Algebraische Zahlentheorie II
Sommersemester 2022

Dr. Katharina Hübner
basierend auf Alexander Schmidts AZT2-Skript von 2014

Inhaltsverzeichnis

1 Galoiskohomologie

Wir untersuchen Kohomologie der additiven und der multiplikativen Gruppe des separablen Abschlusses als Modul unter der absoluten Galoisgruppe.

1.1 Die Abhängigkeit von der Auswahl des separablen Abschlusses

Sei K ein Körper und $\overline{K}_1, \overline{K}_2$ zwei separable Abschlüsse von K. Dann existiert ein (unkanonischer) K-Isomorphismus

$$\varphi : \overline{K}_1 \xrightarrow{\sim} \overline{K}_2.$$

Dieser induziert einen Isomorphismus

$$\begin{aligned} \varphi^* : G_2 = G(\overline{K}_2/K) &\xrightarrow{\sim} G_1 = G(\overline{K}_1/K), \\ \sigma &\longmapsto \varphi^{-1} \circ \sigma \circ \varphi. \end{aligned}$$

Nun sei $\dagger \in \{+, \times\}$. Dann ist $\overline{K}_i^\dagger$ ein diskreter $G(\overline{K}_i/K)$-Modul, $i = 1, 2$. Das Paar $\varphi^* : G_2 \xrightarrow{\sim} G_1$, $\varphi : \overline{K_1} \to \overline{K_2}$ ist kompatibel und wir erhalten einen Isomorphismus

$$H^i(G_1, \overline{K}_1^\dagger) \xrightarrow{\sim} H^i(G_2, \overline{K}_2^\dagger) \quad \forall\, i.$$

Ist nun

$$\varphi' : \overline{K}_1 \xrightarrow{\sim} \overline{K}_2$$

ein weiterer K-Isomorphismus, so erhalten wir das kommutative Diagramm

$$\begin{array}{ccc}
H^i(G_1, \overline{K}_1^\dagger) & \stackrel{(\varphi^*,\varphi)}{\longrightarrow} & H^i(G_2, \overline{K}_2^\dagger) \\
\| & & \downarrow ((\varphi'\circ\varphi^{-1})^*, \varphi'\circ\varphi^{-1}) \\
H^i(G_1, \overline{K}_1^\dagger) & \stackrel{(\varphi'^*,\varphi')}{\longrightarrow} & H^i(G_2, \overline{K}_2^\dagger)
\end{array}$$

Nun ist $(\varphi'\circ\varphi^{-1})^*$ ein innerer Automorphismus von G_2, also gilt nach Satz 1.18 in Kapitel 3.2:

$$((\varphi' \circ \varphi^{-1})^*, \varphi' \circ \varphi^{-1}) = \mathrm{id}_{H^i(G_2, \overline{K}_2^\dagger)}.$$

Wir erhalten daher einen *kanonischen* Isomorphismus

$$H^i(G(\overline{K}_1/K_1), \overline{K}_1^\dagger) \xrightarrow{\sim} H^i(G(\overline{K}_2/K_2), \overline{K}_2^\dagger)$$

für alle i.
Man benutzt oft die invarianten Schreibweisen

$$\begin{aligned}
H^i(K, \mathbb{G}_a) &= H^i(G(\overline{K}/K), \overline{K}^+) \\
H^i(K, \mathbb{G}_m) &= H^i(G(\overline{K}/K), \overline{K}^\times).
\end{aligned}$$

1.2 Additive Theorie

Satz 1.1. *Sei $L|K$ eine Galoiserweiterung mit Gruppe G. Dann gilt*

$$H^i(G, L^+) = 0 \qquad \forall\, i \geq 1.$$

Beweis. Wegen

$$H^i(G, L^+) = \varinjlim_{K \subset K' \subset L} H^i(G(K'|K), K'^+)$$

sei ohne Einschränkung $L|K$ endlich . Dann ist wegen der Existenz einer Normalbasis L^+ ein induzierter G-Modul. □

Korollar 1.2. *Ist $L|K$ endlich, so gilt $\hat{H}^i(G, L^+) = 0 \quad \forall\, i \in \mathbb{Z}$.*

Beweis. L^+ ist induziert, also kohomologisch trivial. □

Sei nun K ein Körper der Charakteristik $p > 0$ und $\overline{K}$ ein separabler Abschluss. Das Polynom $f(X) = X^p - X$ ist separabel, daher ist der Homomorphismus(!)

$$\begin{aligned}
\wp : \overline{K} &\longrightarrow \overline{K} \\
x &\longmapsto x^p - x
\end{aligned}$$

surjektiv. Der Kern von $\wp$ besteht aus den Nullstellen von f, d.h.

$$\ker(\wp) = \mathbb{F}_p \subset \overline{K}^+$$

(der Primkörper). Wir erhalten somit eine kurze exakte Folge von G_K-Moduln

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \overline{K}^+ \xrightarrow{\wp} \overline{K}^+ \longrightarrow 0$$

