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

Protokoll zur Vorlesung Zahlentheorie 2 · Wintersemester 2007/08

1. Kohomologische Nachträge

1. *Das Cupprodukt*

Wir betrachten zwei G-Moduln M_1 und M_2 und die durch $(m_1, m_2) \mapsto m_1 \otimes m_2$ definierte Abbildung $M_1^G \otimes_{\mathbb{Z}} M_2^G \to (M_1 \otimes_{\mathbb{Z}} M_2)^G$ (die G-Wirkung ist, wie immer, diagonal). Für $(m_1, m_2) \in N_G(M_1) \times N_G(M_2)$ folgt $m_1 \otimes m_2 \in N_G(M_1 \otimes M_2)$. Dies wiederum induziert die Cupproduktabbildung

$$H^0(G, M_1) \times H^0(G, M_2) \xrightarrow{\cup} H^0(G, M_1 \otimes M_2)$$

Ohne Beweis geben wollen wir den folgenden Satz an (vgl. etwa Neukirchs Buch *Klassenkörpertheorie*).

Satz. *Sei G eine endliche Gruppe. Dann gibt es genau ein System von Abbildungen*

$$H^p(G, M_1) \times H^q(G, M_2) \xrightarrow{\cup} H^{p+q}(G, M_1 \otimes M_2)$$

für alle $p, q \in \mathbb{Z}$ und alle G-Moduln M_1, M_2 mit

(a) Für $p = q = 0$ ist $\cup$ die oben definierte Cupproduktabbildung.

(b) Sind $M_1' \rightarrowtail M_1 \twoheadrightarrow M_1''$ und $M_1' \otimes M_2 \rightarrowtail M_1 \otimes M_2 \twoheadrightarrow M_1'' \otimes M_2$ exakt, dann kommutiert

$$\begin{array}{ccc} H^p(G, M_1'') \times H^q(G, M_2) & \xrightarrow{\cup} & H^{p+q}(G, M_1'' \otimes M_2) \\ d \times 1 \downarrow & & d \downarrow \\ H^{p+1}(G, M_1') \times H^q(G, M_2) & \xrightarrow{\cup} & H^{p+1+q}(G, M_1' \otimes M_2) \end{array}$$

wobei d stets den jeweiligen Verbindungshomomorphismus bezeichnet.

(c) Sind $M_2' \rightarrowtail M_2 \twoheadrightarrow M_2''$ und $M_1 \otimes M_2' \rightarrowtail M_1 \otimes M_2 \twoheadrightarrow M_1 \otimes M_2''$ exakt, dann kommutiert

$$\begin{array}{ccc} H^p(G, M_1) \times H^q(G, M_2'') & \xrightarrow{\cup} & H^{p+q}(G, M_1 \otimes M_2'') \\ 1 \times d \downarrow & & (-1)^p d \downarrow \\ H^p(G, M_1) \times H^{q+1}(G, M_2') & \xrightarrow{\cup} & H^{p+q+1}(G, M_1 \otimes M_2') \end{array}$$

Eigenschaften:

$\cup$ ist assoziativ für $M_1 \otimes M_2 \otimes M_3$.

$\cup$ ist antikommutativ: $f \cup g = (-1)^{pq} g \cup f$ (und $M_1 \otimes M_2 = M_2 \otimes M_1$).

Sind $f : M_1 \to N_1$ und $g : M_2 \to N_2$ Abbildungen von G-Moduln, so gilt: $(f \otimes g)(a \cup b) = f(a) \cup g(b)$.

$res(a \cup b) = res(a) \cup res(b)$

$cor(a \cup res(b)) = (cor(a)) \cup b$

Beispiel und Erinnerung: Sei $G = \langle g \rangle$ zyklisch. Dann ist $\Delta G = \mathbb{Z}G(g-1)$ und wir haben 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 die exakte Sequenz $\mathbb{Z} \overset{\hat{G}}{\rightarrowtail} \mathbb{Z}G \overset{g-1}{\to} \mathbb{Z}G \twoheadrightarrow \mathbb{Z}$ und damit $H^q(G,M) = H^{q+2}(G,M)$ für alle $q \in \mathbb{Z}$. Es gilt nun: Ist $H^2(G,\mathbb{Z}) \simeq \mathbb{Z}/n$ erzeugt von a, so induziert $- \cup a$ einen Isomorphismus $H^q(G,M) \simeq H^{q+2}(G,M)$.

2. *Der Herbrandquotient*

Definition. *Für einen endlich erzeugten G-Modul M setze $h_q(M) := |H^q(G,M)|$. $h(M) := h_0(M)/h_1(M)$ heißt der Herbrandquotient von M.*

Lemma. *Sei G zyklisch. Dann gilt:*

(a) $h(M) = h(M')h(M'')$, falls $M' \rightarrowtail M \twoheadrightarrow M''$ exakt ist.

(b) M endlich $\implies h(M) = 1$

3. *Kohomologische Trivialität*

Definition. *Ein G-Modul M heißt kohomologisch trivial (c.t.), falls $H^q(U,M) = 0$ für alle $q \in \mathbb{Z}$ und alle Untergruppen U von G gilt.*

Als Beispiel kennen wir bereits die (ko-)induzierten Moduln. Wir wollen nun einige Kriterien für kohomologische Trivialität herleiten. Die wichtigste Beobachtung dabei beschreibt folgender

Satz. *Sei G eine endliche p-Gruppe und M ein G-Modul mit $pM = 0$. Falls $H_1(G,M) = 0$, so ist M frei über $\mathbb{F}_pG$.*

Wir skizzieren den Beweis für endlich erzeugtes M. Da M_G von p annulliert wird, ist M_G ein $\mathbb{F}_p$-Vektorraum. Wir liften eine Basis hoch nach M und bezeichnen den $\mathbb{F}_pG$-Aufspann davon mit M'. Wir definieren M'' über $M' \rightarrowtail M \twoheadrightarrow M''$. Da $M'_G \simeq M_G$, ist $M''_G = 0$ und damit auch $M'' = 0$ nach dem

Lemma. *Sei G eine p-Gruppe und M ein endlich erzeugter $\mathbb{F}_pG$-Modul. Dann gilt: $M_G = 0 \implies M = 0$.*

Also erhalten wir $M = M'$. Weiter wählen wir eine über $\mathbb{F}_pG$ freien Modul F mit $F \twoheadrightarrow M$. Der Kern ist dann nach einem ähnlichen Schluß wieder trivial.
Für das Lemma zeigt man induktiv, daß die invertierbaren Elemente in $\mathbb{F}_pG$ gerade die $c \in \mathbb{F}_pG \setminus \Delta G$ sind. Damit ist $\mathbb{F}_pG$ ein lokaler Ring mit maximalem beidseitigem Ideal ΔG. Die Behauptung liefert jetzt Nakajamas Lemma.

Wir fassen die Folgerungen aus obigem Resultat im folgendem Satz zusammen. Sie beschreiben die bereits angesprochenen Kriterien für kohomologische Trivialität.

SATZ. *(a) Sei G eine p-Gruppe, M ein G-Modul mit $pM = 0$. Dann sind äquivalent:*

- *i. M ist frei über $\mathbb{F}_pG$.*
- *ii. M ist induziert.*
- *iii. M ist c.t.*
- *iv. $H^q(G, M) = 0$ für ein $q \in \mathbb{Z}$.*

(b) Sei G eine p-Gruppe, M ein G-Modul ohne p-Torsion. Dann sind äquivalent:

- *i. M ist c.t.*
- *ii. $H^q(G, M) = H^{q+1}(G, M) = 0$ für ein $q \in \mathbb{Z}$.*
- *iii. M/p ist frei über $\mathbb{F}_pG$.*

(c) Sei G eine p-Gruppe, M ein $\mathbb{Z}$ freier G-Modul und c.t. Dann ist auch $Hom(M, A)$ c.t. für alle $\mathbb{Z}$-freien G-Moduln A.

(d) Sei G eine endliche Gruppe, M ein $\mathbb{Z}$-freier G-Modul. Dann gilt: M ist projektiv über $\mathbb{Z}G \iff M$ ist c.t. über $\mathbb{Z}P$ für alle p-Sylowgruppen P von G. Insbesondere ist projektiv äquivalent zu [c.t. und frei über $\mathbb{Z}$].

(e) Sei G eine endliche Gruppe, M ein G-Modul. Dann sind äquivalent:

- *i. $H^q(P, M) = H^{q+1}(P, M) = 0$ für alle p-Sylowgruppen P von G und ein $q = q(p)$.*
- *ii. M ist c.t.*
- *iii. $pd_{\mathbb{Z}G}(M) \leq 1$*

Insbesondere: $pd_{\mathbb{Z}G}(M) \leq 1 \iff pd_{\mathbb{Z}G}(M) < \infty$.

4. *Technische Anwendungen; ein Satz von Tate*

SATZ A. *G sei endlich und $f : M \to M'$ eine G-Modulabbildung. Für die in der Kohomologie induzierte Abbildung $f^{(i)} : H^i(P, M) \to H^i(P, M')$, wobei P alle Sylowuntergruppen von G durchlaufe, gelte: $f^{(i)}$ ist surjektiv für ein $i = n = n(P)$, bijektiv für $i = n + 1$ und injektiv für $i = n + 2$. Ist dann N ein G-Modul mit $\mathrm{Tor}(M, N) = 0 = \mathrm{Tor}(M', N)$, so ist $f_U^{(i)} : H^i(U, M \otimes N) \to H^i(U, M' \otimes N)$ bijektiv für alle $i \in \mathbb{Z}$ und alle Untergruppen $U \leq G$.*

Beweisskizze: Setze $\tilde{M} = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, M) \supset M$, $X = \tilde{M} \oplus M'$, $f : M \rightarrowtail X, m \mapsto m + f(m)$, $Y = X/f(M)$. Dann haben X und M' dieselbe Kohomologie, da $\tilde{M}$ koinduziert ist, und deshalb ist $H^q(P, Y) = 0$ für $q = n, n + 1$, also Y c.t.. Nun ist X eine direkte Summe aus den $\mathbb{Z}$-Moduln M und M', woraus zuerst $\mathrm{Tor}(X, N) = 0$ und daraus dann $\mathrm{Tor}(Y, N) = 0$ resultiert. Somit ist auch $Y \otimes N$ c.t. und $M \otimes N \rightarrowtail X \otimes N \twoheadrightarrow Y \otimes N$ liefert $H^q(U, M \otimes N) \simeq H^q(U, X \otimes N)$. Aber zufolge der Definition von X gilt auch $H^q(U, X \otimes N) \simeq H^q(U, M' \otimes N)$.

FOLGERUNG. *L, M, N seien G-Moduln und $\varphi : L \times M \to N$ eine bilineare, G-invariante Abbildung. Weiter seien ein $a \in H^q(G, L)$, eine Untergruppe $U \leq G$ und ein G-Modul Q so gegeben, daß die vom Cupprodukt mit $res_G^U a$ und φ induzierte Abbildung*

$$f_n(U, Q) : H^n(U, M \otimes Q) \to H^{n+q}(U, N \otimes Q)$$

für alle $U = P$ und ein $n = n(P)$ surjektiv, für $n + 1$ bijektiv und für $n + 2$ injektiv ist. Dann ist $f_n(U, Q)$ bijektiv für alle $n \in \mathbb{Z}, U \leq G$ und alle Q mit $\mathrm{Tor}(M, Q) = 0 = \mathrm{Tor}(Q, N)$.

Der Beweis geschieht durch Dimensionsverschiebung $q-1 \to q$; $q=0$ ist Satz A.

SATZ B. *Gegeben sei ein $a \in H^2(G,M)$, dessen Restriktion auf jede Sylowuntergruppe P Erzeugendes von $H^2(P,M)$ mit der Ordnung $|P|$ sei; außerdem gelte $H^1(P,M) = 0$. Dann stiftet das Cupprodukt mit $\mathrm{res}_G^U(a)$ einen Isomorphismus $H^n(U,Q) \simeq H^{n+2}(U, M \otimes Q)$ für alle $n \in \mathbb{Z}$ und alle $U \leq G$, sofern $\mathrm{Tor}(M,Q) = 0$ ist.*

Dazu setze in der Folgerung das dortige $M = \mathbb{Z}$ und $L = N =$ das neue M, sowie $q = 2$, und wähle $\varphi : M \times \mathbb{Z} \to M$ kanonisch; $n(P) = -1$.

FOLGERUNG. *In obiger Situation ist das Cupprodukt mit $\mathrm{res}_G^U(a)$ ein Isomorphismus $H^n(U,\mathbb{Z}) \simeq H^{n+2}(U,M)$.*

2. Kohomologischer Aufbau der Klassenkörpertheorie, 1

Es sei K ein lokaler Körper oder ein Zahlkörper und G_K seine absolute Galoisgruppe. Wir betrachten die offenen Untergruppen $G_L \leq G_K$ für alle endlichen Erweiterungen L/K. Ein G_K-Modul ist per definitionem ein $\mathbb{Z}G_K$-Modul M mit der Eigenschaft

$$\forall\, m \in M \exists\, L/K : \{\sigma \in G_K : m^\sigma = m\} = G_L\,.$$

Wir schreiben M_L für $M^{G_L} = \{m \in M : m^\sigma = m\,(\forall\, \sigma \in G_L)\} = H^0(G_L, M)$ mit dem gewöhnlichen H^0. Beachte $M = \bigcup_L M_L$.

Ist L/F eine galoissche Erweiterung von über K endlichen Körpern, so ist $G(L/F) = G_F/G_L$ und $H^0(G(L/F), M_L) = M_F$. Galoissche Erweiterungen L/F und L'/F' mit $L \subset L'$ und $F \subset F'$ liefern Gruppenabbildungen

$$\begin{array}{ccccc} G(L'/F') & & \to & & G(L/F) \\ & \searrow & & \nearrow & \\ & & G(L/F') & & \end{array}$$

und in der Kohomologie die Inflation (für $q \geq 0$), $H^q(G(L/F), M_L) \to H^q(G(L'/F), M_{L'})$, die Restriktion und Corestriktion (für alle $q \in \mathbb{Z}$), $H^q(G(L/F), M_L) \leftrightarrows H^q(G(L/F'), M_L)$, sowie die Konjugation mit $\sigma \in G_K$, $H^q(G(L/F), M_L) \to H^q(Gl^\sigma/F^\sigma, M_{L^\sigma}))$, wieder für alle $q \in Z$.

SATZ. *Ist K lokal, so erfüllt $M = (K^c)^\times$*

1. *$H^1(G(L/F), M_L) = 0$*
2. *$\exists\, \mathrm{inv}_F : H^2(G(L/F), M_L) \rightarrowtail \mathbb{Q}/\mathbb{Z}$, so daß das Bild $\mathrm{im}\,(\mathrm{inv}_F)$ die zyklische Untergruppe der Ordnung $[L:F]$ von $\mathbb{Q}/\mathbb{Z}$ ist und*

   $$\mathrm{inv}_{F'}\mathrm{res}_{\,F/F'} = [F':F]\mathrm{inv}_F$$

   gilt.

Dabei ist 1. Hilberts Satz 90 und 2. eine Folgerung aus den Ergebnissen des nächsten Paragraphen.

Ist K global, so liefert $M_L = C_L$, die Idèleklassengruppe von L (an Stelle von $L^\times$), denselben Satz. Der Beweis wird dann aber erheblich schwieriger.

3. Die Brauergruppe eines lokalen Körpers

K sei endlich über $\mathbb{Q}_p$ mit Ganzheitsring $\mathfrak{o}$, maximalem Ideal $\mathfrak{p}$, Primelement π, Restklassenkörper k und Bewertung v. D sei ein zentraler Schiefkörper über K der Dimension s^2. Die folgenden Beobachtungen zeigen unter anderem, daß v eindeutig zu einer Bewertung w von D erweitert werden kann und daß es in D, wie in K, einen Ganzheitsring $\mathfrak{O}$ gibt.

1. Ist $f(x) \in K[x]$ irreduzibel und normiert, so impliziert $f(0) \in \mathfrak{o}$, daß $f(x) \in \mathfrak{o}[x]$ liegt. (Das ist im wesentlichen Hensels Lemma.)

2. Sei $d \in D$. Das (reduzierte) charakteristische Polynom von d hat Grad s und ist eine Potenz der irreduziblen Gleichung $f_d(x)$ von d über K (dem Minimalpolynom von d).

3. Definiere : $D \ni d$ heiße ganz, falls $\mathrm{nr}(d)$ ganz in K ist.
   Die reduzierte Norm von d, $\mathrm{nr}(d)$, ist der konstante Koeffizient vom charakteristischen Polynom von d.

   Somit : $d \in D$ ganz $\iff$ $f_d(x) \in \mathfrak{o}[x]$ und

   (a) die ganzen Elemente von D bilden einen Ring $\mathfrak{O}$
   (b) $\mathfrak{o} \subset \mathfrak{O}$
   (c) zu $d \in D$ gibt es ein $\alpha \in \mathfrak{o}$ mit αd ist ganz
   (d) $\mathfrak{O}$ ist über $\mathfrak{o}$ endlich erzeugt und hat den Rang s^2
   (e) alle Ideale sind zweiseitig und Potenzen des Hauptideal $\Pi\mathfrak{O}$, wobei Π ein Element in D ist, so daß $\mathrm{nr}(\Pi)$ minimalen positiven Wert habe
   (f) jedes $0 \neq d \in D$ ist schreibbar als $d = \Pi^\delta \varepsilon$ mit $\delta \in \mathbb{Z}$ und $\varepsilon \in \mathfrak{O}^\times$; $w(d) = \delta$ definiert die Bewertung von D
   (g) $\mathfrak{O}/\Pi$ ist ein kommutativer Körper vom Grad f über k
   (h) $e = w(\pi)$ und f erfüllen $e = f = s$
   (i) mit $|k| = q$ gilt $\zeta \overset{\mathrm{def}}{=} \zeta_{q^s-1} \in D$; es gibt ein $\Pi \in D^\times$ mit

   $$\Pi\zeta\Pi^{-1} = \zeta^{q^r}\ ,\ (r,s) = 1\ ,\ \Pi^s = \pi$$

   (j) D ist durch r eindeutig bestimmt und zu jedem r existiert ein $D \in \mathrm{Br}(K)$ vom Schurindex s.

Für die letzte Aussage gehe man auf die kohomologische Beschreibung zurück: Unser D ist das verschränkte Produkt $(K_s/K, \sigma, \pi^{r'})$ mit der unverzweigten Erweiterung K_s/K vom Grad s, dem Frobeniusautomorphismus $\sigma \in G(K_s/K)$ und $r' < s$ so, daß $r \cdot r' \equiv 1 \mod s$ gilt (wir vergessen im folgenden r und schreiben dann r für r'). Man sieht: diese Beschreibung ist unabhängig von der Wahl des Primelementes π in K, da alle Einheiten aus K Normen von K_s sind; aus dem gleichen Grund liefern verschiedene r verschiedene D. Lassen wir die Voraussetzung $(r,s) = 1$ fallen, so erhalten wir noch zentral-einfache K-Algebren, aber nicht unbedingt mehr Schiefkörper; allerdings gilt $(K_s/K,\sigma,\pi^r) \sim (K_{s'}/K,\sigma',\pi^{r'})$, wenn $\frac{r}{s} = \frac{r'}{s'}$ mit teilerfremden r', s' geschrieben wird und $K_{s'}$ die unverzweigte Erweiterung von K vom Grad s' und σ' deren Frobeniusautomorphismus bezeichnet. Genau dann ist $(K_s/K,\sigma,\pi^r)$ ein Schiefkörper, wenn $(r,s)=1$ gilt.

