Z}G \twoheadrightarrow \Delta G$, wobei die erste Abbildung durch $1 \mapsto \hat{G} = \sum_{x \in G} x$ und die zweite durch $1 \mapsto g - 1$ gegeben ist. Durch Zusammensetzen mit $\Delta G \rightarrowtail \mathbb{Z}G \twoheadrightarrow \mathbb{Z}$ erhält man eine exakte Sequenz $\mathbb{Z} \overset{\hat{G}}{\rightarrowtail} \mathbb{Z}G \overset{g-1}{\to} \mathbb{Z}G \twoheadrightarrow \mathbb{Z}$.

Das Aneinanderhängen dieser Vierersequenzen liefert

LEMMA. *Sei G zyklisch und M ein G-Modul. Dann gilt $H^q(G,M) = H^{q+2}(G,M)$ für alle $q \in \mathbb{Z}$.*

Insbesondere gilt $H^2(G,M) = H^0(G,M) = M^G/N_G M$ und $H^1(G,M) = H^{-1}(G,M) = \ker N_G/(g-1)M$ mit $G = \langle g \rangle$. Für zyklisches G ist daher Hilberts Satz 90 genau der in der Algebra bewiesene Satz *Ist L/K zyklisch und $N_{L/K}(\lambda) = 1$, so gilt $\lambda = \alpha/g(\alpha)$ für ein $\alpha \in L^\times$.*

Als nächstes wollen wir Homomorphismen $f : G \to H$ von Gruppen betrachten. Ist M ein H-Modul, so wird M über $gm = f(g)m$ auch zu einem G-Modul. f induziert dann eine Abbildung $H^q(H,M) \to H^q(G,M)$. Ist nämlich $\psi : H \times \ldots \times H \to M$ ein q-Kozykel bzgl. H, so ist $\phi : G \times \ldots \times G \to M$, $(g_1, \ldots, g_q) \mapsto \psi(f(g_1), \ldots, f(g_q))$ ein q-Kozykel bzgl. G.

Im folgenden schreiben wir $H^q(G,M)$ für $\hat{H}^q(G,M)$, falls keine Verwechslungsgefahr besteht. Sei nun M ein G-Modul und U eine Untergruppe von G. Dann kann die Abbildung

$$H^0(G,M) \to H^0(U,M)\,, \quad m \mapsto m : M \to M$$

über die induzierten bzw. koinduzierten Moduln für alle $q \in \mathbb{Z}$ fortgesetzt werden. Ist $G = \bigcup x_i U$ eine Zerlegung von G in Nebenklassen, so kann man entsprechend die Abbildung

$$N_{G/U} : H^0(U,M) \to H^0(G,M)\,, \quad m \mapsto \sum x_i m : M \to M$$

für alle $q \in \mathbb{Z}$ fortsetzen.

DEFINITION. *Die Abbildung* $\mathrm{res} : H^q(G,M) \to H^q(U,M)$ *heißt Restriktion, die Abbildung* $\mathrm{cor} : H^q(U,M) \to H^q(G,M)$ *Korestriktion.*

Es gilt: $\mathrm{cor}(\mathrm{res}\,(y)) = [G:U]y$. Ist also insbesondere $U = 1$, so folgt $|G|H^q(G,M) = 0$ aus $H^q(1,M) = 0$.

FOLGERUNG. *Ist* M *endlich erzeugt über* $\mathbb{Z}G$*, so ist* $H^q(G,M)$ *endlich.*

Auf dem Niveau $q = -2$ definiert die Restriktion eine Abbildung $G/G' \to U/U'$, nämlich die gruppentheoretische Verlagerung. In umgekehrter Richtung gibt die Korestriktion die natürliche Einbettung zurück.

Aus der Sequenz $\mathbb{Z} \rightarrowtail \mathbb{Q} \twoheadrightarrow \mathbb{Q}/\mathbb{Z}$ erhalten wir noch

$$H^2(G,\mathbb{Z}) \simeq \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z})\,.$$

DEFINITION. *Sei* M *ein* G*-Modul,* N *ein Normalteiler in* G *und* $f : G \to G/N$ *die Projektion. Dann heißt die über* $H^q(G/N, M^N) \to H^q(G,M^N) \to H^q(G,M)$ *definierte Abbildung* $\mathrm{inf} : H^q(G/N,M^N) \to H^q(G,M)$ *die Inflation (hier ist* $q \geq 1$*).*

SATZ (Restriktion-Inflationsequenz). *1.* $H^1(G/N,M^N) \overset{\mathrm{inf}}{\rightarrowtail} H^1(G,M) \overset{\mathrm{res}}{\to} H^1(N,M)$ *ist exakt.*

2. Falls $H^i(N,M) = 0$ *für* $1 \leq i \leq q-1$*, so ist* $H^q(G/N,M^N) \overset{\mathrm{inf}}{\rightarrowtail} H^q(G,M) \overset{\mathrm{res}}{\to} H^q(N,M)$ *exakt.*

Dazu rechnet man den ersten Teil direkt nach. Den zweiten Teil erhält man induktiv durch Dimensionsverschiebung: Man bettet M in einen induzierten Modul C ein, $M \rightarrowtail C \twoheadrightarrow M'$. Dann ist $H^i(N,M') = H^{i+1}(N,M) = 0$ für $1 \leq i \leq q-1$ und wir erhalten per Induktion die entsprechende Sequenz für M' auf dem Niveau $q-1$. Diese stimmt mit der für M auf dem Niveau q überein.

Eine wichtige Verallgemeinerung des Prinzips der Dimensionsverschiebung resultiert aus dem

LEMMA (Shapiros Lemma). *Ist* U *eine Untergruppe von* G *und* M *ein* U*-Modul, so gilt für* $q \geq 0$*:* $H^q(G,\mathrm{Hom}_U(\mathbb{Z}G,M)) = H^q(U,M)$ *sowie* $H_q(G,\mathbb{Z}G \otimes_{\mathbb{Z}U} M) = H_q(U,M)$.

Schlußbemerkungen :

1. Dieses letzte Kapitel ist zumindest insofern unvollständig, als weder das *Cupprodukt* der Kohomologietheorie noch die sogenannten *kohomologisch trivialen* G-Moduln Erwähnung fanden. Das soll deshalb in der Fortsetzungsvorlesung im kommenden Semester am Anfang stehen; erst dann ist ein stabiles Fundament für die Herleitung der *Klassenkörpertheorie* gelegt.