Aus der langen exakten Kohomologiefolge und 1.1 erhalten wir

Korollar 1.3. *(„Artin-Schreier-Theorie"). Sei K ein Körper der Charakteristik $p > 0$. Dann gilt*

$$H^i(G_K, \mathbb{Z}/p\mathbb{Z}) = \begin{cases} \mathbb{Z}/p\mathbb{Z} & i = 0 \\ K^+/\wp K^+ & i = 1 \\ 0 & i \geq 2. \end{cases}$$

Bemerkung. Es gilt

$$H^1(G_K, \mathbb{Z}/p\mathbb{Z}) = \mathrm{Hom}(G_K, \mathbb{Z}/p\mathbb{Z}).$$

D.h. die Elemente $\neq 0$ in $H^1(G_K, \mathbb{Z}/p\mathbb{Z})$ entsprechen surjektiven Homomorphismen

$$G_K \twoheadrightarrow \mathbb{Z}/p\mathbb{Z}.$$

Dies entspricht den folgenden Daten:

- eine zyklische Teilerweiterung $K'|K$ von $\overline{K}|K$ vom Grad p
- ein Isomorphismus $G(K'|K) \cong \mathbb{Z}/p\mathbb{Z}$, d.h. ein ausgezeichneter Erzeuger von $G(K'|K)$.

Daher misst $\dim_{\mathbb{F}_p} H^1(G_K, \mathbb{Z}/p\mathbb{Z})$ die maximale Anzahl linear unabhängiger zyklischer Erweiterungen vom Grad p.

Beispiel. Sei $\mathbb{F}_q$, $q = p^f$, ein endlicher Körper. Dimensionszählung in der exakten Folge

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{F}_q \xrightarrow{\wp} \mathbb{F}_q \longrightarrow H^1(G_{\mathbb{F}_q}, \mathbb{Z}/p\mathbb{Z}) \longrightarrow 0$$

liefert

$$\dim_{\mathbb{F}_q} H^1(G_{\mathbb{F}_q}, \mathbb{Z}/p\mathbb{Z}) = 1,$$

d.h. $\mathbb{F}_q$ hat genau eine zyklische Erweiterung vom Grad p. (Das wußten wir sowieso schon).

Bemerkung. Dies läßt sich von $\mathbb{Z}/p\mathbb{Z}$ auf $\mathbb{Z}/p^n\mathbb{Z}$ verallgemeinern. Die Rolle von $\overline{K}^+$ wird dann von den „Wittvektoren" übernommen.

1.3 Multiplikative Theorie – Hilberts Satz 90

Satz 1.4. *(Hilberts Satz 90)*
Sei $L|K$ eine Galoiserweiterung mit Gruppe G. Dann gilt

$$H^1(G, L^\times) = 0.$$

Beweis. Wie vorher reduziert man auf den Fall $L|K$ endlich. Sei $a : G \to L^\times$ eine Derivation. Für $c \in L^\times$ setzen wir

$$b = \sum_{g \in G} a(g) \cdot g(c).$$

Wegen der linearen Unabhängigkeit der Charaktere

$$L^\times \to L^\times, \quad c \mapsto gc$$

für $g \in G$ (siehe Algebra-Vorlesung) existiert ein $c \in L^\times$, so dass $b \neq 0$. Für $\tau \in G$ erhalten wir

$$a(\tau g) = a(\tau) \cdot \tau(a(g))$$

also

$$a(\tau)^{-1} a(\tau g) = \tau(a(g)).$$

Und daher:

$$\begin{aligned} \tau(b) &= \sum_{g \in G} \tau(a(g)) \cdot \tau g(c) \\ &= \sum_{g \in G} a(\tau)^{-1} a(\tau g) \cdot \tau g(c) \\ &= a(\tau)^{-1}\, b. \end{aligned}$$

$\rightsquigarrow \quad a(\tau) = b/\tau(b) \quad \forall\, \tau \rightsquigarrow \quad a$ ist innere Derivation. □

Korollar 1.5 (klassischer Hilbertscher Satz 90)**.** *Sei $L|K$ eine endliche Galoiserweiterung mit zyklischer Gruppe G. Sei σ ein Erzeuger von G. Dann ist jedes $x \in L^\times$ mit $N_{L|K}(x) = 1$ von der Form $x = y/\sigma y$ für ein $y \in L^\times$.*

Beweis. G zyklisch $\Longrightarrow$

$$\hat{H}^{-1}(G, L^\times) \cong H^1(G, L^\times) = 0.$$

Es folgt $\ker(N_G) = I_G L^\times = (1 - \sigma) \cdot L^\times$. □

Sei n eine natürliche Zahl prim zu $\mathrm{char}(K)$. Dann ist das Polynom $x^n - a$ für jedes $a \in \overline{K}^\times$ separabel, also der Homomorphismus $\overline{K}^\times \xrightarrow{\cdot n} \overline{K}^\times$, $x \mapsto x^n$, surjektiv. Wir erhalten eine exakte Folge (die „Kummer-Folge“) von G_K-Moduln

$$0 \longrightarrow \mu_n \longrightarrow \overline{K}^\times \xrightarrow{\cdot n} \overline{K}^\times \longrightarrow 0.$$

Nach Hilberts Satz 90 folgt

Korollar 1.6 („Kummer-Theorie").

$$H^1(G_K, \mu_n) \cong K^\times / K^{\times n}.$$

Nun nehmen wir an, dass eine primitive n-te Einheitswurzel ζ_n in K liegt.