FOLGERUNG. *Ordnung in* $\mathrm{Br}(K)$ *und Schurindex stimmen überein. De weiteren ist jeder lokale Schiefkörper zyklisch (enthält also mittig einen über K zyklischen [nämlich unverzweigten] kommutativen Teilkörper).*

Die Definition der Invarianten ist nun offensichtlich:

$$\mathrm{inv}_K(K_s/K,\sigma,\pi^r) = r/s \mod \mathbb{Z} \quad (\text{in } \mathbb{Q}/\mathbb{Z}).$$

Multiplikativität und Injektivität sind nach obigem klar; die Kommutativität des Diagramms

$$\begin{array}{rcl} \mathrm{Br}(K) & \xrightarrow{\mathrm{inv}_K} & \mathbb{Q}/\mathbb{Z} \\ L\otimes_K - \downarrow & & [L:K]\downarrow \\ \mathrm{Br}(L) & \xrightarrow{\mathrm{inv}_L} & \mathbb{Q}/\mathbb{Z} \end{array}$$

rechnet man für endliche Erweiterungen L/K ohne weiteres nach. Das Diagramm hat die Folgerung

> *Ist L/F galoissch endlich, so ist* $\mathrm{inv}_F(H^2(G(L/F),L^\times))$ *die zyklische Untergruppe der Ordnung $[L:F]$ in $\mathbb{Q}/\mathbb{Z}$.*
>
> *L zerfällt $D \in \mathrm{Br}(K) \iff s_D \mid [L:K]$*
>
> *Jede Erweiterung L/K vom Grad $\mid s_D$ läßt sich in D einbetten.*

4. Kohomologischer Aufbau der Klassenkörpertheorie, 2

Als Anwendung des Satzes aus §2 erhalten wir

> *Sei L/F galoissch endlich und F' ein Zwischenkörper. Dann ist die Restriktion* $\mathrm{res}_{F/F'} : H^2(G(L/F),L^\times) \to H^2(G(L/F'),L^\times)$ *surjektiv und die Korestriktion* $\mathrm{cor}_{F'/F} : H^2(G(L/F'),L^\times) \to H^2(G(L/F),L^\times)$ *injektiv; des weiteren gilt*
>
> $$\mathrm{inv}_F \circ \mathrm{cor}_{F'/F} = \mathrm{inv}_{F'} \quad \text{und} \quad \mathrm{inv}_{\sigma(F)} \circ \sigma = \mathrm{inv}_F \quad \forall\, \sigma \in G_K.$$

Mit $u_{L/F} \in H^2(G(L/F),L^\times)$ werde die *Fundamentalklasse von L/F* bezeichnet, also $\mathrm{inv}_F(u_{L/F}) = 1/[L:F] \in \mathbb{Q}/\mathbb{Z}$. Offenbar gelten die Gleichheiten

1. $\mathrm{infl}_{F'/L}(u_{F'/F}) = [F':F]u_{L/F}$ falls F'/F galoissch ist
2. $\mathrm{res}_{L/F}(u_{L/F}) = u_{L/F'}$
3. $\mathrm{cor}_{L/F'}(u_{L/F'}) = [F':F]u_{L/F}$
4. $u_{\sigma L/\sigma F} = \sigma(u_{L/F})$ für $\sigma \in G_K$.

Und Tates Satz liefert die Isomorphismen *Cupprodukt mit der Fundamentalklasse*

$$H^n(G(L/F),\mathbb{Z}) \xrightarrow{\theta^n} H^{n+2}(G(L/F),L^\times)\,,$$

dessen Umkehrung, für $n=-2$, wir die *Reziprozitätsabbildung*

$$F^\times/N_{L/F}L^\times \xrightarrow{\simeq} G(L/F)^{\mathrm{ab}}\,,\ a\mapsto (a,L/F)$$

nennen. Beachte hier $H^{-2}(G(L/F),\mathbb{Z}) = G(L/F)^{\mathrm{ab}}$ (kanonisch, nämlich wegen $\Delta G \rightarrowtail \mathbb{Z}G \twoheadrightarrow \mathbb{Z}$) und $\theta=\theta^{-2} : G(L/F)^{\mathrm{ab}} \xrightarrow{\simeq} F^\times/N_{L/F}L^\times$.

Folgerung. *Ist L/F galoissch endlich und L_{ab} die größte über F abelsche Erweiterung in L (also $G(L/F)^{\mathrm{ab}} = G(L_{\mathrm{ab}}/F)$), so gilt*

$$N_{L/F}(L^\times) = N_{L_{\mathrm{ab}}/F}(L_{\mathrm{ab}}^\times)\,.$$

θ^n vertauscht mit der Restriktion und der Korestriktion; für die Reziprozitätsabbildung haben wir die Formel

$$(*) \qquad \chi((a,L/F)) = \mathrm{inv}_F(a\cdot d\chi)\,,$$

wobei $\chi\in \mathrm{Hom}(G(L/F),\mathbb{Q}/\mathbb{Z})$ (der Dualgruppe von $G(L/F)^{\mathrm{ab}}$) und $d: H^1(G(L/F),\mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G(L/F),\mathbb{Q}/\mathbb{Z}) \xrightarrow{\simeq} H^2(G(L/F),\mathbb{Z})$ der Verbindungshomomorphismus ist. Im Beweis dieser Formel geht die Gleichung

$$\begin{array}{ccc} H^1(G,B) & \xrightarrow{\cdot\overline{\sigma}} & H^{-1}(G,B) \\ f & \mapsto & f(\sigma) \end{array}$$

ein, in der $\overline{\sigma}\in G^{\mathrm{ab}} = H^{-2}(G,\mathbb{Z}) = \Delta G/\Delta^2 G$ dem $\sigma-1\in\Delta G$ entspreche und das Urbild σ in G habe.

Schließlich sehen wir die folgenden kommutativen Quadrate, induziert von der Korestriktion in Dimension 0 bzw. -2, der Restriktion in Dimension 0 bzw. -2 und der Konjugation für die ersten drei Diagramme (im Uhrzeigersinn). Das vierte Diagramm, für den Körperturm $L\supset F'\supset F$ mit galoisschem L/F und galoisschem F'/F resultiert aus obiger Formel $(*)$.

$$\begin{array}{ccccccc} F'^\times & \xrightarrow{N} & F^\times & \qquad & F^\times & \xrightarrow{\subset} & F'^\times \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ G(L/F')^{\mathrm{ab}} & \xrightarrow{\text{kan}} & G(L/F)^{\mathrm{ab}} & & G(L/F)^{\mathrm{ab}} & \xrightarrow{\text{ver}} & G(L/F')^{\mathrm{ab}} \\ & & & & & & \\ F^\times & \xrightarrow{\sigma} & (\sigma F)^\times & & F^\times & \xrightarrow{=} & F^\times \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ G(L/F)^{\mathrm{ab}} & \xrightarrow{\sigma} & G(\sigma L/\sigma F)^{\mathrm{ab}} & & G(L/F)^{\mathrm{ab}} & \xrightarrow{\text{kan}} & G(F'/F)^{\mathrm{ab}} \end{array}$$

Als Anwendung des letzten Quadrates und des Reziprozitätsisomorphismus erhalten wir schließlich für abelsche Erweiterungen L_1/K und L_2/K zuerst, daß

$$N_{L_1/K}L_1^\times \cap N_{L_2/K}L_2^\times = N_{L_1L_2/K}(L_1L_2)^\times$$

und daraus, daß die Korrespondenz $[\,L/K \text{ abelsch} \leftrightarrow N_{L/K}L^\times\,]$ eineindeutig ist.

Satz. *Die Normengruppen der endlichen abelschen Erweiterungen von K sind genau die Untergruppen von $K^\times$, die ein $K^{\times m}$ für ein $m \in \mathbb{N}$ enthalten. Es sind damit genau diejenigen Untergruppen oberhalb $\langle \pi^f \rangle \times U_K^{(n)}$ mit $f \in \mathbb{N}$, $n \in \mathbb{Z}_{\geq 0}$, oder, in topologischer Sprechweise, die offenen Untergruppen von endlichem Index.*

Bemerkung: Die zu diesen ausgezeichneten Untergruppen gehörigen abelschen Körpererweiterungen von K heißen *Klassenkörper*. Jede endliche abelsche Erweiterung von K ist also Teilkörper eines geeigneten Klassenkörpers.

Ein Beispiel: Im unverzweigten Fall ($L = K_s$) ist $u_{K_s/K}$ repräsentiert von $(K_s/K, \sigma, \pi) \in H^0(K_s/K, K_s^\times) \subset \mathrm{Br}(K)$ und es gilt $(a, K_s/K) = \sigma^\alpha$ mit $v(a) = \alpha$. Dies resultiert aus Anwendung der exakten Sequenzen (mit $G = \langle \sigma \rangle = G(K_s/K)$)

$$\Delta G \rightarrowtail \mathbb{Z}G \twoheadrightarrow \mathbb{Z} \quad , \quad \mathbb{Z} \overset{N_G}{\rightarrowtail} \mathbb{Z}G \overset{\cdot(\sigma-1)}{\twoheadrightarrow} \Delta G$$

(die beide über $\mathbb{Z}$ zerfallen), indem man $\sigma^i \in G$ zuerst mit $\sigma^i - 1 \in H^{-1}(K_s/K, \Delta G)$ und dann mit i in $H^0(K_s/K, \mathbb{Z})$ identifiziert ($\sigma^i - 1$ hat das Urbild $\frac{\sigma^i - 1}{\sigma - 1}$ in $\mathbb{Z}G$, worauf nun N_G anzuwenden ist, um nach $H^0(K_s/K, \mathbb{Z})$ zu kommen: beachte aber, daß $\mathbb{Z}$ über N_G in $\mathbb{Z}G$ eingebettet ist). Als Folgerung erhält man eine erste Verzweigungsaussage über die Reziprozitätsabbildung, nämlich *ist L/K abelsch, so ist das Bild der Einheitengruppe U_K von K unter der Reziprozitätsabbildung die Trägheitsgruppe G_0 von $G = G(L/K)$.*

Eine Frage (an ME; 'man versuche, den kohomologischen Apparat zu vermeiden'): $G = G(L/K)$ sei abelsch und χ ein Charakter in $\hat{G}$. Definiere eine Paarung $\hat{G} \times K^\times / N_{L/K} L^\times \to \mathbb{Q}/\mathbb{Z}$ über $(\chi, a) = (L_\chi/K, \sigma_\chi, a) \in \mathrm{Br}(K)$, wobei L_χ der Fixkörper von $\ker \chi \leq G$ in L ist und σ_χ durch $\chi(\sigma_\chi) = e^{2\pi i/[L_\chi : K]}$ definiert sei. Ist diese Paarung nicht ausgeartet, so daß also ein Isomorphismus $G \simeq K^\times / N_{L/K} L^\times$ resultiert? Welche Eigenschaften hat der?

Der globale Fall: man zeigt, daß die Ersetzung der Galoismoduln $L^\times$ durch C_L zu den für den globalen Fall analogen Ergebnissen führt. Im Existenzsatz ist jetzt die topologische Sprechweise die geeignete (die Normengruppen sind die abgeschlossenen Untergruppen von endlichem Index in C_K und dies sind die Obergruppen von $C_k^{\mathfrak{m}} = J_K^{\mathfrak{m}}/K$ mit $J_K^{\mathfrak{m}} = \prod_{\mathfrak{p}} U_{\mathfrak{p}}^{(n_{\mathfrak{p}})}$ und $U_{\mathfrak{p}}^{(n_{\mathfrak{p}})}$ der Einseinheitengruppe der Stufe $n_{\mathfrak{p}}$ in $K_{\mathfrak{p}}$ bei endlichem $\mathfrak{p}$ und $= \mathbb{R}_+, \mathbb{R}^\times, \mathbb{C}^\times$ im Falle eines reellen $\mathfrak{p}$ mit $n_{\mathfrak{p}} = 1$, bzw. mit $n_{\mathfrak{p}} = 0$, bzw. eines komplexen $\mathfrak{p}$; $\mathfrak{m}$ ist das Tupel der $n_{\mathfrak{p}} \geq 0$ (mit der genannten Einschränkung für reelle Stellen) und von denen fast alle $= 0$ seien).

5. Kronecker-Weber

Der Satz, nach obigen Herren benannt, hat eine globale und eine lokale Version, nämlich

ist $K/\mathbb{Q}$ endlich abelsch, so gilt $K \subset \mathbb{Q}(\zeta_n)$ für geeignetes n

sowie

ist $K/\mathbb{Q}_p$ endlich abelsch, so gilt $K \subset \mathbb{Q}_p(\zeta_n)$ für geeignetes n.

Damit sind also die Einheitswurzelkörper sowohl die sämtlichen Klassenkörper über $\mathbb{Q}$ als auch über $\mathbb{Q}_p$.

1. *Rückführung der globalen Aussage auf die lokale.* Sei dazu $K/\mathbb{Q}$ abelsch und $V = \{p$ Primzahl, p verzweigt in $K\}$. Wähle gemäß der lokalen Aussage ein n mit $K_{\mathfrak{p}} \subset \mathbb{Q}_p(\zeta_n)$ für die (endlich vielen) $p \in V$ (mit $\mathfrak{p}|p$) und setze $m = \prod_{p \in V} n_p$, wobei n_p die höchste Potenz von p in n ist. Man zeigt nun $K(\zeta_m) = \mathbb{Q}(\zeta_m)$, also $K \subset \mathbb{Q}(\zeta_m)$. Und zwar so:

(a) Ist p verzweigt in $K(\zeta_m)$, so ist $p \in V$.

(b) Die Verzweigungsgruppe von $K(\zeta_m)/\mathbb{Q}$ bei p (also die der lokalen Galoisgruppe) hat eine Ordnung $\leq \varphi(n_p)$, weil $K(\zeta_m)_{\mathfrak{P}} = K_{\mathfrak{p}}(\zeta_m) \subset \mathbb{Q}_p(\zeta_{n_p n'})$ mit $p \nmid n'$.

(c) $|\prod_{p \in V} G_0(K(\zeta_m)_{\mathfrak{P}}/\mathbb{Q}_p)| \leq \prod_{p \in V} \varphi(n_p) = \varphi(m) = [\mathbb{Q}(\zeta_m) : \mathbb{Q}]$

(d) Der Fixkörper von $\prod_{p \in V} G_0(K(\zeta_m)_{\mathfrak{P}}/\mathbb{Q}_p)$ ist unverzweigt über $\mathbb{Q}$, also $= \mathbb{Q}$, und damit ist diese Gruppe $= G(K(\zeta_m)/\mathbb{Q})$.

(e) $|G(K(\zeta_m)/\mathbb{Q}))| \leq [\mathbb{Q}(\zeta_m) : \mathbb{Q}]$.

2. *Beweis der lokalen Aussage.* Dazu reicht es, Körper $K/\mathbb{Q}_p$ mit Gruppe $G(K/\mathbb{Q}_p) = \mathbb{Z}/l^m$ für Primzahlen l zu betrachten.

$l \neq p$ $F/\mathbb{Q}_p$ sei die maximal unverzweigte Erweiterung in $K/\mathbb{Q}_p$. Sicher gilt $F = \mathbb{Q}_p(\zeta)$ für ein geeignetes ζ. Weiter ist K/F rein und zahm verzweigt, also $K = F(\sqrt[r]{\pi_F})$ mit $r = [K : F]$, prim zu p. Schreibe $\pi_F = -p\varepsilon$ mit einer Einheit $\varepsilon \in F$. Es folgt

i. $F(\sqrt[r]{\varepsilon})/F$ ist unverzweigt, weil $p \nmid r$; insbesondere ist $F(\sqrt[r]{\varepsilon})/\mathbb{Q}_p$ unverzweigt und also $\mathbb{Q}_p(\sqrt[r]{\varepsilon})/\mathbb{Q}_p$ abelsch und enthalten in einem Einheitswurzelkörper.

ii. $\mathbb{Q}_p(\sqrt[r]{\varepsilon}) \subset K$, also ist auch $\mathbb{Q}_p(\sqrt[r]{\pi_F})/\mathbb{Q}_p$ abelsch.

iii. $\mathbb{Q}_p(\sqrt[r]{-p})/\mathbb{Q}_p$ ist abelsch und rein verzweigt, somit $\zeta_{p^r} \in \mathbb{Q}_p$ und $r \mid p-1$.

iv. Wegen $\mathbb{Q}_p(\zeta_p) = \mathbb{Q}_p(\sqrt[p-1]{-p})$, ist damit $\mathbb{Q}_p(\sqrt[r]{-p}) \subset \mathbb{Q}_p(\zeta_p)$.

$l = p \neq 2$ Sei F die unverzweigte Erweiterung von $\mathbb{Q}_p$ vom Grad $p^m = l^m$ und L der Teilkörper von $\mathbb{Q}_p(\zeta_{p^{m+1}})$ vom Index $p-1$. Wäre K nicht in FL enthalten, so hätte das Kompositum KFL eine Gruppe vom Typ $\mathbb{Z}/p^m \times \mathbb{Z}/p^m \times \mathbb{Z}/p^{m'}$ mit $m' \geq 1$ über $\mathbb{Q}_p$, und die wiederum eine Faktorgruppe vom Typ $(\mathbb{Z}/p)^3$. Zum entsprechenden Teilkörper gehört dann eine Normengruppe N mit

$$\mathbb{Q}_p{}^\times = \langle p \rangle \times \langle \zeta_{p-1} \rangle \times U^{(1)} \supset N \supset \langle p^f \rangle \times U^{(r)}$$

(für ein Paar $(f, r) \in \mathbb{N} \times \mathbb{N}$) mit $\mathbb{Q}_p{}^\times/N = (\mathbb{Z}/p)^3$. Das ist aber unmöglich, weil $U^{(1)}/U^{(r)}$ zyklisch ist (erzeugt von $1 + p$).

$l = p = 2$ Die Diskussion verläuft analog zur vorhergehenden, nur daß jetzt $\mathbb{Q}_2(\zeta_{2^{m+2}})$ (statt $\mathbb{Q}_p(\zeta_{p^{m+1}})$) betrachtet wird und man auf eine Faktorgruppe des Typs $(\mathbb{Z}/2)^4$ stößt.

6. Lubin-Tate

In diesem Kapitel werden die Klassenkörper zu den Normgruppen $\langle \pi^f \rangle U_K^{(n)}$ konstruiert. Neben der Originalarbeit von Lubin und Tate ist Neukirchs *Klassenkörpertheorie* eine gute Quelle.

Wir gehen etwas direkter vor. Wie früher fixieren wir eine endliche Erweiterung $K/\mathbb{Q}_p$, den Ring der ganzen Zahlen $\mathfrak{o}$ in K, darin ein Primelement π und die Ordnung q des Restklassenkörpers k. Im ersten Schritt wird mit Hilfe von Potenzreihen (*formale Gruppen*) gezeigt, daß der Körper $L_{\pi,n}$, der durch Adjunktion der Wurzeln von einer aus $x^q + \pi x = 0$ abgeleiteten Gleichung an K entsteht, eine rein verzweigte abelsche Erweiterung von K mit Galoisgruppe $\simeq U_K/U_K^{(n)}$ ist. Im nächsten Schritt wird gezeigt, daß mit $K^{\mathrm{nr}} \overset{\mathrm{def}}{=} \bigcup_s K_s$, *der maximal unverzweigten Erweiterung von* K [1], $K^{\mathrm{nr}} L_{\pi,n}$ unabhängig von der speziellen Wahl des Primelementes π ist. Und schließlich, im dritten Schritt, wird die Artinsche Reziprozitätsabbildung für $K^{\mathrm{nr}} L_{\pi,n}/K$ berechnet und, mit $L_\pi \overset{\mathrm{def}}{=} \bigcup_n L_{\pi,n}$, $K^{\mathrm{ab}} = K^{\mathrm{nr}} L_\pi$ nachgewiesen.

[1] K_s/K ist, wie zuvor, die unverzweigte Erweiterung vom Grad s

1. $\mathfrak{o}[[T]]$ bezeichne den Potenzreihenring in der Variablen T über $\mathfrak{o}$; gelegentlich mag T auch endlich viele voneinander unabhängige, vertauschbare Variable abkürzen. *Wir betrachten nur solche Potenzreihen in* $\mathfrak{o}[[T]]$*, die für* $T = 0$ *Null ergeben.* Man sieht sofort, daß die Substitution von T durch eine solche Potenzreihe nicht aus $\mathfrak{o}[[T]]$ hinausführt. Ist $f(T) \in \mathfrak{o}[[T]]$ mit $f(0) = 0$, so bezeichne $f^{[n]}(T)$ das Ergebnis vom n-maligen sukzessiven Einsetzen von f für T. Im folgenden ist $f(T) = T^q + \pi T$.

