Über die Zetafunktion von Formen von Fermatgleichungen

DISSERTATION ZUR ERLANGUNG DES DOKTORGRADES
DER NATURWISSENSCHAFTEN (DR. RER. NAT.)
DER MATHEMATISCHEN FAKULTÄT
DER UNIVERSITÄT REGENSBURG

vorgelegt von

Lars Brünjes
aus Köln

2002

Promotionsgesuch eingereicht am: 12. April 2002
Die Arbeit wurde angeleitet von: Prof. Dr. Uwe Jannsen
Prüfungsausschuß: Prof. Dr. G. Tamme, Prof. Dr. U. Jannsen,
Prof. Dr. K. Künnemannn, Prof. Dr. W. Hackenbroch

Einleitung

Versuchte man, ein mathematisches Gebiet durch die in ihm untersuchten Gleichungen zu charakterisieren, so wären diese im Falle der Algebraischen Geometrie polynomiale Gleichungen über beliebigen Ringen, im Falle der Zahlentheorie bzw. Arithmetischen Geometrie spezieller polynomiale Gleichungen über Zahlkörper, deren Ganzheitsringen oder endlichen Körpern.

Ein besonders berühmtes Beispiel ist die *Fermatgleichung P_n^m über R*:

$$X_1^m + X_2^m + \ldots + X_n^m = 0$$

für natürliche Zahlen $m, n \geq 2$ und Unbestimmte $X_1, \ldots, X_n$ aus R. Im Falle $m \geq 3$, $n = 3$ und $R = \mathbb{Z}$ ist sie Gegenstand der berühmten, 1993 von Andrew Wiles bewiesenen, *Fermatschen Vermutung*; im Falle $R = \mathbb{F}_q$ ein endlicher Körper diente sie André Weil 1949 in seinem wegweisenden Artikel [Wei49] als Motivation zur Formulierung der *Weil-Vermutungen*, deren endgültiger Beweis durch Pierre Deligne im Jahre 1973 zweifellos zu einem der Höhepunkte der Mathematik des 20. Jahrhunderts gehört.

Auch bei vielen anderen aktuellen Problemen der Algebraischen Geometrie wird die Fermatgleichung bzw. die durch sie definierte *Fermathyperfläche* im projektiven Raum oft als Beispiel herangezogen, so etwa bei den bedeutenden *Vermutungen von Hodge und Tate*, und obwohl man — insbesondere dank Tetsuji Shiodas intensiven Bemühungen ([SK79], [Shi79], [Shi82], [Shi83], [Shi87], [Shi88]) — über die Fermathyperflächen wesentlich mehr weiß als über allgemeine Hyperflächen oder gar beliebige Varietäten, sind doch noch immer viele Fragen offen; sowohl die Hodge- als auch die Tate-Vermutung etwa konnte von Shioda zwar für viele, aber eben nicht für alle Fermathyperflächen bewiesen werden.

Sei jetzt speziell $R = k = \mathbb{F}_q$ ein endlicher Körper. Offenbar hat dann jede homogene Gleichung $f(X_1, \ldots, X_n) = 0$ über k nur endlich viele Lösungen $\nu^{(i)}$ in den endlichen Erweiterungen $\mathbb{F}_{q^i}$ von k, und die Zusammenfassung all dieser $\nu^{(i)}$ zur *Zetafunktion*

$$\zeta(f,t) := \exp\left(\sum_{i=1}^{\infty} \frac{\nu^{(i)}}{i} t^i\right) \in \mathbb{Q}(t) \subset \mathbb{Q}((t)),$$

ist eine der grundlegendsten und wichtigsten Invarianten von f bzw. der durch f in $\mathbb{P}_k^{n-1}$ definierten $(n-2)$-dimensionalen projektiven Hyperfläche $X(f)$.

Eine feinere Invariante ist die l-adische Kohomologie $H^*_{\text{ét}}(\bar{X}(f), \mathbb{Q}_l)$ von $\bar{X}(f) := X(f) \times_k \bar{k}$ (für eine Primzahl $l \neq \text{char}\,(k)$) und die Operation der absoluten Galoisgruppe G_k auf ihr, und aus dieser kann man die Zetafunktion leicht berechnen, weil die Zahl $\nu^{(i)}$ gerade die Spur der i-ten Potenz des Frobenius $x \mapsto x^q$ aus G_k ist.

Die Zetafunktion der Fermathyperfläche $X_n^m := X(P_n^m)$ war schon Weil bekannt; er hatte sie in dem oben genannten Artikel berechnet und insbesondere gezeigt, daß sie nicht bloß eine Potenzreihe, sondern sogar eine *rationale* Funktion ist; und es war — wie schon oben bemerkt — unter anderem dieses Beispiel, das ihn zu seiner Vermutung führte, die Zeta-Funktion einer Varietät über k sei stets rational.

Deligne hat dann in [Del82] auch die Galoisoperation auf $H^*_{\text{ét}}(\bar{X}_n^m, \mathbb{Q}_l)$ genau bestimmt, sie ist in diesem Fall besonders einfach, da die Kohomologie in kanonisch definierte „motivische“, vom Grundkörper k unabhängige, eindimensionale Unterräume zerfällt, auf denen der Frobenius durch gewisse Größencharaktere — sogenannte *Jacobisummen* — operiert.

Ausgehend von der Fermathyperfläche ist es ein natürlicher Schritt, etwas allgemeinere Klassen von Hyperflächen zu betrachten, etwa die *diagonalen Hyperflächen*, die durch Gleichungen der Form

$$a_1 X_1^m + \ldots + a_n X_n^m = 0$$

mit Konstanten $a_1, \ldots, a_n$ aus einem Körper k, sogenannten *diagonalen Gleichungen*, gegeben werden; diese werden (im Fall $k = \mathbb{F}_q$ mit $q \equiv 1 \pmod{m}$) ausführlich von Fernando Q. Gouvêa und Noriko Yui in dem Buch [GY95] untersucht; mit Hilfe von Delignes und Weils Resultaten ist es dann nicht schwer, zum Beispiel die Zetafunktion solcher diagonalen Gleichungen zu berechnen.

„Geometrisch“, d.h. über dem separablen algebraischen Abschluß $\bar{k}$, ist jede diagonale Gleichung Q vom Grad m in n Unbestimmten zur Fermatgleichung P_n^m isomorph, d.h. geht durch lineare Variablensubstitution mit Koeffizienten in $\bar{k}$ aus P_n^m hervor: Ein Isomorphismus wird einfach durch $X_i \mapsto \sqrt[m]{a_i} X_i$ gegeben. Die Betrachtung der diagonalen Gleichungen ist also nur interessant, wenn der Grundkörper k nicht algebraisch abgeschlossen ist, wenn also „arithmetische“ Fragen berührt werden. Wie schon der Vergleich der beiden quadratischen diagonalen Gleichungen

$$\begin{array}{ll} P_3^2: & X_1^2 + X_2^2 + X_3^2 = 0 \quad \text{und} \\ Q: & X_1^2 - 2X_2^2 - X_3^2 = 0 \end{array}$$

über $\mathbb{Q}$ zeigt, kann das Lösungsverhalten vollkommen unterschiedlich sein: Während P_3^2 überhaupt keine nicht-triviale Lösung in $\mathbb{Q}$ besitzt, hat Q unendlich viele („Pellsche Gleichung“).

Dennoch ist es möglich, die Tatsache, daß alle diagonalen Gleichungen über $\bar{k}$ isomorph werden, auszunutzen, um aus Kenntnissen über die Fermatgleichung Informationen über die diagonalen Gleichungen zu gewinnen mittels eines sehr allgemeinen Prinzips, das gemeinhin *Galois-Abstieg* bzw. *-Descent* genannt wird:

Ist K/k eine Galoiserweiterung mit Galoisgruppe G und X ein „über k“ definiertes „Objekt“, so definiert jedes ebenfalls über k definiert Objekt Y, das „über K“ isomorph zu X wird (man nennt Y dann eine *K/k-Form* von X), eine Kohomologieklasse in $H^1(G, A(X))$, wobei $A(X)$ die (im allgemeinen nicht abelsche) Automorphismengruppe von X über K ist. Die Idee ist nun, Eigenschaften von Y aus den entsprechenden Eigenschaften von X mittels „Twist“ mit dieser Kohomologieklasse abzuleiten. — Insbesondere kann man dies im Falle einer diagonalen Gleichung tun, die ja eine $\bar{k}/k$-Form der Fermatgleichung ist.

Jetzt liegt die Frage nahe: *Gibt es auch $\bar{k}/k$-Formen der Fermatgleichung, sogenannte „getwistete Fermatgleichungen“, die nicht diagonal sind?* — Man kann dann versuchen, auch für diese mittels Galois-Descent Fragen nach Kohomologie, Zetafunktion usw. zu beantworten.

Im Fall $K = \bar{k}$ ist $A(P_n^m)$ das Kranzprodukt $S_n \int \mu_m$ der symmetrischen Gruppe S_n mit der Gruppe der m-ten Einheitswurzeln μ_m in $\bar{k}$; dabei operiert S_n durch Permutation der X_i und μ_m^n durch $X_i \mapsto \zeta_i X_i$ (für $(\zeta_i)_i \in \mu_m^n$).

Die $\bar{k}/k$-Formen von P_n^m werden dann durch Kohomologieklassen in $H^1(G_k, S_n \int \mu_m)$ gegeben, und es stellt sich heraus, daß die diagonalen Gleichungen genau diejenigen Formen der Fermatgleichung sind, deren zugehörige Kohomologieklasse schon in $H^1(G, \mu_m^n)$ liegt; vom Standpunkt der K/k-Formen aus bilden die diagonalen Gleichungen also nur

ein spezielles Beispiel und stellen eine künstliche Einschränkung der natürlichen Allgemeinheit dar.

Ziel der vorliegenden Arbeit ist es deshalb, *alle* Formen von P_n^m gleichberechtigt zu betrachten, sie zunächst zu klassifizieren, um sie dann mit Hilfe der Descent-Methode zu untersuchen und im Falle $k = \mathbb{F}_q$ schließlich ihre Zetafunktion zu berechnen.

Im Gegensatz zum Fall der diagonalen Gleichungen sieht man den Gleichungen einer allgemeinen Form von P_n^m ihre Verwandtschaft zur Fermatgleichung nur selten an — so ist etwa die durch

$$4X_1^2X_2 + 3X_1X_2^2 + 3X_1^2X_3 + 4X_2^2X_4 + 4X_1X_3X_4 + X_1X_4^2 \\ + 4X_2X_3^2 + X_2X_3X_4 + X_3X_4^2 + 2X_3^3 + X_3^2X_4 + 2X_3X_4^2 + 3X_4^3 = 0$$

definierte Gleichung eine Form der Fermatgleichung P_4^3 über dem Körper $\mathbb{F}_5$, die nicht diagonal ist. Und auch für diese wie auch für alle anderen, beliebig kompliziert anmutenden, Formen erhalten wir mit Hilfe der Descent-Methode Resultate wie die Berechnung der Automorphismengruppe oder die Berechnung der Zeta-Funktion.

Andererseits ist es natürlich auch ein kleiner Nachteil, daß die allgemeinen Formen keine augenscheinliche Symmetrie mehr besitzen, denn diese Tatsache erschwert es oft, von einer gegebenen Gleichung zu entscheiden, ob sie denn nun eine Form der Fermatgleichung ist oder nicht.

Eine besonders interessante Ausnahme bildet hier der Fall $m = 3$, $n = 2$, d.h. der Fall der *binären kubischen Formen*, weil dort *alle* homogenen Polynome in zwei Unbestimmten vom Grad drei, die „nicht-ausgeartet“ sind, Formen von P_2^3 sind. Wir können die nicht-ausgearteten binären kubischen Formen über einem beliebigem Körper K mit unserer Methode nicht nur klassifizieren, sondern diese Klassifikation sogar vollständig explizit machen, so daß es tatsächlich möglich wird, zu jeder gegebenen (nicht-ausgearteten) kubischen Form die Klasse anzugeben und im Falle $k = \mathbb{F}_q$ die Zetafunktion zu berechnen.

Obwohl die Descent-Methode „Folklore“ ist, steckt auch hier der Teufel wie so oft im Detail. Deshalb widmet sich das *erste Kapitel* einer Axiomatisierung der Situation, in der wir Galois-Descent anwenden können:

> **Definition:** Eine *Koeffizientenerweiterung* (zu einer gegebenen Galoiserweiterung K/k mit Galoisgruppe G) besteht aus zwei Kategorien $\mathcal{C}_k$ und $\mathcal{C}_K$, einem kovarianten Funktor $F : \mathcal{C}_k \to \mathcal{C}_K$ und einer Links-G-Operation auf allen Isomorphismenmengen $\mathrm{Iso}_{\mathcal{C}_K}(FY, FZ)$ für Objekte Y und Z aus $\mathcal{C}_k$, so daß die folgenden beiden Bedingungen erfüllt sind:
>
> - Die Operation ist verträglich mit Kompositionen, d.h. für Objekte X ,Y und Z aus $\mathcal{C}_k$, Isomorphismen $X \xrightarrow{g} Y$ und $Y \xrightarrow{f} Z$ und ein Element $s \in G$ gilt:
> $$^s(fg) = {}^sf\,{}^sg.$$
> - Genau die Morphismen, die „von unten“ kommen, sind fix unter der G-Operation, d.h. für Objekte $Y, Z \in \mathrm{Ob}(\mathcal{C}_k)$ gilt:
> $$\mathrm{Im}\left(\mathrm{Iso}_{\mathcal{C}_k}(Y,Z) \xrightarrow{F} \mathrm{Iso}_{\mathcal{C}_K}(FY,FZ)\right) \;=\; \left[\mathrm{Iso}_{\mathcal{C}_K}(FY,FZ)\right]^G.$$

Zwei Beispiele für Koeffizientenerweiterungen sind besonders wichtig für unsere Untersuchung der K/k-Formen von Fermatgleichungen: Zum einen betrachten wir die Kategorien $\mathcal{F}_k^{n,m}$ bzw. $\mathcal{F}_K^{n,m}$, deren Objekte homogene Gleichungen vom Grad m in n Unbestimmten mit Koeffizienten in k bzw. K und deren Morphismen Elemente aus $\mathrm{GL}\,(n,k)$ bzw. $\mathrm{GL}\,(n,K)$ sind, aufgefaßt als lineare Variablensubstitutionen. Die Koeffizientenerweiterung wird dann durch den offensichtlichen Funktor $\mathcal{F}_k^{n,m} \to \mathcal{F}_K^{n,m}$ und die natürliche G-Operation auf $\mathrm{GL}\,(n,K)$ gegeben.

Die Bedeutung dieser Koeffizientenerweiterung für uns ist offensichtlich: Die Fermatgleichung P_n^m ist ein Objekt von $\mathcal{F}_k^{n,m}$, und die uns interessierenden K/k-Formen von P_n^m sind genau die Objekte aus $\mathcal{F}_k^{n,m}$, die in $\mathcal{F}_K^{n,m}$ isomorph zu P_n^m werden.

Das zweite wichtige Beispiel sind die Kategorien $\mathbf{Rep}_{\mathbb{Q}_l}^{G_k}$ und $\mathbf{Rep}_{\mathbb{Q}_l}^{G_K}$ der $\mathbb{Q}_l$-G_k-Darstellungen bzw. $\mathbb{Q}_l$-G_K-Darstellungen mit dem Funktor $\mathbf{Rep}_{\mathbb{Q}_l}^{G_k} \to \mathbf{Rep}_{\mathbb{Q}_l}^{G_K}$, der einer Darstellung $G_k \xrightarrow{\varphi} \mathrm{Aut}_{\mathbb{Q}_l}(V)$ die Einschränkung $\varphi|G_K$ zuordnet. Hier wird die $G = G_k/G_K$-Operation eines $\bar{s} \in G$ auf $(V,\varphi) \xrightarrow{f} (W,\psi)$ durch „Konjugation“, d.h. durch $f \mapsto \psi(s) f \varphi(s)^{-1}$ gegeben.

Diese Koeffizientenerweiterung ist wichtig für uns, weil die l-adische Kohomologie $H^*_{\text{ét}}(\bar{X}_n^m, \mathbb{Q}_l)$ ein Objekt von $\mathbf{Rep}_{\mathbb{Q}_l}^{G_k}$ ist und weil die Kohomologie einer Form der Fermathyperfläche eine Form von $H^*_{\text{ét}}(\bar{X}_n^m, \mathbb{Q}_l)$ ist.

Obwohl die beiden genannten in Hinblick auf unsere Ziele die wichtigsten Beispiele sind, treten Koeffizientenerweiterungen noch an vielen anderen Stellen auf, und wir führen einige weitere interessanten Beispiele an, so etwa den natürlichen Funktor aus der Kategorie der geometrisch irreduziblen Varietäten über k mit dominanten rationalen Abbildungen als Morphismen in die Kategorie der geometrisch irreduziblen Varietäten über K oder — im Falle $k = \mathbb{Q}$ — den natürlichen Funktor aus der Kategorie der Motive über einem Körper in die Kategorie der Motive mit Koeffizienten in K über demselben Körper.

Wir haben oben schon erwähnt, daß wir für den Galois-Descent die Kohomologie $H^1(G,A)$ für im allgemeinen nicht-abelsche Gruppen A benötigen werden, weil die Automorphismengruppen der Objekte, die uns interessieren, oft nicht abelsch sein werden — das Kranzprodukt $A(P_n^m) = S_n \int \mu_m$ zum Beispiel ist für $n \geq 2$ nicht kommutativ. Deshalb wollen wir im *zweiten Kapitel* die grundlegenden Definitionen und Resultate der nicht-abelschen Gruppenkohomologie vorstellen, wobei wir im Wesentlichen Serres Ausführungen in [Ser97] folgen. Allerdings betrachten wir einen leicht allgemeineren Fall, nämlich beliebige topologische Gruppen G und nicht bloß proendliche, was den Vorteil hat, daß wir unsere Galoisgruppe G sowohl als diskrete als auch als proendliche Gruppe betrachten können.

Im *dritten Kapitel* werden wir dann das Prinzip des Galois-Descents im Falle einer beliebigen Koeffizientenerweiterung $F : \mathcal{C}_k \to \mathcal{C}_K$ entwickeln. Ist X ein Objekt aus $\mathcal{C}_k$, so bezeichnet $E(K/k,X)$ die Menge[†] der *K/k-Formen von X*, d.h. der Isomorphieklassen $[Y]$ von Objekten aus $\mathcal{C}_k$, die in $\mathcal{C}_K$ isomorph zu X werden (d.h. für die FY und FX in $\mathcal{C}_K$ isomorph sind). Ist Y eine solche K/k-Form von X, und ist $FY \xrightarrow{f} FX$ ein Isomorphismus in $\mathcal{C}_K$, so definiert $s \mapsto f^s(f^{-1})$ einen 1-Kozykel $a = (a_s)$ von $G := \mathrm{Gal}\,(K/k)$ in $A(X) := \mathrm{Aut}_{\mathcal{C}_K}(FX)$ und damit eine Kohomologieklasse $\vartheta[Y]$ in $H^1(G, A(X))$.

[†]A priori ist dies nur eine Klasse, aber wir werden beweisen, daß es sich tatsächlich um eine Menge handelt.

Satz: *Die Zuordnung* $[Y] \mapsto \vartheta[Y]$ *definiert eine wohldefinierte Injektion von* $E(K/k, X)$ *in* $H^1(G, A(X))$.

Als erste Anwendung werden wir die Automorphismengruppe von Y (in $\mathcal{C}_k$!) berechnen: Es ist $\boxed{\mathrm{Aut}_{\mathcal{C}_k}(Y) = (A(X)_a)^G}$, wobei $A(X)_a$ die Gruppe $A(X)$ mit *um den 1-Kozykel* a *getwisteter* G*-Operation* ist, d.h. $s \in G$ operiert als $b \mapsto a_s {}^s b a_s^{-1}$.

Ist ${\mathcal{C}_k}' \to {\mathcal{C}_K}'$ eine zweite Koeffizientenerweiterung, und sind $\mathcal{C}_k \xrightarrow{H_k} {\mathcal{C}_k}'$ und $\mathcal{C}_K \xrightarrow{H_K} {\mathcal{C}_K}'$ Funktoren, die miteinander und mit den G-Operationen kompatibel sind (wir werden dies im dritten Kapitel natürlich präzisieren), so sprechen wir von einem *Morphismus von Koeffizientenerweiterungen*, und wir erhalten ein kommutatives Diagramm

$$\begin{array}{ccc} E(K/k, X) & \xrightarrow[[Y] \mapsto [H_k Y]]{} & E(K/k, H_k X) \\ \big\downarrow \vartheta & = & \big\downarrow \vartheta \\ H^1(G, A(X)) & \xrightarrow[(a_s) \mapsto (H_K a_s)]{} & H^1(G, A(H_k X)) \end{array}$$

Dieses Ergebnis ist für unsere Zwecke sehr wichtig, denn wenn wir für die beiden Koeffizientenerweiterungen die beiden Hauptbeispiele aus dem ersten Kapitel und für H_k bzw. H_K den Funktor der étalen Kohomologie einsetzen, dann besagt die Kommutativität des Diagramms:

Ist Q *eine* K/k*-Form der Fermatgleichung* P_n^m*, charakterisiert durch die Kohomologieklasse* $\vartheta[Q]$*, so wird die Kohomologie der Hyperfläche* $X(Q)$ *und damit auch die Zetafunktion von* Q *durch die Kohomologieklasse* $H_{\acute{e}t}\,\vartheta[Q]$ *charakterisiert.*

Anstatt die Kohomologie von $X(Q)$ zur Berechnung der Zetafunktion von Q direkt bestimmen zu müssen, können wir also stattdessen die Komposition $\vartheta^{-1} \circ H_{\text{ét}} \circ \vartheta$ berechnen und müssen dazu folgendes tun:

- die Galoisoperation auf der étalen Kohomologie der Fermathyperfläche X verstehen — dies leistet gerade das oben beschriebene Ergebnis von Deligne,
- für einen Automorphismus $a \in A(P_n^m)$ den zugehörigen Automorphismus $H_{\text{ét}}(a)$ der Kohomologie $H^*_{\text{ét}}(\bar{X}, \mathbb{Q}_l)$ berechnen und
- das Urbild einer gegebenen Kohomologieklasse unter der Injektion ϑ berechnen.

Aus der Tatsache, daß das Kranzprodukt $S_n \int \mu_m$ auf X_n^m operiert, kann man auf die Zerlegung der étalen Kohomologie von X_n^m in Eigenräume schließen, die zu den Charakteren der abelschen Gruppe μ_m^n korrespondieren.

Im *vierten Kapitel* werden wir allgemeiner die Situation untersuchen, daß ein semidirektes Produkt $A \rtimes S$ zweier endlicher Gruppen auf einem Objekt M einer pseudoabelschen Kategorie operiert. Auch dann hat man eine Zerlegung von M in die direkte Summe von Eigenräumen M_χ zu den Charakteren χ von A, und bezeichnet p_χ den Projektor, der M_χ

aus M „herausschneidet“, so kommutiert für $s \in S$ das Diagramm

$$\begin{array}{ccc} M_{s_\chi} & \xrightarrow{p_\chi \cdot s \cdot p_{s_\chi}} & M_\chi \\ \downarrow & = & \downarrow \\ M & \xrightarrow[s]{} & M \end{array}$$

So sehen wir, daß die Zerlegung von $H^*_{\text{ét}}(\bar{X}^m_n, \mathbb{Q}_l)$ in Eigenräume eine „motivische“ Zerlegung ist, d.h. sie ist die l-adische Realisierung der entsprechenden Zerlegung des Grothendieck-Motivs $h(X^m_n)$ von X^m_n.

Das *fünfte Kapitel* widmet sich dem Studium der Kohomologie $H^1(G, S_n \int \mu_m)$, d.h. der Klassifikation der $\bar{k}/k$-Formen von P^m_n in $\mathcal{F}^{n,m}_k$. Dabei rekapitulieren wir im Wesentlichen nur die Ergebnisse aus der Diplomarbeit [Rup96] von Christopher Rupprecht, machen allerdings die auftretenden Abbildungen expliziter, weil wir zur Berechnung der Zetafunktion explizite Formeln benötigen. — Außerdem berechnen wir zusätzlich die Automorphismengruppen der getwisteten Fermatformen. Die Hauptergebnisse dieses Kapitels sind:

Ist $m \geq 3$, so haben wir eine Bijektion

$$\boxed{E(\bar{k}/k, P^m_n) \cong \coprod_L \mathrm{Aut}_k(L) \backslash (L^\times / L^{\times m})}$$

wobei die disjunkte Vereinigung über Isomorphieklassen separabler k-Algebren L vom Grad n über k läuft. Bezeichnet Q die Gleichung, die unter dieser Bijektion zu einem Paar (L, x) korrespondiert, so haben wir die folgende kanonische exakte Sequenz:

$$\boxed{1 \to \prod_{i=1}^{r} (L_i \cap \mu_m) \to \mathrm{Aut}_k(Q) \to \left\{ a \in \mathrm{Aut}_k(L)^{\mathrm{opp}} \,\middle|\, \tfrac{ax}{x} \in L^{\times m} \right\} \to 1}$$

Im *sechsten Kapitel* betrachten wir speziell den Fall der binären kubischen Formen über einem Körper k mit $\mathrm{char}\,(k) \geq 5$, in dem — wie oben schon gesagt — *alle* nicht-ausgearteten Objekte, d.h. solche mit nicht-verschwindender Diskriminante, Formen der Fermatgleichung P^3_2 sind. Als Anwendung des fünften Kapitels listen wir zunächst die $\bar{k}/k$-Formen von P^3_2 für den Fall, daß k ein *endlicher* Körper ist, vollständig auf. Dann zeigen wir, daß die Klassifikation aus dem fünften Kapitel in diesem Fall besonders explizit gemacht werden kann: Zu einer gegebenen Gleichung kann das Paar (L, x) aus obiger Bijektion mit der folgenden Formel berechnet werden:

Theorem: *Es sei $Q(X,Y) = aX^3 + bX^2Y + cXY^2 + dY^3$ eine nicht-ausgeartete Form über k mit $a \neq 0$. Setze*

$$\boxed{\begin{array}{lcll} \delta & := & -\dfrac{\Delta(Q)}{27} & \in k^\times, \\ e & := & \dfrac{a}{2} - \dfrac{27a^2d + 2b^3 - 9abc}{2\Delta(Q)}\sqrt{\delta} & \in k(\sqrt{\delta})^\times, \end{array}}$$

wobei

$$\Delta(Q) := -27a^2d^2 + 18abcd + b^2c^2 - 4b^3d - 4ac^3$$

die Diskriminante von Q *ist und die Wurzel von* δ *so zu wählen ist, daß* $e \neq 0$ *ist.*

Dann gehört Q *zu dem Paar:*

$$\boxed{\begin{cases} \left(k \times k, \left(e, \dfrac{\sqrt{\delta}}{e}\right)\right) & \text{falls } \delta \in k^{\times 2}, \\ \left(k(\sqrt{\delta}), e\right) & \text{sonst.} \end{cases}}$$

Die reellen Polynome $x^4+y^4+z^4$ und $-x^4-y^4-z^4$ sind im Sinne des fünften Kapitels nicht isomorph, d.h. sie lassen sich nicht durch eine lineare Koordinatentransformation ineinander überführen. Wenn wir die Polynome als Gleichungen interpretieren, erscheint dies aber unnatürlich, denn selbstverständlich haben beide Gleichungen dieselbe Lösungsmenge und „sollten“ also isomorph sein. Dieser Intuition wird mit dem Übergang zu einer anderen Kategorie Rechnung getragen, in der Polynome, die sich nur um skalare Vielfache unterscheiden, isomorph sind. Morphismen sind dann keine Elemente aus $\mathrm{GL}(n,k)$ mehr, sondern Elemente aus $\mathrm{PGL}(n,k)$. Es ist naheliegend, daß es in dieser Kategorie „weniger“ Formen der Fermatgleichung geben wird, und wir werden im *siebten Kapitel* zeigen, wie man dieses „weniger“ präzisieren kann:

Satz: *Zwei Paare* (L,x) *und* (L,x') *geben in der neuen Kategorie genau dann dasselbe Objekt, wenn es ein* $a \in Aut_k(L)$*, ein* $\lambda \in k^\times$ *und ein* $y \in L^\times$ *gibt, so daß* $\boxed{x' = a[\lambda x y^m]}$ *gilt.*

Wenn K ein Zahlkörper oder allgemeiner der Quotientenkörper eines Dedekindringes $\mathcal{O}_K$ und $\mathfrak{p}$ ein Primideal von $\mathcal{O}_K$ ist, so haben wir eine intuitive Vorstellung davon, was die Reduktion eines homogenen Polynoms P modulo $\mathfrak{p}$ sein sollte: Wir erweitern die Koeffizienten derart, daß alle in $\mathcal{O}_K$ liegen, und reduzieren sie dann modulo $\mathfrak{p}$. — Dabei sollte es so sein, daß die Reduktion einer L/K-Form Q von P eine Form der Reduktion von P ist.

Es wird sich herausstellen, daß diese intuitive Vorstellung nur beinahe richtig ist und daß man sich auf sogenannte „$\mathfrak{p}$-reduzible Formen“ Q von P beschränken muß, wenn man einen vernünftigen Begriff von Reduktion modulo $\mathfrak{p}$ erhalten will, der auch die Eigenschaft, Form zu sein, respektiert. Dabei sind die $\mathfrak{p}$-reduziblen Formen solche, die nicht bloß durch eine lineare Variablentsubstitution aus $\mathrm{PGL}(n,L)$ in P übergehen, sondern sogar durch eine Substitution aus $\mathrm{PGL}(n,\mathcal{O}_{L,\mathfrak{P}})$ für ein über $\mathfrak{p}$ liegendes Primideal $\mathfrak{P}$ von L.

Hat man die Reduktion einmal definiert, so stellt sich natürlich die Frage, wie sie sich in Termen unserer kohomologischen Beschreibung von Formen ausdrücken läßt, d.h. welchen 1-Kozykel man einem 1-Kozykel von $\mathrm{Gal}(L/K)$ mit Werten in $\mathrm{Aut}_L(P)$ zuordnen muß, um den die Reduktion repräsentierenden 1-Kozykel zu erhalten.

Im *achten Kapitel* werden wir die Reduktion modulo $\mathfrak{p}$ sowohl für Formen als auch für 1-Kozykel definieren und insbesondere zeigen, daß diese beiden Reduktionen miteinander verträglich sind. Wir werden dann speziell den Fall der Fermatgleichung P_n^m betrachten und untersuchen, wie sich die Reduktion in Termen der Charakterisierung von 1-Kozykeln durch Paare (L,x) ausdrücken läßt.

Das *neunte Kapitel* ist das technische Herzstück unserer Arbeit, denn dort wird berechnet, welchen Isomorphismus auf der mittleren Kohomologie ein Isomorphismus τ von X_n^m, d.h. ein Element des Kranzproduktes $S_n \int \mu_m$, induziert. Schon aus dem vierten Kapitel ist das Ergebnis für Elemente $\tau \in \mu_m^n$ bekannt, so daß sich die Frage auf Permutationen $\tau \in S_n$ und dann weiter auf den Fall der Transposition $\tau = (12)$ reduzieren läßt.

Als Ergebnis können wir die Existenz einer Basis $\{v_a\}_a$ von V_{prim}, dem primitiven Teil der Kohomologie von X_n^m, beweisen, auf der die Operation von $S_n \int \mu_m$ explizit bekannt ist.

In den Arbeiten von Shioda, Gouvêa und Yui wird stets vorausgesetzt, daß der Grundkörper k die m-ten Einheitswurzeln enthält, und in diesem Fall ist auch die Matrix der Galoisoperation bezüglich der Basis $\{v_a\}_a$ wohlbekannt, so daß unsere Ergebnisse aus dem dritten Kapitel es uns dann tatsächlich gestatten, die Galoisoperation auf der Kohomologie einer jeden getwisteten Fermathyperfläche über k genau zu beschreiben. Darüber hinaus gelingt es uns, für beliebige Grundkörper zumindest Teilaussagen zu machen, die uns oft erlauben werden, auch dort wenigstens die Zetafunktion einer gegebenen getwisteten Fermatgleichung zu berechnen.

Im *zehnten Kapitel* wird zum ersten Mal explizit von der Zetafunktion die Rede sein — wir werden sie definieren und erklären, wie man sie mit Hilfe der Ergebnisse aus den vorangegangenen Kapiteln für getwistete Fermatgleichungen berechnen kann.

Das *elfte Kapitel* schließlich untersucht das Problem, wie zu verfahren sei, wenn die m-ten Einheitswurzeln *nicht* in k enthalten sind, exemplarisch am Fall von Kubiken in zwei und vier Variablen (der Fall von drei Variablen ist leichter, vgl. 9.19!).

Das kostet zwar einige Mühen, aber am Ende kann auch in diesen Fällen die Matrix der Galoisoperation bezüglich der Basis $\{v_a\}_a$ genau angegeben werden; insbesondere kann man also jetzt die Zetafunktionen von Spezialisierungen von Kubiken über $\mathbb{Q}$ für $n \in \{2, 4\}$ berechnen, und wir geben eine vollständige Liste der Zetafunktionen an, die bei binären Kubiken über beliebigen endlichen Körpern auftreten können.

Im Zusammenspiel mit unseren Ergebnissen aus Kapitel sechs erlaubt uns dies, zu jeder nicht-ausgearteten binären kubischen Form über einem endlichen Körper die Zetafunktion zu berechnen.

Ganz herzlich bedanken möchte ich mich bei meinem Doktorvater Prof. Dr. Uwe Jannsen, der stets ein reges Interesse an meinen Fortschritten gezeigt hat und den ich immer um Rat fragen konnte, bei meiner besten Freundin und Kollegin Kirsten Schneider, die mir viele Stunden ihrer Zeit geopfert, geduldig meinen Problemen gelauscht und mir so manchen wertvollen Tip gegeben hat, ferner bei meinem Kollegen Christopher Rupprecht, dem ich viele Erkenntnisse über die Klassifikation von Fermatgleichungen verdanke, und dann natürlich bei meiner Frau June Roberts — für ihr Vertrauen und ihre Geduld in den letzten Jahren.

Inhaltsverzeichnis

1 Koeffizientenerweiterungen

In diesem Kapitel werden wir zunächst den Begriff der *Koeffizientenerweiterung* definieren, der die Situation axiomatisiert, in der Galois-Abstieg angewandt werden kann. Dann werden wir im Rest des Kapitels Beispiele für Koeffizientenerweiterungen betrachten; nicht nur, weil wir manche von ihnen später zur Berechnung der Zetafunktionen von Formen von Fermatgleichungen brauchen werden, sondern auch, weil sie für sich genommen interessant sind und weil sie demonstrieren, in welch vielfältigen Situationen die Descent-Methode nützlich sein kann.

Es sei K/k eine beliebige galoissche Körpererweiterung mit Galoisgruppe $G := \mathrm{Gal}\,(K/k)$.

1.1 Definition. Eine *Koeffizientenerweiterung* (von k nach K) besteht aus zwei Kategorien $\mathcal{C}_k$ und $\mathcal{C}_K$, einem kovarianten Funktor $F : \mathcal{C}_k \to \mathcal{C}_K$ und einer Links-G-Operation auf $\mathrm{Iso}_{\mathcal{C}_K}(FY, FZ)$ für alle $Y, Z \in \mathrm{Ob}(\mathcal{C}_k)$, so daß die folgenden beiden Bedingungen erfüllt sind:

(KE1) Die Operation ist verträglich mit Kompositionen, d.h. für Objekte $X, Y, Z \in \mathrm{Ob}(\mathcal{C}_k)$, Isomorphismen $X \xrightarrow{g} Y$ und $Y \xrightarrow{f} Z$ und ein Element $s \in G$ gilt:

$$^s(fg) = {}^sf\,{}^sg.$$

(KE2) Genau die Morphismen, die „von unten“ kommen, sind fix unter der G-Operation, d.h. für Objekte $Y, Z \in \mathrm{Ob}(\mathcal{C}_k)$ gilt:

$$\mathrm{Im}\left(\mathrm{Iso}_{\mathcal{C}_k}(Y,Z) \xrightarrow{F} \mathrm{Iso}_{\mathcal{C}_K}(FY,FZ)\right) \;=\; \left[\mathrm{Iso}_{\mathcal{C}_K}(FY,FZ)\right]^G.$$

1.2 Lemma. Es seien $\mathcal{C}_k$ und $\mathcal{C}_K$ Kategorien, $F : \mathcal{C}_k \longrightarrow \mathcal{C}_K$ ein kovarianter Funktor, und für alle Objekte X und Y aus $\mathcal{C}_k$ operiere G derart auf $\mathrm{Mor}_K(FX, FY)$, daß die folgenden beiden Bedingungen erfüllt sind:

(KE1') Die Operation ist verträglich mit Kompositionen, d.h. für Objekte $X, Y, Z \in \mathrm{Ob}(\mathcal{C}_k)$, Morphismen $X \xrightarrow{g} Y$ und $Y \xrightarrow{f} Z$ und ein Element $s \in G$ gilt:

$$^s(fg) = {}^sf\,{}^sg.$$

(KE2') Genau die Morphismen, die „von unten“ kommen sind fix unter der G-Operation, d.h. für Objekte $Y, Z \in \mathrm{Ob}(\mathcal{C}_k)$ gilt:

$$\mathrm{Im}\left(\mathrm{Mor}_k(Y,Z) \xrightarrow{F} \mathrm{Mor}_K(FY,FZ)\right) \;=\; \mathrm{Mor}_K(FY,FZ)^G.$$

Dann wird F durch Einschränkung der G-Operation auf Isomorphismen zu einer Koeffizientenerweiterung.

Beweis: Man muß sich nur überlegen, daß die gegebene G-Operation Isomorphismen wieder in Isomorphismen überführt: Ist $f : FX \xrightarrow{\sim} FY$ ein Isomorphismus mit Inversem $g : FY \xrightarrow{\sim} FX$, und ist $s \in G$ beliebig, so folgt aus (KE1') zunächst ${}^sf \circ {}^sg = {}^s(f \circ g) = {}^s1_Y$, und weil die Identität „von unten" kommt, ist dies nach (KE2') gleich der Identität, d.h. auch ${}^sf$ ist ein Isomorphismus mit Inversem ${}^sg$. **q.e.d.**

1.3 Satz. Es sei $\mathcal{C}_k$ eine beliebige Kategorie, $\mathfrak{K}$ ein Objekt aus $\mathcal{C}_k$, auf dem G von links operiert, und für alle Objekte X aus $\mathcal{C}_k$ möge das Produkt $X \times \mathfrak{K}$ existieren. Sei dann $\mathcal{C}_K$ die Kategorie $\mathcal{C}_k/\mathfrak{K}$ der Objekte über $\mathcal{K}$ und $\mathcal{C}_k \xrightarrow{F} \mathcal{C}_K$ der Funktor $X \mapsto (X \times \mathfrak{K} \xrightarrow{\mathrm{pr}_2} \mathfrak{K})$.

(i) Für $s \in G$ und einen Morphismus $Y \xrightarrow{f} Z$ aus $\mathcal{C}_k$ wird durch

$$\begin{array}{ccc} Y \times \mathfrak{K} & \xrightarrow{\quad f \quad} & Z \times \mathfrak{K} \\ {\scriptstyle 1_Y \times s}\downarrow & = & \downarrow{\scriptstyle 1_Z \times s} \\ Y \times \mathfrak{K} & \xrightarrow[{}^sf]{} & Z \times \mathfrak{K} \end{array}$$

eine Links-Operation von G auf $\mathrm{Mor}_{\mathcal{C}_K}(FY, FZ)$ definiert, die (KE1') erfüllt und für die

$$\mathrm{Im}\left(\mathrm{Mor}_{\mathcal{C}_k}(Y,Z) \xrightarrow{F} \mathrm{Iso}_{\mathcal{C}_K}(FY,FZ)\right) \subseteq \left[\mathrm{Iso}_{\mathcal{C}_K}(FY,FZ)\right]^G.$$

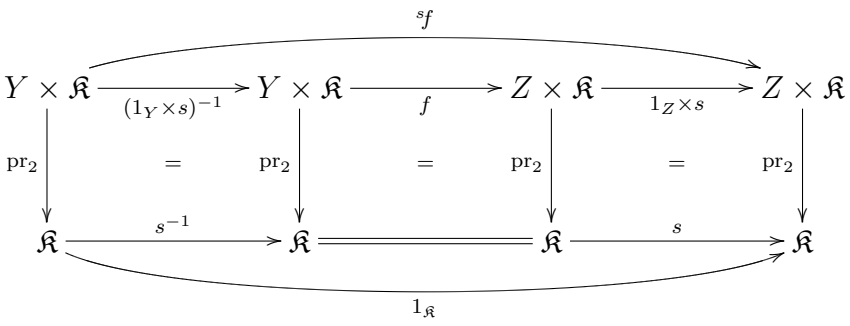
gilt.