2. Eine Zahlentheorievorlesung ohne L-Reihen ist ein Torso. Auch hier sei auf die Fortsetzungsvorlesung verwiesen.

3. Die Herleitung der Gruppenkohomologie aus den Funktoren $M \rightsquigarrow M^G$ und $M \rightsquigarrow M_G$ ist ein Spezialfall der Herleitung sogenannter *abgeleiteter Funktoren*. Genauso prominente Beispiele wie $H^*(G,M)$ sind etwa $\mathrm{Ext}^*_R(M,N)$ und $\mathrm{Tor}^*_R(M,N)$. Bei den beiden letzteren wird von R-Moduln M und N (im zweiten Fall M_R und ${}_RN$) und den Funktoren $N \rightsquigarrow \mathrm{Hom}_R(M,N)$, $N \rightsquigarrow M \otimes_R N$ ausgegangen (M ist also fest, N läuft; R ist ein Ring mit 1). Der erste Funktor ist linksexakt, der zweite rechtsexakt. Nimmt man eine R-projektive Auflösung $\ldots \to P_2 \to P_1 \to P_0 \twoheadrightarrow M$ von M und die Homologie in

$$\begin{aligned}
&\to \mathrm{Hom}_R(P_{q-1},N) \xrightarrow{d_{q-1}} \mathrm{Hom}_R(P_q,N) \xrightarrow{d_q} \mathrm{Hom}_R(P_{q+1},N) \xrightarrow{d_{q+1}} \quad \text{bzw.}\\
&\to P_{q+1} \otimes_R N \xrightarrow{d_{q+1}} P_q \otimes_R N \xrightarrow{d_q} P_{q-1} \otimes_R N \xrightarrow{d_{q+1}}, \quad \text{also}\\
&\mathrm{Ext}^q_R(M,N) \overset{\mathrm{def}}{=} \ker d_q/\mathrm{im}\, d_{q-1} \quad \text{bzw.} \quad \mathrm{Tor}^q_R(M,N) \overset{\mathrm{def}}{=} \ker d_q/\mathrm{im}\, d_{q+1},
\end{aligned}$$

so erhält man durch R, M, N wohlbestimmte abelsche Gruppen $\mathrm{Ext}^*_R(M,N)$, $\mathrm{Tor}^*_R(M,N)$, die in zu einer kurzen exakten Sequenz $N' \rightarrowtail N \twoheadrightarrow N''$ gehörige lange exakte Sequenzen

$$\begin{aligned}
&\to \mathrm{Ext}^q_R(M,N') \to \mathrm{Ext}^q_r(M,N) \to \mathrm{Ext}^q_R(M,N'') \to \mathrm{Ext}^{q+1}_R(M,N') \to\\
&\quad (\, q \geq 0\,,\ \mathrm{Ext}^0_R(M,N) = \mathrm{Hom}_R(M,N)\,) \quad \text{bzw.}\\
&\to \mathrm{Tor}^q_R(M,N') \to \mathrm{Tor}^q_R(M,N) \to \mathrm{Tor}^q_R(M,N'') \to \mathrm{Tor}^{q-1}_R(M,N) \to\\
&\quad (\, q \geq 0\,,\ \mathrm{Tor}^0_R(M,N) = M \otimes_R N\,)
\end{aligned}$$

passen. Der Beweis davon ist analog dem für $H^*(G,M)$ – mit zwei Ausnahmen:

i) solange nicht M endlich erzeugt über R und zudem R noethersch ist, kann man keine Auflösung von M durch endlich erzeugte projektive Moduln P_q erreichen,

ii) der Beweis der Unabhängigkeit von der Wahl der Auflösung verlangt ein Extraargument, da wir hier nicht über das Konzept von koinduzierten oder induzierten Objekten verfügen ($R = \mathbb{Z}G$ ist ein sehr spezieller Ring: nämlich eine *Ordnung* über dem ganz einfachen Ring $\mathbb{Z}$).

Übungen zur Vorlesung Zahlentheorie I, SS 2007, gestellt von Dipl.-Math. A. Nickel

(Lösungshilfen im Anschluß an Blatt 11)

Blatt 1

1. Sind $\frac{1+2\sqrt{6}}{1-\sqrt{6}}$ und $\frac{3+2\sqrt{6}}{1-\sqrt{6}}$ ganz über $\mathbb{Z}$?

2. Sei R ein (kommutativer) Ring. Zeige:
   R faktoriell $\Longrightarrow$ R ist ganz abgeschlossen in seinem Quotientenkörper

   (Zur Erinnerung: Ein Element $r \in R$ heißt irreduzibel, falls $r \notin R^\times$ und aus $r = st$ mit $s, t \in R$ folgt, dass $s \in R^\times$ oder $t \in R^\times$. Ein Ring R heißt faktoriell oder ZPE-Ring, falls er nullteilerfrei ist, und jedes Element $r \in R$ bis auf Einheiten eindeutig in irreduzible Elemente faktorisiert werden kann.)

3. (a) Seien $R \subset S$ Ringe, R noethersch. Zeige: R ist genau dann ganz abgeschlossen in S, wenn $R[x]$ in $S[x]$ ganz abgeschlossen ist.
   Hinweis: Verwende folgendes Resultat aus der Algebra: Ist R ein noetherscher Ring und M ein endlich erzeugter R-Modul, so ist jeder Untermodul von M auch endlich erzeugt.

   (b) Sei R ein noetherscher, nullteilerfreier Ring mit Quotientenkörper K. Zeige:
   R ist ganz abgeschlossen in K $\iff$ R[x] ist ganz abgeschlossen in K(x)

Blatt 2

1. Sei $d \in \mathbb{Z}$ quadratfrei, $K = \mathbb{Q}(\sqrt{d})$ und $\mathfrak{o}_K = \mathbb{Z} \oplus \omega\mathbb{Z}$ der Ring der ganzen Zahlen in K, wobei $\omega = \sqrt{d}$ bzw. $\omega = \frac{1+\sqrt{d}}{2}$ für $d \not\equiv 1 \bmod 4$ bzw. $d \equiv 1 \bmod 4$. Zeige:

   (a) Die Teilringe S mit $\mathbb{Z} \subset S \subset \mathfrak{o}_K$ sind gegeben durch die Ringe $R_f := \mathbb{Z} + f\mathfrak{o}_K$ mit $f \in \mathbb{N}_0$.

   (b) R_f ist für $f \neq 0, 1$ kein Dedekindring.

2. Sei $d = -p_1 \cdot \ldots \cdot p_t$ quadratfrei mit $t \geq 2$ und $d \not\equiv 1 \bmod 4$, $K = \mathbb{Q}(\sqrt{d})$ und $\mathfrak{o}_K = \mathbb{Z} \oplus \omega\mathbb{Z}$ mit ω wie in Aufgabe 1. Sei außerdem $b \in \mathbb{Z}$ ein Teiler von d und $\mathfrak{a}_b := b\mathbb{Z} \oplus \omega\mathbb{Z}$. Zeige:

   (a) $\mathfrak{a}_b$ ist ein Ideal in $\mathfrak{o}_K$.

   (b) Für $1 < b < d$ ist $\mathfrak{a}_b$ kein Hauptideal.

   (c) Seien b_1 und b_2 Teiler von d mit $1 < b_1, b_2 < d$ und $\mathrm{ggT}(b_1, b_2) = 1$. Dann gilt: $\mathfrak{a}_{b_1}\mathfrak{a}_{b_2} = \mathfrak{a}_{b_1 b_2}$.

(d) Die Klassengruppe cl_K enthält eine Untergruppe der Ordnung 2^{t-1} vom Typ $C_2 \times \cdots \times C_2$.

3. Sei R ein nullteilerfreier Ring. Ein Element $\pi \in R$ heißt prim, falls das Hauptideal (π) ein Primideal in R ist. Zeige:

   (a) π prim $\Longrightarrow \pi$ irreduzibel

   (b) Ist R ein Hauptidealring, so gilt in (a) auch die Umkehrung.

