

Galoiskohomologie algebraischer Gruppen

Holger Kammeyer

LaTeX-Transkription und Übersetzung handschriftlicher Vorlesungsnotizen generiert von ChatGPT 6 Astra. Für die Erstellung der handschriftlichen Originale wurde keine KI verwendet.

Lizenz: CC BY-SA 4.0

<https://creativecommons.org/licenses/by-sa/4.0/deed.de>

Inhaltsverzeichnis

I	Einleitung	1
II	Zahlentheoretische Grundlagen	4
II.1	Zahlkörper	4
II.2	Ganzheit in Zahlkörpern	5
II.3	Die Arithmetik algebraisch ganzer Zahlen	6
II.4	Zerlegung und Verzweigung	8
II.5	Bewertungen und Vervollständigungen	8
II.6	Lokal-global-Prinzipien	11
II.7	Tate–Schafarewitsch-Gruppen	12
III	Galoiskohomologie endlicher abelscher Moduln	14
III.1	Gruppenkohomologie	14
III.2	Tate-Kohomologie	16
III.3	Cup-Produkte	17
III.4	Kohomologie proendlicher Gruppen	18
III.5	Galoiskohomologie	20
III.6	Die Brauergruppe und lokale Dualität	22
III.7	Unverzweigte Kohomologie	24
III.8	Poitou–Tate-Dualität	24
IV	Galoiskohomologie einfacher algebraischer Gruppen	28
IV.1	Nichtkommutative Kohomologie	28
IV.2	Twisten	29
IV.3	Nichtkommutative Galoiskohomologie und Formen	30
IV.4	Affine algebraische Gruppenschemata	31
IV.5	Klassifikation einfacher Gruppen über algebraisch abgeschlossenen Körpern	32
IV.6	Klassifikation einfacher Gruppen über p -adischen Körpern	33
IV.7	Klassifikation einfacher Gruppen über Zahlkörpern	35

Kapitel I

Einleitung

Sei L/K eine (etwa endliche) galoissche Körpererweiterung. Dann wirkt die Galoisgruppe $G = \text{Gal}(L/K)$ auf natürliche Weise auf verschiedenen interessanten Objekten:

- 1.) $G \curvearrowright L$ (durch K -lineare Automorphismen).
- 2.) $G \curvearrowright L^*$ (durch Gruppenautomorphismen).
- 3.) $G \curvearrowright \mu_n(L)$, wobei $\mu_n(L) = \{x \in L^* \mid x^n = 1\} \leq L^*$.
- 4.) $G \curvearrowright \mathbb{Z}/n\mathbb{Z}$ (trivial).
- 5.) $G \curvearrowright M$, wobei M endlich (abelsch) ist und die Wirkung trivial ist.
- 6.) $G \curvearrowright \text{GL}_n(L)$ (auf den Matrixeinträgen, durch Gruppenautomorphismen).
- 7.) $G \curvearrowright \mathbf{G}(L) \leq \text{GL}_n(L)$ (definiert durch Polynome mit K -Koeffizienten).

Man beachte, dass 1.)–6.) Spezialfälle von 7.) sind, das heißt, G wirkt auf den L -Punkten einer algebraischen K -Gruppe $\mathbf{G}$.

Häufig von Interesse: Für eine gegebene Wirkung $G \curvearrowright A$ bestimme man die G -Fixpunkte

$$A^G = \{a \in A \mid \sigma a = a \text{ für alle } \sigma \in G\}.$$

Zum Beispiel ist $\mathbf{G}(L)^G = \mathbf{G}(L) \cap \text{GL}_n(K) =: \mathbf{G}(K)$.

Idee. Untersuche den Funktor $(\cdot)^G$!

Beachte: Ist A eine abelsche Gruppe, so ist sie ein $\mathbb{Z}G$ -Modul. Betrachten wir also zunächst $(\cdot)^G: \mathbb{Z}G\text{-mod} \rightarrow \text{Ab}$.

Lemma I.1. *Ist $0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0$ exakt in $\mathbb{Z}G\text{-mod}$, so ist auch $0 \rightarrow A^G \rightarrow B^G \rightarrow C^G$ exakt in Ab .*

Beweis. Sei $b \in \ker g \cap B^G$. Dann gibt es $a \in A$ mit $f(a) = b$. Es gilt aber $f(\sigma a - a) = \sigma f(a) - f(a) = 0$ und $\ker f = 0$, also $a \in A^G$. $\square$

Also ist $(\cdot)^G$ linksexakt. Ist er vielleicht auch rechtsexakt?

Seien $c \in C^G$ und $b \in B$ mit $g(b) = c$. Wir wissen nur, dass $\sigma b - b \in A$ (wobei wir f als Inklusion $A \leq B$ auffassen). Wir erhalten also eine Abbildung

$$G \rightarrow A, \quad \sigma \mapsto \sigma b - b =: a_\sigma,$$

für die

$$a_{\sigma\tau} = \sigma\tau b - b = (\sigma b - b) + \sigma(\tau b - b) = a_\sigma + \sigma a_\tau,$$

gilt, also einen 1-Kozyklus $a_\sigma \in Z^1(G, A)$. Hätten wir statt b den Vertreter $b + a'$ ($a' \in A$) gewählt, so würde sich a_σ um den Kozyklus $\sigma a' - a'$ unterscheiden. Wir definieren daher die 1-Koränder als die Untergruppe

$$B^1(G, A) = \{a_\sigma \in Z^1(G, A) \mid \exists a' \in A : a_\sigma = \sigma a' - a'\}.$$

Die Obstruktion dafür, dass $c \in C^G$ ein Urbild in B^G hat, ist also gegeben durch

$$\delta(c) := [a_\sigma] \in H^1(G, A) := Z^1(G, A)/B^1(G, A),$$

das heißt,

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \xrightarrow{\delta} H^1(G, A)$$

ist exakt in Ab.

Übung. Zeige, dass $H^1(G, \cdot)$ funktoriell ist und

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \xrightarrow{\delta} H^1(G, A) \longrightarrow H^1(G, B) \longrightarrow H^1(G, C)$$

exakt und natürlich ist. Finde ein Beispiel mit $\delta \neq 0$.

Mithilfe injektiver Auflösungen kann man rechtsabgeleitete Funktoren $H^i(G, \cdot)$ definieren, die die exakte Sequenz fortsetzen. Daher ist es sinnvoll, $H^0(G, \cdot) := (\cdot)^G$ zu setzen.

Kehren wir zu einem möglicherweise nichtabelschen A zurück (zum Beispiel $G \curvearrowright A = \mathbf{G}(L) \leq \mathrm{GL}_n(L)$), so sehen wir, dass wir nichtkommutative Versionen des Obigen benötigen. Die Verträglichkeit mit dem abelschen Fall legt nahe, Folgendes zu setzen:

$$H^0(G, A) = A^G, \quad H^1(G, A) = Z^1(G, A)/\sim,$$

mit

$$Z^1(G, A) = \{a_\sigma : G \longrightarrow A \mid a_{\sigma\tau} = a_\sigma {}^\sigma a_\tau\}$$

und

$$a_\sigma \sim b_\sigma \iff \exists a' \in A : b_\sigma = (a')^{-1} a_\sigma {}^\sigma a'.$$

Achtung. $H^1(G, A)$ ist nur eine punktierte Menge! Aber:

Proposition I.2. Für $A \leq_G B$ erhalten wir $G \curvearrowright B/A$, und

$$1 \longrightarrow H^0(G, A) \longrightarrow H^0(G, B) \longrightarrow H^0(G, B/A) \longrightarrow H^1(G, A) \longrightarrow H^1(G, B)$$

ist exakt (Urbild eines Basispunktes = Bild des vorhergehenden Pfeils).

Beweis. Wie zuvor. □

Besonderheit

Ist X ein „ K -Objekt“, so gilt

$$H^1(G, \mathrm{Aut}_L X) \xleftarrow{1:1} \{Y \mid Y \cong_L X\} / \cong_K$$

(vergleiche Meta-Satz IV.3.1).

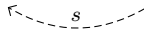
Klassifikationsstrategie: Zunächst bis auf „ $\cong_L$ “ klassifizieren (typischerweise $L = \overline{K}$ oder K_{sep}), dann für jeden L -Typ X eine geeignete K -Form X_0 finden und $H^1(G, \mathrm{Aut}_L X_0)$ berechnen.

In unserem Fall: $\mathbf{G}$ ist eine einfache, 1-zusammenhängende lineare algebraische K -Gruppe.

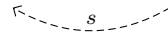
- Klassifikation bis auf „ $\cong_{\overline{K}}$ “ mittels Dynkin-Diagrammen Δ .

- Sei $\mathbf{G}_0$ eine K -zerfallende Gruppe mit gegebenem Dynkin-Diagramm Δ . Betrachte die kurze exakte Sequenz der inneren und äußeren Automorphismen:

$$1 \longrightarrow \mathrm{Ad} \mathbf{G}_0 \longrightarrow \mathrm{Aut} \mathbf{G}_0 \xrightarrow{\quad} \mathrm{Sym} \Delta \longrightarrow 1.$$



$$1 \longrightarrow H^1(G, \mathrm{Ad} \mathbf{G}_0) \longrightarrow H^1(G, \mathrm{Aut} \mathbf{G}_0) \xrightarrow{p} H^1(G, \mathrm{Sym} \Delta) \longrightarrow 1.$$



- im $s \xleftarrow{1:1}$ K -quasizerfallende Formen von $\mathbf{G}$.
- $p^{-1}(\alpha) \xleftarrow{1:1} H^1(G, \mathrm{Ad} \mathbf{G}_1)/\Gamma_\alpha$, wobei $\alpha = [a]$, $\mathbf{G}_1$ die zu $s(\alpha)$ gehörige K -quasizerfallende Gruppe und $\Gamma_\alpha = {}_a(\mathrm{Sym} \Delta)(K)$ die Gruppe der K -rationalen Automorphismen des getwisteten Dynkin-Diagramms ist (siehe Abschnitt IV.6).
- Betrachte $1 \longrightarrow Z(\mathbf{G}_1) \longrightarrow \mathbf{G}_1 \longrightarrow \mathrm{Ad} \mathbf{G}_1 \longrightarrow 1$:

$$H^1(G, \mathbf{G}_1) \longrightarrow H^1(G, \mathrm{Ad} \mathbf{G}_1) \longrightarrow H^2(G, Z(\mathbf{G}_1)).$$

- Satz (Kneser, 1960er-Jahre): K p -adisch $\implies H^1(G, \mathbf{G}_1) = 1$. Also $H^1(G, \mathrm{Ad} \mathbf{G}_1) \cong H^2(G, Z(\mathbf{G}_1))$; Berechnung möglich.
- k : Zahlkörper $\implies$ Lokal-global-Prinzip

$$H^2(\mathrm{Gal}(k), M) \hookrightarrow \prod_v H^2(\mathrm{Gal}(k_v), M)$$

für gewisse endliche abelsche M , nach der „Poitou–Tate-Dualität“.

Vorlesungsübersicht

Zahlentheoretisches Handwerkszeug; Galoiskohomologie endlicher abelscher Moduln; Galoiskohomologie einfacher algebraischer Gruppen.

Grundlagen aus der algebraischen Zahlentheorie

II.1 Zahlkörper

Definition II.1.1. Ein *algebraischer Zahlkörper* ist eine endliche Körpererweiterung $k/\mathbb{Q}$.

- Satz vom primitiven Element $\implies k = \mathbb{Q}(a)$ für ein $a \in k$ mit (eindeutigem) Minimalpolynom $f \in \mathbb{Q}[X]$ vom Grad $d = [k : \mathbb{Q}]$.
- Die Nullstellen $\{a_1, \dots, a_d\} \subseteq \overline{\mathbb{Q}} \subseteq \mathbb{C}$ von f heißen die (Galois-)Konjugierten von a .
- Die Vorschrift $a \mapsto a_i$ definiert $\mathbb{Q}(a) \cong \mathbb{Q}(a_i)$, und jede Einbettung $\mathbb{Q}(a) \hookrightarrow \mathbb{C}$ muss a auf ein a_i abbilden. Es gibt also genau d Einbettungen $\sigma_i: k \hookrightarrow \mathbb{C}$.
- Beachte, dass $\{a_1, \dots, a_d\} = \{\bar{a}_1, \dots, \bar{a}_d\}$, also $\sigma_i(k) \subseteq \mathbb{R}$ genau dann, wenn $\bar{a}_i = a_i$.
Setze

$$r_1 := \#\{\text{reelle Einbettungen von } k\} \quad (\text{„reelle Stellen“}),$$

$$r_2 := \#\{\{\sigma_i, \bar{\sigma}_i\} \mid \sigma_i(k) \not\subseteq \mathbb{R}\} \quad (\text{„komplexe Stellen“}).$$

Dann ist $d = r_1 + 2r_2$.

Beispiel. $\mathbb{Q}(\sqrt[3]{2})$: $r_1 = 1$, $r_2 = 1$. Für $\mathbb{Q}(e^{2\pi i/n})$ mit $n \geq 3$: $r_1 = 0$, $r_2 = \varphi(n)/2$.

Definition II.1.2. Für $\alpha \in k$ heißen die rationalen Zahlen

$$N_{k/\mathbb{Q}}(\alpha) = \sigma_1(\alpha) \cdots \sigma_d(\alpha), \quad \text{Tr}_{k/\mathbb{Q}}(\alpha) = \sigma_1(\alpha) + \cdots + \sigma_d(\alpha)$$

die *Norm* und die *Spur* von α .

Seien $\alpha_1, \dots, \alpha_d \in k$ und $\lambda_1, \dots, \lambda_d \in \mathbb{Q}$. Dann gilt

$$\lambda_1 \alpha_1 + \cdots + \lambda_d \alpha_d = 0 \iff \lambda_1 \sigma_i(\alpha_1) + \cdots + \lambda_d \sigma_i(\alpha_d) = 0$$

für alle i . Mit der linearen Unabhängigkeit der Einbettungen σ_i erhalten wir

$$\{\alpha_i\} \text{ eine Basis von } k \iff \det(\sigma_i(\alpha_j)) \neq 0.$$

Definition II.1.3. Die *Diskriminante* einer Basis $\{\alpha_i\} \subseteq k$ ist

$$\text{discr}\{\alpha_1, \dots, \alpha_d\} = \det(\sigma_i(\alpha_j))^2 \in \mathbb{Q}.$$

Übung.

$$\text{discr}\{\alpha_1, \dots, \alpha_d\} = \det(\text{Tr}_{k/\mathbb{Q}}(\alpha_i \alpha_j)).$$

Zeige für $k = \mathbb{Q}(a)$, dass

$$\text{discr}\{1, a, \dots, a^{d-1}\} = \prod_{i < j} (\sigma_i(a) - \sigma_j(a))^2.$$

Definiere analog für l/k die Diskriminante $\text{discr}_{l/k}$ mithilfe derjenigen $\sigma_i: l \hookrightarrow \mathbb{C}$ mit $\sigma_i|_k = \text{id}_k$.

II.2 Ganzheit in Zahlkörpern

Von nun an sei k ein Zahlkörper.

Definition II.2.1. Der *Ring der ganzen Zahlen* in k ist gegeben durch

$$\mathcal{O}_k = \{\alpha \in k \mid f(\alpha) = 0 \text{ für ein normiertes } f \in \mathbb{Z}[X]\}.$$

Beispiel. $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$ (Lemma von Gauß).

„ $\mathcal{O}_k$ verhält sich zu k wie $\mathbb{Z}$ zu $\mathbb{Q}$.“ Dabei besteht $\mathcal{O}_k$ aus den algebraisch ganzen Zahlen in k und $\mathbb{Z}$ aus den rationalen ganzen Zahlen.

Proposition II.2.2. Seien $\alpha_1, \dots, \alpha_r \in k$. Dann gilt

$$\alpha_1, \dots, \alpha_r \in \mathcal{O}_k \iff \mathbb{Z}[\alpha_1, \dots, \alpha_r] \text{ ist als } \mathbb{Z}\text{-Modul endlich erzeugt.}$$

Korollar II.2.3. $\mathcal{O}_k$ ist ein Ring.

Beweis. $\mathbb{Z}[\alpha_1, \alpha_2, \alpha_1 + \alpha_2, \alpha_1 \alpha_2] = \mathbb{Z}[\alpha_1, \alpha_2]$. □

Lemma II.2.4. Für $\alpha \in k$ gibt es $\beta \in \mathcal{O}_k$, $0 \neq m \in \mathbb{Z}$ mit $\alpha = \beta/m$.

Beweis. $a_n \alpha^n + \dots + a_0 = 0$, $a_i \in \mathbb{Z}$. Multiplikation mit a_n^{n-1} ergibt $(a_n \alpha)^n + \dots + a_n^{n-1} a_0 = 0$, also $a_n \alpha \in \mathcal{O}_k$. □

Von nun an können und werden wir $k = \mathbb{Q}(a)$ mit $a \in \mathcal{O}_k$ annehmen.

Proposition II.2.5.

$$\mathbb{Z}[a] \subseteq \mathcal{O}_k \subseteq \frac{1}{\text{discr}(1, \dots, a^{d-1})} \mathbb{Z}[a].$$

Hier ist $\text{discr}(1, \dots, a^{d-1}) \in \mathcal{O}_k \cap \mathbb{Q} = \mathbb{Z}$.