   (a) $f^{[n]}(T) = f^{[n-1]}(T)(f^{[n-1]}(T)^{q-1} + \pi)$, und der rechte Faktor ist ein Eisensteinpolynom vom Grad $(q-1)q^{n-1} = |U_K/U_K^{(n)}|$. Ist also α_0 eine Wurzel dieses Eisensteinpolynoms (und damit von $f^{[n]}(T)$), so erzeugt α_0 eine Erweiterung von K vom Grad $|U_K/U_K^{(n)}|$.

   (b) Die Gleichung $f^{[n]}(T)$ ist separabel und hat q^n Wurzeln. Der Gesamtheit $W_{\pi,n}$ dieser kann eine $\mathfrak{o}$-Modulstruktur aufgeprägt werden, so daß $W_{\pi,n} \simeq \mathfrak{o}/\pi^n$ wird. Insbesondere folgt $[L_{\pi,n} : K] \leq |U_K/U_K^{(n)}|$ und weiter $L_{\pi,n} = K(\alpha_0)$ und die Gleichheit $[L_{\pi,n} : K] = |U_K/U_K^{(n)}|$, sowie daß $L_{\pi,n}/K$ rein verzweigt abelsch mit $G(L_{\pi,n}/K) \simeq U_K/U_K^{(n)}$ ist.

   Die $\mathfrak{o}$-Modulstruktur auf $W_{\pi,n}$ resultiert dabei aus einer neuen $\mathfrak{o}$-Modulstruktur vom maximalen Ideal $\mathfrak{p}_{\pi,n}$ von $L_{\pi,n}$ und die wiederum aus dem folgenden Hilfssatz:

   Es existieren eindeutig bestimmte Potenzreihen $F(X,Y) \in \mathfrak{o}[[X,Y]]$ *und, für* $a \in \mathfrak{o}$*,* $A(T) \in \mathfrak{o}[[T]]$ *mit*

   $$F(X,Y) \equiv X + Y \mod \text{grad} 2\,, \quad f(F[X,Y)) = F(f(X), f(Y))$$
   $$A(T) \equiv aT \mod \text{grad} 2\,, \quad f(A(T)) = A(f(T))\,.$$

   Es folgt unmittelbar [2]

   $$F(X,Y) = F(Y,X)\,,\ F(F(X,Y),Z) = F(X, F(Y,Z))$$
   $$A(F(X,Y)) = F(A(X), A(Y))\,,\ A(B(T)) = (AB)(T)\,,\ (A+B)(T) = F(A(T), B(T))$$
   $$\Pi^n(T) = f^{[n]}(T) \text{ mit } \Pi(T) \leftrightarrow \pi \in \mathfrak{o}\,.$$

   In eine Potenzreihe ohne nullten Koeffizient können Elemente aus $L_{\pi,n}$ vom Wert > 0 eingesetzt werden mit einem Ergebnis wieder vom Wert > 0 in $L_{\pi,n}$. Damit erhält man auf dem maximalen Ideal $\mathfrak{p}_{\pi,n}$ von $L_{\pi,n}$ eine von $F(X,Y)$ gestiftete neue Addition und eine von $A(T)$ gestiftete skalare Multiplikation mit $a \in \mathfrak{o}$, nämlich über:

   $$\alpha_1 \oplus \alpha_2 = F(a_1 + \alpha_2)\,,\ a \circ \alpha = A(\alpha)\,,$$

   und damit gilt dann

   $$W_{\pi,n} \simeq \mathfrak{o}/\pi^n \quad \text{und} \quad \mathrm{Aut}_{\mathfrak{o}}(W_{\pi,n}) = U_K/U_K^{(n)}\,.$$

2. Die Abhängigkeit von der Wahl von π geht erst nach dem Kompositum von $L_{\pi,n}$ mit der maximal unverzeigten Erweiterung K^{nr} von K verloren: *Sind* π_1, π_2 *zwei Primelemente von* K*, so gilt* $K^{\mathrm{nr}}L_{\pi_1,n} = K^{\mathrm{nr}}L_{\pi_2,n}$. Dies folgt aus der Beobachtung

[2] dabei gehört $B(T)$ zu $b \in \mathfrak{o}$ und $(A \dotplus B)(T)$ zu $a \dotplus b$

(a) *Ist $\pi_2 = u\pi_1$, so existiert eine Einheit ε in der Komplettierung $\widehat{K^{\mathrm{nr}}}$ von K^{nr} (bezüglich der diskreten Bewertung auf K^{nr}) mit $u = \varepsilon^{\sigma-1}$, wobei σ die stetige Fortsetzung des Frobeniusautomorphismus von K^{nr}/K auf $\widehat{K^{\mathrm{nr}}}$ ist.*

(b) *Es existiert eine Potenzreihe $P(T)$ mit ganzen Koeffizienten aus $\widehat{K^{\mathrm{nr}}}$ und folgenden Eigenschaften*

  i. $P(T) \equiv \varepsilon T \mod \mathrm{grad} 2\,,\ P^\sigma(T) = P(U_1(T))$

  ii. $P(F_1(X,Y)) = F_2(P(X),P(Y))\,,\ P(A_1(T)) = A_2(P(T))\,.$

  Hier bezeichnet U_1 die zu u hinsichtlich $f_1(T) = \pi_1 T + T^q$ gehörige Potenzreihe; entsprechend F_1, F_2, A_1, A_2.

Der Übergang zu $\widehat{K^{\mathrm{nr}}}$ ist deshalb erforderlich, weil erst im Restklassenkörper k^{c} von K^{nr} Gleichungen der Form $x^q - \overline{u}x = 0$ lösbar werden und Lösungen dann mittels Hensels Lemma in die Komplettierung $\widehat{K^{\mathrm{nr}}}$ von K^{nr} hochgehoben werden können, so also ein ε mit $\varepsilon^\sigma - u\varepsilon = 0$, i.e., $\varepsilon^{\sigma-1} = u$, liefern.

Die ersten beiden an $P(T)$ gestellten Bedingungen gehören zusammen und führen wegen $\varepsilon^{\sigma-1} = u$ in der schon früher gezeigten Art zu einer Potenzreihe mit diesen beiden Eigenschaften. Eine leichte Verallgemeinerung des Hilfssatzes aus dem ersten Schritt ist vonnöten, um das so gefundene $P(T)$ noch abändern zu können, damit auch die beiden weiteren Eigenschaften gelten. Im Hilfssatz kann nämlich ohne extra Mühe $f(T) = T^q + \pi T$ durch eine Potenzreihe $f(T) \equiv T^q + \pi T \mod \pi T^2$ ersetzt werden und darüber hinaus führen zwei solche f_1, f_2 (zum selben Primelement π) zu Potenzreihen $F_1(X,Y), F_2(X,Y)$, $A_1(T), A_2(T)$ mit

$$\begin{aligned} &F_i(X,Y) \equiv X + Y \mod \mathrm{grad} 2\,,\ F_i(f_i(X), f_i(Y)) = f_i(F_i(X,Y)) \ \ (i = 1,2) \\ &A_{12}(T) \equiv aT \mod \mathrm{grad} 2\,,\ f_1(A_{12}(T)) = A_{12}(f_2(T)) \quad \&\mathrm{c.}\,; \end{aligned}$$

schließlich gilt noch $W_{f_1,n} \simeq W_{f_2,n}$ bei Anwendung von $A_{12}(T)$.

Da ε eine Einheit ist, existiert eine Potenzreihe $Q(T)$ mit $Q(0) = 0$ und $(P(Q(T)) = T$. Damit liefert P einen Isomorphismus zwischen $W_{\pi_1,n}$ (mit der F_1-Struktur über $\mathfrak{o}$) und $W_{\pi_2,n}$ (mit der F_2-Struktur über $\mathfrak{o}$). Es resultiert $\widehat{K^{\mathrm{nr}}}L_{\pi_1,n} = \widehat{K^{\mathrm{nr}}}L_{\pi_2,n}$ und deshalb auch $K^{\mathrm{nr}}L_{\pi_1,n} = K^{\mathrm{nr}}L_{\pi_2,n}$.

Bemerkung : Auch die Normgruppen $\langle\pi\rangle U_K^{(n)}$ hängen von π ab!

3. Betrachte nun die Körper $K^{\mathrm{nr}}L_{\pi,n}$. Deren Galoisgruppen sind zu $G(K^{\mathrm{nr}}/K) \times G_{\pi,n} = \hat{\mathbb{Z}} \times U_K/U_K^{(n)}$ isomorph; $\hat{\mathbb{Z}}$ ist vom Frobenisautomorphismus σ erzeugt. Die Artinsche Reziprozitätsabbildung [3] $(-, K^{\mathrm{nr}}L_{\pi,n}/K) : K^\times \to \hat{\mathbb{Z}} \times G_{\pi,n}$ sendet

$$a = \pi^m u \in K^\times \quad \text{auf} \quad (\sigma^m, (\pi^m u, K^{\mathrm{nr}}L_{\pi,n}/K)_{|L_{\pi,n}})\,,$$

denn bei unverzweigten Erweiterungen ght π auf σ und Einheiten auf 1 – und dies ist verträglich mit der Limesbildung $K^{\mathrm{nr}} = \bigcup_s K_s$ wegen des vierten Diagramms (S.7) bezüglich des Verhaltens des Normrestsymbols. Dieses Diagramm liefert darüber hinaus

$$(\pi^m u, K^{\mathrm{nr}}L_{\pi,n}/K)_{|L_{\pi,n}} = (\pi^m u, L_{\pi,n}/K) = (u, L_{\pi,n}/K)\,;$$

[3] auch das *Normrestsymbol* genannt

letzteres, weil π Norm aus $L_{\pi,n}$ ist. Wir müssen nun $(u, L_{\pi,n}/K)$ ausrechnen.

Dazu definieren wir eine zweite Abbildung

$$\begin{array}{l}\Phi_\pi : K^\times \to \hat{\mathbb{Z}} \times G_{\pi,n}\,, \quad \Phi(\pi^m u) = (\sigma^m, \Phi_\pi(u)) \\ \text{wobei} \quad \Phi_\pi(u) \quad \text{der Automorphismus} \quad W_{\pi,n} \ni \alpha \mapsto U^{-1}(\alpha) \quad \text{sei.}\end{array}$$

Man erinnere sich hier an $G_{\pi,n} \simeq U_K/U_K^{(n)}$, $\tau_u \leftrightarrow U(-)$; U^{-1} ist natürlich durch $U(U^{-1}(T)) = T$ definiert.

Man zeigt nun, daß Φ_π das Normrestsymbol ist und nützt dazu aus, daß $K^\times$ von den Primelementen erzeugt und unsere beiden Abbildungen multiplikativ sind, sowie $K^{\mathrm{nr}} L_{\pi,n} = K^{\mathrm{nr}} L_{\pi_1,n}$ für $\pi_1 = u\pi$. Auf π selbst stimmen beide Abbildungen natürlich überein und $(\pi_1, K^{\mathrm{nr}} L_{\pi_1,n}/K) = (\sigma, 1) \in \hat{\mathbb{Z}} \times G_{\pi_1,n}$, $\Phi_\pi(\pi_1) = (\sigma, \Phi_\pi(\pi_1)_{|G_{\pi_1,n}})$. Also müssen wir $\Phi_\pi(\pi_1)_{|G_{\pi_1,n}} = 1$ zeigen, d.h.

$$\Phi_\pi(\pi_1)(P(\alpha) = P(\alpha) \quad \text{für} \quad \alpha \in W_{\pi,n}$$

(weshalb $P(\alpha) \in W_{\pi_1,n}$). Dies resultiert aus der zweiten Eigenschaft der Potenzreihe $P(T) \in \widehat{K^{\mathrm{nr}}}[[T]]$ aus 2., auf der $\Phi_\pi(\pi)$ wie σ wirkt (aber $\Phi_\pi(\pi)$ wirkt nicht auf α).

Bemerkungen:

(a) Es gilt also $(u, L_{\pi,n}/K) = [\alpha \mapsto U^{-1}(\alpha)]$. Das weist $\langle \pi^s \rangle U_K^{(n)}$ als Normgruppe von $K_s L_{\pi,n}$ aus (vgl. Aufgabe 6) und liefert explizite Reziprozitätsgesetze, wenn man die Potenzreihen U kennt. Z.B. für $\mathbb{Q}_p(\zeta)/\mathbb{Q}_p$, mit einer primitiven p^k-ten Einheitswurzel ζ, erhält man $(up^m, \mathbb{Q}_p(\zeta)/\mathbb{Q}_p)(\zeta) = \zeta^t$ mit $t \equiv u^{-1} \mod p^k$ bei $\mathbb{Z}/p^k = \mathbb{Z}_p/p^k$.

(b) Da die $K_s L_{\pi,n}$ die sämtlichen Klassenkörper sind, folgt $K^{\mathrm{ab}} = K^{\mathrm{nr}} L_\pi$.

7. Globales

Es wurde bereits bemerkt, daß im Zahlkörperfall, also für endlich abelsche Erweiterungen L/K von Zahlkörpern, die Idèleklassengruppe C_L von L die Rolle der im Lokalen erscheinenden Gruppe $L^\times$ übernimmt und daß eine globale Klassenkörpertheorie auf

$$H^1(L/K, C_L) = 1 \quad \text{und} \quad H^2(L/K, C_L) \text{ ist zyklisch von der Ordnung } [L:K] \textit{ plus} \ldots$$

aufbaut. Wir werden uns im folgenden mit der Bedeutung dieser beiden kohomologischen Eigenschaften von C_L beschäftigen.

Vorab eine kohomologische Vorbereitung. Es bezeichne J_L die Idèlegruppe von L und, für eine endliche Menge von Primstellen $\mathfrak{p}$ von K, die alle in L verzweigten $\mathfrak{p}$ enthalte, J_L^S die Gruppe $\prod_{\mathfrak{P}|\mathfrak{p}\notin S} U_{\mathfrak{P}} \times \prod_{\mathfrak{P}|\mathfrak{p}\in S} L_{\mathfrak{P}}^\times$. Es gilt dann

$$H^q(L/K, J_L) = \bigoplus_{\mathfrak{p}} H^q(L_{\mathfrak{P}_0}/K_{\mathfrak{p}}, L_{\mathfrak{P}_0}^\times)\,,\; H^q(L/K, J_L^S) = \prod_{\mathfrak{p}\in S} H^q(L_{\mathfrak{P}_0}/K_{\mathfrak{p}}, L_{\mathfrak{P}_0}^\times)\,,$$

wobei $\mathfrak{P}_0$ irgendeine über $\mathfrak{p}$ gelegene Stelle von L ist. Das folgt aus $\prod_{\mathfrak{P}|\mathfrak{p}} U_{\mathfrak{P}} = \mathrm{ind}_{G_{\mathfrak{P}_0}}^G U_{\mathfrak{P}_0}$ (und entsprechend für $L_{\mathfrak{P}}^\times$ statt $U_{\mathfrak{P}}$) und aus $H^q(G_{\mathfrak{P}}, U_{\mathfrak{P}}) = 1$, falls $\mathfrak{P}|\mathfrak{p}$ unverzweigt ist: denn dann ist die Zerlegungsgruppe $G_{\mathfrak{P}}$ zyklisch und alle Einheiten sind Normen, i.e., $H^0 = 1$, und $H^1(G_{\mathfrak{P}}, L_{\mathfrak{P}}^\times) = 1$ erzwingt $H^1(G_{\mathfrak{P}}, U_{\mathfrak{P}}) = 1$ wegen $U_{\mathfrak{P}} \rightarrowtail L_{\mathfrak{p}}^\times \twoheadrightarrow \mathbb{Z}$. Man vergewissere sich hier, daß die Kohomologie mit der Bildung direkter Summen und direkter Produkte verträglich ist, weil dies für den Hom-Funktor zutrifft.

SATZ 1. *1.* $H^1(L/K, C_L) = 1$ *für zyklische* L/K *impliziert die Injektivität von* $\mathrm{Br}(K) \to \bigoplus_{\mathfrak{p}} \mathrm{Br}(K_{\mathfrak{p}})$ *wobei* $\mathfrak{p}$ *die sämtlichen (also auch die archimedischen) Primstellen von* K *durchläuft. Die Brauerabbildung ist von* $A \mapsto K_{\mathfrak{p}} \otimes_K A$ *induziert; vgl. Aufgabe 3.*

2. Umgekehrt impliziert die Injektivität der Brauerabbildng $\mathrm{Br}(K) \to \bigoplus_{\mathfrak{p}} \mathrm{Br}(K_{\mathfrak{p}})$ *die Trivialität von* $H^1(L/K, C_L)$ *für jedes galoissche* L/K.

3. $H^1(L/K, C_L) = 1$ *für zyklisches* L/K *ist gleichbedeutend mit*

$$a \in K^\times \text{ ist Norm aus } L^\times \iff a \in K_{\mathfrak{p}}^\times \text{ ist Norm aus } L_{\mathfrak{p}}^\times .$$

Zur Notation: $a \in K^\times \subset K_{\mathfrak{p}}^\times$ *weist* $a \in K$ *als Element in* $K_{\mathfrak{p}}$ *aus;* $L_{\mathfrak{p}}$ *steht künftig für* $L_{\mathfrak{P}_0}$.

Wir beweisen zunächst 1. Wäre die Brauerabbildung nicht injektiv, so existierte ein $1 \neq A \in \mathrm{Br}(K)$ mit $A_{\mathfrak{p}} = 1$ für alle $\mathfrak{p}$. Sei $s \neq 1$ der Schurindex von A und $p|s$ ein Primteiler. Wähle einen über K galoisschen Zerfällungskörper L von A von kleinstmöglichem Grad und eine p-Sylowuntergruppe $P \leq G = G(L/K)$ mit Fixkörper F. Dann ist $F \otimes_K A \neq 1$ in $\mathrm{Br}(F)$ und wir dürfen folglich $K = F$, $G = P$ annehmen. Wähle in P ein zentrales Element der Ordnung p und bezeichne mit F dessen Fixkörper. Dieser ist galoissch über K und zerfällt also A nicht. Bilde $F \otimes_K A$. Für diese nicht zerfallende, lokal aber überall zerfallende Algebra ist L ein Zerfälungskörper vom Grad p. Also

$$\begin{array}{ccc} \mathrm{Br}(L/F) & \to & \bigoplus_{\mathfrak{p}} \mathrm{Br}(L_{\mathfrak{p}}/F_{\mathfrak{p}}) \\ \| & & \| \\ H^2(L/F, L^\times) & \to & \bigoplus_{\mathfrak{p}} H^2(L_{\mathfrak{p}}/F_{\mathfrak{p}}, L_{\mathfrak{p}}^\times) \end{array}$$

was zusammen mit $L^\times \rightarrowtail J_L \twoheadrightarrow C_L$ und $1 = H^1(L/F, C_L) \to H^2(L/F, L^\times) \to H^2(L/F, J_L)$ einen Widerspruch liefert.

Zu 2. und 3. Ist L/K zyklisch mit $\langle\sigma\rangle = G(L/K)$, so betrachte die Algebra $A = (L/K, \sigma, a) \in Br(L/K)$ für ein $a \in K^\times$, das lokal überall Norm ist. Also zerfällt A lokal überall und damit schlechthin, weshalb nun a eine globale Norm st. Und ist L/K irgendeine galoissche Erweiterung, so benütze $H^1(L/K, L_L) = 1$ und $H^1(L/K, C_L) \rightarrowtail \mathrm{Br}(L/K) \to \bigoplus_{\mathfrak{p}} \mathrm{Br}(L_{\mathfrak{p}}/K_{\mathfrak{p}})$.

Bemerkung: Die Aussage $[\,a \in K^\times$ ist Norm aus $L^\times \iff a \in K_{\mathfrak{p}}^\times$ ist Norm aus $L_{\mathfrak{p}}^\times\,]$ heißt *Hassescher Normensatz.* Sie ist i.allg. nur für zyklische L/K richtig. Sie ist zugleich der Hauptbestandteil des Beweises von $H^1(L/K, C_L) = 1$.