   (c) Im Allgemeinen ist die Umkehrung in (a) falsch.
   (Betrachte etwa Zerlegungen der Zahl 6 in $\mathbb{Z}[\sqrt{-5}]$)

   (d) Jeder nullteilerfreie Hauptidealring ist faktoriell.

Blatt 3

1. Sei $\mathfrak{o}$ ein Dedekindring mit Quotientenkörper K. Zeige:

   (a) $\mathfrak{o}$ ist genau dann faktoriell, wenn die Klassenzahl $h_K = 1$ ist.

   (b) Sei $\mathfrak{m} \neq 0$ ein ganzes Ideal von $\mathfrak{o}$. Dann liegt in jeder Idealklasse von cl_K ein ganzes, zu $\mathfrak{m}$ teilerfremdes Ideal.

2. Sei $K = \mathbb{Q}(\alpha)$ eine endliche Erweiterung von $\mathbb{Q}$ vom Grad n mit ganzem α und $f(x) = f_\alpha(x) \in \mathbb{Z}[x]$ das Minimalpolynom von α.

   (a) Sei $M = \bigoplus_{i=0}^{n-1} \alpha^i \mathbb{Z} \subset \mathfrak{o}_K$. Dann gilt:

   $$d(M) = d_f = (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(f'(\alpha)).$$

   (Erinnerung: Für $f(x) = \prod(x - \omega_j)$ ist $d_f = \prod_{i<j}(\omega_i - \omega_j)^2$. Benutze die Vandermondesche Determinante!)

   (b) $d_K = d(\mathfrak{o}_K) \in \mathbb{Z}$ und $d_K \equiv 0, 1 \bmod 4$ (Stickelbergerscher Diskriminantensatz).
   (Hinweis: Die Determinante $\det(\sigma_i(\omega_j))$ einer Ganzheitsbasis ω_j ist eine Summe von Termen, die mit einem Plus- oder Minuszeichen versehen sind (Laplacescher Entwicklungssatz). Ist P bzw. N die Summe der Terme mit Plus- bzw. Minuszeichen, so gilt $d_K = (P - N)^2 = (P + N)^2 - 4PN$.)

   (c) Für $f(x) = x^3 + 13x + 5$ und $f(x) = x^3 + 13x + 4$ ist $\mathfrak{o}_K = \mathbb{Z} \oplus \alpha\mathbb{Z} \oplus \alpha^2\mathbb{Z}$.

3. Sei L das Kompositum zweier reell quadratischer Teilkörper. Man zeige:

   (a) L hat über $\mathbb{Q}$ den Grad 4 und besitzt genau drei reell quadratische Teilkörper.

   (b) Die Einheiten von L sind von der Form $E =< -1 > \times < \eta_1 > \times < \eta_2 > \times < \eta_3 >$ mit Grundeinheiten η_i, $i = 1, 2, 3$.

   (c) Seien $\epsilon_1, \epsilon_2, \epsilon_3 > 1$ die Grundeinheiten der reell quadratischen Teilkörper von L und $E_0 =< -1 > \times < \epsilon_1 > \times < \epsilon_2 > \times < \epsilon_3 >$. Dann ist der Regulator des Systems $\epsilon_1, \epsilon_2, \epsilon_3$ von Null verschieden, also $q := [E : E_0] < \infty$.

   (d) $q|8$.

(e) Für $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ ist $q \neq 1$.

Blatt 4

1. Sei $K/\mathbb{Q}$ eine endliche Körpererweiterung vom Grad $n = r+2s$, wobei r bzw. s die Anzahl der reellen bzw. konjugiert komplexen Einbettungen von K bezeichne. Sei außerdem $0 \neq \mathfrak{a}$ ein ganzes Ideal in $\mathfrak{o}_K$, dem Ring der ganzen Zahlen von K. Wir definieren die Minkowski-Schranke
$$M = \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}.$$
Dann gilt:
   (a) Es gibt ein $0 \neq a \in \mathfrak{a}$ mit $|N_{K/\mathbb{Q}}(a)| \leq M \cdot N(\mathfrak{a})$.
   Hinweis: Die Menge
   $$C = \{(x_1, \ldots, x_r, x_{r+1}, \ldots, x_{r+s}) \in \mathbb{R}^r \oplus \mathbb{C}^s | \sum_{i=1}^{r} |x_i| + 2\sum_{i=1}^{s} |x_{r+i}| \leq t\}$$
   hat das Volumen $2^r \pi^s \frac{t^n}{n!}$ (ohne Beweis!). Verwende außerdem die Ungleichung zwischen geometrischem und arithmetischem Mittel: $\frac{1}{n}\sum_{i=1}^{n} |z_i| \geq (\prod_{i=1}^{n} |z_i|)^{1/n}$.
   (b) Es gibt ein ganzes Ideal $\mathfrak{a}_1$ in der Idealklasse $[\mathfrak{a}] \in \mathrm{cl}_K$ mit $N(\mathfrak{a}_1) \leq M$.
2. Bestimme mit Hilfe der Minkowski-Schranke die Klassenzahl von $K = \mathbb{Q}(\sqrt{-15})$.
3. Sei $K/\mathbb{Q}$ eine endliche Erweiterung. Dann enthält $\mathfrak{o}_K$ unendlich viele Primideale von Restklassengrad 1.
   Hinweis: Betrachte $\log \zeta_K(\sigma)$ für $\sigma > 1$ und verwende die Reihenentwicklung $\log(1-x) = -\sum_{n=1}^{\infty} \frac{x^n}{n}$ für $|x| < 1$. Trenne die Terme für $n = 1$ und $n > 1$. Welche Terme konvergieren schon für kleinere σ?

Blatt 5

1. Sei $f(x) \in \mathbb{Z}[x]$ ein irreduzibles Polynom vom Grad $n > 1$. Dann ist die Diskriminante $d_f \neq \pm 1$.
   Hinweis: Verwende die Minkowski-Schranke.
2. Sei $K = \mathbb{Q}(\zeta)$ mit einer primitiven l^n-ten Einheitswurzel ζ, l eine Primzahl. Sei weiter $\lambda = 1 - \zeta \in \mathfrak{o}_K$. Zeige:
   (a) Das Hauptideal (λ) ist ein Primideal und es gilt $l\mathfrak{o}_K = (\lambda)^e$ mit $e = [K : \mathbb{Q}]$. Insbesondere ist der Restklassengrad f von (λ) gleich 1.
   Hinweis: Betrachte $f_\zeta(x) \in \mathbb{Z}[x]$, das Minimalpolynom von ζ, an der Stelle $x = 1$.
   (b) $d := d(1, \zeta, \ldots, \zeta^{e-1}) = \pm l^s$ mit $s = l^{n-1}(nl - n - 1)$.
   Hinweis: Differenziere die Gleichung $(x^{l^{n-1}} - 1) f_\zeta(x) = x^{l^n} - 1$ nach x und setze ζ ein.

(c) $\mathfrak{o}_K = \mathbb{Z}[\zeta]$.
Hinweis: $d\mathfrak{o}_K \subset \mathbb{Z}[\zeta]$ und $\mathfrak{o}_K = \mathbb{Z}[\zeta] + (\lambda)$, warum?

(d) Bestimme die Differente $\mathfrak{D}_{K/\mathbb{Q}}$.