Wir erhalten einen Isomorphismus von G_K-Moduln

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mu_n, \quad 1 + n\mathbb{Z} \longmapsto \zeta_n,$$

und folglich einen (von der Wahl von ζ abhängenden) Isomorphismus

$$\mathrm{Hom}(G_K, \mathbb{Z}/n\mathbb{Z}) \cong H^1(G_K, \mu_n) = K^\times / K^{\times n}.$$

Für ein $\overline{x} \in K^\times / K^{\times n}$ sei $\varphi_{\overline{x}} : G_K \to \mathbb{Z}/n\mathbb{Z}$ der assoziierte Homomorphismus. $U_{\overline{x}} := \ker(\varphi_{\overline{x}}) \subset G_K$ ist ein offener Normalteiler und es gilt

$$\begin{array}{ccc} G_K/U_{\bar{x}} & \xrightarrow{\sim} & \frac{n}{d}\mathbb{Z}/n\mathbb{Z} \subset \mathbb{Z}/n\mathbb{Z} \\ & & \wr\| \\ & & \mathbb{Z}/d\mathbb{Z} \end{array}$$

für einen Teiler $d \mid n$. Nun gilt

$$\overline{K}^{U_{\overline{x}}} = K\left(\sqrt[n]{x}\right)$$

wobei $x \in K^\times$ ein Vertreter von $\overline{x} \in K^\times/K^{\times n}$ ist. Der zu $\frac{n}{d} + n\mathbb{Z}$ zugehörige Erzeuger der zyklischen Gruppe $G_K/U_{\bar{x}}$ ist der Körperautomorphismus

$$\begin{array}{rcl} K\left(\sqrt[n]{x}\right) & \longrightarrow & K\left(\sqrt[n]{x}\right), \\ \sqrt[n]{x} & \longmapsto & \zeta_n^{\frac{n}{d}} \cdot \sqrt[n]{x}. \end{array}$$

D.h: Der Körper zu $\overline{x} \in K^\times/K^{\times n}$ ist kanonisch, der assoziierte Erzeuger der zyklischen Gruppe $G\left(K\left(\sqrt[n]{x}\right)|K\right)$ hängt von der Wahl der primitiven Einheitswurzel ζ_n ab.

Übungsaufgabe: Man verifiziere diese Behauptungen und überlege sich, wie die Situation im Fall der Artin-Schreier-Theorie

$$\mathrm{Hom}(G_K, \mathbb{Z}/p\mathbb{Z}) \Longrightarrow K/\wp K, \quad p = \mathrm{char}(K) > 0$$

aussieht.

1.4 Multiplikative Theorie – die Brauergruppe

Definition. Sei $L|K$ eine Galoiserweiterung mit Gruppe G. Die Gruppe

$$Br(L|K) = H^2(G, L^\times).$$

heißt **relative Brauergruppe** von L/K und

$$Br(K) = Br(\overline{K}|K) = H^2(G_K, \overline{K}^\times)$$

heißt die **(absolute) Brauergruppe** von K.

Erinnerung: Ist G eine Gruppe, $H \subset G$ ein Normalteiler und A ein G-Modul mit $H^i(H,A) = 0$, $i = 1, \dots, n-1$, so haben wir eine exakte Folge

$$0 \longrightarrow H^n(G/H, A^H) \xrightarrow{\text{inf}} H^n(G,A) \xrightarrow{res} H^n(H,A).$$

Ist nun $M|L|K$ ein Turm von Galoiserweiterungen und $A = M^\times$, so folgt mit Hilberts Satz 90, dass die Inflation

$$Br(L|K) \longrightarrow Br(M|K)$$

injektiv ist. Wir können die Formel

$$H^2(G_K, \overline{K}^\times) = \varinjlim_{K \subseteq L \subset \overline{K}} H^2(G(L|K), L^\times)$$

daher in der Form

$$Br(K) = \varinjlim_{K \subseteq L \subset \overline{K}} Br(L|K) = \bigcup_{K \subseteq L \subset \overline{K}} Br(L|K)$$

schreiben. Die obige exakte Folge liest sich

$$0 \longrightarrow Br(L|K) \longrightarrow Br(K) \longrightarrow Br(L).$$

Definition. Man sagt, dass ein $x \in Br(K)$ in einer Erweiterung $L|K$ **zerfällt**, wenn das Bild von x in $Br(L)$ gleich 0 ist.

Bemerkungen. Ist $L|K$ galoissch, so besteht $Br(L|K)$ gerade aus den $x \in Br(K)$, die über L zerfallen.

– Jedes $x \in Br(K)$ zerfällt in einer endlichen Erweiterung.

Zwischenbemerkung: Woher die Terminologie? Es gibt einen Isomorphismus

$$Br(K) \cong \left\{ \begin{array}{l} \text{endlich-dimensionale zentrale} \\ \text{einfache } K-\text{Algebren} \end{array} \right\} / \text{gewisse Äquivalenzrelation } \sim$$

Ein $A \in Br(K)$ zerfällt über L wenn $A \otimes_K L \sim M_n(L)$ für ein n.