Beweis. Schreibe $\mathcal{O}_k \ni \alpha = \lambda_0 \cdot 1 + \dots + \lambda_{d-1} a^{d-1}$ mit $\lambda_j \in \mathbb{Q}$. Multiplikation mit a^i und Anwendung von $\text{Tr}_{k/\mathbb{Q}}$ ergeben

$$\underbrace{\text{Tr}_{k/\mathbb{Q}}(a^i \alpha)}_{\in \mathbb{Z}} = \sum_{j=0}^{d-1} \text{Tr}_{k/\mathbb{Q}}(a^i a^j) \lambda_j.$$

Die Koeffizientenmatrix hat die Determinante $\text{discr}\{a^i\}$, also $\lambda_j \in \frac{1}{\text{discr}\{a^i\}} \mathbb{Z}$. □

Korollar II.2.6. $\mathcal{O}_k$ hat eine $\mathbb{Z}$ -Basis vom Rang d .

Jede solche heißt *Ganzheitsbasis*.

Korollar II.2.7. $\mathcal{O}_k$ ist noethersch.

Beweis. $\mathfrak{a} \subseteq \mathcal{O}_k$ ist endlich erzeugt in $\mathbb{Z}\text{-mod}$, also endlich erzeugt in $\mathcal{O}_k\text{-mod}$. □

Definition II.2.8. Die *Diskriminante* von k ist gegeben durch

$$\text{discr}_k = d_k = \text{discr}\{\alpha_1, \dots, \alpha_d\}$$

für eine Ganzheitsbasis $\{\alpha_i\}$.

Dies ist wohldefiniert, denn $\det(T_{\{\alpha_i\}}^{\{\beta_i\}}) = \pm 1$. Allgemeiner gilt

$$\mathfrak{d}_{l/k} = (\text{discr}\{\beta_i\} \mid \beta_i \in \mathcal{O}_l, \{\beta_i\} \text{ eine Basis von } l) \subseteq \mathcal{O}_k.$$

Übung. Sei $k = \mathbb{Q}(\sqrt{D})$ für eine quadratfreie ganze Zahl $D \neq 1$.

	Ganzheitsbasis	d_k
$D \equiv 1 \pmod{4}$	$1, \frac{1 + \sqrt{D}}{2}$	D
$D \equiv 2, 3 \pmod{4}$	$1, \sqrt{D}$	$4D$

II.3 Die Arithmetik algebraisch ganzer Zahlen

Betrachten wir das Beispiel $k = \mathbb{Q}(\sqrt{-5})$, also $\mathcal{O}_k = \mathbb{Z}[\sqrt{-5}]$. In $\mathcal{O}_k$ gilt

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}),$$

und alle diese Faktoren sind irreduzibel. Sei zum Beispiel $3 = \alpha\beta$, $\alpha, \beta \notin \mathcal{O}_k^*$. Dann ist $N_{k/\mathbb{Q}}(\alpha)N_{k/\mathbb{Q}}(\beta) = 9$, also $N_{k/\mathbb{Q}}(\alpha) = \pm 3$, denn nur Einheiten haben Norm ± 1 . Aber

$$N_{k/\mathbb{Q}}(x + y\sqrt{-5}) = x^2 + 5y^2 \not\equiv 3 \pmod{4}.$$

Schlechte Nachricht: $\mathcal{O}_k$ ist kein faktorieller Ring!

Kummers Ausweg

In einer idealen Welt gäbe es ideale Zahlen $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4$ mit

$$\begin{aligned} (3) &= \mathfrak{p}_1\mathfrak{p}_2, & (7) &= \mathfrak{p}_3\mathfrak{p}_4, \\ (1 + 2\sqrt{-5}) &= \mathfrak{p}_1\mathfrak{p}_3, & (1 - 2\sqrt{-5}) &= \mathfrak{p}_2\mathfrak{p}_4. \end{aligned}$$

Also $(21) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4 = \mathfrak{p}_1\mathfrak{p}_3\mathfrak{p}_2\mathfrak{p}_4$: eindeutige Zerlegung!

Offenbar folgt aus $\mathfrak{p}_1 \mid 3$, $\mathfrak{p}_1 \mid 1 + 2\sqrt{-5}$, dass $\mathfrak{p}_1 \mid \lambda \cdot 3 + \mu(1 + 2\sqrt{-5})$, und $\mathfrak{p}_1$ sollte durch die Menge aller $\alpha \in \mathcal{O}_k$ bestimmt sein, die es teilt. Setze also

$$\mathfrak{p}_1 = (3, 1 + 2\sqrt{-5}), \quad \mathfrak{p}_2 = (3, 1 - 2\sqrt{-5}), \quad \dots$$

Satz II.3.1. *Der Ring $\mathcal{O}_k$ ist*

- 1.) *noethersch,*
- 2.) *ganzabgeschlossen: Aus $\alpha \in k$, $f(\alpha) = 0$ für ein normiertes $f \in \mathcal{O}_k[X]$ folgt $\alpha \in \mathcal{O}_k$,*
- 3.) *und von null verschiedene Primideale sind maximal.*

Definition II.3.2. Ein Integritätsring mit 1.), 2.), 3.) heißt *Dedekindring*.

Satz II.3.3 (Dedekind). *Jedes Ideal $\mathfrak{a} \neq (0), (1)$ in einem Dedekindring $\mathcal{O}$ hat eine eindeutige Zerlegung $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ in Primideale $\mathfrak{p}_i \subseteq \mathcal{O}$.*

Wie erhalten wir Inverse von Idealen? Sei $\mathcal{O}$ ein Dedekindring mit Quotientenkörper K .

Definition II.3.4. Ein *gebrochenes Ideal* von K ist ein endlich erzeugter $\mathcal{O}$ -Untermodul $\mathfrak{a} \neq (0)$ von K .

Beispiel. $(a) = a\mathcal{O}$ für jedes $a \in K^*$. Jedes von null verschiedene (ganze) Ideal $\mathfrak{a} \subseteq \mathcal{O}$.

Beachte: Ein von null verschiedener $\mathcal{O}$ -Untermodul $\mathfrak{a} \subseteq K$ ist genau dann ein gebrochenes Ideal, wenn es $0 \neq c \in \mathcal{O}$ mit $c\mathfrak{a} \subseteq \mathcal{O}$ gibt.

Damit sehen wir, dass für $\mathfrak{a} \neq 0$ auch

$$\mathfrak{a}^{-1} := \{x \in K \mid x\mathfrak{a} \subseteq \mathcal{O}\}$$

ein gebrochenes Ideal ist. Definieren wir $\mathfrak{a}\mathfrak{b}$ wie üblich, so gilt $(1)\mathfrak{a} = \mathfrak{a}$ und $\mathfrak{a}\mathfrak{a}^{-1} = (1)$.

Satz II.3.5. Die gebrochenen Ideale bilden eine abelsche Gruppe, die Idealgruppe J_K von K .

Korollar II.3.6. Für $\mathfrak{a} \in J_K$ gilt eindeutig

$$\mathfrak{a} = \prod_{\substack{0 \neq \mathfrak{p} \\ \text{prim}}} \mathfrak{p}^{v_{\mathfrak{p}}}$$

mit $v_{\mathfrak{p}} \in \mathbb{Z}$ (fast alle null).

Also ist J_K frei abelsch mit Basis $(\text{Spec } \mathcal{O}) \setminus \{(0)\}$. Sei $P_K = \{(a) \mid a \in K^*\} \leq J_K$ die Untergruppe der gebrochenen Hauptideale.

Definition II.3.7. Die (Ideal-)Klassengruppe von K ist $\text{Cl}_K = J_K/P_K$.

Also ist

$$\begin{aligned} 1 &\longrightarrow \mathcal{O}^* \longrightarrow K^* \longrightarrow J_K \longrightarrow \text{Cl}_K \longrightarrow 1 \\ a &\longmapsto (a) \end{aligned}$$

exakt. Damit beschreibt Cl_K den Gewinn und $\mathcal{O}^*$ den Verlust beim Übergang von Zahlen zu Ideal(zahl)en. Wir müssen Cl_K und $\mathcal{O}^*$ untersuchen! Zurück zu $K = k$ und $\mathcal{O} = \mathcal{O}_k$.

Satz II.3.8 (Gauß, Minkowski). Cl_k ist endlich.

Wir nennen $h_k = |\text{Cl}_k|$ die Klassenzahl von k .

Beispiel. Sei $D > 0$ quadratfrei. Dann gilt

$$h_{\mathbb{Q}(\sqrt{-D})} = 1 \iff D \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}.$$

(Vermutung: Gauß; Beweis: Baker–Stark–Heegner.)

Offen: Gibt es unendlich viele D mit $h_{\mathbb{Q}(\sqrt{D})} = 1$?

Satz II.3.9 (Dirichlet). $\mathcal{O}_k^* \cong \mu(k) \oplus \mathbb{Z}^{r_1+r_2-1}$, wobei $\mu(k)$ die Gruppe der Einheitswurzeln in k ist.

Beweise von II.3.8 und II.3.9: „Geometrie der Zahlen“.

Übung. Zeige, dass $\mathcal{O}_k/\mathfrak{a}$ für jedes Ideal $(0) \neq \mathfrak{a} \subseteq \mathcal{O}_k$ endlich ist. Hinweis: Nimm zunächst an, dass $\mathfrak{a} = \mathfrak{p}$ ein Primideal ist. (Dies beweist auch II.3.1(3).)

Definition II.3.10. Die (absolute) Norm von $(0) \neq \mathfrak{a} \subseteq \mathcal{O}_k$ ist $n(\mathfrak{a}) = |\mathcal{O}_k/\mathfrak{a}|$.

Übung. Für $0 \neq a \in \mathcal{O}_k$ gilt $n((a)) = |N_{k/\mathbb{Q}}(a)|$. Außerdem gilt $n(\mathfrak{a}\mathfrak{b}) = n(\mathfrak{a})n(\mathfrak{b})$ (Hinweis: chinesischer Restsatz). Gewinne daraus einen Homomorphismus $n: J_k \longrightarrow \mathbb{R}_{>0}^*$.

II.4 Zerlegung und Verzweigung

Sei p eine rationale Primzahl. Dann gilt

$$p\mathcal{O}_k = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}. \quad (*)$$

Beachte, dass $\mathcal{O}_k/\mathfrak{p}_i$ ein endlicher Körper ist, also $n(\mathfrak{p}_i) = p_i^{f_i}$. Wende n auf $(*)$ an: $p^d = p_1^{f_1 e_1} \cdots p_r^{f_r e_r}$, also ist $p_i = p$ und

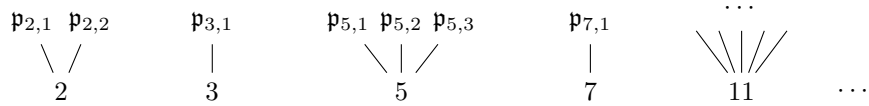
$$f_1 e_1 + \cdots + f_r e_r = d \quad (\text{„Fundamentalgleichung“}).$$

Dabei ist e_i der *Verzweigungsindex* von $\mathfrak{p}_i$ über p und f_i der *Trägheitsgrad* von $\mathfrak{p}_i$ über p .

Extremfälle:

- $r = d$: „ p ist vollständig zerlegt“.
- $r = 1, f_1 = 1$: „ p ist total verzweigt“.
- $r = 1, e_1 = 1$: „ p ist träge“.

Beachte $p\mathcal{O}_k \subseteq \mathfrak{p}_i$ ($\iff \mathfrak{p}_i \mid p$) für ein eindeutiges p : „ $\mathfrak{p}_i$ liegt über p “.



Definition II.4.1. $\mathfrak{p}$ heißt *verzweigt* in k , wenn $e_{\mathfrak{p}} > 1$. Eine rationale Primzahl p heißt *verzweigt* in k , wenn $e_{\mathfrak{p}} > 1$ für ein $\mathfrak{p} \mid p$.

Satz II.4.2. Eine rationale Primzahl p ist genau dann verzweigt in k , wenn $p \mid d_k$.

Korollar II.4.3. Fast alle p sind unverzweigt.

Bemerkung. Ist $k/\mathbb{Q}$ galoissch und $\sigma \in \text{Gal}(k/\mathbb{Q})$, so gilt $\sigma(\mathcal{O}_k) = \mathcal{O}_k$ und

$$\sigma(\mathfrak{p}) \cap \mathbb{Z} = \sigma(\mathfrak{p} \cap \mathbb{Z}) = \sigma((p)) = (p),$$

also permutiert $\text{Gal}(k/\mathbb{Q})$ die Prim(ideale) über p . Die Wirkung ist transitiv (Übung!) und erhält e_i und f_i , also nimmt die Fundamentalgleichung die Form $e \cdot f \cdot r = d$ an. Ist $k/\mathbb{Q}$ zyklisch von Primzahlgrad, so können nur die obigen Extremfälle auftreten.

II.5 Bewertungen und Vervollständigungen

Definition II.5.1. Eine *Bewertung* von k ist eine Abbildung $|\cdot|: k \rightarrow \mathbb{R}$, sodass für alle $x, y \in k$ gilt:

- 1.) $|x| \geq 0$ und $|x| = 0 \iff x = 0$,
- 2.) $|xy| = |x| |y|$,
- 3.) $|x + y| \leq |x| + |y|$.

(Wir schließen die triviale Bewertung $|x| = 1$ für alle $x \in k^*$ aus.) Erfüllt $|\cdot|$ die stärkere Bedingung

$$3'.) \quad |x + y| \leq \max\{|x|, |y|\},$$

so heißt $|\cdot|$ *nichtarchimedisch*, andernfalls *archimedisch*.

Beispiele. *Archimedisch:* Sei $\sigma: k \hookrightarrow \mathbb{C}$ und setze $|x|_\sigma := |\sigma(x)|$.

Nichtarchimedisch: Sei $0 \neq \mathfrak{p}_0 \subseteq \mathcal{O}_k$ ein Primideal. Schreibe für $x \in k^*$ die Zerlegung $x\mathcal{O}_k = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(x)}$ und setze

$$|x|_{\mathfrak{p}_0} := q^{-v_{\mathfrak{p}_0}(x)}, \quad q = |\mathcal{O}_k/\mathfrak{p}_0| = p^{f_{\mathfrak{p}_0}} \quad \text{für } \mathfrak{p}_0 \cap \mathbb{Z} = (p).$$

„ $\mathfrak{p}$ -adische Bewertung.“

Definition II.5.2.

$$|\cdot|_1 \sim |\cdot|_2 \iff \exists a > 0: |\cdot|_1 = |\cdot|_2^a.$$

Äquivalent dazu definieren $d_i(x, y) := |y - x|_i$ dieselben Topologien auf k .

Satz II.5.3 (Ostrowski). *Die obigen Beispiele erfassen alle Bewertungen auf k bis auf „ $\sim$ “.*

Definition II.5.4. Die $\sim$ -Klassen von (nichtarchimedischen / archimedischen) Bewertungen auf k heißen (endliche / unendliche) *Stellen*.

Notation: $V(k) = V_\infty(k) \cup V_f(k)$ (Menge der Stellen). Beachte $|V_\infty(k)| = r_1 + r_2$, da komplex konjugierte Einbettungen dieselbe archimedische Bewertung definieren. Wir schreiben wahlweise $v \in V(k)$ oder $\mathfrak{p} \in V(k)$.

Vorzüge der Stellen:

- Die unendlichen Stellen „vervollständigen das Bild“:

$$\prod_{v \in V(k)} |x|_v^{n_v} = 1 \quad \text{für alle } x \in k^*, \quad n_v = \begin{cases} 2 & v \text{ komplex,} \\ 1 & \text{sonst.} \end{cases}$$

- Sie ermöglichen die *Vervollständigung*, sodass auch $v \in V_f(k)$ einer Einbettung „ $k \hookrightarrow k_v$ “ in einen vollständigen Körper k_v entspricht.

Definition II.5.5. $k \hookrightarrow k_v$ ist die Vervollständigung von k bezüglich $d_v(x, y) = |y - x|_v$:

$$k_v = \frac{\{\text{Cauchyfolgen in } k\}}{\{\text{Nullfolgen in } k\}}, \quad k \hookrightarrow k_v \quad (\text{konstante Folgen}).$$

v setzt sich auf k_v fort: (x_n) Cauchyfolge $\implies (v(x_n)) \subseteq \mathbb{R}$ Cauchyfolge.

Beispiel. $k = \mathbb{Q}$, $v = p$:

$$k_v = \mathbb{Q}_p \cong \text{Frac}\left(\varprojlim_k \mathbb{Z}/p^k\mathbb{Z}\right),$$

„ p -adische Zahlen“. Allgemeiner nennen wir für $\mathfrak{p} \in V_f(k)$ den Körper $k_{\mathfrak{p}}$ einen *p -adischen Körper*.

Definition II.5.6. Sei $v \in V_f(k)$. Dann heißen

$$\mathcal{O}_{(v)} = \{x \in k \mid v(x) \leq 1\} \subseteq k, \quad \mathcal{O}_v = \{x \in k_v \mid v(x) \leq 1\} \subseteq k_v$$

die *Bewertungsringe* der bewerteten Körper k beziehungsweise k_v .