(e) Sei $K^+ = \mathbb{Q}(\zeta + \overline{\zeta})$ und $l \neq 2$. Bestimme die Differenten $\mathfrak{D}_{K/K^+}$ und $\mathfrak{D}_{K^+/\mathbb{Q}}$.

Blatt 6

1. Sei $a = \sum_{\nu=-k}^{\infty} a_\nu p^\nu \in \mathbb{Q}_p$ mit $0 \leq a_\nu < p$ eine p-adische Zahl. Zeige:
Es gilt $a \in \mathbb{Q}$ genau dann, wenn die Folge der a_ν periodisch wird.

   Hinweis: Für die Richtung „$a \in \mathbb{Q} \Longrightarrow (a_\nu)_{\nu \geq -k}$ wird periodisch“ überlege man sich zunächst, dass a genau dann periodisch wird, wenn es $-a$ wird. Sei dann $\frac{m}{n} \in \mathbb{Q}$ und ohne Einschränkung $(p, n) = 1$ und $\frac{m}{n} < 0$. Dann gibt es ganze Zahlen l, j, b, c mit $0 \leq b < p^l$ und $0 \leq c < p^j$, so dass $\frac{m}{n} = b + c\frac{p^l}{1-p^j}$. Letzteres muss nicht notwendig bewiesen werden.

2. Zeige: $\zeta_{p-1} \in \mathbb{Z}_p$.

3. Sei $\mathbb{Q}_p^c$ der algebraische Abschluss von $\mathbb{Q}_p$. Zeige:

   (a) Der Betrag $|\ |_p$ auf $\mathbb{Q}_p$ setzt sich eindeutig auf $\mathbb{Q}_p^c$ fort.

   (b) $\mathbb{Q}_p^c$ ist nicht komplett.
   Hinweis: Man betrachte das Element $\alpha = \sum_{n=1}^{\infty} \zeta_{n'} p^n$, wobei $n' = n$ für $p \nmid n$ und $n' = 1$ für $p \mid n$. Wäre nun $\mathbb{Q}_p^c$ komplett, so wäre $\alpha \in K$ für ein K von endlichem Grad über $\mathbb{Q}_p$. Zeige nun mittels Induktion, dass $\zeta_m \in K$ für alle $p \nmid m$. Beachte dabei, dass zwei verschiedene m-te Einheitswurzeln niemals kongruent sind $\bmod p$ wegen $\prod_{\zeta^m=1, \zeta \neq 1}(1 - \zeta) = m$.

   (c) Sei $\mathbb{C}_p$ die Komplettierung von $\mathbb{Q}_p^c$ bezüglich $|\ |_p$. Dann ist $\mathbb{C}_p$ algebraisch abgeschlossen.

Blatt 7

1. Sei $K/\mathbb{Q}_p$ endlich, $\mathfrak{p} = (\pi)$ das maximale Ideal in $\mathfrak{o}_K$ und $q = |\mathfrak{o}/\mathfrak{p}| = |\overline{K}|$. Dann gilt:

$$K^\times \simeq \pi^{\mathbb{Z}} \times \mu_{q-1} \times U^{(1)},$$

   wobei μ_{q-1} die Gruppe der $(q-1)$-ten Einheitswurzeln bezeichne.

2. Sei $K/\mathbb{Q}_p$ endlich. Dann gibt es einen eindeutig bestimmten Homomorphismus $\log : K^\times \to K$ mit $\log p = 0$ und

$$\log(1 + x) = \sum_{\nu=1}^{\infty} (-1)^{\nu+1} \frac{x^\nu}{\nu}$$

   für $1 + x \in U^{(1)}$.

3. Sei $K/\mathbb{Q}_p$ endlich, $\mathfrak{p}$ das maximale Ideal in $\mathfrak{o}_K$ und $q = |\mathfrak{o}/\mathfrak{p}| = |\overline{K}|$. Sei außerdem $n \in \mathbb{N}$ teilerfremd zu p und $L = K(\zeta_n)$. Zeige:

   (a) L/K ist eine unverzweigte Erweiterung vom Grade f, wobei $f = \operatorname{ord}(q \bmod n)$.

   (b) L/K ist galoissch zyklisch mit Gruppe $G(L/K) \simeq G(\overline{L}/\overline{K})$, erzeugt von $\phi : \zeta_n \mapsto \zeta_n^q$.

   (c) $\mathfrak{o}_L = \mathfrak{o}_K[\zeta_n]$.

Blatt 8

1. Sei K endlich über $\mathbb{Q}$ und L/K eine galoissche Erweiterung mit Gruppe G. Bezeichne weiter $\mathfrak{D} = \mathfrak{D}_{L/K}$ bzw. $D = D_{L/K}$ die Differente bzw. die Diskriminante von L/K. Ein Primideal $\mathfrak{p} \lhd \mathfrak{o}_K$ heißt unverzweigt in L/K, wenn $e = 1$ in der Primidealzerlegung $\mathfrak{p}\mathfrak{o}_L = \prod_{i=1}^{r} \mathfrak{P}_i^e$, sonst verzweigt. Zeige:

   (a) $\mathfrak{p}$ ist genau dann in L/K verzweigt, wenn $\mathfrak{P}_i \mid \mathfrak{D}$ für ein (und damit für alle) i. Insbesondere gibt es nur endlich viele in L/K verzweigte Primideale.

   (b) $\mathfrak{p}$ ist genau dann in L/K verzweigt, wenn $\mathfrak{p} \mid D$.

   (c) Sei G nicht zyklisch. Dann gibt es nur endlich viele unzerlegte Primideale $\mathfrak{P}$ in L, i.e. Primideale mit $G_{\mathfrak{P}} = G$.

2. Sei $K_n = \mathbb{Q}_p(\zeta_{p^n})$. Bestimme die i-ten Verzweigungsgruppen der Erweiterung $K_n/\mathbb{Q}_p$ für alle $i \geq 0$.

3. Für welche Primzahlen p und welche $n \in \mathbb{N}$ ist die A_n als Galoisgruppe über $\mathbb{Q}_p$ realisierbar?

Blatt 9

1. Zeige, dass für einen globalen Zahlkörper K gilt: $\mathrm{cl}_K \simeq \mathcal{J}_K/\mathcal{J}_\infty K^\times$.

2. Sei $d \in \mathbb{Z}$ quadratfrei, $d \neq 0, 1$ und $K = \mathbb{Q}(\sqrt{d})$. Dann ist $K/\mathbb{Q}$ galoissch mit Gruppe $< \sigma >$ mit $\sigma : \sqrt{d} \mapsto -\sqrt{d}$.

   (a) Zeige, dass es für eine Primzahl $p \in \mathbb{Z}$ genau die folgenden Möglichkeiten von Primidealzerlegungen in $\mathfrak{o}_K$ gibt:

      i. $p\mathfrak{o}_K = \mathfrak{p}$ ist prim (p heißt *träge*)

      ii. $p\mathfrak{o}_K = \mathfrak{p}^2$ mit $\mathfrak{p}$ prim (p heißt *verzweigt*)

      iii. $p\mathfrak{o}_K = \mathfrak{p} \cdot \mathfrak{p}^\sigma$ mit $\mathfrak{p} \neq \mathfrak{p}^\sigma$ prim (p heißt *zerlegt*)

   (b) Bezeichne d_K die Diskriminante von K. Stelle einen Zusammenhang zwischen obigen Zerlegungen und der Zahl $(\frac{d_K}{p})$ her.