Trivialerweise gilt falls $K = \overline{K}$:

$$Br(K) = H^2(G_K, \overline{K}^\times) = H^2(\{1\}, \overline{K}^\times) = 0.$$

Satz 1.7. *Sei K ein endlicher Körper. Dann gilt $Br(K) = 0$.*

Beweis. Sei $L|K$ eine endliche Erweiterung. Dann ist $G = G(L|K)$ zyklisch. Weil $L^\times$ endlich ist, gilt

$$h(G, L^\times) = 1;$$

also

$$\#H^2(G, L^\times) = \#H^1(G, L^\times) = 1.$$

Dies zeigt $Br(L|K) = 0$ für jede endliche Erweiterung $L|K$ und somit

$$Br(K) = \bigcup_L Br(L|K) = 0.$$

□

Bemerkung. Verschieben in die andere Richtung liefert: $\hat{H}^0(G, L^\times) = 0$, d.h. $K^\times = L^{\times G} = N_G L^\times$. Mit anderen Worten: Für jede endliche Erweiterung $L|K$ endlicher Körper ist die Normabbildung

$$N_{L|K} : L^\times \longrightarrow K^\times$$

surjektiv.

1.5 Die Brauergruppe eines lokalen Körpers

Dieser Abschnitt ist angelehnt an Denis Vogels Zahlentheorievorlesung vom Sommersemester 2021. Es sei K ein nichtarchimedischer lokaler Körper. Unser Ziel ist die Konstruktion eines natürlichen Isomorphismus

$$inv_K : Br(K) \to \mathbb{Q}/\mathbb{Z},$$

der sogenannten *Invariantenabbildung*.

Lemma 1.8. *Für eine endliche Gruppe G und ein projektives System $(A_i)_{i\in\mathbb{N}}$ kohomologisch trivialer G-Moduln ist auch $\varprojlim_i A_i$ kohomologisch trivial.*

Beweis. Übung. □

Satz 1.9. *Sei L/K eine endliche zyklische Erweiterung und $G = \mathrm{Gal}(L/K)$. Dann gilt*

$$\mid \hat{H}^n(G, L^\times) \mid = \begin{cases} [L:K], & n \text{ gerade} \\ 1 & n \text{ ungerade} \end{cases}$$

Insbesondere ist $\mid Br(L|K) \mid = [L:K]$.

Beweis. Nach Satz 1.10 in Kapitel 4 ist $\hat{H}^n(G, L^\times) \cong \hat{H}^{n+2}(G, L^\times)$ für alle $n \in \mathbb{Z}$. Nach Hilberts Satz 90 is $\mid \hat{H}^1(G, L^\times) \mid = 1$ Es reicht also zu zeigen, dass der Herbrandindex

$$h(G, L^\times) = \frac{\mid \hat{H}^0(G, L^\times) \mid}{\mid \hat{H}^1(G, L^\times) \mid}$$

gleich $[L : K]$ ist.

Sei σ in Erzeuger von G und es sei $|G| = n$ also $G = \{1, \sigma, \dots, \sigma^{n-1}\}$. Nach dem Satz vom primitiven Element gibt es $a \in L^\times$ mit $L = K(a)$. Dann ist $\{\sigma^i a\}_{i=1,\dots n-1}$ eine Basis von L und insbesondere sind die $\sigma^i a$ linear unabhängig über $\mathcal{O}_K$. Nach Multiplikation mit einem Element von K können wir annehmen, dass $a \in \mathcal{O}_L$. Wir betrachten den G-Untermodul

$$M := \bigoplus_{i=0}^{n-1} \sigma^i a \mathcal{O}_K \subseteq \mathcal{O}_L.$$

Es ist $M \cong \mathcal{O}_K[G]$. Außerdem ist M abgeschlossen in $\mathcal{O}_L$ und $(\mathcal{O}_L : M) < \infty$, denn M und $\mathcal{O}_L$ haben beide Rang n und $\mathcal{O}_L$ ist endlich erzeugt. Daraus folgt, dass M offen in $\mathcal{O}_L$ ist. Das bedeutet, dass es $N \in \mathbb{N}$ gibt mit $\pi_K^N \mathcal{O}_L \subseteq M$, wobei π_K eine Uniformisierende von K ist.

Wir setzen für $i \geq 0$

$$A_i := 1 + \pi_K^{N+i} M \subseteq \mathcal{O}_L^\times.$$

Die A_i bilden eine offene Umgebungsbasis der 1 in $\mathcal{O}_L^\times$. Wir behaupten, dass A_i ein G-Untermodul von endlichem Index ist. Um zu zeigen, dass es ein G-Untermodul ist, berechnen wir für $x, y \in M$ und $\sigma \in G$:

$$\begin{aligned}
(1 + \pi_K^{N+i} x)(1 + \pi_K^{N+i} y) &= 1 + \pi_K^{N+i}(x + y + \pi_K^{N+i} xy) \in A_i \\
(1 - \pi_K^{N+i} x)^{-1} &= 1 + \pi_K^{N+i}(x + \sum_{j=1}^{\infty} x^{j+1} (\pi_K^{N+i})^j) \in A_i \quad (\mathcal{O}_L \text{ vollständig}) \\
\sigma(1 + \pi_K^{N+i} x) &= 1 + \pi_K^{N+i} \sigma(x) \in A_i
\end{aligned}$$

Außerdem ist $(\mathcal{O}_L^\times : A_i) < \infty$, da A_i offen in $\mathcal{O}_L^\times$ und $\mathcal{O}_L^\times$ kompakt ist.