(ii) Gelte spezieller, daß G *endlich* ist, daß $\mathcal{C}_k$ ein Endobjekt $\mathfrak{k}$ besitzt, daß in $\mathcal{C}_k$ Faserprodukte existieren, daß der kanonische Morphismus $\mathfrak{K} \to \mathfrak{k}$ ein *universeller effektiver Epimorphismus in* $\mathcal{C}_k$[†] ist, daß die Summe $\coprod_{s\in G} \mathfrak{K}$ in $\mathcal{C}_k$ existiert und daß der kanonische Morphismus $\coprod_{s\in G} \mathfrak{K} \xrightarrow{\amalg_{s\in G}(1_{\mathfrak{K}}, s)} \mathfrak{K} \times \mathfrak{K}$ ein Isomorphismus ist.

Dann erfüllt $\mathcal{C}_k \xrightarrow{F} \mathcal{C}_K$, zusammen mit der in (i) definierten Operation, auch das Axiom (KE2'), ist also eine Koeffizientenerweiterung.

Beweis:

(i) • *Wohldefiniertheit:* Seien $s \in G$ und ein Morphismus $X \times \mathfrak{K} \xrightarrow{f} Y \times \mathfrak{K}$ über $\mathfrak{K}$ vorgegeben. Es ist zu zeigen, daß ${}^sf$ ein Morphismus über $\mathfrak{K}$ ist, was aber sofort aus der Kommutativität des folgenden Diagramms von Morphismen in $\mathcal{C}_k$ folgt:



[†]Ein *effektiver Epimorphismus* in einer Kategorie mit Faserprodukten ist ein Morphismus $X \to Y$, für den die Sequenz $X \times_Y X \rightrightarrows X \to Y$ exakt ist. Ein Morphismus $X \to Y$ ist ein *universeller* effektiver Epimorphismus, wenn für jeden Morphismus $Y' \to Y$ auch $X \times_Y Y' \to Y'$ ein effektiver Epimorphismus ist.

- *Linksoperation:* Seien $s,t \in G$ und $Y \times \mathfrak{K} \xrightarrow{f} Z \times \mathfrak{K}$ über $\mathfrak{K}$ vorgegeben. Dann folgt:

$$\begin{aligned}
{}^{1}f &= (1_Z \times 1_{\mathfrak{K}}) \circ f \circ (1_Y \times 1_{\mathfrak{K}})^{-1} \\
&= 1_Z \circ f \circ 1_Y^{-1} \\
&= f,
\end{aligned}$$

$$\begin{aligned}
{}^{st}f &= (1_Z \times st) \circ f \circ (1_Y \times st)^{-1} \\
&= \Big((1_Z \times s) \circ (1_Z \times t)\Big) \circ f \circ \Big((1_Y \times s) \circ (1_Y \times t)\Big)^{-1} \\
&= (1_Z \times s) \circ \Big((1_Z \times t) \circ f \circ (1_Y \times t)^{-1}\Big) \circ (1_Y \times s)^{-1} \\
&= (1_Z \times s) \circ {}^{t}f \circ (1_Y \times s)^{-1} \\
&= {}^{s}\big({}^{t}f\big).
\end{aligned}$$

- *(KE1'):* Seien $s \in G$ und Morphismen $X \times \mathfrak{K} \xrightarrow{g} Y \times \mathfrak{K} \xrightarrow{f} Z \times \mathfrak{K}$ über $\mathfrak{K}$ vorgegeben, dann folgt:

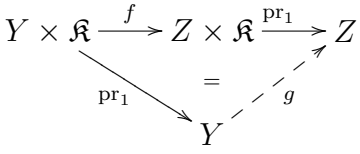
$$\begin{aligned}
{}^{s}(fg) &= (1_Z \times s) \circ (fg) \circ (1_X \times s)^{-1} \\
&= (1_Z \times s) \circ f \circ (1_Y \times s)^{-1} \\
&\qquad \circ (1_Y \times s) \circ g \circ (1_X \times s)^{-1} \\
&= {}^{s}f \circ {}^{s}g.
\end{aligned}$$

- „$\subseteq$“: Seien $Y \xrightarrow{f} Z$ ein beliebiger Morphismus in $\mathcal{C}_k$ und $s \in G$ beliebig. Dann gilt

$${}^{s}(Ff) = {}^{s}(f \times 1_{\mathfrak{K}}) = (1_Z \times s) \circ (f \times 1_{\mathfrak{K}}) \circ (1_Y \times s)^{-1} = f \times 1_{\mathfrak{K}} = Ff,$$

  d.h. F operiert trivial auf Morphismen, die „von unten“ kommen.

(ii) Seien also Y und Z Objekte aus $\mathcal{C}_k$, und sei $X \times \mathfrak{K} \xrightarrow{f} Y \times \mathfrak{K}$ ein Morphismus über $\mathfrak{K}$, der fix unter der G-Operation ist. Wir müssen zeigen, daß $\mathrm{pr}_1 f$ über ein $Y \xrightarrow{g} Z$ faktorisiert, denn dies bedeutet ja gerade $f = Fg = g \times 1_{\mathfrak{K}}$:



Anders formuliert, müssen wir beweisen, daß $\mathrm{pr}_1 f$ im Bild von

$$\mathrm{Mor}_{\mathcal{C}_k}(Y,Z) \xrightarrow{\mathrm{pr}_1^*} \mathrm{Mor}_{\mathcal{C}_k}(Y \times \mathfrak{K}, Z), \quad g \mapsto g\mathrm{pr}_1$$

liegt. Nun ist aber nach Voraussetzung $Y \times \mathfrak{K} \xrightarrow{\mathrm{pr}_1^*} Y$ ein effektiver Epimorphismus, d.h. insbesondere die folgende Sequenz von Mengen ist exakt:

$$\mathrm{Mor}_{\mathcal{C}_k}(Y,Z) \xrightarrow{\mathrm{pr}_1^*} \mathrm{Mor}_{\mathcal{C}_k}(Y \times \mathfrak{K}, Z) \underset{\mathrm{pr}_2^*}{\overset{\mathrm{pr}_1^*}{\rightrightarrows}} \mathrm{Mor}_{\mathcal{C}_k}\big((Y \times \mathfrak{K}) \times_Y (Y \times \mathfrak{K}), Z\big)$$

Nun gilt

$$(Y \times \mathfrak{K}) \times_Y (Y \times \mathfrak{K}) \cong Y \times (\mathfrak{K} \times \mathfrak{K}) \overset{\text{Vor.}}{\cong} Y \times \coprod_{s \in G} \mathfrak{K} \overset{\#G<\infty}{\cong} \coprod_{s \in G} (Y \times \mathfrak{K}),$$

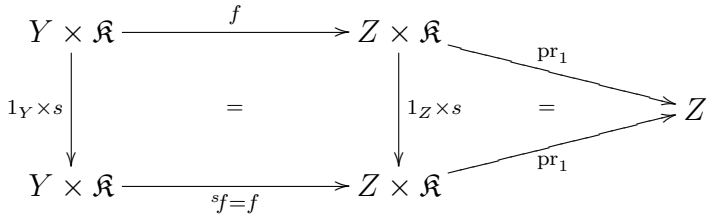
also

$$\mathrm{Mor}_{\mathcal{C}_k}\big((Y \times \mathfrak{K}) \times_Y (Y \times \mathfrak{K}), Z\big) \cong \prod_{s \in G} \mathrm{Mor}_{\mathcal{C}_k}(Y \times \mathfrak{K}, Z),$$

und wir erhalten die exakte Sequenz

$$\mathrm{Mor}_{\mathcal{C}_k}(Y, Z) \xrightarrow{\mathrm{pr}_1^*} \mathrm{Mor}_{\mathcal{C}_k}(Y \times \mathfrak{K}, Z) \underset{\prod_{s \in G}(1_Y \times s)^*}{\overset{\mathrm{diag}}{\rightrightarrows}} \prod_{s \in G} \mathrm{Mor}_{\mathcal{C}_k}(Y \times \mathfrak{K}, Z). \quad (1)$$

Sei nun $s \in G$ beliebig; nach Voraussetzung gilt ${}^s f = f$, d.h. wir haben das folgende kommutative Diagramm:



Es folgt:

$$(1_Y \times s)^*(\mathrm{pr}_1 f) = \mathrm{pr}_1 \circ f \circ (1_Y \times s) = \mathrm{pr}_1 \circ {}^s f \circ (1_Y \times s) = \mathrm{pr}_1 f,$$

d.h. $\mathrm{pr}_1 f$ liegt im Differenzkern, ist also wegen der Exaktheit von (1) von der Form $g\mathrm{pr}_1$ für ein geeignetes $g \in \mathrm{Mor}_{\mathcal{C}_k}(Y, Z)$; und das war genau das, was wir zu zeigen hatten.

q.e.d.

1.4 Lemma. Es seien X ein geometrisch irreduzibles k-Schema und X_K der Basiswechsel $X \times_k K$; die erste Projektion $X_K \to X$ bezeichnen wir mit p und die generischen Punkte von X und X_K mit η_X und η_{X_K}. Dann gilt $p^{-1}(\eta_X) = \{\eta_{X_K}\}$.

Beweis: Mit $\mathrm{Spec}\,(K) \to \mathrm{Spec}\,(k)$ ist auch p treuflach und damit surjektiv, d.h. $p(\eta_{X_K}) = \eta_X$.

Sei nun zunächst speziell K ein separabler algebraischer Abschluß von k. Wir benutzen den folgenden Satz ([Mum94, II.4]):

> *Es sei Z ein beliebiges k-Schema. Dann identifiziert sich der Z unterliegende topologische Raum via $Z_K \xrightarrow{can} Z$ mit dem Quotienten von Z_K nach der Operation von G.*

Wir erhalten also die Faser $p^{-1}(\eta_X)$ als Orbit von η_{X_K} unter der G-Aktion. Aber unter einem Automorphismus von X_K kann der generische Punkt η_{X_K} natürlich nur wieder auf sich selbst abgebildet werden; die Behauptung ist also in diesem Fall bewiesen.

Sei jetzt K beliebig, und sei $\bar{K}$ ein separabler algebraischer Abschluß von K. Sei $x \in p^{-1}(\eta_X)$ beliebig. Mit der gleichen Begründung wie oben ist auch $X_{\bar{K}} \xrightarrow{p'} X_K$ surjektiv, d.h. wir finden einen Punkt $x' \in X_{\bar{K}}$ mit $p'(x') = x$. Es gilt also $(pp')(x') = \eta_X$, und aus dem schon bewiesenen Fall folgt, daß x' der generische Punkt von $X_{\bar{K}}$ ist. Wieder mit der gleichen Begründung wie oben folgt dann aber $x = p'(x') = \eta_{X_K}$, und das Lemma ist vollständig bewiesen. **q.e.d.**

Die folgenden beiden Lemmata werden wir unten in Beispiel 1.6(ii) benötigen, um zu zeigen, daß man Galois-Descent in der Kategorie $\mathbf{Var'_k}$ der geometrisch-irreduziblen Varietäten über k mit dominanten rationalen Abbildungen als Morphismen anwenden kann.

1.5 Lemma. Es seien X ein beliebiges k-Schema und $U \subseteq X_K$ ein offenes Unterschema. Dann ist U genau dann Urbild eines offenen Unterschemas von X, wenn U invariant unter der G-Operation ist, d.h. wenn für alle $s \in G$ gilt: $\big(1_X \times \operatorname{Spec}(s)\big)(U) \subseteq U$.

Beweis: Ist K separabel algebraisch abgeschlossen, so folgt die Behauptung unmittelbar aus dem Satz aus [Mum94], den wir im Beweis von 1.4 zitiert haben.

Sei jetzt K beliebig, sei $\bar{K}$ ein separabler algebraischer Abschluß von K, und sei $G_k := \operatorname{Gal}(\bar{K}/k)$ die absolute Galoisgruppe. Wir betrachten die Projektionen $X_{\bar{K}} \xrightarrow{p'} X_K \xrightarrow{p} X$.

Ist U unter p Urbild eines offenen Unterschemas von X, so ist U natürlich invariant unter der G-Operation. Sei also umgekehrt U invariant unter der G-Operation, und sei $U' := {p'}^{-1}(U)$ das Urbild von U in $X_{\bar{K}}$. Dann ist U' invariant unter der G_k-Operation, d.h. aus dem schon bewiesenen Fall folgt, daß $U' = (pp')^{-1}(V)$ für ein offenes V aus X ist. Es folgt:

$$p^{-1}(V) \overset{p' \text{ surjektiv}}{=} p'\big((pp')^{-1}(V)\big) = p'(U') = p'\big(p'^{-1}(U)\big) \overset{p' \text{ surjektiv}}{=} U.$$

q.e.d.

1.6 Beispiele.

(i) Es seien $\mathbf{Var_k}$ und $\mathbf{Var_K}$ die Kategorien der quasiprojektiven Varietäten über k bzw. K. Der Funktor F sei Basiswechsel mit K über k:

$$\begin{array}{lcl} X & \mapsto & X_K := X \times_k K \\ (X \xrightarrow{f} Y) & \mapsto & X_K \xrightarrow{f \times 1_K} Y_K. \end{array}$$

Die Operation eines $s \in G$ sei durch die Kommutativität des folgenden Diagrammes definiert:

$$\begin{array}{ccc} Y_K & \xrightarrow{\quad f \quad} & Z_K \\ {\scriptstyle 1_Y \times \operatorname{Spec} s}\uparrow\wr & = & \wr\uparrow{\scriptstyle 1_Z \times \operatorname{Spec} s} \\ Y_K & \xrightarrow[{}^s f]{} & Z_K \end{array}$$

(Dabei beachte man, daß die vertikalen Pfeile keine Morphismen in $\mathbf{Var_K}$, d.h. keine K-Morphismen, sondern nur k-Morphismen sind!)
Es gilt also:

$$\boxed{{}^s f = (1_Z \times \operatorname{Spec} s)^{-1} \circ f \circ (1_Y \times \operatorname{Spec} s)} \tag{2}$$

(ii) Es seien $\mathbf{Var'_k}$ und $\mathbf{Var'_K}$ die Kategorien der *geometrisch irreduziblen* quasiprojektiven Varietäten über k bzw. K mit *dominanten, rationalen Abbildungen* als Morphismen.

Der Funktor $\mathbf{Var'_k} \xrightarrow{F} \mathbf{Var'_K}$ sei auf Objekten derselbe wie in (i), und er bilde die dominante rationale Abbildung $Y \supseteq U \xrightarrow{f} Z$ auf die rationale Abbildung $Y_K \supseteq U_K \xrightarrow{f \times 1_K} Z_K$ ab. Die Operation von G sei wieder durch Gleichung (2) gegeben, wobei jetzt alle dort auftretenden Morphismen als dominante, rationale Abbildungen gedeutet werden.

(iii) Seien $p, q \in \mathbb{N}_0$. Betrachte die Kategorien $\mathcal{V}_k^{p,q}$ und $\mathcal{V}_K^{p,q}$, deren Objekte Paare (V, x) sind, wobei V ein endlich-dimensionaler k- bzw. K-Vektorraum ist und x ein Tensor über V vom Typ (p, q), d.h.

$$x \in T_q^p := V^{\otimes p} \otimes (V^*)^{\otimes q}.$$

Morphismen $(V, x) \xrightarrow{f} (W, y)$ seien k- bzw. K-Isomorphismen $V \xrightarrow{f} W$ mit

$$\left[f^{\otimes p} \otimes ((f^{-1})^*)^{\otimes q}\right](x) = y.$$

Der Funktor $F : \mathcal{V}_k^{p,q} \to \mathcal{V}_K^{p,q}$ schicke ein Paar (V, x) auf das Paar (V_K, x_K) mit $V_K := V \otimes_k K$ und $x_K := x \otimes 1 \in T_q^p(V_K) = T_q^p(V) \otimes_k K$, einen Morphismus f auf $f \otimes 1$. Die Operation von $s \in G$ sei durch die Kommutativität des folgenden Diagrammes definiert:

$$\begin{array}{ccc} (V_K, x_K) & \xrightarrow{f}_{\sim} & (W_K, y_K) \\ {\scriptstyle 1\otimes s}\downarrow\wr & = & \wr\downarrow{\scriptstyle 1\otimes s} \\ (V_K, x_K) & \xrightarrow[{}^s f]{\sim} & (W_K, y_K) \end{array}$$

(Wieder sind die vertikalen Pfeile keine Morphismen in $\mathcal{V}_K^{p,q}$, sondern nur k-lineare Abbildungen.)
Es gilt also:

$$\boxed{{}^s f = (1 \otimes s) \circ f \circ (1 \otimes s)^{-1}} \tag{3}$$

(iv) Es seien $n, m \in \mathbb{N}_+$ positive natürliche Zahlen. Betrachte die folgenden Kategorien $\mathcal{F}_k^{n,m}$ und $\mathcal{F}_K^{n,m}$: Die Objekte seien von Null verschiedene homogene Polynome vom Grad m in $X_1, \ldots, X_n$ über k bzw. K, und ein Morphismus $P \to Q$ sei eine reguläre $n \times n$-Matrix $A = (a_{ij})$ mit $Q(AX) := Q\left(\sum_{j=1}^n a_{1j}X_j, \ldots, \sum_{j=1}^n a_{nj}X_j\right) = P$. (Man beachte, daß offenbar alle Morphismen Isomorphismen sind!) Der Funktor $F : \mathcal{F}_k^{n,m} \to \mathcal{F}_K^{n,m}$ sei der offensichtliche, durch $k[X_i] \hookrightarrow K[X_i]$ bzw. $\mathrm{GL}(n,k) \hookrightarrow \mathrm{GL}(n,K)$ induzierte. Ist $(a_{ij}) \in \mathrm{GL}(n,K)$ Morphismus in $\mathcal{F}_K^{n,r}$ und $s \in G$, so setze

$$\boxed{{}^s(a_{ij}) := ({}^s a_{ij})} \tag{4}$$

Es sei speziell $\mathrm{char}\,(k) \notin \{2, 3\}$, $n := m := 3$, und man betrachte die beiden Objekte $P := X_1^3 + X_2^3 + X_3^3$ und $Q := X_1^3 + \frac{1}{12}X_2^2X_3 + \frac{1}{4}X_3^3$ aus $\mathcal{F}_k^{3,3}$ bzw. $\mathcal{F}_K^{3,3}$. Dann

definiert $A := \begin{pmatrix} 0 & 0 & 1 \\ 3 & -3 & 0 \\ 1 & 1 & 0 \end{pmatrix}$ wegen $Q(X_3, 3X_1 - 3X_2, X_1 + X_2) = P(X_1, X_2, X_3)$ einen Morphismus von P nach Q.

(v) Es seien wieder $n, m \in \mathbb{N}_+$ positive natürliche Zahlen, und man definiere die Kategorien $\widetilde{\mathcal{F}_k^{n,m}}$ und $\widetilde{\mathcal{F}_K^{n,m}}$ wie folgt: Die Objekte seien dieselben wie in $\mathcal{F}_k^{n,m}$ bzw. $\mathcal{F}_K^{n,m}$, aber ein Morphismus $P \to Q$ sei jetzt ein Element $\bar{A}$ aus $\mathrm{PGL}(n,k)$ bzw. $\mathrm{PGL}(n,K)$ mit der Eigenschaft, daß es für jeden Repräsentanten A von $\bar{A}$ aus $\mathrm{GL}(n,k)$ bzw. $\mathrm{GL}(n,K)$ ein λ aus $k^\times$ bzw. $K^\times$ gibt mit $Q(AX) = \lambda \cdot P$. (Dann sind wieder alle Morphismen Isomorphismen!)

Der Funktor $F : \widetilde{\mathcal{F}_k^{n,m}} \to \widetilde{\mathcal{F}_K^{n,m}}$ sei wieder der offensichtliche, nämlich der durch $k[X_i] \hookrightarrow K[X_i]$ bzw. $\mathrm{PGL}(n,k) \hookrightarrow \mathrm{PGL}(n,K)$ induzierte, und die G-Operation auf den Isomorphismen oben, die von unten kommen, sei auf Repräsentanten durch Gleichung (4) definiert!

Wie oben in (iv) sei jetzt speziell $\mathrm{char}\,(k) \notin \{2,3\}$, $n := m := 3$, $P := X_1^3 + X_2^3 + X_3^3$ und $Q := X_1^3 + \frac{1}{12}X_2^2X_3 + \frac{1}{4}X_3^3$ sowie $Q' := 12X_1^3 + X_2^2X_3 + 3X_3^3$, wobei wir P, Q und Q' jetzt als Objekte aus $\widetilde{\mathcal{F}_k^{3,3}}$ bzw. $\widetilde{\mathcal{F}_K^{3,3}}$ betrachten. Dann zeigt obige Rechnung, das die Matrix A, jetzt aufgefaßt als Element aus $\mathrm{PGL}(3,k)$, einen Morphismus von P nach Q' definiert (hier mit $\lambda = \frac{1}{12}$).

(vi) Für eine Kategorie $\mathcal{C}$ und eine Gruppe S bezeichne $\mathbf{Rep}_{\mathcal{C}}^S$ die Kategorie, deren Objekte Paare (X, φ) sind, bestehend aus einem Objekt X aus $\mathcal{C}$ und einer Linksoperation φ von S auf X, d.h. einem Gruppenhomomorphismus $S \xrightarrow{\varphi} \mathrm{Aut}_{\mathcal{C}}(X)$, und deren Morphismen $(X, \varphi) \xrightarrow{f} (Y, \psi)$ äquivariante Morphismen aus $\mathcal{C}$ sind, d.h. Morphismen $X \xrightarrow{f} Y$, so daß für alle $s \in S$ folgendes Diagramm kommutiert:

$$\begin{array}{ccc} X & \xrightarrow{\quad f \quad} & Y \\ {\scriptstyle \varphi(s)}\downarrow & = & \downarrow{\scriptstyle \psi(s)} \\ X & \xrightarrow[\quad f \quad]{} & Y \end{array}$$

Es sei $\bar{K}$ ein separabler algebraischer Abschluß von K, und es seien $G_k := \mathrm{Gal}\,(\bar{K}/k)$ sowie $G_K := \mathrm{Gal}\,(\bar{K}/K)$ die absoluten Galoisgruppen von k bzw. K — es gilt also $G = G_k/G_K$.

Sei ferner $\mathcal{C}$ eine beliebige Kategorie, und man betrachte die Kategorien $\mathbf{Rep}_{\mathcal{C}}^{G_k}$ und $\mathbf{Rep}_{\mathcal{C}}^{G_K}$ sowie den Funktor $F : \mathbf{Rep}_{\mathcal{C}}^{G_k} \to \mathbf{Rep}_{\mathcal{C}}^{G_K}$, der ein Paar (X, φ) auf $(X, \varphi|G_K)$ und Morphismen auf sich selbst abbildet.

Sei $s \in G$ beliebig, und wähle einen Repräsentanten $\tilde{s} \in G_k$. Dann ist die Aktion von s auf einem Isomorphismus $(X, \varphi|G_K) \xrightarrow{f} (Y, \psi|G_K)$ durch die Kommutativität des folgenden Diagrammes definiert:

$$\begin{array}{ccc} (X, \varphi|G_K) & \xrightarrow[\sim]{\quad f \quad} & (Y, \psi|G_K) \\ {\scriptstyle \varphi(\tilde{s})}\downarrow \wr & = & \wr \downarrow {\scriptstyle \psi(\tilde{s})} \\ (X, \varphi|G_K) & \xrightarrow[{}^{s}f]{\sim} & (Y, \psi|G_K) \end{array}$$

(Wieder sind die vertikalen Pfeile keine Morphismen in $\mathbf{Rep}_{\mathcal{C}}^{G_K}$, sondern nur Morphismen in $\mathcal{C}$.)

Es gilt also:

$$\boxed{{}^s f = \psi(\tilde{s}) \circ f \circ \varphi(\tilde{s})^{-1}} \tag{5}$$

Sei speziell L ein beliebiger Körper und $\mathcal{C}$ die Kategorie der L-Vektorräume. In diesem Fall, der uns besonders interessieren wird, bezeichnen wir $\mathbf{Rep}_{\mathcal{C}}^{G_k}$ und $\mathbf{Rep}_{\mathcal{C}}^{G_K}$ mit $\mathbf{Rep}_L^{G_k}$ bzw. $\mathbf{Rep}_L^{G_K}$.

(vii) Für eine Kategorie $\mathcal{C}$ bezeichne $\mathcal{C}^{\mathrm{Iso}}$ die Kategorie mit $\mathrm{Ob}(\mathcal{C}^{\mathrm{Iso}}) := \mathrm{Ob}(\mathcal{C})$ und $\mathrm{Mor}_{\mathcal{C}^{\mathrm{Iso}}}(X,Y) := \mathrm{Iso}_{\mathcal{C}}(X,Y)$. Ist $\mathcal{C}_k \xrightarrow{F} \mathcal{C}_K$ eine Koeffizientenerweiterung, so ist auch ${\mathcal{C}_k}^{\mathrm{Iso}} \to {\mathcal{C}_K}^{\mathrm{Iso}}$ eine Koeffizientenerweiterung.

Beweis: Wir wollen zeigen, daß es sich bei den angegebenen Beispielen tatsächlichen um Koeffizientenerweiterungen handelt, d.h. daß die angegebenen Operationen von G wohldefiniert sind und die Eigenschaften (KE1) und (KE2) erfüllen:

(i) Wir wenden Satz 1.3 auf $\mathcal{C}_k := \mathbf{Var_k}$, $\mathfrak{K} := \mathrm{Spec}\,(K)$ und die Operation

$$G \longrightarrow \mathrm{Aut}_{\mathbf{Var_k}}\big(\mathrm{Spec}\,(K)\big), \quad s \mapsto \mathrm{Spec}\,(s^{-1}) = \big(\mathrm{Spec}\,(s)\big)^{-1}$$

an. Dann ist $\mathcal{C}_K$ gerade gleich $\mathbf{Var_K}$, und die in 1.3(i) definierte Operation übersetzt sich dann genau in (2), d.h. wir wissen, daß die Operation wohldefiniert ist und (KE1') erfüllt.

Zum Beweis von (KE2') nehmen wir zunächst an, G sei endlich. Die Kategorie $\mathbf{Var_k}$ besitzt das Endobjekt $\mathrm{Spec}\,(k)$, und in $\mathbf{Var_k}$ existieren beliebige Faserprodukte. Um zu beweisen, daß $\mathrm{Spec}\,(K) \xrightarrow{\varphi} \mathrm{Spec}\,(k)$ ein universeller effektiver Epimorphismus in $\mathbf{Var_k}$ ist, benutzen wir den folgenden Satz ([Gro71, 5.3.]):

> *Ein treuflacher, quasikompakter Morphismus ist ein universeller effektiver Epimorphismus in der Kategorie* **Sch** *der Schemata.*

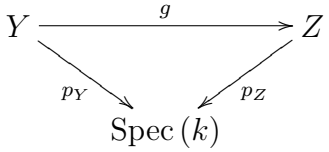
φ ist natürlich treuflach und quasikompakt, d.h. der Satz ist anwendbar, und es folgt, daß φ ein universeller effektiver Morphismus *in* **Sch** ist. Seien nun Y und Z beliebige quasiprojektive Varietäten über k bzw. K. Dann ist also

$$\mathrm{Mor}_{\mathbf{Sch}}(Y,Z) \to \mathrm{Mor}_{\mathbf{Sch}}(Y_K,Z) \rightrightarrows \mathrm{Mor}_{\mathbf{Sch}}(Y_K \times_k Y_K, Z)$$

exakt. Um zu beweisen, daß auch

$$\mathrm{Mor}_{\mathbf{Var_k}}(Y,Z) \to \mathrm{Mor}_{\mathbf{Var_k}}(Y_K,Z) \rightrightarrows \mathrm{Mor}_{\mathbf{Var_k}}(Y_K \times_k Y_K, Z)$$

exakt ist, müssen wir für beliebiges $f \in \mathrm{Mor}_{\mathbf{Var_k}}(Y_K,Z)$ aus dem Differenzkern zeigen, daß das $g \in \mathrm{Mor}_{\mathbf{Sch}}(Y,Z)$ mit $f = g\mathrm{pr}_1$ ein Morphismus in $\mathbf{Var_k}$ ist, d.h. daß



kommutiert (wobei für ein k-Schema X der Strukturmorphismus mit p_X bezeichnet werde). Nun ist $Y \times_k K \xrightarrow{\mathrm{pr}_1} Y$ als *effektiver* Epimorphismus insbesondere auch ein *Epimorphismus* in **Sch**, d.h. die beiden Morphismen $Y \xrightarrow{p_Y} \mathrm{Spec}\,(k)$ und $Y \xrightarrow{p_Z g} \mathrm{Spec}\,(k)$ sind genau dann gleich, wenn sie es nach Vorschalten von pr_1 sind:

$$p_Y \circ \mathrm{pr}_1 \overset{\mathrm{pr}_1\ k\text{-Morphismus}}{=} p_{(Y\times_k K)} \overset{f\ k\text{-Morphismus}}{=} p_Z f = p_Z \circ (g\mathrm{pr}_1) = (p_Z g) \circ \mathrm{pr}_1.$$

Damit haben wir bewiesen, daß φ ein universeller effektiver Epimorphismus in der Kategorie $\mathbf{Var_k}$ ist.

Es bleibt zu zeigen, daß $\coprod_{s\in G} \mathfrak{K} \xrightarrow{\amalg(1_{\mathfrak{K}}\times s)} \mathfrak{K} \times \mathfrak{K}$ ein Isomorphismus ist; in unserem Fall bedeutet dies genau, daß $K \otimes_k K \xrightarrow{\prod(1_K \otimes s^{-1})} \prod_{s\in G} K$ ein Isomorphismus von k-Algebren ist. Dies ist aber klar, denn weil K/k endlich und galoissch ist, finden wir ein primitives separables Element $\alpha \in K$ mit Minimalpolynom $f \in k[X]$, und es ergibt sich:

$$\begin{aligned} K \otimes_k K \cong K \otimes_k k[X]/(f) &\cong K[X]/(f) \\ &= K[X]/\left(\textstyle\prod_{s\in G}(X - s\alpha)\right) \cong \prod_{s\in G} K[X]/(X - s\alpha) \cong \prod_{s\in G} K, \end{aligned}$$

und die Abbildungsvorschrift ist offenbar gerade die gewünschte. — Damit sind alle Voraussetzungen von 1.3(ii) erfüllt, und (KE2') folgt im Fall $\#G < \infty$.

Sei nun G beliebig. Seien Y und Z beliebige k-Varietäten, und sei $Y_K \xrightarrow{f} Z_K$ ein K-Morphismus, der fix unter der G-Operation ist. Weil Y und Z als quasiprojektive Varietäten von endlichem Typ über k sind, ist f schon über einem Körper K' definiert, der endlich über k ist:

Der Morphismus f wird gegeben durch endlich viele Morphismen zwischen endlich vielen affinen offenen Teilen von Y_K und Z_K. Die affinen offenen Teile werden durch endlich viele Gleichungen mit Koeffizienten aus K gegeben, ebenso werden die Morphismen durch Polynome mit endlich vielen Koeffizienten aus K gegeben; als K' kann man dann den Körper wählen, der durch Adjunktion all dieser endlich vielen Koeffizienten zu k entsteht.

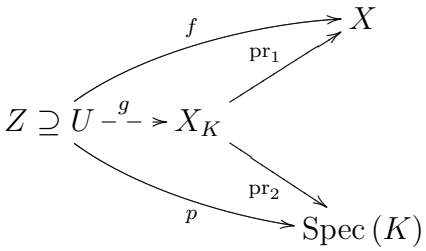
— Durch Übergang zur normalen Hülle können wir annehmen, daß K'/k endlich und galoissch mit Galoisgruppe G' ist.

Fassen wir nun f als K'-Morphismus von $Y_{K'}$ nach $Z_{K'}$ auf, so ist f nach Voraussetzung fix unter der G'-Operation, und weil G' endlich ist, folgt dann mit unseren obigen Überlegungen, daß f sogar schon über k definiert ist. Damit ist (KE2') auch in diesem Fall bewiesen.

(ii) Ähnlich wie in (i) wollen wir 1.3(i) auf $\mathcal{C}_k := \mathbf{Var'_k}$, $\mathfrak{K} := \mathrm{Spec}\,(K)$ und die Operation $s \mapsto \mathrm{Spec}\,(s^{-1})$ anwenden, um die Wohldefiniertheit von F, von der Operation von G auf den Morphismenmengen und die Gültigkeit von (KE1') zu zeigen.

Dazu überlegen wir uns zunächst, daß für $X \in \mathrm{Ob}\,(\mathbf{Var'_k})$ die Varietät X_K ein Produkt von X und $\mathfrak{K}$ in $\mathbf{Var'_k}$ ist: Zunächst ist X_K überhaupt ein *Objekt* in $\mathbf{Var'_k}$, weil wir X als *geometrisch* irreduzibel vorausgesetzt haben, und die Projektionen $X_K \to \mathrm{Spec}\,(K)$ und $X_K \to X$ sind dominant — die erste trivialerweise, die zweite nach 1.4. Sei nun $Z \in \mathrm{Ob}\,(\mathbf{Var'_k})$ beliebig, und seien $Z \supseteq U \xrightarrow{f} X$ und $Z \supseteq V \xrightarrow{p} \mathrm{Spec}\,(K)$ zwei dominante rationale Abbildungen. Durch Übergang zu $U \cap V$ können

wir ohne Beschränkung der Allgemeinheit $U = V$ annehmen. Nach der universellen Eigenschaft von X_K gibt es dann genau einen Morphismus $U \xrightarrow{g} X_K$ *in* $\mathbf{Var_k}$, der das Diagramm



kommutativ ergänzt. Wir müssen zeigen, daß g *dominant* ist: Seien η_Z, η_X und η_{X_K} die generischen Punkte von Z, X und X_K. Weil f nach Voraussetzung dominant ist, gilt $f(\eta_Z) = \mathrm{pr}_1\big(g(\eta_Z)\big) = \eta_X$, d.h. $g(\eta_Z) \in \mathrm{pr}_1^{-1}(\eta_X)$. Aus 1.4 folgt daher $g(\eta_Z) = \eta_{X_K}$, d.h. g ist tatsächlich dominant.

Sei $Z \supseteq U' \xrightarrow{g'} X_K$ eine weitere dominante rationale Abbildung, die obiges Diagramm kommutativ ergänzt. Durch Übergang zu $U \cap U'$ können wir ohne Beschränkung der Allgemeinheit $U = U'$ annehmen, und dann folgt $g = g'$ aus der Eindeutigkeit von g. — Wir haben also bewiesen, daß X_K das Produkt von X mit $\mathrm{Spec}\,(K)$ in der Kategorie $\mathbf{Var'_k}$ ist, und es folgt aus 1.3(i), daß der Funktor F und die Operation von G wohldefiniert sind und daß sie (KE1') erfüllen.

Zum Beweis von (KE2') wollen wir diesmal nicht 1.3(ii) benutzen, sondern die Behauptung auf Beispiel (i) zurückführen: Seien also Y und Z geometrisch irreduzible, quasiprojektive Varietäten über k, und sei $f : Y_K \dashrightarrow Z_K$ eine dominante rationale Abbildung, die fix unter der G-Operation ist.

Sei f auf einem dichten offenen Teil U von Y_K definiert, und sei $W := Y_K \setminus U$ das abgeschlossene Komplement. Weil Y_K von endlichem Typ über K ist, wird W durch endlich viele Gleichungen mit endlich vielen Koeffizienten aus K definiert, die alle in einem Körper $K' \subseteq K$ liegen, der *endlich* über k ist; bezeichne $H \leq G$ die Galoisgruppe $\mathrm{Gal}\,(K/K')$, sie ist offen und von endlichem Index in G. Für $s \in H$ gilt $(1 \times s)(Z) = Z$, d.h. es gilt

$$U' := \bigcap_{s\in G}(1\times s)(U) = \bigcap_{s\in G}\Big(Y_K \setminus (1\times s)(Z)\Big) = Y_K \setminus \bigcup_{s\in G}(1\times s)(Z)$$
$$= Y_K \setminus \bigcup_{sH\in G/H}(1\times s)(Z) = \bigcap_{sH\in G/H}(1\times s)(U),$$

und wegen $(G : H) < \infty$ ist dies ein *endlicher* Schnitt, d.h. U' ist offen und dicht.

Nach Konstruktion ist U' invariant unter der G-Operation, so daß wir nach 1.5 wissen, daß $U' = \mathrm{pr}_1^{-1}(V) = V_K$ für ein offenes $V \subseteq Y$ gilt. Der Morphismus $V_K \xrightarrow{g|V_K} Z_K$ in $\mathbf{Var_K}$ ist nach Voraussetzung invariant unter der G-Operation, und deshalb folgt aus (i), daß $g|V_K$ Basiswechsel eines $V \xrightarrow{h} Z$ ist.

Ist h dominant? Ja, denn bezeichnen wir die Projektionen $V_K \to V$ und $Z_K \to Z$ mit p_V und p_Z und die generischen Punkte von V_K, V, Z_K und Z mit η_{V_K}, η_V, η_{Z_K} und η_Z, so folgt:

$$h(\eta_V) \overset{1.4}{=} (hp_V)(\eta_{V_K}) = (p_Z g)(\eta_{V_K}) \overset{g \text{ dominant}}{=} p_Z(\eta_{Z_K}) \overset{1.4}{=} \eta_Z.$$

Also definiert h in $\mathbf{Var}'_{\mathbf{k}}$ einen Morphismus h' von Y nach Z, und offenbar gilt $f = Fh'$ — damit ist auch (KE2') bewiesen.

(iii)

- *Wohldefiniertheit:* Seien $s \in G$ und $f : (V_K, x_K) \xrightarrow{\sim} (W_K, y_K)$ vorgegeben. Es ist zunächst zu zeigen, daß ${}^s f$ nicht bloß k-linear, sondern sogar K-linear ist. Für beliebiges $v = \sum v_i \otimes \lambda_i \in V_K$ und $\lambda \in K$ gilt

$$\begin{aligned}(1 \otimes s)(\lambda v) &= (1 \otimes s) \sum v_i \otimes \lambda\lambda_i = \sum v_i \otimes s(\lambda\lambda_i) \\ &= s(\lambda) \sum v_i \otimes s(\lambda_i) = s(\lambda) \cdot (1 \otimes s)(v).\end{aligned} \tag{6}$$

  Also folgt:

$$\begin{aligned}{}^s f(\lambda v) &= \left[(1 \otimes s) \circ f \circ (1 \otimes s)^{-1}\right](\lambda v) \overset{(6)}{=} \left[(1 \otimes s) \circ f\right]\Big(s^{-1}(\lambda) \cdot (1 \otimes s)^{-1}(v)\Big) \\ &= (1 \otimes s)\Big(s^{-1}(\lambda) \cdot \left[f \circ (1 \otimes s)^{-1}\right](v)\Big) \\ &\overset{(6)}{=} s(s^{-1}(\lambda)) \cdot \left[(1 \otimes s) \circ f \circ (1 \otimes s)^{-1}\right](v) = \lambda \cdot {}^s f(v).\end{aligned}$$

  Bleibt zu zeigen, daß die Tensoren von ${}^s f$ respektiert werden, daß also gilt:

$$\left[{}^s f^{\otimes p} \otimes (({}^s f^{-1})^*)^{\otimes q}\right](x_K) = y_K.$$

  Für $w \in V$ gilt aber offenbar ${}^s f(w \otimes 1) = f(w \otimes 1)$, so daß die Behauptung folgt, da x_K „von unten“ kommt.