   (c) Wann besitzt $K \otimes_{\mathbb{Q}} \mathbb{Q}_p$ Nullteiler?

(d) Für $p|d$ bestimme die i-ten Verzweigungsgruppen der Erweiterung $K_\mathfrak{p}/\mathbb{Q}_p$ für $i \geq -1$, wobei $\mathfrak{p}$ das Primideal über p bezeichne.

Blatt 10

1. Sei L/K eine globale Erweiterung von Zahlkörpern und $\mathfrak{p}$ eine Primstelle von K. Setze $L_\mathfrak{p} = L \otimes_K K_\mathfrak{p}$ und betrachte für $\alpha_\mathfrak{p} \in L_\mathfrak{p}^\times$ den $K_\mathfrak{p}$-Vektorraumhomomorphismus

$$f_{\alpha_\mathfrak{p}} : L_\mathfrak{p} \to L_\mathfrak{p},\ x \mapsto \alpha_\mathfrak{p} \cdot x.$$

Definiere $N_{L_\mathfrak{p}/K_\mathfrak{p}}(\alpha_\mathfrak{p}) = \det(f_{\alpha_\mathfrak{p}})$. Zeige:

(a) Die Homomorphismen $N_{L_\mathfrak{p}/K_\mathfrak{p}} : L_\mathfrak{p}^\times \to K_\mathfrak{p}^\times$ setzen sich zu einer Normabbildung

$$N_{L/K} : \mathcal{J}_L \to \mathcal{J}_K,\ (\ldots, \alpha_\mathfrak{P}, \ldots) \mapsto (\ldots, \prod_{\mathfrak{P}|\mathfrak{p}} N_{L_\mathfrak{P}/K_\mathfrak{p}}(\alpha_\mathfrak{P}), \ldots)$$

zusammen.

(b) $N_{L/K}$ induziert einen wohldefinierten Homomorphismus $N_{L/K} : C_L \to C_K$.

(c) Für ein Idèl $x \in \mathcal{J}_L$ schreibe (x) für das Bild unter der kanonischen Abbildung $\mathcal{J}_L \to I_L$, entsprechend für Idèle in K. Dann gilt: $N_{L/K}((x)) = (N_{L/K}(x))$.

(d) Sei nun $x \in \mathcal{J}_K$ und bezeichne $i_{L/K}$ die Inklusion $\mathcal{J}_K \rightarrowtail \mathcal{J}_L$. Dann gilt: $N_{L/K}(i_{L/K}(x)) = x^{[L:K]}$.

(e) Betrachte außerdem die kanonischen Abbildungen $\mathcal{N}_F : \mathcal{J}_F \to \mathbb{R}_{>0}$ für $F = L$ und $F = K$. Dann gilt für $x \in \mathcal{J}_L$: $\mathcal{N}_K N_{L/K}(x) = \mathcal{N}_L(x)$.

(f) Für $x \in \mathcal{J}_K$ gilt: $\mathcal{N}_L i_{L/K}(x) = \mathcal{N}_K(x)^{[L:K]}$.

2. Sei K ein globaler Zahlkörper und $\mathfrak{p}$ eine Primstelle von K. Für $\mathfrak{p}$ reell setze $U_\mathfrak{p}^{(0)} = \mathbb{R}_{>0}$ und für $\mathfrak{p}$ komplex $U_\mathfrak{p}^{(0)} = \mathbb{C}^\times$. Für ein ganzes Ideal $\mathfrak{m} = \prod_{\mathfrak{p} \subset K} \mathfrak{p}^{n_\mathfrak{p}} \subset K$ definiere

$$\mathcal{J}_K^\mathfrak{m} = \prod_\mathfrak{p} U_\mathfrak{p}^{(n_\mathfrak{p})} \leq \mathcal{J}_K$$

und

$$C_K^\mathfrak{m} = \mathcal{J}_K^\mathfrak{m} K^\times / K^\times \leq C_K,$$

wobei wir $n_\mathfrak{p} = 0$ setzen für alle unendlichen Primstellen $\mathfrak{p}$. $C_K^\mathfrak{m}$ heißt die Kongruenzuntergruppe $\mod \mathfrak{m}$. Zeige:
Die abgeschlossenen Untergruppen von endlichem Index in C_K sind genau diejenigen Untergruppen, die eine Kongruenzuntergruppe $C_K^\mathfrak{m}$ enthalten.

Blatt 11

1. Sei K/k eine galoissche Erweiterung lokaler Körper mit Gruppe G. Zeige: K/k ist genau dann unverzweigt, wenn $H^1(G, U_K) = 1$.

2. Sei M ein $\mathbb{Z}G$-Modul. Dann existiert für jede ganze Zahl $m \geq 0$ ein $\mathbb{Z}G$-Modul M_m mit:

$$H^n(G, M_m) \simeq H^{n+m}(G, M) \ \forall n > 0$$

$$\text{und } H^0(G, M_m) \twoheadrightarrow H^m(G, M).$$

3. Sei M ein $\mathbb{Z}G$-Modul und

$$0 \to M \to Y_0 \to Y_1 \to Y_2 \to \dots$$

eine azyklische Auflösung von M, d.h. die Sequenz ist exakt und $H^n(G, Y_i) = 0$ für alle $n > 0$, $i \geq 0$. Betrachte den Komplex

$$0 \xrightarrow{\partial_{-1}} Y_0^G \xrightarrow{\partial_0} Y_1^G \xrightarrow{\partial_1} Y_2^G \xrightarrow{\partial_2} \dots$$

Dann gilt: $H^n(G, M) \simeq \ker(\partial_n)/\mathrm{im}\,(\partial_{n-1})$.

Lösungsvorschläge

Blatt 1

1. Sei $\alpha = \frac{1+2\sqrt{6}}{1-\sqrt{6}}$. Dann ist $N_{\mathbb{Q}(\sqrt{6})/\mathbb{Q}}(\alpha) \notin \mathbb{Z}$, also α nicht ganz. Das Minimalpolynom von $\beta = \frac{3+2\sqrt{6}}{1-\sqrt{6}}$ ist $x^2 + 7x + 5 \in \mathbb{Z}[x]$, also β ganz.
2. Siehe [Eis], p. 125
3. Siehe [Eis], p. 729, Ex. 4.17 und Ex. 4.18