Die G-Moduln A_i / A_{i+1} sind kohomologisch trivial, da wir folgende Isomorphismen haben (k ist der Restklassenkörper von K):

$$\begin{aligned}
A_i / A_{i+1} &\xrightarrow{\sim} M / \pi_K M \\
1 + \pi_K^{N+i} x + A_{i+1} &\mapsto x + \pi_K M,
\end{aligned}$$

$$\begin{aligned}
M / \pi_K M &\xrightarrow{\sim} k[G] \\
\sigma^i a + \pi_K M &\mapsto \sigma^i.
\end{aligned}$$

Mithilfe der exakten Folgen

$$0 \to A_i/A_{i+} \to A_0/A_{i+1} \to A_0/A_i \to 0$$

und Induktion schließen wir, dass A_0/A_i für alle i kohomologisch trivial ist. Wegen Lemma 1.8 ist daher $A_0 = \varprojlim_i A_0/A_i$ kohomologisch trivial.

Wir wollen nun den Herbrandindex $h(G, L^\times) = h(L^\times)$ bestimmen. Weil er multiplikativ in kurzen exakten Folgen ist (Satz 1.12 aus Kapitel 4), bekommen wir aus der exakten Folge

$$0 \to \mathcal{O}_L^\times \to L^\times \xrightarrow{v_L} \mathbb{Z} \to 0$$

die Gleichung

$$h(L^\times) = h(\mathcal{O}_L^\times)h(\mathbb{Z}) = h(\mathcal{O}_L)[L : K].$$

Außerdem ist $h(\mathcal{O}_L/A_0) = 1$, da A_0 endlichen Index in $\mathcal{O}_L$ hat (siehe Satz 1.13 aus Kapitel 4). Deshalb ist $h(\mathcal{O}_L^\times) = h(A_0)$ und das ist 1, weil A_0 kohomologisch trivial ist. Daraus folgt

$$h(G, L^\times) = [L : K].$$

□

Lemma 1.10. *Sei L/K eine unverzweigte Erweiterung und $G = \mathrm{Gal}(L/K)$. Dann sind $\mathcal{O}_L^\times$ und $U_L^{(1)}$ kohomologisch triviale G-Moduln.*

Beweis. Für eine abgeschlossene Untergruppe $H \subseteq G$ ist

$$H^i(H, \mathcal{O}_L^\times) = H^i(\mathrm{Gal}(L/L^H), \mathcal{O}_L^\times) = \varprojlim_{L/M/L^H} H^i(\mathrm{Gal}(M/L^H), \mathcal{O}_M^\times),$$

wobei der projektive Limes über alle Zwischenerweiterungen $L/M/L^H$ läuft mit M/L^H endlich. Die analoge Aussage gilt für $U_L^{(1)}$. Damit haben wir uns auf den Fall endlicher Erweiterungen zurückgezogen. Wir können also im Folgenden annehmen, dass L/K endlich ist.

Sei ℓ/k die zu L/K gehörige Restklassenkörpererweiterung. Wir betrachten die Filtrierung

$$\ldots \subset U_L^{(2)} \subset U_L^{(1)} \subset \mathcal{O}_L^\times$$

Es ist

$$U_L^{(i-1)}/U_L^{(i)} \cong \ell^+ \cong k^+[G],$$

wobei wir für den zweiten Isomorphismus benutzt haben, dass L/K unverzweigt ist und damit $G = \mathrm{Gal}(L/K) = \mathrm{Gal}(\ell/k)$. Damit ist $U_L^{(i-1)}/U_L^{(i)}$ induziert, also kohomologisch trivial. Per Induktion folgt mithilfe der exakten Folge

$$1 \to U_L^{(i-1)}/U_L^{(i)} \to U_L^{(1)}/U_L^{(i)} \to U_L^{(1)}/U_L^{(i-1)} \to 1,$$

dass $U_L^{(1)}/U_L^{(i)}$ kohomologisch trivial ist für alle $i \geq 1$ und damit nach Lemma 1.8 auch $U_L^{(1)}$.

Um einzusehen, dass $\mathcal{O}_L^\times$ kohomologisch trivial ist, untersuchen wir die exakte Folge

$$1 \to U_L^{(1)} \to \mathcal{O}_L^\times \to \ell^\times \to 1.$$

Wir wissen schon, dass $U_L^{(1)}$ kohomologisch trivial ist. Außerdem ist $\ell^\times$ kohomologisch trivial, denn $H^1(G, \ell^\times) = H^1(\mathrm{Gal}(\ell/k), \ell^\times) = 0$ nach Hilberts Satz 90. Weil G zyklisch ist, reicht es daher zu zeigen, dass der Herbrandindex

$$h(G, \ell^\times) = \frac{|\hat{H}^0(G, \ell^\times)|}{|\hat{H}^1(G, \ell^\times)|}$$

trivial ist. Dies ist der Fall, weil $\ell^\times$ endlich ist (siehe Satz 1.13 aus Kapitel 4). Das gleiche Argument zeigt, dass die Kohomologiegruppen $H^i(H, \ell^\times)$ für jede Untergruppe H von G verschwinden. Insgesamt schließen wir mit obiger exakter Folge, dass $\mathcal{O}_L^\times$ kohomologisch trivial ist. □

Korollar 1.11. *Sei L/K eine endliche unverzweigte Erweiterung. Dann ist die Norm*

$$N_{L/K} : \mathcal{O}_L^\times \to \mathcal{O}_K^\times$$

surjektiv.