Beachte, dass $\mathcal{O}_{(v)} = \mathcal{O}_v \cap k$ und $\mathcal{O}_v = \overline{\mathcal{O}_{(v)}}$. Die Ringe $\mathcal{O}_v$ und $\mathcal{O}_{(v)}$ sind Hauptidealringe mit eindeutigen maximalen Idealen

$$\pi\mathcal{O}_{(v)} = \{x \in \mathcal{O}_{(v)} \mid v(x) < 1\}, \quad \pi\mathcal{O}_v = \{x \in \mathcal{O}_v \mid v(x) < 1\},$$

also sind sie *diskrete Bewertungsringe* (DVR). Das bis auf Assoziiertheit eindeutige Element $\pi \in \mathcal{O}_{(v)} \subseteq \mathcal{O}_v$ heißt eine *Uniformisierende*. Wir haben einen kanonischen Isomorphismus

$$\mathcal{O}_{(v)}/\pi\mathcal{O}_{(v)} \xrightarrow{\cong} \mathcal{O}_v/\pi\mathcal{O}_v$$

der *Restklassenkörper*.

Satz II.5.7. *Sei K vollständig bezüglich der Bewertung v und L/K algebraisch. Dann lässt sich v eindeutig auf L fortsetzen. Ist $d = [L : K] < \infty$, so gilt $\bar{v}(x) = \sqrt[d]{v(N_{L/K}(x))}$.*

Beweis. Hensels Lemma. □

Insbesondere setzt sich v_p auf $\mathbb{Q}_p$ eindeutig zu $\bar{v}_p$ auf $\overline{\mathbb{Q}_p}$ fort. Für $\sigma: k \hookrightarrow \overline{\mathbb{Q}_p}$ erhalten wir $v_\sigma := \bar{v}_p \circ \sigma$. Ist $\tau \in \text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$, so gilt $\bar{v}_p = \bar{v}_p \circ \tau$, also $v_\sigma = v_{\tau \circ \sigma}$.

Satz II.5.8. 1.) *Jede Fortsetzung w von v_p von $\mathbb{Q}$ auf k hat die Form $w = v_\sigma$ für ein $\sigma: k \hookrightarrow \overline{\mathbb{Q}_p}$.*

2.) *Es gilt $v_\sigma = v_{\sigma'}$ genau dann, wenn es ein $\tau \in \text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ mit $\sigma' = \tau \circ \sigma$ gibt.*

Bemerkung. Dies gilt auch für $p = \infty$, wobei $\mathbb{Q}_\infty = \mathbb{R}$.

Komplexe unendliche Stellen $\xleftrightarrow{1:1}$ Konjugationsklassen von $k \xrightarrow{\sigma} \mathbb{C}$, $\sigma(k) \not\subseteq \mathbb{R}$,

Reelle unendliche Stellen $\xleftrightarrow{1:1}$ Einbettungen $k \xrightarrow{\sigma} \mathbb{R}$,

Endliche Stellen über $p \xleftrightarrow{1:1}$ Konjugationsklassen von $k \xrightarrow{\sigma} \overline{\mathbb{Q}_p}$,

$\xleftrightarrow{1:1}$ Primideale $0 \neq \mathfrak{p} \subseteq \mathcal{O}_k$ mit $\mathfrak{p} \mid p$.

Außerdem gilt $k_w = \sigma(k) \cdot \mathbb{Q}_p \subseteq \overline{\mathbb{Q}_p}$ für $w = v_\sigma$, also

$$\begin{array}{ccc} k & \longrightarrow & k_w \\ \text{global} \uparrow & & \uparrow \text{lokal} \\ \mathbb{Q} & \longrightarrow & \mathbb{Q}_p \end{array}$$

Satz II.5.9. *Es gilt $k \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \prod_{w|p} k_w$ und $[k_w : \mathbb{Q}_p] = e_w f_w$ für $p < \infty$.*

Beweis. Sei $k = \mathbb{Q}(a)$ mit Minimalpolynom $f \in \mathbb{Q}[X]$. Dann ist $f(X) = \prod_{v|p} f_v(X)$ über $\mathbb{Q}_p$, und der chinesische Restsatz liefert

$$\begin{array}{ccc} \mathbb{Q}_p[X]/(f) & \xrightarrow{\cong} & \prod_{v|p} \mathbb{Q}_p[X]/(f_v) \\ \cong \downarrow & & \downarrow \cong \\ k \otimes_{\mathbb{Q}} \mathbb{Q}_p & \longrightarrow & \prod_{v|p} k_v. \end{array}$$

□

Definition II.5.10. Der *Adelring* von k ist $\mathbb{A}_k = \prod'_{v \in V(k)} k_v$ (fast alle Koordinaten liegen in $\mathcal{O}_v$). Die *Idelgruppe* ist $\mathbb{I}_k = \mathbb{A}_k^*$.

Wir haben diagonale Einbettungen $k \hookrightarrow \mathbb{A}_k$, $k^* \hookrightarrow \mathbb{I}_k$ mit diskretem Bild, wobei $\mathbb{A}_k$ die folgende Basis offener Mengen hat:

$$\prod_{v \in V(k)} U_v, \quad U_v \subseteq k_v \text{ offen und } U_v = \mathcal{O}_v \text{ für fast alle } v.$$

Analog für $\mathbb{I}_k$ mit $U_v \subseteq k_v^*$ und $U_v = \mathcal{O}_v^*$ für fast alle v . (Nicht die Teilraumtopologie von $\mathbb{I}_k \subseteq \mathbb{A}_k^*$!)

II.6 Lokal-global-Prinzipien

Idee. Sei $p \in k[X]$. Angenommen, $x \in k$ erfüllt $p(x) = 0$. Dann definiert $x \in k \subseteq k_v$ natürlich eine Lösung $x \in k_v$ von $p(x) = 0$. Wenn wir umgekehrt für alle $v \in V(k)$ eine lokale Lösung $x_v \in k_v$ mit $p(x_v) = 0$ finden, folgt daraus die Existenz einer globalen Lösung $x \in k$ mit $p(x) = 0$?

Satz II.6.1 (Globaler Quadratsatz). *Ja, falls $p(X) = X^2 - a$ für ein $a \in k^*$. Tatsächlich ist $a \in k^*$ genau dann global ein Quadrat, wenn es für fast alle $v \in V(k)$ lokal ein Quadrat ist.*

Satz II.6.2 (Hasse–Minkowski). *Sei $f(X_1, \dots, X_n) = a_1 X_1^2 + \dots + a_n X_n^2$ mit $a_i \in k$ eine quadratische Form. Dann existiert genau dann ein $0 \neq X \in k^n$ mit $f(X) = 0$, wenn für alle $v \in V(k)$ ein $0 \neq X_v \in k_v^n$ mit $f(X_v) = 0$ existiert.*

Satz II.6.3 (Hassesches Normprinzip). *Sei $k/\mathbb{Q}$ zyklisch und $x \in \mathbb{Q}$. Dann gilt $x = N_{k/\mathbb{Q}}(y)$ für ein $y \in k$ genau dann, wenn $x = N_{k_v/\mathbb{Q}_p}(y_v)$ für ein $y_v \in k_v$ für alle $v \mid p$ und Primstellen $p \leq \infty$ gilt.*

Vorsicht

1.) II.6.1 besagt

$$k^*/(k^*)^2 \xrightarrow{\text{diag.}} \prod_{v \notin S} k_v^*/(k_v^*)^2$$

für alle endlichen $S \subseteq V(k)$. Gilt

$$k^*/(k^*)^n \hookrightarrow \prod_{v \notin S} k_v^*/(k_v^*)^n \quad (*)$$

für alle $n \geq 2$? Nein: In $k = \mathbb{Q}(\sqrt{7})$ ist 16 überall lokal eine 8-te Potenz, aber nicht global.

Satz II.6.4 (Grunwald–Wang, 1933, 1948). *(*) gilt außer in gewissen „speziellen“ Fällen, die von (k, S, n) abhängen und nur auftreten können, wenn $8 \mid n$ (und dann ist $\ker \cong \mathbb{Z}/2$).*

- 2.) Auch II.6.2 lässt sich nicht verallgemeinern: $3X^3 + 4Y^3 + 5Z^3$ stellt die Null in allen $\mathbb{Q}_p$ dar, aber nicht in $\mathbb{Q}$ [Selmer, 1951].
- 3.) II.6.3 lässt sich nicht auf abelsche Erweiterungen ausdehnen: Für $k = \mathbb{Q}(\sqrt{13}, \sqrt{17})$ ist jedes rationale Quadrat überall eine lokale Norm, aber 25 ist keine globale Norm [Serre–Tate].

Lokal-global-Prinzipien für k -Isomorphie

Satz II.6.5. *Seien f und f' quadratische Formen über k mit $f \cong_{k_v} f'$ für alle $v \in V(k)$. Dann gilt $f \cong_k f'$.*

Beweis. Die Radikale haben dieselbe Dimension, also genügt es, die nicht ausgearteten Anteile zu betrachten. Der Fall von Rang null ist trivial. Wähle ein von f dargestelltes $a \in k^*$. Dann stellt $f - az^2$ die Null global dar, also überall lokal, somit stellt auch $f' - az^2$ die Null überall lokal dar, also nach II.6.2 global. Gilt für das Element $(X_1, \dots, X_n, z)$, das die Null darstellt, $z \neq 0$, so ist $f'(X_1/z, \dots, X_n/z) = a$. Ist $z = 0$, so stellt f' die 0 dar, also gilt $f' \cong \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \perp f''$, und somit stellt es ganz k dar. Also ist $f = g + az^2$, $f' = g' + az^2$, und aus $f \cong_{k_v} f'$ folgt $g \cong_{k_v} g'$ nach dem Wittschen Kürzungssatz. Nach Induktionsvoraussetzung (der Fall von Rang null ist trivial) gilt $g \cong_k g'$, also $f \cong_k f'$. $\square$

Satz II.6.6 (Hasse-Prinzip für zentral einfache Algebren). *Sei A eine zentral einfache Algebra über k vom Grad d . Dann gilt $A \cong M_d(k)$ genau dann, wenn $A \otimes_k k_v \cong M_d(k_v)$ für alle $v \in V(k)$.*

Beweis. Für Quaternionenalgebren folgt dies aus II.6.5, da

$$\left(\frac{a, b}{k} \right) \xrightarrow{1:1} \langle -a, -b, ab \rangle$$

(quadratische Formen vom Rang 3 mit Diskriminante 1). Allgemeiner Fall: globale Klassenkörpertheorie (siehe unten). $\square$

II.7 Tate–Schafarewitsch-Gruppen

Für einen Galoismodul $\text{Gal}(k) = \text{Gal}(\bar{k}/k) \curvearrowright A$ und $S \subseteq V(k)$ definieren wir die n -te Tate–Schafarewitsch-Gruppe

$$\text{III}^n(k, S, A) = \ker \left(H^n(k, A) \xrightarrow{\text{diag.}} \prod_{v \notin S} H^n(k_v, A) \right)$$

(kyrillisches „Scha“), wobei wir $H^n(k, \cdot) = H^n(\text{Gal}(k), \cdot)$ schreiben und

$$\begin{array}{ccc} \bar{k} & \longrightarrow & \bar{k}_v \\ \uparrow & & \uparrow \\ k & \longrightarrow & k_v \end{array} \quad \text{liefert} \quad \text{Gal}(k_v) \longrightarrow \text{Gal}(k)$$

(A abelsch für $n > 1$; für nichtabelsches A und $n = 1$ ist dies eine punktierte Menge). Wir können die Lokal-global-Prinzipien aus Abschnitt II.6 mithilfe von Tate–Schafarewitsch-Gruppen umformulieren:

- **II.6.1:** $\text{III}^1(k, S, \mu_2) = \{1\}$ für endliches S . In der Tat ist μ_2 ein trivialer $\text{Gal}(k)$ -Modul, also

$$\begin{aligned} H^1(k, \mu_2) &\cong \text{Hom}_{\text{cont}}(\text{Gal}(k), \mu_2) \\ &\cong \{l/k \mid [l:k] \leq 2\} / \cong_k \cong k^*/(k^*)^2. \end{aligned}$$

- II.6.4, für endliches S :

$$\mathrm{III}^1(k, S, \mu_n) \cong \begin{cases} \mathbb{Z}/2 & \text{Spezialfall,} \\ 1 & \text{sonst.} \end{cases}$$

In der Tat ist $1 \longrightarrow \mu_n \longrightarrow \mathrm{GL}_1 \xrightarrow{(\cdot)^n} \mathrm{GL}_1 \longrightarrow 1$ auf $\bar{k}$ exakt, also

$$k^* \xrightarrow{(\cdot)^n} k^* \longrightarrow H^1(k, \mu_n) \longrightarrow \underbrace{H^1(k, \mathrm{GL}_1)}_{0 \text{ (Hilbert 90)}},$$

somit $H^1(k, \mu_n) \cong k^*/(k^*)^n$.

- II.6.3:

$$\mathrm{III}^1(\mathbb{Q}, \emptyset, \mathrm{R}_{k/\mathbb{Q}}^{(1)}(\mathrm{GL}_1)) \begin{cases} = 1 & \text{für } k/\mathbb{Q} \text{ zyklisch,} \\ \neq 1 & \text{für } k = \mathbb{Q}(\sqrt{13}, \sqrt{17}). \end{cases}$$

In der Tat gilt

$$1 \longrightarrow \mathrm{R}_{k/\mathbb{Q}}^{(1)}(\mathrm{GL}_1) \longrightarrow \mathrm{R}_{k/\mathbb{Q}}(\mathrm{GL}_1) \xrightarrow{\text{norm}} \mathrm{GL}_1 \longrightarrow 1.$$

Dabei ist $\mathrm{R}_{k/\mathbb{Q}}^{(1)}(\mathrm{GL}_1)$ ein „Norm-Eins-Torus“; die Weil-Restriktion erfüllt $\mathrm{R}_{k/\mathbb{Q}}(\mathbf{G})(\mathbb{Q}) \cong \mathbf{G}(k)$. Also gilt

$$k^* \xrightarrow{N_{k/\mathbb{Q}}} \mathbb{Q}^* \longrightarrow H^1(\mathbb{Q}, \mathrm{R}_{k/\mathbb{Q}}^{(1)}(\mathrm{GL}_1)) \longrightarrow H^1(\mathbb{Q}, \mathrm{R}_{k/\mathbb{Q}}(\mathrm{GL}_1)),$$

wobei die letzte Gruppe nach Shapiro und Hilbert 90 gleich $H^1(k, \mathrm{GL}_1) = 0$ ist. Somit

$$H^1(\mathbb{Q}, \mathrm{R}_{k/\mathbb{Q}}^{(1)}(\mathrm{GL}_1)) \cong \mathbb{Q}^*/N_{k/\mathbb{Q}}(k^*).$$

- II.6.5: $\mathrm{III}^1(k, \emptyset, \mathrm{O}(f)) = \{1\}$. Siehe die „Besonderheit“ in Kapitel I.
- II.6.6: $\mathrm{III}^1(k, \emptyset, \mathrm{PGL}_d) = \{1\}$. In der Tat liefern $\mathrm{Aut}(M_d) \cong \mathrm{PGL}_d$ nach Skolem–Noether und

$$1 \longrightarrow \mathrm{GL}_1 \longrightarrow \mathrm{GL}_d \longrightarrow \mathrm{PGL}_d \longrightarrow 1$$

das Diagramm

$$\begin{array}{ccccc} \underbrace{H^1(k, \mathrm{GL}_d)}_{0 \text{ (d-dimensionales H. 90)}} & \longrightarrow & H^1(k, \mathrm{PGL}_d) & \longrightarrow & H^2(k, \mathrm{GL}_1) \cong \mathrm{Br}(k) \\ & & \downarrow & & \downarrow \text{A-B-H-N} \\ & & \prod_v H^1(k_v, \mathrm{PGL}_d) & \longrightarrow & \prod_v \mathrm{Br}(k_v). \end{array}$$

Die rechte Injektion ist Albert–Brauer–Hasse–Noether. Ist also $\alpha \in \mathrm{III}^1(k, \emptyset, \mathrm{PGL}_d)$, so zeigt eine Diagrammjagd, dass α ein Urbild in $H^1(k, \mathrm{GL}_d) = 1$ hat, also ist α trivial.

Bemerkung. Es gibt einen exzeptionellen Isomorphismus $\mathrm{PGL}_2 \cong_k \mathrm{SO}_3$, wobei SO_3 zerfallend ist; dies erklärt die Korrespondenz zwischen Quaternionenalgebren und quadratischen Formen vom Rang 3 mit trivialer Diskriminante (siehe die Bemerkung nach Meta-Satz IV.3.1).

Fazit

Untersuche Lokal-global-Prinzipien für die Galoiskohomologie algebraischer Gruppen!