Blatt 2

1. (a) Man wähle f als den größten gemeinsamen Teiler aller $y \in \mathbb{Z}$ mit $y\omega \in S$. Dann folgt leicht, dass $S = R_f$.
   (b) Der Quotientenkörper aller R_f mit $f \neq 0$ ist K. Wegen $R_f \neq \mathfrak{o}_K$ ist R_f nicht ganz abgeschlossen in K, also kein Dedekindring.
2. (a) Man überprüfe die Eigenschaften eines Ideals. Wesentlich geht dabei ein, dass $\omega^2 = d \in \mathfrak{a}_b$.
   (b) Angenommen $\mathfrak{a}_b = (\gamma)$ mit einem $\gamma = x + y\omega \in \mathfrak{o}_K$. Wegen $b, \omega \in \mathfrak{a}_b$ ist dann $N(\gamma) = x^2 - dy^2$ ein Teiler von $N(b) = b^2$ und von $N(\omega) = -d$, also von b. Das führt zu nicht lösbaren Gleichungen.
   (c) Wegen $(b_1, b_2) = 1$ existieren ganze Zahlen s und t mit $sb_1 + tb_2 = 1$. Damit:
   $$\mathfrak{a}_{b_1}\mathfrak{a}_{b_2} = (b_1, \omega)(b_2, \omega) = (b_1b_2, b_1\omega, b_2\omega, \omega^2) = (b_1b_2, \omega) = \mathfrak{a}_{b_1b_2}$$
   (d) Für eine Primzahl $p|d$ berechnet man wie oben, dass $\mathfrak{a}_p^2 = (p)$. Somit erzeugen die Idealklassen von $\mathfrak{a}_{p_i}$, $i = 1 \ldots t-1$ eine Untergruppe von cl_K mit der gewünschten Eigenschaft.
3. Für (b) und (d) siehe [Eis], p. 14. Zu (a): Ist π prim und $\pi = ab$, also insbesondere $\pi|ab$, so teilt π auch (etwa) a, also $a = \pi x$ für ein $x \in R$. Wegen der Nullteilerfreiheit von R und $\pi = \pi xb$ folgt $xb = 1$, also $b \in R^\times$.
   Zu (c): In $R = \mathbb{Z}[\sqrt{-5}]$ lässt sich 6 zerlegen in $2 \cdot 3$ und $(1+\sqrt{-5})(1-\sqrt{-5})$. Mit Hilfe der Norm zeigt man, dass 2 in R irreduzibel ist, aber kein Teiler von $1 \pm \sqrt{-5}$.

Blatt 3

1. (a) Ist die Klassenzahl $h_K = 1$, so ist $\mathfrak{o}$ ein Hauptidealring, also faktoriell. Ist umgekehrt $\mathfrak{o}$ faktoriell, wähle für jedes Primideal $\mathfrak{p} \neq (0)$ ein $0 \neq a \in \mathfrak{p}$ und schreibe $a = \prod_i \pi_i$ mit Primelementen π_i. Da $\mathfrak{p}$ ein Primideal ist, liegt eines dieser π_i in $\mathfrak{p}$, also sogar $\mathfrak{p} = (\pi_i)$. Dass auch jedes beliebige Ideal ein Hauptideal ist, folgt nun aus der eindeutigen Primidealzerlegung in $\mathfrak{o}$.

(b) Sei $[\mathfrak{a}] \in \mathrm{cl}_K$. Ohne Einschränkung können wir $\mathfrak{a}$ als ganz annehmen. Schreibe $\mathfrak{m} = \prod_{i=1}^m \mathfrak{p}_i^{e_i}$ und $\mathfrak{a} = \prod_{i=1}^m \mathfrak{p}_i^{n_i}\mathfrak{b}$ mit $(\mathfrak{b}, \mathfrak{m}) = 1$. Der Chinesische Restsatz liefert nun ein Element $x \in \mathfrak{o}_K$, so dass $x^{-1}\mathfrak{a}$ teilerfremd zu $\mathfrak{p}_1$ ist. Nochmals mit dem Chin. Restsatz erhalten wir ein Element $g \in \mathfrak{o}_K$, so dass $gx^{-1}\mathfrak{a}$ ganz und immer noch teilerfremd zu $\mathfrak{p}_1$ ist. Die Behauptung folgt nun mit Induktion nach m.

2. (a) Seien $\alpha = \omega_1, \ldots, \omega_n$ die Konjugierten von α. Dann ist nach der Vandermondeschen Determinante $d(M) = \det(\omega_j^i)^2 = \prod_{i<j}(\omega_i - \omega_j)^2 = d_f$.
Mit $f'(\alpha) = \prod_{i=2}^n(\omega_1 - \omega_i)$ lässt sich $N_{K/\mathbb{Q}}(f'(\alpha))$ direkt ausrechnen.

(b) Die Behauptung folgt aus dem Hinweis, wenn wir zeigen, dass $P + N$ und PN in $\mathbb{Z}$ liegen. Nach Definition der Diskriminante sind sie zumindest ganz.
Ein $\sigma \in I(K/\mathbb{Q})$ bewirkt auf $P + N$ nur eine Permutation der Summanden, so dass $\sigma(P + N) = P + N$, also $P + N \in \mathbb{Q}$ und damit $P + N \in \mathbb{Z}$. Wegen $PN = \frac{-d_k - (P+N)^2}{4} \in \mathbb{Q}$ liegt auch PN in $\mathbb{Z}$.

(c) Im ersten Fall ist $d_f = -9463$ prim, im zweiten ist $d_f = -4 \cdot 5 \cdot 461$. Da sich d_f von d_K um ein Quadrat unterscheidet, kommt für d_K nur d_f oder $d_f/4$ in Frage. Letzteres ist aber kongruent $-1 \bmod 4$ im Widerspruch zu (b). Es gilt also in beiden Fällen $d_f = d_K$ und somit $\mathfrak{o}_K = \mathbb{Z} \oplus \alpha\mathbb{Z} \oplus \alpha^2\mathbb{Z}$.

3. (a) Klar, da $G(L/\mathbb{Q}) \simeq C_2 \times C_2$.

(b) Folgt aus dem Dirichletschen Einheitensatz, da L total reell ist.

(c) Man rechnet nach, dass $R_L(\epsilon_1, \epsilon_2, \epsilon_3) = 4R_{K_1}R_{K_2}R_{K_3} \neq 0$, wobei die K_i die drei reell quadratischen Teilkörper von L seien.

(d) Sei $\epsilon \in E$. Es genügt $\epsilon^2 \in E_0$ zu zeigen. Wähle dazu n minimal mit $\epsilon^n \in E_0$ und schreibe $\epsilon^n = \epsilon_1^{a_1}\epsilon_2^{a_2}\epsilon_3^{a_3}$. Indem man nun von dieser Gleichung alle Normen N_{L/K_i} betrachtet, folgert man $n|2$.

(e) Die reell quadratischen Zwischenkörper mit den zugehörigen Grundeinheiten sind $K_1 = \mathbb{Q}(\sqrt{2})$ mit $\epsilon_1 = 1 + \sqrt{2}$, $K_2 = \mathbb{Q}(\sqrt{3})$ mit $\epsilon_2 = 2 + \sqrt{3}$ und $K_3 = \mathbb{Q}(\sqrt{6})$ mit $\epsilon_3 = 5 + 2\sqrt{6}$. Aber $\epsilon = \sqrt{2} + \sqrt{3} \in E \setminus E_0$.