Beweis. Weil $\mathcal{O}_L^\times$ kohomologisch trivial ist, gilt

$$0 = \hat{H}^0(\mathrm{Gal}(L/K), \mathcal{O}_L^\times) = \mathcal{O}_K^\times / N_{L/K}\mathcal{O}_L^\times.$$

□

Für eine unverzweigte Erweiterung L/K mit Galoisgruppe $G = \mathrm{Gal}(L/K)$ und Bewertung $v : L^\times \to \mathbb{Z}$ konstruieren wir nun die Invariantenabbildung

$$inv_{L/K} : Br(L/K) \to \mathbb{Q}/\mathbb{Z}.$$

Die exakte Folge

$$1 \to \mathcal{O}_L^\times \to L^\times \xrightarrow{v} \mathbb{Z} \to 0$$

diskreter G-Moduln gibt uns wegen der kohomologischen Trivialität von $\mathcal{O}_L^\times$ einen Isomorphismus

$$Br(L/K) = H^2(G, L^\times) \xrightarrow{\sim} H^2(G, \mathbb{Z}).$$

Nun betrachten wir die exakte Folge

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0.$$

Weil $\mathbb{Q}$ eindeutig teilbar ist, ist es kohomologisch trivial und wir erhalten einen Isomorphismus

$$H^2(G,\mathbb{Z}) \xleftarrow{\sim} H^1(G,\mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z}).$$

Weil L/K unverzweigt ist, haben wir $G = \mathrm{Gal}(\ell/k)$ und $\mathrm{Gal}(\ell/k)$ wird topologisch erzeugt vom Frobeniusautomorphismus, der $x \in \ell$ auf x^q schickt, wobei $q = \#k$. Es gibt also einen eindeutig bestimmten Frobeniusautomorphismus $\mathrm{Frob}_{L/K}$ auf L, der den Frobeniusautomorphismus auf ℓ induziert und dieser ist ein topologischer Erzeuger der Gruppe G. Wir definieren

$$\eta : H^1(G,\mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z}) \to \mathbb{Q}/\mathbb{Z}, \qquad \varphi \mapsto \varphi(\mathrm{Frob}_{L/K}).$$

Diese Abbildung ist injektiv, da $\mathrm{Frob}_{L/K}$ die Gruppe G topologisch erzeugt und mit $\mathrm{Hom}(G,-)$ die stetigen Homomorphismen gemeint sind.

Definition. Die Komposition

$$inv_{L/K} : Br(L/K) = H^2(G,L^\times) \cong H^2(G,\mathbb{Z}) \cong H^1(G,\mathbb{Q}/\mathbb{Z}) \hookrightarrow \mathbb{Q}/\mathbb{Z}$$

heißt Invariantenabbildung.

Lemma 1.12. *Sei $M/L/K$ ein Turm unverzweigter Erweiterungen. Dann kommutiert das Diagramm*

$$\begin{tikzcd} Br(L|K) \arrow[r, "inv_{L/K}"] \arrow[d, hook, "\mathrm{inf}"] & \mathbb{Q}/\mathbb{Z} \arrow[d, equal] \\ Br(M/K) \arrow[r, "invM/K"] & \mathbb{Q}/\mathbb{Z}. \end{tikzcd}$$

Beweis. Alle in der Definition der Invariantenabbildung vorkommenden Abbildungen sind funktoriell, ebenso die Inflation. □

Satz 1.13. *Es existiert ein eindeutig bestimmter Isomorphismus*

$$inv_K : Br(K^{\mathrm{nr}}|K) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$$

(nämlich $inv_K = inv_{K^{\mathrm{nr}}/K}$), so dass für alle endlichen Galoiserweiterungen L/K in K^{nr} das Diagramm

$$\begin{tikzcd} Br(L|K) \arrow[r, "inv_{L|K}"] \arrow[d, hook, "\mathrm{inf}"] & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \arrow[d, hook] \\ Br(K^{\mathrm{nr}}|K) \arrow[r, "\sim", "inv_K"'] & \mathbb{Q}/\mathbb{Z} \end{tikzcd}$$

kommutiert.