- *Linksoperation:* Seien $s, t \in G$ und $f : (V_K, x_K) \xrightarrow{\sim} (W_K, y_K)$ vorgegeben. Dann folgt:

$$\begin{aligned}{}^1 f &\overset{(3)}{=} (1 \otimes 1_K) \circ f \circ (1 \otimes 1_K)^{-1} \\ &= 1 \circ f \circ f^{-1} \\ &= f,\end{aligned}$$

$$\begin{aligned}{}^{st} f &\overset{(3)}{=} (1 \otimes st) \circ f \circ (1 \otimes st)^{-1} \\ &= \Big((1 \otimes s) \circ (1 \otimes t)\Big) \circ f \circ \Big((1 \otimes s) \circ (1 \otimes t)\Big)^{-1} \\ &= (1 \otimes s) \circ \Big((1 \otimes t) \circ f \circ (1 \otimes t)^{-1}\Big) \circ (1 \otimes s)^{-1} \\ &= (1 \otimes s) \circ {}^t f \circ (1 \otimes s)^{-1} \\ &= {}^s\big({}^t f\big).\end{aligned}$$

- *(KE1):* Seien $s \in G$ und Morphismen $(V_K, x_K) \xrightarrow{g} (W_K, y_K) \xrightarrow{f} (U_K, z_K)$ in $\mathcal{V}_K^{p,q}$ vorgegeben, dann folgt:

$$\begin{aligned}{}^s(fg) &\overset{(3)}{=} (1 \otimes s) \circ (fg) \circ (1 \otimes s)^{-1} \\ &= (1 \otimes s) \circ f \circ (1 \otimes s)^{-1} \\ &\qquad \circ (1 \otimes s) \circ g \circ (1 \otimes s)^{-1} \\ &= {}^s f \circ {}^s g.\end{aligned}$$

- *(KE2):* Sei $f : (V_K, x_K) \xrightarrow{\sim} (W_k, y_K)$ fix unter der G-Operation. Seien (v_j) und (w_i) k-Basen von V bzw. W. Dann sind $(v_j \otimes 1)$ und $(w_i \otimes 1)$ K-Basen von V_K bzw. W_K; sei (a_{ij}) die zugehörige Matrix von f. Für $s \in G$ folgt dann:

$$\begin{aligned} {}^s f(v_j \otimes 1) &\overset{(3)}{=} \left[(1 \otimes s) \circ f \circ (1 \otimes s)^{-1}\right](v_j \otimes 1) = \left[(1 \otimes s) \circ f\right](v_j \otimes 1) \\ &= (1 \otimes s)\left(\sum_i w_i \otimes a_{ij}\right) = \sum_i s(a_{ij}) w_i. \end{aligned}$$

  Wir erhalten also folgende Formel für die Operation von G, wenn f als Matrix gegeben ist:

$$\boxed{{}^s(a_{ij}) \;=\; ({}^s a_{ij})}, \tag{7}$$

  wobei ${}^s a_{ij} := s(a_{ij})$. Da nach Voraussetzung f fix unter der G-Operation war, sind also alle a_{ij} ebenfalls fix, liegen demnach schon in k. Also kommt f tatsächlich „von unten“.

(iv)
- *Wohldefiniertheit:* Sei ohne Beschränkung der Allgemeinheit $n = 1$. Seien $P, Q \in k[X_1]$ und $a \in \mathrm{GL}(1, K) = K^\times$ ein Morphismus $FP \to FQ$ in $\mathcal{F}_K^{n,m}$, d.h. $Q(aX_1) = P = \sum c_i X_1^i$. Dann gilt für $s \in G$:

$$Q({}^s a X_1) \overset{Q \in k[X_1]}{=} \sum {}^s c_i X_1^i \overset{c_i \in k}{=} \sum c_i X_1^i = P,$$

  d.h. auch ${}^s a$ ist ein Morphismus in $\mathcal{F}_K^{n,m}$.
- *Linksoperation:* Klar!
- *(KE1):* Klar!
- *(KE2):* Klar!

(v)
- *Wohldefiniertheit:* Seien $P, Q \in \mathrm{Ob}\,(\widetilde{\mathcal{F}_k^{n,m}})$, und sei $FP \xrightarrow{\bar{A}} FQ$ ein Isomorphismus mit zwei Repräsentanten (a_{ij}) und $(\tilde{a}_{ij})$. Dann gibt es ein $\lambda \in K^\times$ mit

$$\forall i, j \in \{1, \ldots, n\} \,:\, \tilde{a}_{ij} = \lambda \cdot a_{ij}.$$

  Dann ist aber $({}^s\tilde{a}_{ij}) = {}^s\lambda \cdot ({}^s a_{ij})$ für $s \in G$, d.h. $({}^s a_{ij})$ und $({}^s\tilde{a}_{ij})$ repräsentieren dasselbe, wohldefinierte Element in $\mathrm{PGL}(n, K)$.
- *Linksoperation:* Klar!
- *(KE1):* Klar!
- *(KE2):* Sei $\tilde{A} \in \mathrm{PGL}(n, K)$ fix unter der Operation von G. Wähle einen Repräsentanten A von $\tilde{A}$, der an mindestens einer Stelle eine Eins stehen hat (was offenbar möglich ist)! Ist $s \in G$ beliebig, so gibt es nach Voraussetzung ein $\lambda \in K^\times$ mit ${}^s A = \lambda \cdot A$. Wegen ${}^s 1 = 1$ folgt aber sofort $\lambda = 1$, d.h. für alle $s \in G$ gilt ${}^s A = A \in \mathrm{GL}(n, K)$, woraus $A \in \mathrm{GL}(n, k)$ und also $\tilde{A} \in \mathrm{PGL}(n, k)$ folgt.

(vi)
- *Wohldefiniertheit:* Seien $s \in G$ und $f : (X, \varphi|G_K) \xrightarrow{\sim} (Y, \psi|G_K)$ vorgegeben. Zunächst wollen wir zeigen, daß ${}^s f$ unabhängig von der Wahl des Repräsentanten $\tilde{s} \in G_k$ von s ist. Sei also $\bar{s} \in G_k$ ein weiterer Repräsentant. Es gibt

dann ein $t \in G_K$ mit $\bar{s} = \tilde{s}t$. Da f eine G_K-äquivariante Abbildung ist, gilt $f \circ \varphi(t^{-1}) = \psi(t^{-1}) \circ f$. Damit folgt:

$$\begin{aligned}\psi(\bar{s}) \circ f \circ \varphi(\bar{s})^{-1} &= \psi(\tilde{s}t) \circ f \circ \varphi(\tilde{s}t)^{-1} \\ &= \psi(\tilde{s}) \circ \psi(t) \circ \big(f \circ \varphi(t)^{-1}\big) \circ \varphi(\tilde{s})^{-1} \\ &= \psi(\tilde{s}) \circ \psi(t) \circ \big(\psi(t)^{-1} \circ f\big) \circ \varphi(\tilde{s})^{-1} \\ &= \psi(\tilde{s}) \circ f \circ \varphi(\tilde{s})^{-1}\end{aligned}$$

Zu zeigen bleibt, daß ${}^s f$ eine G_K-äquivariante Abbildung ist. Sei hierzu $t \in G_K$ beliebig. Weil G_K ein Normalteiler in G_k ist, gibt es ein $t' \in G_K$ mit $t\tilde{s} = \tilde{s}t'$. Es folgt:

$$\begin{aligned}\psi(t) \circ {}^s f &\overset{(5)}{=} \psi(t\tilde{s}) \circ f \circ \varphi(\tilde{s}) = \psi(\tilde{s}t') \circ f \circ \varphi(\tilde{s}) \\ &= \psi(\tilde{s}) \circ f \circ \varphi(t'\tilde{s}) = \psi(\tilde{s}) \circ f \circ \varphi(\tilde{s}t) \\ &\overset{(5)}{=} {}^s f \circ \varphi(t).\end{aligned}$$

- *Linksoperation:* Folgt formal genau wie in (iii)!
- *(KE1):* Folgt ebenfalls genau wie in (iii)!
- *(KE2):* Sei $f : (X, \varphi|G_K) \xrightarrow{\sim} (Y, \psi|G_K)$ fix unter der Operation von G. Wir müssen zeigen, daß f dann sogar G_k-äquivariant ist. Sei dazu $\tilde{s} \in G_k$ beliebig und s das Bild in G. Nach Voraussetzung gilt ${}^s f = f$, also

$$\psi(\tilde{s}) \circ f \circ \varphi(\tilde{s})^{-1} = f \quad \Longrightarrow \quad \psi(\tilde{s}) \circ f = f \circ \varphi(\tilde{s}),$$

was genau die Behauptung ist.

(vii) Klar, da alle zu prüfenden Eigenschaften sich nur auf Isomorphismen beziehen!

q.e.d.

1.7 Satz/ Definition. Es sei $\mathcal{C}_k$ eine pseudoabelsche, k-lineare Kategorie (d.h. alle Morphismenmengen sind k-Vektorräume, und die Komposition von Morphismen ist k-bilinear). Definiere $\mathcal{C}_K$, *die Kategorie $\mathcal{C}_k$ mit Koeffizienten in K*, als die pseudoabelsche Hülle der folgenden Kategorie: Objekte sind dieselben wie in $\mathcal{C}_k$, für zwei Objekte X, Y ist

$$\mathrm{Mor}_K(X, Y) := \mathrm{Mor}_k(X, Y) \otimes_k K,$$

und die Verknüpfung zweier Morphismen $\sum f_i \otimes x_i$ und $\sum g_j \otimes y_j$ ist $\sum (f_i \circ g_j) \otimes (x_i y_j)$. Die Kategorie $\mathcal{C}_K$ ist dann pseudoabelsch und K-linear. Wir haben einen offensichtlichen Funktor $F : \mathcal{C}_k \to \mathcal{C}_K$, der ein Objekt X auf $(X, 1_X)$ und einen Morphismus f auf $f \otimes 1$ schickt. Sind X und Y Objekte aus $\mathcal{C}_k$, so operiert die Galoisgruppe G auf $\mathrm{Mor}_K(FX, FY)$ via ${}^s(\sum f_i \otimes x_i) := \sum f_i \otimes {}^s x_i$, und diese Operation hat die Eigenschaften (KE1') und (KE2') aus 1.2, so daß der Funktor F zu einer Koeffizientenerweiterung wird.

Beweis:

- *Wohldefiniertheit:* Es sei $s \in G$ beliebig, und es seien X und Y beliebige Objekte aus $\mathcal{C}_k$. Dann gilt $\mathrm{Mor}_K(FX, FY) = \mathrm{Mor}_k(X, Y) \otimes_k K$, und die Abbildung

$$\mathrm{Mor}_k(X, Y) \times K \longrightarrow \mathrm{Mor}_k(X, Y) \otimes_k K, \quad (f, x) \mapsto f \otimes {}^s x$$

  ist offenbar k-bilinear und induziert daher über die universelle Eigenschaft des Tensorproduktes einen k-Endomorphismus von $\mathrm{Mor}_K(FX, FY)$, der gerade $\sum f_i \otimes x_i$ auf $\sum f_i \otimes {}^s x$ abbildet. Die Operation hängt also nicht von der Darstellung eines Morphismus als Summe von Tensoren ab.

- *Linksoperation:* Klar!

- *(KE1'):* Es seien X, Y und Z beliebige Objekte aus $\mathcal{C}_k$, ferner $f = \sum f_i \otimes x_i \in \mathrm{Mor}_K(FY, FZ)$ und $g = \sum g_j \otimes y_j \in \mathrm{Mor}_K(FX, FY)$ beliebig. Dann gilt für jedes $s \in G$:

$$\begin{aligned} {}^s(fg) = {}^s\Big(\sum f_i g_j \otimes x_i y_j\Big) &= \sum f_i g_j \otimes {}^s(x_i y_j) \\ &= \sum f_i g_j \otimes {}^s x_i \, {}^s y_j = \Big(\sum f_i \otimes {}^s x_i\Big) \circ \Big(\sum g_j \otimes {}^s y_j\Big) = {}^s f \circ {}^s g. \end{aligned}$$

- *(KE2'):* Es seien X und Y Objekte aus $\mathcal{C}_k$, und sei zunächst $f : X \to Y$ ein Morphismus „unten“. Dann gilt $Ff = f \otimes 1$, und für alle $s \in G$ ist ${}^s Ff = f \otimes {}^s 1 = f \otimes 1 = Ff$, d.h. Ff ist tatsächlich fix unter der G-Operation.

  Wähle eine k-Basis $\{f_i\}_i$ von $\mathrm{Mor}_k(X, Y)$ (so daß also $\{f_i \otimes 1\}_i$ eine K-Basis von $\mathrm{Mor}_K(FX, FY)$ ist), und sei nun umgekehrt $f = \sum x_i \cdot (f_i \otimes 1) = \sum f_i \otimes x_i$ ein Morphismus von FX nach FY, der fix unter der G-Operation ist. Dann gilt für alle $s \in G$:

$$\sum x_i \cdot (f_i \otimes 1) = f = {}^s f = \sum f_i \otimes {}^s x_i = \sum {}^s x_i \cdot (f_i \otimes 1),$$

  so daß die Koeffizienten $x_i \in K$ fix unter der G-Operation und also schon aus k sind, d.h.

$$f = F \underbrace{\Big(\sum x_i \cdot f_i\Big)}_{\in \mathrm{Mor}_k(X,Y)}.$$

q.e.d.

2 Nicht-abelsche Gruppenkohomologie

In diesem Kapitel werden wir die nicht-abelsche Gruppenkohomologie in dem Maße entwickeln, in dem wir sie in den folgenden Kapiteln benötigen werden. Dabei folgen wir im Wesentlichen Serres Ausführungen in [Ser97], betrachten allerdings beliebige topologische Gruppen und nicht bloß proendliche.

In diesem Kapitel bezeichne S stets eine topologische Gruppe.

2.1 Definition. Eine *S-Menge* ist eine Menge, auf der S von links operiert. Eine *diskrete S-Menge* ist eine S-Menge A, bei der die Operation $S \times A \to A$ *stetig* ist, wobei A mit der diskreten Topologie versehen wird. (Insbesondere ist also jede S-Menge diskret, wenn S die diskrete Topologie trägt.)
Ein *Morphismus von (diskreten) S-Mengen* A und B ist eine mit der S-Operation verträgliche Abbildung $A \xrightarrow{f} B$, d.h.

$$\forall s \in S \; \forall a \in A \; : \; f({}^s a) = {}^s[f(a)].$$

Wir erhalten so die *Kategorie der (diskreten) S-Mengen*, wobei die Verkettung von Morphismen selbstverständlich durch die Verkettung der unterliegenden Abbildungen definiert wird.

2.2 Lemma. Für eine S-Menge A sind die folgenden drei Aussagen äquivalent:

(i) A ist eine diskrete S-Menge.

(ii) Für alle $a \in A$ ist $\mathrm{Stab}_S(a)$, der Stabilisator von a in S, eine offene Untergruppe von S.

(iii) Es gilt $A = \bigcup_U A^U$, wobei sich die Vereinigung über alle offenen Untergruppen U von S erstreckt.

Beweis:

- *(i)⇒(ii):* Seien also $S \times A \xrightarrow{\varphi} A$ stetig und $a \in A$ beliebig. Es ist A diskret, also $\{a\} \subseteq A$ offen und damit nach Voraussetzung $T := \varphi^{-1}(\{a\})$ offen. Wegen $(1, a) \in T$ gibt es also eine offene Umgebung U von 1 in S mit $S \times \{a\} \subseteq T$, d.h.

  $$\forall u \in U \; : \; {}^u a = \varphi(u, a) = a \qquad \Longrightarrow \qquad 1 \in U \subseteq \mathrm{Stab}_S(a).$$

  Das neutrale Element ist also ein innerer Punkt des Stabilisators von a; dann sind aber auch alle anderen Elemente von $\mathrm{Stab}_S(a)$ innere Punkte, der Stabilisator ist also offen in S.

- *(ii)⇒(iii):* Die Inklusion „$\supseteq$“ ist trivial, es ist also nur „$\subseteq$“ zu zeigen. Sei dazu $a \in A$ beliebig. Nach Voraussetzung ist dann $U := \mathrm{Stab}_S(a)$ eine offene Untergruppe von S, und natürlich gilt $a \in A^U$.

- *(iii)⇒(i):* Wir müssen zeigen, daß $S \times A \xrightarrow{\varphi} A$ stetig ist. Eine Abbildung in eine diskrete Menge ist aber offenbar genau dann stetig, wenn sie lokalkonstant ist, wir haben also zu zeigen, daß φ lokalkonstant ist. Sei dazu $(s, a) \in S \times A$ beliebig. Nach Voraussetzung gibt es eine offene Untergruppe U von S mit $a \in A^U$. Dann ist $M := sU \times \{a\}$ offen in $S \times A$, und

$$\forall u \in U \,:\, \varphi(su, a) = {}^{s}({}^{u}a) = {}^{s}a,$$

d.h. $\varphi|M$ ist konstant.

q.e.d.

2.3 Definition. Eine *S-Gruppe* ist eine (nicht notwendig abelsche) Gruppe A, die zugleich eine S-Menge ist, wobei S mittels Gruppenhomomorphismen operiert, d.h.

$$\forall s \in S \; \forall a, b \in A \,:\, {}^{s}(ab) = {}^{s}a \cdot {}^{s}b.$$

Eine *diskrete S-Gruppe* ist eine S-Gruppe, die sogar eine *diskrete* S-Menge ist. (Insbesondere ist also jede S-Gruppe diskret, wenn S die diskrete Topologie trägt.)

Ein *Morphismus von (diskreten) S-Gruppen* ist ein Gruppenhomomorphismus, der zugleich ein Morphismus von (diskreten) S-Mengen ist, d.h. ein S-äquivarianter Gruppenhomomorphismus.

Wir erhalten so die *Kategorie der (diskreten) S-Gruppen*, wobei die Verkettung von Morphismen wieder durch die Verkettung der unterliegenden Gruppenhomomorphismen gegeben wird.

Die Kohomologie $H^1_{\mathrm{cont}}(S, A)$, die wir unten in 2.7 definieren werden, ist für nichtabelsches A im allgemeinen keine *Gruppe* mehr, sondern bloß eine *punktierte Menge* — wir erinnern deswegen zunächst kurz an die Kategorie der punktierten Mengen und an den Begriff der Exaktheit einer Sequenz von punktierten Mengen.

2.4 Definition. Die *Kategorie der punktierten Mengen* ist wie folgt definiert: Objekte sind Paare (L, x), bestehend aus einer Menge L und einem Element $x \in L$, dem sogenannten *ausgezeichneten Punkt*, und ein *Morphismus von punktierten Mengen* $(L, x) \to (M, y)$ ist eine Abbildung $L \xrightarrow{f} M$ mit $f(x) = y$.

Ein Morphismus f von punktierten Mengen heißt, *injektiv*, *surjektiv* bzw. *bijektiv*, wenn f, aufgefaßt als bloße Abbildung, injektiv, surjektiv bzw. bijektiv ist.

Ist $(L, x) \xrightarrow{f} (M, y)$ ein Morphismus von punktierten Mengen, so ist der *Kern von f* die punktierte Menge

$$\mathrm{Ker}\,(f) := \big(f^{-1}(\{y\}), x\big),$$

und das *Bild von f* ist die punktierte Menge

$$\mathrm{Im}\,(f) := \big(f(L), y\big).$$

Eine Sequenz $(L, x) \xrightarrow{f} (M, y) \xrightarrow{g} (N, z)$ von punktierten Mengen heißt *exakt*, wenn $\mathrm{Ker}\,(g) = \mathrm{Im}\,(f)$ gilt. Allgemeiner heißt eine Sequenz

$$(L_0, x_0) \xrightarrow{f_0} (L_1, x_1) \xrightarrow{f_1} \ldots \xrightarrow{f_{n-1}} (L_n, x_n) \xrightarrow{f_n} (L_{n+1}, x_{n+1})$$

von punktierten Mengen *exakt*, wenn für alle $1 \leq i \leq n$ die Sequenzen $(L_{i-1}, x_{i-1}) \xrightarrow{f_{i-1}} (L_i, x_i) \xrightarrow{f_i} (L_{i+1}, x_{i+1})$ exakt sind.
Das Endobjekt in der Kategorie der punktierten Mengen, also die einelementige Menge mit dem einzigen Element als ausgezeichnetem Punkt, wird mit $*$ bezeichnet.

2.5 Bemerkung. Es sei $(L, x) \xrightarrow{f} (M, y)$ ein Morphismus von punktierten Mengen. Die Sequenz $(L, x) \xrightarrow{f} (M, y) \to *$ ist genau dann exakt, wenn f surjektiv ist, und ist f injektiv, so ist die Sequenz $* \to (L, x) \xrightarrow{f} (M, y)$ exakt. — Die Umkehrung hiervon ist jedoch im allgemeinen falsch.

Jetzt können wir die Kohomologien $H^0(S, A)$ und $H^1_{\text{cont}}(S, A)$, die Gegenstand dieses Kapitels sind, definieren.

2.6 Definition. Für eine S-Gruppe A definiere die *nullte Kohomologie* als die Gruppe

$$H^0(S, A) := A^S := \{a \in A \,|\, \forall s \in S : {}^s a = a\}.$$

Ist $A \xrightarrow{f} B$ ein Morphismus von S-Gruppen, so gilt offenbar $f(A^S) \subseteq B^S$, und wir erhalten einen induzierten Gruppenhomomorphismus

$$H^0(f) := f|A^S : H^0(S, A) \longrightarrow H^0(S, B),$$

wodurch $H^0(S, \_)$ zu einem kovarianten Funktor von der Kategorie der S-Gruppen in die Kategorie der Gruppen wird.
Im Folgenden werden wir die nullte Kohomologie oft nur als *punktierte Menge* (mit dem neutralen Element als ausgezeichnetem Element) und $H^0(S, \_)$ als Funktor in die Kategorie der punktierten Mengen auffassen.

2.7 Lemma/ Definition. Sei A eine S-Gruppe. Die Menge $Z^1(S, A)$ der *1-Kozykel von S in A* ist definiert als die Menge der Abbildungen $s \mapsto a_s$ von S nach A, die folgende *1-Kozykelbedingung* erfüllen:

$$\forall s, t \in S : \; a_{st} = a_s {}^s a_t.$$

$Z^1(S, A)$ ist eine punktierte Menge mit dem ausgezeichneten Element $s \mapsto 1$, dem sogenannten *trivialen Kozykel*. Auf der Menge der 1-Kozykel wird wie folgt eine Äquivalenzrelation definiert:

$$(a_s) \sim (a'_s) \;:\Leftrightarrow\; \exists b \in A : \forall s \in S : a'_s = b^{-1} a_s {}^s b.$$

Zwei äquivalente Elemente heißen *kohomolog*, und $H^1(S, A) := Z^1(S, A)/\sim$, die *erste Kohomologie*, sei die Menge der Äquivalenzklassen.
Ist $A \xrightarrow{f} B$ ein Morphismus von S-Gruppen, und (a_s) ein 1-Kozykel von S in A, so ist $(f a_s)$ ein 1-Kozykel von S in B, und sind $(a_s) \sim (a'_s)$ kohomologe 1-Kozykel, so sind auch $(f a_s)$ und $(f a'_s)$ kohomolog, so daß wir eine induzierte Abbildung

$$H^1(f) : H^1(S, A) \longrightarrow H^1(S, B)$$

von punktierten Mengen erhalten. Dadurch wird auch $H^1(S, \_)$ zu einem kovarianten Funktor von der Kategorie der S-Gruppen in die Kategorie der punktierten Mengen.

Sei A jetzt eine *diskrete* S-Gruppe, und betrachte die Teilmenge $Z^1_{\text{cont}}(S, A) \subseteq Z^1(S, A)$ der *stetigen* 1-Kozykel von S in A, wobei wir A wieder mit der diskreten Topologie versehen. Der triviale 1-Kozykel ist als konstante Abbildung natürlich stetig, so daß wir $Z^1_{\text{cont}}(S, A)$ als punktierte Teilmenge aller 1-Kozykel auffassen können. Die punktierte Menge der Kohomologieklassen aus $Z^1_{\text{cont}}(S, A)$ bezeichnen wir mit $H^1_{\text{cont}}(S, A)$; wir haben dann eine Inklusion von punktierten Mengen

$$H^1_{\text{cont}}(S, A) \hookrightarrow H^1(S, A).$$

(Insbesondere gilt also $H^1_{\text{cont}}(S, A) = H^1(S, A)$, wenn S die diskrete Topologie trägt.)

Ist auch B eine diskrete S-Gruppe und $A \xrightarrow{f} B$ ein Morphismus von diskreten S-Gruppen, so faktorisiert $H^1(f)|H^1_{\text{cont}}(S, A)$ über $H^1_{\text{cont}}(S, B)$ und definiert so eine Abbildung von punktierten Mengen

$$H^1_{\text{cont}}(f) : H^1_{\text{cont}}(S, A) \longrightarrow H^1_{\text{cont}}(S, B),$$

wodurch $H^1_{\text{cont}}(S, \_)$ zu einem kovarianten Funktor von der Kategorie der diskreten S-Gruppen in die Kategorie der punktierten Mengen wird.[†]

Beweis: Klar! **q.e.d.**

2.8 Lemma. Werde speziell S topologisch von einem Element $\sigma \in S$ erzeugt (ist S zum Beispiel die absolute Galoisgruppe eines endlichen Körpers $\mathbb{F}_q$, so wird S topologisch von dem Frobenius $x \mapsto x^q$ erzeugt), und sei A eine diskrete S-Gruppe. Dann wird ein stetiger 1-Kozykel (a_s) von S in A schon eindeutig durch das Element $a_\sigma \in A$ festgelegt.

Beweis: Sei (a'_s) ein weiterer stetiger 1-Kozykel von S in A mit $a'_\sigma = a_\sigma$. Wegen der 1-Kozykelbedingung stimmen dann (a_s) und (a'_s) auf ganz $M := \{\sigma^n \in S \,|\, n \in \mathbb{Z}\}$ überein. Nach Voraussetzung ist M aber eine dichte Teilmenge von S, und zwei stetige Abbildungen, die auf einer dichten Teilmenge des Definitionsbereichs übereinstimmen, müssen schon gleich sein. **q.e.d.**

2.9 Lemma. Sei speziell $S = \langle\sigma\rangle$ zyklisch von der Ordnung $m \in \mathbb{N}_+$, versehen mit der diskreten Topologie, und sei A eine S-Gruppe. Dann sind

$$\begin{array}{ccc} Z^1(S, A) & \longleftrightarrow & \left\{ a \in A \,\middle|\, \prod_{i=0}^{m-1} \sigma^i a = 1 \right\} \\ (a_s)_s & \longmapsto & a_\sigma \\ \left(\prod_{i=0}^{r-1} \sigma^i a \right)_{\sigma^r} & \longmapsfrom & a \end{array}$$

zueinander inverse Bijektionen, und zwei 1-Kozykel $(a_s)_s$ und $(a'_s)_s$ sind genau dann kohomolog, wenn es ein $b \in A$ gibt mit $a'_\sigma = b^{-1} a_\sigma {}^\sigma b$.

[†]Ist A sogar eine *abelsche* Gruppe, so ist $H^1_{\text{cont}}(S, A)$ offenbar nicht bloß eine punktierte Menge, sondern sogar eine abelsche Gruppe.

Beweis: Bezeichne α die Abbildung „$\rightarrow$“ und β die Abbildung „$\leftarrow$“.

- α *wohldefiniert:* Wir zeigen zunächst die Formel

$$\forall (a_s)_s \in Z^1(S,A)\ \forall r \in \mathbb{N}_0\ :\ a_{\sigma^r} = \prod_{i=0}^{r-1} {}^{\sigma^i} a_\sigma. \tag{8}$$

  mittels vollständiger Induktion über r:

  - $\underline{r = 0}$: Klar!
  - $\underline{r \Rightarrow r+1}$: $a_{\sigma^{r+1}} = a_{\sigma^r \cdot \sigma} = a_{\sigma^r} \cdot {}^{\sigma^r} a_\sigma = \left(\prod_{i=0}^{r-1} {}^{\sigma^i} a_\sigma \right) \cdot {}^{\sigma^r} a_\sigma$.

  Damit folgt:

$$1 = a_1 = a_{\sigma^m} \overset{(8)}{=} \prod_{i=0}^{m-1} {}^{\sigma^i} a_\sigma.$$

- β *wohldefiniert:* Seien $a \in A$ mit $\prod_{i=0}^{m-1} {}^{\sigma^i} a = 1$ und $s \in S$ beliebig, und wähle ein $r \in \mathbb{N}_0$ mit $s = \sigma^r$. Zunächst wollen wir uns überlegen, daß die Definition von $\beta(a)_s$ unabhängig von der Wahl von r ist. Sei also eine weitere natürliche Zahl $r' \in \mathbb{N}_0$ gegeben, für die auch $s = \sigma^{r'}$ gilt. Natürlich gilt dann $r \equiv r' \bmod m$, und wir können offenbar ohne Beschränkung der Allgemeinheit den Fall $r' = r + m$ betrachten:

$$\prod_{i=0}^{r'-1} {}^{\sigma^i} a = \underbrace{\left(\prod_{i=0}^{m-1} {}^{\sigma^i} a \right)}_{=1} \cdot \left(\prod_{i=m}^{r+m-1} {}^{\sigma^i} a \right) = 1 \cdot \prod_{i=0}^{r-1} {}^{(\sigma^m \cdot \sigma^i)} a = \prod_{i=0}^{r-1} {}^{\sigma^i} a.$$

  Es bleibt zu zeigen, daß $\beta(a)$ die 1-Kozykelbedingung erfüllt. Wir geben uns also noch ein beliebiges $t \in S$ vor, gelte etwa $t = \sigma^u$ für $u \in \mathbb{N}_0$. Es folgt:

$$\beta(a)_{st} = \beta(a)_{\sigma^{r+u}} = \prod_{i=0}^{r+u-1} {}^{\sigma^i} a = \underbrace{\left(\prod_{i=0}^{r-1} {}^{\sigma^i} a \right)}_{=\beta(a)_s} \cdot \left(\prod_{i=r}^{r+u-1} {}^{\sigma^i} a \right)$$

$$= \beta(a)_s \cdot {}^{\sigma^r} \underbrace{\left(\prod_{i=0}^{u-1} {}^{\sigma^i} a \right)}_{=\beta(a)_t} = \beta(a)_s \cdot {}^{s}\beta(a)_t.$$

- $\alpha \circ \beta = id$: Klar!
- $\beta \circ \alpha = id$: Klar nach (8)!
- *kohomolog:* Die Notwendigkeit der Bedingung ist klar nach Definition von „kohomolog“. Seien nun $(a_s)_s$ und $(a'_s)_s$ 1-Kozykel, und es gelte $a'_\sigma = b^{-1} a_\sigma {}^\sigma b$ für ein geeignetes $b \in A$. Für beliebiges $r \in \mathbb{N}_0$ folgt dann:

$$a'_{\sigma^r} \overset{(8)}{=} \prod_{i=0}^{r-1} {}^{\sigma^i} a'_\sigma = \prod_{i=0}^{r-1} {}^{\sigma^i}\left(b^{-1} a_\sigma {}^\sigma b \right) = \prod_{i=0}^{r-1} {}^{\sigma^i}(b^{-1}) {}^{\sigma^i} a_\sigma {}^{\sigma^{i+1}} b$$

$$= b^{-1} \cdot \left(\prod_{i=0}^{r-1} {}^{\sigma^i} a_\sigma \right) \cdot {}^{\sigma^r} b \overset{(8)}{=} b^{-1} a_{\sigma^r} {}^{\sigma^r} b.$$

q.e.d.

Als nächstes zeigen wir, daß die Kohomologien $H^0(S,A)$ und $H^1_{\mathrm{cont}}(S,A)$ verträglich mit direkten Summen sind, wie man dies auch im abelschen Fall gewohnt ist.

2.10 Lemma/ Definition. Es sei $r \in \mathbb{N}_+$ eine positive natürliche Zahl, und es seien $A_1, \ldots, A_r$ diskrete S-Gruppen.

(i) Das direkte Produkt $\prod_{i=1}^r A_i$ ist vermöge

$$^s(a_1, \ldots, a_r) := ({}^s a_1, \ldots, {}^s a_r) \quad \text{für } s \in S$$

eine diskrete S-Gruppe.

(ii) Bezeichnen $p_i : \prod_{j=1}^r A_j \twoheadrightarrow A_i$ für $i \in \{1, \ldots, r\}$ die kanonischen Projektionen, so sind die dadurch induzierten Abbildungen

$$\begin{array}{rcccccl} \iota_0 & := & \prod H^0(p_i) & : & H^0(S, \prod_{i=1}^r A_i) & \longrightarrow & \prod_{i=1}^r H^0(S, A_i) \quad \text{und} \\ \iota_1 & := & \prod H^1_{\mathrm{cont}}(p_i) & : & H^1_{\mathrm{cont}}(S, \prod_{i=1}^r A_i) & \longrightarrow & \prod_{i=1}^r H^1_{\mathrm{cont}}(S, A_i) \end{array}$$

Bijektionen von punktierten Mengen.

(iii) Es sei für jedes $i \in \{1, \ldots, r\}$ eine diskrete S-Gruppe B_i und ein Morphismus $A_i \xrightarrow{\varphi_i} B_i$ gegeben. Dann sind die folgenden beiden Diagramme kommutativ in der Kategorie der punktierten Mengen:

$$\begin{array}{ccc} H^0(S, \prod_{i=1}^r A_i) & \xrightarrow{H^0(\prod \varphi_i)} & H^0(S, \prod_{i=1}^r B_i) \\ \iota_0 \downarrow \wr & = & \wr \downarrow \iota_0 \\ \prod_{i=1}^r H^0(S, A_i) & \xrightarrow[\prod H^0(\varphi_i)]{} & \prod_{i=1}^r H^0(S, B_i) \end{array}$$

und

$$\begin{array}{ccc} H^1_{\mathrm{cont}}(S, \prod_{i=1}^r A_i) & \xrightarrow{H^1_{\mathrm{cont}}(\prod \varphi_i)} & H^1_{\mathrm{cont}}(S, \prod_{i=1}^r B_i) \\ \iota_1 \downarrow \wr & = & \wr \downarrow \iota_1 \\ \prod_{i=1}^r H^1_{\mathrm{cont}}(S, A_i) & \xrightarrow[\prod H^1_{\mathrm{cont}}(\varphi_i)]{} & \prod_{i=1}^r H^1_{\mathrm{cont}}(S, B_i). \end{array}$$

Beweis:

(i)
- *S-Gruppe:* Klar!
- *diskret:* Ist $a := (a_i) \in \prod A_i$ beliebig, so gibt es nach 2.2(i)⇒(iii) offene Untergruppen $U_1, \ldots, U_r$ von S mit $a_i \in A_i^{U_i}$ für $i \in \{1, \ldots, r\}$. Dann ist aber auch $U := \bigcap_{i=1}^r U_i$ eine offene Untergruppe von S, und offenbar gilt $a \in \left(\prod A_i\right)^U$, so daß die Behauptung aus 2.2(iii)⇒(i) folgt.

(ii)
- ι_0 *bijektiv:* Klar, da

$$(a_i)_i \in \left(\prod_{i=1}^r A_i\right)^S \iff \forall s \in S : \underbrace{{}^s(a_1, \ldots, a_r)}_{=({}^s a_1, \ldots, {}^s a_r)} = (a_1, \ldots, a_r)$$
$$\iff \forall s \in S : {}^s a_1 = a_1, \ldots, {}^s a_r = a_r \iff a_1 \in A_1^S, \ldots, a_r \in A_r^S.$$

- ι_1 *bijektiv:* Wir behaupten, daß die Umkehrabbildung zu ι_1 wie folgt gegeben wird:

$$\begin{array}{ccc} \prod_{i=1}^r H^1_{\mathrm{cont}}(S, A_i) & \xrightarrow{\ j\ } & H^1_{\mathrm{cont}}(S, \prod_{i=1}^r A_i) \\ \left((a_s^{(1)})_s, \ldots, (a_s^{(r)})_s\right) & \mapsto & \left(a_s^{(1)}, \ldots, a_s^{(r)}\right)_s \end{array}$$

Dazu überlegen wir zunächst, daß die Bilder unter dieser Abbildung tatsächlich 1-Kozykel sind. Seien $\left((a_s^{(1)})_s, \ldots, (a_s^{(r)})_s\right) \in \prod_{i=1}^r H^1_{\mathrm{cont}}(S, A_i)$ und $s, t \in S$ beliebig. Dann gilt:

$$\left(a_{st}^{(1)}, \ldots, a_{st}^{(r)}\right) = \left(a_s^{(1)} {}^s a_t^{(1)}, \ldots, a_s^{(r)} {}^s a_t^{(r)}\right) = \left(a_s^{(1)}, \ldots, a_s^{(r)}\right) {}^s\left(a_t^{(1)}, \ldots, a_t^{(r)}\right),$$

d.h. die 1-Kozykelbedingung ist erfüllt.

Als nächstes zeigen wir, daß j wohldefiniert ist. Seien $\left((a_s^{(1)})_s, \ldots, (a_s^{(r)})_s\right) \in \prod_{i=1}^r H^1_{\mathrm{cont}}(S, A_i)$ und $b_i \in A_i$ für $i \in \{1, \ldots, r\}$ beliebig vorgegeben. Wir haben zu zeigen, daß dann die beiden 1-Kozykel

$$\left(a_s^{(1)}, \ldots, a_s^{(r)}\right)_s \qquad \text{und} \qquad \left(b_1^{-1} a_s^{(1)} {}^s b_1, \ldots, b_r^{-1} a_s^{(r)} {}^s b_r\right)_s$$

kohomolog sind: Sei $s \in S$ beliebig, dann folgt:

$$\left(b_1^{-1} a_s^{(1)} {}^s b_1, \ldots, b_r^{-1} a_s^{(r)} {}^s b_r\right)_s = (b_1, \ldots, b_r)^{-1} \left(a_s^{(1)}, \ldots, a_s^{(r)}\right)_s {}^s(b_1, \ldots, b_r),$$

und wir sehen, daß j tatsächlich eine wohldefinierte Abbildung punktierter Mengen ist.

Daß ι_1 und j invers zueinander sind, sieht man sofort!

(iii) Klar!

q.e.d.

Im abelschen Fall ist die „lange exakte Kohomologiesequenz“ eines der wichtigsten Hilfsmittel. Wir stellen nun das Analogon im nicht-abelschen Fall vor.

2.11 Lemma/ Definition. Eine *exakte Sequenz von (diskreten) S-Gruppen* ist eine exakte Sequenz von Gruppen, in der alle Morphismen auch Morphismen von (diskreten) S-Gruppen sind. Ist

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

eine kurze exakte Sequenz von diskreten S-Gruppen, so ist $iA \trianglelefteq B$ ein *S-invarianter Normalteiler*, d.h. $\forall s \in S, a \in A : {}^s(ia) \in iA$.

Ist umgekehrt B eine (diskrete) G-Gruppe und $A \trianglelefteq B$ ein S-invarianter Normalteiler, so definiert die Einschränkung der S-Operation von B auf A die Struktur einer (diskreten) S-Gruppe, die auf B/A vermöge ${}^s\bar{b} := \overline{{}^s b}$ definierte S-Operation ist wohldefiniert (und stetig), und die Sequenz

$$1 \longrightarrow A \longrightarrow B \longrightarrow B/A \longrightarrow 1$$

ist eine exakte Sequenz von (diskreten) S-Gruppen.

Beweis:

- *Operation wohldefiniert:* Seien $s \in S$ und $\bar{b} \in B/A$ beliebig. Ist $b' \in B$ ein weiterer Repräsentant von $\bar{b}$, so haben wir $\overline{{}^s b} = \overline{{}^s b'}$ zu zeigen: Wegen $\bar{b} = \overline{b'}$ gibt es ein $a \in A$ mit $b = b'a$, d.h. es gilt

$$\overline{{}^s b} = \overline{{}^s(b'a)} = \overline{{}^s b' {}^s a} = \overline{{}^s b'} \cdot \overline{{}^s a} \overset{{}^s a \in A}{=} \overline{{}^s(b')}.$$

- *Operation stetig:* Sei $\bar{b} \in B/A$ beliebig, und sei $U := \mathrm{Stab}_S(b)$. Weil B eine diskrete S-Gruppe ist, ist U nach 2.2(i)⇒(iii) eine offene Untergruppe von S. Trivialerweise gilt aber dann $\bar{b} \in (B/A)^U$, und die Stetigkeit der Operation folgt aus 2.2(iii)⇒(i).]

q.e.d.