Kapitel III

Galoiskohomologie endlicher abelscher Moduln

III.1 Gruppenkohomologie

Wir erinnern daran, dass wir in Kapitel I für eine endliche Gruppe G und eine kurze exakte Folge von (linken) $\mathbb{Z}G$ -Moduln

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0,$$

eine Ad-hoc-Konstruktion einer exakten Folge angegeben haben:

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \xrightarrow{\delta^0} H^1(G, A).$$

Es gibt verschiedene Möglichkeiten, höhere Kohomologiegruppen einzuführen, um diese zu einer langen exakten Folge zu erweitern:

$$\begin{aligned} 0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \xrightarrow{\delta^0} H^1(G, A) \longrightarrow H^1(G, B) \\ \longrightarrow H^1(G, C) \longrightarrow H^2(G, A) \longrightarrow \dots \end{aligned}$$

1.) Durch injektive Auflösungen

Ein $\mathbb{Z}G$ -Modul I heißt *injektiv*, falls

$$\begin{array}{ccc} 0 & \longrightarrow & A \longrightarrow B \\ & & \downarrow \swarrow \exists \\ & & I \end{array}$$

oder äquivalent, falls $\text{Hom}_{\mathbb{Z}G}(\cdot, I)$ exakt ist. Die (abelsche) Kategorie $\mathbb{Z}G\text{-mod}$ hat genügend injektive Objekte: Für jeden $\mathbb{Z}G$ -Modul A finden wir $0 \longrightarrow A \longrightarrow I$, also auch eine *injektive Auflösung*

$$0 \longrightarrow A \longrightarrow I_0 \longrightarrow I_1 \longrightarrow I_2 \longrightarrow \dots,$$

und wir definieren $H^i(G, A)$ als die Kohomologiegruppen $\ker d^i / \text{im } d^{i-1}$ des Kokettenkomplexes

$$0 \longrightarrow I_0^G \xrightarrow{d^0} I_1^G \xrightarrow{d^1} I_2^G \longrightarrow \dots$$

Dies ist nach dem Hauptsatz der homologischen Algebra wohldefiniert. Die lange exakte Folge ergibt sich dann aus dem Hufeisenlemma und dem Schlangenlemma. Die Konstruktion ist funktoriell: $H^i(G, \cdot)$ sind die *rechtsabgeleiteten Funktoren* von $(\cdot)^G$.

2.) Durch projektive Auflösungen

Ein $\mathbb{Z}G$ -Modul P heißt *projektiv*, falls dual dazu

$$\begin{array}{ccc} 0 & \leftarrow & A \leftarrow B \\ & \uparrow & \nearrow \exists \\ & P & \end{array}$$

oder äquivalent, falls $\text{Hom}_{\mathbb{Z}G}(P, \cdot)$ exakt ist. $\mathbb{Z}G\text{-mod}$ hat genügend projektive Objekte ($\forall A \exists P \rightarrow A \rightarrow 0$), also wählen wir eine *projektive Auflösung* des trivialen Moduls $\mathbb{Z}$:

$$\cdots \rightarrow P_2 \rightarrow P_1 \rightarrow P_0 \rightarrow \mathbb{Z} \rightarrow 0$$

und definieren $H^i(G, A)$ als die Kohomologie von

$$0 \rightarrow \text{Hom}_{\mathbb{Z}G}(P_0, A) \rightarrow \text{Hom}_{\mathbb{Z}G}(P_1, A) \rightarrow \text{Hom}_{\mathbb{Z}G}(P_2, A) \rightarrow \cdots$$

Man beachte, dass $\text{Hom}_{\mathbb{Z}G}(\mathbb{Z}, A) = A^G$!

Bemerkung. Ist BG ein zusammenhängender CW-Komplex mit $\pi_1 BG \cong G$ und $EG := \widetilde{BG} \simeq \bullet$, so ist $C_*^{\text{CW}}(EG, \mathbb{Z})$ eine freie (also projektive) Auflösung von $\mathbb{Z}$. Wegen

$$C_{\text{CW}}^*(BG; A) := \text{Hom}_{\mathbb{Z}G}(C_*^{\text{CW}}(EG, \mathbb{Z}), A),$$

gilt somit $H^*(G, A) \cong H_{\text{CW}}^*(BG; A)$ (Kohomologie „mit lokalen Koeffizienten“ in der Terminologie der algebraischen Topologie).

3.) Durch homogene Koketten (Konkretisierung von 2.)

Sei L_i der freie $\mathbb{Z}$ -Modul mit Basis G^{i+1} . Die diagonale Wirkung $G \curvearrowright G^{i+1}$ verleiht L_i die Struktur eines freien $\mathbb{Z}G$ -Moduls, und

$$\cdots \rightarrow L_2 \xrightarrow{d_2} L_1 \xrightarrow{d_1} L_0 \xrightarrow{d_0} \mathbb{Z} \rightarrow 0$$

ist eine freie (also projektive) Auflösung, wobei

$$d_i(g_0, \dots, g_i) = \sum_{j=0}^i (-1)^j (g_0, \dots, \widehat{g_j}, \dots, g_i).$$

Man beachte, dass

$$\text{Hom}_{\mathbb{Z}G}(L_i, A) \cong \{f: G^{i+1} \rightarrow A \mid f \text{ ist } G\text{-äquivariant}\}$$

(„homogene Koketten“).

4.) Durch (inhomogene) Koketten

Sei X_i der freie $\mathbb{Z}G$ -Modul mit Basis G^i . Dann ist

$$\cdots \rightarrow X_2 \xrightarrow{d_2} X_1 \xrightarrow{d_1} X_0 \xrightarrow{d_0} \mathbb{Z}$$

eine freie Auflösung, wobei

$$\begin{aligned} d_i(g_1, \dots, g_i) &= g_1 \cdot (g_2, \dots, g_i) \\ &+ \sum_{j=1}^{i-1} (-1)^j (g_1, \dots, g_j g_{j+1}, \dots, g_i) + (-1)^i (g_1, \dots, g_{i-1}). \end{aligned}$$

Übung. Man zeige, dass durch

$$(g_1, \dots, g_i) \mapsto (1, g_1, g_1 g_2, \dots, g_1 \cdots g_i)$$

ein Isomorphismus von $\mathbb{Z}G$ -Komplexen $X_\bullet \cong L_\bullet$ definiert wird.

Übung. Man zeige, dass $Z^1(\text{Hom}_{\mathbb{Z}G}(X_\bullet, A))$ und $B^1(\text{Hom}_{\mathbb{Z}G}(X_\bullet, A))$ mit unseren bisherigen Definitionen der 1-Kozyklen und 1-Koränder übereinstimmen.

Aus 3.) und 4.) sehen wir, dass $H^*(G, A)$ endlich ist, wenn G und A endlich sind.

III.2 Tate-Kohomologie

Sei weiterhin G eine endliche Gruppe.

Definition III.2.1. Die *Norm* von $\mathbb{Z}G$ ist das Element $N_G = \sum_{g \in G} g$. Das *Augmentationsideal* ist

$$I_G = \ker \left(\mathbb{Z}G \longrightarrow \mathbb{Z}, \quad \sum_{g \in G} a_g g \mapsto \sum_{g \in G} a_g \right).$$

Für jeden $\mathbb{Z}G$ -Modul A sei $N: A \rightarrow A$, $a \mapsto N_G a$. Dann gilt $I_G A \subseteq \ker N$ und im $N \subseteq A^G = H^0(G, A)$.

Definition III.2.2. Wir nennen $A_G := H_0(G, A) := A/I_G A$ die *Koinvarianten* von A .

Nach dem Obigen induziert N eine Abbildung $N^*: H_0(G, A) \rightarrow H^0(G, A)$.

Definition III.2.3. Setze $\hat{H}_0(G, A) := \ker N^*$, $\hat{H}^0(G, A) := \text{coker } N^*$.

Man beachte, dass die Funktoren $(\cdot)_G$ und $\mathbb{Z} \otimes_{\mathbb{Z}G} (\cdot)$ natürlich isomorph sind, also ist $(\cdot)_G$ rechtsexakt. Dual zu III.1.1) definieren wir $H_i(G, \cdot)$ als die *linksabgeleiteten Funktoren* von $(\cdot)_G$. Ähnlich wie in III.1.2) ist $H_i(G, A)$ auch die algebraische Homologie von $P_\bullet \otimes_{\mathbb{Z}G} A$ für eine projektive Auflösung $P_\bullet \rightarrow \mathbb{Z}$ durch Rechts- $\mathbb{Z}G$ -Moduln.

Beispiel. Ist A trivial, so gilt $H_1(G, A) = G_{\text{ab}} \otimes_{\mathbb{Z}} A$.

Definition III.2.4. Wir definieren die *Tate-Kohomologiegruppen* durch

$$\begin{aligned} \hat{H}^n(G, A) &= H^n(G, A) && \text{für } n \geq 1, \\ \hat{H}^0(G, A) &= A^G / N A && (\text{siehe oben}), \\ \hat{H}^{-1}(G, A) &= \hat{H}_0(G, A) = \ker N / I_G A && (\text{siehe oben}), \\ \hat{H}^{-n}(G, A) &= H_{n-1}(G, A) && \text{für } n \geq 2. \end{aligned}$$

Satz III.2.5. $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ in $\mathbb{Z}G\text{-mod}$ induziert

$$\begin{aligned} \cdots \rightarrow \hat{H}^{-2}(G, C) \rightarrow \hat{H}^{-1}(G, A) \rightarrow \hat{H}^{-1}(G, B) \rightarrow \hat{H}^{-1}(G, C) \\ \rightarrow \hat{H}^0(G, A) \rightarrow \hat{H}^0(G, B) \rightarrow \hat{H}^0(G, C) \rightarrow \hat{H}^1(G, A) \rightarrow \cdots \end{aligned}$$

III.3 Cup-Produkte

Sei weiterhin G endlich und $K^i(G, A) = \text{Hom}_{\mathbb{Z}G}(L_i, A)$ der Kokettenkomplex der homogenen Koketten. Für $\mathbb{Z}G$ -Moduln A und B erhalten wir eine Links- $\mathbb{Z}G$ -Modulstruktur auf $A \otimes B := A \otimes_{\mathbb{Z}} B$ durch $g \cdot (a \otimes b) = (ga) \otimes (gb)$.

Definition III.3.1. Das *Cup-Produkt* auf homogenen Koketten ist die bilineare Abbildung, die durch

$$K^p(G, A) \times K^q(G, B) \xrightarrow{\cup} K^{p+q}(G, A \otimes B),$$

$$(a \cup b)(g_0, \dots, g_{p+q}) = a(g_0, \dots, g_p) \otimes b(g_p, \dots, g_{p+q})$$

definiert wird.

Satz III.3.2. Wir erhalten ein induziertes bilineares Cup-Produkt

$$H^p(G, A) \times H^q(G, B) \longrightarrow H^{p+q}(G, A \otimes B).$$

Beweis. Wohldefiniert, da eine einfache Rechnung ergibt:

$$d(a \cup b) = (da) \cup b + (-1)^p(a \cup db).$$

□

Bemerkung. Für $a \in H^0(G, A) = A^G$, $b \in H^q(G, B)$ gilt $a \cup b = f_*(b)$, wobei f_* durch $B \longrightarrow A \otimes B$, $x \longmapsto a \otimes x$ induziert wird. Für $p = q = 0$ gilt also

$$\cup: A^G \times B^G \longrightarrow (A \otimes B)^G, \quad (a, b) \longmapsto a \otimes b.$$

Eine G -äquivalente bilineare Abbildung $A \times B \xrightarrow{\varphi} C$ faktorisiert als

$$\begin{array}{ccc} A \otimes B & & \\ \uparrow & \searrow \bar{\varphi} & \\ A \times B & \xrightarrow{\varphi} & C, \end{array}$$

sodass wir ein induziertes Cup-Produkt erhalten:

$$H^p(G, A) \times H^q(G, B) \longrightarrow H^{p+q}(G, C).$$

Zu jeder G -äquivalenten bilinearen Paarung $A \times B \xrightarrow{\varphi} C$, $p, q \in \mathbb{Z}$, erhalten wir auch ein Cup-Produkt

$$\hat{H}^p(G, A) \times \hat{H}^q(G, B) \longrightarrow \hat{H}^{p+q}(G, C).$$

Es wird mithilfe der Fortsetzung $X_{-1-n} = \mathbb{Z}[G^{n+1}]$ von $X_\bullet$ konstruiert, wobei

$$d_{-n}(g_0, \dots, g_{n-1}) = \sum_{g \in G} \sum_{i=0}^n (-1)^i (g_0, \dots, g_{i-1}, g, g_i, \dots, g_{n-1})$$

für $n \geq 1$ und $d_0(g_0) = \sum_{g \in G} g$. Für $p = q = 0$ ist dies die durch φ induzierte Paarung

$$A^G/NA \times B^G/NB \longrightarrow C^G/NC.$$

Für $p, q > 0$ stimmt es mit dem zuvor definierten Cup-Produkt überein.

III.4 Kohomologie proendlicher Gruppen

Definition III.4.1. Eine topologische Gruppe G heißt *proendlich*, falls $G = \varprojlim G_i$ für ein inverses System endlicher Gruppen $(G_i)_{i \in I}$.

Satz III.4.2. G ist genau dann proendlich, wenn G kompakt und total unzusammenhängend ist.

Beweis. „ $\Rightarrow$ “: $\varprojlim G_i \leq \prod_{i \in I} G_i$ ist abgeschlossen.

„ $\Leftarrow$ “: (schwieriger) $G \cong \varprojlim_N G/N$ mit offenem $N \trianglelefteq G$. Hier ist $[G : N] < \infty$, da G kompakt ist. $\square$

Beispiele. Endliche Gruppen.

$$\mathrm{Gal}(k) = \mathrm{Gal}(\bar{k}/k) \cong \varprojlim_{l/k \text{ endlich galoissch}} \mathrm{Gal}(l/k) = \varprojlim_{\substack{N \trianglelefteq \mathrm{Gal}(k) \\ \text{abgeschlossen, endlicher Index}}} \mathrm{Gal}(k)/N.$$

Für eine diskrete abelsche Torsionsgruppe M ist die *Pontryagin-Duale* $M^* = \mathrm{Hom}(M, \mathbb{Q}/\mathbb{Z})$ mit der kompakt-offenen Topologie proendlich. In der Tat gilt

$$M^* = \mathrm{Hom} \left(\varprojlim_{\substack{N \trianglelefteq M \\ \text{endlich}}} N, \mathbb{Q}/\mathbb{Z} \right) = \varprojlim_{\substack{N \trianglelefteq M \\ \text{endlich}}} \mathrm{Hom}(N, \mathbb{Q}/\mathbb{Z}).$$

Tatsächlich ist $(\cdot)^*$ eine Antiäquivalenz zwischen diskreten abelschen Torsionsgruppen und abelschen proendlichen Gruppen. (Für eine abelsche proendliche Gruppe G ist $\mathrm{Hom}_{\mathrm{cont}}(G, \mathbb{Q}/\mathbb{Z})$ eine diskrete abelsche Torsionsgruppe.)

Vorsicht. Für $M = \mathbb{Z}$ gilt

$$M^* = \mathbb{Q}/\mathbb{Z} \cong \bigoplus_p \mathbb{Z}(p^\infty), \quad M^{**} \cong \prod_p \mathbb{Z}_p \cong \hat{\mathbb{Z}}.$$

Hier ist $\mathbb{Z}(p^\infty) = \varinjlim_n \mathbb{Z}/p^n$ die Prüfer- p -Gruppe, und $\hat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n$. Für alle $v \in V_f(k)$ sind die Gruppen $\mathcal{O}_v$ und $\mathcal{O}_v^*$ proendlich (insbesondere $\mathbb{Z}_p$ und $\mathbb{Z}_p^*$).

Bis auf Weiteres sei G eine proendliche Gruppe.

Definition III.4.3. Ein *diskreter G -Modul* ist eine diskrete abelsche Gruppe A mit einer stetigen Wirkung $G \curvearrowright A$.

Dies bedeutet, dass für alle $a \in A$ die Bahnabbildung $G \rightarrow A$, $g \mapsto ga$ stetig ist ($\iff G_a = \{g \in G \mid ga = a\}$ ist offen).

Beispiele (mit $G = \mathrm{Gal}(k)$). $A = \bar{k}^*$. Für $a \in \bar{k}^*$ ist $G_a = \mathrm{Gal}(\bar{k}/k(a))$ nach der unendlichen Galoistheorie abgeschlossen und von endlichem Index, also ist G_a offen.

$A = \mu_n(\bar{k})$ (ein invarianter Untermodul von $\bar{k}^*$).

Der triviale diskrete G -Modul M (z. B. $M = \mathbb{Z}/n$, zu unterscheiden von $\mu_n(\bar{k})$).

Die vorigen Beispiele $\bar{k}^*$, $\mu_n(\bar{k})$, $\mathbb{Z}/n$ sind Beispiele für kommutative affine Gruppenschemata über k (vgl. Kapitel IV): GL_1 , μ_n , $\mathbb{Z}/n$ (konstant), und $(\sigma : \bar{k} \rightarrow \bar{k}) \in G$ wirkt funktoriell.

Sei M ein endliches kommutatives Gruppenschema über k . Dann ist das *Cartier-Duale* von M gegeben durch $M' = \text{Hom}(M, \text{GL}_1)$ mit der G -Wirkung $(\sigma f)(m) = \sigma \cdot f(\sigma^{-1}m)$. Zum Beispiel gilt

$$(\mu_n)' = \text{Hom}(\mu_n, \text{GL}_1) = \text{Hom}(\mu_n, \mu_n) = \{(\cdot)^k \mid k = 0, \dots, n-1\}$$

und $\sigma(\sigma^{-1}z)^k = z^k$, also ist $G \curvearrowright (\mu_n)'$ trivial, was $\mu_n' = \mathbb{Z}/n$, $(\mathbb{Z}/n)' = \mu_n$ bedeutet.

Sei $G\text{-mod}_\delta$ die Kategorie der diskreten G -Moduln. Dann hat $G\text{-mod}_\delta$ genügend injektive Objekte (wähle $0 \rightarrow A \rightarrow I$ in $\mathbb{Z}G\text{-mod}$, dann $0 \rightarrow A \rightarrow \varinjlim_{U \leq_o G} I^U$), also:

Definition III.4.4. Für einen diskreten G -Modul A definieren wir $H^i(G, A)$ als die rechtsabgeleiteten Funktoren von $(\cdot)^G$.