SATZ 2. (Brauer-Hasse-Noether) $\mathrm{Br}(K) \rightarrowtail \bigoplus_{\mathfrak{p}} \mathrm{Br}(K_{\mathfrak{p}}) \overset{\Sigma}{\twoheadrightarrow} \mathbb{Q}/\mathbb{Z}$ *ist exakt. Dabei ist* Σ *die Summenabbildung*

$$(\ldots, A_{\mathfrak{p}}, \ldots) \mapsto \sum \mathfrak{p}\mathrm{inv}_{\mathfrak{p}}(A_{\mathfrak{p}}) .$$

Dies zu beweisen erfordert einigen Aufwand und zu $H^1(L/K, C_L) = 1$ auch noch $H^2(L/K, C_L)$ *ist zylisch von der Ordnung* $[L : K]$; wir werden darüber hinaus zusätzliche Eigenschaften von H^2 kennenlernen.

DEFINITION. *Die globale Reziprozitätsabbildung* $J_K \to G(L/K)$ *sei*

$$\alpha \mapsto (\alpha, L/K) = \prod_{\mathfrak{p}} (\alpha_{\mathfrak{p}}, L_{\mathfrak{p}}/K_{\mathfrak{p}}) .$$

Hier ist α das Idèle $(\ldots, \alpha_{\mathfrak{p}}, \ldots)$ und $(\alpha_{\mathfrak{p}}, L_{\mathfrak{p}}/K_{\mathfrak{p}}) \in G(L_{\mathfrak{p}}/K_{\mathfrak{p}}) \leq G(L/K)$. Man beachte, daß im abelschen Fall die Zerlegungsgruppe $G(L_{\mathfrak{p}}/K_{\mathfrak{p}})$ von $\mathfrak{p}$ unabhängig von der gewählten Fortsetzung von $\mathfrak{p}$ auf L ist. Und weil $\alpha_{\mathfrak{p}} \in U_{\mathfrak{p}}$ f.i. [4] und $\mathfrak{p}$ f.i. unverzweigt in L/K ist, ist das Produkt ein endliches Produkt.

Bemerkungen :

1. Ist $\mathfrak{p}$ reell und $L_{\mathfrak{p}} = \mathbb{C}$, so ist $(\alpha_{\mathfrak{p}}, L_{\mathfrak{p}}/K_{\mathfrak{p}})(\sqrt{-1}) = \pm\sqrt{-1}$ je nachdem, ob $\alpha_{\mathfrak{p}} > 0$ oder < 0 ist.

2. Obige Definition liefert für die globale Reziprozitätsabbildung zu denen für die lokalen Reziprozitätsabbildungen analoge kommutative Diagramme (S.7).

3. $N_{L/K}J_L$ liegt im Kern der Reziprozitätsabbildung.

4. Die Reziprozitätsabbildung ist surjektiv und hat offenen Kern.
Denn ist $G(L/F) \leq G(L/K)$ das Bild, so gilt $(\alpha, F/K) = 1$ für alle $\alpha \in J_K$ und also $\alpha_{\mathfrak{p}} \in N_{F_{\mathfrak{p}}/K_{\mathfrak{p}}} F_{\mathfrak{p}}^{\times}$, weshalb alle lokalen Normrestsymbole trivial sind, mithin $F_{\mathfrak{p}} = K_{\mathfrak{p}}$ $(\forall\, \mathfrak{p})$. Das erzwingt $F = K$: Ohne Einschränkung sei jetzt F/K zyklisch. Wir benützen im folgenden nur, daß $S \overset{\text{def}}{=} \{\mathfrak{p} : F_{\mathfrak{p}} = K_{\mathfrak{p}}\}$ endlich (statt leer) ist. Finde nun Hauptidèle $a \in K^{\times}$, so daß $\alpha_{\mathfrak{p}} a^{-1}$ lokal überall Norm ist (nämlich über eine Approximation der $\alpha_{\mathfrak{p}}$ für $\mathfrak{p} \in S$ unter Ausnützung der Offenheit der lokalen Normgruppen). Dann ist $\alpha_{\mathfrak{p}} a^{-1} \in N_{F/K} J_F$, oder $\alpha \in (N_{F/K} J_F) K^{\times}$, i.e., $C_K = N_{F/K} C_F$, was $F = K$ wegen $H^2 = H^0$ bedeutet, denn $|H^2(F/K, C_F)| = [F : K]$.
Der Kern der Reziprozitätsabbildung ist offen, weil $\prod_{\mathfrak{p} \in S} N_{L_{\mathfrak{p}}/K_{\mathfrak{p}}}(L_{\mathfrak{p}}^{\times}) \times \prod_{\mathfrak{p} \notin S} U_{\mathfrak{p}}$ für jede endliche Menge S, die alle verzweigten Stellen enthält, offen in J_K ist und die α hierheraus auf 1 bei der Reziprozitätsabbildung gehen.

5. Für $\chi \in \widehat{G(L/K)}$ gilt $\chi((\alpha, L/K)) = \sum_{\mathfrak{p}} \mathrm{inv}_{\mathfrak{p}}(L_{\chi_{\mathfrak{p}}}, \sigma_{\chi_{\mathfrak{p}}}, \alpha_{\mathfrak{p}})$. Dabei ist $\chi_{\mathfrak{p}} = \mathrm{res}_{G}^{G_{\mathfrak{p}}} \chi$ und $\chi_{\mathfrak{p}}(\sigma_{\chi_{\mathfrak{p}}}) = 1/[L_{\mathfrak{p}} : K_{\mathfrak{p}}] \mod \mathbb{Z}$. Ist $\alpha = a$ ein Hauptidèle, so wird daraus $\chi((a, L/K)) = \sum_{\mathfrak{p}} \mathrm{inv}_{\mathfrak{p}}(L_{\chi}, \sigma_{\chi}, a)$ (mit offenkundiger Bezeichnung).

Satz 3. $a \in K^{\times} \implies (a, L/K) = 1$, *die Reziprozitätsabbildung faktorisiert also über* C_K.

Es ist dazu $\sum_{\mathfrak{p}} \mathrm{inv}_{\mathfrak{p}}(L_{\chi}, \sigma_{\chi}, a) = 0$ für alle χ zu zeigen und das ist Teil der Exaktheitsbehauptung in Satz 2.

Wir beweisen jetzt diesen Teil von Satz 2, starten dazu mit einem $A \in \mathrm{Br}(K)$ und benutzen, daß es einen über K zyklischen Zerfällungskörper L von A mit $L \subset K(\zeta)$ für eine geeignete Einheitswurzel ζ gibt (dies wird weiter unten begründet). Wir können somit $A = (L/K, \sigma, a)$ mit $\langle\sigma\rangle = G(L/K)$ und einem $a \in K$ schreiben und wollen $\sum_{\mathfrak{p}} \mathrm{inv}_{\mathfrak{p}}(L_{\mathfrak{p}}/K_{\mathfrak{p}}, \sigma_{\mathfrak{p}}, a) = 0$,i.e., $(a, L/K) = 1$ (aber jetzt mit dem neuen L und dem neuen a) zeigen. Die fürs Normrestsymbol gültigen kommutativen Diagramme erlauben die folgenden Reduktionen

$$\begin{aligned}&(a, K(\zeta)/K)) = 1\,,\ (N_{K/\mathbb{Q}}(a), K(\zeta)/\mathbb{Q})) = 1\,,\ (a, \mathbb{Q}(\zeta)/\mathbb{Q})) = 1\ (\forall\, a \in \mathbb{Q}^{\times})\\ &(a, \mathbb{Q}(\zeta_{l^m}/\mathbb{Q})) = 1\ (\forall\,\text{Primzahlen } l)\,;\end{aligned}$$

und schließlich, dank der Multiplikativität des Normrestsymbols, bleibt nur $(\pm p, \mathbb{Q}(\zeta_{l^m}/\mathbb{Q})) = 1$ für alle Primzahlen p zu zeigen. Dies rechnet man mit dem expliziten Normrestsymbol für $\mathbb{Q}_r(\zeta_{l^m})/\mathbb{Q}_r$ nach ($r \leq \infty$ ist hier eine beliebige Primzahl).

[4] fast immer

Die behauptete Gleichheit $\mathrm{Br}(K) = \bigcup_L \mathrm{Br}(L/K)$, wobei L die zyklischen Erweiterungen von K, enthalten in Kreiskörpern über K, durchläuft, ist sofort auf den Fall $K = \mathbb{Q}$ zurückgeführt und erfordert hier (nach Kronecker-Weber) zu $A \in \mathrm{Br}(\mathbb{Q})$ die Konstruktion eines über $\mathbb{Q}$ zyklischen Zerfällungskörper L. Dazu sei s das Produkt der lokalen Schurindizes von A und $\{p\}$ die Menge der Primteiler von s. Für jedes ungerade dieser p betrachte den Teilkörper vom Index $p-1$ in $\mathbb{Q}(\zeta_{p^n})$ für hinreichend großes n; der ist zyklisch. Für $p = 2$ (ob 2 oben vorkommt oder nicht) nimm den Teilkörper $F \subset \mathbb{Q}(\zeta_{2^{n+2}})$ vom Index 2, der weder reell ist noch $\mathbb{Q}(\zeta_4)$ enthält; $F/\mathbb{Q}$ ist dann zyklisch und nicht reell. Das Kompositum über all diese zyklischen Erweiterungen von $\mathbb{Q}$ ist dann selbst zyklisch über $\mathbb{Q}$, nicht reell und hat, sogar nach Komplettierung bei den $p \mid s$, einen durch s teilbaren Grad. Damit zerfällt A über diesem Körper.

Satz 4. *$|H^2(L/K, C_L)| = [L:K]$ für zyklische L/K impliziert, daß stets $N_{L/K}C_L$ der Kern des Normrestsymbols $(-, L/K)$ ist.*

Denn das stimmt nach Voraussetzung und wegen Satz 3 sowie der Surjektivität des Normrestsymbols, solange L/K zyklisch ist. Für den allgemeinen Fall sei, der Einfachheit wegen, L/K als abelsch angenommen und F/K sei eine zyklische (nichttriviale) Teilerweiterung. Dann folgt $[(a, L/K) = 1 \implies (a, F/K) = 1 \implies a = N_{F/K}b]$ und weiter $[(b, L/F) = (N_{F/K}(b), L/K) = 1]$, womit $b \in C_F$ Norm aus C_L (nach Induktion) ist, damit auch a.

Zufolge von $\mathrm{Br}(K) = \bigcup_L \mathrm{Br}(L/K)$ (siehe oben) folgt nun auch ohne weiteres der zweite Teil der Exaktheitsaussage im Satz 2.

Satz 5. (Existenzsatz) *Die Normengruppen in C_K sind gerade die abgeschlossenen Untergruppen von endlichem Index.*

Daß C_L abgeschlossen ist, resultiert aus der früher beobachteten Zerlegung $C_L = C_L^0 \times \Gamma$, $\Gamma \simeq \mathbb{R}_{>0}$, mit kompaktem C_L^0. Der endliche Index ist eine Konsequenz von $C_K/N_{L/K}(C_L) \simeq G(L/K)^{\mathrm{ab}}$. Für die Umkehrung braucht man eine etwas langwierige Indexberechnung, um $C_K^n \overline{U}_K^S$ als eine Normgruppe zu erkennen; hier steht $\overline{U}_K^S$ für das Bild in C_K von $\prod_{\mathfrak{p}\notin S} U_\mathfrak{p} \times \prod_{\mathfrak{p}\in S} 1$ für eine hinreichend große (endliche) Menge S von Primstellen. Tatsächlich läßt sich die Umkehrung auf den Kummerschen Fall $\zeta_n \in K$ zurückführen (weil Obergruppen von Normgruppen selbst Normgruppen sind), und man zeigt $C_K^n \overline{U}_K^S = N_{L/K}C_L$ mit $L = K(\sqrt[n]{E_K^S})$, wobei E_K^S die Gruppe der S-Einheiten von K bezeichnet. Der Nachweis davon ist eng verknüpft mit dem von $H^1(L/K, C_L) = 1$ und $|H^2(L/K, C_L)| = [L:K]$ für zyklische L/K, siehe weiter unten.

Bemerkungen:

1. $C_K \twoheadrightarrow cl_K$ hat den Kern $J_\infty K^\times/K^\times$; dies ist also eine abgeschlossene Untergruppe von endlichem Index und gehört zu einer abelschen Erweiterung H/K. Wegen $(\alpha, H/K) = 1$ für $\alpha \in J_\infty$, deshalb auch $((1, \ldots, 1, \alpha_\mathfrak{p}, 1, \ldots, 1), H/K) = 1$ für $\alpha_\mathfrak{p} \in U_\mathfrak{p}$, ist jede Einheit in $K_\mathfrak{p}$ Norm aus $H_\mathfrak{p}$ und folglich $H_\mathfrak{p}/K_\mathfrak{p}$ unverzweigt, i.e., H/K ist überall (im Endlichen) unverzweigt. Damit ist H die maximal abelsche unverzweigte Erweiterung von K, der sogenannte *Hilbertkörper* über K. Es gilt $G(H/K) \simeq cl_K$.

2. Die Sequenz

$$\begin{array}{ccccccc} H^2(L/K,L^\times) & \rightarrowtail & H^2(L/K,J_L) & \to & H^2(L/K,C_L) & \to & H^3(L/K,L^\times) \\ \| & & \| & & \| \, 1 & & \| \, 2 \\ \mathrm{Br}(L/K) & \rightarrowtail & \sum_{\mathfrak{p}} \mathrm{Br}(L_{\mathfrak{p}}/K_{\mathfrak{p}}) & \xrightarrow{*} & \mathbb{Z}/[L:K] & \to & 0 \end{array}$$

(mit exakten Zeilen) zeigt die Gleichheit $\|$ 1, falls die Abbildung $*$ surjektiv ist (s.u.), denn $\|$ 2 folgt aus der vom Cupprodukt mit der lokalen Fundamentalklasse $u_{\mathfrak{p}}$ gelieferten Isomorphie $H^1(L_{\mathfrak{p}}/K_{\mathfrak{p}},\mathbb{Z}) \simeq H^3(L_{\mathfrak{p}}/K_{\mathfrak{p}},L_{\mathfrak{p}}^\times)$. Damit ist nun auch die Zyklizität von $H^2(L/K,C_L)$ gezeigt und darüber hinaus gibt $\|$ 1 ein kanonisches Erzeugendes, die *global Fundamentalklasse*, in $H^2(L/K,C_L)$, die auf offenkundige Weise mit den lokalen Fundamentalklassen zusammenhängt.
Die Abbildung $*$ ist jedenfalls surjektiv, wenn L/K zyklisch ist. Denn das Kompositum G_1 der $G_{\mathfrak{p}}$ ist $= G(L/K)$ (weil alle $\mathfrak{p}$ im Fixlörper von G_1 voll zerlegt sind) und deshalb $\mathrm{kgV}_{\mathfrak{p}}\{|G_{\mathfrak{p}}|\} = |G(L/K)|$. Ist L/K nicht länger zyklisch, so wähle zunächst eine über K zyklische Erweiterung F vom Grad $[L:K]$ (etwa mit Hilfe von Kreiskörpern), nenne $M = LF$ das Kompositum aus L und F und betrachte das kanonische Diagramm

$$\begin{array}{ccccc} & & & & H^2(M/L,M^\times) = \mathrm{Br}(M/L) \\ & & & & \downarrow \\ H^2(F/K,J_F) & \overset{\text{infl}}{\rightarrowtail} & H^2(M/K,J_M) & \overset{\text{res}}{\dashrightarrow} & H^2(M/L,J_M) = \bigoplus_{\mathfrak{P}} \mathrm{Br}(M_{\mathfrak{P}}/L_{\mathfrak{P}}) \\ \downarrow & & \downarrow & & \downarrow \\ H^2(F/K,C_F) & \overset{\text{infl}}{\rightarrowtail} & H^2(M/K,C_M) & \overset{\text{res}}{\dashrightarrow} & H^2(M/L,C_M) = \langle \frac{1}{[M:L]} \rangle \,. \end{array}$$

Es zeigt, daß das Bild von $a \in H^2(F/K,J_F)$ in $H^2(M/L,J_M)$ unter der oberen Restriktion eine Nullsumme von lokalen Invarianten hat, denn liegen die $\mathfrak{P}$ von L über dem $\mathfrak{p}$ von K, so entspricht der 'res' lokal die Multiplikation mit $[L_{\mathfrak{P}}:K_{\mathfrak{p}}]$, also insgesamt die Multiplikation mit $[L:K] = \sum_{\mathfrak{P}|\mathfrak{p}}[L_{\mathfrak{P}}:K_{\mathfrak{p}}]$. Es resultiert $H^2(F/K,C_F) \le H^2(L/K,C_L) =$ Kern der unteren Restriktion. Aber $|H^2(F/K,C_F)| = [F:K] = [L:K]$ und offensichtlich ist $|H^2(L/K,C_L)| \le [L:K]$ auf Grund des anfänglichen Diagramms dieser Bemerkung.

3. Das Normrestsymbol kann über den kanonischen Homomorphismus $J_K \to I_K$ (I_K ist die Gruppe der Ideale von K) statt in Idèle-Sprechweise in eine Ideal-Sprechweise übersetzt werden. Das soll unter Zuhilfenahme gängiger Lehrbücher zur Klassenkörpertheorie hier nur als eine Übungsaufgabe erwähnt sein (siehe etwa Neukirchs Klassenkörpertheorie, S. 292-301). Man erinnere sich in dem Zusammenhang auch an den letzten Absatz von §4 und vergleiche die Bemerkung a) am Schluß dieses Paragraphen.

Wir beweisen nun $H^1(L/K,C_L) = 1$ und $|H^2(L/K,C_L)| = [L:K]$ für zyklische L/K (und beenden damit zugleich den Beweis des Existenzsatzes). Zuerst eine Vorbemerkung. Ist S eine endliche Primstellenmenge von K (mit $S \supset S_\infty$), so kann S zu einer endlichen Primstellenmenge S_1 vergrößert werden, die $J_K^{S_1}K^\times = J_K$ erfüllt. Dazu betrachte die natürliche Abbildung $J_K \to cl_K$, $\alpha \mapsto \mathfrak{a} = \prod_{\mathfrak{p}<\infty} \mathfrak{p}^{w_{\mathfrak{p}}(\alpha)}$ und füge dem S Primideale hinzu, die die endliche Idealklassengruppe cl_K erzeugen.

Weil L/K zyklisch ist, können wir mit den Herbrandquotienten $h(C_L), h(J_L), \ldots$ arbeiten und beobachten

1. enthält S alle in L/K verzweigten Stellen, so ist $h(J_L^S) = \prod_{\mathfrak{p}\in S}[L_{\mathfrak{p}}:K_{\mathfrak{p}}]$,

2. $h(E_L^S) = \frac{\prod_{\mathfrak{p}\in S}[L_\mathfrak{p}:K_\mathfrak{p}]}{[L:K]}$,

3. $h(C_L) = [L:K]$.

Dabei resultiert 3. aus 2., wenn man nur S groß genug wählt und dann die exakte Sequenz $E_L^S \rightarrowtail J_L^S \twoheadrightarrow C_L$ verwendet; 1. ist i.w. Hilberts Satz 90. Die Gleichheit 2. ist eine Kombination aus Dirichlets Einheitensatz und dem Lemma

> *G wirke auf dem n-dimensionalen reellen Vektorraum durch Permutationen von Basiselementen v_i. Dann liegen in jedem G-stabilen vollen $\mathbb{Z}$-Gitter auf V Basiselemente w_i, die in gleicher Weise von G wie die v_i permutiert werden.*

Folgerung.

$$H^1(L/K, C_L) = 1 \iff |H^2(L/K, C_L)| = [L:K] \iff [C_K : N_{L/K}C_L] \leq [L:K]$$

Im folgenden wird nun $[C_K : N_{L/K}C_L] \leq [L:K]$ für zyklische L/K bewiesen (man vergleiche dazu etwa Neukirchs Buch *Algebraische Zahlentheorie*, Seiten 397-400).