2.12 Satz/ Definition. Es sei

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

eine kurze exakte Sequenz von diskreten S-Gruppen. Wir haben dann folgende wohldefinierte, funktorielle Abbildung punktierter Mengen:

$$\delta : H^0(S, C) \to H^1_{\mathrm{cont}}(S, A), \quad \bar{b} \mapsto (b^{-1} \cdot {}^s b),$$

wobei „funktoriell“ das folgende bedeuten möge: Ist

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \xrightarrow{i} & B & \xrightarrow{p} & C & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 1 & \longrightarrow & A' & \xrightarrow{i'} & B' & \xrightarrow{p'} & C' & \longrightarrow & 1 \end{array}$$

ein kommutatives Diagramm von diskreten S-Gruppen mit exakten Zeilen, so kommutiert das Diagramm

$$\begin{array}{ccc} H^0(S, C) & \xrightarrow{\delta} & H^1_{\mathrm{cont}}(S, A) \\ \downarrow{\scriptstyle H^0(\gamma)} & & \downarrow{\scriptstyle H^1_{\mathrm{cont}}(\alpha)} \\ H^0(S, C') & \xrightarrow{\delta} & H^1_{\mathrm{cont}}(S, A'). \end{array}$$

Die folgende Sequenz ist dann exakt in der Kategorie der punktierten Mengen:

$$H^0(S,A) \overset{H^0(i)}{\hookrightarrow} H^0(S,B) \xrightarrow{H^0(p)} H^0(S,C) \xrightarrow{\delta}$$
$$H^1_{\mathrm{cont}}(S,A) \xrightarrow{H^1_{\mathrm{cont}}(i)} H^1_{\mathrm{cont}}(S,B) \xrightarrow{H^1_{\mathrm{cont}}(p)} H^1_{\mathrm{cont}}(S,C).$$

Beweis:

- δ *wohldefiniert:* Als erstes wollen wir für beliebiges $b \in B$ mit $\bar{b} \in C^S$ und $s \in S$ zeigen, daß $b^{-1} \cdot {}^s b$ tatsächlich in A liegt:

  $$\overline{b^{-1} \cdot {}^s b} = \bar{b}^{-1} \cdot {}^s\bar{b} \overset{\bar{b} \in C^S}{=} \bar{b}^{-1} \cdot \bar{b} = \bar{1} \quad \Longrightarrow \quad b^{-1} \cdot {}^s b \in A.$$

  Als nächstes rechnen wir nach, daß $(b^{-1} \cdot {}^s b)$ die 1-Kozykelbedingung erfüllt; seien dazu $s,t \in S$ beliebig:

  $$b^{-1} \cdot {}^{st} b = b^{-1} \cdot \big({}^s b \cdot {}^s(b^{-1})\big) \cdot {}^s\big({}^t b\big) = \big(b^{-1} \cdot {}^s b\big) \cdot {}^s\big(b^{-1} \cdot {}^t b\big).$$

  Nun beweisen wir, daß $(b^{-1} \cdot {}^s b)$ ein *stetiger* 1-Kozykel ist. Sei dazu $U \subseteq S$ die nach 2.2(i)⇒(ii) offene Untergruppe $\mathrm{Stab}_S(a)$. Dann ist die Nebenklasse sU ebenfalls offen in S, und offenbar ist $(b^{-1} \cdot {}^s b)$ konstant auf dieser offenen Teilmenge, also eine lokalkonstante Abbildung und damit stetig.

  Schließlich zeigen wir, daß die Definition von δ nicht von der Wahl eines Repräsentanten für $\bar{b}$ abhängt. Sei also $b' \in B$ ein weiterer Repräsentant von $\bar{b}$, d.h. $b = b'a$ mit $a \in A$. Dann folgt:

  $$\forall s \in S \ : \ b^{-1} \cdot {}^s b = (b'a)^{-1} \cdot {}^s(b'a) = a^{-1} \cdot \Big(b'^{-1} \cdot {}^s b'\Big) \cdot {}^s a$$
  $$\Longrightarrow \quad (b^{-1} \cdot {}^s b) \sim (b'^{-1} \cdot {}^s b').$$

  Die durch b und b' definierten 1-Kozykel sind also kohomolog und definieren damit dasselbe wohlbestimmte Element in der Kohomologie.

- δ *funktoriell:* Ist $\bar{b} \in C^S$ beliebig, so gilt

  $$\big(\delta \circ H^0(\gamma)\big)(\bar{b}) = \delta(\overline{\beta(b)}) = (\beta(b)^{-1} \cdot {}^s\beta(b)) = (\beta(\underbrace{b^{-1} \cdot {}^s b}_{\in A}))$$
  $$= (\alpha(b^{-1} \cdot {}^s b)) = \big(H^1_{\mathrm{cont}}(\alpha) \circ \delta\big)(\bar{b}).$$

- $H^0(i)$ *injektiv*: Klar!

- *Exaktheit bei* $H^0(S,B)$*:* Klar!

- *Exaktheit bei* $H^0(S,C)$*:* Ist $b \in B^S$ beliebig, so ist

  $$\delta(p(b)) = \delta(\bar{b}) = (b^{-1} \cdot {}^s b) \overset{{}^s b = b}{=} (b^{-1} \cdot b) = (1),$$

  also der triviale 1-Kozykel. Sei umgekehrt $\bar{b} \in C^S$ beliebig und $\delta(\bar{b})$ kohomolog zum trivialen 1-Kozykel von S in A. Es gibt also ein $a \in A$ mit

  $$\forall s \in S \ : \ 1 = a^{-1} \cdot \big(b^{-1} \cdot {}^s b\big) \cdot {}^s a = (ba)^{-1} \cdot {}^s(ba) \quad \Longrightarrow \quad ba \in B^S.$$

  Wegen $\bar{b} = \overline{ba}$ folgt hieraus die Behauptung.

- *Exaktheit bei $H^1_{cont}(S,A)$:* Sei zunächst $\bar{b} \in C^S$ beliebig. Dann ist

$$H^1_{\mathrm{cont}}(i)(\delta(\bar{b})) = (b^{-1} \cdot {}^s b) = (b^{-1} \cdot 1 \cdot {}^s b) \sim (1) \in Z^1_{\mathrm{cont}}(S,B).$$

  Sei nun (a_s) ein stetiger 1-Kozykel von S in A, der als 1-Kozykel in B kohomolog zum trivialen 1-Kozykel wird. Dann gibt es also ein $b \in B$ mit

$$\forall s \in S : \; a_s = b^{-1} \cdot 1 \cdot {}^s b = b^{-1} \cdot {}^s b.$$

  Daraus folgt zunächst

$$\forall s \in S : \; {}^s b = b a_s \in bA \quad \Longrightarrow \quad \bar{b} \in C^S$$

  und dann $(a_s) \sim \delta(\bar{b})$.

- *Exaktheit bei $H^1_{cont}(S,B)$:* Ist $(a_s) \in Z^1_{\mathrm{cont}}(S,A)$ beliebig, so gilt für alle $s \in S$ trivialerweise $\overline{a_s} = \bar{1} \in C$, d.h. (a_s) wird unter $H^1_{\mathrm{cont}}(p) \circ H^1_{\mathrm{cont}}(i)$ auf den trivialen 1-Kozykel abgebildet.

  Sei nun umgekehrt (b_s) ein beliebiger stetiger 1-Kozykel von S in B, der in C kohomolog zum trivialen 1-Kozykel wird. Es gibt dann also ein $\bar{b} \in C$ mit

$$\forall s \in S : \; \overline{b_s} = \bar{b}^{-1} \cdot \bar{1} \cdot {}^s\bar{b} = \bar{b}^{-1} \cdot \overline{{}^s b}. \tag{9}$$

  Betrachte nun den zu (b_s) kohomologen 1-Kozykel $(b'_s) := (b b_s {}^s(b^{-1}))$! Es gilt:

$$\forall s \in S : \; \overline{b'_s} = \overline{b b_s {}^s(b^{-1})} = \bar{b} \cdot \overline{b_s} \cdot \overline{{}^s(b^{-1})} \overset{(9)}{=} \bar{b} \cdot \left(\bar{b}^{-1} \cdot \overline{{}^s b}\right) \cdot \overline{{}^s(b^{-1})} = \bar{1},$$

  woraus folgt, daß die b'_s Elemente aus A sind, d.h. wir können (b'_s) als Element aus $H^1_{\mathrm{cont}}(S,A)$ betrachten, und es gilt $(b_s) = H^1_{\mathrm{cont}}(i)(b'_s)$.

q.e.d.

2.13 Korollar. Es sei

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

ein kurze exakte Sequenz von S-Gruppen. Dann haben wir eine wohldefinierte, funktorielle Abbildung von punktierten Mengen

$$\delta : H^0(S,C) \to H^1(S,A), \;\; \bar{b} \mapsto (b^{-1} \cdot {}^s b),$$

und die folgende Sequenz ist exakt in der Kategorie der punktierten Mengen:

$$H^0(S,A) \overset{H^0(i)}{\hookrightarrow} H^0(S,B) \xrightarrow{H^0(p)} H^0(S,C) \xrightarrow{\delta} H^1(S,A) \xrightarrow{H^1(i)} H^1(S,B) \xrightarrow{H^1(p)} H^1(S,C).$$

Beweis: Folgt sofort aus 2.12, wenn wir S mit der diskreten Topologie versehen. **q.e.d.**

Wie wir schon aus der Einleitung wissen, wird in den folgenden Kapiteln das Kranzprodukt $S_n \int \mu_m$ eine zentrale Rolle spielen. In 2.15 werden wir an die Definition des Kranzproduktes erinnern. Insbesondere ist jedes Kranzprodukt ein semidirektes Produkt, und daher wollen wir nun untersuchen, was man in dem Fall, daß A ein semidirektes Produkt oder spezieller ein Kranzprodukt ist, über die Kohomologien $H^0(S,A)$ und $H^1_{\mathrm{cont}}(S,A)$ sagen kann.

2.14 Korollar. Es sei T eine Gruppe und A sowohl eine T-Gruppe als auch eine diskrete S-Gruppe derart, daß

$$\forall s \in S : \forall t \in T : \forall a \in A : {}^s({}^t a) = {}^t({}^s a). \tag{10}$$

Dann wird das semidirekte Produkt $A \rtimes T$ von T mit A (mit $tat^{-1} = {}^t a$ für $t \in T$ und $a \in A$) via

$$\begin{array}{ccccc} S & \times & A \rtimes T & \longrightarrow & A \rtimes T \\ (s & , & a \cdot t) & \mapsto & {}^s(a \cdot t) := {}^s a \cdot t \end{array}$$

zu einer diskreten S-Gruppe mit der Eigenschaft, daß $A \trianglelefteq A \rtimes T$ ein S-invarianter Normalteiler und die Inklusion $T \hookrightarrow A \rtimes T$ ein Morphismus von diskreten S-Mengen ist, wobei S auf T trivial operiere.

Außerdem erhalten wir die folgenden kurzen exakten Sequenzen in der Kategorie der punktierten Mengen:

$$\begin{array}{ccccccccc} & & H^0(S,A) & \hookrightarrow & H^0(S, A \rtimes T) & \longrightarrow & T & \longrightarrow & * \quad \text{und} \\ * & \longrightarrow & H^1_{\mathrm{cont}}(S,A) & \longrightarrow & H^1_{\mathrm{cont}}(S, A \rtimes T) & \longrightarrow & H^1_{\mathrm{cont}}(S,T) & \longrightarrow & *. \end{array}$$

Beweis:

- $A \rtimes T$ *diskrete S-Gruppe:* Seien $s, s' \in S$ sowie $a, a' \in A$ und $t, t' \in T$ beliebig. Es gilt:

$$\begin{aligned} &{}^s(at \cdot a't') = {}^s(a\,{}^t a' \cdot tt') = {}^s a\,{}^s({}^t a')tt' \overset{(10)}{=} {}^s a\,{}^t({}^s a')tt' = {}^s at\,{}^s a't' = {}^s(at) \cdot {}^s(a't'), \\ &{}^{ss'}(at) = {}^{ss'}a \cdot t = {}^s({}^{s'}a) \cdot t = {}^s({}^{s'}at) = {}^s({}^{s'}(at)) \quad \text{und} \\ &{}^1(at) = {}^1at = at. \end{aligned}$$

  Also ist $A \rtimes T$ eine S-Gruppe. Die S-Operation ist *stetig*, denn für beliebiges $a \cdot t \in A \rtimes T$ gilt:

$$s \in \mathrm{Stab}_S(at) \iff {}^s at = at \iff {}^s a = a \iff s \in \mathrm{Stab}_S(a),$$

  d.h. $\mathrm{Stab}_S(at) = \mathrm{Stab}_S(a)$, und letzteres ist nach 2.2(i)⇒(ii) eine offene Untergruppe von S, da A ja eine *diskrete* S-Gruppe ist — die Behauptung folgt also aus 2.2(ii)⇒(i).

- $A \trianglelefteq A \rtimes T$ *ist S-invarianter Normalteiler:* Klar!

- $T \hookrightarrow A \rtimes T$ *Morphismus von S-Gruppen:* Klar!

- *Sequenzen exakt:* Bezeichne $A \rtimes T \xrightarrow{p} T$ die kanonische Projektion. Nach 2.12 erhalten wir zunächst die folgende lange exakte Sequenz von punktierten Mengen:

$$\begin{aligned} H^0(S,A) \hookrightarrow H^0(S, A \rtimes T) \longrightarrow H^0(S,T) \xrightarrow{\delta} \\ H^1_{\mathrm{cont}}(S,A) \longrightarrow H^1_{\mathrm{cont}}(S, A \rtimes T) \xrightarrow{H^1_{\mathrm{cont}}(p)} H^1_{\mathrm{cont}}(S,T). \end{aligned}$$

  Weil S trivial auf T operiert, haben wir $H^0(S,T) = T$. Wir müssen also nur noch zeigen, daß δ alles auf die Klasse des trivialen 1-Kozykels abbildet und daß $H^1_{\mathrm{cont}}(p)$ surjektiv ist, um die beiden kurzen exakten Sequenzen zu erhalten.

Ist $t \in T$ beliebig, so ist $\delta(t)$ nach Definition gleich der Klasse von $(t^{-1} \cdot {}^s t)_s$, was aber der triviale 1-Kozykel ist, da S auf T trivial operiert.

Die Inklusion $i : T \hookrightarrow A \rtimes T$ ist ein Schnitt von p in der Kategorie der diskreten S-Gruppen. Per Funktoralität ist dann aber auch $H^1_{\mathrm{cont}}(i)$ ein Schnitt von $H^1_{\mathrm{cont}}(p)$, so daß letztere Abbildung also insbesondere surjektiv ist!

q.e.d.

2.15 Definition. Seien $r \in \mathbb{N}_+$ eine positive natürliche Zahl und A eine abelsche Gruppe. Dann ist das *Kranz-Produkt* $S_r \int A$ von der symmetrischen Gruppe S_r mit A definiert als das semidirekte Produkt $A^r \rtimes S_r$ von A^r mit S_r, wobei S_r auf A^r durch Permutation der Komponenten operiert, d.h. für $\sigma \in S_r$ und $(a_i)_i \in A^r$ ist

$$ {}^{\sigma}(a_1, \ldots, a_r) := (a_{\sigma^{-1}(1)}, \ldots, a_{\sigma^{-1}(r)}). $$

Für $a, b \in A^r$ und $\sigma, \tau \in S_r$ gilt dann also

$$ \begin{array}{lcll} (a \cdot \sigma)(b \cdot \tau) & = & (a\,{}^{\sigma}b) \cdot (\sigma\tau) & = & (a_1 b_{\sigma^{-1}(1)}, \ldots, a_r b_{\sigma^{-1}(r)}) \cdot \sigma\tau \text{ und} \\ (a \cdot \sigma)^{-1} & = & {}^{\sigma^{-1}}(a^{-1}) \cdot \sigma^{-1} & = & (a^{-1}_{\sigma(1)}, \ldots, a^{-1}_{\sigma(r)}) \cdot \sigma^{-1}. \end{array} $$

2.16 Lemma/ Definition. Sei $r \in \mathbb{N}_+$ eine positive natürliche Zahl und A eine abelsche, diskrete S-Gruppe (also ein diskreter S-Modul). Dann wird durch

$$ {}^s\big((x_i)_i \cdot \sigma\big) := ({}^s x_i)_i \cdot \sigma \qquad (\text{für } s \in G,\ x_1, \ldots, x_r \in A \text{ und } \sigma \in S_r \text{ beliebig}) $$

auf dem Kranz-Produkt $S_r \int A$ eine stetige Links-G-Operation definiert, d.h. $S_r \int A$ trägt die Struktur einer diskreten G-Menge.
Der Normalteiler $A^r \trianglelefteq S_r \int A$ ist invariant unter dieser Operation von G auf $S_r \int A$.

Beweis:

- *stetige Links-G-Operation:* G operiert stetig auf A und damit auch stetig auf A^r. Ist $(x_i)_i \in A^r$, $s \in G$ und $\sigma \in S_r$, so gilt

  $$ {}^s({}^{\sigma}(x_i)_i) = {}^s(x_{\sigma^{-1}(i)})_i = ({}^s x_{\sigma^{-1}(i)})_i = {}^{\sigma}({}^s(x_i)_i), $$

  d.h. Gleichung (10) aus 2.14 ist erfüllt; nach 2.14 erhalten wir also eine stetige G-Operation auf $S_r \int A = (A^r) \rtimes S_r$, die gerade die hier betrachtete ist.

- *Normalteiler invariant:* Klar nach 2.14!

q.e.d.

2.17 Korollar. Es sei wieder $r \in \mathbb{N}_+$ eine positive natürliche Zahl und A ein diskreter S-Modul. Seien $A^r \xrightarrow{i} S_r \int A$ und $S_r \int A \xrightarrow{p} S_r$ die kanonische Einbettung bzw. Projektion. Dann ist die folgende Sequenz punktierter Mengen exakt (und δ ist die triviale Abbildung), wobei die Surjektion $H^1_{\text{cont}}(p)$ einen kanonischen Schnitt besitzt:

$$* \longrightarrow H^0(G, A^r) \xrightarrow{H^0(i)} H^0(G, S_r \int A) \xrightarrow{H^0(p)} H^0(G, S_r) \xrightarrow{\delta}$$
$$H^1_{\text{cont}}(G, A^r) \xrightarrow{H^1_{\text{cont}}(i)} H^1_{\text{cont}}(G, S_r \int A) \xrightarrow{H^1_{\text{cont}}(p)} H^1_{\text{cont}}(G, S_r) \longrightarrow *.$$

Beweis: Folgt sofort aus 2.16 und 2.14. **q.e.d.**

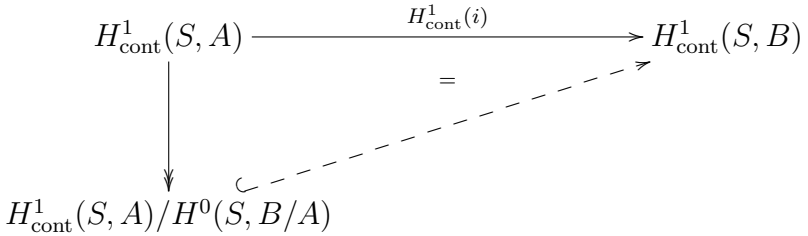
Ist $0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0$ eine kurze exakte Sequenz *abelscher* S-Gruppen, so folgt aus der langen exakten Kohomologiesequenz, daß die Faser $\left[H^1_{\text{cont}}(p)\right]^{-1}(\{c\})$ für eine Klasse $c \in H^1_{\text{cont}}(S, C)$ entweder leer oder gleich $b + \text{Ker}\,(H^1_{\text{cont}}(p)) = b + H^1_{\text{cont}}(S, A)/H^0(S, C)$ für ein beliebiges Element b aus der Faser ist.

Ist B keine abelschen Gruppe und damit $H^1_{\text{cont}}(S, B)$ nur eine punktierte Mengen, so stimmt dies im allgemeinen nicht mehr. Die Kenntnis des Kerns von $H^1_{\text{cont}}(p)$ reicht dann nicht mehr aus, um die (nicht-leeren) Fasern berechnen zu können. Im Folgenden wollen wir zeigen, wie man diese Schwierigkeit umgehen kann, indem man durch Übergang zu einer „getwisteten“ Operation von S auf B erreicht, daß die fragliche Faser zum Kern wird.

2.18 Lemma/ Definition. Es sei B eine diskrete S-Gruppe und $A \subseteq B$ ein S-invarianter Normalteiler. Dann wird durch

$$\begin{array}{ccccc} H^1_{\text{cont}}(S, A) & \times & H^0(S, B/A) & \longrightarrow & H^1_{\text{cont}}(S, A) \\ \big((a_s) & , & \bar{b}\big) & \mapsto & (a_s)^{\bar{b}} := (b^{-1} a_s {}^s b) \end{array}$$

eine Rechts-Operation von $H^0(S, B/A)$ auf $H^1_{\text{cont}}(S, A)$ definiert.
Zwei Kohomologieklassen $[a], [a'] \in H^1_{\text{cont}}(S, A)$ liegen genau dann im selben $H^0(S, B/A)$-Orbit, wenn $[a]$ und $[a']$ unter $H^1_{\text{cont}}(i)$ dasselbe Bild in $H^1_{\text{cont}}(S, B)$ haben, wobei $i : A \hookrightarrow B$ die Einbettung bezeichne:



Beweis:

- *wohldefiniert:* Sei $(a_s) \in Z^1_{\text{cont}}(S, A)$ beliebig, und sei $b \in B$ mit $\bar{b} \in (B/A)^S$. Zunächst müssen wir sehen, daß $b^{-1} a_s {}^s b$ für alle $s \in S$ tatsächlich in A liegt: Wegen $\bar{b} \in (B/A)^S$ gibt es ein $x_s \in A$ mit ${}^s b = b x_s$. Es ist also $b^{-1} a_s {}^s b = (b^{-1} a_s b) \cdot x_s \in A$, weil $x_s \in A$ und $b^{-1} a_s b \in A$; letzteres, da A Normalteiler in B ist.

Als nächstes wollen wir prüfen, ob $(b^{-1}a_s{}^s b)$ die 1-Kozykelbedingung erfüllt! Seien dazu $s,t \in S$ beliebig:

$$b^{-1}a_{st}{}^{st}b = b^{-1}\cdot a_s{}^s a_t \cdot {}^{st}b = b^{-1}a_s \cdot {}^s b({}^s b)^{-1}\cdot {}^s a_t{}^{st}b = (b^{-1}a_s{}^s b)\cdot {}^s(b^{-1}a_t{}^t b).$$

Um zu beweisen, daß der 1-Kozykel $b^{-1}a_s{}^s b$ *stetig* ist, wählen wir zunächst gemäß 2.2(i)⇒(iii) eine offene Untergruppe V von S mit $b \in V^S$. Ist nun $s \in S$ beliebig, so gibt es wegen der Stetigkeit von (a_s) eine offene Umgebung $V_s \subseteq S$ von s, auf der (a_s) konstant ist. Dann ist auch $U_s := V_s \cap (Vs) \subseteq S$ eine offene Umgebung von s in S, und offenbar ist $(b^{-1}a_s{}^s b)$ auf U_s konstant.

Um den Beweis der Wohldefiniertheit zu vollenden, müssen wir noch die Unabhängigkeit von den getroffenen Wahlen zeigen. Sei $b' \in B$ ein Element mit $\bar{b} = \bar{b'} \in B/A$. Es gibt dann ein $\alpha \in A$ mit $b' = b\alpha$, und es folgt (für $s \in S$ beliebig):

$$b'^{-1}a_s{}^s b' = (b\alpha)^{-1}a_s{}^s b\alpha = \alpha^{-1}\cdot(ba_s{}^s b)\cdot {}^s\alpha,$$

d.h. die beiden 1-Kozykel $(b'^{-1}a_s{}^s b')$ und $(b^{-1}a_s{}^s b)$ sind kohomolog.

Sei schließlich $(a'_s) \in Z^1_{\mathrm{cont}}(S,A)$ ein zu (a_s) kohomologer 1-Kozykel. Es gibt also ein $\alpha \in A$ mit $a'_s = \alpha^{-1}a_s{}^s\alpha$ für alle $s \in S$. Für $s \in S$ beliebig ergibt sich also:

$$b^{-1}a'_s{}^s b = b^{-1}\cdot(\alpha^{-1}a_s{}^s\alpha)\cdot {}^s b = (\alpha b)^{-1}\cdot a_s \cdot {}^s(\alpha b).$$

Weil A ein Normalteiler in B ist, gibt es ein $\alpha' \in A$ mit $\alpha b = b\alpha'$, d.h. $(b^{-1}a'_s{}^s b) = ((b\alpha')^{-1}a_s{}^s(b\alpha'))$, und daß dieser 1-Kozykel kohomolog zu $(b^{-1}a_s{}^s b)$ ist, haben wir oben schon gesehen. Die Wohldefiniertheit ist damit vollständig bewiesen!

- *Operation:* Seien $\bar{b},\bar{c} \in (B/A)^S$ und $(a_s) \in H^1_{\mathrm{cont}}(S,A)$ beliebig. Wir rechnen nach:

$$\begin{aligned}(a_s)^{\bar{1}} &= (1^{-1}\cdot a_s\cdot {}^s 1) = (1\cdot a_s\cdot 1) = (a_s),\\ (a_s)^{\bar{b}\cdot\bar{c}} &= (a_s)^{\overline{bc}} = \big((bc)^{-1}a_s{}^s(bc)\big) = \big(c^{-1}\cdot(b^{-1}a_s{}^s b)\cdot {}^s c\big) = \big((a_s)^b\big)^c.\end{aligned}$$

- *Orbit:* Die Klassen $[a]$ und $[a']$ mögen durch stetige 1-Kozykel $a = (a_s)$ und $a' = (a'_s)$ repräsentiert werden. Gelte zunächst, daß $[a]$ und $[a']$ im selben Orbit liegen! Es gibt also ein $\bar{b} \in B/A$, repräsentiert durch $b \in B$, mit $[a'] = [a]^{\bar{b}}$, d.h. es gibt ein $\alpha \in A$ mit

$$\forall s \in S : a'_s = \alpha^{-1}\cdot(b^{-1}a_s{}^s b)\cdot {}^s\alpha = (b\alpha)^{-1}\cdot a_s\cdot {}^s(b\alpha).$$

Aufgefaßt als 1-Kozykel in B sind a und a' folglich kohomolog.

Gelte umgekehrt $H^1_{\mathrm{cont}}(i)[a] = H^1_{\mathrm{cont}}(i)[a']$, d.h. die 1-Kozykel a und a' seien kohomolog in $Z^1_{\mathrm{cont}}(S,B)$. Dann gibt es ein $b \in B$ mit

$$\forall s \in S : a'_s = b^{-1}a_s{}^s b,$$

woraus zunächst

$$\forall s \in S : {}^s b = a_s^{-1}ba'_s \quad\Longrightarrow\quad \forall s \in S : {}^s\bar{b} = \bar{b} \quad\Longrightarrow\quad \bar{b} \in H^0(S, B/A)$$

und dann sofort $[a'] = [a]^{\bar{b}}$ folgt. Also liegen $[a']$ und $[a]$ wirklich im selben Orbit.

q.e.d.

2.19 Korollar. Es seien B eine diskrete S-Gruppe und $A \subseteq B$ ein S-invarianter Normalteiler, und bezeichne $i : A \hookrightarrow B$ die Einbettung und $p : B \twoheadrightarrow B/A$ die Projektion. Dann induziert $H^1_{\text{cont}}(i)$ eine Bijektion

$$H^1_{\text{cont}}(S, B)/H^0(S, B/A) \xrightarrow{\sim} \text{Ker}\left(H^1_{\text{cont}}(S, B) \xrightarrow{H^1_{\text{cont}}(p)} H^1_{\text{cont}}(S, B/A)\right).$$

Beweis: Folgt sofort aus 2.12 und 2.18! **q.e.d.**

2.20 Lemma. Sei A eine Gruppe, und man mache A durch die triviale S-Operation zu einer diskreten S-Gruppe. Dann ist ein (stetiger) 1-Kozykel von S in A einfach ein (stetiger) Gruppenhomomorphismus von S nach A, und zwei solche sind genau dann kohomolog, wenn sie konjugiert sind.

Beweis: Ist (a_s) ein 1-Kozykel, so wird die 1-Kozykelbedingung wegen der Trivialität der Operation zu $a_{st} = a_s {}^s a_t = a_s a_t$, aber das ist gerade die Homomorphiebedingung für einen Gruppenhomomorphismus. Zwei 1-Kozykel (a_s) und (a'_s) sind genau dann kohomolog, wenn es ein $b \in A$ gibt mit $a'_s = b^{-1} a_s {}^s b = b^{-1} a_s b$, d.h. genau wenn sie konjugiert sind. **q.e.d.**

2.21 Korollar. Sei $n \in \mathbb{N}^+$ eine natürliche Zahl, und S operiere trivial auf der symmetrischen Gruppe S_n. Bezeichnet M eine beliebige n-elementige Menge, so gilt

$$H^1_{\text{cont}}(S, S_n) = \{\varphi : S \times M \to M \,|\, \varphi \text{ stetige Links-}S\text{-Operation auf } M\}/\text{Isomorphie.} \quad (11)$$

Ist speziell k ein Körper mit fixiertem separablen algebraischen Abschluß K und $G_k = \text{Gal}\,(K/k)$ die absolute Galoisgruppe von k, versehen mit der Krull-Topologie, so gilt

$$H^1_{\text{cont}}(G_k, S_n) = \{L \,|\, L \text{ endliche, kommutative, separable } k\text{-Algebra vom Grad } n\}/\text{Isomorphie.}$$

Ist L eine solche endliche, separable k-Algebra, so ist $M := \text{Hom}_{k\text{-Alg}}(L, K)$ eine n-elementige Menge, und die zu L korrespondierende Kohomologieklasse wird vermöge (11) durch die offensichtliche Operation

$$\begin{array}{ccccc} G_k & \times & M & \longrightarrow & M \\ (s & , & \varphi) & \mapsto & s \circ \varphi \end{array}$$

von G_k auf M gegeben.

Beweis: Nach 2.20 gilt

$$Z^1_{\text{cont}}(S, S_n) = \text{Hom}_{\text{cont}}(S, S_n) = \text{Hom}_{\text{cont}}(S, \text{Aut}\,(M)),$$

d.h. die stetigen 1-Kozykel von S in S_n entsprechen genau den stetigen Links-S-Operationen auf M. Offenbar sind zwei solche Operationen genau dann isomorph, wenn die zugehörigen Homomorphismen $S \to S_n$ konjugiert sind, was nach 2.20 genau bedeutet, daß sie als 1-Kozykel kohomolog sind — dies beweist (11).

Die 1-1-Korrespondenz zwischen stetigen G_k-Operationen auf einer n-elementigen Menge und endlichen, kommutativen, separablen k-Algebren vom Grad n ist wohlbekannt und wird zum Beispiel in [Tam94, II.2.1, S.93] bewiesen. **q.e.d.**

2.22 Lemma. Sei A eine S-Gruppe und $(a_s) \in Z^1(S, A)$ ein 1-Kozykel. Dann gilt $a_1 = 1$.

Beweis: $$a_1 = a_{1\cdot 1} = a_1 {}^1a_1 = a_1 a_1 \quad \Rightarrow \quad a_1 = 1.$$

q.e.d.

2.23 Lemma/ Definition. Sei A eine diskrete S-Gruppe und F eine diskrete S-Menge, auf der A von links derart operiert, daß

$$\forall s \in S \ \ \forall a \in A \ \ \forall f \in F \ : \ {}^s({}^af) = {}^{({}^sa)}({}^sf).$$

Eine derartige A-Operation nennen wir *verträglich*.

Ist $a := (a_s) \in Z^1_{\text{cont}}(S, A)$ ein stetiger 1-Kozykel, so wird durch

$${}^{s\prime}f := {}^{a_s}({}^sf) \tag{12}$$

eine neue, stetige Links-S-Operation auf F definiert, die sogenannte *mit a getwistete Operation*. Die mit dieser Operation versehene diskrete S-Menge nennen wir F_a.

Ist F sogar eine diskrete *S-Gruppe*, und operiert A verträglich mittels *Gruppenhomomorphismen* auf F, so ist auch F_a eine diskrete S-Gruppe.

Beweis:

- *Operation:* Ist $f \in F$ beliebig, so gilt zunächst
$${}^{1\prime}f = {}^{a_1}({}^{1_S}f) \overset{2.22}{=} {}^{1_A}({}^{1_S}f) = f.$$
Seien nun noch $s, t \in S$ beliebig. Dann ergibt sich:
$${}^{st\prime}f = {}^{a_{st}}({}^{st}f) = {}^{({}^sa_t)}({}^{st}f) = {}^{a_s}\big({}^{({}^sa_t)}{}^{st}f\big) \overset{\text{verträglich}}{=} {}^{a_s}\big({}^s\underbrace{\big[{}^{a_t}({}^tf)\big]}_{={}^{t\prime}f}\big) = {}^{s\prime}\big({}^{t\prime}f\big).$$

- *stetig:* Sei $f \in F$ beliebig. Da F eine diskrete S-Menge ist, gibt es nach 2.2(i)⇒(iii) eine offene Untergruppe $U_1 \subseteq S$ von S, die f fix läßt. Andererseits ist a nach Voraussetzung stetig und demnach lokalkonstant, d.h. wegen 2.22 gibt es eine offene Untergruppe $U_2 \subseteq S$ von S mit $a|U_2 = 1_A$. Dann ist $U := U_1 \cap U_2$ ebenfalls eine offene Untergruppe von S, und offenbar ist f fix unter der neuen Operation von U, so daß die Behauptung aus 2.2(iii)⇒(i) folgt.

- *S-Gruppe* Sei jetzt F eine S-Gruppe, und A operiere mittels Gruppenhomomorphismen auf F. Seien $s \in S$ und $f, g \in F$ beliebig. Dann rechnen wir nach:
$$^{s\prime}(f \cdot g) = {}^{a_s}\big({}^s(f \cdot g)\big) = {}^{a_s}({}^s f \cdot {}^s g) = {}^{a_s}({}^s f) \cdot {}^{a_s}({}^s g) = {}^{s\prime}f \cdot {}^{s\prime}g.$$
Also ist F_c wirklich eine S-Gruppe.

q.e.d.

2.24 Lemma/ Definition. Sei B eine diskrete S-Gruppe und $A \subseteq B$ ein S-invarianter Normalteiler. Dann ist die Operation von B auf A mittels innerer Automorphismen mit der S-Operation verträglich, und wir wollen uns in Zukunft S-invariante Normalteiler immer als mit dieser Operation versehen denken.

Sei $b = (b_s) \in Z^1_{\mathrm{cont}}(S, B)$ ein stetiger 1-Kozykel, dann wird die getwistete S-Operation auf A_b explizit durch
$$^{s\prime}a = b_s \cdot {}^s a \cdot b_s^{-1} \tag{13}$$
gegeben.

(Liegt A sogar im *Zentrum* von B, so zeigt (13) sofort, daß die neue Operation gleich der alten ist, d.h. $A = A_b$.)

Insbesondere ist B selbst ein solcher S-invarianter Normalteiler, d.h. auch B_b ist definiert und mit der in (13) beschriebenen stetigen S-Operation versehen, und offenbar ist die S-Operation auf A_b gerade die Einschränkung der S-Operation auf B_b; mit anderen Worten: Die Einbettung $A_b \hookrightarrow B_b$ ist wieder ein Morphismus von diskreten S-Gruppen.

Beweis: Seien $s \in S$, $a \in A$ und $b \in B$ beliebig. Dann wird die Verträglichkeit durch folgende Rechnung bewiesen:
$${}^s({}^b a) = {}^s(bab^{-1}) = {}^s b\, {}^s a\, \underbrace{{}^s(b^{-1})}_{=({}^s b)^{-1}} = {}^{({}^s b)}({}^s a).$$
Gleichung (13) entsteht durch einfaches Einsetzen in die Definition (12). **q.e.d.**

2.25 Lemma. Wie in 2.14 sei T eine Gruppe und A sowohl eine T-Gruppe als auch eine diskrete S-Gruppe derart, daß (10) erfüllt ist. Wir fordern hier aber zusätzlich, daß A *abelsch* ist. Weiter sei $b \in Z^1_{\mathrm{cont}}(S, A \rtimes T)$ ein stetiger 1-Kozykel. Dann hängt der Twist A_b nur vom Bild von b in $Z^1_{\mathrm{cont}}(S, T)$ ab, das heißt genauer: Bezeichnet $p : A \rtimes T \twoheadrightarrow T$ die kanonische Projektion, $j : T \hookrightarrow A \rtimes T$ den kanonischen Schnitt von p und t den stetigen 1-Kozykel jpb, so sind die diskreten S-Gruppen A_b und A_t gleich.

Beweis: Seien also $s \in S$ und $a \in A$ beliebig, und sei $b = (a_s \cdot t_s)$ mit $a_s \in A$ und $t_s \in T$. Dann ist $t = (t_s)$, und es ergibt sich:
$$\begin{aligned} b_s \cdot {}^s a \cdot b_s^{-1} &= (a_s \cdot t_s) \cdot {}^s a \cdot (a_s \cdot t_s)^{-1} = (a_s \cdot t_s) \cdot {}^s a \cdot ({}^{t_s^{-1}}(a_s^{-1}) \cdot t_s^{-1}) \\ &= \Big[a_s \cdot {}^{t_s}({}^s a) \cdot {}^{t_s \cdot t_s^{-1}}(a_s^{-1})\Big] \cdot \big[t_s \cdot t_s^{-1}\big] = \big[a_s \cdot {}^{t_s}({}^s a) \cdot (a_s^{-1})\big] \overset{\text{abelsch}}{=} {}^{t_s}({}^s a) = t_s \cdot {}^s a \cdot t_s^{-1}. \end{aligned}$$

q.e.d.

2.26 Lemma/ Definition. Es sei $B \xrightarrow{\varphi} C$ ein Morphismus von diskreten S-Gruppen und $b = (b_s) \in Z^1_{\text{cont}}(S, B)$ ein stetiger 1-Kozykel. Dann ist $\varphi \circ b$ ein stetiger 1-Kozykel von S in C, d.h. $C_{\varphi \circ b}$ ist definiert. Wir wollen $C_{\varphi \circ b}$ einfach mit C_b bezeichnen, wenn klar ist, welches φ gemeint ist.
Dann ist φ auch ein Morphismus zwischen den diskreten S-Gruppen B_b und C_b.

Beweis: Wir haben nur zu zeigen, daß $B_b \xrightarrow{\varphi} C_b$ eine S-äquivariante Abbildung ist. Seien dazu $s \in S$ und $b \in B$ beliebig:

$$\varphi({}^{s'}b) \overset{(13)}{=} \varphi(b_s {}^{s}b b_s^{-1}) = \varphi(b_s) \cdot \varphi({}^{s}b) \cdot \varphi(b_s^{-1}) = (\varphi \circ b)_s {}^{s}\varphi(b)(\varphi \circ b)_s^{-1} = {}^{s'}\varphi(b).$$

q.e.d.

2.27 Korollar. Es sei

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

eine kurze exakte Sequenz von diskreten S-Mengen und $b = (b_s) \in Z^1_{\text{cont}}(S, B)$ ein stetiger 1-Kozykel. Dann ist die folgende Sequenz exakt in der Kategorie der punktierten Mengen:

$$H^0(S, A_b) \overset{H^0(i)}{\hookrightarrow} H^0(S, B_b) \xrightarrow{H^0(p)} H^0(S, C_b) \xrightarrow{\delta} H^1_{\text{cont}}(S, A_b) \xrightarrow{H^1_{\text{cont}}(i)} H^1_{\text{cont}}(S, B_b) \xrightarrow{H^1_{\text{cont}}(p)} H^1_{\text{cont}}(S, C_b).$$

Beweis: Nach 2.24 und 2.26 sind $A_b \xrightarrow{i} B_b$ bzw. $B_b \xrightarrow{p} C_b$ ebenfalls S-Morphismen, d.h. wir haben die kurze exakte Sequenz

$$1 \longrightarrow A_b \xrightarrow{i} B_b \xrightarrow{p} C_b \longrightarrow 1,$$

und die Behauptung folgt aus 2.12. **q.e.d.**

2.28 Lemma. Wie in 2.14 sei T eine Gruppe und A sowohl eine T-Gruppe als auch eine diskrete S-Gruppe derart, daß (10) erfüllt ist. Bezeichne $j : T \hookrightarrow A \rtimes T$ den kanonischen Schnitt, und sei $c \in H^1_{\text{cont}}(S, T)$ ein stetiger 1-Kozykel, den wir via j auch als Element von $H^1_{\text{cont}}(S, A \rtimes T)$ auffassen wollen. Dann haben wir einen kanonischen Isomorphismus

$$H^0(S, (A \rtimes T)_c) \cong H^0(S, A_c) \rtimes H^0(S, T_c).$$

Beweis: Nach 2.27 erhalten wir zunächst die kanonische exakte Sequenz

$$1 \longrightarrow H^0(S, A_c) \longrightarrow H^0(S, (A \rtimes T)_c) \xrightarrow{p} H^0(S, T_c).$$

Ist $t \in H^0(S, T_c)$ beliebig, so liegt jt offenbar in $H^0(S, (A \rtimes T)_c)$. Also definiert die Einschränkung von j auf $H^0(S, T_c)$ einen wohldefinierten Schnitt von p, und aus der Existenz eines Schnittes folgt die Behauptung. **q.e.d.**

2.29 Lemma/ Definition. Es sei wie in 2.21 k ein Körper mit fixiertem separablen algebraischen Abschluß K und absoluter Galoisgruppe G, ferner $n \in \mathbb{N}_+$ eine positive natürliche Zahl und A ein diskreter G-Modul.

Betrachte einen beliebigen 1-Kozykel $c \in Z^1_{\mathrm{cont}}(G, S_n)$, und bezeichne auch sein Bild in $Z^1_{\mathrm{cont}}(G, S_n \int A)$ unter dem durch $S_n \hookrightarrow S_n \int A$ induzierten kanonischen Schnitt der Surjektion $Z^1_{\mathrm{cont}}(G, S_n \int A) \twoheadrightarrow Z^1_{\mathrm{cont}}(G, S_n)$ mit c!