Im Allgemeinen muss $G\text{-mod}_\delta$ jedoch nicht genügend projektive Objekte haben. (Für unendliches G ist der $\mathbb{Z}G$ -Modul $\mathbb{Z}G$ nicht diskret, da der Stabilisator von $1 \in \mathbb{Z}G$ trivial und somit nicht offen ist.) Für explizite Berechnungen definieren wir daher allgemeiner

$$K^i(G, A) = \{f: G^i \rightarrow A \mid f \text{ stetig (äquivalent: lokal konstant)}\}$$

und $d^i(f) = f \circ d_{i+1}$ mit d_{i+1} wie in III.1.4), wobei f $\mathbb{Z}G$ -linear fortgesetzt wird.

Satz III.4.5. Für jeden diskreten G -Modul A gilt $H^i(G, A) = H^i(K^\bullet(G, A))$.

Proposition III.4.6. Sei (G_i) ein inverses System von (pro-)endlichen Gruppen und (A_i) ein induktives System diskreter G_i -Moduln mit Übergangsabbildungen $p_{ji}: G_j \rightarrow G_i$ und $u_{ij}: A_i \rightarrow A_j$, sodass

$$\begin{array}{ccc} G_j & \xrightarrow{p_{ji}} & G_i \\ \downarrow g \mapsto g u_{ij}(a) & & \downarrow g \mapsto ga \\ A_j & \xleftarrow{u_{ij}} & A_i \end{array}$$

für alle $a \in A_i$ kommutiert. Setze $G = \varprojlim_i G_i$ und $A = \varinjlim_i A_i$. Dann gilt $H^q(G, A) = \varinjlim_i H^q(G_i, A_i)$.

Beweis. Es gilt sogar, dass die Kolimesabbildung

$$\varinjlim_i K^\bullet(G_i, A_i) \rightarrow K^\bullet(G, A)$$

ein Isomorphismus ist. □

Korollar III.4.7. $H^q(G, A) = \varinjlim_{U \leq_o G} H^q(G/U, A^U)$.

Beweis. Wie oben besprochen ist $G = \varprojlim G/U$, und es gilt $A = \varinjlim A^U$, da $a \in A$ in A^{G_a} liegt. □

Korollar III.4.8. $H^q(G, A)$ ist eine abelsche Torsionsgruppe für $q \geq 1$.

Beweis. Dies folgt aus III.4.7 und daraus, dass für endliches G , $H \leq G$ und $q \geq 1$ der Homomorphismus

$$\text{cores}_H \circ \text{res}_H: H^q(G, A) \rightarrow H^q(G, A)$$

die Multiplikation mit $[G : H]$ ist (anwenden auf $H = \{1\}$). (Siehe „Oberseminar Algebra und Geometrie“.) □

III.5 Galoiskohomologie

In diesem Abschnitt seien $G = \text{Gal}(k)$ und $A \in G\text{-mod}_\delta$. Zu einer Erweiterung k_1/k und einem algebraischen Abschluss $\bar{k}_1/k_1$ finden wir ein Diagramm:

$$\begin{array}{ccc} \bar{k} & \xrightarrow{j} & \bar{k}_1 \\ \uparrow & & \uparrow \\ k & \xrightarrow{i} & k_1 \end{array}$$

Dies induziert $f: \text{Gal}(k_1) \rightarrow \text{Gal}(k)$. Ersetzen wir j durch j' , so ergibt sich

$$\begin{aligned} f'(\sigma) &= (j')^{-1} \circ \sigma \circ j' \\ &= (j')^{-1} \circ (j \circ j^{-1}) \circ \sigma \circ (j \circ j^{-1}) \circ j' \\ &= ((j')^{-1} \circ j) \circ j^{-1} \circ \sigma \circ j \circ (j^{-1} \circ j') \\ &= \tau^{-1} \circ f(\sigma) \circ \tau, \end{aligned}$$

mit $\tau = j^{-1} \circ j' \in \text{Gal}(k)$.

Proposition III.5.1. *Sei $\tau \in G$. Dann induzieren $\sigma \mapsto \tau^{-1}\sigma\tau$ und $a \mapsto \tau a$ einen Automorphismus Φ_τ von $H^q(G, A)$, und es gilt $\Phi_\tau = \text{id}$.*

(Funktorialität: $f: G' \rightarrow G$ und eine additive Abbildung $g: A \rightarrow A'$ mit $g(f(\sigma')a) = \sigma'g(a)$ induzieren $H^q(G, A) \rightarrow H^q(G', A')$.)

Beweis. Lässt sich an der Beschreibung von $H^1(G, A)$ durch Kozyklen überprüfen. Der allgemeine Fall folgt mit homologischer Algebra. $\square$

Somit ist der induzierte Homomorphismus

$$H^q(\text{Gal}(k), A) \rightarrow H^q(\text{Gal}(k_1), A)$$

unabhängig von j . Insbesondere folgt für $k_1 = k$, dass je zwei algebraische Abschlüsse $\bar{k}, \bar{k}_1$ kanonisch isomorphe Gruppen liefern:

$$H^q(\text{Gal}(k), A) \cong H^q(\text{Gal}(k_1), A),$$

sodass wir $H^q(k, A) := H^q(\text{Gal}(k), A)$ schreiben können und dies die q -te *Galoiskohomologie* von k mit Koeffizienten in A nennen. Ist A ein kommutatives affines Gruppenschema über k und k_1/k eine beliebige Körpererweiterung, so erfüllen $f: \text{Gal}(k_1) \rightarrow \text{Gal}(k)$ und $g: A(\bar{k}) \rightarrow A(\bar{k}_1)$ die Bedingung $g(f(\sigma)a) = \sigma g(a)$. Somit erhalten wir

$$\begin{array}{ccc} H^q(\text{Gal}(k), A(\bar{k})) & \longrightarrow & H^q(\text{Gal}(k_1), A(\bar{k}_1)) \\ \parallel & & \parallel \\ H^q(k, A) & \longrightarrow & H^q(k_1, A) \end{array}$$

wohldefiniert und funktoriell in k , d. h. A definiert

$$H^q(\cdot, A): \text{FieldExt}/k \rightarrow \text{Ab}.$$

Beispiele

1.) $A = \mathbb{G}_a$, das additive Gruppenschema über k mit $\mathbb{G}_a(\bar{k}) = (\bar{k}, +)$.

Satz III.5.2. Es gilt $H^q(K, \mathbb{G}_a) = 0$ für jede Erweiterung K/k und jedes $q \geq 1$.

Außerdem gilt $\hat{H}^q(\text{Gal}(L/K), L) = 0$ für jede endliche Galoiserweiterung L/K und jedes $q \in \mathbb{Z}$.

Beweis. Jede endliche Galoiserweiterung L/K besitzt eine Normalbasis, d. h.

$$L = \bigoplus_{\sigma \in \text{Gal}(L/K)} K\sigma(x) \quad \text{für ein } x \in L.$$

Dies bedeutet, dass L ein $\text{Gal}(L/K)$ -induzierter Modul ist. (Definition: A heißt G -induziert, wenn $A \cong \bigoplus_{g \in G} gD$ für ein $D \leq A$ gilt.) Für eine endliche Gruppe G hat ein G -induzierter Modul A triviale Tate-Kohomologie, denn

$$\text{Hom}_{\mathbb{Z}G}(X_\bullet, A) \cong \text{Hom}_{\mathbb{Z}}(X_\bullet, D)$$

ist exakt: Die in Abschnitt III.3 beschriebene vollständige Auflösung $X_\bullet$ ist über $\mathbb{Z}$ spaltend exakt. Somit gilt für $q \geq 1$

$$H^q(K, \mathbb{G}_a) \cong \varinjlim_{L/K \text{ endlich galoissch}} H^q(\text{Gal}(L/K), L) = 0$$

nach III.4.7 (woraus sich Isomorphismen der Komplexe ergeben). $\square$

2.) $A = \mathbb{G}_m = \text{GL}_1$, das multiplikative Gruppenschema über k mit $\mathbb{G}_m(\bar{k}) = (\bar{k}^*, \cdot)$.

Satz III.5.3 („Hilbert 90“). $H^1(k, \mathbb{G}_m) = 0$.

Beweis. Wie oben genügt es zu zeigen, dass $H^1(\text{Gal}(L/k), L^*) = 0$ für jede endliche Galoiserweiterung L/k gilt. Setze $G := \text{Gal}(L/k)$. Sei $\sigma \mapsto a_\sigma$ ein Kozyklus in $Z^1(G, L^*)$. Nach dem Satz von Dedekind ist $G \subseteq \text{Hom}_k(L, L)$ linear unabhängig über L . Somit finden wir $x \in L^*$ mit $b := \sum_{\sigma \in G} a_\sigma \sigma(x) \neq 0$. Für alle $\tau \in G$ folgt

$$\begin{aligned} \tau(b) &= \sum_{\sigma \in G} {}^\tau a_\sigma \tau \sigma(x) = \sum_{\sigma \in G} a_{\tau\sigma} a_\tau^{-1} \tau \sigma(x) \\ &= a_\tau^{-1} \sum_{\sigma \in G} a_\sigma \sigma(x) = a_\tau^{-1} b, \end{aligned}$$

also ist $a_\tau = b\tau(b)^{-1} = \tau(b^{-1})(b^{-1})^{-1}$ ein Korand. $\square$

Übung. Zeige: Ist $\text{Gal}(L/k) = \langle \sigma \rangle$ zyklisch, so gibt es für jedes $x \in L$ mit $N_{L/k}(x) = 1$ ein $c \in L^*$ mit $x = \sigma(c)/c$ (Hilberts ursprünglicher Satz 90). Hinweis: Verwende $\hat{H}^{-1}(G, A) \cong \hat{H}^1(G, A)$ für zyklische Gruppen G .

Definition III.5.4. Die abelsche Gruppe $H^2(k, \mathbb{G}_m)$ heißt *Brauergruppe* $\text{Br}(k)$ von k .

3.) $A = \mu_n$, das endliche abelsche Gruppenschema der n -ten Einheitswurzeln.

Satz III.5.5. $H^1(k, \mu_n) \cong k^*/(k^*)^n$.

Beweis. Die exakte Folge $1 \rightarrow \mu_n \rightarrow \mathbb{G}_m \xrightarrow{(\cdot)^n} \mathbb{G}_m \rightarrow 1$ (d. h.

$$1 \rightarrow \mu_n(\bar{k}) \rightarrow \bar{k}^* \xrightarrow{(\cdot)^n} \bar{k}^* \rightarrow 1$$

ist exakt) liefert

$$k^* \xrightarrow{(\cdot)^n} k^* \xrightarrow{\delta^0} H^1(k, \mu_n) \rightarrow \underbrace{H^1(k, \mathbb{G}_m)}_{0 \text{ (H. 90)}}.$$

Somit gilt $H^1(k, \mu_n) \cong \text{coker}(k^* \xrightarrow{(\cdot)^n} k^*) = k^*/(k^*)^n$. $\square$

Satz III.5.6. $H^2(k, \mu_n) \cong \text{Br}(k)[n]$, die Untergruppe von $\text{Br}(k)$ aus den Elementen, deren Ordnung n teilt.

Beweis.

$$0 = H^1(k, \mathbb{G}_m) \xrightarrow{\delta^1} H^2(k, \mu_n) \longrightarrow H^2(k, \mathbb{G}_m) \xrightarrow{(\cdot)^n} H^2(k, \mathbb{G}_m),$$

$$\text{also } H^2(k, \mu_n) \cong \ker(\text{Br}(k) \xrightarrow{(\cdot)^n} \text{Br}(k)) = \text{Br}(k)[n]. \quad \square$$

Korollar III.5.7. Enthält k eine primitive n -te Einheitswurzel, so gilt $H^1(k, \mathbb{Z}/n) = k^*/(k^*)^n$ und $H^2(k, \mathbb{Z}/n) \cong \text{Br}(k)[n]$.

Beweis. In diesem Fall gilt $\mu_n(\bar{k}) \subseteq k^*$, sodass $\mu_n \cong \mathbb{Z}/n$ ein trivialer $\text{Gal}(k)$ -Modul ist. $\square$

4.) „Hilbert 90“ besitzt die folgende nichtkommutative Verallgemeinerung (für einen beliebigen Körper K).

Satz III.5.8. $H^1(K, \text{GL}_n) = 0$.

Beweis. Bilde wie zuvor für einen Kozyklus $\sigma \mapsto a_\sigma$ $b = \sum_{\sigma \in G} a_\sigma \sigma(x)$ und überprüfe $\tau(b) = a_\tau^{-1}b$. Zeige dann, dass sich $x \in \text{GL}_n(L)$ für eine endliche Galoiserweiterung L/K so wählen lässt, dass b invertierbar ist. $\square$

III.6 Die Brauergruppe und lokale Dualität

Erinnerung: Jede CSA A über einem (etwa perfekten) Körper K hat die Form $A \cong M_n(D_A)$ für eine eindeutig bestimmte Divisionsalgebra D_A über K . Definiere $A \sim B : \iff D_A \cong D_B$. Dann versteht „ $\otimes_K$ “ die Menge der Äquivalenzklassen von CSAs über K mit einer wohldefinierten Struktur einer abelschen Gruppe $\text{CSA}(K)$.

Satz III.6.1. $\text{CSA}(K) \cong \text{Br}(K)$.

Beweis. Nach Skolem–Noether gilt $\text{Aut}(M_n(\bar{K})) \cong \text{PGL}_n(\bar{K})$.

$$1 \longrightarrow \text{GL}_1 \longrightarrow \text{GL}_n \longrightarrow \text{PGL}_n \longrightarrow 1$$

liefert

$$\underbrace{H^1(K, \text{GL}_n)}_{0 \text{ nach III.5.8}} \longrightarrow H^1(K, \text{PGL}_n) \xrightarrow{\delta^1} H^2(K, \text{GL}_1).$$

Dies definiert $\text{CSA}(K) \longrightarrow \text{Br}(K)$, $A \mapsto \delta^1_{\sqrt{\dim_K A}}([A])$, und liefert den Isomorphismus. $\square$

Beispiele

- 1.) Ist $K = \bar{K}$, so gilt $\text{Br}(K) = 0$.
- 2.) Ist K endlich, so gilt $\text{Br}(K) = 0$ nach III.6.1 und dem Satz von Wedderburn, dass jeder endliche Schiefkörper ein Körper ist. (Beweis aus dem BUCH.)
- 3.) $\text{Br}(\mathbb{R}) \cong \mathbb{Z}/2$, denn die einzigen zentralen Divisionsalgebren über $\mathbb{R}$ sind $\mathbb{R}$ und $\mathbb{H}$.
- 4.) Hat $K/\mathbb{Q}_p$ endlichen Grad, so gilt $\text{Br}(K) \cong \mathbb{Q}/\mathbb{Z}$. (Erinnerung an das Oberseminar zur Klassenkörpertheorie.) Ist K_{ur}/K die maximale unverzweigte Erweiterung, so gilt $\text{Gal}(K_{\text{ur}}/K) \cong \hat{\mathbb{Z}}$.

Daher gibt es für jedes n eine eindeutige unverzweigte Erweiterung L_n/K vom Grad n , und für alle endlichen Galoiserweiterungen L/K mit $[L : K] = n$ gilt

$$H^2(L/K, \mathbb{G}_m) = H^2(L_n/K, \mathbb{G}_m) \leq H^2(K, \mathbb{G}_m).$$

Somit gilt $\mathrm{Br}(K) = \varinjlim_n H^2(L_n/K, \mathbb{G}_m)$ und

$$\mathrm{inv}_{L_n/K} : H^2(L_n/K, \mathbb{G}_m) \xrightarrow{\cong} \frac{1}{n} \mathbb{Z}/\mathbb{Z},$$

also $\mathrm{Br}(K) \cong \mathbb{Q}/\mathbb{Z}$.

Korollar III.6.2. $H^1(K, \mu_n) \cong K^*/(K^*)^n$ ist endlich, ebenso wie

$$H^2(K, \mu_n) \cong (\mathbb{Q}/\mathbb{Z})[n] \cong \frac{1}{n} \mathbb{Z}/\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}.$$

Ein Argument mit Spektralsequenzen zeigt dann, dass tatsächlich $H^i(K, M)$ für jeden endlichen kommutativen $\mathrm{Gal}(K)$ -Modul M endlich ist.

5.) Aus der globalen Klassenkörpertheorie folgt:

Satz III.6.3 (Albert–Brauer–Hasse–Noether).

$$1 \longrightarrow \mathrm{Br}(k) \longrightarrow \bigoplus_{v \in V(k)} \mathrm{Br}(k_v) \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 1.$$

Sei wieder $K/\mathbb{Q}_p$ ein p -adischer Körper und M ein endliches kommutatives Gruppenschema über K (äquivalent dazu: ein endlicher kommutativer (diskreter) $\mathrm{Gal}(K)$ -Modul). Auswertung liefert eine Paarung von $\mathrm{Gal}(K)$ -Moduln $M \times M' \longrightarrow \mathrm{GL}_1$, die ein Cup-Produkt induziert:

$$H^i(K, M) \times H^{2-i}(K, M') \longrightarrow \mathrm{Br}(K) = \mathbb{Q}/\mathbb{Z}.$$

Satz III.6.4 (Lokale Tate-Dualität). Für $i = 0, 1, 2$ ist

$$H^i(K, M) \times H^{2-i}(K, M') \longrightarrow \mathbb{Q}/\mathbb{Z}$$

eine perfekte Paarung endlicher abelscher Gruppen.