Beweis. Für eine endliche unverzweigte Erweiterung L/K ist die Galoisgruppe $G = \mathrm{Gal}(L/K)$ endlich zyklisch und wird vom Frobeniusautomorphismus $\mathrm{Frob}_{L/K}$ erzeugt. Wir können somit einen Homomorphismus $f \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) = H^1(G, \mathbb{Q}/\mathbb{Z})$ definieren dadurch, dass

$$f(\mathrm{Frob}_{L/K}) = \frac{1}{[L:K]} + \mathbb{Z}.$$

Insbesondere ist das Bild von $inv_{L/K}$ gleich $\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$. Da $\inf_{L/K}$ injektiv ist, ist

$$\mathrm{im}(inv_{L/K}) \cong Br(L|K) \cong H^1(G, \mathbb{Q}/\mathbb{Z}) \cong \mathrm{Hom}(\mathbb{Z}/[L:K]\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \cong \mathbb{Z}/[L:K]\mathbb{Z},$$

das heißt

$$\mathrm{im}(inv_{L|K}) = \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}.$$

Das Diagramm in der Aussage des Satzes kommutiert wegen Bemerkung 1.12. Außerdem ist inv_K surjektiv, da

$$Br(K^{\mathrm{nr}}|K) = \bigcup_{K^{\mathrm{nr}}/L/K \text{ endl.}} Br(L|K)$$

und es zu jedem $n \in \mathbb{N}$ eine unverzweigte Erweiterung L/K vom Grad n gibt. Außerdem folgt daraus, dass inv_K durch $inv_{L/K}$ für endliche unverzweigte Erweiterungen L/K eindeutig bestimmt ist. □

Theorem 1.14. *Sei L/K eine endliche separable Erweiterung. Dann existiert ein kanonischer Homomorphismus*

$$res : Br(K^{\mathrm{nr}}|K) \to Br(L^{\mathrm{nr}}|L),$$

so dass das folgende Diagramm kommutiert:

$$\begin{array}{ccc} Br(K^{\mathrm{nr}}|K) & \xrightarrow{res} & Br(L^{\mathrm{nr}}|L) \\ \big\downarrow{\scriptstyle inv_K} & & \big\downarrow{\scriptstyle inv_L} \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{\cdot[L:K]} & \mathbb{Q}/\mathbb{Z}. \end{array}$$

Ist L/K galoissch, so kann der Kern von res kanonisch mit einer zyklischen Untergruppe der Ordnung $[L:K]$ von $Br(L|K)$ identifiziert werden.

Beweis. Wir setzen $\Gamma_K := \mathrm{Gal}(K^{\mathrm{nr}}/K)$ und $\Gamma_L := \mathrm{Gal}(L^{\mathrm{nr}}/L)$. Es ist $L^{\mathrm{nr}} = LK^{\mathrm{nr}}$. Insbesondere haben wir eine natürliche Inklusion $\varphi : \Gamma_L \hookrightarrow \Gamma_K$. Wir betrachten das Diagramm

$$\begin{array}{ccccccc} Br(K^{\mathrm{nr}}|K) & \xrightarrow[\sim]{v_K} & H^2(\Gamma_K, \mathbb{Z}) & \xrightarrow[\sim]{\delta^{-1}} & H^1(\Gamma_K, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\eta_K} & \mathbb{Q}/\mathbb{Z} \\ \big\downarrow{\scriptstyle res} & & \big\downarrow{\scriptstyle e_{L/K}\cdot res} & & \big\downarrow{\scriptstyle e_{L/K}\cdot res} & & \big\downarrow{\scriptstyle e_{L/K}f_{L/K}=[L:K]} \\ Br(L^{\mathrm{nr}}|L) & \xrightarrow[\sim]{v_L} & H^2(\Gamma_L, \mathbb{Z}) & \xrightarrow[\sim]{\delta^{-1}} & H^1(\Gamma_K, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\eta_L} & \mathbb{Q}/\mathbb{Z}. \end{array}$$

Dieses kommutiert wegen $v_L|_{K^{\mathrm{nr}}} = e_{L/K} v_K$ und $\mathrm{Frob}_L|_{K^{\mathrm{nr}}} = \mathrm{Frob}_K^{f_{L/K}}$. Daraus folgt die erste Behauptung.

Für eine endliche Galoiserweiterung L/K ist L^{nr}/K galoissch (das liegt an der Maximalität von L^{nr}/L; für $\sigma \in G_K$ ist σL^{nr} unverzweigt über $\sigma L = L$ und somit enthalten in L^{nr}). Wir erhalten ein kommutatives Diagramm mit exakten Zeilen

$$\begin{tikzcd}
0 \arrow[r] & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \arrow[r] & \mathbb{Q}/\mathbb{Z} \arrow[r, "\cdot [L:K]"] & \mathbb{Q}/\mathbb{Z} \\
0 \arrow[r] & \ker(res) \arrow[r] \arrow[u, "\sim"'] \arrow[d, hook] & Br(K^{\mathrm{nr}}|K) \arrow[r, "res"] \arrow[u, "inv_K"', "\sim"] \arrow[d, hook, "\inf"] & Br(L^{\mathrm{nr}}|L) \arrow[u, "inv_L"', "\sim"] \arrow[d, equal] \\
0 \arrow[r] & Br(L|K) \arrow[r, "\inf"] & Br(L^{\mathrm{nr}}|K) \arrow[r, "res"] & Br(L^{\mathrm{nr}}|L),
\end{tikzcd}$$

woraus sich die zweite Behauptung ergibt. □

Korollar 1.15. *Sei L/K eine endliche Galoiserweiterung. Dann ist $Br(L|K)$ zyklisch der Ordnung $[L : K]$.*