Gemäß 2.27 sind dann die getwisteten diskreten G-Gruppen $A^n_c := (A^n)_c$, $(S_n \int A)_c$ und $(S_n)_c$ definiert, und wir erhalten eine exakte Sequenz von punktierten Mengen

$$H^0(G, A^n_c) \hookrightarrow H^0(G, (S_n \int A)_c) \longrightarrow H^0(G, (S_n)_c) \xrightarrow{\delta} H^1_{\mathrm{cont}}(G, A^n_c) \longrightarrow H^1_{\mathrm{cont}}(G, (S_n \int A)_c) \longrightarrow H^1_{\mathrm{cont}}(G, (S_n)_c).$$

Gemäß 2.21 wird c durch eine endliche, kommutative, separable k-Algebra L vom Grad n gegeben, d.h. $L \cong \prod_{i=1}^r L_i$, wobei r eine natürliche Zahl und die $L_i \subseteq K$ separable Körpererweiterungen von k sind mit $\sum_{i=1}^r [L_i : k] = n$.

Wie in 2.21 bezeichne M die n-elementige Menge $\mathrm{Hom}_{k\text{-Alg}}(L, K)$. Wir wollen einen Isomorphismus $\{1, 2, \ldots, n\} \xrightarrow{\sim} M$ fixieren und die Gruppe S_n mit dessen Hilfe mit der Gruppe $\mathrm{Aut}\,(M)$ identifizieren. Elemente aus A^n_c können wir dann als Tupel $(x_\varphi)_{\varphi \in M}$ (mit $x_\varphi \in A$) schreiben, entsprechend Elemente aus $(S_n \int A)_c$ in der Form $(x_\varphi)_{\varphi \in M} \cdot \sigma$ mit $x_\varphi \in A$ und $\sigma \in \mathrm{Aut}\,(M)$. Vermöge dieser Identifizierungen wird die getwistete Operation von G auf A^n_c und $(S_n)_c$ wie folgt gegeben:

$$\begin{array}{lllllll} G & \times & A^n_c & \longrightarrow & A^n_c, & \big(s, (x_\varphi)_{\varphi \in M}\big) & \mapsto & ({}^s x_{s^{-1} \circ \varphi})_{\varphi \in M} \\ G & \times & (S_n)_c & \longrightarrow & (S_n)_c, & (s, \sigma) & \mapsto & \big[\varphi \mapsto s \circ \sigma(s^{-1} \circ \varphi)\big]. \end{array}$$

In Zukunft wollen wir diese Identifizierungen stets vornehmen!

Beweis: Klar nach 2.21, (13) und 2.15! **q.e.d.**

2.30 Lemma. Wie in 2.21 und 2.29 sei k ein Körper mit fixiertem separablen algebraischen Abschluß K und G die absolute Galoisgruppe, ferner seien $n, r \in \mathbb{N}_+$ und $n_1, \ldots, n_r \in \mathbb{N}_+$ positive natürliche Zahlen mit $\sum_{i=1}^r n_i = n$ und $L_1, \ldots, L_r \subseteq K$ separable Körpererweiterungen von k mit $[L_i : k] = n_i$. Bezeichne $L := \prod_{i=1}^r L_i$ das Produkt, das offenbar eine separable k-Algebra vom Grad n ist. Gemäß 2.21 definieren die L_i 1-Kozykel $c_i \in Z^1_{\mathrm{cont}}(G, S_{n_i})$, und L definiert einen 1-Kozykel c in $Z^1_{\mathrm{cont}}(G, S_n)$.

Sei nun A ein diskreter G-Modul. Wir erhalten dann die in 2.29 definierten diskreten G-Gruppen $A^{n_i}_{c_i}$ und A^n_c. Setze $M_i := \mathrm{Hom}_k(L_i, K)$ und $M := \mathrm{Hom}_k(L, K)$, dann induzieren die Abbildungen

$$M_i \longrightarrow M, \quad \varphi \mapsto \varphi \circ p_i$$

eine Bijektion $\coprod_{i=1}^r M_i \xrightarrow{\sim} M$ und damit einen kanonischen Gruppenisomorphismus

$$\begin{array}{lll} A^n_c & \xrightarrow{\sim} & \displaystyle\prod_{i=1}^r A^{n_i}_{c_i} \\ (x_\varphi)_{\varphi \in M} & \mapsto & \big[(x_{\varphi \circ p_i})_{\varphi \in M_i}\big]_{i=1,\ldots,r}. \end{array}$$

Dieser Gruppenisomorphismus ist sogar ein Isomorphismus von diskreten G-Gruppen.

Beweis: Wir haben offenbar nur zu zeigen, daß der im Lemma definierte Gruppenisomorphismus $A_c^n \xrightarrow{\sim} \prod_{i=1}^r A_{c_i}^{n_i}$ ein Morphismus von (diskreten) G-Gruppen ist. Hierzu wiederum genügt es zu sehen, daß für jedes i die Abbildung $A_c^n \twoheadrightarrow A_{c_i}^{n_i}$, die wir hier mit ψ_i bezeichnen wollen, ein G-äuivarianter Morphismus ist.

Seien also $i \in \{1, \ldots, r\}$, $s \in G$ und $(x_\varphi)_{\varphi \in M} \in A_c^n$ beliebig. Dann folgt:

$$\psi_i\,[{}^s(x_\varphi)_{\varphi\in M}] = \psi_i\,[({}^s x_{s^{-1}\varphi})_{\varphi\in M}] = ({}^s x_{s^{-1}\varphi p_i})_{\varphi\in M_i} = {}^s[(x_{\varphi p_i})_{\varphi\in M_i}] = {}^s(\psi_i\,[(x_\varphi)_{\varphi\in M}]).$$

q.e.d.

2.31 Lemma/ Definition. Es sei B eine diskrete S-Gruppe, und es sei $b = (b_s) \in Z^1_{\mathrm{cont}}(S, B)$ ein stetiger 1-Kozykel. Dann ist die Abbildung

$$\begin{array}{rccc} t_b: & Z^1_{\mathrm{cont}}(S, B_b) & \longrightarrow & Z^1_{\mathrm{cont}}(S, B) \\ & (a_s) & \mapsto & (a_s \cdot b_s) \end{array}$$

eine wohldefinierte Bijektion, die durch Übergang zu den Quotienten eine Bijektion

$$\tau_b : H^1_{\mathrm{cont}}(S, B_b) \xrightarrow{\sim} H^1_{\mathrm{cont}}(S, B)$$

induziert. Unter τ_b wird die triviale Klasse auf die Klasse von b abgebildet.

Beweis:

- *wohldefiniert:* Sei $a = (a_s) \in Z^1_{\mathrm{cont}}(S, B_b)$ beliebig. Wir müssen zeigen, daß $t_b(a)$ die 1-Kozykelbedingung erfüllt, seien also $s, t \in S$ beliebig. Es ergibt sich:

$$\begin{aligned}[t_b(a)]_{st} = a_{st}b_{st} = a_s{}^{s\prime}a_t b_s{}^s b_t &\overset{(13)}{=} a_s b_s{}^s a_t b_s^{-1} b_s{}^s b_t \\ &= a_s b_s{}^s a_t{}^s b_t = a_s b_s{}^s(a_t b_t) = [t_b(a)]_s{}^s[t_b(a)]_t.\end{aligned}$$

  Die Stetigkeit von $t_b(a)$ folgt sofort aus der Stetigkeit von a und b.

- *bijektiv:* Offenbar kommt nur

$$\begin{array}{rccc} s_b: & Z^1_{\mathrm{cont}}(S, B) & \longrightarrow & Z^1_{\mathrm{cont}}(S, B_b) \\ & (a_s) & \mapsto & (a_s \cdot b_s^{-1}) \end{array}$$

  als Umkehrabbildung in Frage, und es ist nur zu zeigen, daß s_b wohldefiniert ist, d.h. wir müssen wieder die 1-Kozykelbedingung nachrechnen. Seien also $s, t \in S$ und $a = (a_s) \in Z^1_{\mathrm{cont}}(S, B)$ beliebig, und wir erhalten:

$$\begin{aligned}[s_b(a)]_{st} = a_{st}b_{st}^{-1} = a_s{}^s a_t(b_s{}^s b_t)^{-1} = a_s(b_s^{-1}b_s)^s a_t({}^s b_t)^{-1}b_s^{-1} \\ = a_s b_s^{-1} b_s{}^s a_t{}^s(b_t^{-1})b_s^{-1} &\overset{(13)}{=} a_s b_s^{-1\,s\prime}(a_t b_t^{-1}) = [s_b(a)]_s{}^{s\prime}[s_b(a)]_t.\end{aligned}$$

  Daß $s_b(a)$ stetig ist, folgt wieder sofort aus der Stetigkeit von a und b.

- *Quotientenbildung:* Wir müssen zeigen, daß t_b und s_b kohomologe 1-Kozykel wieder auf kohomologe 1-Kozykel abbilden. Seien zunächst $a = (a_s)$ und $\tilde{a} = (\tilde{a}_s)$ kohomologe 1-Kozykel aus $Z^1_{\mathrm{cont}}(S, B_b)$. Es gibt also ein $\beta \in B$ mit

$$\forall s \in S\,:\, \tilde{a}_s = \beta^{-1}a_s{}^{s\prime}\beta \overset{(13)}{=} \beta^{-1}a_s b_s{}^s \beta b_s^{-1}.$$

Es folgt:

$$[t_b(\tilde{a})]_s = \beta^{-1} a_s b_s {}^s\beta b_s^{-1} \cdot b_s = \beta^{-1} \cdot a_s b_s \cdot {}^s\beta = \beta^{-1} \cdot [t_b(a)]_s \cdot {}^s\beta,$$

d.h. $t_b(a)$ und $t_b(\tilde{a})$ sind wirklich kohomolog. Seien umgekehrt $a = (a_s)$ und $\tilde{a} = (\tilde{a}_s)$ kohomologe 1-Kozykel aus $Z^1_{\text{cont}}(S, B)$, dann gibt es ein $\beta \in B$ mit $\tilde{a}_s = \beta^{-1} a_s {}^s\beta$ für alle $s \in S$. Daraus folgt:

$$\begin{aligned}[s_b(\tilde{a})]_s = \beta^{-1} a_s {}^s\beta \cdot b_s^{-1} = \beta^{-1} a_s \cdot b_s^{-1} b_s \cdot {}^s\beta b_s^{-1} \\ = \beta^{-1} \cdot a_s b_s^{-1} \cdot b_s {}^s\beta b_s^{-1} \overset{(13)}{=} \beta^{-1} \cdot [s_b(a)]_s \cdot {}^{s'}\beta.\end{aligned}$$

Also sind auch $s_b(a)$ und $s_b(\tilde{a})$ kohomolog, und die Behauptung folgt.

- $\tau_b(1) = b$: Klar!

q.e.d.

2.32 Lemma. Seien $B \xrightarrow{\varphi} C$ ein Morphismus von diskreten S-Mengen und $b = (b_s) \in Z^1_{\text{cont}}(S, B)$ ein stetiger 1-Kozykel. Dann ist folgendes Diagramm kommutativ in der Kategorie der Mengen (jedoch *nicht* in der Kategorie der *punktierten* Mengen!):

$$\begin{array}{ccc} H^1_{\text{cont}}(S, B) & \xrightarrow{H^1_{\text{cont}}(\varphi)} & H^1_{\text{cont}}(S, C) \\ {\scriptstyle \tau_b}\uparrow\wr & = & \wr\uparrow{\scriptstyle \tau_{\varphi \circ b}} \\ H^1_{\text{cont}}(S, B_b) & \xrightarrow[H^1_{\text{cont}}(\varphi)]{} & H^1_{\text{cont}}(S, C_b) \end{array}$$

Beweis: Sei $[c] \in H^1_{\text{cont}}(S, B_b)$ beliebig, repräsentiert durch den 1-Kozykel $c = (c_s)$. Dann folgt sofort:

$$\begin{aligned}\big(H^1_{\text{cont}}(\varphi) \circ \tau_b\big)[c] = H^1_{\text{cont}}(\varphi)[c_s \cdot b_s] = [\varphi(c_s b_s)] \\ = [\varphi(c_s) \cdot \varphi(b_s)] = \tau_{\varphi \circ b}[\varphi(c_s)] = \big(\tau_{\varphi \circ b} \circ H^1_{\text{cont}}(\varphi)\big)[c].\end{aligned}$$

q.e.d.

2.33 Korollar. Es sei

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

eine kurze exakte Sequenz von diskreten S-Mengen, und sei $b = (b_s) \in Z^1_{\text{cont}}(S, B)$ ein stetiger 1-Kozykel. Dann ist folgendes Diagramm kommutativ, und die untere Zeile ist exakt in der Kategorie der punktierten Mengen:

$$\begin{array}{ccccccc} & & H^1_{\text{cont}}(S, B) & \xrightarrow{H^1_{\text{cont}}(p)} & H^1_{\text{cont}}(S, C) & & \\ & & {\scriptstyle \tau_b}\uparrow\wr & = & \wr\uparrow{\scriptstyle \tau_{pb}} & & \\ H^0(S, C_b) & \xrightarrow[\delta]{} & H^1_{\text{cont}}(S, A_b) & \xrightarrow[H^1_{\text{cont}}(i)]{} & H^1_{\text{cont}}(S, B_b) & \xrightarrow[H^1_{\text{cont}}(p)]{} & H^1_{\text{cont}}(S, C_b). \end{array}$$

Die Abbildung $\tau_b \circ H^1_{\mathrm{cont}}(i)$ induziert eine Bijektion

$$\begin{array}{ccc} H^1_{\mathrm{cont}}(S, A_b)/H^0(S, C_b) & \xrightarrow{\sim} & \{[b'] \in H^1_{\mathrm{cont}}(S, B) \mid H^1_{\mathrm{cont}}(p)[b'] = H^1_{\mathrm{cont}}(p)[b]\} \\ (a_s) & \mapsto & (a_s \cdot b_s) \end{array}$$

Beweis: Klar nach 2.19, 2.27 und 2.32! **q.e.d.**

Als letztes wollen wir in diesem Kapitel noch beweisen, daß man auch im nicht-abelschen Fall die Inflations-Restriktions-Sequenz zur Verfügung hat.

2.34 Lemma/ Definition. Es sei A eine diskrete S-Gruppe, R eine zweite topologische Gruppe und $R \xrightarrow{\varphi} S$ ein stetiger Gruppenhomomorphismus.
Dann wird durch die Komposition

$$R \xrightarrow{\varphi} S \longrightarrow \mathrm{Aut}\,(A)$$

eine stetige R-Operation auf A gegeben; die dadurch definierte diskrete R-Gruppe wollen wir mit $\varphi^* A$ bezeichnen. Die Identität auf A bzw. die Einschränkung von 1-Kozykeln von S auf R definiert kanonische Abbildungen

$$\begin{array}{ccccc} H^0(S, A) & \xrightarrow{\mathrm{can}} & H^0(R, \varphi^* A) & \text{und} & H^1_{\mathrm{cont}}(S, A) \xrightarrow{\mathrm{can}} H^1_{\mathrm{cont}}(R, \varphi^* A) \\ a & \mapsto & a & & \alpha = (a_s) \mapsto \alpha \circ \varphi = (a_{\varphi(r)})_r. \end{array}$$

Sei nun B eine diskrete R-Gruppe und $A \xrightarrow{f} B$ ein Gruppenhomomorphismus. Der Morphismus f heißt *verträglich mit* φ, wenn $\varphi^* A \xrightarrow{f} B$ ein Morphismus von diskreten R-Gruppen ist, d.h. wenn

$$\forall r \in R \ \forall a \in A : f({}^{\varphi(r)}a) = {}^{r}(f(a)).$$

Ist f verträglich mit φ, so definieren die Kompositionen

$$\begin{array}{ccccc} H^0(S, A) & \xrightarrow{\mathrm{can}} & H^0(R, \varphi^* A) & \xrightarrow{H^0(f)} & H^0(R, B) \quad \text{und} \\ H^1_{\mathrm{cont}}(S, A) & \xrightarrow{\mathrm{can}} & H^1_{\mathrm{cont}}(R, \varphi^* A) & \xrightarrow{H^1_{\mathrm{cont}}(f)} & H^1_{\mathrm{cont}}(R, B) \end{array}$$

kanonische Abbildungen $H^0(S, A) \to H^0(R, B)$ und $H^1_{\mathrm{cont}}(S, A) \to H^1_{\mathrm{cont}}(R, B)$ von punktierten Mengen.

Beweis: Klar! **q.e.d.**

2.35 Lemma/ Definition. Es sei A eine diskrete S-Gruppe.

(i) Sei R eine abgeschlossene Untergruppe von S, und bezeichne die Inklusion $R \hookrightarrow S$ mit i. Dann ist die Identität auf $i^* A$ verträglich mit i, und die dadurch gemäß 2.34 definierten Abbildungen bezeichnen wir als *Restriktion*:

$$\begin{array}{ccccc} H^0(S, A) & \xrightarrow{\mathrm{res}} & H^0(R, A) & \text{und} & H^1_{\mathrm{cont}}(S, A) \xrightarrow{\mathrm{res}} H^1_{\mathrm{cont}}(R, A) \\ a & \mapsto & a & & \alpha = (a_s)_s \mapsto \alpha | R = (a_r)_r. \end{array}$$

(ii) Sei N ein abgeschlossener Normalteiler von S. Dann ist A^N via ${}^{\bar{s}}a := {}^{s}a$ eine diskrete S/N-Gruppe, und die Inklusion $A^N \hookrightarrow A$ ist verträglich mit der Projektion $p : S \twoheadrightarrow S/N$. Die dadurch gemäß 2.34 definierten Abbildungen bezeichnen wir als *Inflation*:

$$\begin{array}{ccccccc} H^0(S/N, A^N) & \xrightarrow{\inf} & H^0(S,A) & \text{und} & H^1_{\text{cont}}(S/N, A^N) & \xrightarrow{\inf} & H^1_{\text{cont}}(S,A) \\ a & \mapsto & a & & (a_{\bar{s}})_{\bar{s}} & \mapsto & (a_{\bar{s}})_s. \end{array}$$

Beweis: Klar! **q.e.d.**

2.36 Satz. Es sei A eine diskrete S-Gruppe und $N \subseteq S$ ein abgeschlossener Normalteiler. Dann ist die folgende Sequenz exakt in der Kategorie der punktierten Mengen, und die Inflation ist injektiv:

$$H^1_{\text{cont}}(S/N, A^N) \xhookrightarrow{\inf} H^1_{\text{cont}}(S,A) \xrightarrow{\text{res}} H^1_{\text{cont}}(N,A).$$

Beweis:

- *Inflation injektiv:* Mögen $\alpha, \alpha' \in H^1_{\text{cont}}(S/N, A^N)$ unter der Inflation auf dieselbe Klasse in $H^1_{\text{cont}}(S,A)$ abgebildet werden. Es werde α durch den 1-Kozykel $(a_{\bar{s}})_{\bar{s}}$ und α' durch den 1-Kozykel $(a'_{\bar{s}})_{\bar{s}}$ repräsentiert. Nach Voraussetzung gibt es ein $b \in A$ mit $a'_{\bar{s}} = b^{-1} a_{\bar{s}} {}^{s}b$ für alle $s \in S$. Wir wollen $b \in A^N$ zeigen, denn dann sind $(a_{\bar{s}})_{\bar{s}}$ und $(a'_{\bar{s}})_{\bar{s}}$ kohomolog, d.h. es gilt $\alpha = \alpha'$. Sei also $t \in N$ beliebig. Es ist dann $\bar{t} = \bar{1} \in S/N$, so daß folgt:

  $$1 \overset{2.22}{=} a'_{\bar{t}} = b^{-1} a_{\bar{t}} {}^{t}b \overset{2.22}{=} b^{-1} {}^{t}b \quad \Longrightarrow \quad {}^{t}b = b.$$

  Es gilt also tatsächlich $b \in A^N$, und die Behauptung ist gezeigt.

- *Exaktheit bei $H^1_{cont}(S,A)$:* Wird $\alpha \in H^1_{\text{cont}}(S/N, A^N)$ durch den 1-Kozykel $(a_{\bar{s}})_{\bar{s}}$ repräsentiert, so gilt

  $$\forall t \in N \,:\, a_{\bar{t}} = a_{\bar{1}} \overset{2.22}{=} 1,$$

  d.h. $(\text{res} \circ \inf)(\alpha)$ ist die triviale Klasse.

  Sei umgekehrt $\alpha \in H^1_{\text{cont}}(S,A)$ eine Klasse, die unter der Restriktion auf die triviale Klasse abgebildet wird. Wenn α durch den 1-Kozykel $(a_s)_s$ repräsentiert wird, gibt es also ein $b \in A$ mit $b^{-1} a_t {}^{t}b = 1$ für alle $t \in N$. Indem wir $(a_s)_s$ durch den kohomologen 1-Kozykel $(b^{-1} a_s {}^{s}b)_s$ ersetzen, können wir also ohne Beschränkung der Allgemeinheit annehmen, daß die Restriktion von $(a_s)_s$ auf N trivial ist.

  Daraus ergibt sich zunächst:

  $$\forall s \in S \;\; \forall t \in N \,:\, a_{st} = a_s {}^{s}a_t = a_s {}^{s}1 = a_s. \tag{14}$$

  Seien nun $s \in S$ und $t \in N$ beliebig. Da N ein Normalteiler in S ist, gibt es ein $t' \in N$ mit $ts = st'$, und es folgt:

  $$a_s \overset{(14)}{=} a_{st'} = a_{ts} = a_t {}^{t}a_s = 1 \cdot {}^{t}a_s = {}^{t}a_s.$$

  Für alle $s \in S$ liegt a_s also in A^N, woraus mit Hilfe von (14) folgt, daß $(a_s)_{\bar{s}}$ ein wohldefinierter stetiger 1-Kozykel von S/N in A^N ist, und es ist klar, daß die Klasse dieses 1-Kozykels ein Urbild von α unter der Inflation ist.

q.e.d.

3 Formen

Sei K/k galoissch mit Galoisgruppe G.

In diesem Kapitel werden wir das Prinzip des Galois-Descents im Falle einer beliebigen Koeffizientenerweiterung $F : \mathcal{C}_k \to \mathcal{C}_K$ entwickeln. Dazu definieren wir für ein Objekt X aus $\mathcal{C}_k$ zunächst die Menge $E(K/k, X)$ der *K/k-Formen von X* und zeigen, daß man eine kanonische Injektion $\vartheta : E(K/k, X) \hookrightarrow H^1(G, A(X)$ hat, wobei $A(X)$ die Automorphismengruppe $\mathrm{Aut}_{\mathcal{C}_K}(FX)$ bezeichnet.

3.1 Satz/ Definition. Es seien $F : \mathcal{C}_k \to \mathcal{C}_K$ eine Koeffizientenerweiterung und $X \in \mathrm{Ob}(\mathcal{C}_k)$ ein Objekt „unten“. Bezeichne $A(X) := \mathrm{Aut}_K(FX)$ die Gruppe der Automorphismen „oben“. Nach Voraussetzung ist $A(X)$ eine G-Gruppe. Die Klasse der *K/k-Formen von X* ist definiert als

$$E(K/k, X) \;:=\; \{Y \in \mathrm{Ob}(\mathcal{C}_k) \,|\, FY \cong_K FX\}/\mathcal{C}_k\text{-Isomorphismen},$$

d.h. als Klasse der Isomorphieklassen von Objekten „unten“, die „oben“ zu X isomorph sind.

Sei Y Repräsentant einer Klasse $[Y]$ aus $E(K/k, X)$, so daß es also einen Isomorphismus $f : FY \xrightarrow{\sim} FX$ in $\mathcal{C}_K$ gibt. Dann ist $[s \mapsto f^s(f^{-1})]$ ein 1-Kozykel von G in $A(X)$, dessen Klasse in $H^1(G, A(X))$ nur von $[Y]$ abhängt. — Wir bezeichnen diese Kohomologieklasse mit $\vartheta[Y]$.

Die Zuordnung $[Y] \mapsto \vartheta[Y]$ ist *injektiv*; insbesondere ist also $E(K/k, X)$ eine *Menge*. Diese Menge punktieren wir, indem wir das Element $[X]$ auszeichnen. Dann erhalten wir eine wohldefinierte, injektive Abbildung von punktierten Mengen

$$\boxed{\vartheta :\; E(K/k, X) \hookrightarrow H^1(G, A(X))}.$$

Beweis:

- *Wohldefiniertheit:* Wir haben zu zeigen, daß $\vartheta[Y]$ tatsächlich eine von den getroffenen Wahlen unabhängige Kohomologieklasse ist:
  - *1-Kozykel:* Für $s \in G$ setze $a_s := f^s(f^{-1})$. Dann gilt:
$$\begin{array}{rcl} a_{st} & = & f^{st}(f^{-1}) = f^s 1_{FY}{}^{st}(f^{-1}) \overset{\text{(KE1)}}{=} f\,[{}^s(f^{-1})\,{}^s f]\,{}^{st}(f^{-1}) \\ & \overset{\text{(KE1)}}{=} & f^s(f^{-1})\,{}^s[f^t(f^{-1})] = a_s\,{}^s a_t. \end{array}$$
  - *unabhängig von der Wahl von f:* Sei $FY \overset{f}{\underset{f'}{\rightrightarrows}} FX$ gegeben. Wir haben also ein kommutatives Dreieck: $\begin{array}{ccc} & \overset{f}{\nearrow} & FX \\ FY & = & \uparrow b \\ & \underset{f'}{\searrow} & FX \end{array}$

    Setze $a'_s := f'^s(f'^{-1})$, dann folgt:
$$a'_s = (b^{-1}f)^s(f^{-1}b) \overset{\text{(KE1)}}{=} b^{-1}\left(f^s(f^{-1})\right){}^s b = b^{-1}a_s\,{}^s b \sim a_s,$$
    d.h. in $H^1(G, A(X))$ definieren (a_s) und (a'_s) dasselbe Element.

– *unabhängig von der Wahl von Y:* Sei $[Y'] = [Y]$ und $g : Y' \xrightarrow{\sim} Y$ beliebig. Dann ist $FY' \xrightarrow{Fg} FY \xrightarrow{f} FX$ ein Isomorphismus, und es gilt

$$(fFg)^s(fFg)^{-1} = fFg \underbrace{{}^s(Fg)^{-1}}_{\overset{(\mathrm{KE2})}{=} Fg^{-1}} {}^sf^{-1} = f^s(f^{-1}) = a_s.$$

- *injektiv:* Seien $[Y]$ und $[Y']$ zwei K/k-Formen von X mit $\vartheta[Y] = \vartheta[Y']$. Wir müssen zeigen, daß Y und Y' dann schon in $\mathcal{C}_k$ isomorph sind. Da zunächst FY, FY' und FX isomorph sind, haben wir Isomorphismen $FY' \xrightarrow{g} FY \xrightarrow{f} FX$. Dann ist

$$\vartheta[Y'] = (a'_s) \text{ mit } a'_s = fg^s(g^{-1}f^{-1}),$$
$$\vartheta[Y] = (a_s) \text{ mit } a_s = f^s(f^{-1}).$$

Nach Voraussetzung gilt $(a'_s) \sim (a_s)$, d.h. es gibt $b \in A(X)$ mit

$$\begin{array}{lcl} \forall s \in G & : & a'_s = b^{-1}a_s{}^sb \\ & \overset{(\mathrm{KE1})}{\Leftrightarrow} & fg^s(g^{-1})^s(f^{-1}) = b^{-1}f^s(f^{-1}) \\ & \overset{(\mathrm{KE1})}{\Leftrightarrow} & \underbrace{{}^s(g^{-1})^s(f^{-1})^s(b^{-1})^sf}_{\overset{(\mathrm{KE1})}{=} {}^s(\underbrace{g^{-1}f^{-1}b^{-1}f}_{=:h})} = \underbrace{g^{-1}f^{-1}b^{-1}f}_{=h} \\ & \Leftrightarrow & {}^sh = h. \end{array}$$

Wir haben also einen Isomorphismus $h : FY \xrightarrow{\sim} FY'$ gefunden, der fix unter der Operation der Galoisgruppe ist. Nach (KE2) kommt h dann aber von einem Isomorphismus aus $\mathcal{C}_k$, d.h. $[Y] = [Y']$.

- *Abbildung punktierter Mengen:* Wählen wir für $f : FX \xrightarrow{\sim} FX$ die Identität, so gilt für alle s offenbar $f^s(f^{-1}) = 1_{FX}$, d.h. $[X]$ wird unter ϑ auf den trivialen Kozykel abgebildet.

q.e.d.

Als erste Anwendung zeigen wir nun, wie man die Automorphismengruppe einer K/k-Form Y von X bei Kenntnis von $\vartheta[Y]$ berechnen kann.

3.2 Satz. Sei $F : \mathcal{C}_k \to \mathcal{C}_K$ eine Koeffizientenerweiterung, $X \in \mathrm{Ob}(\mathcal{C}_k)$ ein Objekt „unten“ und Y eine K/k-Form von X, gemäß 3.1 charakterisiert durch die Klasse $\vartheta[Y]$, die durch den 1-Kozykel $a = (a_s) = (f^s(f^{-1}))$ (für ein $f : FY \xrightarrow{\sim} FX$) repräsentiert werde.
Es sei $A(X)_a$ die mit a-getwistete Automorphismengruppe im Sinne von 2.24. Dann ist

$$\begin{array}{ccc} A(Y) & \longrightarrow & A(X)_a \\ b & \mapsto & fbf^{-1} \end{array}$$

ein Isomorphismus von G-Gruppen.

Beweis: Daß die Abbildung ein Gruppenisomorphismus ist, ist klar, weil f ein Isomorphismus ist. Es ist also nur zu zeigen, daß die Abbildung auch G-äquivariant ist. Seien dazu $s \in G$ und $b \in A(Y)$ beliebig; es ergibt sich:

$$^{s'}(fbf^{-1}) = a_s \cdot {}^s(fbf^{-1}) \cdot a_s^{-1} \overset{(KE1)}{=} f^s(f^{-1}) \cdot {}^sf{}^sb{}^s(f^{-1}) \cdot {}^sff^{-1} = f({}^sb)f^{-1}$$

q.e.d.

3.3 Korollar. Sei $F : \mathcal{C}_k \to \mathcal{C}_K$ eine Koeffizientenerweiterung, $X \in \mathrm{Ob}(\mathcal{C}_k)$ ein Objekt „unten“ und Y eine K/k-Form von X mit $\vartheta[Y] = [a]$ für einen 1-Kozykel a. Dann gilt

$$\mathrm{Im}\left(\mathrm{Aut}_k(Y) \xrightarrow{F} A(Y)\right) \cong (A(X)_a)^G .$$

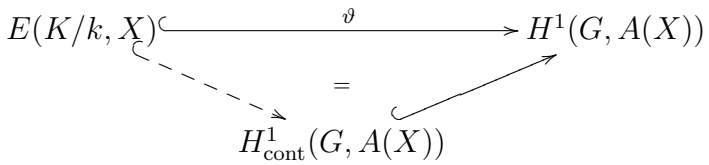
Ist insbesondere $\mathrm{Aut}_k(Y) \xrightarrow{F} A(Y)$ *injektiv* (was zum Beispiel bei allen Koeffizientenerweiterungen aus Beispiel 1.6 der Fall ist), so erhalten wir

$$\boxed{\mathrm{Aut}_k(Y) \cong (A(X)_a)^G.}$$

Beweis: Klar nach 3.2 und (KE2)! **q.e.d.**

Als nächstes definieren wir eine Bedingung an unsere Koeffizientenerweiterung $F : \mathcal{C}_k \to \mathcal{C}_K$, unter der ϑ schon über $H^1_{\mathrm{cont}}(G, A(X))$ faktorisiert.

3.4 Lemma/ Definition. Eine *stetige* Koeffizientenerweiterung ist eine Koeffizientenerweiterung $F : \mathcal{C}_k \to \mathcal{C}_K$ mit der Eigenschaft, daß für alle $X, Y \in \mathrm{Ob}\,(\mathcal{C}_k)$ die Mengen $\mathrm{Iso}_K\,(FX, FY)$ *diskrete* G-Mengen sind. Ist F eine stetige Koeffizientenerweiterung, so gilt für alle $X \in \mathrm{Ob}\,(\mathcal{C}_k)$, daß ϑ über $H^1_{\mathrm{cont}}(G, A(X))$ faktorisiert:



Beweis: Sei $[Y] \in E(K/k, X)$ beliebig. Wähle einen Isomorphismus $f : FY \xrightarrow{\sim} FX$, und sei $(a_s) = (f^s(f^{-1}))$ der dadurch definierte 1-Kozykel, der $\vartheta[Y]$ repräsentiert. Wir müssen zeigen, daß (a_s) stetig ist. Nach Voraussetzung ist $\mathrm{Iso}_K(FY, FX)$ eine diskrete G-Menge, d.h. wir finden nach 2.2(i)⇒(ii) eine offene Untergruppe $U \subseteq G$ mit $f \in \mathrm{Iso}_K\,(FY, FX)^U$. Für beliebiges $u \in U$ haben wir:

$$1_{FX} = {}^u1_{FX} = {}^u(ff^{-1}) = {}^uf{}^u(f^{-1}) = f^u(f^{-1}) = a_u.$$

Der 1-Kozykel (a_s) ist also konstant, wenn wir ihn auf U einschränken. Für $s \in G$ beliebig folgt daraus:

$$a_{su} = a_s{}^sa_u = a_s{}^s1_{FX} = a_s,$$

d.h. (a_s) ist konstant auf sU für jedes $s \in G$, also lokalkonstant, also stetig. **q.e.d.**

3.5 Beispiele.

(i) Die Koeffizientenerweiterung $F : \mathbf{Var_k} \to \mathbf{Var_K}$ aus Beispiel 1.6(i) ist stetig, denn wenn X und Y Varietäten über k sind und $f : FX \xrightarrow{\sim} FY$ ein Isomorphismus über K, so ist f auch schon über einem Zwischenkörper k' der Erweiterung K/k definiert, der endlich über k ist (f wird durch endlich viele Polynome über K beschrieben; als k' kann dann der Körper gewählt werden, der aus k durch Adjunktion der Koeffizienten dieser Polynome entsteht). Dann ist f fix unter der offenen Untergruppe $\mathrm{Gal}(K/k')$ von G.

(ii) Die Koeffizientenerweiterungen $\mathcal{F}_k^{n,r} \to \mathcal{F}_K^{n,r}$ und $\widetilde{\mathcal{F}_k^{n,r}} \to \widetilde{\mathcal{F}_K^{n,r}}$ aus den Beispielen 1.6(iv) und (v) sind ebenfalls stetig: Sind P und Q Objekte aus $\widetilde{\mathcal{F}_k^{n,r}}$, und ist $\bar{B} \in \mathrm{PGL}(n,K) = \mathrm{Iso}_K(FP, FQ)$ ein Isomorphismus, repräsentiert durch $B = (b_{ij}) \in \mathrm{GL}\,(n,K)$, so definiere den Körper k' als den Zwischenkörper der Erweiterung K/k, der aus k durch Adjunktion der Koeffizienten b_{ij} entsteht. Dann ist k'/k endlich, die Galoisgruppe $G' := \mathrm{Gal}(K/k')$ also eine offene Untergruppe von G, und $\bar{B}$ ist fix unter der Operation von G'.
Daß $\mathcal{F}_k^{n,r} \to \mathcal{F}_K^{n,r}$ stetig ist, sieht man ganz genauso!

In der Einleitung haben wir gesehen, daß wir zur Berechnung der Zetafunktion einer Form der Fermatgleichung unter anderem ϑ^{-1} für die Koeffizientenerweiterung $\mathbf{Rep}_{\mathbb{Q}_l}^{G_k} \to \mathbf{Rep}_{\mathbb{Q}_l}^{G_K}$ berechnen müssen. Dies wollen wir jetzt tun.

3.6 Lemma/ Definition. Sei $F : \mathbf{Rep}_L^{G_k} \to \mathbf{Rep}_L^{G_K}$ die Koeffizientenerweiterung aus Beispiel 1.6(vi), $V := (V, \varphi) \in \mathrm{Ob}(\mathbf{Rep}_L^{G_k})$ und $\xi = (a_{\bar{s}}) \in Z^1(G, A(V))$. Für $s \in G_k$ bezeichne $\bar{s}$ das Bild in G. Durch

$$G_k \longrightarrow \mathrm{Aut}\,(V),\ s \mapsto \varphi^\xi(s) := a_{\bar{s}}\varphi(s)$$

wird eine neue Operation φ^ξ auf V definiert. V, versehen mit dieser neuen Operation, nennen wir $V(\xi)$. Dann gilt: $V(\xi)$ ist eine K/k-Form von V, und es gilt

$$\vartheta[V(\xi)] \quad = \quad [\xi] \in H^1(G, A(V)).$$

Insbesondere ist ϑ also in diesem Fall auch surjektiv.

Beweis:

- *Operation:* Mit $a_{\bar{s}}$ und $\varphi(s)$ ist auch $\varphi^\xi(s)$ ein k-Automorphismus von V, und für $s, t \in G_k$ gilt:

$$\begin{aligned} \varphi^\xi(st) &= a_{\bar{s}\bar{t}}\varphi(st) = a_{\bar{s}}{}^{\bar{s}}a_{\bar{t}}\varphi(st) \\ &\overset{(5)}{=} a_{\bar{s}}\left[\varphi(s)a_{\bar{t}}\varphi(s)^{-1}\right]\varphi(st) \\ &= \left[a_{\bar{s}}\varphi(s)\right]\left[a_{\bar{t}}\varphi(t)\right] = \varphi^\xi(s)\varphi^\xi(t). \end{aligned}$$

- *Form:* Ist $s \in G_K \subseteq G_k$, so gilt $\bar{s} = 1 \in G$, d.h.

$$\forall s \in G_K\ :\ \varphi^\xi(s) \overset{2.22}{=} 1 \cdot \varphi(s) = \varphi(s).$$

Also ist $(V, \varphi^\xi|G_K) = (V, \varphi|G_K)$, d.h. $V(\xi)$ ist eine K/k-Form von V.

- *Urbild von* $[\xi]$*:* Wie wir gerade gesehen haben, können wir als Isomorphismus $f : FV(\xi) \xrightarrow{\sim} FV$ die Identität wählen. Es ergibt sich $\vartheta[V(\xi)] = [b_{\bar{s}}]$ mit

$$b_{\bar{s}} = 1 \cdot {}^{\bar{s}}(1^{-1}) \overset{(5)}{=} 1 \cdot \varphi^{\xi}(s) \cdot 1 \cdot \varphi(s)^{-1} = a_{\bar{s}}\varphi(s)\varphi(s)^{-1} = a_{\bar{s}},$$

  wobei s ein Urbild von $\bar{s}$ in G_k sei.

q.e.d.

3.7 Bemerkung. Auch für die Koeffizientenerweiterungen aus Beispiel 1.6(i) und (iii) gilt, daß ϑ eine Bijektion ist, falls G endlich ist. (Vgl. [Ser97, S.121ff]!)

Jetzt definieren wir den zweiten zentralen Begriff dieses Kapitels, den des *Morphismus* von zwei Koeffizientenerweiterungen $F : \mathcal{C}_k \to \mathcal{C}_K$ und $F' : \mathcal{C}_k{}' \to \mathcal{C}_K{}'$.

Für unsere Zwecke besonders wichtig wird der Fall der Erweiterungen $\mathcal{F}_k^{n,m} \to \mathcal{F}_K^{n,m}$ und $\mathbf{Rep}_{\mathbb{Q}_l}^{G_k} \to \mathbf{Rep}_{\mathbb{Q}_l}^{G_K}$ sein, bei dem der Morphismus durch die l-adische Kohomologie gegeben wird. Wir werden insbesondere sehen, daß für eine getwistete Fermatgleichung Q die Kohomologie der zugehörigen Hyperfläche $X(Q)$ durch die Kohomologieklasse $H_{\text{ét}}\,\vartheta[Q]$ charakterisiert wird.