Beweis. Man überprüft, dass der Funktor

$$(\mathrm{Gal}(K)\text{-mod}_{\mathrm{fin}}^\delta)^{\mathrm{op}} \longrightarrow \mathbf{Ab}, \quad A \longmapsto H^2(K, A)^*$$

natürlich isomorph zur Einschränkung von $\mathrm{Hom}_{\mathrm{Gal}(K)}(\cdot, \mu)$ auf endliche diskrete Moduln ist, wobei $\mu = \mu(\overline{K}) = \varinjlim_n \mu_n(\overline{K})$. Explizit gilt

$$H^2(K, A)^* \cong \mathrm{Hom}_{\mathrm{Gal}(K)}(A, \mu) \quad \text{natürlich in } A.$$

Wegen

$$\mathrm{Hom}_{\mathrm{Gal}(K)}(M, \mu) = \mathrm{Hom}_{\mathrm{Gal}(K)}(M, \mathrm{GL}_1) = H^0(K, M'),$$

folgt $H^2(K, M)^* \cong H^0(K, M')$, und dieser Isomorphismus wird durch das Cup-Produkt gegeben. Damit ist der Fall $i = 2$ gezeigt. Für $i = 0$ ersetze M durch M' . Für $i = 1$ überprüfe, dass $H^1(K, M) \longrightarrow H^1(K, M')^*$ injektiv ist. $\square$

III.7 Unverzweigte Kohomologie

Weiterhin sei $K/\mathbb{Q}_p$ eine endliche Erweiterung.

Definition III.7.1. Wir nennen $A \in \text{Gal}(K)\text{-mod}^\delta$ *unverzweigt*, wenn $\text{Gal}(\overline{K}/K_{\text{ur}})$ trivial auf A wirkt. In diesem Fall setzen wir $H_{\text{ur}}^i(K, A) = H^i(\text{Gal}(K_{\text{ur}}/K), A)$.

Proposition III.7.2. Sei A endlich und unverzweigt. Dann gilt $H_{\text{ur}}^0(K, A) = H^0(K, A)$ und $H_{\text{ur}}^i(K, A) = 0$ für $i \geq 2$. Für $i = 1$ ist $H_{\text{ur}}^1(K, A) \leq H^1(K, A)$ eine (möglicherweise nichttriviale, möglicherweise echte) Untergruppe.

Beweis.

$$H_{\text{ur}}^0(K, A) = A^{\text{Gal}(K_{\text{ur}}/K)} = A^{\text{Gal}(\overline{K}/K)/\text{Gal}(\overline{K}/K_{\text{ur}})} = A^{\text{Gal}(\overline{K}/K)} = H^0(K, A).$$

Dass $H_{\text{ur}}^i(K, A) = 0$ für $i \geq 2$ gilt, folgt aus $\text{cd}(\widehat{\mathbb{Z}}) = 1$ [kohomologische Dimension: Verwende $\widehat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$ und

$$H^2(\mathbb{Z}/p^n, \mathbb{Z}/p) \stackrel{\text{period.}}{\cong} \widehat{H}^0(\mathbb{Z}/p^n, \mathbb{Z}/p) \cong H^0(\mathbb{Z}/p^n, \mathbb{Z}/p) \cong \mathbb{Z}/p,$$

also

$$H^2(\mathbb{Z}_p, \mathbb{Z}/p) \stackrel{\text{III.4.6}}{=} \varinjlim_n H^2(\mathbb{Z}/p^n, \mathbb{Z}/p) = 0$$

denn die Übergangsabbildungen sind $\mathbb{Z}/p \xrightarrow{p} \mathbb{Z}/p$, also trivial. Für eine Pro- p -Gruppe G gilt $\text{cd}_p(G) \leq n$, falls $H^{n+1}(G, \mathbb{Z}/p) = 0$, also $\text{cd}_p(\mathbb{Z}_p) \leq 1$. Andererseits gilt

$$H^1(\mathbb{Z}_p, \mathbb{Z}/p) \cong \text{Hom}_{\text{cont}}(\mathbb{Z}_p, \mathbb{Z}/p) \cong \text{Hom}(\mathbb{Z}_p/p\mathbb{Z}_p, \mathbb{Z}/p) = \mathbb{Z}/p,$$

also $\text{cd}_p(\mathbb{Z}_p) = 1$, woraus $\text{cd}(\widehat{\mathbb{Z}}) = \sup_p \text{cd}_p(\mathbb{Z}_p) = 1$ folgt.] Schließlich gilt $0 \rightarrow H_{\text{ur}}^1(K, A) \rightarrow H^1(K, A)$ nach Inflation–Restriktion. $\square$

Sei A endlich und unverzweigt mit $p \nmid |A|$. Bezüglich der lokalen Tate-Dualität (III.6.4) gilt:

- Der Cartier-duale Modul A' ist ebenfalls endlich und unverzweigt.
- Es gilt $H_{\text{ur}}^i(K, A)^\perp = H_{\text{ur}}^{2-i}(K, A')$ für $i = 0, 1, 2$.

Übung. (i) Zeige, dass μ_n unverzweigt ist, falls $p \nmid n$. (ii) Zeige, dass dann $H_{\text{ur}}^1(K, \mu_n) \cong \mathcal{O}_K^*/(\mathcal{O}_K^*)^n$ gilt. (Hinweis: Verwende, dass für $\mathcal{O}_K^{\text{ur}*} \leq K_{\text{ur}}^*$ die Gleichung $H_{\text{ur}}^1(K, \mathcal{O}_K^{\text{ur}*}) = 0$ gilt.)

III.8 Poitou–Tate-Dualität

Sei M ein endlicher $\text{Gal}(k)$ -Modul. **Ziel:** ein Lokal-global-Prinzip finden, das Auskunft über die Diagonalabbildungen gibt:

$$\beta^i: H^i(k, M) \rightarrow \prod_{v \in V(k)} H^i(k_v, M).$$

Konvention. Für $i = 0$ und $v \in V_\infty(k)$ soll $H^i(k_v, M)$ in diesem Abschnitt $\widehat{H}^0(k_v, M)$ bedeuten, also ist $H^0(k_v, M) = 0$ für komplexes v und

$$H^0(k_v, M) \cong M^{\text{Gal}(\mathbb{C}/\mathbb{R})}/N_{\text{Gal}(\mathbb{C}/\mathbb{R})}M$$

für reelles v .

Proposition III.8.1. *Der Modul M ist außerhalb endlich vieler $v \in V(k)$ unverzweigt (als $\text{Gal}(k_v)$ -Modul).*

Beweis. Die Untergruppe $G = \{\sigma \in \text{Gal}(k) \mid \sigma m = m \text{ für alle } m \in M\} \leq \text{Gal}(k)$ ist offen, hat also endlichen Index, und die zugehörige Körpererweiterung l/k ist an allen $v \nmid \text{discr}_{l/k}$ unverzweigt. Also wirkt $\text{Gal}(k_v^{\text{ur}}) \leq \text{Gal}(l_w) \leq \text{Gal}(l)$ für jedes $w \mid v \nmid \text{discr}_{l/k}$ trivial. $\square$

Definition III.8.2. Wir definieren $P^i(k, M)$ als das restringierte Produkt

$$P^i(k, M) = \prod'_{v \in V(k)} H^i(k_v, M) \quad \text{bezüglich } H_{\text{ur}}^i(k_v, M).$$

Aus III.7.2 folgt daher:

- $P^0(k, M) = \prod_v H^0(k_v, M)$ ist kompakt.
- $P^2(k, M) = \bigoplus_v H^2(k_v, M) = \prod_v H^2(k_v, M)$ ist diskret.
- $P^1(k, M) = \prod'_v H^1(k_v, M) = \prod_v H^1(k_v, M)$ ist lokal kompakt (die Notation „ $\prod$ “ wurde von Tate vorgeschlagen).

Außerdem gilt $P^i(k, M) = \bigoplus_{v \text{ reell}} H^i(k_v, M)$ für $i \geq 3$, denn $\text{cd}(\text{Gal}(k_v)) = 2$ für endliches v . [In der Tat gilt

$$\text{cd}(\text{Gal}(k_v)) \leq \underbrace{\text{cd}(\text{Gal}(k_v^{\text{ur}}))}_{\substack{\leq 1, \text{ „weil“} \\ \text{Br}(k_v^{\text{ur}}) = 0}} + \underbrace{\text{cd}(\text{Gal}(k_v^{\text{ur}}/k_v))}_{\leq 1 \text{ wie oben}} \leq 2,$$

und $H^2(k_v, \mu_n) \cong \mathbb{Z}/n\mathbb{Z}$ nach III.6.2.]

Proposition III.8.3. *Die Diagonalabbildung*

$$\beta^i = \beta_M^i: H^i(k, M) \longrightarrow \prod_{v \in V(k)} H^i(k_v, M)$$

hat ihr Bild in $P^i(k, M)$.

Beweis. Sei $\alpha \in H^i(k, M)$. Wähle l/k endlich galoissch so, dass $\text{Gal}(l)$ trivial auf M wirkt und α im Bild der Inflation $H^i(l/k, M) \longrightarrow H^i(k, M)$ liegt. Ist v unverzweigt in l/k und $w \mid v$ eine beliebige Stelle von l , so zeigt

$$\begin{array}{ccccc} H^i(l/k, M) & \xrightarrow{\text{inf}} & H^i(k, M) & \longrightarrow & H^i(k_v, M) \\ \downarrow & & & \nearrow & \\ H^i(l_w/k_v, M) & \longrightarrow & H^i(k_v^{\text{ur}}/k_v, M) & & \end{array}$$

für fast alle v , dass α nach $H_{\text{ur}}^i(k_v, M)$ abgebildet wird. $\square$

Proposition III.8.4 (Reelle lokale Dualität). *Sei M_0 ein endlicher $\text{Gal}(\mathbb{C}/\mathbb{R})$ -Modul. Dann definiert das Cup-Produkt eine perfekte Paarung endlicher abelscher 2-Gruppen*

$$\hat{H}^i(\mathbb{R}, M_0) \times \hat{H}^{2-i}(\mathbb{R}, M_0') \longrightarrow \text{Br } \mathbb{R} \cong \mathbb{Z}/2\mathbb{Z}.$$

Proposition III.8.5. *Die lokale Tate-Dualität induziert Isomorphismen*

$$P^0(k, M)^* \cong P^2(k, M') \quad \text{und} \quad P^1(k, M)^* \cong P^1(k, M').$$

Beweis. Für $i = 0, 1, 2$ gilt

$$P^i(k, M)^* = \left(\prod'_v H^i(k_v, M) \right)^* \cong \prod'_v H^i(k_v, M)^*$$

restringiert bezüglich $(H^i(k_v, M)/H_{\text{ur}}^i(k_v, M))^*$. Nach III.6.4 und III.8.4 gilt daher

$$P^i(k, M)^* \cong \prod'_v H^{2-i}(k_v, M')$$

restringiert bezüglich

$$(H^i(k_v, M)/H_{\text{ur}}^i(k_v, M))^* \cong H_{\text{ur}}^i(k_v, M)^\perp = H_{\text{ur}}^{2-i}(k_v, M')$$

für fast alle v : nämlich an den endlichen Stellen, an denen M unverzweigt ist und die Restklassencharakteristik $|M|$ nicht teilt. $\square$

Analog sei $\gamma^i: P^i(k, M) \rightarrow H^{2-i}(k, M')^*$ die duale Abbildung zu $\beta_{M'}^{2-i}: H^{2-i}(k, M') \rightarrow P^{2-i}(k, M')$. Wir erinnern daran, dass

$$\ker \beta_M^i = \text{III}^i(k, \emptyset, M) =: \text{III}^i(k, M)$$

gilt (siehe Abschnitt II.7).

Satz III.8.6 (Poitou–Tate). *(i) Für $i \geq 3$ gilt $H^i(k, M) \cong \bigoplus_{v \text{ reell}} H^i(k_v, M)$.*

(ii) Die Tate-Schafarewitsch-Gruppen $\text{III}^1(k, M')$ und $\text{III}^2(k, M)$ sind endlich und zueinander dual.

(iii) Es gibt eine neungliedrige exakte Sequenz

[illegible]

Die Randabbildung δ^1 ergibt sich als

$$\begin{aligned} H^2(k, M')^* &\longrightarrow \operatorname{coker}(\gamma^0) = \operatorname{coker}(\beta_{M'}^{2*}) = (\ker(\beta_{M'}^2))^* \\ &= (\operatorname{III}^2(k, M'))^* \stackrel{\text{(ii)}}{\cong} \operatorname{III}^1(k, M) \leq H^1(k, M), \end{aligned}$$

und analog für δ^2 .

Beispiel. $k = \mathbb{Q}$, $M = \mathbb{Z}/2$. (Zur Erinnerung: $(\mathbb{Z}/2)' \cong \mu_2 \cong \mathbb{Z}/2$.)

$$\begin{array}{ccccccc}
 0 & \longrightarrow & \mathbb{Z}/2 & \longrightarrow & \prod_{p \leq \infty} \mathbb{Z}/2 & \longrightarrow & \text{Br}(\mathbb{Q})[2]^* & \longrightarrow & 0 \\
 & & & & & & & & \uparrow \\
 & & & & & & & & \text{Br}(\mathbb{Q})[2] \longrightarrow \bigoplus_{p \leq \infty} \mathbb{Z}/2 \longrightarrow (\mathbb{Z}/2)^* \longrightarrow 0. \\
 & & & & & & & & \uparrow \\
 & & & & & & & & \mathbb{Q}^*/(\mathbb{Q}^*)^2 \longrightarrow \mathbb{I}_{\mathbb{Q}}/\mathbb{I}_{\mathbb{Q}}^2 \longrightarrow (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^* \longrightarrow 0 \\
 & & & & & & & & \uparrow
 \end{array}$$

Die beiden verschwindenden Randabbildungen erklären sich durch II.6.1 bzw. II.6.6 ($d = 2$).

Aus Satz II.6.4 wissen wir, dass

$$\mathbb{Z}/2 \cong \text{III}^1(\mathbb{Q}(\sqrt{7}), \mu_8) \cong \text{III}^2(\mathbb{Q}(\sqrt{7}), \mathbb{Z}/8),$$

also ist für $k = \mathbb{Q}(\sqrt{7})$ die erste Randabbildung nichttrivial, wenn $M = \mu_8$, und die zweite Randabbildung nichttrivial, wenn $M = \mathbb{Z}/8$.

Beachte, dass die zur Poitou–Tate-Sequenz für M duale Sequenz die Poitou–Tate-Sequenz für M' ist. Beachte auch, dass die Poitou–Tate-Sequenz topologisch die Form

$$\begin{array}{ccccccc}
 0 & \longrightarrow & \text{endlich} & \longrightarrow & \text{kompakt} & \longrightarrow & \text{kompakt} & \longrightarrow & 0 \\
 & & & & & & & & \uparrow \\
 & & & & & & & & \text{diskret} \longrightarrow \text{lokal kompakt} \longrightarrow \text{kompakt} \\
 & & & & & & & & \uparrow \\
 & & & & & & & & \text{diskret} \longrightarrow \text{diskret} \longrightarrow \text{endlich} \longrightarrow 0.
 \end{array}$$

hat.

Galoiskohomologie einfacher algebraischer Gruppen

IV.1 Nichtkommutative Kohomologie

Sei G eine proendliche Gruppe.

Definition IV.1.1. Eine G -Menge ist ein diskreter topologischer Raum A mit einer stetigen G -Wirkung. Trägt A zudem eine Gruppenstruktur, die von der Wirkung erhalten wird (${}^\sigma(ab) = {}^\sigma a {}^\sigma b$ für $a, b \in A$, $\sigma \in G$), so nennen wir A eine G -Gruppe.

Beachte, dass eine G -Gruppe mit abelschem A gerade ein diskreter G -Modul wie in Definition III.4.3 ist. Wir gehen wie in Kapitel I vor:

- Für eine G -Menge E setzen wir $H^0(G, E) = E^G$.
- Für eine G -Gruppe A setzen wir

$$Z^1(G, A) = \{a: G \longrightarrow A \text{ stetig} \mid a_{\sigma\tau} = a_\sigma {}^\sigma a_\tau \text{ für alle } \sigma, \tau \in G\}.$$

- Für $a, a' \in Z^1(G, A)$ definieren wir $a \sim a'$ genau dann, wenn es ein $b \in A$ gibt, sodass $a_\sigma = b^{-1} a'_\sigma {}^\sigma b$ für alle $\sigma \in G$ gilt.
- Setze $H^1(G, A) = Z^1(G, A) / \sim$ (punktierte Menge).

Man überprüft:

- $H^1(G, A) = \varinjlim_{U \trianglelefteq_o G} H^1(G/U, A^U)$.
- $H^i(G, A)$ ist für $i = 0, 1$ funktoriell in A .
- Für kommutatives A stimmt dies mit der bisherigen Definition überein.