Lemma 1. *Es seien n eine Primzahlpotenz, $\zeta_n \in K$, L/K eine abelsche Erweiterung mit Gruppe $\simeq (\mathbb{Z}/n)^r$ und S eine endliche Menge von Primstellen in K mit $S \supset S_\infty \cup S_{\mathrm{ram}_{L/K}} \cup \{\mathfrak{p}|n\}$ und $J_K^S K^\times = J_K$. Dann gilt $s \overset{\mathrm{def}}{=} |S| \geq r$, $\exists T = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_{s-r}\} \subset \complement S$: $L = K(\sqrt[n]{\Delta})$ mit $\Delta = \ker(E_K^S \to \prod_{\mathfrak{p}\in T} K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^n)$.*

Es seien nur die wichtigsten Ingredienzen des Beweises genannt.

1. $L \overset{!}{=} K(\sqrt[n]{\Delta})$ mit $\Delta = (L^\times)^n \cap E_K^S$:

   Dazu schreibe zuerst mittels Kummertheorie $L = K(\sqrt[n]{D})$ mit $D = (L^\times)^n \cap K^\times$. Für $d \in D$ und $\mathfrak{p} \notin S$ ist dann $K_\mathfrak{p}(\sqrt[n]{d})/K_\mathfrak{p}$ unverzweigt und deshalb $d = u_\mathfrak{p} y_\mathfrak{p}^n$ mit einer Einheit $u_\mathfrak{p}$ und einer Potenz $y_\mathfrak{p}$ eines Primelementes von $K_\mathfrak{p}$ darstellbar. Setze $\alpha = (\ldots, y_\mathfrak{p}, \ldots) \in J_K$, wobei $y_\mathfrak{p} = 1$ wenn $\mathfrak{p} \in S$. Wegen $J_K^S K^\times = J_K$ ist $\alpha = \beta x$ mit $\beta \in J_K^S$ und $x \in K^\times$. Es folgt $dx^{-n} \in J_K^S \cap K^\times = E_K^S$ oder $D = \Delta \cdot (K^\times)^n$.

2. Setze $M = K(\sqrt[n]{E_K^S}) \supset L = K(\sqrt[n]{(L^\times)^n \cap E_K^S})$. Kummertheorie liefert $G(M/K) \simeq (\mathbb{Z}/n)^s$, woraus $s \geq r$ und $G(M/L) \simeq (\mathbb{Z}/n)^{s-r} = \langle \sigma_1, \ldots, \sigma_{s-r} \rangle_{\mathbb{Z}/n}$ resultiert. Der Fixkörper von σ_i sei M_i. Wähle nun $\mathfrak{P}_i$ in M_i so: sie sind unzerlegt in M und geben verschiedene $\mathfrak{p}_i$ auf K, die alle nicht in S liegen. (Das ist möglich, weil M/M_i zyklisch von Primzahlpotenzgrad ist: Gäbe es nur endlich viele in M unzerlegte $\mathfrak{P}$'s, so wären alle anderen in der Teilerweiterung N/M_i vom Primzahlgrad voll zerlegt, was wegen $[C_{M_i} : N_{N/M_i}(C_N)] \geq [N : M_i]$ Unsinn ist [5].) Setze nun $T = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_{s-r}\}$.

3. $\Delta = (L^\times)^n \cap E_K^S \overset{!}{=} \ker(E_K^S \to \prod_T K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^n)$:

   Über $\mathfrak{P}_i$ liegt genau ein $\mathfrak{P}_i'$ von M und M_i ist der Zerlegungskörper von $\mathfrak{P}_i'|\mathfrak{p}_i$, da $\mathfrak{p}_i$ unverzweigt in M ist; also $(M_i)_{\mathfrak{P}_i} = K_{\mathfrak{p}_i}$. Damit ist L/K die maximale Teilerweiterung von M/K, in der alle $\mathfrak{p}_i$ voll zerlegt sind: $L = \bigcap_i M_i$. Nun benutze

$$e \in \Delta \iff K(\sqrt[n]{e}) \subset L \iff K_{\mathfrak{p}_i}(\sqrt[n]{e}) = K_{\mathfrak{p}_i} \iff e \in (K_{\mathfrak{p}_i}^\times)^n .$$

[5] ohne die Zyklizität von M/M_i ist das falsch, denn $G = G_\mathfrak{p}$ macht G zyklisch, weil die $\mathfrak{p}$ f.i. unverzweigt sind

LEMMA 2. *Mit den Bezeichnungen aus dem vorhergehenden Lemma und mit*

$$J_K^{S,T} = \prod_{\mathfrak{p}\in S}(K_\mathfrak{p}^\times)^n \times \prod_{\mathfrak{p}\in T} K_\mathfrak{p}^\times \times \prod_{\mathfrak{p}\notin S\cup T} U_\mathfrak{p}$$

gilt $J_K^{S,T} \cap K^\times = (E_K^{S\cup T})^n$.

Es ist nur " $\subset$" zu zeigen. Dazu betachte die zyklische Erweiterung $N = K(\sqrt[n]{y})/K$ für ein $y \in J_K^{S,T} \cap K^\times$. Wegen $[C_K : N_{N/K}C_N] \geq [N : K]$ reicht es, $N_{N/K}C_N = C_K$ oder $N = K$, also $y \in (K^\times)^n \cap J_K^{S,T} \cap K^\times$ nachzuweisen.
Starte mit $\alpha \in J_K^S$. Nenne Δ wieder den Kern von $E_K^S \to \prod_T U_\mathfrak{p}/U_\mathfrak{p}^n$,. Zufolge von

$$|E_K^S/\Delta| = \frac{[E_K^S : (E_K^S)^n]}{[\Delta : (E_K^S)^n]} = \frac{n^s}{|G(L:K)|} = n^{s-r} = \prod_{\mathfrak{p}\in T} |U_\mathfrak{p}/U_\mathfrak{p}^n| \,,$$

(man erinnere sich an $[U_\mathfrak{p} : U_\mathfrak{p}^n] = [U_\mathfrak{p}^{(1)} : U_\mathfrak{p}^{(2)}]^{w_\mathfrak{p}(n)} \cdot |\mu_n|$) ist $E_K^S \to \prod_T U_\mathfrak{p}/U_\mathfrak{p}^n$ surjektiv und daher $\alpha_\mathfrak{p} = u_\mathfrak{p} x$ für $\mathfrak{p} \in T$, also $\alpha = \beta \cdot x$. Es reicht nun, $\beta_\mathfrak{p} \in N_{N_\mathfrak{p}/K_\mathfrak{p}} N_\mathfrak{p}^\times$ für alle $\mathfrak{p}$ einzusehen. Für $\mathfrak{p} \in S$ ist das keine Bedingung; für $\mathfrak{p} \in T$ ist $\beta_\mathfrak{p} = u_\mathfrak{p}^n$, also Norm aus $N_\mathfrak{p}$, und für die anderen (allesamt unverzweigten) $\mathfrak{p}$ ist $\beta_\mathfrak{p}$ eine Einheit.

LEMMA 3. *Für das Bild* $C_K^{S,T}$ *von* $J_K^{S,T}$ *gilt*

$$N_{L/K}C_L \supset C_K^{S,T} \quad \& \quad [C_K : C_K^{S,T}] = [L : K] \,.$$

Der Beweis zerfällt in zwei Teile.

1. Berechne die individuellen Ordnungen der Einträge in der exakten Sequenz

$$J_K^{S\cup T} \cap K^\times / J_K^{S,T} \cap K^\times \rightarrowtail J_K^{S\cup T}/J_K^{S,T} \twoheadrightarrow J_K^{S\cup T}K^\times/J_K^{S,T}K^\times$$

   unter Ausnützung der Formel $[K_\mathfrak{p}^\times : (K_\mathfrak{p}^\times)^n] = n^2 p^{f_{\mathfrak{p}|p} w_\mathfrak{p}(n)}$ für endliche $\mathfrak{p}$, also $\prod_{\mathfrak{p}\in S}[K_\mathfrak{p} : (K_\mathfrak{p}^\times)^n] = n^{2s}$ aufgrund der Produktformel, nämlich weil $w_\mathfrak{p}(n) = 0$ für $\mathfrak{p} \notin S$ und $[\mathbb{C}^\times : (\mathbb{C}^\times)^n] = 1$ (denn $\zeta_n \in K$). Es folgt sofort die zweite Behauptung.

2. $C_K^{S,T} \subset N_{L/K}C_L$:

   Es muß $\alpha \in N_{L/K}J_L$ für $\alpha \in J_K^{S,T}$ gezeigt werden. Dies tu wieder für die drei Fälle $\mathfrak{p} \in S, \mathfrak{p} \in T, \mathfrak{p} \notin S \cup T$ einzeln und verwende $\alpha_\mathfrak{p} = \beta_\mathfrak{p}^n \in N(K_\mathfrak{p}(\sqrt[n]{K_\mathfrak{p}^\times})), L_\mathfrak{p} = K_\mathfrak{p}, \alpha_\mathfrak{p} \in U_\mathfrak{p}$ der Reihe nach.

FOLGERUNG. *Ist* L/K *zyklisch von Primzahlpotenzordnung* n *und* $\zeta_n \in K$, *so gilt* $[C_K : N_{L/K}C_L] = [L : K]$.

Die Zyklizität wird dabei für $[L : K] \leq [C_K : N_{L/K}C_L]$ benötigt. Mittels Induktion folgt dann $[C_K : N_{L/K}C_L] = [L : K]$ aus der Inflations-Restriktions-Sequenz ($H^2 = H^0$), solange L/K zyklisch von beliebigem Grad n und $\zeta_n \in K$ ist. Ohne die Einheitswurzelvoraussetzung liefert dasselbe Argument die Abschätzung $[C_K : N_{L/K}C_L] \leq [L : K]$ für abelsches L/K, sofern der Induktionsanfang $[L : K] = p$ gesichert ist. Dazu betrachte die aus $G(L/K) \simeq G(L(\zeta_p)/K(\zeta_p))$ resultierende Abbildung $C_K/N_{L/K}C_L \to C_{K(\zeta_p)}/N_{L(\zeta_p)/K(\zeta_p)}C_{L(\zeta_p)} = \mathbb{Z}/p$.

Die ist als Abbildung zwischen p-Gruppen injektiv, weil $p \nmid d \overset{\text{def}}{=} [K(\zeta_p) : K]$ und $x^d = N_{L(\zeta_p)/K(\zeta_p)}(x)$ für $x \in C_K$ gilt.

Für den Übergang von zyklischen zu abelschen Erweiterungen vergleiche endlich die Bemerkung 2. weiter oben.

Der Existenzsatz ist schließlich eine direkte Konsequenz aus $N_{L/K}C_L = J_K^{S,\emptyset}K^\times/K^\times$ mit $L = K(\sqrt[n]{E_K^S}\,)$.

Bemerkungen:

a) Wir erinnern an den Begriff eines Moduls $\mathfrak{m}$ (siehe Ende von §4) und definieren

$$J_K^{\mathfrak{m}} = \{\alpha \in J_K : \alpha_{\mathfrak{p}} \in U_{\mathfrak{p}}^{(n_{\mathfrak{p}})}\}\,,\; C_K^{\mathfrak{m}} = J_K^{\mathfrak{m}}K^\times/K^\times \leq C_K\,.$$

Für $\mathfrak{m} = 1$, also $n_{\mathfrak{p}} = 0$ für alle $\mathfrak{p}$ (archimedisch und nichtarchimedisch), ist damit $J_K^1 = J_\infty$ und $C_K/C_K^1 \simeq cl_K$. Die $C_K^{\mathfrak{m}}$ heißen *Kongruenzuntergruppen* und sind abgeschlossene Untergruppen von endlichem Index in C_K. Mehr noch: Jede Normgruppe ist Obergruppe einer geeigneten Kongruenzuntergruppe $C_K^{\mathfrak{m}}$. Die zu $C_K^{\mathfrak{m}}$ gehörige abelsche Erweiterung L von K, i.e., $N_{l/K}C_L = C_K^{\mathfrak{m}}$, heißt der *Strahlklassenkörper modulo* $\mathfrak{m}$.

Bezeichnet $I_K^{\mathfrak{m}}$ die Gruppe aller zu $\mathfrak{m}$ teilerfremden Ideale $\mathfrak{a}$ von K (also $\mathfrak{p} \nmid \mathfrak{a}$ für $n_{\mathfrak{p}} > 0$) und $H_0^{\mathfrak{m}}$ die Gruppe aller Hauptideale $a\mathfrak{o}_K$ mit $a \in K^\times$ und $a \in U_{\mathfrak{p}}^{(n_{\mathfrak{p}})}$ für $n_{\mathfrak{p}} > 0$ (der sogenannte *Strahl modulo* $\mathfrak{m}$), so heißt $I_K^{\mathfrak{m}}/H_0^{\mathfrak{m}}$ die *Strahlklassengruppe modulo* $\mathfrak{m}$; für $\mathfrak{m} = 1$ ist das die gewöhnliche Idealklassengruppe cl_K von K.

Die abelsche Erweiterung L/K erfülle $C_K^{\mathfrak{m}} \subset N_{L/K}C_L$. Dann sind in L nur $\mathfrak{p}$ mit $n_{\mathfrak{p}} > 0$ verzweigt und wir können eine multiplikative Abbildung

$$\left(\frac{L/K}{-}\right) : I_K^{\mathfrak{m}} \to G(L/K) \quad \text{durch} \quad \left(\frac{L/K}{\mathfrak{p}}\right) = \varphi_{\mathfrak{p}}$$

definieren, wobei $\mathfrak{p}$ den Frobeniusautomorphismus von $\mathfrak{p}$ bezeichnet. Weil die kanonische Abbildung $J_K \to I_K$ das kommutative Diagramm $\begin{array}{ccc} C_K/C_K^{\mathfrak{m}} & \overset{\simeq}{\to} & I_K^{\mathfrak{m}}/H_0^{\mathfrak{m}} \\ \cup & & \cup \\ N_{L/K}C_L/C_K^{\mathfrak{m}} & \overset{\simeq}{\to} & H^{\mathfrak{m}}/H_0^{\mathfrak{m}} \end{array}$ mit horizontalen Isomorphismen und $H^{\mathfrak{m}} = N_{L/K}I_L^{\mathfrak{m}} \cdot H_0^{\mathfrak{m}}$ induziert (approximiere bei $\mathfrak{m}$ durch Hauptidèle) ist die obige Abbildung (*das Artin-Symbol*) surjektiv mit Kern $H^{\mathfrak{m}}/H_0^{\mathfrak{m}}$.

b) Der *Führer* $\mathfrak{f}_{L/K}$ der abelschen Erweiterung L/K ist der größte gemeinsame Teiler aller Moduln $\mathfrak{m}$ mit $C_K^{\mathfrak{m}} \subset N_{L/K}C_L$. In L sind genau die $\mathfrak{p} \mid \mathfrak{f}_{L/K}$ verzweigt (wenn man Verzweigtheit bei einem archimedischen $\mathfrak{p}$ durch $L_{\mathfrak{p}} \neq K_{\mathfrak{p}}$ erklärt).

c) Das *Zerlegungsgesetz* für unverzweigte $\mathfrak{p}$ in einer abelschen Erweiterung L/K liest sich so: $f_{\mathfrak{p}} =$ *Ordnung von* $\varphi_{\mathfrak{p}} =$ *Ordnung von* $(\ldots, 1, \pi, 1, \ldots) \mod N_{LK/K}C_L$, wobei π ein Primelement in $\mathfrak{p}$ ist und an der $\mathfrak{p}$-Komponente der Idèleklasse des oben ausgeschriebenen Idèles steht.

d) Der *Hauptidealsatz* besagt, daß jedes Ideal von K Hauptideal im Hilbertschen Klassenkörper H von K wird und ist eine Folgerung aus dem kommutativen Diagramm $\begin{array}{ccc} K & \subset & H \\ \downarrow & & \downarrow \\ G(H_1/K)^{\mathrm{ab}} & \overset{\mathrm{ver}}{\to} & G(H_1/H) \end{array}$ in dem H_1 der Hilbertsche Klassenkörper von H ist und die vertikalen Pfeile die jeweiligen Normrestsymbole bezeichnen. Die Verlagerung übersetzt sich in die natürliche Abbildung $cl_K \to cl_H$, und die ist trivial zufolge des gruppentheoretischen Satzes $G \overset{\mathrm{ver}}{\to} [G, G]$ *ist trivial, falls* $[G, G]$ *abelsch ist.*

8. Analytisches: L-Reihen, Satz von Čebotarev

K ist weiterhin ein algebraischer Zahlkörper. Für eine Menge P von (endlichen) Primstellen $\mathfrak{p}$ von K werde die *Dichte* $\delta(P)$ durch

$$\delta(P) = \lim_{s\to 1+} \frac{\sum_{\mathfrak{p}\in P}(N\mathfrak{p})^{-s}}{\sum_{\text{alle }\mathfrak{p}}(N\mathfrak{p})^{-s}}$$

definiert (falls der Grenzwert überhaupt existiert). Wegen $(*)$ $\lim_{s\to 1+}(\sum_{\text{alle }\mathfrak{p}}(N\mathfrak{p})^{-s}) = \infty$, ist $\delta(P) \in [0,1]$ (sofern existent) und $\delta(P) = 0$ für endliche P. Besitzen P_1 und P_2 Dichten und sind disjunkt, so gilt $\delta(P_1 \cup P_2) = \delta(P_1) + \delta(P_2)$.

Zu $(*)$: $\zeta_K(s) = \sum_{\mathfrak{a}\text{ ganz}} 1/(N\mathfrak{a})^s = \prod_{\mathfrak{p}}(1 - \frac{1}{(N\mathfrak{p})^s})^{-1}$ hat einen einfachen Pol bei 1; wende nun den Logarithmus an. Bezeichnet noch ρ_K das Residuum bei $s = 1$ (*analytische Klassenzahlformel*), so erhalten wir [6] $\log(s-1) + \sum_{\mathfrak{p}}(N\mathfrak{p})^{-s} \to c \le \log\rho_k$ und daraus [7] $\delta(P) = \lim_{s\to 1+} \frac{\sum_P (N\mathfrak{p})^{-s}}{-\log(s-1)}$.

Theorem (Satz von Čebotarev). *L/K sei eine endliche galoissche Erweiterung mit Gruppe G und C eine Konjugiertenklasse in G. Dann hat die Menge $P = \{\mathfrak{p} : \varphi_{\mathfrak{p}} \in C\}$ die Dichte $|C|/[L:K]$.*

Bemerkungen:

1. Weil endliche Mengen von der Dichte 0 sind, können wir uns bei obigem P auf die in P liegenden in L unverzweigten $\mathfrak{p}$ beschränken. Mit $\varphi_{\mathfrak{p}}$ ist dann (salopp) der Frobeniusautomorphismus von $\mathfrak{P}|\mathfrak{p}$ gemeint, wobei $\mathfrak{P} \subset L$ über $\mathfrak{p}$ liegt: der hängt zwar von der Wahl von $\mathfrak{P}$ ab, allerdings nur bis auf Konjugation in G.
2. Ist L/K abelsch, so ist $\varphi_{\mathfrak{p}}$ das Bild der Idèleklasse $\overline{(\dots,1,\pi,1,\dots)}$) mit einem Primelement $\pi \in \mathfrak{p}$ an der Stelle $\mathfrak{p}$. Oder, in der Sprache der Artinschen Reziprozitätsabbildung, $\varphi_{\mathfrak{p}} = \left(\frac{L/K}{\mathfrak{p}}\right)$.