Blatt 4

1. (a) Betrachte das Diagramm

$$\begin{array}{rcc} K^\times & \stackrel{\Phi}{\to} & \mathbb{R}^r \times \mathbb{C}^s \\ |N_{K/\mathbb{Q}}| \downarrow & & N \downarrow \\ \mathbb{R} & = & \mathbb{R} \end{array}$$

Für $a \in K^\times$ schreibe $\Phi(a) = (x_1, \ldots, x_{r+s})$. Dann folgt mit dem Hinweis:

$$|N_{K/\mathbb{Q}}(a)| = N(\Phi(a)) \leq (\frac{1}{n}\sum_{i=1}^r |x_i| + 2\sum_{j=1}^s |x_{r+j}|)^n \leq MN(\mathfrak{a})$$

genau dann, wenn $\sum_{i=1}^r |x_i| + 2\sum_{j=1}^s |x_{r+j}| \leq n\sqrt[n]{MN(\mathfrak{a})} =: t$. Da $\Phi(\mathfrak{a})$ ein volles $\mathbb{Z}$-Gitter in $\mathbb{R}^r \times \mathbb{C}^s$ ist, folgt die Behauptung aus dem Satz von Minkowski.

(b) Der Beweis geht analog zu dem in [Neu], Theorem (6.3), p. 38 f.

2. Die Minkowski-Schranke berechnet sich hier zu $M = 2,46\ldots < 3$. Die Idealklassengruppe ist demnach von Primidealen $\mathfrak{p}$ mit $N(\mathfrak{p}) \leq 2$ erzeugt. Dabei kommen nur Primideale über 2 infrage. Ein solches ist $\mathfrak{p} = 2\mathbb{Z} + \frac{1+\sqrt{-15}}{2}\mathbb{Z}$ und das einzig mögliche weitere deshalb $\mathfrak{p}^\sigma$. Wegen $\mathfrak{p}+\mathfrak{p}^\sigma = \mathfrak{o}_K$ ist tatsächlich $\mathfrak{p} \neq \mathfrak{p}^\sigma$. Man zeigt, dass $\mathfrak{p}$ kein Hauptideal ist, aber $\mathfrak{p}^2$ schon. Mit $(2) = \mathfrak{p}\mathfrak{p}^\sigma$ erzeugen also $\mathfrak{p}$ und $\mathfrak{p}^\sigma$ die gleiche Idealklasse und wir erhalten $h_K = 2$.

3. Siehe [Lo], p. 125

Blatt 5

1. Nach Aufgabe 2 von Blatt 3 ist die Diskriminante d_K ein Teiler von d_f, wobei $K = \mathbb{Q}(\alpha)$ und α eine beliebige Nullstelle von f ist. Zeige also $d_K \neq \pm 1$. Aus Aufgabe 1(a) von Blatt 4 für $\mathfrak{a} = \mathfrak{o}_K$ ergibt sich die Abschätzung $\sqrt{|d_K|} \geq \frac{n^n}{n!}(\frac{\pi}{4})^{n/2}$ Die rechte Seite ist minimal bei $n = 2$ und damit immer noch größer 1.

2. Für (a) und (b) siehe [Neu], Kapitel I Lemma (10.1), p. 62. Für (c) siehe ebenfalls [Neu], Satz (10.2), p.63.
(d) folgt aus (b) mit $N_{K/\mathbb{Q}}(\mathfrak{D}_{K/\mathbb{Q}}) = (d_K)$. Zu (e): $\mathfrak{o}_K = \mathbb{Z}[\zeta] = \mathfrak{o}_{K^+}[\zeta] = \mathfrak{o}_{K^+} \oplus \mathfrak{o}_{K^+} \cdot \zeta$. Man bestimmt nun die Dualbasis von $1, \zeta$ gemäß Skript, p. 12/3 und erhält $\mathfrak{D}_{K/K^+} = (\lambda)$. Aus $\mathfrak{D}_{K/\mathbb{Q}} = \mathfrak{D}_{K/K^+}\mathfrak{D}_{K^+/\mathbb{Q}}$ erhält man $\mathfrak{D}_{K^+/\mathbb{Q}} = \mathfrak{P}_+^{\frac{s-1}{2}}$ mit $\mathfrak{P}_+ = (\lambda) \cap K^+$.

Blatt 6

1. Wir können o.E. annehmen, dass $k = 0$. Wird die Folge der a_ν periodisch, so kann man a schreiben als

$$a = \sum_{\nu=0}^{l-1} a_\nu p^\nu + p^l \sum_{\nu=0}^{j-1} a_\nu p^\nu \cdot \sum_{i=0}^{\infty} p^{ij} = b + c\frac{p^l}{1-p^j} \in \mathbb{Q}.$$

Hierbei ist l hinreichend groß, j die Periodenlänge und $b, c \in \mathbb{Z}$.
Sei nun umgekehrt $a = \sum_\nu a_\nu p^\nu \in \mathbb{Q}$. Dann ist $-a = \sum_\nu (p - a_\nu - 1)p^\nu + 1$, so dass a genau dann periodisch wird, wenn $-a$ periodisch wird. Wir können also $a < 0$ annehmen. Schreibe $a = \frac{m}{n}$ mit $p \nmid n$ (wegen k=0). Dann existiert ein $j \in \mathbb{N}$ mit $p^j \equiv 1 \bmod n$ und wir können den Bruch erweitern zu $\frac{m}{n} = \frac{m'}{1-p^j}$ mit $m' > 0$. Wähle $l > 0$ so groß, dass $m' < p^l$ und $0 \leq b < p^l$, so dass $m' - b(1-p^j) \equiv 0 \bmod p^l$. Dann kann man a schreiben wie oben und die gleiche Rechnung rückwärts lesen.

2. Das Polynom $x^{p-1} - 1$ zerfällt über $\mathbb{F}_p[x]$ und damit nach Hensels Lemma auch über $\mathbb{Z}_p[x]$.

3. Siehe [Wa], Proposition 5.1 und 5.2, p. 48.

Blatt 7

1. Siehe [Neu], Kapitel II, Satz (5.3), p.142.

2. Siehe [Neu], Kapitel II, Satz (5.4), p. 142.

3. Siehe [Neu], Kapitel II, Satz (7.12), p. 166.

Blatt 8

1. (a) Die Differente verträgt sich mit Lokalisiereung und dort kennen wir das Resultat (Skript p. 20).
   (b) Folgt aus $N_{L/K}(\mathfrak{D}_{L/K}) = D_{L/K}$.
   (c) Ist $G_{\mathfrak{P}}$ nicht zyklisch, hat die Surjektion $G_{\mathfrak{P}} \twoheadrightarrow G(\overline{L}/\overline{K})$ einen nichttrivialen Kern. Damit sind alle solchen Primideale verzweigt.

2. $K_n/\mathbb{Q}_p$ ist rein verzweigt vom Grad $(p-1)p^{n-1}$ und $\mathfrak{o}_{K_n} = \mathbb{Z}_p[\zeta_{p^n}]$ mit maximalem Ideal $\mathfrak{p}_n = (1-\zeta_{p^n})$. Die Galoisgruppe $G = G(K_n/\mathbb{Q}_p)$ ist isomorph zu $(\mathbb{Z}/p^n\mathbb{Z})^\times$ und ein $\sigma_l \in G$ wirkt auf ζ_{p^n} als $\sigma_l(\zeta_{p^n}) = \zeta_{p^n}^l$. Es ist also $\sigma_l \in G_i$ genau dann, wenn $w(\zeta_{p^n}^l - \zeta_{p^n}) = w(1-\zeta_{p^n}^{l-1}) \geq i+1$. Dieser Wert hängt nur von der p-Potenz in $l-1$ ab, und wir erhalten:
$$\sigma_l \in G_i \iff p^{w_p(l-1)} \geq i+1$$
Andererseits ist genau dann $\sigma_l \in G(K_n/K_j)$, wenn $p^j \mid l-1$. Es folgt: $G_{-1} = G_0 = G$, $G_1 = \ldots = G_{p-1} = G(K_n/K_1)$, $G_p = \ldots = G_{p^2-1} = G(K_n/K_2)$ usw. bis schließlich $G_i = 1$ für $i \geq p^{n-1}$.