Proposition IV.1.2 (vgl. Proposition I.2). *Seien $A \leq_G B$ G -Gruppen. Dann ist $G \curvearrowright B/A$ eine G -Menge (eine G -Gruppe, falls $A \trianglelefteq_G B$), und*

$$1 \longrightarrow H^0(G, A) \longrightarrow H^0(G, B) \longrightarrow H^0(G, B/A) \xrightarrow{\delta^0} H^1(G, A) \xrightarrow{i^1} H^1(G, B)$$

ist exakt, mit einem weiteren Pfeil $H^1(G, B) \xrightarrow{j^1} H^1(G, B/A)$, falls A normal ist.

Beschreibung von δ^0 : Für $bA \in (B/A)^G$ setze $\delta^0(bA) = [b^{-1} {}^\sigma b]$.

Übung. (i) Überprüfe, dass $\delta^0(bA)$ eine wohldefinierte Kohomologieklass ist, und beweise IV.1.2.

Beachte, dass es für $A \leq_G B$ eine Rechtswirkung $H^1(G, A) \curvearrowright (B/A)^G$ gibt, die wie folgt definiert ist: Für $bA \in (B/A)^G$ und $[a] \in H^1(G, A)$ setze

$$[a] \cdot bA = [\sigma \longmapsto b^{-1} a_\sigma {}^\sigma b].$$

Proposition IV.1.3. $i^1(\alpha) = i^1(\alpha')$ gilt genau dann, wenn $\alpha' \in \alpha \cdot (B/A)^G$.

Beweis. Schreibe $\alpha = [a]$, $\alpha' = [a']$. Dann gibt es ein $b \in B$ mit $a'_\sigma = b^{-1}a_\sigma \sigma b$. Dann gilt

$$\sigma b (a'_\sigma)^{-1} = a_\sigma^{-1} b = b \underbrace{(b^{-1} a_\sigma^{-1} b)}_{\in A},$$

also $bA \in (B/A)^G$ und $[a] \cdot bA = [a']$. Die Umkehrung ist klar. $\square$

Proposition IV.1.4. Ist $A \trianglelefteq_G B$ zentral, so ist

$$H^1(G, B) \longrightarrow H^1(G, B/A) \xrightarrow{\delta^1} H^2(G, A)$$

exakt, und δ^0 ist ein Homomorphismus.

Beschreibung von δ^1 : Wähle für $a \in Z^1(G, B/A)$ einen mengentheoretischen Schnitt $s: B/A \rightarrow B$ und setze $b = s \circ a$ (dies ist stetig, da B/A und B diskret sind). Setze

$$\delta^1([a]) = [(\sigma, \tau) \mapsto b_\sigma \sigma b_\tau b_{\sigma\tau}^{-1}].$$

IV.2 Twisten

Sei $1 \rightarrow A \xrightarrow{i} B \xrightarrow{p} C \rightarrow 1$ eine kurze exakte Sequenz von G -Gruppen, und sei $\beta = [b] \in H^1(G, B)$. Um die Faser $(p^1)^{-1}(p^1(\beta))$ der Abbildung

$$p^1: H^1(G, B) \longrightarrow H^1(G, C)$$

zu beschreiben, definieren wir die *getwistete G -Gruppe* ${}_bB$, die als Gruppe mit B übereinstimmt, deren neue G -Wirkung aber durch

$$\sigma' x := b_\sigma \cdot \sigma x \cdot b_\sigma^{-1} \quad \text{für } x \in B, \sigma \in G$$

gegeben ist. Dies definiert auch ${}_bA$, da $A \trianglelefteq B$, und ${}_bC := {}_{p \circ b}C$. Wir erhalten also

$$1 \longrightarrow {}_bA \longrightarrow {}_bB \longrightarrow {}_bC \longrightarrow 1$$

und entsprechend

$$\begin{array}{ccccc} H^1(G, A) & \xrightarrow{i^1} & H^1(G, B) & \xrightarrow{p^1} & H^1(G, C) \\ & & \tau_b \uparrow \cong & & \tau_{p \circ b} \uparrow \cong \\ H^1(G, {}_bA) & \xrightarrow{{}_b i^1} & H^1(G, {}_bB) & \xrightarrow{{}_b p^1} & H^1(G, {}_bC) \end{array}$$

wobei τ_b , definiert durch $\tau_b([x]) = [x \cdot b]$, und $\tau_{p \circ b}$ Bijektionen sind, die die triviale Klasse auf β bzw. $p^1(\beta)$ abbilden. Dies überführt die Faser über $p^1(\beta)$ in $\ker {}_b p^1$. Analog erhalten wir für eine zentrale Erweiterung

$$1 \longrightarrow A \xrightarrow{i} B \xrightarrow{p} C \longrightarrow 1$$

von G -Gruppen und $\gamma = [c] \in H^1(G, C)$

$$\begin{array}{ccccc} H^1(G, B) & \longrightarrow & H^1(G, C) & \xrightarrow{\delta^1} & H^2(G, A) \\ & & \tau_c \uparrow \cong & & \\ H^1(G, {}_cB) & \longrightarrow & H^1(G, {}_cC) & \xrightarrow{{}_c \delta^1} & H^2(G, A) \end{array}$$

mit

$$\delta^1(\tau_c(\gamma')) = {}_c \delta^1(\gamma') + \delta^1(\gamma), \quad \text{also} \quad (\delta^1)^{-1}(\delta^1(\gamma)) \cong \ker {}_c \delta^1.$$

IV.3 Nichtkommutative Galoiskohomologie und Formen

Von nun an sei K vollkommen. Wir erinnern an Kapitel I:

Meta-Satz IV.3.1. *Ist L/K galoissch und X ein „ K -Objekt“, so gilt*

$$\underbrace{\{Y \text{ ein } K\text{-Objekt} \mid X \cong_L Y\}}_{\text{„}L/K\text{-Formen von } X\text{“}} / \cong_K \xrightarrow{1:1} H^1(L/K, \text{Aut}_L X).$$

Meta-Beweis. Sei Y ein K -Objekt und $f: X \xrightarrow[\sim]{L} Y$. Setze

$$a: \text{Gal}(L/K) \longrightarrow \text{Aut}_L X, \quad \sigma \longmapsto a_\sigma = f^{-1} \circ {}^\sigma f.$$

Dann gilt

$$\begin{aligned} a_{\sigma\tau} &= f^{-1} \circ {}^{\sigma\tau} f = f^{-1} \circ {}^\sigma (f \circ (f^{-1} \circ {}^\tau f)) \\ &= (f^{-1} \circ {}^\sigma f) \circ {}^\sigma (f^{-1} \circ {}^\tau f) = a_\sigma \circ {}^\sigma a_\tau, \end{aligned}$$

also können wir $Y \longmapsto [a] \in H^1(L/K, \text{Aut}_L X)$ zuordnen. Da für zwei $f, f': X \xrightarrow[\sim]{L} Y$ die Gleichung $f' = f \circ \underbrace{(f^{-1} \circ f')}_{=: b \in \text{Aut}_L X}$ gilt, erhalten wir

$$a'_\sigma := (f')^{-1} \circ {}^\sigma f' = b^{-1} \circ (f^{-1} \circ {}^\sigma f) \circ {}^\sigma b,$$

also ist $[a] = [a']$ wohldefiniert.

Injektivität. Angenommen, Y_1 und Y_2 definieren $[f_1^{-1} \circ {}^\sigma f_1] = [f_2^{-1} \circ {}^\sigma f_2]$. Dann gibt es ein $b \in \text{Aut}_L X$ mit

$$f_2^{-1} \circ {}^\sigma f_2 = b^{-1} \circ f_1^{-1} \circ {}^\sigma f_1 \circ {}^\sigma b = (f_1 \circ b)^{-1} \circ {}^\sigma (f_1 \circ b).$$

Daher gilt

$$\begin{aligned} {}^\sigma (f_2 \circ b^{-1} \circ f_1^{-1}) &= {}^\sigma f_2 \circ {}^\sigma (f_1 \circ b)^{-1} \\ &= {}^\sigma f_2 \circ {}^\sigma f_2^{-1} \circ f_2 \circ b^{-1} \circ f_1^{-1} \\ &= f_2 \circ b^{-1} \circ f_1^{-1}, \end{aligned}$$

also ist der Isomorphismus $f_2 \circ b^{-1} \circ f_1^{-1}$ über K definiert; folglich $Y_1 \cong_K Y_2$.

Surjektivität. Verwende $[a] \in H^1(L/K, \text{Aut}_L X)$, um die Wirkung $\text{Gal}(L/K) \curvearrowright X_L$ zu „twisten“, und setze ${}_a X = X_L / \text{Gal}(L/K)$. Dann gilt ${}_a X \longmapsto [a]$. $\square$

Bemerkung. Damit $X_L / \text{Gal}(L/K)$ ein K -Objekt definiert, muss man in der Regel Voraussetzungen stellen. Ist X beispielsweise eine K -Varietät V , so sollte sie quasiprojektiv sein (zum Beispiel eine algebraische Gruppe).

Ebenso ist $\text{Aut } V$ nicht immer darstellbar, und selbst wenn es darstellbar ist, muss das darstellende Objekt nicht von endlichem Typ sein. Bei der Anwendung des Meta-Satzes ist also etwas Vorsicht geboten.

Wir sehen, dass K -Objekte, deren L -Automorphismengruppen als $\text{Gal}(L/K)$ -Gruppen isomorph sind, bijektiv einander entsprechende L/K -Formen haben. Beispielsweise werden Quaternionenalgebren und Severi–Brauer-Kurven beide durch $H^1(K, \text{PGL}_2)$ klassifiziert.

Sei $\text{char } K \neq 2$. Sei $q_0 = \langle -1, -1, 1 \rangle$ mit Diskriminante 1, und schreibe $\text{SO}_3 = \text{SO}(q_0)$ für die zerfallende Gruppe. Die volle Automorphismengruppe einer ternären quadratischen Form q ist

$O(q)$, auch wenn ihre Diskriminante 1 ist: $-\text{id}$ erhält q , hat aber Determinante -1 . Wegen $O(q_0) \cong \mu_2 \times \text{SO}_3$ gilt

$$H^1(K, O(q_0)) \cong K^*/(K^*)^2 \times H^1(K, \text{SO}_3).$$

Der erste Faktor erfasst die Diskriminante. Somit klassifiziert $H^1(K, \text{SO}_3)$ genau die nichtausgearteten ternären quadratischen Formen mit Diskriminante 1. Zusammen mit $\text{SO}_3 \cong \text{PGL}_2$ ergeben sich daraus die Korrespondenzen

$$\begin{array}{ccccc} \text{Quaternionen-} & \xleftarrow{1:1} & \text{Severi-Brauer-} & \xleftarrow{1:1} & \text{nichtausgeartete ternäre} \\ \text{algebren} & & \text{Kurven} & & \text{quadratische Formen mit Diskriminante 1} \end{array}$$

zwischen K -Isomorphieklassen.

IV.4 Affine algebraische Gruppenschemata

Von nun an sei $\text{char}(K) = 0$.

Definition IV.4.1. Eine (*affine*) (*algebraische*) K -Gruppe (bzw. ein Gruppenschema) ist ein Funktor $G: K\text{-Alg} \rightarrow \text{Set}$, der durch eine endlich erzeugte K -Algebra $\mathcal{O}(G)$ darstellbar ist, zusammen mit einer natürlichen Transformation $m: G \times G \rightarrow G$, sodass für alle $A \in K\text{-Alg}$

$$m_A: G(A) \times G(A) \rightarrow G(A)$$

eine Gruppenstruktur auf $G(A)$ definiert. *Morphismen* sind natürliche Transformationen, die die Gruppenstruktur erhalten.

Beispiele. • μ_n mit $\mathcal{O}(\mu_n) = K[X]/(X^n - 1)$.

- Eine endliche Gruppe M definiert ein *konstantes Gruppenschema* M mit $\mathcal{O}(M) = K^M \cong \prod_{g \in M} K$, sodass

$$M(K) = \text{Hom}_{K\text{-alg}}(K^M, K) \cong M$$

(die Standardbasis (e_g) von K^M besteht aus Idempotenten, und $1 = \phi(1) = \sum_{g \in M} \underbrace{\phi(e_g)}_{\in \{0,1\}}$).

- SL_n mit $\mathcal{O}(\text{SL}_n) = K[X_{11}, \dots, X_{nn}]/(\det(X_{ij}) - 1)$.
- Sei G eine K -Gruppe und L/K eine Körpererweiterung. Dann definiert Präkomposition mit $L\text{-Alg} \rightarrow K\text{-Alg}$ die L -Gruppe G_L mit $\mathcal{O}(G_L) = L \otimes_K \mathcal{O}(G)$, genannt *Basiserweiterung* von G von K nach L .

Proposition IV.4.2. Sei G eine algebraische K -Gruppe und L/K eine Galoiserweiterung. Dann ist $G(L)$ durch die funktorielle Wirkung eine $\text{Gal}(L/K)$ -Gruppe.

Beweis. Sei $a \in G(L) = \text{Hom}_{K\text{-alg}}(K[X_1, \dots, X_n]/(\dots), L)$ durch $l_1, \dots, l_n \in L$ bestimmt, und setze $L_0 = K(l_1, \dots, l_n)$. Dann gilt

$$\text{Gal}(L/K)_a \supseteq \text{Gal}(L/L_0) \leq_o \text{Gal}(L/K).$$

Für $a, b \in G(L)$ und $\sigma \in \text{Gal}(L/K)$ gilt

$$\sigma(ab) = G(\sigma)(m_L(a, b)) \stackrel{\text{nat.}}{=} m_L(G(\sigma)(a), G(\sigma)(b)) = \sigma a \sigma b. \quad \square$$

Eine (*normale*) *algebraische Untergruppe* $H \leq G$ ist ein Unterfunctor, sodass $H(A) \leq G(A)$ für alle $A \in K\text{-Alg}$ eine (*normale*) Untergruppe ist und H durch einen Quotienten von $\mathcal{O}(G)$ dargestellt wird. Es gilt

$$\{H \leq G\} \xleftarrow{1:1} \{H \leq_c G(\bar{K}) \mid \text{Gal}(K)(H) \subseteq H\}.$$

Morphismen $G_1 \rightarrow G_2$ haben Kerne, und für $H \trianglelefteq G$ ist die *Faktorgruppe* G/H definiert (subtil...).

IV.5 Klassifikation einfacher Gruppen über algebraisch abgeschlossenen Körpern

Wir vereinbaren, dass sich nicht eigens definierte Eigenschaften von G (z. B. „abelsch“ oder „zusammenhängend“) auf $G(\overline{K})$ beziehen.

Definition IV.5.1. Eine algebraische K -Gruppe G heißt *einfach*, wenn sie zusammenhängend und nichtkommutativ ist und jede echte normale Untergruppe von G endlich ist. Wir nennen G *absolut einfach*, wenn darüber hinaus $G_{\overline{K}}$ einfach ist.

Definition IV.5.2. Eine einfache K -Gruppe G heißt *einfach zusammenhängend*, wenn jeder surjektive Morphismus $\overline{G} \rightarrow G$ mit endlichem Kern und zusammenhängendem $\overline{G}$ einen trivialen Kern hat.

Satz IV.5.3. Sei K algebraisch abgeschlossen. Dann ist jede einfach zusammenhängende einfache algebraische K -Gruppe G zu genau einer der Gruppen SL_{n+1} ($n \geq 1$), Spin_{2n+1} ($n \geq 2$), Sp_n ($n \geq 3$), Spin_{2n} ($n \geq 4$), oder zu einer der fünf exzeptionellen Gruppen isomorph.

„Beweis“. Wähle einen *maximalen Torus* $(\mathrm{GL}_1)^n \cong T \leq G$. Dann definiert (G, T) ein Paar $(\mathfrak{g}, \mathfrak{h})$ aus einer *einfachen Lie-Algebra* und einer *Cartan-Unteralgebra* $\mathfrak{h} = \mathrm{Lie}(T)$, das ein *irreduzibles Wurzelsystem* $\Phi(\mathfrak{g}, \mathfrak{h}) \leq \mathfrak{h}^*$ liefert. Diese werden durch *Dynkin-Diagramme* $\Delta = \Delta(\mathfrak{g}, \mathfrak{h})$ klassifiziert und bilden eine vollständige Invariante:

Typ	Dynkin-Diagramm	Lie-Algebra
A_n ($n \geq 1$)		$\mathfrak{sl}_{n+1}$
B_n ($n \geq 2$)		$\mathfrak{so}_{2n+1}$
C_n ($n \geq 3$)		$\mathfrak{sp}_n$
D_n ($n \geq 4$)		$\mathfrak{so}_{2n}$
E_6		$\mathfrak{e}_6$
E_7		$\mathfrak{e}_7$
E_8		$\mathfrak{e}_8$
F_4		$\mathfrak{f}_4$
G_2		$\mathfrak{g}_2$

Exzeptionelle Typen

www.math.uni-duesseldorf.de/~kammeyer/lie-algebren.pdf

□

Die A_n - G_2 -Klassifikation bleibt für allgemeine K mit $\mathrm{char} K = 0$ unter der Annahme gültig, dass G über K zerfällt, d. h., dass es einen maximalen Torus $(\mathrm{GL}_1)^n \cong T \leq G$ gibt, sodass $T_{\overline{K}} \leq G_{\overline{K}}$ weiterhin maximal ist.

Satz IV.5.4. Die K -Gruppen SL_{n+1} ($n \geq 1$), $\mathrm{Spin}(n, n+1)$ ($n \geq 2$), Sp_n ($n \geq 3$), $\mathrm{Spin}(n, n)$ ($n \geq 4$) und die über K zerfallenden Gruppen vom Typ E_6 , E_7 , E_8 , F_4 und G_2 bilden ein vollständiges Repräsentantensystem für die Isomorphieklassen der über K zerfallenden einfach zusammenhängenden absolut einfachen K -Gruppen.