3.8 Definition. Ein *Morphismus* zwischen zwei Koeffizientenerweiterungen $\mathcal{C}_k \xrightarrow{F} \mathcal{C}_K$ und $\mathcal{C}_k{}' \xrightarrow{F'} \mathcal{C}_K{}'$ wird durch kovariante Funktoren $H_k : \mathcal{C}_k \to \mathcal{C}_k{}'$ und $H_K : \mathcal{C}_K \to \mathcal{C}_K{}'$ sowie eine natürliche Äquivalenz $h : H_K F \xrightarrow{\sim} F' H_k$ gegeben:

$$\begin{array}{ccc} \mathcal{C}_K & \xrightarrow{H_K} & \mathcal{C}_K{}' \\ {\scriptstyle F}\uparrow & \overset{h}{\swarrow} & \uparrow{\scriptstyle F'} \\ \mathcal{C}_k & \xrightarrow[H_k]{} & \mathcal{C}_k{}' \end{array}$$

Dabei soll zusätzlich gelten, daß für alle $Y, Z \in \mathrm{Ob}(\mathcal{C}_k)$ die Komposition

$$\mathrm{Iso}_{\mathcal{C}_K}(FY, FZ) \xrightarrow{H_K} \mathrm{Iso}_{\mathcal{C}_K{}'}(H_K FY, H_K FZ) \xrightarrow{h} \mathrm{Iso}_{\mathcal{C}_K{}'}(F' H_k Y, F' H_k Z)$$

G-äquivariant ist.

3.9 Bemerkung. Sind $\mathcal{C}_k \xrightarrow{F} \mathcal{C}_K$, $\mathcal{C}_k{}' \xrightarrow{F'} \mathcal{C}_K{}'$ und $\mathcal{C}_k{}'' \xrightarrow{F''} \mathcal{C}_K{}''$ Koeffizientenerweiterungen und $(\mathcal{C}_k \xrightarrow{H_k} \mathcal{C}_k{}', \mathcal{C}_K \xrightarrow{H_K} \mathcal{C}_K{}', H_K F \xrightarrow{h} F' H_k)$ und $(\mathcal{C}_k{}' \xrightarrow{H'_k} \mathcal{C}_k{}'', \mathcal{C}_K{}' \xrightarrow{H'_K} \mathcal{C}_K{}'', H'_K F' \xrightarrow{h'} F'' H'_k)$ Morphismen von Koeffizientenerweiterungen, so ist offenbar auch $(\mathcal{C}_k \xrightarrow{H'_k H_k} \mathcal{C}_k{}'', \mathcal{C}_K \xrightarrow{H'_K H_K} \mathcal{C}_K{}'', H'_K H_K F \xrightarrow{(h' H_k)(H'_K h)} F'' H'_k H_k)$ ein Morphismus von Koeffizientenerweiterungen.

Man überlegt sich leicht, daß die so definierte Komposition von Morphismen von Koeffizientenerweiterungen *assoziativ* ist, d.h. wir erhalten auf diese Weise die *Kategorie der Koeffizientenerweiterungen.*[†]

[†]Ist $F : \mathcal{C}_k \to \mathcal{C}_K$ eine Koeffizientenerweiterung, so ist die *Identität auf* F der offensichtliche Morphismus $(1_{\mathcal{C}_k}, 1_{\mathcal{C}_K}, 1_{\mathcal{C}_K} F \xrightarrow{=} F 1_{\mathcal{C}_k})$.

3.10 Satz. Sei (H_k, H_K, h) ein Morphismus zwischen den beiden Koeffizientenerweiterungen $\mathcal{C}_k \xrightarrow{F} \mathcal{C}_K$ und $\mathcal{C}_k{}' \xrightarrow{F'} \mathcal{C}_K{}'$. Dann ist für jedes $X \in \mathrm{Ob}(\mathcal{C}_k)$ das folgende Diagramm von Abbildungen punktierter Mengen kommutativ:

$$\begin{array}{ccc} E(K/k, X) & \xrightarrow[[Y] \mapsto [H_k Y]]{\varphi} & E(K/k, H_k X) \\ \vartheta \downarrow & = & \downarrow \vartheta \\ H^1(G, A(X)) & \xrightarrow[\psi]{(a_s) \mapsto (hH_K a_s)} & H^1(G, A(H_k X)) \end{array}$$

Beweis:

- *Wohldefiniertheit von φ:*
  - Gilt $Y \cong Y'$, so auch $H_k Y \cong H_k Y'$, d.h. $\varphi([Y])$ ist unabhängig von der Wahl des Repräsentanten Y.
  - Ist $FY \xrightarrow{f} FX$ ein Isomorphismus, so auch $hH_K f : F'H_k Y \xrightarrow{\sim} F'H_k X$, d.h. aus $[Y] \in E(K/k, X)$ folgt $[H_k Y] \in E(K/k, H_k X)$.
  - Das ausgezeichnete Element $[X]$ geht unter φ auf das ausgezeichnete Element $[H_k X]$.
- *Wohldefiniertheit von ψ:*
  - Sei $(a_s) \in Z^1(G, A(X))$ ein 1-Kozykel und seien $s, t \in G$. Dann folgt:

    $$hH_K a_{st} = hH_K\left(a_s {}^s a_t\right) = \left(hH_K a_s\right)\left(hH_K {}^s a_t\right) \overset{3.8}{=} \left(hH_K a_s\right) {}^s\!\left(hH_K a_t\right).$$

    Also ist $(hH_k a_s)$ ebenfalls ein 1-Kozykel.
  - Seien $(a_s), (a'_s) \in Z^1(G, A(X))$ zwei kohomologe 1-Kozykel, sei $b \in A(X)$ so gewählt, daß $a'_s = b^{-1} a_s {}^s b$ für alle $s \in G$ gilt. Dann folgt

    $$hH_K a'_s = hH_K\left(b^{-1} a_s {}^s b\right) = \underbrace{\left(hH_K b^{-1}\right)}_{= (hH_K b)^{-1}} \left(hH_K a_s\right) \underbrace{\left(hH_K {}^s b\right)}_{\overset{3.8}{=} {}^s(hH_K b)}$$

    d.h. $(hH_K a_s) \sim (hH_K a'_s)$.
  - Ist $(a_s) \in Z^1(G, A(X))$ der triviale Kozykel, so ist offenbar auch $(hH_K a_s)$ trivial, d.h. unter ψ geht das ausgezeichnete Element auf das ausgezeichnete Element.
- *Kommutativität des Diagramms:* Sei $[Y] \in E(K/k, X)$, und wähle einen Isomorphismus $FY \xrightarrow{f} FX$. Dann gilt für alle $s \in G$:

  $$\left(\vartheta\varphi[Y]\right)_s = \left(\vartheta[H_k Y]\right)_s = \left(hH_K f\right) {}^s\!\left(hH_K f^{-1}\right) \overset{3.8}{=} hH_K \underbrace{\left(f {}^s\!\left(f^{-1}\right)\right)}_{= (\vartheta[Y])_s} = \left(\psi\vartheta[Y]\right)_s .$$

q.e.d.

3.11 Beispiele.

(i) Seien $n \geq 2$ und $r \geq 1$ natürliche Zahlen. Wir betrachten die Koeffizientenerweiterungen $F : \widetilde{\mathcal{F}_k^{n,r}} \to \widetilde{\mathcal{F}_K^{n,r}}$ und $F' : \mathbf{Var}_{\mathbf{k}}^{\mathrm{Iso}} \to \mathbf{Var}_{\mathbf{K}}^{\mathrm{Iso}}$ aus Beispiel 1.6(v) bzw. (i)+(vii). Wir wollen Funktoren $F_k : \widetilde{\mathcal{F}_k^{n,r}} \to \mathbf{Var}_{\mathbf{k}}^{\mathrm{Iso}}$ und $F_K : \widetilde{\mathcal{F}_K^{n,r}} \to \mathbf{Var}_{\mathbf{K}}^{\mathrm{Iso}}$ definieren:
Für $P \in k[X_1, \ldots, X_n]$ sei $F_k P := \operatorname{Proj} k[X_1, \ldots, X_n]/P$, die durch P definierte Hyperfläche in $\mathbb{P}_k^{n-1}$. Ist $\bar{A} \in \mathrm{PGL}(n,k) : P \to Q$ ein Morphismus in $\widetilde{\mathcal{F}_k^{n,r}}$, so sei $F_k\bar{A}$ der dadurch gegebene Automorphismus des $\mathbb{P}_k^{n-1}$, eingeschränkt auf $F_k P$. Offenbar ist dann $F_k A : F_k P \to F_k Q$ ein Morphismus von projektiven Varietäten über k, womit F_k zu einem Funktor wird. F_K werde ganz genauso definiert, nur mit K anstelle von k!
Für $P \in k[X_i]$ haben wir einen kanonischen Isomorphismus

$$f_P : F_K F P = \operatorname{Proj} K[X_1, \ldots, X_n]/P \xrightarrow{\sim} \operatorname{Proj} k[X_1, \ldots, X_n]/P \times_k K;$$

mit seiner Hilfe erhalten wir eine natürliche Äquivalenz $f : F_K F \to F' F_k$. Das Tripel (F_k, F_K, f) ist dann ein Morphismus zwischen den Koeffizientenerweiterungen F und F'. (Daß die drei Funktoren die geforderten Eigenschaften erfüllen, überlegt man sich leicht!)

(ii) Sei $l \neq \mathrm{char}(k)$ eine Primzahl, $i \in \mathbb{N}_0$ eine natürliche Zahl, und seien $F' : \mathbf{Var}_{\mathbf{k}}^{\mathrm{Iso}} \to \mathbf{Var}_{\mathbf{K}}^{\mathrm{Iso}}$ und $F'' : \mathbf{Rep}_{\mathbb{Q}_l}^{G_k} \to \mathbf{Rep}_{\mathbb{Q}_l}^{G_K}$ die Koeffizientenerweiterungen aus Beispiel 1.6(i)+(vii) bzw. (vi). Wir definieren Funktoren $F'_k : \mathbf{Var}_{\mathbf{k}}^{\mathrm{Iso}} \to \mathbf{Rep}_{\mathbb{Q}_l}^{G_k}$ und $F'_K : \mathbf{Var}_{\mathbf{K}}^{\mathrm{Iso}} \to \mathbf{Rep}_{\mathbb{Q}_l}^{G_K}$ wie folgt:
Für projektive Varietäten X/k und Y/K sei $F'_k X := \mathrm{H}^i_{\text{ét}}(X \times_k \bar{K}, \mathbb{Q}_l)$ und $F'_K X := \mathrm{H}^i_{\text{ét}}(Y \times_K \bar{K}, \mathbb{Q}_l)$; für Elemente $s \in G_k$, $t \in G_K$ werde die Operation durch $\varphi_X(s) := \mathrm{H}^i_{\text{ét}}(1_X \times \operatorname{Spec} s)$ bzw. $\mathrm{H}^i_{\text{ét}}(1_Y \times \operatorname{Spec} t)$ gegeben. Für einen Isomorphismus $g : X \xrightarrow{\sim} X'$ in $\mathbf{Var}_{\mathbf{k}}^{\mathrm{Iso}}$ setzen wir $F'_k g := \mathrm{H}^i_{\text{ét}}(g \times_k 1_{\bar{K}})^{-1}$, entsprechend für F'_K. Man beachte, daß dadurch die Funktoren F'_k und F'_K kovariant werden!
Für X/k projektiv haben wir einen kanonischen Isomorphismus

$$X_k \times_k \bar{K} \xrightarrow{\tilde{f}_X} X_K \times_K \bar{K},$$

der einen kanonischen Isomorphismus

$$\mathrm{H}^i_{\text{ét}}(X_k \times_k \bar{K}, \mathbb{Q}_l) \cong \mathrm{H}^i_{\text{ét}}(X_K \times_K \bar{K}, \mathbb{Q}_l)$$

und damit eine natürliche Äquivalenz $f' : F'_K F' \to F'' F'_k$ induziert. Das Tripel (F'_k, F'_K, f') definiert dann einen Morphismus von Koeffizientenerweiterungen, was wir uns kurz überlegen wollen:
Seien dazu $Y, Z \in \mathrm{Ob}(\mathbf{Var}_{\mathbf{k}}^{\mathrm{Iso}})$, $g : Y_K \xrightarrow{\sim} Z_K$ und $\bar{s} \in G$ beliebig, sei ferner $s \in G_k$ ein Repräsentant von $\bar{s}$. Offenbar ist das folgende Diagramm kommutativ:

$$\begin{array}{ccc}
Y_K \times_K \bar{K} & \xrightarrow[\sim]{\left((1_Z \times \operatorname{Spec} \bar{s})^{-1} g (1_Y \times \operatorname{Spec} \bar{s})\right) \times 1_{\bar{K}}} & Z_K \times_K \bar{K} \\
\Big\downarrow \tilde{f}_Y \wr & = & \wr \tilde{f}_Z \Big\downarrow \\
Y \times_k \bar{K} & \xrightarrow[(1_Z \times \operatorname{Spec} s)^{-1} (\tilde{f}_Z g \tilde{f_Y}^{-1}) (1_Y \times \operatorname{Spec} s)]{\sim} & Z \times_k \bar{K}
\end{array}$$

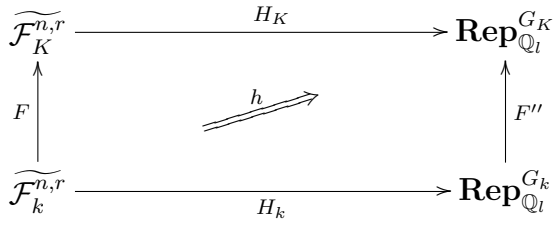
Also erhalten wir:

$$f'F'_K{}^{\bar{s}}g = \left[\mathrm{H}^i_{\text{ét}}\left((1_Z \times \operatorname{Spec} s^{-1})(\tilde{f}_Z g \tilde{f}_Y{}^{-1})(1_Y \times \operatorname{Spec} s)\right)\right]^{-1}$$
$$= \varphi_Z(s)(f'F'_k g)\varphi_Y(s)^{-1} = {}^{\bar{s}}(f'F'_k g).$$

(iii) Seien n, r, i und l wie oben. Wenden wir Bemerkung 3.9 auf die Beispiele (i) und (ii) an und setzen

$$H_k := F'_k F_K, \quad H_K := F'_K F_K, \quad h := (f'F_k)(F'_K f),$$

so erhalten wir den folgenden Morphismus von Koeffizientenerweiterungen:



(iv) Seien $n, r \in \mathbb{N}_+$ natürliche Zahlen, und betrachten wir die Koeffizientenerweiterungen $G : \mathcal{F}_k^{n,r} \to \mathcal{F}_K^{n,r}$ und $F : \widetilde{\mathcal{F}_k^{n,r}} \to \widetilde{\mathcal{F}_K^{n,r}}$ aus 1.6(iv) bzw. (v)! Wir definieren Funktoren $G_k : \mathcal{F}_k^{n,r} \to \widetilde{\mathcal{F}_k^{n,r}}$ und $G_K : \mathcal{F}_K^{n,r} \to \widetilde{\mathcal{F}_K^{n,r}}$ wie folgt: Auf Objekten seien G_k bzw. G_K die Identität, auf Morphismen seien sie durch die kanonischen Surjektionen $\mathrm{GL}(n,k) \twoheadrightarrow \mathrm{PGL}(n,k)$ bzw. $\mathrm{GL}(n,K) \twoheadrightarrow \mathrm{PGL}(n,K)$ gegeben. Dann ist der identische Funktor eine natürliche Transformation von $G_K G$ nach $F G_k$, und das Tripel (G_k, G_K, id) erfüllt offenbar alle Bedingungen eines Morphismusses von Koeffizientenerweiterungen.

3.12 Korollar. Seien $n \geq 2$, $r \geq 1$ und $i \geq 0$ natürliche Zahlen, $l \neq \mathrm{char}(k)$ eine Primzahl und $P \in k[X_1, \ldots, X_n]$ homogen vom Grad r. Sei X die durch P definierte Hyperfläche in $\mathbb{P}_k^{n-1}$. Dann haben wir eine Operation φ der absoluten Galoisgruppe G_k auf der l-adischen étalen Kohomologie von X:

$$\varphi_X : G_k \longrightarrow \mathrm{Aut}_{\mathbb{Q}_l} \underbrace{\mathrm{H}^i_{\text{ét}}(X \times_k \bar{K}, \mathbb{Q}_l)}_{=:V}.$$

Sei nun Q eine K/k-Form von P und $\vartheta[Q] =: [(A_s)] \in \mathrm{H}^1(G, A(P))$ die zugehörige Kohomologieklasse, ferner $Y \subseteq \mathbb{P}_k^{n-1}$ die durch Q definierte Hyperfläche. Wegen $Y_K \cong X_K$ ist die l-adische étale Kohomologie von Y als $\mathbb{Q}_l$-Vektorraum isomorph zu V. Sei φ_Y die zugehörige Galoisoperation auf V. Dann wird φ_Y wie folgt gegeben:

$$\boxed{\varphi_Y : G_k \longrightarrow \mathrm{Aut}_{\mathbb{Q}_l}(V),\ s \mapsto \mathrm{H}^i_{\text{ét}}\left(\widetilde{A_{\bar{s}}}^{-1}\right) \circ \varphi_X(s)} \tag{15}$$

Dabei werde für $s \in G_k$ das Bild in G mit $\bar{s}$ bezeichnet, und $\widetilde{A_{\bar{s}}}$ bezeichne das Element $f(F_k A_{\bar{s}} \times 1_{\bar{K}}) \in \mathrm{Aut}(X \times_k \bar{K})$ (mit den Notationen aus Beispiel 3.11).

Sei nun speziell k ein *endlicher* Körper, $f \in G_k$ der arithmetische Frobenius und $F_X^* := \varphi_X(f)^{-1}$ bzw. $F_Y^* := \varphi_Y(f)^{-1}$ der geometrische Frobenius von X bzw. Y. Dann gilt:

$$\boxed{F_Y^* = \mathrm{H}^i_{\text{ét}}\left(\widetilde{\bar{f}^{-1} A_{\bar{f}}}\right) \circ F_X^*} \tag{16}$$

Beweis: Nach Satz 3.10 gilt $\vartheta[(V,\varphi_Y)] = \left(\mathrm{H}^i_{\text{ét}}(\widetilde{A_{\bar{s}}^{-1}})\right) =: \xi$, woraus nach 3.6 folgt, daß $(V,\varphi_Y) = (V,\varphi_X)(\xi)$ gilt. Das liefert Gleichung (15).
Sei nun k endlich. Wegen (15) haben wir nur zu zeigen, daß $\left(A_{\bar{f}^{-1}}\right)^{-1} = {}^{\bar{f}^{-1}}A_{\bar{f}}$ gilt:

$$1 = A_1 = A_{\bar{f}\bar{f}^{-1}} = A_{\bar{f}}{}^{\bar{f}}A_{\bar{f}^{-1}} \quad\Longrightarrow\quad A_{\bar{f}^{-1}} = {}^{\bar{f}^{-1}}\left(A_{\bar{f}}^{-1}\right) = \left({}^{\bar{f}^{-1}}A_{\bar{f}}\right)^{-1}.$$

q.e.d.

3.13 Beispiel. Es sei in Beispiel 3.11(i) speziell k ein Zahlkörper, $K := \bar{\mathbb{Q}}$, $n := 3$, $r := 3$ und $P_3^3 := X_1^3 + X_2^3 + X_3^3$. In Beispiel 1.6(v) haben wir gesehen, daß P_3^3 in $\widetilde{\mathcal{F}_k^{3,3}}$ isomorph zu $Q' = 12X_1^3 + X_2^2X_3 + 3X_3^3$ ist. Also ist X_3^3, die durch P_3^3 definierte Kurve in $\mathbb{P}_k^2$, isomorph zur elliptischen Kurve mit projektiver Weierstraß-Gleichung Q', d.h. mit affiner Weierstraß-Gleichung $y^2 = -12x^3 - 3$. Diese Kurve hat j-Invariante 0, und bekanntlich sind zwei elliptische Kurven über $\overline{\mathbb{Q}}$ genau dann isomorph, wenn sie dieselbe j-Invariante haben (vgl. [Kna92, S.66]). Es ist also

$$\begin{aligned}\{Y \subset \mathbb{P}_k^2 \,|\, Y \text{ elliptische Kurve mit } j\text{-Invariante } 0\}/k\text{-Isomorphismen}\\ = \left\{\,[Y] \in E(\bar{\mathbb{Q}}/k, X_3^3) \;\middle|\; Y \text{ besitzt einen } k\text{-rationalen Punkt}\right\}.\end{aligned}$$

Korollar 3.12 gestattet es also im Prinzip, bei Kenntnis der G_k-Darstellung $\mathrm{H}^i_{\text{ét}}(\bar{X}_3^3, \mathbb{Q}_l)$ für jede elliptische Kurve Y/k mit j-Invariante 0 die G_k-Darstellung $\mathrm{H}^i_{\text{ét}}(\bar{Y}, \mathbb{Q}_l)$ zu berechnen, d.h. insbesondere die L-Reihe von Y.

3.14 Korollar. Es sei $k = \mathbb{F}_q$ ein endlicher Körper, $n \geq 2$ und $r \geq 1$ natürliche Zahlen, $P \in k[X_1, \ldots, X_n]$ homogen vom Grad r und X die durch P definierte $(n-2)$-dimensionale Hyperfläche in $\mathbb{P}_k^{n-1}$. Weiter sei Q eine K/k-Form von P in $\widetilde{\mathcal{F}_k^{n,r}}$, $\vartheta[Q] =: [(A_s)] \in \mathrm{H}^1(G, A(P))$ die zugehörige Kohomologieklasse und $Y \subseteq \mathbb{P}_k^{n-1}$ die durch Q definierte Hyperfläche.
Wir betrachten den geometrischen Frobenius

$$F_X \,:\, X_{\bar{K}} \longrightarrow X_{\bar{K}}, \quad (x_1 : \ldots : x_n) \mapsto (x_1^q : \ldots : x_n^q)$$

und den Automorphismus $a := \widetilde{{}^{\bar{f}^{-1}}A_{\bar{f}}}$ von $X_{\bar{K}}$, wobei $f \in G_k$ wieder den arithmetischen Frobenius bezeichne (zur Notation vgl. 3.12!).
Dann hat der Morphismus $F_X a : X_{\bar{K}} \to X_{\bar{K}}$ nur isolierte Fixpunkte, und deren Anzahl ist gleich $\#Y(k)$, der Anzahl der k-rationalen Punkte von Y:

$$\boxed{\#\left\{x \in X(\bar{K}) \;\middle|\; F_X a(x) = x\right\} = \#Y(k) = \frac{\#\left\{x \in k^n \;\middle|\; Q(x) = 0\right\} - 1}{q-1}} \qquad (17)$$

Beweis: Offenbar verschwindet das Differential dF_X, d.h. $1 - d(F_X a) = 1$, woraus folgt, daß die Fixpunkte von $F_X a$ isoliert sind und daß ihre Anzahl N mit der Lefschetzschen Spurformel berechnet werden kann (vgl. [Har93, S.453]!):

$$N = \sum_{i=0}^{2n-2} (-1)^i \cdot \mathrm{Tr}\left[(F_X a)^* \,\middle|\, \mathrm{H}^i_{\text{ét}}\,(X_{\bar{K}}, \mathbb{Q}_l) \right],$$

wobei l eine Primzahl ungleich p sei. Nun ist $(F_X a)^* = a^* F_X^*$, was keinen Bezeichnungskonflikt mit dem in 3.12 auftretenden F_X^* darstellt, weil bekanntlich (vgl. [Mil80, S.292,13.5.]!) F_X in der Kohomologie als Inverses des arithmetischen Frobenius operiert, so daß wir nach (16) $(Fa)^* = F_Y^*$ erhalten, was aus demselben Grund die Kohomologie des geometrischen Frobenius $F_Y : Y_{\bar{K}} \to Y_{\bar{K}}$ ist. Jetzt wenden wir die Lefschetzsche Spurformel in der anderen Richtung an und erhalten

$$\begin{aligned} N &= \sum_{i=0}^{2n-2} (-1)^i \cdot \mathrm{Tr}\left[(F_X a)^* \,\middle|\, \mathrm{H}^i_{\text{ét}}\,(X_{\bar{K}}, \mathbb{Q}_l) \right] \\ &= \sum_{i=0}^{2n-2} (-1)^i \cdot \mathrm{Tr}\left[F_Y^* \,\middle|\, \mathrm{H}^i_{\text{ét}}\,(Y_{\bar{K}}, \mathbb{Q}_l) \right] = \#\Big\{ x \in Y(\bar{K}) \,\Big|\, F_Y(x) = x \Big\}, \end{aligned}$$

und die Anzahl der Fixpunkte des geometrischen Frobenius ist ja gerade die Anzahl der k-rationalen Punkte (vgl. [Mil80, S.186]!). **q.e.d.**

3.15 Korollar. Es seien k, n, r und P wie in 3.14, aber jetzt werde P als Objekt der Kategorie $\mathcal{F}_k^{n,r}$ aufgefaßt; $\tilde{X}$ sei die durch P definierte $(n-1)$-dimensionale **affine** Hyperfläche in $\mathbb{A}_k^n$. Weiter sei Q eine K/k-Form von P in $\mathcal{F}_k^{n,r}$, $\vartheta[Q] =: [(A_s)] \in \mathrm{H}^1(G, A(P))$ die zugehörige Kohomologieklasse und $\tilde{Y} \subseteq \mathbb{A}_k^n$ die durch Q definierte Hyperfläche.

Wieder betrachten wir den geometrischen Frobenius

$$F_{\tilde{X}} \,:\, \tilde{X}_{\bar{K}} \longrightarrow \tilde{X}_{\bar{K}}, \quad (x_1, \ldots, x_n) \mapsto (x_1^q, \ldots, x_n^q)$$

und den Automorphismus $\tilde{a} := \widetilde{f^{-1} A_{\bar{f}}}$ von $\tilde{X}_{\bar{K}}$, der in analoger Weise wie in 3.12 bzw. 3.14 definiert sei.

Dann ist die Anzahl der Fixpunkte von $F_{\tilde{X}} \tilde{a} : \tilde{X}_{\bar{K}} \to \tilde{X}_{\bar{K}}$ gleich $\#\tilde{Y}(k)$, der Anzahl der k-rationalen Punkte von $\tilde{Y}$:

$$\boxed{\#\Big\{ x \in \tilde{X}(\bar{K}) \,\Big|\, F_{\tilde{X}} \tilde{a}(x) = x \Big\} = \#\tilde{Y}(k) = \#\Big\{ x \in k^n \,\Big|\, Q(x) = 0 \Big\}} \tag{18}$$

Beweis: Wir wollen die Abbildung

$$\begin{array}{rccc} f: & \Big\{ x \in \tilde{X}(\bar{K}) \,\Big|\, F_{\tilde{X}} \tilde{a}(x) = x \Big\} \setminus \{0\} & \longrightarrow & \Big\{ x \in X(\bar{K}) \,\Big|\, F_X a(x) = x \Big\} \\ & (x_1, \ldots, x_n) & \mapsto & (x_1 : \ldots : x_n) \end{array}$$

betrachten, wobei X, F_X und a wie in 3.14 definiert seien, wenn man P als Objekt von $\widetilde{\mathcal{F}_k^{n,r}}$ auffaßt. Die Wohldefiniertheit von f folgt aus der offensichtlichen Tatsache, daß das

folgende Diagramm von Varietäten über $\bar{K}$ kommutiert:

$$\begin{array}{ccc} \tilde{X}_{\bar{K}} \setminus \{0\} & \xrightarrow{F_{\tilde{X}}\tilde{a}} & \tilde{X}_{\bar{K}} \setminus \{0\} \\ \downarrow{\scriptstyle p} & = & \downarrow{\scriptstyle p} \\ X_{\bar{K}} & \xrightarrow[F_X]{} & X_{\bar{K}} \end{array}$$

wobei p den Morphismus bezeichne, der $(x_1, \ldots, x_n)$ auf $(x_1 : \ldots : x_n)$ abbildet. Wie behaupten, daß f *surjektiv* ist:

Sei dazu $(x_1 : \ldots : x_n)$ ein Fixpunkt von $F_X a$. Es gibt dann also ein $\lambda \in \bar{K}^\times$ mit

$$F_{\tilde{X}}\tilde{a}(x_1, \ldots, x_n) = (\lambda x_1, \ldots, \lambda x_n). \tag{19}$$

Weil $\tilde{a}$ ein linearer Automorphismus ist, gilt für beliebiges $\mu \in \bar{K}^\times$:

$$\begin{aligned} F_{\tilde{X}}\tilde{a}(\mu x_1, \ldots, \mu x_n) &= \mu^q \cdot F_{\tilde{X}}\tilde{a}(x_1, \ldots, x_n) \\ &\overset{(19)}{=} \mu^q \lambda \cdot (x_1, \ldots, x_n) = \mu^{q-1}\lambda \cdot (\mu x_1, \ldots, \mu x_n). \end{aligned} \tag{20}$$

Da $\bar{K}$ algebraisch abgeschlossen ist, können wir ein $\mu \in \bar{K}^\times$ finden mit $\mu^{q-1}\lambda = 1$. Setzen wir dieses μ in (20) ein, so sehen wir, daß $x := (\mu x_1, \ldots, \mu x_n)$ ein Fixpunkt von $F_{\tilde{X}}\tilde{a}$ ist, d.h. x ist ein Urbild von $(x_1 : \ldots : x_n)$ unter f. Die Surjektivität von f ist damit bewiesen.

Als nächstes zeigen wir, daß jeder Fixpunkt $(x_1 : \ldots : x_n)$ von $F_X a$ genau $q - 1$ Urbilder hat. Wegen der Surjektivität von f, die wir soeben bewiesen haben, gibt es zumindest ein Urbild — sei ohne Beschränkung der Allgemeinheit $(x_1, \ldots, x_n)$ ein solches Urbild. Alle anderen Urbilder sind dann offenbar von der Gestalt $(\mu x_1, \ldots, \mu x_n)$ für $\mu \in \bar{K}^\times$. Andererseits müssen solche Elemente Fixpunkte unter $F_{\tilde{X}}\tilde{a}$ sein:

$$F_{\tilde{X}}\tilde{a}(\mu x_1, \ldots, \mu x_n) = \mu^q \cdot F_{\tilde{X}}\tilde{a}(x_1, \ldots, x_n) = \mu^q \cdot (x_1, \ldots, x_n) \overset{!}{=} (\mu x_1, \ldots, \mu x_n),$$

d.h. es muß gelten $\mu^q = \mu$, was äquivalent zu $\mu \in k$ ist. Es folgt, daß genau die $\mu \in k^\times$ Urbilder liefern, d.h. es gibt genau $\#(k^\times) = q - 1$ Urbilder von $(x_1 : \ldots : x_n)$ unter f — genau, wie wir behauptet haben.

Wir wissen also jetzt, daß f surjektiv ist, und wir kennen die Kardinalität der Fasern, so daß wir die Kardinalität der Quelle und somit die Anzahl der Fixpunkte von $F_{\tilde{X}}\tilde{a}$ berechnen können:

$$\begin{aligned} \#\left\{x \in \tilde{X}(\bar{K}) \,\middle|\, F_{\tilde{X}}\tilde{a}(x) = x\right\} &= 1 + (q-1)\#\left\{x \in X(\bar{K}) \,\middle|\, F_X a(x) = x\right\} \\ &\overset{(17)}{=} 1 + (q-1)\#Y(k) = \#\tilde{Y}(k). \end{aligned}$$

q.e.d.

4 Spezielle Projektoren

Nachdem wir in den letzten Kapiteln die Methode des Galois-Descents entwickelt haben, wenden wir uns nun einer weiteren „Zutat“ zu, die wir später zur Berechnung der Kohomologie von getwisteten Fermathyperflächen brauchen werden:

In der Einleitung haben wir erwähnt, daß man aus der Tatsache, daß das Kranzprodukt $S_n \int \mu_m$ auf der Fermathyperfläche X_n^m operiert, auf die Zerlegung der l-adischen Kohomologie von X_n^m in Eigenräume schließen kann, die zu den Charakteren der abelschen Gruppe μ_m^n korrespondieren.

In diesem Kapitel werden wir allgemeiner die Situation untersuchen, daß ein semidirektes Produkt $A \rtimes S$ zweier endlicher Gruppen auf einem Objekt M einer pseudoabelschen Kategorie operiert, und zeigen, daß man auch dann eine Zerlegung von M in die direkte Summe von Eigenräumen M_χ zu den Charakteren χ von A hat.

So sehen wir, daß die Zerlegung von $H^*_{\text{ét}}(\bar{X}_n^m, \mathbb{Q}_l)$ in Eigenräume eine „motivische“ Zerlegung ist, d.h. sie ist die l-adische Realisierung der entsprechenden Zerlegung des Grothendieck-Motivs $h(X_n^m)$ von X_n^m.

4.1 Lemma/ Definition. Seien S eine Gruppe und A eine endliche, abelsche S-Gruppe. Dann ist auch die duale abelsche Gruppe $\check{A}$ eine S-Gruppe via

$$\forall s \in S : \forall \chi \in \check{A} : \forall a \in A : \ {}^s\chi(a) := \chi({}^{s^{-1}}a).$$

Beweis: Seien $s \in S$ und $\chi \in \check{A}$ beliebig. Dann ist auch ${}^s\chi \in \check{A}$, denn für $a, b \in A$ gilt:

$${}^s\chi(ab) = \chi({}^{s^{-1}}(ab)) = \chi({}^{s^{-1}}a\,{}^{s^{-1}}b) = \chi({}^{s^{-1}}a)\chi({}^{s^{-1}}b) = {}^s\chi(a)\,{}^s\chi(b).$$

Sei nun zusätzlich $t \in S$ beliebig, dann gilt

$${}^{st}\chi(a) = \chi({}^{t^{-1}s^{-1}}a) = {}^t\chi({}^{s^{-1}}a) = {}^s\big({}^t\chi\big)(a),$$

d.h. es gilt ${}^{st}\chi = {}^s({}^t\chi)$, woraus folgt, daß es sich tatsächlich um eine Links-S-Operation handelt. **q.e.d.**

4.2 Lemma/ Definition. Es seien A eine endliche, abelsche Gruppe der Ordnung n mit Exponent m und $R \subseteq \mathbb{C}$ ein Ring, der die m-ten Einheitswurzeln enthält und in dem n invertierbar ist. Sei $\chi \in \check{A}$ ein Charakter (der dann automatisch über R faktorisiert). Definiere

$$p_\chi := \frac{1}{n} \sum_{a \in A} \chi(a)^{-1} a \in R[A].$$

Dann bilden die $(p_\chi)_{\chi \in \check{A}}$ ein vollständiges System von Idempotenten in $R[A]$, d.h.

$$\forall \chi, \psi \in \check{A} : \ p_\chi p_\psi = \begin{cases} 1 & \text{falls } \chi = \psi \\ 0 & \text{sonst} \end{cases}, \quad \text{und} \ \sum_{\chi \in \check{A}} p_\chi = 1 \in R[A].$$

Beweis: Das folgt aus der allgemeineren Aussage für beliebige endliche Gruppen in [Lan93, S.675f]. **q.e.d.**

4.3 Lemma. Seien S eine Gruppe, A eine endliche, abelsche S-Gruppe der Ordnung n mit Exponent m und $A \rtimes S$ das semidirekte Produkt von S mit A (so definiert, daß $sas^{-1} = {}^s a$ für $a \in A$ und $s \in S$). Sei wieder $R \subseteq \mathbb{C}$ ein Ring, in dem n invertierbar ist und der die m-ten Einheitswurzeln enthält. Via $R[A] \hookrightarrow R[A \rtimes S]$ fassen wir die in 4.2 definierten Idempotenten als Elemente in $R[A \rtimes S]$ auf. Dann gilt für alle $s \in S$, $b \in A$ und $\chi \in \check{A}$:

$$s \cdot p_\chi = p_{{}^s\chi} \cdot s \quad \text{und} \quad b \cdot p_\chi = \chi(b) \cdot p_\chi.$$

Beweis:

$$\begin{aligned} s \cdot p_\chi &= s \cdot \frac{1}{n} \sum_{a \in A} \chi(a)^{-1} a = \frac{1}{n} \sum_{a \in A} \chi(a)^{-1} sa = \frac{1}{n} \sum_{a \in A} \chi(a)^{-1} [{}^s a] \cdot s \\ &= \frac{1}{n} \sum_{a \in A} \chi({}^{s^{-1}}[{}^s a])^{-1} [{}^s a] \cdot s = \frac{1}{n} \sum_{a \in A} {}^s\chi([{}^s a])^{-1} [{}^s a] \cdot s = \frac{1}{n} \sum_{a \in A} {}^s\chi(a)^{-1} a \cdot s \\ &= p_{{}^s\chi} \cdot s. \end{aligned}$$

$$\begin{aligned} b \cdot p_\chi &= \frac{1}{n} \sum_{a \in A} \chi(a)^{-1} [ba] = \frac{1}{n} \sum_{a \in A} \chi(b^{-1}[ba])^{-1} [ba] = \frac{1}{n} \sum_{a \in A} \chi(b) \cdot \chi([ba])^{-1} [ba] \\ &= \frac{1}{n} \sum_{a \in A} \chi(b) \cdot \chi(a)^{-1} a = \chi(b) \cdot p_\chi. \end{aligned}$$

q.e.d.

4.4 Korollar. Es seien alle Bezeichnungen wie in 4.3, ferner sei $\psi \in \check{A}$ beliebig. Dann gilt:

$$R[A \rtimes S] \ni p_\psi \cdot s \cdot p_\chi = \begin{cases} p_\psi \cdot s & \text{falls } \psi = {}^s\chi \\ 0 & \text{sonst} \end{cases} \quad \text{und}$$

$$p_\psi \cdot b \cdot p_\chi = \begin{cases} \chi(b) \cdot p_\chi & \text{falls } \psi = \chi \\ 0 & \text{sonst.} \end{cases}$$

Beweis: Klar nach 4.2 und 4.3! **q.e.d.**

4.5 Korollar. Seien A, S und R wie in Lemma 4.4, seien $\boldsymbol{\mathcal{M}}$ eine pseudoabelsche, R-lineare Kategorie und $M \in \mathrm{Ob}(\boldsymbol{\mathcal{M}})$ ein Objekt, auf dem $A \rtimes S$ *von rechts* operiert. $A = A^{\mathrm{opp}} \to \mathrm{Aut}(M)$ induziert $R[A] \to \mathrm{End}(M)$, d.h. wir können für $\chi \in \check{A}$ das Idempotente

p_χ als Projektor in $\mathrm{End}(M)$ auffassen — sei M_χ der durch p_χ herausgeschnittene Teil, dann gilt

$$M = \bigoplus_{\chi \in \check{A}} M_\chi.$$

Sind $s \in S$, $b \in A$ und $\chi \in \check{A}$ beliebig, so haben wir die folgenden beiden kommutativen Diagramme, die die Zerlegung der Automorphismen s und b auf M bezüglich der Zerlegung von M in die M_χ beschreiben:

$$\begin{array}{ccc} M_{{}^s\chi} & \xrightarrow{p_\chi \cdot s \cdot p_{{}^s\chi}} & M_\chi \\ \downarrow & = & \downarrow \\ M & \xrightarrow[s]{} & M \end{array} \qquad \begin{array}{ccc} M_\chi & \xrightarrow{\chi(b)} & M_\chi \\ \downarrow & = & \downarrow \\ M & \xrightarrow[b]{} & M \end{array}$$

Beweis: Die Zerlegung von M in die direkte Summe der M_χ folgt sofort aus 4.2, das rechte Diagramm folgt aus dem zweiten Teil von Lemma 4.4.

Die Komposition von Gruppenhomomorphismen

$$A \rtimes S \xrightarrow{x \mapsto x^{-1}} (A \rtimes S)^{\mathrm{op}} \to \mathrm{Aut}(M)$$

induziert einen Ringhomomorphismus

$$\varphi : R[A \rtimes S] \longrightarrow \mathrm{End}(M),$$

und per definitionem gilt $\varphi(p_{\chi^{-1}}) = p_\chi$ für $\chi \in \check{A}$ und $\varphi(s^{-1}) = s$ für $s \in S$. Nach Lemma 4.4 ist für $\chi, \psi \in \check{A}$ und $s \in S$ das Element $p_{\psi^{-1}} \cdot s^{-1} \cdot p_{\chi^{-1}}$ höchstens dann ungleich null, wenn $\psi^{-1} = {}^{(s^{-1})}(\chi^{-1})$ gilt, aber

$$\psi^{-1} = {}^{(s^{-1})}(\chi^{-1}) \quad \Longleftrightarrow \quad {}^s(\psi^{-1}) = \chi^{-1} \quad \Longleftrightarrow \quad \chi = {}^s\psi.$$

Also erhalten wir:

$$\mathrm{End}(M) \ni p_\psi \cdot s \cdot p_\chi = \varphi(p_{\psi^{-1}} \cdot s^{-1} \cdot p_{\chi^{-1}}) = \begin{cases} p_\psi \cdot s & \text{, falls } \chi = {}^s\psi \\ 0 & \text{, sonst} \end{cases}.$$

q.e.d.