Beweis. Wir beweisen das per Induktion nach $n = [L : K]$. Für $n = 1$ ist die Aussage klar und für $n > 1$ und L/K zyklisch folgt sie aus dem Satz 1.14 und Satz 1.9. Falls L/K nicht zyklisch ist, finden wir eine nichttiviale galoissche Zwischenerweiterung $L/M/K$, denn die absolute Galoisgruppe eines lokalen Körpers ist auflösbar. Nach Induktionsvoraussetzung ist $|Br(L|M)| = [L : M]$ und $|Br(M|K)| = [M : K]$. Außerdem haben wir die exakte Folge

$$0 \to Br(M|K) \to Br(L|K) \to Br(L|M),$$

also

$$|Br(L|K)| \leq |Br(M|K)| \cdot |Br(L|M)| = [M : K] \cdot [L : M] = [L : K].$$

Wegen Satz 1.14 enthält $Br(L|K)$ aber eine zyklische Untergruppe der Ordnung $[L : K]$, muss also gleich dieser zyklischen Untergruppe sein. □

Theorem 1.16. *Es existiert ein eindeutig bestimmer Isomorphismus*

$$inv_K : Br(K) \to \mathbb{Q}/\mathbb{Z},$$

so dass für jede endliche separable Erweiterung $L|K$ das Diagramm

$$\begin{tikzcd}
Br(K) \arrow[r, "res"] \arrow[d, "inv_K"] & Br(L) \arrow[d, "inv_L"] \\
\mathbb{Q}/\mathbb{Z} \arrow[r, "\cdot [L:K]"] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

kommutiert und für jede endliche Galoiserweiterung L/K das Diagramm

$$\begin{tikzcd}
0 \arrow[r] & Br(L/K) \arrow[r, "\mathrm{inf}"] \arrow[d, "inv_{L/K}"] & Br(K) \arrow[r, "res"] \arrow[d, "inv_K"] & Br(L) \arrow[d, "inv_L"] \\
0 \arrow[r] & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \arrow[r] & \mathbb{Q}/\mathbb{Z} \arrow[r, "\cdot[L:K]"] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

kommutiert.

Beweis. Wegen Korollar 1.15 ist für eine endliche galoissche Erweiterung L/K der Kern der Restriktion

$$res : Br(K^{\mathrm{nr}}|K) \to Br(L^{\mathrm{nr}}|L),$$

gleich $Br(L/K)$ (siehe Theorem 1.14). Das heißt wir können $Br(L/K)$ kanonisch als Untergruppe von $Br(K^{\mathrm{nr}}|K)$ auffassen. Außerdem ist

$$Br(K) = \bigcup_{L/K \text{ endl. gal.}} Br(L|K),$$

das heißt $\mathrm{inf} : Br(K^{\mathrm{nr}}|K) \to Br(K)$ is ein Isomorphismus. Wir können also in Satz 1.13 die maximal unverzweigte Erweiterung K^{nr} von K durch einen separablen Abschluss K^{sep} von K ersetzen. Dann folgt die Behauptung. □

Korollar 1.17. *Sei L/K endlich separabel. Dann kommutiert das Diagramm*

$$\begin{tikzcd}
Br(L) \arrow[r, "cor"] \arrow[d, "inv_L"'] & Br(K) \arrow[d, "inv_K"] \\
\mathbb{Q}/\mathbb{Z} \arrow[r, equal] & \mathbb{Q}/\mathbb{Z}.
\end{tikzcd}$$

Beweis. Betrachte das Diagramm

$$\begin{tikzcd}
Br(K) \arrow[r, "res"] \arrow[d, "inv_K"] & Br(L) \arrow[r, "cor"] \arrow[d, "inv_L"] & Br(K) \arrow[d, "inv_K"] \\
\mathbb{Q}/\mathbb{Z} \arrow[r, "\cdot[L:K]"] & \mathbb{Q}/\mathbb{Z} \arrow[r, "\varphi"] & \mathbb{Q}/\mathbb{Z},
\end{tikzcd}$$

wobei φ so gewählt ist, dass das Diagramm kommutiert. Da $cor \circ res = [L:K]$, muss φ die Identität sein. □

Korollar 1.18. *Sei $M/L/K$ ein Turm endlicher Galoiserweiterungen. Dann kommutiert das Diagramm*

$$\begin{tikzcd}
Br(L|K) \arrow[r, hook, "\mathrm{inf}"] \arrow[d, "inv_{L/K}"] & Br(M|K) \arrow[r, "res"] \arrow[d, "inv_{M/K}"] & Br(M|L) \arrow[d, "inv_{M/L}"] \\
\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \arrow[r, hook] & \frac{1}{[M:K]}\mathbb{Z}/\mathbb{Z} \arrow[r, "\cdot[L:K]"] & \frac{1}{[M:L]}\mathbb{Z}/\mathbb{Z}.
\end{tikzcd}$$

Beweis. Das rechte Quadrat kommutiert wegen Theorem 1.16 und das linke wegen Bemerkung 1.12. □

Definition. Sei L/K eine endliche Galoiserweiterung. Das Element

$$inv_{L/K}^{-1}(\frac{1}{[L:K]} + \mathbb{Z}) \in Br(L|K)$$

heißt Fundamentalklasse von L/K.