Ergebnis

Klassifikation über $\overline{K}$ durch den *Cartan–Killing-Typ* A_n – G_2 . Jeder Typ hat eine eindeutige über K zerfallende K -Form G_0 .

Ziel

Finde alle anderen K -Formen oder äquivalent (nach IV.3.1): Bestimme für jede über K zerfallende Form G_0 die Menge $H^1(K, \text{Aut } G_0)$.

IV.6 Klassifikation einfacher Gruppen über p -adischen Körpern

Sei G_0 eine über K zerfallende einfach zusammenhängende absolut einfache K -Gruppe mit Dynkin-Diagramm Δ . Dann ist $\text{Aut } G_0$ eine K -Gruppe, und

$$1 \longrightarrow \text{Ad } G_0 \longrightarrow \text{Aut } G_0 \xrightarrow{\quad} \text{Sym } \Delta \longrightarrow 1$$

↖

ist eine zerfallende exakte Sequenz von $\text{Gal}(K)$ -Gruppen. Dabei besteht $\text{Ad } G_0$ aus inneren Automorphismen, und $\text{Sym } \Delta$ ist ein konstantes Gruppenschema. Aus IV.1.2 erhalten wir

$$1 \longrightarrow H^1(K, \text{Ad } G_0) \longrightarrow H^1(K, \text{Aut } G_0) \xrightarrow{p} H^1(K, \text{Sym } \Delta) \longrightarrow 1.$$

↖
s

Es gilt $\text{Sym } \Delta = 1$, also $H^1(K, \text{Sym } \Delta) \cong 1$, wenn G_0 vom Typ $A_1, B_n, C_n, E_7, E_8, F_4$ oder G_2 ist. Nach III.5.7 erhalten wir $H^1(K, \text{Sym } \Delta) \cong K^*/(K^*)^2$, wenn G_0 vom Typ A_n ($n \geq 2$), D_n ($n \geq 5$) oder E_6 ist (im Typ D_4 gilt $\text{Sym } \Delta \cong S_3 \cong \mathbb{Z}/3 \rtimes \mathbb{Z}/2$: „Triality“).

Für $\alpha = [a] \in H^1(K, \text{Sym } \Delta)$ entspreche $[G_1]$ gemäß IV.3.1 dem Element $s(\alpha)$. Die K -Gruppe G_1 heißt die *quasizerfallende Form mit Diskriminante* α . Durch Twisten erhalten wir

$$\begin{array}{ccccccc} 1 & \rightarrow & H^1(K, \text{Ad } G_0) & \rightarrow & H^1(K, \text{Aut } G_0) & \xrightarrow{p} & H^1(K, \text{Sym } \Delta) \rightarrow 1 \\ & & \uparrow & & \uparrow & & \uparrow \\ & & 1 \mapsto [G_1] & & 1 \mapsto \alpha & & \\ & & | & & | & & \\ 1 & \rightarrow & H^1(K, \text{Ad } G_1) & \rightarrow & H^1(K, \text{Aut } G_1) & \xrightarrow{\text{soa}p} & H^1(K, {}_a(\text{Sym } \Delta)) \rightarrow 1 \end{array}$$

Dabei gilt $\text{soa}(\text{Ad } G_0) \cong_{\text{Gal}(K)} \text{Ad } G_1$, $\text{soa}(\text{Aut } G_0) \cong_{\text{Gal}(K)} \text{Aut } G_1$ und ${}_a(\text{Sym } \Delta) = \text{Sym } \Delta$, sofern G_1 nicht vom Typ D_4 ist. Setze

$$\Gamma_\alpha := {}_a(\text{Sym } \Delta)(K),$$

die Gruppe der K -rationalen Automorphismen des getwisteten Dynkin-Diagramms. Somit ist $\Gamma_\alpha = \text{Sym } \Delta$ außerhalb des Typs D_4 ; im Typ D_4 ist sie der Zentralisator des Bildes von a in S_3 . Nach IV.1.3 gilt

$$p^{-1}(\alpha) \cong H^1(K, \text{Ad } G_1)/\Gamma_\alpha.$$

Es bleibt also, $H^1(K, \text{Ad } G_1)/\Gamma_\alpha$ für alle quasizerfallenden Formen G_1 zu bestimmen. Nach IV.1.4 liefert die Sequenz

$$1 \longrightarrow Z(G_1) \longrightarrow G_1 \longrightarrow \text{Ad } G_1 \longrightarrow 1$$

die exakte Sequenz

$$H^1(K, G_1) \longrightarrow H^1(K, \text{Ad } G_1) \xrightarrow{\delta^1} H^2(K, Z(G_1)),$$

und δ^1 ist Γ_α -äquivariant (beachte, dass Γ_α auf $Z(G_1)$ durch K -Automorphismen wirkt).

Satz IV.6.1 (M. Kneser). *Sei $K/\mathbb{Q}_p$ endlich und G eine einfach zusammenhängende einfache K -Gruppe. Dann gilt $H^1(K, G) = \{1\}$.*

Beweis. Eine Untersuchung durch Fallunterscheidung. □

Korollar IV.6.2. *Für endliches $K/\mathbb{Q}_p$ ist die Abbildung δ^1 eine Bijektion.*

Beweis. Injektivität: Nach dem Vorangegangenen gilt $\ker \delta^1 = \{1\}$. Durch Twisten erhalten wir

$$(\delta^1)^{-1}(\delta^1([a])) = \ker {}_a\delta^1 = \{1\}$$

für alle $[a] \in H^1(K, \text{Ad } G_1)$, ebenfalls nach dem Vorangegangenen. Die Surjektivität ist ein „Nebenprodukt“ des Beweises von IV.6.1. □

Bemerkung IV.6.3. Die Surjektivität gilt auch über Zahlkörpern.

Schließlich liefert für endliches $K/\mathbb{Q}_p$ die lokale Tate-Dualität (III.6.4)

$$H^2(K, Z(G_1)) \cong H^0(K, Z(G_1)')^*,$$

was sich leicht berechnen lässt. Ist beispielsweise G_1 vom Typ A_1 , B_n , C_n oder E_7 , so gilt $Z(G_1) = \mu_2$, also

$$H^0(K, Z(G_1)')^* \cong H^0(K, \mathbb{Z}/2)^* \cong \mathbb{Z}/2.$$

Die Wirkung $\Gamma_\alpha \curvearrowright H^2(K, Z(G_1))$ muss trivial sein, wenn $H^2(K, Z(G_1))$ die Ordnung eins oder zwei hat. In den Typen A_n ($n \geq 2$), D_{2n-1} ($n \geq 3$) und E_6 wirkt $\Gamma_\alpha = \text{Sym } \Delta \cong \mathbb{Z}/2$ durch Inversion. Im Typ D_{2n} ($n \geq 3$) wirkt die geometrische Diagrammgruppe $\text{Sym } \Delta \cong \mathbb{Z}/2$ auf $Z(G_1)(\bar{K}) \cong (\mathbb{Z}/2)^2$ als Untergruppe der Ordnung zwei von $\text{Aut}((\mathbb{Z}/2)^2) \cong S_3$; im Typ D_4 ist die geometrische Diagrammgruppe die volle Automorphismengruppe S_3 . Die K -rationale Wirkung ist die Einschränkung auf Γ_α . Die Ergebnisse lassen sich in der folgenden Tabelle zusammenfassen.

Typ von G_1	1A_n	${}^2A_{2n-1}$	${}^2A_{2n}$	B_n	C_n	${}^1D_{2n-1}$	${}^2D_{2n-1}$
$H^2(K, Z(G_1))$	$\mathbb{Z}/(n+1)$	$\mathbb{Z}/2$	0	$\mathbb{Z}/2$	$\mathbb{Z}/2$	$\mathbb{Z}/4$	$\mathbb{Z}/2$
$ p^{-1}(\alpha) $	$\left\lfloor \frac{n+3}{2} \right\rfloor$	2	1	2	2	3	2

${}^1D_{2n}$	${}^2D_{2n}$	3D_4	6D_4	1E_6	2E_6	E_7	E_8	F_4	G_2
$(\mathbb{Z}/2)^2$	$\mathbb{Z}/2$	0	0	$\mathbb{Z}/3$	0	$\mathbb{Z}/2$	0	0	0
$(2 \text{ für } n=2)$	2	1	1	2	1	2	1	1	1

IV.7 Klassifikation einfacher Gruppen über Zahlkörpern

Sei G_0 eine über k zerfallende einfach zusammenhängende absolut einfache k -Gruppe. Aus dem vorigen Abschnitt sehen wir, dass sich die Bestimmung von $H^1(k, \text{Aut } G_0)$ auf die Bestimmung folgender Mengen aufteilt:

- (i) $H^1(k, \text{Sym } \Delta)$ und
- (ii) $H^1(k, \text{Ad } G_1)/\Gamma_\alpha$ mit $[G_1] = s(\alpha)$ für $\alpha = [a] \in H^1(k, \text{Sym } \Delta)$.

Dabei ist $\Gamma_\alpha = {}_a(\text{Sym } \Delta)(k)$ wie in Abschnitt IV.6. (i) Sofern G_0 nicht vom Typ D_4 ist, gilt $\text{Sym } \Delta \cong 1$ oder $\mathbb{Z}/2$, also $H^1(k, \text{Sym } \Delta) \cong 1$ oder $k^*/(k^*)^2$ nach III.5.7. Wie im Beispiel zur Poitou–Tate-Sequenz lassen sich solche globalen Quadratklassen durch

$$0 \longrightarrow k^*/(k^*)^2 \longrightarrow \mathbb{I}_k/\mathbb{I}_k^2 \longrightarrow (k^*/(k^*)^2)^* \longrightarrow 0$$

lokal vorschreiben (wobei $*$ das Pontrjagin-Dual bezeichnet). (ii) Wir haben ein Diagramm

$$\begin{array}{ccc} H^1(k, \text{Ad } G_1) & \xrightarrow{\text{IV.6.3}} & H^2(k, Z(G_1)) \\ \downarrow & & \downarrow \\ \prod_{v \in V_f(k)} H^1(k_v, \text{Ad } G_1) & \xrightarrow[\text{IV.6.2}]{\cong} & \prod_{v \in V_f(k)} H^2(k_v, Z(G_1)). \end{array}$$

Da $Z(G_1)$ ein endlicher kommutativer $\text{Gal}(k)$ -Modul ist, zeigt die Poitou–Tate-Dualität sogar, dass

$$\begin{array}{ccc} H^1(k, \text{Ad } G_1) & \xrightarrow{\text{IV.6.3}} & H^2(k, Z(G_1)) \\ \downarrow & & \downarrow \\ \bigoplus_{v \in V_f(k)} H^1(k_v, \text{Ad } G_1) & \xrightarrow[\text{IV.6.2}]{\cong} & \bigoplus_{v \in V_f(k)} H^2(k_v, Z(G_1)). \end{array}$$

Satz IV.7.1 (Kneser, Harder, Chernousov). *Sei G eine einfach zusammenhängende absolut einfache k -Gruppe. Dann gilt*

$$H^1(k, G) \xrightarrow{\cong} \prod_{v \in V_\infty(k)} H^1(k_v, G).$$

Ist also k total imaginär, so liefern die exakte Sequenz und Twisten

$$\begin{array}{ccc} H^1(k, \text{Ad } G_1)/\Gamma_\alpha & \xrightarrow{\cong} & H^2(k, Z(G_1))/\Gamma_\alpha \\ \downarrow & & \downarrow \bar{\beta}_{Z(G_1)}^2 \\ \left(\bigoplus_{v \in V_f(k)} H^1(k_v, \text{Ad } G_1) \right) / \Gamma_\alpha & \xrightarrow{\cong} & \left(\bigoplus_{v \in V_f(k)} H^2(k_v, Z(G_1)) \right) / \Gamma_\alpha. \end{array}$$

Dabei wirkt die eine globale Gruppe Γ_α diagonal auf jeder gesamten direkten Summe. Die Abbildung $\bar{\beta}_{Z(G_1)}^2$ wird vom Lokalisierungshomomorphismus $\beta_{Z(G_1)}^2$ vor dem Übergang zu den Bahnen induziert. Außerdem prüft man durch Fallunterscheidung, dass $\ker \beta_{Z(G_1)}^2 = 0$. Die Poitou–Tate-Sequenz

$$0 \longrightarrow H^2(k, Z(G_1)) \xrightarrow{\beta^2} \bigoplus_v H^2(k_v, Z(G_1)) \xrightarrow{\gamma^2} H^0(k, Z(G_1)')^* \longrightarrow 0$$

vervollständigt somit die Klassifikation.

Nun lassen wir zu, dass k reelle Stellen hat, und betrachten

$$\begin{array}{ccccccc}
 H^1(k, Z(G_1)) & \longrightarrow & H^1(k, G_1) & \longrightarrow & H^1(k, \text{Ad } G_1) & \xrightarrow{\delta^1} & H^2(k, Z(G_1)) \\
 \downarrow & & \cong \downarrow & & \downarrow \eta & & \downarrow \beta_{Z(G_1)}^2 \\
 \bigoplus_{v \text{ reell}} H^1(k_v, Z(G_1)) & \longrightarrow & \bigoplus_{v \text{ reell}} H^1(k_v, G_1) & \longrightarrow & \bigoplus_v H^1(k_v, \text{Ad } G_1) & \xrightarrow{\bigoplus_v \delta_v^1} & \bigoplus_v H^2(k_v, Z(G_1)) \\
 & & & & & & \downarrow \gamma^2 \\
 & & & & & & H^0(k, Z(G_1)')^*.
 \end{array}$$

Satz IV.7.2. Die Abbildung η ist injektiv, und es gilt $\text{im } \eta = \ker(\gamma^2 \circ \bigoplus_v \delta_v^1)$.

Beweis. Durch Diagrammjagd im Sinne eines „Viererlemmas“ ergibt sich $\ker \eta = 1$. Durch Twisten folgt die Injektivität von η . Die Inklusion $\text{im } \eta \subseteq \ker(\gamma^2 \circ \bigoplus_v \delta_v^1)$ folgt unmittelbar aus der Exaktheit der vertikalen Poitou–Tate-Sequenz.

Sei $(\alpha_v) \in \ker(\gamma^2 \circ \bigoplus_v \delta_v^1)$. Dann gibt es $\beta = [b] \in H^1(k, \text{Ad } G_1)$ mit

$$\beta^2(\delta^1(\beta)) = \bigoplus_v \delta_v^1(\alpha_v).$$

Twisten mit b liefert die kurze exakte Sequenz

$$\begin{array}{ccccccc}
 1 & \longrightarrow & Z(G_1) & \longrightarrow & {}_b(G_1) & \longrightarrow & {}_b(\text{Ad } G_1) \longrightarrow 1 \\
 & & \parallel & & \parallel & & \parallel \\
 1 & \longrightarrow & Z(G_2) & \longrightarrow & G_2 & \longrightarrow & \text{Ad } G_2 \longrightarrow 1
 \end{array}$$

wobei G_2 die durch β definierte innere k -Form von G_1 ist. Im zugehörigen Diagramm

$$\begin{array}{ccccccc}
 H^1(k, G_2) & \xrightarrow{p^1} & H^1(k, \text{Ad } G_2) & \xrightarrow{\delta^1} & H^2(k, Z(G_2)) \\
 \cong \downarrow & & \downarrow \eta & & \downarrow \beta^2 \\
 \bigoplus_{v \text{ reell}} H^1(k_v, G_2) & \xrightarrow{\bigoplus p^1} & \bigoplus_v H^1(k_v, \text{Ad } G_2) & \xrightarrow{\bigoplus \delta_v^1} & \bigoplus_v H^2(k_v, Z(G_2)),
 \end{array}$$

entspricht die Familie $(\alpha_v) \in \bigoplus_v H^1(k_v, \text{Ad } G_1)$ einer Familie $(\alpha'_v) \in \bigoplus_v H^1(k_v, \text{Ad } G_2)$ mit $(\alpha'_v) \in \ker \bigoplus_v \delta_v^1 = \text{im } \bigoplus p^1$. Also gibt es $\alpha' \in \text{im } p^1$ mit $\eta(\alpha') = (\alpha'_v)$. Bei der Rückübersetzung entspricht $\alpha' \in H^1(k, \text{Ad } G_2)$ einer Klasse $\alpha \in H^1(k, \text{Ad } G_1)$, deren Lokalisierungen die Familie (α_v) ergeben. $\square$

Somit können wir lokale Klassen $\alpha_v \in H^1(k_v, \text{Ad } G_1)$, die für fast alle v trivial sind, unter der Bedingung $\gamma^2(\bigoplus_v \delta_v(\alpha_v)) = 0$ vorschreiben und erhalten eine eindeutige globale Klasse $\xi \in H^1(k, \text{Ad } G_1)$, die die vorgeschriebenen lokalen Klassen realisiert. Innere k -Formen von G_1 entsprechen eindeutig den Γ_α -Bahnen in $H^1(k, \text{Ad } G_1)$, wobei α die fest gewählte Klasse in $H^1(k, \text{Sym } \Delta)$ ist. Damit ist die Klassifikation der einfach zusammenhängenden absolut einfachen k -Gruppen abgeschlossen.