4.6 Lemma/ Definition. Seien die Notationen wie in Korollar 4.5, und sei $\chi \in \check{A}$ beliebig. Bezeichne $[\chi] \subseteq \check{A}$ den Orbit von χ unter der Aktion von S aus 4.1. Setze

$$M_{[\chi]} := \bigoplus_{\chi \in [\chi]} M_\chi.$$

(Dann ist also $M_{[\chi]}$ der von dem Projektor $p_{[\chi]} := \sum_{\chi \in [\chi]} p_\chi$ herausgeschnittene Teil.) Aus Korollar 4.5 folgt offenbar, daß $A \rtimes S$ auf $M_{[\chi]}$ operiert. Ist also $\check{A} = [\chi_1] \sqcup \ldots \sqcup [\chi_r]$ eine disjunkte Zerlegung in Orbiten, so ist

$$M = M_{[\chi_1]} \oplus \ldots \oplus M_{[\chi_r]}$$

eine Zerlegung von M in $(A \rtimes S)$-invariante Unterobjekte.

Beweis: Klar! **q.e.d.**

4.7 Beispiele. Seien A und S wie oben, sei m ein Exponent von A und $\zeta \in \mathbb{C}$ eine primitive m-te Einheitswurzel. Sei k ein Körper, G_k die absolute Galoisgruppe und X/k eine glatte, projektive Varietät, auf der $A \rtimes S$ von links operiert.

(i) Sei $\boldsymbol{\mathcal{M}}$ die Kategorie $\boldsymbol{\mathcal{M}_k^E}$ der Grothendieck-Motive über k mit Koeffizienten in E, und sei $h(X)$ das Motiv zu X. Per Funktoralität operiert dann $A \rtimes S$ von rechts auf $h(X)$, und wir erhalten gemäß Korollar 4.5 eine Zerlegung

$$h(X) = \bigoplus_{\chi \in \check{A}} h(X)_\chi.$$

(ii) Sei $l \neq \mathrm{char}(k)$ eine Primzahl mit $l \equiv 1 \pmod{m}$ und $i \in \mathbb{N}_0$ eine natürliche Zahl. Nach Hensels Lemma enthält $\mathbb{Q}_l$ dann die m-ten Einheitswurzeln, d.h. nach Auswahl einer primitiven m-ten Einheitswurzel erhalten wir eine Einbettung $\mathbb{Q}(\zeta) \hookrightarrow \mathbb{Q}_l$, durch die $\boldsymbol{\mathcal{M}} := \mathbf{Rep}_{\mathbb{Q}_l}^{G_k}$ eine $\mathbb{Q}(\zeta)$-lineare (pseudo-)abelsche Kategorie wird. Bezeichnet $V \in \mathrm{Ob}(\boldsymbol{\mathcal{M}})$ die $\mathbb{Q}_l$-G_k-Darstellung $\mathrm{H}^i_{\text{ét}}(X \times_k \bar{k}, \mathbb{Q}_l)$, so operiert $A \rtimes S$ per Funktoralität von rechts auf V. Aus Korollar 4.5 folgt dann, daß sich V in eine direkte Summe von $\mathbb{Q}_l$-G_k-Darstellungen V_χ zerlegt, wobei gerade gilt:

$$V_\chi = \{v \in V \mid \forall a \in A : \; v \cdot a = \chi(a) \cdot v\}.$$

4.8 Lemma. Seien S, A, n, m und R wie in 4.4, sei $\boldsymbol{\mathcal{M}}$ eine pseudoabelsche, R-lineare Kategorie und $M, N \in \mathrm{Ob}(\boldsymbol{\mathcal{M}})$ Objekte, auf denen A operiert. Sei ferner $f \in \mathrm{Mor}_{\mathcal{M}}(M, N)$ ein A-äquivarianter Morphismus und $\chi \in \check{A}$ ein beliebiger Charakter. Dann kommutiert das folgende Diagramm A-äquivarianter Morphismen:

$$\begin{array}{ccc} M_\chi & \xrightarrow{p_\chi \circ f \circ p_\chi} & N_\chi \\ \downarrow & = & \downarrow \\ M & \xrightarrow[f]{} & N \end{array}$$

Ist zusätzlich S eine beliebige Gruppe und A eine S-Gruppe und operiert $A \rtimes S$ von rechts so auf M und N, daß f sogar $(A \rtimes S)$-äquivariant ist, dann kommutiert das folgende Diagramm $(A \rtimes S)$-äquivarianter Morphismen:

$$\begin{array}{ccc} M_{[\chi]} & \xrightarrow{p_{[\chi]} \circ f \circ p_{[\chi]}} & N_{[\chi]} \\ \downarrow & = & \downarrow \\ M & \xrightarrow[f]{} & N \end{array}$$

Beweis: Klar wegen

$$f \circ p_\chi = f \circ \left(\frac{1}{n} \sum_{a \in A} \chi(a)^{-1} a \right) = \frac{1}{n} \sum_{a \in A} \chi(a)^{-1} (f \circ a) =$$
$$\frac{1}{n} \sum_{a \in A} \chi(a)^{-1} (a \circ f) = \left(\frac{1}{n} \sum_{a \in A} \chi(a)^{-1} a \right) \circ f = p_\chi \circ f.$$

q.e.d.

4.9 Lemma. Seien S, A, n, m und R wie in 4.4, sei B ein Quotient von A via $A \xrightarrow{\varphi} B \to 0$ und $\chi \in \check{B}$ ein beliebiger Charakter sowie $\varphi^* \chi \in \check{A}$ der auf A zurückgezogene Charakter. Dann wird unter der durch φ induzierten Abbildung $R[A] \xrightarrow{\varphi_*} R[B]$ das Idempotente $p_{\varphi^* \chi}$ auf das Idempotente p_χ abgebildet.

Beweis: Es sei $C := \ker \varphi$ und $\mathcal{B} \subseteq A$ ein Repräsentantensystem von B. Es ergibt sich:

$$\varphi_* p_{\varphi^* \chi} = \varphi_* \left(\frac{1}{n} \sum_{a \in A} \chi(\varphi a)^{-1} a \right) = \frac{1}{n} \sum_{a \in A} \chi(\varphi a)^{-1} \varphi a =$$
$$\frac{1}{n} \sum_{c \in C} \sum_{b \in \mathcal{B}} \chi(\varphi(cb))^{-1} \varphi(cb) = \frac{\#C}{n} \sum_{b \in \mathcal{B}} \chi(\varphi b)^{-1} \varphi b = \frac{1}{\#B} \sum_{b \in B} \chi(b)^{-1} b = p_\chi.$$

q.e.d.

4.10 Korollar. Seien S, A, n, m, R und $\boldsymbol{\mathcal{M}}$ wie in 4.8 und $N \in \mathrm{Ob}(\boldsymbol{\mathcal{M}})$ ein Objekt, auf dem A operiert. Ferner sei B ein Quotient von A via $A \xrightarrow{\varphi} B \to 0$ und $M \in \mathrm{Ob}(\boldsymbol{\mathcal{M}})$ ein Objekt, auf dem B operiert. Sei schließlich ein Morphismus $f \in \mathrm{Mor}_{\mathcal{M}}(M, N)$ gegeben mit der Eigenschaft, daß für alle $a \in A$ das folgende Diagramm kommutativ ist:

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle \varphi(a)}\downarrow & = & \downarrow{\scriptstyle a} \\ M & \xrightarrow[f]{} & N \end{array}$$

Sei nun $\chi \in \check{B}$ ein beliebiger Charakter und $\varphi^* \chi \in \check{A}$ der auf A zurückgezogene Charakter. Bezeichne M_χ den durch $p_\chi \in R[B] \hookrightarrow \mathrm{End}\,(M)$ aus M herausgeschnittenen Teil, dann ist das folgende Diagramm kommutativ (mit A-äquivarianten Morphismen bezüglich der durch φ auf M induzierten Operation):

$$\begin{array}{ccc} M_\chi & \xrightarrow{p_{\varphi^* \chi} \circ f \circ p_\chi} & N_{\varphi^* \chi} \\ \downarrow & = & \downarrow \\ M & \xrightarrow[f]{} & N \end{array}$$

Sei zusätzlich S eine beliebige Gruppe, die so auf A operiert, daß $\ker\varphi$ invariant ist. Dann gibt es genau eine Operation von S auf B, die φ zu einem S-äquivarianten Morphismus macht, wodurch ein kanonischer Morphismus $A \rtimes S \xrightarrow{\varphi_*} B \rtimes S$ induziert wird. Operiert $A \rtimes S$ von rechts so auf N und M (dort via φ_*), daß f sogar $(A \rtimes S)$-äquivariant ist, dann kommutiert das folgende Diagramm $(A \rtimes S)$-äquivarianter Morphismen:

$$\begin{array}{ccc} M_{[\chi]} & \xrightarrow{p_{[\varphi^*\chi]} \circ f \circ p_{[\chi]}} & N_{[\varphi^*\chi]} \\ \downarrow & = & \downarrow \\ M & \xrightarrow[f]{} & N \end{array}$$

Beweis: Klar nach 4.8 und 4.9! **q.e.d.**

5 Formen der Fermatgleichung in $\mathcal{F}_k^{n,m}$

Es seien $m, n \geq 1$ natürliche Zahlen, k ein Körper mit $(\operatorname{char} k) \nmid m!$, $K := \bar{k}$ ein separabler algebraischer Abschluß von k und $G := \operatorname{Gal}(K/k)$ die absolute Galoisgruppe. Setze $P_n^m := X_1^m + \ldots + X_n^m \in k[X_i]$. — P_n^m ist also ein Objekt aus $\mathcal{F}_k^{n,m}$ und aus $\widetilde{\mathcal{F}_k^{n,m}}$, wir wollen es in diesem Kapitel aber nur als Objekt von $\mathcal{F}_k^{n,m}$ auffassen und in dieser Kategorie die K/k-Formen von P_n^m bestimmen.

Wie wir aus dem dritten Kapitel wissen, müssen wir zunächst die Automorphismengruppe $A(P_n^m)$ berechnen, bevor wir die Descent-Methode anwenden können:

5.1 Lemma/ Definition. Seien $r \in \mathbb{N}_+$ eine positive natürliche Zahl, R ein kommutativer Ring mit Eins und $A \subseteq R^\times$ eine Untergruppe der multiplikativen Gruppe von R. Dann wird durch

$$\begin{array}{rcl} S_r \int A & \longrightarrow & \mathrm{GL}(r,R) \\ (a_i)_i \cdot \sigma & \mapsto & \big(a_i \cdot \delta_{i,\sigma(j)}\big)_{i,j} \end{array}$$

ein injektiver Gruppenhomomorphismus aus dem Kranz-Produkt von S_r mit A (vgl. 2.15!) in die Gruppe der regulären $r \times r$-Matrizen über R definiert. (Dabei werden die Elemente aus S_r gerade als Permutationsmatizen, die Elemente aus A^r als Diagonalmatrizen nach $\mathrm{GL}(r,R)$ eingebettet.)

Beweis: Die Abbildung werde mit f bezeichnet!

- *multiplikativ:* Seien $(a_i)_i \cdot \sigma$ und $(b_i)_i \cdot \tau$ aus $S_r \int A$ beliebig. Dann ergibt sich:

$$\begin{array}{rcl} & & f\big((a_i)_i \cdot \sigma\big) \cdot f\big((b_i)_i \cdot \tau\big) \\ &=& \big(a_i \cdot \delta_{i,\sigma(k)}\big)_{i,k} \cdot \big(b_k \cdot \delta_{k,\tau(j)}\big)_{k,j} \;=\; \big(\textstyle\sum_{k=1}^r a_i \cdot \delta_{i,\sigma(k)} \cdot b_k \cdot \delta_{k,\tau(j)}\big)_{i,j} \\ &=& \big(a_i \cdot \delta_{i,\sigma\tau(j)} \cdot b_{\tau(j)}\big)_{i,j} \;=\; \big(a_i b_{\sigma^{-1}(i)} \cdot \delta_{i,\sigma\tau(j)}\big)_{i,j} \\ &=& f\big((a_i b_{\sigma^{-1}(i)})_i \cdot \sigma\tau\big) \;=\; f\big([(a_i)_i \cdot \sigma] \cdot [(b_i)_i \cdot \tau]\big). \end{array}$$

- *wohldefiniert:* Offenbar gilt $f((1,\ldots,1)\cdot\mathrm{id}) = E_r$, woraus mit Hilfe der soeben bewiesenen Multiplikativität folgt, daß f ein wohldefinierter Gruppenhomomorphismus ist.

- *injektiv:* Klar, denn aus $f((a_i)_i \cdot \sigma) = E_r$ folgt zunächst $\sigma = \mathrm{id}$ und dann sofort $(a_i)_i = (1,\ldots,1)$!

q.e.d.

5.2 Satz. Ist $m \geq 3$, so gilt

$$\operatorname{Aut}_{\mathcal{F}_K^{n,m}}(P_n^m) = S_n \int \mu_m \subseteq \mathrm{GL}(n,K),$$

wobei $S_n \int \mu_m$, das Kranz-Produkt der symmetrischen Gruppe S_n mit der Gruppe μ_m der m-ten Einheitswurzeln in K, wie in 5.1 beschrieben nach $\mathrm{GL}(n,K)$ eingebettet sei.

Beweis: Siehe [Shi88]! **q.e.d.**

5.3 Lemma. Das Kranz-Produkt $S_n \int \mu_m$ ist nach 2.16 eine diskrete G-Gruppe. Ist $m \geq 3$ (und also $S_n \int \mu_m = \mathrm{Aut}_K(P_n^m)$ nach 5.2), so stimmt die dort definierte G-Operation mit der in Beispiel 1.6(iv) definierten und nach Beispiel 3.5(ii) stetigen Operation überein.

Beweis: Sei also $m \geq 3$! Für jede Operation von G auf $S_n \int \mu_m$ muß ${}^s((\mu_i)_i \cdot \sigma) = {}^s(\mu_i)_i \cdot {}^s\sigma$ gelten, und nach Gleichung (4) operiert G auf $\mathrm{GL}(n, K)$ durch Operation auf den Matrixeinträgen, woraus ${}^s(\mu_i)_i = ({}^s\mu_i)_i$ und ${}^s\sigma = \sigma$ folgt, da das Bild von σ in $\mathrm{GL}(n, K)$ eine Permutationsmatrix mit Einträgen aus $\{0, 1\}$, also insbesondere aus k, ist und σ demnach fix unter der Galois-Operation ist. **q.e.d.**

Nachdem wir $A(P_n^m)$ bestimmt haben, werden wir uns nun mit Hilfe der Methoden aus dem zweiten Kapitel an die Berechnung der Kohomologie $H^1_{\mathrm{cont}}(G, A(P_n^m))$ machen, um die Ergebnisse des dritten Kapitels anwenden zu können.

5.4 Lemma/ Definition. Es sei $c \in Z^1_{\mathrm{cont}}(G, S_n)$. Dann werden in 2.29 (indem wir $A := K^\times$ bzw. $A := \mu_m$ setzen) die diskreten G-Moduln $(K^\times)_c^n$ und $(\mu_m)_c^n$ definiert, und die folgende kurze exakte Sequenz ist exakt in der Kategorie der diskreten G-Moduln:

$$1 \longrightarrow (\mu_m)_c^n \longrightarrow (K^\times)_c^n \xrightarrow{m} (K^\times)_c^n \longrightarrow 1.$$

Beweis: Die Sequenz ist einfach die n-fache Summe der wohlbekannten Kummersequenz, und man sieht sofort, daß alle Morphismen G-äquivariant sind. **q.e.d.**

5.5 Lemma. (Hilbert 90)
Es sei $c \in Z^1_{\mathrm{cont}}(G, S_n)$ beliebig. Dann gilt:

$$H^1_{\mathrm{cont}}(G, (K^\times)_c^n) = 0.$$

Diese Aussage stimmt auch, wenn K eine beliebige Galoiserweiterung von k mit Galoisgruppe G und kein separabler algebraischer Abschluß ist, und wir werden sie für diesen etwas allgemeineren Fall beweisen.

Beweis: Wir befinden uns in der Situation von 2.29 und wollen alle dort vorgenommenen Identifizierungen vornehmen. Insbesondere wird c also durch eine (bis auf k-Isomorphie eindeutig bestimmte) endliche, kommutative, separable k-Algebra L vom Grad n über k gegeben, wir setzen $M := \mathrm{Hom}_k(L, K)$ und identifizieren S_n mit $\mathrm{Aut}\,(M)$.

Wegen 2.30 und 2.10 können wir ohne Beschränkung der Allgemeinheit annehmen, daß L ein Körper ist.

- *1. Fall:* $k = \mathbb{F}_q$, $K = L = \mathbb{F}_{q^n}$.
  Hier gilt also $G = \langle F \rangle = \langle 1, F, \ldots, F^{n-1} \rangle$, wobei F für den Frobenius stehe, und wegen $K = L$ und L/k galoissch ist $M := \mathrm{Hom}_k(L, K) = G$. Sei $(a_s)_s \in Z^1(G, (K^\times)_c^n)$ beliebig, und sei $a_F = (x_\varphi)_{\varphi \in M}$. Nach 2.9 gilt

$$1 = \prod_{j=0}^{n-1} {}^{F^j} a_F = \left(\prod_{j=0}^{n-1} {}^{F^j} x_{F^{-j}\varphi} \right)_{\varphi \in M} = \left(\prod_{j=0}^{n-1} x_{F^{-j}\varphi}^{q^j} \right)_{\varphi \in M}.$$

  Speziell folgt für $\varphi = F^0 = \mathrm{id}$:

$$1 = \prod_{j=0}^{n-1} x_{F^{-j}}^{q^j} = \prod_{j=0}^{n-1} x_{F^j}^{q^j}. \tag{21}$$

  Setze nun

$$b := (b_{F^0}, \ldots, b_{F^{n-1}}) := \left(\prod_{j=1}^{i} x_{F^j}^{-q^{i-j}} \right)_{F^i \in M}.$$

  Für $i \in \{1, \ldots, n-1\}$ folgt zunächst

$$(b^{-1} \cdot {}^F b)_{F^i} = b_{F^i}^{-1} \cdot b_{F^{i-1}}^q = \left(\prod_{j=1}^{i} x_{F^j}^{q^{i-j}} \right) \cdot \left(\prod_{j=1}^{i-1} x_{F^j}^{-q^{1+(i-1)-j}} \right) = x_{F^i}^{q^{i-i}} = x_{F^i},$$

  und außerdem gilt

$$({}^F b)_{F^0} = b_{F^{-1}}^q = b_{F^{n-1}}^q = \prod_{j=1}^{n-1} x_{F^j}^{-q^{1+(n-1)-j}} = \prod_{j=1}^{n-1} x_{F^j}^{-q^{-j}} = x_{F^0} \cdot \prod_{j=0}^{n-1} x_{F^j}^{-q^{-j}} \overset{(21)}{=} x_{F^0},$$

  also auch

$$(b^{-1} \cdot {}^F b)_{F^0} = 1 \cdot x_{F^0} = x_{F^0},$$

  also insgesamt $b \cdot {}^F b = a_F$, d.h. $(a_s)_s$ ist kohomolog zur trivialen Klasse nach 2.9. — Für diesen Fall haben wir das Lemma also bewiesen.

- *2. Fall:* $k = \mathbb{F}_q$, $K/L = \mathbb{F}_{q^n}$ beliebig.
  Betrachte den abgeschlossenen Normalteiler $H := \mathrm{Gal}\,(K/L)$ in G! Nach 2.36 erhalten wir eine exakte Sequenz

$$0 \longrightarrow \underbrace{H^1\big(\underbrace{G/H\,(K/L)}_{=\mathrm{Gal}\,(L/k)}, \underbrace{\big[(K^\times)_c^n\big]^H}_{=(L^\times)_c^n}\big)}_{=0 \quad \text{(nach dem 1. Fall!)}} \xrightarrow{\inf} H^1_{\mathrm{cont}}(G, (K^\times)_c^n) \xrightarrow{\mathrm{res}} H^1_{\mathrm{cont}}(H, (K^\times)_c^n).$$

  Offenbar operiert H einfach komponentenweise auf $(K^\times)_c^n$, d.h. als H-Gruppen sind $(K^\times)_c^n$ und $(K^\times)^n$ isomorph. Daraus folgt

$$H^1_{\mathrm{cont}}(H, (K^\times)_c^n) = H^1_{\mathrm{cont}}(H, (K^\times)^n) = \big(\underbrace{H^1_{\mathrm{cont}}(H, K^\times)}_{=0 \ \text{(Hilbert 90!)}}\big)^n = 0,$$

  Insgesamt folgt also aus der Exaktheit obiger Sequenz die Behauptung auch in diesem Fall, d.h. wir haben das Lemma für den Fall, daß k ein *endlicher* Körper ist, vollständig bewiesen.

- *3. Fall:* k unendlich, $[K:k] < \infty$.

  In diesem Fall wollen wir nach dem Vorbild von Serre in seinem Beweis des „Hilbert 90“ aus [Ser79, S.150] vorgehen: Sei $(a_s) = \big((a_{s,\varphi})_{\varphi\in M}\big) \in Z^1_{\mathrm{cont}}(G,(K^\times)_c^n)$ beliebig. Da die $s \in G$, aufgefaßt als Elemente des K-Vektorraums $\mathrm{Hom}_k(K,K)$, K-linear unabhängig sind, ist für jedes Tupel $\alpha = (\alpha_s)_{s\in G} \in (K^\times)^{[K:k]}$ die Linearform $K \xrightarrow{l_\alpha} K$ mit $l_\alpha(x) := \sum_{s\in G} \alpha_s \cdot {}^s\!x$ ungleich null, d.h. ihr Kern ist ein echter k-Untervektorraum von K. Speziell trifft dies auf die l_{α_φ} mit $\alpha_\varphi := (\alpha_{s,\varphi})_{s\in G}$ für $\varphi \in M$ zu. Die Vereinigung der Kerne der l_{α_φ} ist dann eine echte Teilmenge von K, weil nach Voraussetzung k *unendlich* viele Elemente hat. Also gibt es ein $d \in K$, auf dem keine dieser Linearformen verschwindet, d.h. das Element

  $$b := \big(l_{\alpha_\varphi}(d)\big)_{\varphi\in M} = \big(\sum_{s\in G} a_{s,\varphi}\cdot {}^s\!d\big)_{\varphi\in M}$$

  liegt in $(K^\times)_c^n$. Setzen wir $D := (d,\ldots,d) \in K_c^n$, so gilt in K_c^n offenbar:

  $$b = \sum_{s\in G} a_s \cdot {}^s\!D.$$

  Für beliebiges $s \in G$ folgt dann

  $${}^s\!b = \sum_{t\in G} \underbrace{{}^s\!a_t}_{=a_s^{-1}a_{st}} \cdot {}^s({}^t\!D) = a_s^{-1}\sum_{t\in G} a_{st}\cdot {}^{st}\!D = a_s^{-1}\cdot b,$$

  also

  $$1 = b^{-1}\cdot a_s \cdot {}^s\!b.$$

  Diese Gleichung gilt zunächst in K_c^n, dann aber auch in $(K^\times)_c^n$, weil beide Seiten darin liegen und die G-Operation auf $(K^\times)_c^n$ die Einschränkung der G-Operation auf K_c^n ist. Der 1-Kozykel a_s ist also kohomolog zum trivialen 1-Kozykel, und das Lemma ist auch in diesem Fall bewiesen.

- *4. Fall:* k unendlich, K beliebig.

  Sei K' ein Zwischenkörper der Erweiterung K/L, der endlich und galoissch über k ist (zum Beispiel die normale Hülle von L in K!). Bezeichnet H den zugehörigen abgeschlossenen Normalteiler $\mathrm{Gal}\,(K/K')$ von G (der nach Wahl von K' endlichen Index in G hat), so erhalten wir wie im zweiten Fall nach 2.36 eine exakte Sequenz

  $$0 \longrightarrow \underbrace{H^1_{\mathrm{cont}}\big(G/H, \underbrace{\big[(K^\times)_c^n\big]^H}_{=(K'^\times)_c^n}\big)}_{=0\ \text{(3. Fall!)}} \xrightarrow{\inf} H^1_{\mathrm{cont}}(G,(K^\times)_c^n) \xrightarrow{\mathrm{res}} \underbrace{H^1_{\mathrm{cont}}(H,(K^\times)_c^n)}_{\begin{array}{l}=\ \big(H^1_{\mathrm{cont}}(H,K^\times)\big)^n\\ =\ 0\ \text{(Hilbert 90!)}\end{array}},$$

  und die Behauptung folgt wie dort.

q.e.d.

5.6 Lemma. Es sei $c \in Z^1_{\mathrm{cont}}(G,S_n)$ und alle Bezeichnungen wie in 2.29. Dann haben wir den folgenden Isomorphismus von abelschen Gruppen (und also insbesondere von punktierten Mengen):

$$\begin{array}{ccc} L^\times & \xrightarrow{\sim} & H^0(G,(K^\times)_c^n) \\ x & \mapsto & (\varphi x)_{\varphi\in M}. \end{array}$$

Beweis: Nenne die Abbildung aus dem Lemma f. Für $i = 1, \ldots, r$ wollen wir die kanonische Abbildung $L \twoheadrightarrow L_i \subseteq K$ mit ι_i bezeichnen; die $\iota_1, \ldots, \iota_r$ sind also Elemente aus M. Wir präzisieren dann die Aussage des Lemmas und behaupten, daß die Umkehrabbildung g zu f wie folgt gegeben wird:

$$\begin{array}{ccc} H^0(G, (K^\times)_c^n) & \xrightarrow{g} & \prod_{i=1}^r L_i^\times = L^\times \\ (x_\varphi)_{\varphi \in M} & \mapsto & (x_{\iota_i})_i. \end{array}$$

Zunächst wollen wir uns überlegen, daß g wohldefiniert ist, daß also für beliebiges $(x_\varphi) \in H^0(G, (K^\times)_c^n))$ und beliebiges $i \in \{1, \ldots, r\}$ das Element x_{ι_i} in L_i liegt. Hierfür müssen wir zeigen, daß x_{ι_i} fix unter der Operation von $G_{L_i} := \mathrm{Gal}\,(K/L_i)$ ist. Sei also $s \in G_{L_i}$ beliebig. Wegen $s \in G_{L_i} \leq G$ ist (x_φ) nach Voraussetzung fix unter s, und es folgt

$$(x_\varphi)_\varphi = {}^s(x_\varphi)_\varphi = ({}^s x_{s^{-1}\varphi})_\varphi \quad \Longrightarrow \quad x_{\iota_i} = {}^s x_{s^{-1}\iota_i} \overset{s|_{L_i}=1}{=} {}^s x_{\iota_i}.$$

Als nächstes wollen wir sehen, daß auch f wohldefiniert ist. Seien dazu $x \in L^\times$ und $s \in G$ beliebig. Dann ergibt sich:

$${}^s(\varphi x)_\varphi = \big({}^s([s^{-1}\varphi]x)\big)_\varphi = (ss^{-1}\varphi x)_\varphi = (\varphi x)_\varphi,$$

d.h. $f(x) = (\varphi x)_\varphi$ ist tatsächlich ein Element aus $H^0(G, (K^\times)_c^n)$.
Da die Abbildungen f und g offensichtlich Gruppenhomomorphismen sind, bleibt nur noch zu zeigen, daß sie invers zueinander sind. Sei zunächst $x = (x_i)_{i=1,\ldots,r} \in L^\times$ beliebig. Es folgt:

$$(gf)(x) = g\big[(\varphi x)_\varphi\big] = (\iota_i x)_i = (x_1, \ldots, x_r) = x.$$

Sei umgekehrt $(x_\varphi)_\varphi \in H^0(G, (K^\times)_c^n)$ gegeben. Wir haben zu zeigen, daß für alle $\varphi \in M$ gilt:

$$x_\varphi = \big[(fg)(x_\varphi)_\varphi\big] = \varphi(x_{\iota_1}, \ldots, x_{\iota_r}).$$

Sei also $\psi \in M$ beliebig. Dann faktorisiert ψ über ein L_i mit $i \in \{1, \ldots, r\}$, und deshalb gibt es ein $s \in G$ mit $\psi = s\iota_i$. Damit ergibt sich:

$$\begin{aligned} &(x_\varphi)_\varphi = {}^s(x_\varphi)_\varphi = ({}^s x_{s^{-1}\varphi})_\varphi \\ &\qquad\qquad \Longrightarrow \quad x_\psi = {}^s x_{s^{-1}\psi} = {}^s x_{\iota_i} = {}^s(\iota_i(x_{\iota_1}, \ldots, x_{\iota_r})) = \psi(x_{\iota_1}, \ldots, x_{\iota_r}). \end{aligned}$$

q.e.d.

5.7 Korollar. Es sei $c \in Z^1_{\mathrm{cont}}(G, S_n)$ und alle Bezeichnungen wie in 2.29. Dann haben wir den folgenden Isomorphismus von abelschen Gruppen:

$$\begin{array}{ccc} L^\times/L^{\times m} & \xrightarrow{\gamma} & H^1_{\mathrm{cont}}(G, (\mu_m^n)_c) \\ \bar{x} & \mapsto & \left(\left(\frac{{}^s\sqrt[m]{s^{-1}\varphi x}}{\sqrt[m]{\varphi x}} \right)_{\varphi \in M} \right)_s. \end{array}$$

(Dabei bezeichne $\sqrt[m]{y}$ für beliebiges $y \in K^\times$ ein Urbild von y unter der Surjektion $K^\times \xrightarrow{m} K^\times$, $z \mapsto z^m$.)

Beweis: Wir betrachten die lange Kohomologiesequenz zur kurzen exakten Sequenz aus 5.4 und erhalten mit Hilfe des Isomorphismus aus 5.6 sowie mit 5.5 das folgende kommutative Diagramm abelscher Gruppen mit exakten Zeilen:

$$\begin{array}{ccccccccc}
H^0(G,(K^\times)_c^n) & \xrightarrow{m} & H^0(G,(K^\times)_c^n) & \xrightarrow[\bar{b}\mapsto(b^{-1}.\bar{b})]{\delta} & H^1_{\mathrm{cont}}(G,(\mu_m)_c^n) & \longrightarrow & H^1_{\mathrm{cont}}(G,(K^\times)_c^n) \\
\wr\uparrow & = & \wr\uparrow & = & \| & = & \| \\
L^\times & \xrightarrow[m]{} & L^\times & \xrightarrow[\delta']{} & H^1_{\mathrm{cont}}(G,(\mu_m)_c^n) & \longrightarrow & 0
\end{array}$$

Die Abbildung δ' induziert also einen Isomorphismus $\gamma : L^\times/L^{\times m} \xrightarrow{\sim} H^1_{\mathrm{cont}}(G,(\mu_m)_c^n)$, und wir müssen nur noch zeigen, daß die angegebene Abbildungsvorschrift die richtige ist. Sei dazu $x \in L^\times$ beliebig, dann ergibt sich:

$$\delta'(x) \overset{5.6}{=} \delta\big[(\varphi x)_\varphi\big] = \left(\left(\frac{1}{\sqrt[m]{\varphi x}}\right)_\varphi \cdot {}^s(\sqrt[m]{\varphi x})_\varphi\right)_s = \left(\left(\frac{s\sqrt[m]{s^{-1}\varphi x}}{\sqrt[m]{\varphi x}}\right)_\varphi\right)_s,$$

und die Behauptung folgt. **q.e.d.**

5.8 Korollar. Es sei $b \in Z^1_{\mathrm{cont}}(G, S_n \int \mu_m)$ beliebig und alle Bezeichnungen wie in 2.29. Dann haben wir folgenden Gruppenisomorphismus:

$$\begin{array}{rccl}
\eta: & \prod_{i=1}^r (L_i \cap \mu_m) & \xrightarrow{\sim} & H^0(G,(\mu_m^n)_c) \\
& x & \mapsto & (\varphi x)_{\varphi\in M}.
\end{array}$$

Beweis: Es bezeichne c das Bild von b in $H^1_{\mathrm{cont}}(G,S_n)$. Nach 2.25 stimmen auf μ_m^n die mit b und c getwisteten G-Operationen überein. Wir dürfen also b durch c ersetzen. Nach 5.4 und 5.6 haben wir dann das folgende kommutative Diagramm von Gruppen mit exakten Zeilen:

$$\begin{array}{ccccccc}
1 & \longrightarrow & H^0(G,(\mu_m^n)_c) & \longrightarrow & H^0(G,(K^\times)_c^n) & \xrightarrow{m} & H^0(G,(K^\times)_c^n) \\
 & & \wr\uparrow\eta & & \wr\uparrow & & \wr\uparrow \\
1 & \longrightarrow & \{x\in L^\times \mid x^m=1\} & \longrightarrow & L^\times & \xrightarrow{m} & L^\times
\end{array}$$

Offenbar gilt $\{x \in L^\times \mid x^m = 1\} = \prod_{i=1}^r (L_i \cap \mu_m)$, und die Abbildungsvorschrift für η ergibt sich aus 5.6. **q.e.d.**

5.9 Lemma. Es sei $c \in Z^1_{\mathrm{cont}}(G,S_n)$ und alle Bezeichnungen wie in 2.29. Dann haben wir den folgenden Gruppenisomorphismus:

$$\begin{array}{rccl}
\mathrm{Aut}_k(L)^{\mathrm{opp}} & \xrightarrow{\alpha} & H^0(G,(S_n)_c) \\
a & \mapsto & [M\to M,\ \varphi\mapsto\varphi\circ a].
\end{array}$$

Beweis: Es seien die Morphismen $\iota_1, \ldots, \iota_r \in M$ wie im Beweis von 5.6 definiert. Mit deren Hilfe definieren wir die Umkehrabbildung β von α wie folgt:

$$\begin{array}{ccc} H^0(G,(S_n)_c) & \xrightarrow{\beta} & \mathrm{Aut}_k(L)^{\mathrm{opp}} \\ \tau & \mapsto & \big(L \xrightarrow{(\tau(\iota_1),\ldots,\tau(\iota_r))} \prod_{i=1}^r L_i = L\big). \end{array}$$

Wir wollen nun schrittweise zeigen, daß α und β wohldefinierte, zueinander inverse Gruppenisomorphismen sind:

- $\alpha(a)$ *bijektiv:* Es sei $a \in \mathrm{Aut}_k(L)^{\mathrm{opp}}$ beliebig. Offenbar ist $\alpha(a)$ injektiv, denn aus $\varphi a = \psi a$ folgt $\varphi = \psi$, weil a bijektiv ist. Da M eine endliche Menge ist, ist $\alpha(a)$ dann aber auch bijektiv.

- α *Gruppenhomomorphismus:* Seien $a, b \in \mathrm{Aut}_k(L)^{\mathrm{opp}}$ und $\varphi \in M$ beliebig. Dann folgt:

  $$\alpha(ab)(\varphi) = \alpha(b \circ a)(\varphi) = \varphi ba = (\varphi b)a = \alpha(a)[\alpha(b)(\varphi)] = [\alpha(a) \circ \alpha(b)](\varphi),$$

  d.h. es gilt $\alpha(ab) = \alpha(a) \circ \alpha(b)$.

- $\alpha(a) \in H^0(G,(S_n)_c)$*:* Seien $a \in \mathrm{Aut}_k(L)^{\mathrm{opp}}$, $s \in G$ und $\varphi \in M$ beliebig. Wir rechnen nach:

  $$\big[{}^s\alpha(a)\big](\varphi) \overset{2.29}{=} s \circ \underbrace{\alpha(a)(s^{-1}\varphi)}_{=s^{-1}\varphi a} = ss^{-1}\varphi a = \varphi a = \alpha(a)(\varphi)$$

  und stellen fest, daß wirklich ${}^s\alpha(a) = \alpha(a)$ gilt. Insgesamt wissen wir also jetzt, daß α ein wohldefinierter Gruppenhomomorphismus ist.

- $\beta(\tau) \in \mathit{End}_k(L)$*:* Seien $\tau \in H^0(G,(S_n)_c)$ und $i \in \{1,\ldots,r\}$ beliebig. Wir müssen zeigen, daß das Bild von $\tau(\iota_i)$ in L_i liegt. Äquivalent dazu ist, daß für alle $s \in G_{L_i} := \mathrm{Gal}\,(K/L_i)$ gilt: $s \circ \tau(\iota_i) = \tau(\iota_i)$. Sei also $s \in G_{L_i}$ beliebig. Nach Voraussetzung gilt aber ${}^s\tau = \tau$, d.h.

  $$\tau(\iota_i) = [{}^s\tau](\iota_i) \overset{2.29}{=} s \circ \tau(s^{-1}\iota_i) \overset{s^{-1}|_{L_i}=1}{=} s \circ \tau(\iota_i).$$

- $\beta(\tau)$ *injektiv:* Sei wieder $\tau \in H^0(G,(S_n)_c)$ beliebig, und liege $x = (x_1,\ldots,x_r)$ im Kern von $\beta(\tau)$. Wir müssen dann zeigen, daß alle x_j schon null sind — sei also $j \in \{1,\ldots,r\}$ beliebig. Der Morphismus $\tau^{-1}(\iota_j) : L \to K$ faktorisiere über L_i; dann gibt es ein $s \in G$ mit $\tau^{-1}(\iota_j) = s\iota_i$. Mit τ ist auch τ^{-1} fix unter G, und es folgt

  $$s\iota_i = \tau^{-1}(\iota_j) = [{}^s\tau^{-1}](\iota_j) = s \circ \tau^{-1}(s^{-1}\iota_j) \quad \Longrightarrow \quad \tau(\iota_i) = s^{-1}\iota_j.$$

  Setzen wir in diese Gleichung x ein, so ergibt sich:

  $$0 = \tau(\iota_i)(x) = [s^{-1}\iota_j](x) = s^{-1}x_j,$$

  und weil s ein Automorphismus ist, folgt $x_j = 0$.

  Die Injektivität von $\beta(\tau)$ ist damit bewiesen, d.h. $\beta(\tau)$ ist ein injektiver Morphismus der endlichen k-Algebra L in sich. Demnach ist $\beta(\tau)$ sogar *bijektiv* und also ein Element von $\mathrm{Aut}_k(L)^{\mathrm{opp}}$ — womit wir die Wohldefiniertheit von β bewiesen haben.

- $\beta\alpha = 1$*:* Sei $a \in \mathrm{Aut}_k(L)^{\mathrm{opp}}$ beliebig. Dann gilt:

$$(\beta\alpha)(a) = \beta\big[M \to M, \varphi \mapsto \varphi a\big] = (\iota_1 a, \ldots, \iota_r a) = a.$$

- $\alpha\beta = 1$*:* Seien umgekehrt $\tau \in H^0(G, (S_n)_c)$ und $\varphi \in M$ beliebig. Der Morphismus φ faktorisiere über L_i, d.h. wir finden ein $s \in G$ mit $\varphi = s\iota_i$, und es ergibt sich:

$$\begin{aligned}\big[(\alpha\beta)(\tau)\big](\varphi) = \big[\alpha(\tau(\iota_1), \ldots, \tau(\iota_r))\big](\varphi) &= \varphi \circ (\tau(\iota_1), \ldots, \tau(\iota_r)) \\ &= s \circ \tau(\iota_i) = s \circ \tau(s^{-1} s\iota_i) = [{}^s\tau](s\iota_i) = \tau(\varphi),\end{aligned}$$

  und das Lemma ist vollständig bewiesen.

q.e.d.

5.10 Korollar. Es sei $c \in Z^1_{\mathrm{cont}}(G, S_n)$ und alle Bezeichnungen wie in 2.29. Dann haben wir das folgende kommutative Diagramm von Rechtsoperationen, wobei die Operation in der oberen Zeile die in 2.18 definierte sei:

$$\begin{array}{ccccc} H^1_{\mathrm{cont}}(G, (\mu_m^n)_c) & \times & H^0(G, (S_n)_c) & \longrightarrow & H^1_{\mathrm{cont}}(G, (\mu_m^n)_c) \\ \gamma \uparrow \wr & & \alpha \uparrow \wr & & \gamma \uparrow \wr \\ L^\times / L^{\times m} & \times & \mathrm{Aut}_k(L)^{\mathrm{opp}} & \longrightarrow & L^\times / L^{\times m} \\ (\bar{x} & , & a) & \longmapsto & \overline{a(x)} \end{array}$$

Beweis: Seien $x \in L^\times$ und $a \in \mathrm{Aut}_k(L)^{\mathrm{opp}}$ beliebig. Es ist:

$$\gamma(\overline{ax}) = \left(\left(\frac{s\sqrt[m]{s^{-1}\varphi a x}}{\sqrt[m]{\varphi a x}} \right)_{\varphi \in M} \right)_s \qquad \text{und}$$

$$\begin{aligned}\gamma(\bar{x})^{\alpha(a)} &= \left(\alpha(a)^{-1} \cdot \left(\frac{s\sqrt[m]{s^{-1}\varphi a x}}{\sqrt[m]{\varphi x}} \right)_{\varphi \in M} \cdot {}^s[\alpha(a)] \right)_s = \left({}^{[\alpha(a)^{-1}]} \left(\frac{s\sqrt[m]{s^{-1}\varphi a x}}{\sqrt[m]{\varphi x}} \right)_{\varphi \in M} \right)_s \\ &= \left(\left(\frac{s\sqrt[m]{s^{-1}\varphi a x}}{\sqrt[m]{\varphi a x}} \right)_{\varphi \in M} \right)_s .\end{aligned}$$

q.e.d.