Folgerung 1. *Jedes Gruppenelement aus G läßt sich als Frobeniusautomorphismus $\varphi_{\mathfrak{p}}$ für unendlich viele $\mathfrak{p}$ schreiben.*

Folgerung 2. *Zu teilerfremden natürlichen Zahlen a und n existieren unendlich viele Primzahlen p mit $p \equiv a \mod n$.*

Das ist Dirichlets Satz über arithmetische Progressionen. Zum Beweis setze $K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta_n)$, also $G = (\mathbb{Z}/n)^\times \ni a \mod n$. Der Frobeniusautomorphismus φ_p von $\mathbb{F}_p(\zeta_n)/\mathbb{F}_p$ erfüllt $\varphi_p(\zeta_n) = \zeta_n^p$ und der entsprechende von $L/\mathbb{Q}$ hat dieselbe Wirkung auf ζ_n.

Der Beweis des Čebotarevschen Satzes wird das ganze Kapitel füllen.

Wir erinnern zuerst an ein Ergebnis, das im Zusammenhang mit der analytischen Klassenzahlformel gewonnen wurde:

---

[6] $\sum_{\mathfrak{p},n\ge 2} \frac{1}{n(N\mathfrak{p})^{sn}} \le \sum_{p,n\ge 2} \frac{d}{np^{sn}} \le d\sum_{p,n\ge 2} \frac{1}{p^{sn}} = d\sum_p\left(\frac{1}{1-\frac{1}{p^s}} - 1 - \frac{1}{p^s}\right) = d\sum_p \frac{1}{p^s(p^s-1)} \le d\sum_p \frac{1}{p(p-1)} \le d\sum_{n\ge 2}\frac{1}{n(n-1)} = d \stackrel{\text{def}}{=} [K:\mathbb{Q}]$

[7] $\frac{\sum_P}{\sum_{\mathfrak{p}}} - \frac{\sum_P}{\sum_{\mathfrak{p}} - c} = \frac{\sum_P}{\sum_{\mathfrak{p}}} - \frac{\sum_P}{x\sum_{\mathfrak{p}}} = \frac{(x-1)\sum_P}{x\sum_{\mathfrak{p}}} \to 0$ weil $x = 1 - \frac{c}{\sum_{\mathfrak{p}}} \to 1$

Es sei $\mathfrak{c}$ eine Idealklasse von K. Die Anzahl $a_{\mathfrak{c}}(t)$ der ganzen Ideale in $\mathfrak{c}$ mit Norm $\leq t$ erfüllt

$$\lim_{t\to\infty} \frac{a_{\mathfrak{c}}(t)}{t} = \frac{2^{r+s}\pi^s R_K}{|\mu_K|\sqrt{|d_K|}} =: \rho\,;$$

vergleiche hierzu die Seiten 8 und 9 im Skript zur Zahlentheorie 1 - Vorlesung. Ist nämlich $\mathfrak{b}$ ein ganzes Ideal in $\mathfrak{c}^{-1}$, so zählt $a_{\mathfrak{c}}(t)$ genau die ganzen Hauptideale, die durch $\mathfrak{b}$ teilbar sind und Absolutnorm $\leq x = t\cdot N(\mathfrak{b})$ haben. Es folgt $a_{\mathfrak{c}}(t) = M(t\cdot N(\mathfrak{b}))$ (mit dem $M(t)$ in der letzten Zeile auf Seite 8) und also $\frac{a_{\mathfrak{c}}(t)}{t} \to v\cdot N(\mathfrak{b})$, und das ist genau die obige Limesformel.

Die lies nun so: $a_{\mathfrak{c}}(t) = \rho\cdot t + tf_{\mathfrak{c}}(t)$ mit $f_{\mathfrak{c}}(t)\to 0$ für $t\to\infty$. Genauer: $f_{\mathfrak{c}}(t) = O(t^{-[K:\mathbb{Q}]^{-1}})$; dafür ist nämlich der Faktor $t^{-\frac{1}{n}}$ (mit $n=[K:\mathbb{Q}]$) in der das $M(t)$ definierenden Gleichheit verantwortlich (zu Einzelheiten siehe auch Langs Buch *Algebraic Number theory*, IV,§3).

All dies läßt sich direkt verallgemeinern auf Stahlklassengruppen $I_K^{\mathfrak{m}}/H_0^{\mathfrak{m}}$ (anstelle von cl_K) zu einem Modul $\mathfrak{m}$ (die sollen fortan immer $n_{\mathfrak{p}} = 1$ für $\mathfrak{p}|\infty$ erfüllen). Man erhält:

Die Anzahl der ganzen Ideale in einer Strahlklasse $\mathfrak{c}\in I_K^{\mathfrak{m}}/H_0^{\mathfrak{m}}$ *mit Norm* $\leq t$ *ist* $= \rho_{\mathfrak{m}}\cdot t + tf_{\mathfrak{c}}(t)$ *mit* $f_{\mathfrak{c}}(t) = O(t^{-[K:\mathbb{Q}]^{-1}})$.

So wie früher ρ nicht von $\mathfrak{c}$ abhing, so ist auch jetzt $\rho_{\mathfrak{m}}$ unabhängig von der Klasse $\mathfrak{c}$.

In diesem Zusammenhang sei noch an die kurze exakte Sequenz endlicher Gruppen

$$H^{\mathfrak{m}}/H_0^{\mathfrak{m}} \rightarrowtail I_K^{\mathfrak{m}}/H_0^{\mathfrak{m}} \twoheadrightarrow G(L/K)$$

erinnert, falls L/K eine abelsche Erweiterung mit $C_K^{\mathfrak{m}} \leq N_{L/K}C_L$ ist.

Die zweite Erinnerung betrifft die Orthogonalitätsrelationen der Charaktere χ einer abelschen Gruppe G:

$$\begin{aligned}
\textstyle\sum_{\sigma\in G}\chi_1(\sigma^{-1})\chi_2(\sigma) &= \begin{cases} |G|\,,\ \chi_1=\chi_2 \\ 0\,,\ \chi_1\neq\chi_2 \end{cases}\\
\textstyle\sum_{\chi}\chi(\sigma^{-1})\chi(\tau) &= \begin{cases} |G|\,,\ \sigma=\tau \\ 0\,,\ \sigma\neq\tau \end{cases}\\
\textstyle\prod_{\chi}(1-\chi(\sigma)x) &= (1-x^f)^{\frac{|G|}{f}} \quad \text{sofern } |\sigma| = f\,.
\end{aligned}$$

Die dritte Gleichheit resultiert aus: $x^f - 1$ hat die Wurzeln $\chi(\sigma)$.

DEFINITION. *Es sei* $\mathfrak{m}$ *ein ganzes Ideal in* K *(das wir zu einem Modul machen, indem wir mit* $\prod_{\mathfrak{p}|\infty}\mathfrak{p}$ *multiplizieren) und* χ *ein Charakter von* $I_K^{\mathfrak{m}}/H_0^{\mathfrak{m}}$. *Setze*

$$L_{\mathfrak{m}}(s,\chi) = \sum_{\substack{(\mathfrak{a},\mathfrak{m})=1\\ \mathfrak{a}\text{ ganz}}} \chi(\mathfrak{a})(N\mathfrak{a})^{-s},\,,\ \Re(s) > 1\,,$$

wobei $\chi(\mathfrak{a})$ *für* $\chi(\mathfrak{a} \mod H_0^{\mathfrak{m}})$ *steht.*

Dies ist eine L-Reihe. Es gilt $L_{\mathfrak{m}}(s,\chi) = \prod_{\mathfrak{p}\nmid\mathfrak{m}}(1-\chi(\mathfrak{p})(N\mathfrak{p})^{-s})^{-1}$.

An dieser Stelle unterbrechen wir kurz mit einem Einschub über Dirichletreihen $\sum_{n\geq 1}a_n n^{-s}$, $a_n\in\mathbb{C}$; $L_{\mathfrak{m}}(s,\chi)$ ist dafür ein Beispiel.

1. *Abels Lemma:*

$$a_n, b_n \in \mathbb{C}\,,\; A_n \overset{\text{def}}{=} \sum_{i=1}^{n} a_i \implies \sum_{n=1}^{N} a_n b_n = A_N b_N + \sum_{n=1}^{N-1} A_n(b_n - b_{n+1})\,.$$

2. $g_\infty(s) = \sum_{n01}^{\infty} a_n n^{-s}$ konvergiere bei s_0. Dann konvergiert g_∞ gleichmäßig auf jedem Kompaktum in $\Re(s) > \Re(s_0)$.

   Dazu schreibe $n^{-s} = n^{-s_0} n^{s_0 - s}$ und verwende 1. mit $g_n(s_0) = \sum_{k=m+1}^{n} \frac{a_k}{k^{s_0}}$:

$$\begin{aligned}&\textstyle\sum_{k=m+1}^{n} \frac{a_k}{k^{s_0}} \frac{1}{k^{s-s_0}} = g_n(s_0) n^{s_0-s} + \sum_{k=m+1}^{n-1} g_k(s_0)\big(\frac{1}{k^{s-s_0}} - \frac{1}{(k+1)^{s-s_0}}\big)\\ &= g_n(s_0) n^{s_0-s} + \textstyle\sum_{k=m+1}^{n-1} g_k(s_0)(s-s_0)\int_k^{k+1} \frac{1}{x^{s-s_0+1}}\,dx\,.\end{aligned}$$

   Wegen $|x^z| = e^{\Re(z)\log x}$ (für $x>0$) wird dies gleichmäßig klein für große $m \le n$.

3. Ist $|A_n| \le c n^\sigma$ für alle n und feste c und $\sigma > 0$, so konvergiert $g_\infty(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ gleichmäßig auf jedem Kompaktum rechts von $\Re(s) = \sigma$.

   Denn, ähnlich wie zuvor,

$$\begin{aligned}&g_n(s) - g_m(s) = A_n \tfrac{1}{n^s} + \textstyle\sum_{k=m+1}^{n-1} A_k\big(\frac{1}{k^s} - \frac{1}{(k+1)^s}\big) - \frac{A_m}{(m+1)^s}\\ &= A_n \tfrac{1}{n^s} + \textstyle\sum_{k=m+1}^{n-1} A_k s \int_k^{k+1} \frac{1}{x^{s+1}}\,dx - \frac{A_m}{(m+1)^s}\end{aligned}$$

   und

$$|A_k \int_k^{k+1} \frac{1}{x^{s+1}}\,dx| \le c k^\sigma \Big| \int_k^{k+1} \frac{1}{x^{s+1}}\,dx \Big| \le c \int_k^{k+1} \frac{1}{x^{\Re(s)-\sigma+1}}\,dx\,;$$

   insgesamt ist also, mit $\Re(s) = \sigma + \delta$, $|g_n(s) - g_m(s)| \le c\Big(n^{-\delta} + s\int_{m+1}^{n-1} \frac{1}{x^{\delta+1}}\,dx + \frac{m^\sigma}{(m+1)^{\Re(s)}}\Big)$ klein für große $m \le n$.

Anwendung auf die L-Reihe $L_{\mathfrak{m}}(s,\chi)$:

1. sie konvergiert für $\Re(s) > 1$ (denn $\chi(\mathfrak{a})| \le 1$),
2. sie besitzt eine analytische Fortsetzung auf $\Re(s) > 1 - \frac{1}{[K:\mathbb{Q}]}$ bis, im Fall $\chi = 1$, auf einen einfachen Pol bei $s = 1$ mit Residuum $[I_K^{\mathfrak{m}} : H_0^{\mathfrak{m}}]\rho_{\mathfrak{m}}$.

Beweis von 2.:

$$\begin{aligned}&L_{\mathfrak{m}}(s,\chi) = \textstyle\sum_{\substack{(\mathfrak{a},\mathfrak{m})=1\\ \mathfrak{a}\,\text{ganz}}} \chi(\mathfrak{a})(N\mathfrak{a})^{-s}\,,\; (\chi \in \widehat{I_K^{\mathfrak{m}}/H_0^{\mathfrak{m}}})\,,\\ &= \textstyle\sum_{\mathfrak{c}\in I_K^{\mathfrak{m}}/H_0^{\mathfrak{m}}} \big(\sum_{\substack{\mathfrak{a}\in\mathfrak{c}\\ \mathfrak{a}\,\text{ganz}}} \chi(\mathfrak{a})(N\mathfrak{a})^{-s}\big) = \sum_{\mathfrak{c}} \chi(\mathfrak{c}) \sum_{\mathfrak{a}\in\mathfrak{c}} (N(\mathfrak{a})^{-s} = \sum_{\mathfrak{c}} \chi(\mathfrak{c})\zeta_{K,\mathfrak{c}}(s)\,.\end{aligned}$$

Nun ist $\zeta_{K,\mathfrak{c}}(s) = \sum_n \frac{a_n}{n^s}$ mit $a_n = \#\{\mathfrak{a} \in \mathfrak{c},\, \mathfrak{a}\,\text{ganz},\, N\mathfrak{a} = n\}$, also $A_n = a_1 + \cdots + a_n = \rho_{\mathfrak{m}} \cdot n + n f_{\mathfrak{c}}(n)$, und wir wandeln obiges 3. ab zu

3a. Gilt $|A_n - n\rho_{\mathfrak{m}}| \le c n^\sigma$ für ein c und ein $\sigma \in [0,1)$, so besitzt $g(s) = \sum_n a_n n^{-s}$ eine analytische Fortsetzung auf $\Re(s) > \sigma$ bis auf einen eventuellen Pol bei $s = 1$ mit Residuum $\rho_{\mathfrak{m}}$.

(Dazu wende 3. auf die Funktion $g(s) - \rho_\mathfrak{m} \cdot \zeta_\mathbb{Q}(s)$ an; wegen $\zeta_\mathbb{Q}(s)$ muß $s = 1$ gesondert betrachtet werden: s.u.)
Setze nun $\sigma = 1 - \frac{1}{[K:\mathbb{Q}]}$ und folgere aus 3a., daß $\zeta_{K,\mathfrak{c}}(s)$ analytisch für $\Re(s) > 1 - \frac{1}{[K:\mathbb{Q}]}$ mit Ausnahme des einfachen Pols bei $s = 1$ mit Residuum $\rho_\mathfrak{m}$ ist. Ist aber $\chi \neq 1$, so verschwindet der Pol für $L_\mathfrak{m}(s, \chi)$ wegen $\sum_\mathfrak{c} \chi(\mathfrak{c}) = 0$: $(s-1)\zeta_{K,\mathfrak{c}}(s) = \rho_\mathfrak{m} + h_\mathfrak{c}(s)$ mit analytischem $h_\mathfrak{c}$ und $h_\mathfrak{c}(1) = 0$.

Für 3a. müssen wir uns noch davon vergewissern, daß die gewöhnliche ζ-Funktion, $\zeta_\mathbb{Q}(s)$, analytisch für $\Re(s) > 0$ (aber mit dem einfachen Pol bei $s = 1$) ist:

$$\zeta_\mathbb{Q}(s) = \frac{2}{2^s}\,\zeta_\mathbb{Q}(s) + \Big(1 - \frac{1}{2^s} + \frac{1}{3^s} - \cdots\Big), \text{ i.e. } \zeta_\mathbb{Q}(s)\Big(1 - \frac{2}{2^s}\Big) \text{ ist analytisch } (s \neq 1)\,.$$

Wir beweisen nun den Čebotarevschen Satz zunächst für abelsches L/K. Wie zuvor gelte $C_K^\mathfrak{m} \le N_{L/K} C_L$.

Sei $\sigma \in G = G(L/K)$ und $P = \{\mathfrak{p} \nmid \mathfrak{m} : \left(\frac{L/K}{\mathfrak{p}}\right) = \sigma\}$, also die Menge der in L/K unverzweigten $\mathfrak{p}$ mit Normrestsymbol σ, i.e. $\varphi_\mathfrak{p} = \sigma$. Hier ist der Trick, der erlaubt $\delta(P)$ zu bestimmen.
Setze $h(s) = \sum_{\chi \in \hat{G}} \chi(\sigma^{-1}) \log(L_\mathfrak{m}(s, \chi))$, wobei das χ in $L_\mathfrak{m}(s, \chi)$ über $\left(\frac{L/K}{-}\right) : I_K^\mathfrak{m}/H_0^\mathfrak{m} \twoheadrightarrow G$ als Charakter von $I_K^\mathfrak{m}/H_0^\mathfrak{m}$ aufgefaßt wird. Wir müssen uns geschwind davon vergewissern, daß $\log(L_\mathfrak{m}(s, \chi))$ in kleinen Umgebungen von $s = 1$ existiert.

1. $\chi \neq 1 \implies L_\mathfrak{m}(1, \chi) \neq 0$

   Denn die *ζ-Funktion* $\zeta_{K,\mathfrak{m}}(s) \overset{\text{def}}{=} L_\mathfrak{m}(s, 1)$ *von K bezüglich* $\mathfrak{m}$ hat bei $s = 1$ einen einfachen Pol (mit Residuum $[I_K^\mathfrak{m} : H_0^\mathfrak{m}]\rho_\mathfrak{m}$). Gehen wir zum Niveau L und zu dem von $\mathfrak{m}$ induzierten Modul $\mathfrak{M}$ von L über, so sehen wir also, daß auch $\zeta_{L,\mathfrak{M}}(s)$ einen einfachen Pol bei $s = 1$ hat; andererseits ist $\zeta_{L,\mathfrak{M}}(s) \overset{*}{=} \prod_{\chi \in \hat{G}} L_\mathfrak{m}(s, \chi)$, wie wir gleich nachprüfen werden. Für $\chi \neq 1$ ist $L_\mathfrak{m}(s, \chi)$ analytisch bei 1. Wäre dies nun einmal $= 0$, so würde im Produkt der einfache Pol von $L_\mathfrak{m}(s, 1)$ verschwinden, also $\zeta_{L,\mathfrak{M}}(s)$ analytisch bei 1 sein.

   Zu $\overset{*}{=}$: Ein $\mathfrak{p} \nmid \mathfrak{m}$ ist in L unverzweigt, also $\mathfrak{p}\mathfrak{o}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_g$ mit $g = [L:K]/f_\mathfrak{p}$. Und weil $\left(\frac{L/K}{\mathfrak{p}}\right) = \varphi_\mathfrak{p}$ die Ordnung $f_\mathfrak{p}$ hat, zeigt die dritte Charakterrelation

   $$\prod_\chi (1 - \chi(\varphi_\mathfrak{p}))(N\mathfrak{p})^{-s} = (1 - (N\mathfrak{p})^{-sf_\mathfrak{p}})^g = \prod_{\mathfrak{P}|\mathfrak{p}} (1 - (N\mathfrak{P})^{-s})\,.$$

   Nun multipliziere über alle $\mathfrak{p} \nmid \mathfrak{m}$ und benütze $\chi(\mathfrak{p}) = \chi(\varphi_\mathfrak{p})$.

2. $\log(\zeta_{K,\mathfrak{m}}(s)) = -\log(s-1) + O(1)$ für $s \to 1+$

   Das haben wir schon früher beobachtet: $(s-1)\zeta_{K,\mathfrak{m}}(s) \to [I_K^\mathfrak{m} : H_0^\mathfrak{m}]\rho_\mathfrak{m}$; hier sind wir im Reellen.