3. Für $n = 1, 2, 3$ ist die A_n zyklisch und es existiert z.B. die unverzweigte Erweiterung von Grad n über $\mathbb{Q}_p$. Für $n > 4$ ist die A_n einfach und damit nicht auflösbar. Im Lokalen existieren aber nur auflösbare Galoisgruppen. Bleibt der Fall $n = 4$:
Angenommen es gibt eine Erweiterung $K/\mathbb{Q}_p$ mit Gruppe A_4, so ist diese verzweigt, da die A_4 nicht zyklisch ist. Die Verzweigungsgruppe G_0 ist also ungleich 1 und ein Normalteiler der A_4, also entweder die A_4 selbst oder die Kleinsche Vierergruppe $V_4 \simeq C_2 \times C_2$. G_1 ist eine p-Gruppe und normal in der A_4. Wäre $G_1 = 1$, dann könnten wir G_0 in $U^{(0)}/U^{(1)} \simeq (\overline{K})^\times$ einbetten. Dann ist G_0 aber zyklisch, Widerspruch. Es muss also $G_1 = V_4$ und damit $p = 2$ sein. Da alle G_i normal in der A_4 sind, muss es ein $i_0 \geq 1$ geben mit $G_{i_0} = V_4$ und $G_{i_0+1} = 1$. Dann lässt sich aber die V_4 einbetten in $U^{(i_0)}/U^{(i_0+1)} \simeq \overline{K}$. Damit folgt $2 \mid f = [\overline{K} : \mathbb{F}_2]$, also $8 \mid f \cdot |G_0| = [K : \mathbb{Q}_p] = 12$, Widerspruch.

Blatt 9

1. Aus dem Diagramm
$$\begin{array}{ccccc} E_\infty & \rightarrowtail & K^\times & \twoheadrightarrow & P_K \\ \downarrow & & \downarrow & & \downarrow \\ \mathcal{J}_\infty & \rightarrowtail & \mathcal{J}_K & \twoheadrightarrow & I_K \\ \downarrow & & \downarrow & & \downarrow \\ \mathcal{J}_\infty/E_\infty & \rightarrowtail & C_K & \twoheadrightarrow & \mathrm{cl}_K \end{array}$$
folgt $\mathrm{cl}_K \simeq C_K/(\mathcal{J}_\infty/E_\infty) = \mathcal{J}_K/K^\times\mathcal{J}_\infty$.

2. (a) Folgt aus der Formel $2 = [K : \mathbb{Q}] = \sum_i e_i f_i$.
   (b) Wir wissen schon, dass p genau dann verzweigt ist, wenn $p \mid d_K$, also genau dann, wenn $(\frac{d_K}{p}) = 0$. Sei nun p unverzweigt. p ist zerlegt $\iff G_{\mathfrak{p}} = 1 \iff K_{\mathfrak{p}} = \mathbb{Q}_p \iff \sqrt{d} \in \mathbb{Q}_p \iff x^2 - d$ zerfällt über $\mathbb{Q}_p[x]$. Für $p \neq 2$ ist das nach Hensels Lemma genau dann der Fall, wenn $x^2 - d$ über $\mathbb{F}_p[x]$ zerfällt, also wenn $(\frac{d_K}{p}) = 1$. Der Fall $p = 2$ kann nur für $d \equiv 1 \bmod 4$ auftreten. In diesem Fall ist immer $(\frac{d_K}{2}) = 1$ und $(2, \frac{1+\sqrt{d}}{2})$ ist ein Primideal in $\mathfrak{o}_K$ von Grad 1, also 2 zerlegt.

(c) Wegen $K \otimes_{\mathbb{Q}} \mathbb{Q}_p = \mathbb{Q}_p[x]/x^2 - d$ treten genau dann Nullteiler auf, wenn $x^2 - d$ reduzibel ist, also wenn $(\frac{d_K}{p}) = 1$.

(d) Für $p \mid d$ ist p verzweigt, also $K_\mathfrak{p}/\mathbb{Q}_p$ eine Erweiterung von Grad 2 mit Gruppe G. Es folgt $G_{-1} = G_0 = G$. G_1 ist die p-Sylowgruppe von G_0, also $G_1 = 1$ für $p \neq 2$ (und damit auch alle $G_i = 1$ für $i > 1$) und $G_1 = G$ für $p = 2$. Sei also nun $p = 2$. Da wir die (globale) Diskriminante kennen, können wir die lokale Differente berechnen: $\mathfrak{D}_{K_\mathfrak{p}/\mathbb{Q}_2} = \mathfrak{p}^3$. Aus der Gleichung $3 = \sum_{i \geq 0}(|G_i| - 1)$ schließen wir $G_2 = G$ und $G_i = 1$ für $i \geq 3$.

Blatt 10

1. (a), (b) und (d) finden sich bei [Neu] Kapitel VI § 2, p. 387ff. (c) und (e) lassen sich direkt nachrechnen, wobei man etwa bei (e) benutzt, dass $||N_{L_\mathfrak{P}/K_\mathfrak{p}}(\alpha_\mathfrak{P})||_\mathfrak{p} = ||\alpha_\mathfrak{P}||_\mathfrak{P}$ für $\alpha_\mathfrak{P} \in L_\mathfrak{P}$. (f) ist eine Folgerung aus (d) und (e).

2. Siehe [Neu], Kapitel VI, Satz (1.8), p. 380.

Blatt 11

1. Wendet man den Funktor $(\_)^G$ auf die exakte Sequenz $U_K \rightarrowtail K^\times \overset{v_K}{\twoheadrightarrow} \mathbb{Z}$ an, erhält man wegen $H^1(G, K^\times) = 0$ eine exakte Sequenz

$$U_k \rightarrowtail k^\times \xrightarrow{v_K} \mathbb{Z} \twoheadrightarrow H^1(G, U_K).$$

   Das Bild von v_K in $\mathbb{Z}$ wird erzeugt von $v_K(\pi) = e$, wobei π ein Primelement in k ist und e der Verzweigungsindex. $H^1(G, U_K)$ verschwindet also genau dann, wenn $e = 1$.

2. Siehe [NSW], Ch. I Proposition (1.3.8), p. 32

3. Siehe [NSW], Ch. I Proposition (1.3.9), p. 33

Literatur

[Eis] Eisenbud, D.: *Commutative Algebra with a view toward Algebraic Geometry* , Springer (1995)

[Neu] Neukirch, J.: *Algebraische Zahlentheorie*, Springer (1992)

[NSW] Neukirch, J., Schmidt, A., Wingberg, K.: *Cohomology of number fields*, Springer (2000)

[Lo] Long, R.: *Algebraic Number Theory*, Dekker (1977)

[Wa] Washington, L. C.: *Introduction to Cyclotomic Fields*, Springer (1982)