Zurück zu $h(s)$. Für $s \to 1+$ bekommen wir die Abschätzung $h(s) = -\log(s-1) + O(1)$, indem wir alle $\chi \neq 1$ in das $O(1)$ hineinpacken. Andererseits ist $L_\mathfrak{m}(s, \chi) = \prod_{\mathfrak{p} \nmid \mathfrak{m}} (1 - \chi(\mathfrak{p})(N\mathfrak{p})^{-s})^{-1}$ und also $\log(L_\mathfrak{m}(s, \chi)) = \sum_{\mathfrak{p} \nmid \mathfrak{m}} \frac{\chi(\mathfrak{p})}{(N\mathfrak{p})^s} + O(1)$. Ausnützung der Orthogonalitätsrelationen liefert

$$\sum_\chi \chi(\sigma^{-1}) \log(L_\mathfrak{m}(s, \chi)) = \sum_{\mathfrak{p} \nmid \mathfrak{m}} \frac{1}{(N\mathfrak{p})^s} \sum_\chi \chi(\sigma^{-1})\chi(\mathfrak{p}) = \sum_{\mathfrak{p} \in P} \frac{[L:K]}{(N\mathfrak{p})^s}\ ,$$

weil nur die Summanden $\mathfrak{p}$ mit $\left(\frac{L/K}{\mathfrak{p}}\right) = \sigma$ übrigbleiben. Damit

$$\delta(P) = \frac{\sum_P (N\mathfrak{p})^{-s}}{-\log(s-1)} = \frac{\sum_P (N\mathfrak{p})^{-s}}{[L:K](\sum_P (N\mathfrak{p})^{-s})} = \frac{1}{[L:K]} \, .$$

Nun, und als letztes, zum allgemeinen fall: L/K ist nur noch galoissch. Deuring führt den auf den zyklischen Fall wie folgt zurück.
C sei eine Konjugiertenklasse in $G = G(L/K)$ und $\sigma \in C$ mit Fixkörper F; P sei schließlich $= \{\mathfrak{p}$ unverzweigt in L, $\varphi_\mathfrak{p} \in C\}$. Definiere

$$P_F = \{\mathfrak{q} \subset F \, , \text{ unverzweigt in bezug auf } K \text{ und } L \, , \overline{F}_\mathfrak{q} = \overline{K}_\mathfrak{p} \text{ für } \mathfrak{q}|\mathfrak{p} \, , \left(\frac{L/F}{\mathfrak{q}}\right) = \sigma\} \, .$$

Man sieht

1. Zu $\mathfrak{p} \in P$ existiert ein $\mathfrak{P}$ von L mit $\varphi_{\mathfrak{P}|\mathfrak{p}} = \sigma$.
2. Über $\mathfrak{q} \in P_F$ liegt genau ein $\mathfrak{P}$ von L.

   Denn $\varphi_{\mathfrak{P}|\mathfrak{q}} = \sigma$, also $[\overline{L}_\mathfrak{P} : \overline{F}_\mathfrak{q}] = |\sigma| = [L:F]$.
3. Das $\mathfrak{P}$ aus 2. erfüllt $\varphi_{\mathfrak{P}|\mathfrak{p}} = \sigma$ für $\mathfrak{p} = \mathfrak{q} \cap K$.

   Denn $\varphi_{\mathfrak{P}|\mathfrak{q}} = (\varphi_{\mathfrak{P}|\mathfrak{p}})^{[\overline{F}_\mathfrak{q} : \overline{K}_\mathfrak{p}]} = \varphi_{\mathfrak{P}|\mathfrak{p}}$.
4. Hat $\mathfrak{P}|\mathfrak{p}$ den Frobeniusautomorphismus σ, so auch $\mathfrak{P}^\tau$ für $\tau \in Z_G(\sigma)$. Mithin gibt es $|Z_G(\sigma)|/|G_\mathfrak{P}|$ viele solcher. Wegen $|Z_G(\sigma)| = |G|/|C|$ und $G_\mathfrak{P} = G(L_\mathfrak{P}/K_\mathfrak{p}) = G(L_\mathfrak{P}/F_\mathfrak{q})$ sind dies $\frac{[L:K]}{|C|[L:F]} = \frac{[F:K]}{|C|}$ viele. Dies ist somit zugleich die Anzahl der $\mathfrak{q}|\mathfrak{p}$ in P_F.

Es folgt

$$\sum_P (N\mathfrak{p})^{-s} = \frac{|C|}{[F:K]} \sum_{P_F} (N\mathfrak{q})^{-s} \, .$$

Wegen $\frac{\sum_{P_F}(N\mathfrak{q})^{-s}}{\sum_\mathfrak{q}(N\mathfrak{q})^{-s}} \to [L:F]^{-1}$ (denn die $\mathfrak{q}$ mit $\left(\frac{L/F}{\mathfrak{q}}\right) = \sigma$ und höherem Restklassengrad tragen nichts zu $\frac{\sum_{\varphi_\mathfrak{q}=\sigma}(N\mathfrak{q})^{-s}}{\sum_\mathfrak{q}(N\mathfrak{q})^{-s}}$ bei), bleibt

$$\frac{\sum_P (N\mathfrak{p})^{-s}}{-\log(s-1)} \to \frac{|C|}{[F:K]} [L:F]^{-1} = \frac{|C|}{[L:K]} \, .$$

9. Artinsche L-Reihen

In diesem Kapitel ist L/K eine endliche galoissche Zahlkörpererweiterung mit Gruppe G und χ ein Charakter von G, also die Spurfunktion einer Darstellung $\rho_\chi : G \to GL_n(\mathbb{C})$. Über ρ_χ wird der n-dimensionale komplexe Vektorraum V ein $\mathbb{C}G$-Modul, der mit V_χ notiert wird. Man erinnere sich daran, daß V_χ durch χ bis auf G-Isomorphie wohlbestimmt ist. Des weiteren stehe, für eine endliche Primstelle $\mathfrak{p}$ von K, $G_\mathfrak{p} \leq G$ bzw. $G_\mathfrak{p}^0 \leq G_\mathfrak{p}$ für die Zerlegungs- bzw. Verzweigungsgruppe einer Fortsetzung $\mathfrak{P}|\mathfrak{p}$ von $\mathfrak{p}$ auf L und $\varphi_\mathfrak{p} \in G_\mathfrak{p}/G_\mathfrak{p}^0$ für den Lift des

Frobeniusautomorphismus der Restklassenkörpererweiterung $\overline{L}_{\mathfrak{P}}/\overline{K}_{\mathfrak{p}}$. Die Abhängigkeit von $G_{\mathfrak{p}}$ und $\varphi_{\mathfrak{p}}$ von der Wahl von $\mathfrak{P}|\mathfrak{p}$ spielt für die folgende Definition kaum eine Rolle:

$$V_\chi^{G^0_{\mathfrak{p}}} = \{v \in V_\chi : gv = v \ (\forall\, g \in G^0_{\mathfrak{p}})\} \simeq V_\chi^{G^0_{\sigma\mathfrak{p}}}\,, \ v \mapsto \sigma v\,,$$

und deshalb gar keine in der

Definition. *Die Artinsche L-Reihe* $L(s,\chi) = L_{L/K}(s,\chi)$ *ist für* $\Re(s) > 1$ *die Funktion*

$$s \mapsto \prod_{\mathfrak{p}\,\text{endlich}} \det(1 - \frac{\varphi_{\mathfrak{p}}}{(N\mathfrak{p})^s} \mid V_\chi^{G^0_{\mathfrak{p}}})^{-1}\,.$$

Der Unterschied zu dem $L_{\mathfrak{m}}(s,\chi)$ des vorangegangenen Kapitels ist zweifach –

1. χ ist nicht unbedingt ein abelscher Charakter,
2. verzweigte $\mathfrak{p}$ sind nicht mehr ausgeschlossen.

Ist allerdings L/K (also G) abelsch und χ ein irreduzibler Charakter, so gilt

$$L(s,\chi) = \prod_{\substack{\mathfrak{p}|\mathfrak{m} \\ G^0_{\mathfrak{p}} \le \ker\chi}} (1 - \frac{\chi(\varphi_{\mathfrak{p}})}{(N\mathfrak{p})^s})^{-1} \cdot L_{\mathfrak{m}}(s,\chi)$$

sofern $C_K^{\mathfrak{m}} \le N_{L/K} C_L$.
Denn jetzt ist V_χ eindimensional und

$$V_\chi^{G^0_{\mathfrak{p}}} = \begin{cases} 0\,, & G^0_{\mathfrak{p}} \not\le \ker\chi \\ V_\chi\,, & G^0_{\mathfrak{p}} \le \ker\chi \text{ (also z.B. wenn } \mathfrak{p} \text{ unverzweigt ist)}\,, \end{cases}$$

somit

$$L(s,\chi) = \prod_{G^0_{\mathfrak{p}} \le \ker\chi} (1 - \frac{\varphi_{\mathfrak{p}}}{(N\mathfrak{p})^s} \mid V_\chi)^{-1} = \prod_{\substack{\mathfrak{p}|\mathfrak{m} \\ G^0_{\mathfrak{p}} \le \ker\chi}} (1 - \frac{\chi(\varphi_{\mathfrak{p}})}{(N\mathfrak{p})^s})^{-1} \cdot \prod_{\mathfrak{p}\nmid\mathfrak{m}} (1 - \frac{\chi(\varphi_{\mathfrak{p}})}{(N\mathfrak{p})^s})^{-1}\,.$$

Ein weiterer Spezialfall ist der des trivialen Charakters $\chi = 1$. Dann gilt offenbar $L(s,1) = \zeta_K(s)$, denn jetzt ist $V_\chi = \mathbb{C}$ (mit trivialer G-Wirkung), also auch $V_\chi^{G^0_{\mathfrak{p}}} = \mathbb{C}$.
Zur Konvergenz der Artinschen L-Reihe:
Die Matrix $\rho_\chi(\varphi_{\mathfrak{p}})$ ist zu einer Diagonalmatrix mit Einheitswurzeln ζ_i auf der Hauptdiagonalen konjugiert und daher

$$\det(1 - \frac{\varphi_{\mathfrak{p}}}{(N\mathfrak{p})^s} \mid V_\chi^{G^0_{\mathfrak{p}}})^{-1} = \prod_{i=1}^{d} (1 - \frac{\zeta_i}{(N\mathfrak{p})^s})^{-1}$$

mit $d = \dim V_\chi^{G^0_{\mathfrak{p}}}$. Folglich

$$\log(\prod_{\mathfrak{p}} \det(1 - \frac{\varphi_{\mathfrak{p}}}{(N\mathfrak{p})^s} \mid V_\chi^{G^0_{\mathfrak{p}}})^{-1} = \sum_{\mathfrak{p}} \sum_{i=1}^{d} \sum_{n=1}^{\infty} \frac{\zeta_i^n}{n(N\mathfrak{p})^{sn}}$$

und $\sum_{\mathfrak{p},i,n} \frac{1}{n|p^{snf_{\mathfrak{p}}}|} \le \sum_{p,i,n} \frac{[K:\mathbb{Q}]}{np^{(1+\delta)n}} = d[K:\mathbb{Q}] \log\zeta(1+\delta)$ liefert eine obere konvergente Schranke für $\Re(s) \ge 1+\delta$ (der Faktor $[K:\mathbb{Q}]$ schätzt die $\mathfrak{p}|p$ ab).

SATZ. *1.* $L(s,\chi_1)\cdot L(s,\chi_2)=L(s,\chi_1+\chi_2)$,

2. für $F\supset L\supset K$ *mit galoisschem* F/K *gilt* $L_{F/K}(s,\operatorname{infl}_L^F\chi)=L_{L/K}(s,\chi)$,

3. ist F *ein zwischen* K *und* L *gelegener Körper und* χ *ein Charakter von* $G(L/F)$, *so gilt* $L_{L/F}(s,\chi)=L_{L/K}(s,\operatorname{ind}_F^K(\chi))$.

FOLGERUNG. $\zeta_L(s)=\zeta_K(s)\cdot\prod_{\chi\neq 1}L(s,\chi)^{\chi(1)}$

Dazu wende den Satz auf den Charakter $\operatorname{ind}_1^G(1)=\sum_{\chi\text{ irreduzibel}}\chi(1)\chi$ der regulären Darstellung von G an.

Zum Beweis des Satzes:

1. folgt aus $V_{\chi_1+\chi_2}=V_{\chi_1}\oplus V_{\chi_2}$ und damit $V_{\chi_1+\chi_2}^{G_\mathfrak{p}^0}=V_{\chi_1}^{G_\mathfrak{p}^0}\oplus V_{\chi_2}^{G_\mathfrak{p}^0}$.

2. folgt so: $\mathfrak{P}\mid\wp\mid\mathfrak{p}$ gehöre zu $F\supset L\supset K$; es sei $G=G(F/K)$ und $\overline{G}=G(L/K)$. Die Inflation von χ von $\overline{G}$ nach G bedeutet, daß $\sigma\in G$ wie die Restriktion $\overline{\sigma}$ von σ auf L auf V_χ wirkt. Die kanonischen Surjektionen $G_{\mathfrak{P}|\mathfrak{p}}\twoheadrightarrow\overline{G}_{\wp|\mathfrak{p}}$, $G^0_{\mathfrak{P}|\mathfrak{p}}\twoheadrightarrow\overline{G}^0_{\wp|\mathfrak{p}}$, $\varphi_{\mathfrak{P}|\mathfrak{p}}\mapsto\varphi_{\wp|\mathfrak{p}}$ liefern schließlich $\det(1-\frac{\varphi_{\mathfrak{P}|\mathfrak{p}}}{(N\mathfrak{p})^s}\mid V_\chi^{G^0_{\mathfrak{P}|\mathfrak{p}}})=\det(1-\frac{\varphi_{\wp|\mathfrak{p}}}{(N\mathfrak{p})^s}\mid V_\chi^{\overline{G}^0_{\wp|\mathfrak{p}}})$.

3. Wie früher sei $\mathfrak{P}\supset\wp\supset\mathfrak{p}$ im Einklang mit $L\supset F\supset K$; U bezeichne die Galoisgruppe $G(L/F)$.

   Man überlegt sich zuerst, daß aus der disjunkten Doppelnebenklassenzerlegung $G=\bigcup_{i=1}^r G_\mathfrak{P}\sigma_i U$ folgendes resultiert:

   (a) die Anzahl der $\wp$'s über $\mathfrak{p}$ ist r, $\mathfrak{P}_i\overset{\text{def}}{=}\sigma_i^{-1}\mathfrak{P}$, $\wp_i\overset{\text{def}}{=}\sigma^{-1}\wp$,

   (b) $\operatorname{ind}_U^G V_\chi=\bigoplus_{i=1}^r V_i$ als $G_\mathfrak{P}$-Modul (Mackey-Formel),

   (c) $f_i\overset{\text{def}}{=}f_{\wp_i|\mathfrak{p}}=[G_\mathfrak{P}^{\sigma_i}:(G_\mathfrak{P}^0)^{\sigma_i}U_{\mathfrak{P}_i}]$, $\varphi_{\wp_i|\mathfrak{p}}=\sigma_i^{-1}\varphi^{f_i}_{\mathfrak{P}|\mathfrak{p}}\sigma_i$,

   (d) die Behauptung folgt aus

$$\det(1-\varphi_{\mathfrak{P}|\mathfrak{p}}(N\mathfrak{p})^{-s}\mid V_i^{G_\mathfrak{P}^0})=\det(1-\varphi^{f_i}_{\mathfrak{P}|\mathfrak{p}}(N\mathfrak{p})^{-f_is}\mid(\sigma_i^{-1}V)^{G^0_\mathfrak{P}\cap\sigma_i^{-1}U\sigma_i}).$$

   Womit wir beim Fall $G=G_\mathfrak{p}$, $r=1$, $f=[G:G^0\cdot U]=$ Restklassengrad von $\wp|\mathfrak{p}$ angelangt sind. Des weiteren dürfen wir jetzt wegen 2. noch $G^0=1$ annehmen. Also $G=\langle\varphi\rangle$, $f=[G:U]$, $\operatorname{ind}_U^G V=\bigoplus_{i=0}^{f-1}\varphi^iV$. Ist nun $d=\dim V$, 1 die $d\times d$-Einheitsmatrix und ϕ die Matrix von φ^f auf V, so erreichen wir für φ die Matrix

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0\\ \vdots & & \ddots & & \vdots\\ 0 & 0 & \cdots & 1 & 0\\ 0 & 0 & \cdots & 0 & 1\\ \phi & 0 & \cdots & 0 & 0\end{pmatrix},$$

   woraus die Behauptung unmittelbar resultiert.

Bemerkungen: [8]

1. Durch Hinzufügen von *archimedischen Eulerfaktoren* an $L(s,\chi)$ entsteht die *vollständige Artinsche L-Reihe*

$$\Lambda(s,\chi) \overset{\text{def}}{=} L(s,\chi)\cdot L_\infty(s,\chi)\cdot(|d_K|^{\chi(1)}\cdot N(\mathfrak{f}(\chi)))^{s/2}$$

mit

$d_K =$ Diskriminante von $K/\mathbb{Q}$,

$L_\infty(s,\chi) = \prod_{\mathfrak{p}|\infty} L_\mathfrak{p}(s,\chi)\,, \quad L_\mathfrak{p}(s,\chi) = \begin{cases} (2(2\pi)^{-s}\Gamma(s))^{\chi(1)}\,, & \mathfrak{p} \text{ komplex} \\ (\pi^{-s/2}\Gamma(s/2))^{n^+}(\pi^{-\frac{s+1}{2}}\Gamma(\frac{s+1}{2}))^{n^-}\,, & \mathfrak{p} \text{ reell,} \end{cases}$

wobei $n^\pm = \frac{\chi(1)\pm\chi(\varphi_\mathfrak{p})}{2}$ und $\langle\varphi_\mathfrak{p}\rangle = G_{\mathfrak{P}|\mathfrak{p}}$,

$\mathfrak{f}(\chi) =$ Artinführer von χ – siehe Kapitel 10.

Diese vollständige Artinsche L-Reihe ist meromorph auf $\mathbb{C}$ und genügt der Funktionalgleichung

$$\Lambda(s,\chi) = W(\chi)\cdot\Lambda(1-s,\check{\chi})\,,$$

wobei $\check{\chi}(g) = \chi(g^{-1})$ und $W(\chi)$ eine komplexe Zahl vom Betrag 1 ist (*die Wurzelzahl zu* χ)).

Auch $\Lambda(s,\chi)$ besitzt die im letzten Satz genannten drei Eigenschaften. Damit braucht die Funktionalgleichung und die Meromorphie von $\Lambda(s,\chi)$ dank des Brauerschen Induktionssatzes für Gruppencharaktere nur für abelsche χ bewiesen zu werden. Aus der Definition von $\Lambda(s,\chi)$ resultiert die meromorphe Fortsetzbarkeit von $L(s,\chi)$ auf ganz $\mathbb{C}$ (und eine abgeleitete Funktionalgleichung). Ist χ abelsch und $\neq 1$, so ist $L(s,\chi)$ sogar eine ganze Funktion. Für nichtabelsche irreduzible χ ist das vermutet, aber noch nicht bewiesen (im Brauerschen Satz treten negative Koeffizienten auf).

Literatur hierzu: Tates Thesis (siehe Cassels-Fröhlich, Algebraic Number Theory (Academic Press 1967)), oder Lang, Algebraic Number Theory (chapter 14)
oder die sogenannte Hecke Theorie in Lang (chapter 13) oder Neukirch, Algebraische Zahlentheorie (Kapitel 7).

2. Die Werte von $L(s,\chi)$ für ganzzahlige n sind noch nicht verstanden. Wie schon die Wurzelzahl [9] hängen auch die eng mit arithmetischen Eigenschaften ausgezeichneter ganzzahliger Galoisstrukturen zusammen (Ganzheitsnormalbasen bei Ganzheitsringen, Klassen- und Einheitengruppen &c.). Man weiß (unter Ausnützung der Funktionalgleichung)

   für $s = -1,-2,-3,\ldots$ ist $L(s,\chi)$ Null, es sei denn, K wäre total reell. In dem Fall ist $L(s,\chi)$ algebraisch über $\mathbb{Q}$ für $s\in\mathbb{Z}_{\leq 0}$ (und $\zeta_K(s)$ $\begin{cases} =0\,, & k<0 \text{ gerade} \\ \neq 0\,, & k<0 \text{ ungerade} \end{cases}$).

   Da die negativen ganzen Zahlen dicht in den p-adisch ganzen Zahlen $\mathbb{Z}_p$ legen, kann man eine p-adische L-Reihe $L_p(s,\chi)$, $s\in\mathbb{Z}_p$, durch Interpolation an den Werten $L(s,\chi)$, $s\in\mathbb{Z}_{<0}$, gewinnen und es zeigt sich, daß die im wesentlichen eine p-adische Potenzreihe ist [10]. Für Einzelheiten siehe etwa Iwasawa, Lectures on p-adic L-functions (Annals

[8] die auszuführen, würde wohl den Inhalt einer Zahlentheorie 3 - Vorlesung ausmachen
[9] siehe Fröhlich, Galois module structure of algebraic integers (Springer 1983)
[10] darauf beruht die Iwasawatheorie

of Mathematics Studies 74), oder Tate, Les Conjectures de Stark sur les fonctions L d'Artin en $s=0$ (Birkhäuser 1984).

3. Man erinnere sich in dem Zusammenhang an Eulers Formel

$$(*) \qquad \zeta_{\mathbb{Q}}(2k) = (-1)^{k-1} \tfrac{(2\pi)^{2k}}{2(2k)!} B_{2k} \text{ für } k \in \mathbb{N}\,,$$

in der B_{2k} die $2k$-te Bernoullizahl ist ($\frac{ze^z}{e^z-1} = \sum_{k=0}^{\infty} B_k \frac{z^k}{k!}$).

$(*)$ kann z.B. über die Funktionalgleichung aus $\zeta_{\mathbb{Q}}(1-k) = -\frac{B_k}{k}$ für $k \in \mathbb{N}$ gefolgert werden. Präzise Angaben über die Werte $\zeta_{\mathbb{Q}}(2k-1)$ sind erst in jüngster Zeit mit Hilfe von algebraischer K-Theorie erhalten worden.

10. Verpasstes

Zuviel ist's hoffentlich nicht. Im Hinblick auf die zuletzt gemachten Bemerkungen gehört allerdings sicher zweierlei dazu, a), (Galois)-Gauß-Summen, und b), Führer; beide treten in der Wurzelzahl $W(\chi)$ auf. Und in b) spiegelt sich darüber hinaus genauere Verzweigungsinformation wider, woraus seinerseits die Verzweigung in Strahlklassenkörpern ablesbar wird. Um das Studium der vollständigen Artinschen L-Reihe und das von L-Werten zu erleichtern, sei hier wenigstens das Folgende zu a) und b) angemerkt.

1. Gaußsummen

Der klassischen *lokalen* Gaußsumme liegt ein lokaler Körper $k \supset \mathbb{Q}_p$ und ein Charakter $\chi : k^\times \to (\mathbb{Q}^c)^\times$ von endlicher Ordnung zugrunde. Der Führer von χ ist $\mathfrak{f}(\chi) = \mathfrak{p}^{f_\chi}$ mit dem minimalen f_χ, so daß χ auf $U_k^{(f_\chi)}$ trivial ist. Der (additive) Standardcharakter ψ_k von k ist durch

$$\psi_k : k^{(+)} \xrightarrow{\mathrm{tr}_{k/\mathbb{Q}_p}} \mathbb{Q}_p \xrightarrow{\psi_p} (\mathbb{Q}^c)^\times \quad \text{mit} \quad \psi_p(\mathbb{Z}_p) = 1\,,\ \psi_p(p^{-r}) = e^{2\pi i/p^r}$$

definiert. Damit wird die Gaußsumme $\tau(\chi)$ zu

$$\tau(\chi) = \sum_u \chi(uc^{-1})\psi_k(uc^{-1})\,,$$

wobei $\mathfrak{f}(\chi) \cdot \mathcal{D}_{k/\mathbb{Q}_p} = c\mathfrak{o}_k$ [11] und $u \in U_k/1+\mathfrak{f}(\chi)$ [12]. Man zeigt, daß die Definition unabhängig von der speziellen Wahl von c und von Vertretern von $1+\mathfrak{f}(\chi)$ in U_k ist. Des weiteren $|\tau(\chi)| = \sqrt{N\mathfrak{f}(\chi)}$. Die lokale Wurzelzahl $W(\chi)$ ist nun

$$W(\chi) = \begin{cases} 1 & k = \mathbb{R} \\ -i & k = \mathbb{C} \\ \tau(\check{\chi})/\sqrt{N\mathfrak{f}(\chi)} & k \supset \mathbb{Q}_p\,. \end{cases}$$

Die *globale* Gaußsumme betrifft den Zahlkörperfall; k ist also jetzt endlich über $\mathbb{Q}$ und χ ein (komplexer) Charakter von C_k von endlicher Ordnung. Aus $k_{\mathfrak{p}}^\times \to C_k \to (\mathbb{Q}^c)^\times$ erhalten wir den lokalen Charakter $\chi_{\mathfrak{p}}$ und setzen

$$\mathfrak{f}(\chi) = \prod_{\mathfrak{p}\nmid\infty} \mathfrak{f}(\chi_{\mathfrak{p}})\,,\ \tau(\chi) = \prod_{\mathfrak{p}\nmid\infty} \tau(\chi_{\mathfrak{p}})$$

[11] $\mathcal{D}_{k/\mathbb{Q}_p}$ ist die Differente

[12] solche Summen über Produkte aus Werten multiplikativer und additiver Charaktere erscheinen schon in der Lagrangeschen Resolvente (im Zusammenhang mit Hilberts Satz 90)

(die Produkte sind endlich). Es zeigt sich, daß dann

$$W(\chi) = \prod_{\mathfrak{p}\nmid\infty} W(\chi_{\mathfrak{p}}) \cdot W_\infty(\chi)\,, \quad W_\infty(\chi) \overset{\text{def}}{=} \prod_{\mathfrak{p}\mid\infty} W(\chi_{\mathfrak{p}})$$

gilt und folglich $W(\chi) = \tau(\check{\chi})W_\infty(\chi)/\sqrt{N\mathfrak{f}(\chi)}$.

Nun zu Galois-Gaußsummen. Zunächst sei wieder $k \supset \mathbb{Q}_p$ lokal und χ ein Charakter von $G_k \overset{\text{def}}{=} G(k^{\mathrm{c}}/k)$ mit offenem Kern (ist χ abelsch, so impliziert die Klassenkörpertheorie, daß χ als ein Charakter von $k^\times$ von endlicher Ordnung aufgefaßt werden kann). Es gibt nun eine eindeutig bestimmte $\mathbb{Q}^{\mathrm{c}}$-wertige Funktion $\chi \mapsto \tau(\chi)$ mit

> $\tau(\chi_1+\chi_2) = \tau(\chi_1)\cdot\tau(\chi_2)$, $\tau(\chi)$ ist das frühere $\tau(\chi)$ im Falle eines abelschen Charakters χ, $\tau(\operatorname{ind}_K^k(\chi)) = \tau(\chi)$ für endliches K/k (also $G_K \le G_k$ und $[G_k : G_K] < \infty$) und (virtuelle) Charaktere χ von G_K vom Grad 0.

Wieder folgt

$$|\tau(\chi)| = \sqrt{N\mathfrak{f}(\chi)}\,,\; W(\chi) = \tau(\check{\chi})/\sqrt{N\mathfrak{f}(\chi)}\,,$$

und, ins Globale gewendet (über $G_{\mathbb{Q}_p} \le G_{\mathbb{Q}}$), $\tau(\chi) = \prod_{\mathfrak{p}\nmid\infty} \tau(\chi_{\mathfrak{p}})$ &c. Was aber ist jetzt $\mathfrak{f}(\chi)$? Dazu gleich; bemerkt sei vorher noch, daß die Galoisautomorphismen von $G_{\mathbb{Q}}$ sowohl auf den χ als auch auf den Werten $\tau(\chi)$ wirken und daß man die beiden Wirkungen vergleichen kann. Erst dieser Vergleich birgt die Möglichkeit des Übergangs zu arithmetischen ganzzahligen Objekten:

> *Galoishomomorphismen auf den Charakteren* $\rightleftarrows$ *kohomologisch triviale Galois-Torsionsmoduln.*

Die Existenz der lokalen Galois-Gaußsummen ist nicht einfach zu beweisen und benutzt deutlich mehr als nur den Brauerschen Induktionssatz.

Literatur: Washington, Introduction to cyclotomic fields (Springer GTM 83), Chapt.6; Fröhlich, loc.cit., Chapt.3; Martinet, Character theory and Artin L-functions (in Fröhlich [ed.], Algebraic Number Fields (AP 1977).

2. Die Herbrandfunktion, Normen, der Satz von Hasse und Arf, Führer

Sei zunächst wieder $k \supset \mathbb{Q}_p$ lokal und K/k galoissch mit Gruppe G. Die Verzweigungsgruppen G_x für $x \in \mathbb{R}_{\ge -1}$ waren so definiert:

$$\sigma \in G_x \iff i_G(\sigma) \ge x+1 \iff w_K(\sigma(a)-a) \ge x+1 \;(\forall\, a \in \mathfrak{o}_K)$$

(die Bedingung rechts braucht tatsächlich nur für ein a mit $\mathfrak{o}_K = \mathfrak{o}_k[a]$ getestet zu werden).

Definition. $\varphi(x) = \int_0^x \frac{dt}{[G_0:G_x]}$ (mit $\varphi(x) = x$ für $-1 \le x \le 0$)

Für $n \in \mathbb{N}$ ist also $\varphi(n) = \frac{1}{|G_0|} \sum_{i=0}^n |G_i| \; - 1$; das ist i.allg. keine ganze Zahl.

Das φ ist stetig, stückweise linear, wachsend, konkav; die Umkehrfunktion ψ auf $[-1,\infty)$, die *Herbrandfunktion*, ist deshalb auch stetig, stückweise linear, wachsend, aber konvex; des weiteren $\psi(0) = 0$, $\psi(n) \in \mathbb{N}$ für $n \in \mathbb{N}$ (denn mit $\nu \le \psi(n) \le \nu+1$ für $\nu \in \mathbb{N}$ wird $|G_0|n = |G_1| + \cdots + |G_\nu| + (n-\nu)|G_{\nu+1}|$ und $|G_{\nu+1}|\,\big|\,|G_i|$ für $i \le \nu$).

DEFINITION. $G^x = G_{\psi(x)}$ *(also $G^{-1} = G$, $G^0 = G_0$, $G^x = 1$ für große x).*

Mit dieser Definition gilt

$$N \lhd G \implies (G/N)^x = G^x N/N\,, \quad \psi_{K/k} = \psi_{K/F} \circ \psi_{F/k} \text{ für } F = K^N\,.$$

Für unverzweigte Erweiterungen K/k ist die Funktion ψ einfach genug, $\psi(x) = x$, und man sieht, daß $N_{K/k}(U_K^{(n)}) = U_k^{(n)}$.

Für vollverzweigte Erweiterungen K/k gilt nur noch

$$N_{K/k}(U_K^{(\psi(n)}) \subset U_k^{(n)}\,,\ N_{K/k}(U_K^{(\psi(n)+1}) \subset U_k^{(n+1)}$$

und man hat eine exakte Sequenz

$$G_{\psi(n)}/G_{\psi(n)+1} \rightarrowtail U_K^{(\psi(n)}/U_K^{(\psi(n)+1} \xrightarrow{N_{K/k}} U_k^{(n)}/U_k^{(n+1)}\,.$$

Aus diesen Beobachtungen resultiert der

SATZ von Hasse-Arf. *Für abelsches G ist ein Sprung s in der Reihe G^x (also ein s mit $G^s \neq G^{s+\varepsilon}$ $(\forall\,\varepsilon > 0)$) eine ganze Zahl.*

DEFINITION. $\alpha_G(\sigma) = \begin{cases} -f_{K/k} i_G(\sigma) & \sigma \neq 1 \\ f_{K/k} \sum_{\omega\neq 1} i_G(\omega) & \sigma = 1 \end{cases}$ *heißt der Artincharakter von K/k.*

Jedenfalls ist α_G eine Klassenfunktion auf G und $(\alpha_G, 1) = 0$. Die Bezeichnung 'Charakter' für α_G ist erst gerechtfertigt, wenn $(\alpha_G, \chi) \in \mathbb{Z}_{\geq 0}$ für alle komplex-irreduziblen Charaktere χ von G gilt. Das ist der Fall, wie aus dem Brauerschen Induktionssatz zusammen mit 1.-6. unten und dem Satz von Hasse-Arf folgt.

(a) $\alpha_G = \operatorname{ind}_{G_0}^G(\alpha_{G_0})$

(b) $\alpha_G = \sum_{i=0}^\infty \frac{1}{[G_0:G_i]} \operatorname{ind}_{G_i}^G(\rho_{G_i} - 1)$ mit dem regulären Charakter ρ_{G_i} von G_i

(c) $(\alpha_G, \chi) = \sum_{i=0}^\infty \frac{1}{[G_0:G_i]}\,(\chi(1) - (\operatorname{res}_G^{G_i}\chi, 1))$

(d) $\alpha_{G/N}(\overline{\sigma}) = \frac{1}{|N|} \sum_{\sigma\mapsto\overline{\sigma}} \alpha_G(\sigma)$ für $N \lhd G$

(e) $\operatorname{res}_G^H(\alpha_G) = w_k(\mathfrak{d}_{F/k})\rho_H + f_{F/k}\alpha_H$ für $H \leq G$ und $F = K^H$ ($\mathfrak{d}_{F/k}$ ist die Diskriminante)

(f) für abelsches χ ist $(\alpha_G, \chi) = \varphi(c_\chi) + 1$ mit $c_\chi = \max_n\{\operatorname{res}_G^{G_n}\chi \neq 1\}$

Der Führer eines Charakters χ von G ist nun als $\mathfrak{f}(\chi) = \mathfrak{p}^{(\alpha_G,\chi)}$ definiert; dies setzt wegen (f) die frühere Definition von Führern abelscher Charaktere auf höherdimensionale χ fort.

Wir globalisieren: K/k ist jetzt eine galoissche Zahlkörpererweiterung mit Gruppe G. Sei $\mathfrak{p}$ ein Primideal von k und $\mathfrak{P}|\mathfrak{p}$ eines von K. Definiere $\alpha_\mathfrak{P}$ als den Artincharakter der lokalen Erweiterung $K_\mathfrak{P}/k_\mathfrak{p}$ mit Gruppe $G_\mathfrak{P}$ und

$$\alpha_\mathfrak{p} = \operatorname{ind}_{G_\mathfrak{P}}^G \alpha_\mathfrak{P}\,;$$

des weiteren, für einen Charakter χ von G, $\mathfrak{f}(\chi) = \prod_\mathfrak{p} \mathfrak{p}^{(\alpha_\mathfrak{p},\chi)}$. Das ist der Führer des (globalen) Charakters χ. Es gilt

$\mathfrak{f}(\chi_1+\chi_2)=\mathfrak{f}(\chi_1)\mathfrak{f}(\chi_2)\,,\quad \mathfrak{f}(1)=1\,,$

$\mathfrak{f}_{K/k}(\mathrm{ind}\,_H^G\chi)=\mathfrak{d}_{F/k}^{\chi(1)}N_{F/k}(\mathfrak{f}_{K/F}(\chi))$ für einen Charakter χ einer Untergruppe H von G mit Fixkörper F,

$\mathfrak{f}_{K/k}(\mathrm{infl}\,_{G/N}^G\chi)=\mathfrak{f}_{F/k}(\chi)$ falls $N\lhd G$, $F=K^N$ und χ ein Charakter von G/N ist

$\mathfrak{d}_{K/k}=\prod_{\chi\,\mathrm{irr}}\mathfrak{f}(\chi)^{\chi(1)}$ *"Führerdiskriminantenproduktformel"*

Literatur: Serre, loc.cit., Chapt.3

3. Maximal abelsche Erweiterungen mit vorgegebener Verzweigung

 (a) Ist $k\supset\mathbb{Q}_p$ lokal, so liefert das Normrestsymbol eine (stetige) Injektion $k^\times\to G_k^{\mathrm{ab}}$, denn der Kern ist $\bigcap_{K/k\,\mathrm{abelsch}}N_{K/k}K^\times=\bigcap_m(k^\times)^m$. Die Abbildung ist nicht surjektiv, weil links eine lokal-kompakte, rechts aber eine kompakte Gruppe steht (das Bild ist jedoch dicht; der Unterschied zur Surjektivität resultiert aus

$$\mathbb{Z}\simeq\pi_k^{\mathbb{Z}}\to\sigma_k^{\mathbb{Z}}\simeq\mathbb{Z}\subsetneq\hat{\mathbb{Z}}=\varprojlim_n\mathbb{Z}/n\,,$$

 wobei $\sigma_k=\varprojlim\sigma_{K/k}$ der Limes der Frobeniusautomorphismen $\sigma_{K/k}$ der unverzweigten Erweiterungen K/k ist).

 (b) Ist $k\supset\mathbb{Q}$ global, so liefert das globale Normrestsymbol die stetige Abbildung $C_k\to G_k^{\mathrm{ab}}$ mit Kern $D_k\overset{\mathrm{def}}{=}\bigcap_{K/k\,\mathrm{abelsch}}N_{K/k}C_K$. Jetzt ist die Abbildung surjektiv (weil C_k^0 kompakt ist); D_k ist aber nicht trivial, sondern die Gruppe aller unendlich dividierbaren Elemente von C_k, i.e., $D_k=\{\alpha\in C_k:\sqrt[n]{\alpha}\in C_k\ (\forall n\in\mathbb{N})\}=\bigcap_n C_k^n\ (\supset\mathbb{R}_{>0})$.

 (c) Ebenso wie in (b) sieht man, daß, wenn $\mathfrak{m}$ die Moduln mit $\begin{cases} n_\mathfrak{p}>0 \text{ für } \mathfrak{p}\in S\\ n_\mathfrak{p}=0 \text{ für } \mathfrak{p}\notin S\end{cases}$ durchläuft, $\bigcap_\mathfrak{m}C_k^\mathfrak{m}$ die Normgruppe der maximal abelschen Erweiterung von k ist, die nur in $S\supset S_\infty$ verzweigt. Restriktionen an die Verzweigung in S bedeuten Einschränkungen an die $n_\mathfrak{p}$ für $\mathfrak{p}\in S$.

 (d) Findet man abelsche Erweiterungen K/k mit vorgegebenen lokalen Erweiterungen $K_\mathfrak{P}/k_\mathfrak{p}$ für endlich viele $\mathfrak{p}$? Dazu sei hier ein Satz (dessen Beweis nicht trivial ist) angemerkt:

  S sei eine endliche Menge von Primidealen $\mathfrak{p}$ des Zahlkörpers k und $s:\prod_S k_\mathfrak{p}^\times\to C_k$ die kanonische Abbildung. Die ist injektiv und stetig, aber nicht offen. Dennoch gilt *unter s entsprechen die offenen Untergruppen von endlichem Index in $\prod_S k_\mathfrak{p}^\times$ eineindeutig denen von* $\mathrm{im}\,(s)$ *(in der von C_k induzierten Topologie). Letztere sind die Durchschnitte von* $\mathrm{im}\,(s)$ *mit den Normgruppen $N_{K/k}C_K$ endlicher abelscher Erweiterungen K/k.*

  SATZ. *i. Zu jedem $\mathfrak{p}\in S$ sei eine positive ganze Zahl $n_\mathfrak{p}$ mit $n_\mathfrak{p}=\begin{cases}1 \text{ oder } 2 \text{ für } \mathfrak{p} \text{ reell}\\ 1 \text{ für } \mathfrak{p} \text{ komplex}\end{cases}$ vorgegeben. Dann existiert eine zyklische Erweiterung K/k vom Grad $\mathrm{kgV}_S\{n_\mathfrak{p}\}$ mit $[K_\mathfrak{P}:k_\mathfrak{p}]=n_\mathfrak{p}$.*

  ii. Zu jedem $\mathfrak{p}\in S$ sei ein lokaler Charakter $\chi_\mathfrak{p}$ der Ordnung $n_\mathfrak{p}$ vorgegeben. Dann existiert ein globaler Charakter χ mit Restriktionen $\chi_\mathfrak{p}$ und Ordnung $\mathrm{kgV}_S\{n_\mathfrak{p}\}$, es sei denn, ein $\mathfrak{p}|2$ liege in S, in welchem Fall vielleicht nur die Ordnung $2\mathrm{kgV}_S\{n_\mathfrak{p}\}$ erreichbar ist.

Das ist eine (schwache) Version des Satzes von Grunwald-Hasse-Wang. Der zweite Teil des Satzes übertrifft den ersten Teil insofern, als die jeweiligen lokalen Erweiterungen (und nicht nur ihre Grade) vorgegeben sind.

Literatur: Artin-Tate, Class Field Theory (Benjamin 1976), Chapt.10,11