5.11 Korollar. Es sei $c \in Z^1_{\mathrm{cont}}(G, S_n)$, und alle Bezeichnungen seien wie in 2.29. Insbesondere wird c also durch eine endliche, kommutative, separable k-Algebra L vom Grad n über k gegeben: Wenn wir $M := \mathrm{Hom}_k(L, K)$ setzen und S_n mit $\mathrm{Aut}\,(M)$ identifizieren, gilt $c_s = [M \to M,\ \varphi \mapsto s \circ \varphi]$.

Bezeichne $p : S_n \int \mu_m \twoheadrightarrow S_n$ die kanonische Projektion, dann haben wir die folgende Bijektion:

$$\boxed{\begin{array}{ccc} \mathrm{Aut}_k(L)\backslash(L^\times/L^{\times m}) & \xrightarrow{\sim} & \left\{ b \in H^1_{\mathrm{cont}}(G, S_n \int \mu_m) \;\middle|\; H^1_{\mathrm{cont}}(p)(b) = [c] \right\} \\ \mathrm{Aut}_k(L) \cdot \bar{x} & \mapsto & \left(\left(\frac{s\sqrt[m]{s^{-1}\varphi x}}{\sqrt[m]{\varphi x}} \right)_{\varphi \in M} \cdot c_s \right)_s \end{array}}$$

Dabei ist die Linksoperation von $\mathrm{Aut}_k(L)$ auf $L^\times/L^{\times m}$ die natürliche, durch ${}^a\bar{x} := \overline{a(x)}$, gegebene.

Insbesondere wird also jede Kohomologieklasse aus $H^1_{cont}(G, S_n \int \mu_m)$ durch ein Paar (L, x) gegeben, wobei L eine kommutative, separable k-Algebra vom Grad n über k und x ein Element aus $L^\times$ ist. Zwei Paare (L, x) und (L', x') geben genau dann dieselbe Klasse, wenn es einen k-Isomorphismus $\psi : L \xrightarrow{\sim} L'$, ein $y \in L^\times$ und ein $a \in Aut_k(L)$ gibt mit $x' = \psi(a[xy^m])$.

Beweis: Klar nach 2.33, 5.7, 5.9 und 5.10, wobei man beachte, daß die Rechtsoperation einer Gruppe eine Linksoperation der Oppositgruppe ist! **q.e.d.**

5.12 Satz. Sei speziell $k = \mathbb{F}_q$ ein *endlicher Körper*, und sei $b \in H^1_{\mathrm{cont}}(G, S_n \int \mu_m)$ beliebig, gemäß 5.11 durch ein Paar (L, x) gegeben.
Sei $L = \prod_{i=1}^r L_i$ mit Teilkörpern L_i von $K = \overline{\mathbb{F}_q}$, die endlich vom Grad n_i über $\mathbb{F}_q$ sind, und sei $x = (x_1, \ldots, x_r)$ mit $x_i \in L_i^\times$. Wähle m-te Wurzeln y_i der x_i in K. Ein 1-Kozykel (b_s), der b repräsentiert, wird nach 2.8 schon durch b_F eindeutig festgelegt, wobei F den Frobenius $x \mapsto x^q$ bezeichne, und in diesem Sinne wird b gegeben durch:

$$\boxed{b_F = \prod_{i=1}^r \left[\left(y_i^{q^{n_i}-1}, 1, \ldots, 1 \right) \cdot z_i \right]}$$

Hierbei bezeichne $z_i \in S_{n_i} \leq S_n$ den Standard-Zykel der Länge n_i.

Beweis: Ohne Beschränkung der Allgemeinheit gelte $r = 1$, d.h. L ist ein Teilkörper von K vom Grad n über $\mathbb{F}_q$, und $y = y_1$ ist eine m-te Wurzel von $x \in L^\times$.

Es gilt $M := \mathrm{Hom}_k(L, K) = \{F^0, \ldots, F^{n-1}\}$, und wir wollen M via $i \mapsto F^i$ mit der Menge $\{0, \ldots, n-1\}$ identifizieren. Wir können $y^{(q^i)}$ für alle $i \in \{0, \ldots, n-1\}$ als m-te Wurzel von $F^i x = x^{(q^i)}$ wählen und müssen wegen 5.11 jetzt nur noch den Term

$$\frac{F\sqrt[m]{F^{-1}\varphi x}}{\sqrt[m]{\varphi x}}$$

für alle $\varphi \in M$, d.h. für alle $i \in \{0, \ldots, n-1\}$ auswerten (denn daß c_F gerade der Standard-Zykel der Länge n ist, ist wegen $F \circ F^i = F^{i+1}$ klar) .

Sei zunächst $\underline{i = 0}$. Wir erhalten:

$$\frac{F\sqrt[m]{F^{-1}F^0 x}}{\sqrt[m]{F^0 x}} = \frac{F\sqrt[m]{F^{-1}x}}{\sqrt[m]{x}} = \frac{F\sqrt[m]{F^{n-1}x}}{y} = \frac{Fy^{(q^{n-1})}}{y} = \frac{\left(y^{(q^{n-1})}\right)^q}{y} = y^{q^{n-1}-1}.$$

Sei jetzt $\underline{i \geq 1}$:

$$\frac{F\sqrt[m]{F^{-1}F^i x}}{\sqrt[m]{F^i x}} = \frac{F\sqrt[m]{F^{i-1}x}}{\sqrt[m]{F^i x}} = \frac{Fy^{(q^{i-1})}}{y^{(q^i)}} = \frac{y^{(q^i)}}{y^{(q^i)}} = 1.$$

q.e.d.

5.13 Beispiel. Sei speziell $n = 6$, $m = 3$, $k = \mathbb{F}_7$ (und also $K = \overline{\mathbb{F}_7}$).

Es gilt $\mathbb{F}_{49} = \mathbb{F}_7(\alpha)$ mit $\alpha^2 + 5\alpha + 5 = 0$ und $\mathbb{F}_{2401} = \mathbb{F}_7(\beta)$ mit $\beta^4 + 5\beta^3 + 4\beta^2 + \beta + 5 = 0$; definiere damit die Klasse $b \in H^1_{\text{cont}}(G, \mu_3 \int S_6)$ durch das Paar $\left(\mathbb{F}_{2401} \times \mathbb{F}_{49}, (\frac{1}{\beta}, \frac{1}{\alpha^2})\right)$.

Wir haben also $n_1 = 4$ und $n_2 = 2$, wählen dritte Wurzeln y_1 von $\frac{1}{\beta}$ und y_2 von $\frac{1}{\alpha^2}$ und rechnen:

$$\begin{aligned} y_1^{7^4-1} &= \left(\tfrac{1}{\beta}\right)^{\frac{7^4-1}{3}} = \left(\tfrac{1}{\beta}\right)^{800} = \beta^{2400-800} = \beta^{1600} = (\beta^{400})^4 = 5^4 = 2, \\ y_2^{7^2-1} &= \left(\tfrac{1}{\alpha^2}\right)^{\frac{7^2-1}{3}} = \left(\tfrac{1}{\alpha^2}\right)^{16} = \alpha^{48-2\cdot 16} = \alpha^{16} = (\alpha^8)^2 = 5^2 = 4. \end{aligned}$$

Nach 5.12 folgt dann, daß einer der b repräsentierenden 1-Kozykel auf dem Frobenius durch folgendes Element aus $\mu_3 \int S_6$ gegeben wird:

$$b_F = (2, 1, 1, 1, 4, 1) \cdot [1234][56].$$

5.14 Korollar. Sei wieder $k = \mathbb{F}_q$ ein endlicher Körper, und sei $L = \prod_{i=1}^r \mathbb{F}_{q^{n_i}}$ eine separable k-Algebra vom Grad n über k. Wähle ein $N \in \mathbb{N}$ so groß, daß $\mathbb{F}_{q^N}$ alle m-ten Wurzeln aus Elementen der $\mathbb{F}_{q^{n_i}}$ und die m-ten Einheitswurzeln enthält, und sei $\alpha \in \mathbb{F}_{q^N}^\times$ ein erzeugendes Element der multiplikativen Gruppe.

Für $i \in \{1, \ldots, r\}$ ist dann $\alpha_i := \alpha^{\frac{q^N-1}{q^{n_i}-1}}$ ein Erzeuger von $\mathbb{F}_{q^{n_i}}^\times$, und es ist $\zeta := \alpha^{\frac{q^N-1}{m}}$ eine primitive m-te Einheitswurzel.
Sei nun $x := (\alpha_1^{k_1}, \ldots, \alpha_r^{k_r}) \in L^\times$ für natürliche Zahlen $k_1, \ldots, k_r$. Dann wird die durch (L, x) definierte Klasse in $H^1_{\text{cont}}(G, S_n \int \mu_m)$ durch einen 1-Kozykel (b_s) repräsentiert, der auf dem Frobenius F den Wert

$$\boxed{b_F = \textstyle\prod_{i=1}^r \left[\left(\zeta^{k_i}, 1, \ldots, 1\right) \cdot z_i\right]}$$

hat.

Beweis: Nach Wahl von N liegen die m-ten Wurzeln der α_i in $\mathbb{F}_{q^N}$, d.h. für jedes i ist $y_i := \alpha^{\frac{k_i \cdot (q^N-1)}{m \cdot (q^{n_i}-1)}} \in \mathbb{F}_{q^N}$ eine m-te Wurzel von $\alpha_i^{k_i}$. Nach 5.12 müssen wir also nur nachrechnen, daß $y_i^{q^{n_i}-1} = \zeta^{k_i}$ gilt:

$$y_i^{q^{n_i}-1} = \alpha^{\frac{k_i \cdot (q^N-1)}{m \cdot (q^{n_i}-1)} \cdot (q^{n_i}-1)} = \left(\alpha^{\frac{q^N-1}{m}}\right)^{k_i} = \zeta^{k_i}.$$

q.e.d.

5.15 Lemma.

(i) Ist L/k eine separable Körpererweiterung und $\nu \in \mathbb{N}_+$ eine natürliche Zahl, so gilt

$$\mathrm{Aut}_k(L^\nu) = S_\nu \int \mathrm{Aut}_k(L),$$

wobei das Kranzprodukt auf L^ν wie folgt operiert:

$${}^{[(a_i)_i \cdot \sigma]}(x_i)_i = \left(a_i x_{\sigma^{-1} i}\right)_i .$$

(ii) Ist L eine endliche, separable k-Algebra, d.h. $L = \prod_{i=1}^r L_i^{\nu_i}$ mit paarweise nichtisomorphen separablen Körpererweiterungen L_i von k, so gilt

$$\mathrm{Aut}_k(L) = \prod_{i=1}^r \mathrm{Aut}_k(L_i^{\nu_i}) \overset{(i)}{=} \prod_{i=1}^r \left(S_{\nu_i} \int \mathrm{Aut}_k(L_i)\right).$$

Beweis: Klar! **q.e.d.**

5.16 Beispiele.

(i) Es sei $k := \mathbb{R}$ (also $K = \mathbb{C}$), $n = 3$ und $m = 4$. Es gibt — bis auf Isomorphie — genau zwei separable $\mathbb{R}$-Algebren vom Grad drei, nämlich $\mathbb{R}^3$ und $\mathbb{C} \times \mathbb{R}$.

Sei zunächst c die durch $L = \mathbb{R}^3$ gegebene Klasse in $H^1_{\mathrm{cont}}(G, S_3)$ (das ist natürlich die triviale Klasse). Es ist $\mathbb{R}^\times/(\mathbb{R}^\times)^4 = \{\overline{-1}, \bar{1}\}$, also $L^\times/L^{\times 4} = \{\overline{-1}, \bar{1}\}^3$. Nach 5.15 ist $\mathrm{Aut}_{\mathbb{R}}(L) = S_3$, und unter der Operation dieser Gruppe wird $L^\times/L^{\times 4}$ in vier Bahnen zerlegt mit Repräsentanten $(\bar{1}, \bar{1}, \bar{1})$, $(\bar{1}, \bar{1}, \overline{-1})$, $(\bar{1}, \overline{-1}, \overline{-1})$ und $(\overline{-1}, \overline{-1}, \overline{-1})$.

Sei nun c die durch $L = \mathbb{C} \times \mathbb{R}$ gegebene Klasse in $H^1_{\mathrm{cont}}(G, S_3)$. Es ist $\mathbb{C}^\times = \mathbb{C}^{\times 4}$, also $L^\times/L^{\times 4} = \{(\bar{1}, \bar{1}), (\bar{1}, \overline{-1})\}$. Die Gruppe $\mathrm{Aut}_{\mathbb{R}}(L)$ ist gleich $\{1, \tau\}$ mit $\tau(a, b) = (\bar{a}, b)$, und diese Gruppe operiert offenbar trivial auf $L^\times/L^{\times 4}$, d.h. in diesem Fall erhalten wir zwei Kohomologieklassen.

Insgesamt gibt es also genau sechs verschiedene Klassen in $H^1_{\mathrm{cont}}(G, S_3 \int \mu_4)$; in der Notation aus 5.11 sind dies:

$$\big(\mathbb{R}^3, (1,1,1)\big), \big(\mathbb{R}^3, (1,1,-1)\big), \big(\mathbb{R}^3, (1,-1,-1)\big), \big(\mathbb{R}^3, (-1,-1,-1)\big),$$
$$\big(\mathbb{C} \times \mathbb{R}, (1,1)\big) \text{ und } \big(\mathbb{C} \times \mathbb{R}, (1,-1)\big).$$

(ii) Sei jetzt $k := \mathbb{F}_5$, $n = 4$ und $m = 3$. Dann gibt es — wieder bis auf Isomorphie — genau die folgenden separablen $\mathbb{F}_5$-Algebren vom Grad vier: $\mathbb{F}_5^4$, $\mathbb{F}_{25} \times \mathbb{F}_5^2$, $\mathbb{F}_{25}^2$, $\mathbb{F}_{125} \times \mathbb{F}_5$ und $\mathbb{F}_{625}$.

Mit Hilfe von 5.15 erhalten wir (wobei F den Frobenius $a \mapsto a^5$ bezeichne):

$$\begin{array}{lcll}
\mathrm{Aut}_{\mathbb{F}_5}(\mathbb{F}_5^4) & = & S_4 \int \mathrm{Aut}\,(\mathbb{F}_5) & = S_4, \\
\mathrm{Aut}_{\mathbb{F}_5}(\mathbb{F}_{25} \times \mathbb{F}_5^2) & = & \mathrm{Aut}\,(\mathbb{F}_{25}) \times \big(S_2 \int \mathrm{Aut}\,(\mathbb{F}_5)\big) & = \{1, F\} \times S_2, \\
\mathrm{Aut}_{\mathbb{F}_5}(\mathbb{F}_{25}^2) & = & S_2 \int \mathrm{Aut}\,(\mathbb{F}_{25}) & = S_2 \int \{1, F\}, \\
\mathrm{Aut}_{\mathbb{F}_5}(\mathbb{F}_{125} \times \mathbb{F}_5) & = & \mathrm{Aut}\,(\mathbb{F}_{125}) \times \mathrm{Aut}\,(\mathbb{F}_5) & = \{1 \times 1, F \times 1, F^2 \times 1\}, \\
\mathrm{Aut}_{\mathbb{F}_5}(\mathbb{F}_{625}) & = & & \{1, F, F^2, F^3\}.
\end{array}$$

Sei zunächst $L := \mathbb{F}_5^4$. Wegen $(4,3) = 1$ ist das Nehmen der dritten Potenz in $\mathbb{F}_5^\times$ bijektiv, d.h. schon $\mathbb{F}_5^\times/{\mathbb{F}_5^\times}^3$ ist einelementig und dann natürlich erst recht $L^\times/{L^\times}^3$ und der Quotient nach $\mathrm{Aut}_{\mathbb{F}_5}(L)$. Zu L gehört also nur die triviale Kohomologieklasse.

Sei jetzt $L := \mathbb{F}_{25} \times \mathbb{F}_5^2$. Wegen $3|24$ ist Potenzieren mit drei in $\mathbb{F}_{25}^\times$ *nicht* bijektiv, vielmehr bilden die dritten Potenzen eine Untergruppe vom Index drei in $\mathbb{F}_{25}^\times$. Sei $\alpha \in \mathbb{F}_{25}^\times$ ein Erzeuger der multiplikativen Gruppe (zum Beispiel können wir für α eine der beiden Wurzeln des Polynoms $T^2 + 2T + 3 \in \mathbb{F}_5[T]$ nehmen), dann gilt $\mathbb{F}_{25}^\times/{\mathbb{F}_{25}^\times}^3 = \{\bar{1}, \bar{\alpha}, \overline{\alpha^2}\}$. wegen $F(\alpha) = \alpha^5 = \alpha^3 \cdot \alpha^2$ liegen $(\bar{\alpha}, \bar{1}, \bar{1})$ und $(\overline{\alpha^2}, \bar{1}, \bar{1})$ im selben Orbit unter der Aktion von $\{1, F\} \times S_2$. Es folgt, daß es für diese Wahl von L genau zwei verschiedene Kohomologieklassen gibt, repräsentiert durch $(1,1,1)$ und $(\alpha, 1, 1)$.

Im Falle $L = \mathbb{F}_{25}^2$ ist $\mathrm{Aut}_{\mathbb{F}_5}(L) = S_2 \int \{1, F\}$, d.h. aus obigen Überlegungen folgt $\mathrm{Aut}_{\mathbb{F}_5}(L) \backslash (L^\times/{L^\times}^3) = \{(\bar{1}, \bar{1}), (\bar{1}, \bar{\alpha}), (\bar{\alpha}, \bar{\alpha})\}$.

Für $L = \mathbb{F}_{125} \times \mathbb{F}_5$ gilt wegen $(124, 3) = 1$ wieder $L^\times = {L^\times}^3$, d.h. wie im ersten Fall gibt es auch hier nur eine Kohomologieklasse, repräsentiert durch $(1,1)$.

Sei schließlich $L = \mathbb{F}_{625}$! Bezeichne γ eine Wurzel des Polynoms $T^4 + T^2 + 3T + 3 \in \mathbb{F}_5[T]$. Dann ist γ ein Erzeuger der multiplikativen Gruppe, und es gilt: $\gamma^{26} = \gamma^3 + 2\gamma^2 + 2\gamma + 1$ ist Wurzel des Polynoms $T^2 + 2T + 3$, d.h. wir können $\alpha := \gamma^{26}$ setzen. Wie oben folgt, daß $L^\times/{L^\times}^3 = \{\bar{1}, \bar{\gamma}, \overline{\gamma^2}\}$ und daß $\bar{\gamma}$ und $\overline{\gamma^2}$ im selben Orbit unter $\mathrm{Aut}_{\mathbb{F}_5}(L)$ liegen — auch in diesem Fall gibt es also zwei Kohomologieklassen, nämlich die durch 1 und γ repräsentierten.

Insgesamt gibt es also die folgenden neun Klassen in $H^1_{\mathrm{cont}}(G, S_4 \int \mu_3)$:

$$\begin{array}{l}\big(\mathbb{F}_5^4, (1,1,1,1)\big),\\ \big(\mathbb{F}_{25} \times \mathbb{F}_5^2, (1,1,1)\big), \big(\mathbb{F}_{25} \times \mathbb{F}_5^2, (\alpha,1,1)\big),\\ \big(\mathbb{F}_{25}^2, (1,1)\big), \big(\mathbb{F}_{25}^2, (1,\alpha)\big), \big(\mathbb{F}_{25}^2, (\alpha,\alpha)\big),\\ \big(\mathbb{F}_{125} \times \mathbb{F}_5, (1,1)\big),\\ \big(\mathbb{F}_{625}, 1\big) \text{ und } \big(\mathbb{F}_{625}, \gamma\big).\end{array}$$

5.17 Satz/ Definition. Es sei $b \in H^1_{\mathrm{cont}}(G, S_n \int \mu_m)$ eine beliebige Kohomologieklasse, gemäß 5.11 repräsentiert durch ein Paar (L, x). Wie immer sei $L = \prod_{i=1}^r L_i$, wobei die L_i Zwischenkörper der Erweiterung K/k vom Grad n_i über k seien.

Es gelte $x = (x_1, \ldots, x_r)$ mit $x_i \in L_i$. Wähle für jedes $i \in \{1, \ldots, r\}$ eine k-Basis $e_1^{(i)}, \ldots, e_{n_i}^{(i)}$ von L_i, und sei $M_i := \mathrm{Hom}_k(L_i, K)$. Definiere damit

$$P_n^m\{b\} := \sum_{i=1}^r \mathrm{Tr}_{L_i/k}\left[\frac{1}{x_i} \cdot \left(\sum_{j=1}^{n_i} e_j^{(i)} X_j^{(i)}\right)^m\right] \in k[X_j^{(i)}],$$

wobei $\mathrm{Tr}_{L_i/k} : L[X_j^{(i)}] \to k[X_j^{(i)}]$ die k-lineare Abbildung sei, die Monome $X_1^{k_1} \cdot \ldots \cdot X_n^{k_n}$ auf sich selbst und die Konstanten auf ihre Spur schickt. Dann ist $P_n^m\{b\}$, die *mit b getwistete Fermatform*, eine K/k-Form von P_n^m, und es gilt $\vartheta(P_n^m\{b\}) = b$. Insbesondere hängt die k-Isomorphieklasse von $P_n^m\{b\}$ also nur von b und nicht von den getroffenen Wahlen ab.

Beweis: Sei $i \in \{1, \ldots, r\}$ beliebig. Für $\varphi \in M_i$ bezeichne auch den k-Algebrenmorphismus $L[X_j^{(i)}] \to K[X_j^{(i)}]$, der auf L durch φ gegeben wird und die X_i auf sich selbst schickt, mit φ! Dann gilt offenbar $\sum_{\varphi \in M_i} \varphi = \mathrm{Tr}_{L/k} : L[X_j^{(i)}] \to K[X_j^{(i)}]$. Definiere nun die Matrix

$$B_i := \left(\frac{\varphi e_j^{(i)}}{\sqrt[m]{\varphi x_i}} \right)_{\varphi \in M_i, j \in \{1,\ldots,n_i\}} \in M(n_i \times n_i, K).$$

Dann gilt

$$\det(B_i) = \underbrace{\frac{1}{\prod_{\varphi \in M_i} \sqrt[m]{\varphi x_i}}}_{\neq 0} \cdot \underbrace{\det\left(\varphi e_j^{(i)}\right)_{\varphi,j}}_{\neq 0} \neq 0, \dagger$$

d.h. B_i liegt in $\mathrm{GL}(n_i, K)$. Sei nun B die aus den B_i für $i = 1, \ldots, r$ gebildete Blockmatrix — B ist also eine reguläre $n \times n$-Matrix über K.
Wir rechnen nun nach, daß $P_n^m(BX) = P_n^m\{b\}$ gilt, daß also B einen Isomorphismus von $P_n^m\{b\}$ nach P_n^m definiert:

$$\begin{aligned} P_n^m(BX) &= \sum_{i=1}^{r} \sum_{\varphi \in M_i} \left(\sum_{j=1}^{n_i} \frac{\varphi e_j^{(i)}}{\sqrt[m]{\varphi x_i}} \cdot X_j^{(i)} \right)^m \\ &= \sum_{i=1}^{r} \sum_{\varphi \in M_i} \varphi \left[\frac{1}{x_i} \cdot \left(\sum_{j=1}^{n_i} e_j^{(i)} \cdot X_j^{(i)} \right)^m \right] \\ &= \sum_{i=1}^{r} \mathrm{Tr}_{L_i/k} \left[\frac{1}{x_i} \cdot \left(\sum_{j=1}^{n_i} e_j^{(i)} \cdot X_j^{(i)} \right)^m \right] \\ &= P_n^m\{b\}. \end{aligned}$$

Also ist $P_n^m\{b\}$ tatsächlich eine K/k-Form von P_n^m, und es gilt $\vartheta[P_n^m\{b\}] = [(C_s)_s]$ mit $C_s := B^s(B^{-1})$.
Sei (b_s) der durch (L, x) definierte 1-Kozykel, aufgefaßt mit Werten in $\mathrm{GL}(n, K)$, dessen Klasse ja gerade b ist. Mit Hilfe von 5.1 und 5.11 erhalten wir die folgende Formel für b_s (wobei wir dieselben m-ten Wurzeln wie in B wählen wollen):

$$b_s = \left(\frac{s\sqrt[m]{s^{-1}\varphi x}}{\sqrt[m]{\varphi x}} \cdot \delta_{\varphi, s\psi} \right)_{\varphi, \psi \in M}$$

Offenbar ist also auch b_s eine Blockmatrix mit Blöcken $b_s^{(i)}$ für $i = 1, \ldots, r$ der folgenden Gestalt:

$$b_s^{(i)} = \left(\frac{s\sqrt[m]{s^{-1}\varphi x_i}}{\sqrt[m]{\varphi x_i}} \cdot \delta_{\varphi, s\psi} \right)_{\varphi, \psi \in M_i}.$$

Wir sind fertig, wenn wir für beliebiges $s \in G$ zeigen können, daß $B_s = b_s$ gilt oder

---

†Nach [Lan93, 5.4,S.286] gilt: Ist L/k eine beliebige separable Körpererweiterung vom Grad n, $\{e_1, \ldots, e_n\}$ eine k-Basis von L und sind $\varphi_1, \ldots, \varphi_n : L \to K$ die verschiedenen k-Einbettungen von L in einen separablen algebraischen Abschluß K von L, so ist die Matrix $(\varphi_i e_j)_{i,j}$ invertierbar.

äquivalent $B = b_s{}^s B$ bzw. $B_i = b_s^{(i)s} B_i$ für alle i:

$$\begin{aligned}
b_s^{(i)s} B_i &= \left(\frac{s \sqrt[m]{s^{-1}\varphi x_i}}{\sqrt[m]{\varphi x_i}} \cdot \delta_{\varphi, s\psi} \right)_{\varphi,\psi \in M_i} \cdot \left(\frac{s\psi e_j^{(i)}}{s \sqrt[m]{\psi x_i}} \right)_{\psi \in M_i,\, j \in \{1,\ldots,n_i\}} \\
&= \left(\sum_{\psi \in M_i} \left[\frac{s \sqrt[m]{s^{-1}\varphi x_i}}{\sqrt[m]{\varphi x_i}} \cdot \delta_{\varphi, s\psi} \cdot \frac{s\psi e_j^{(i)}}{s \sqrt[m]{\psi x_i}} \right] \right)_{\varphi \in M_i,\, j \in \{1,\ldots,n_i\}} \\
&= \left(\frac{s \sqrt[m]{s^{-1}\varphi x_i}}{\sqrt[m]{\varphi x_i}} \cdot \frac{s(s^{-1}\varphi) e_j^{(i)}}{s \sqrt[m]{(s^{-1}\varphi) x_i}} \right)_{\varphi \in M_i,\, j \in \{1,\ldots,n_i\}} \\
&= \left(\frac{\varphi e_j^{(i)}}{\sqrt[m]{\varphi x_i}} \right)_{\varphi \in M_i,\, j \in \{1,\ldots,n_i\}} \\
&= B_i.
\end{aligned}$$

q.e.d.

5.18 Korollar. Ist $m \geq 3$, so ist ϑ nicht nur injektiv, sondern auch *surjektiv*, d.h. wir erhalten eine kanonische Bijektion

$$\boxed{\vartheta : E\left(K/k, P_n^m\right) \xrightarrow{\sim} H^1_{\mathrm{cont}}\left(G, S_n \textstyle\int \mu_m\right)}$$

von punktierten Mengen.

Beweis: Klar nach 3.1, 5.2, 5.3 und 5.17! **q.e.d.**

5.19 Bemerkung. Es sei A ein beliebiger kommutativer Ring mit Eins und B eine projektive A-Algebra von endlichem Rang. Wie in [Brü98] gezeigt, kann man dann eine kanonische A-lineare Abbildung $\mathrm{Tr}_{B/A} : B \longrightarrow A$ definieren, die *Spur von B nach A*, die unter anderem folgende Eigenschaften hat:

(i) Ist A ein Körper und B eine endliche Körpererweiterung von A (oder allgemeiner A beliebig und B eine *freie* A-Algebra), so ist $\mathrm{Tr}_{B/A}$ die übliche Spur.

(ii) Ist A' eine beliebige A-Algebra, so gilt $\mathrm{Tr}_{(B \otimes_A A')/A'} = \mathrm{Tr}_{B/A} \otimes 1_{A'}$.

(iii) Ist $B = \prod_{i=1}^r B_i$ endliches direktes Produkt von projektiven A-Algebren B_i von endlichem Rang, so gilt $\mathrm{Tr}_{B/A} = \sum_i \mathrm{Tr}_{B_i/A}$.

(iv) Ist C eine projektive B-Algebra von endlichem Rang, so gilt $\mathrm{Tr}_{C/A} = \mathrm{Tr}_{B/A} \circ \mathrm{Tr}_{C/B}$.

Benutzt man diese Spurabbildung, so erhält man aus den Eigenschaften (i)-(iii) offenbar (wobei alle Bezeichnungen wie in 5.17 seien):

$$\boxed{P_n^m\{b\} = \mathrm{Tr}_{L[X_j^{(i)}]/k[X_j^{(i)}]} \left[\frac{1}{x} \left(\sum_{i,j} e_j^{(i)} X_j^{(i)} \right)^m \right].}$$

5.20 Korollar. Es sei wieder $m \geq 3$, und man betrachte eine beliebige Körpererweiterung k'/k. Für ein Polynom $f \in k[X_1, \ldots, X_n]$ werde auch das Bild von f unter $k[X_i] \overset{\text{can}}{\hookrightarrow} k'[X_i]$ mit f bezeichnet. Bezeichnet K' einen separablen algebraischen Abschluß von k', so haben wir das folgende kommutative Diagramm von punktierten Mengen:

$$\begin{array}{ccccc}
[Q] & \in & E(K/k, P_n^m) \xrightarrow[\sim]{\vartheta} H^1_{\text{cont}}(G_k, \text{Aut}_K(P_n^m)) & \ni & (L,x) \\
\downarrow & & \downarrow \quad = \quad \downarrow & & \downarrow \\
[Q] & \in & E(K'/k', P_n^m) \xrightarrow[\vartheta]{\sim} H^1_{\text{cont}}(G_{k'}, \text{Aut}_{K'}(P_n^m)) & \ni & (L\otimes_k k', x\otimes 1)
\end{array}$$

Dabei werden für die rechte vertikale Abbildung Kohomologieklassen mit Paaren (L, x) gemäß 5.11 identifiziert.

Beweis: Zuerst wollen wir uns überlegen, daß die vertikalen Abbildungen wohldefiniert sind: Wir können K nach K' einbetten und daher ohne Beschränkung der Allgemeinheit annehmen, daß $K \subseteq K'$ gilt. Wenn es dann über K einen Isomorphismus von Q nach P_n^m gibt, so ist dieser insbesondere auch über K' definiert; sind Q und P_n^m schon über k isomorph, so erst recht auch über k'; dies zeigt, daß die linke vertikale Abbildung wohldefiniert ist.

Ist L eine separable k Algebra vom Grad n, so ist auch $L \otimes_k k'$ eine separable k'-Algebra vom Grad n, und mit x ist auch $x \otimes 1$ invertierbar. Geben (L, x) und (L', x') dieselbe Klasse, so gibt es nach 5.11 einen k-Isomorphismus $\psi : L \xrightarrow{\sim} L'$, ein $y \in L^\times$ und ein $a \in \text{Aut}_k(L)$ mit $x' = \psi(a[xy^m])$. Dann ist aber $\psi \otimes 1_{k'}$ ein k'-Isomorphismus von $L \otimes_k k'$ nach $L' \otimes_k k'$, und es gilt $x' \otimes 1 = (\psi \otimes 1_{k'})((a \otimes 1_{k'})[(x \otimes 1)(y \otimes 1)^m])$, d.h. auch $(L \otimes_k k', x \otimes 1)$ und $(L' \otimes_k k', x' \otimes 1)$ repräsentieren dieselbe Klasse. — Also ist auch die rechte vertikale Abbildung wohldefiniert, und es ist offensichtlich, daß die beiden vertikalen Abbildungen das ausgezeichnete Element auf das ausgezeichnete Element abbilden.

Weil nach 5.18 ϑ ein Isomorphismus ist, können wir die Kommutativität des Diagramms nachrechnen, indem wir rechts oben mit einem Paar (L, x) starten und zeigen, daß links unten dasselbe herauskommt:
Unter ϑ^{-1} wird (L, x) nach 5.17 auf $[P_n^m\{(L, x)\}]$ abgebildet. Wir müssen also beweisen, daß $P_n^m\{(L, x)\}$ und $P_n^m\{(L \otimes_k k', x \otimes 1)\}$ über K' isomorph sind. Nach 5.19 gilt aber

$$\begin{aligned}
P_n^m\{(L \otimes_k k', x \otimes 1)\} &= \text{Tr}_{\left[L[X_j^{(i)}]\otimes_k k'\right]/\left[k[X_j^{(i)}]\otimes_k k'\right]} \left[\frac{1}{x \otimes 1}\left(\sum_{i,j}(e_j^{(i)} \otimes 1)(X_j^{(i)} \otimes 1)\right)^m\right] \\
&\overset{5.19(ii)}{=} \left(\text{Tr}_{L[X_j^{(i)}]/k[X_j^{(i)}]}\left[\frac{1}{x}\left(\sum_{i,j} e_j^{(i)} X_j^{(i)}\right)^m\right]\right) \otimes 1 = P_n^m\{(L, x)\} \otimes 1,
\end{aligned}$$

und das Korollar ist bewiesen. **q.e.d.**

5.21 Korollar. Es sei wieder $m \geq 3$, und man betrachte eine K/k-Form $P_n^m\{(L, x)\}$ von P_n^m. Dann sind $P_n^m\{(L, x)\}$ und P_n^m über einer Körpererweiterung k' von k genau dann isomorph, wenn $L \otimes_k k' \cong (k')^n$ und wenn $x \otimes 1$ in $L \otimes_k k'$ eine m-te Potenz ist.

Beweis: Klar nach 5.20 und 5.11! **q.e.d.**

Nachdem wir die Berechnung von $E(K/k, P_n^m)$ bzw. $H^1_{\mathrm{cont}}(G, A(P_n^m))$ abgeschlossen haben, können wir nun 3.3 anwenden, um die Automorphismengruppen von getwisteten Fermatgleichungen zu bestimmen.

5.22 Korollar. Es sei $m \geq 3$, $b \in H^1_{\mathrm{cont}}(G, S_n \int \mu_m)$ eine beliebige Kohomologieklasse, gemäß 5.11 repräsentiert durch ein Paar (L, x) mit $L = \prod_{i=1}^r L_i$, und es sei $P_n^m\{b\}$ die in 5.17 definierte K/k-Form von P_n^m. Dann haben wir folgende kurze exakte Sequenz von Gruppen:

$$\boxed{1 \to \prod_{i=1}^{r} (L_i \cap \mu_m) \to \mathrm{Aut}_k\Big(P_n^m\{b\}\Big) \to \Big\{a \in \mathrm{Aut}_k(L)^{\mathrm{opp}} \Big| \tfrac{ax}{x} \in L^{\times m}\Big\} \to 1} \tag{22}$$

Ist speziell $x = 1$, so erhalten wir genauer:

$$\boxed{\mathrm{Aut}_k\Big(P_n^m\{b\}\Big) \cong \left(\prod_{i=1}^{r} (L_i \cap \mu_m)\right) \rtimes \mathrm{Aut}_k(L)^{\mathrm{opp}}} \tag{23}$$

Dabei wird das semidirekte Produkt über die folgende Operation gegeben:

$$\begin{array}{ccccc} \mathrm{Aut}_k(L)^{\mathrm{opp}} & \times & (\prod_{i=1}^r (L_i \cap \mu_m)) & \longrightarrow & (\prod_{i=1}^r (L_i \cap \mu_m)) \\ (a & , & x) & \mapsto & a^{-1}(x) \end{array}$$

Beweis: Ausgehend von der exakten Sequenz

$$1 \longrightarrow \mu_m^n \longrightarrow S_n \int \mu_m \longrightarrow S_n \longrightarrow 1$$

erhalten wir nach Twisten mit dem 1-Kozykel b gemäß 2.27 zunächst die Exaktheit der folgenden Sequenz von punktierten Mengen:

$$1 \longrightarrow H^0(G, (\mu_m^n)_b) \longrightarrow H^0(G, (S_n \int \mu_m)_b) \longrightarrow H^0(G, (S_n)_b) \xrightarrow{\delta} H^1_{\mathrm{cont}}(G, (\mu_m^n)_b).$$

Bezeichne c das Bild von b in $Z^1_{\mathrm{cont}}(G, S_n)$. Dann gilt $(S_n)_b = (S_n)_c$ und wegen 2.25 auch $(\mu_m^n)_b = (\mu_m^n)_c$. Außerdem identifiziert sich $H^0(G, (S_n \int \mu_m)_b)$ nach 3.3 mit der Gruppe $\mathrm{Aut}_k(P_n^m\{b\})$. Aus 5.8 und 5.9 folgt dann, daß folgendes Diagramm von punktierten Mengen kommutativ ist und exakte Zeilen hat:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H^0(G, (\mu_m^n)_c) & \longrightarrow & H^0(G, (S_n \int \mu_m)_b) & \longrightarrow & H^0(G, (S_n)_c) & \xrightarrow{\delta} & H^1_{\mathrm{cont}}(G, (\mu_m^n)_c) \\ & & \wr\uparrow \eta & = & \wr\uparrow & = & \wr\uparrow \alpha & = & \wr\uparrow \gamma \\ 1 & \longrightarrow & \prod_{i=1}^r (L_i \cap \mu_m) & \longrightarrow & \mathrm{Aut}_k\Big(P_n^m\{b\}\Big) & \longrightarrow & \mathrm{Aut}_k(L)^{\mathrm{opp}} & \xrightarrow[\tilde{\delta}]{} & L^\times / L^{\times m} \end{array}$$

Dabei wissen wir sogar von allen im Diagramm auftretenden Morphismen außer α, γ, δ und $\tilde{\delta}$, daß sie *Gruppenhomomorphismen* sind. Um zu beweisen, daß (22) eine exakte Sequenz von Gruppen ist, müssen wir also nur beweisen, daß

$$\mathrm{Ker}\,(\tilde{\delta}) = \Big\{a \in \mathrm{Aut}_k(L)^{\mathrm{opp}} \Big| \frac{ax}{x} \in L^{\times m}\Big\}$$

gilt. Offenbar folgt dies, falls wir zeigen können, daß die Abbildungsvorschrift von $\tilde{\delta}$ wie folgt gegeben wird:

$$\begin{array}{rccc} \tilde{\delta}: & \mathrm{Aut}_k(L)^{\mathrm{opp}} & \longrightarrow & L^\times/L^{\times m} \\ & a & \mapsto & \frac{ax}{x}. \end{array}$$

Dies können wir wegen $\delta\alpha = \gamma\tilde{\delta}$ leicht nachrechnen (dabei gelte $b = (b_s)$ für $b_s = a_s \cdot c_s$ mit $a_s \in \mu_m^n$, $c_s \in \mathrm{Aut}\,(M)$):

$$\begin{aligned} \delta\alpha(a) &= \delta[\varphi \mapsto \varphi \circ a] \\ &= \Big([\varphi \mapsto \varphi \circ a]^{-1} \cdot {}^{s'}[\varphi \mapsto \varphi \circ a]\Big)_s \\ &= \Big([\varphi \mapsto \varphi \circ a]^{-1} \cdot b_s \cdot [\varphi \mapsto \varphi \circ a] \cdot b_s^{-1}\Big)_s \\ &= \Big([\varphi \mapsto \varphi \circ a]^{-1} \cdot a_s \cdot c_s \cdot [\varphi \mapsto \varphi \circ a] \cdot c_s^{-1} \cdot a_s^{-1}\Big)_s \\ &= \Big(\big([\varphi \mapsto \varphi \circ a]^{-1}\big) a_s \cdot a_s^{-1}\Big)_s \\ &\overset{5.11}{=} \left[\left(\frac{s\sqrt[m]{s^{-1}\varphi a x}}{\sqrt[m]{\varphi a x}} \cdot \frac{\sqrt[m]{\varphi x}}{s\sqrt[m]{s^{-1}\varphi x}}\right)_{\varphi \in M}\right]_s \\ &= \left[\left(\frac{s\sqrt[m]{s^{-1}\varphi\left(\frac{ax}{x}\right)}}{\sqrt[m]{\varphi\left(\frac{ax}{x}\right)}}\right)_{\varphi \in M}\right]_s \\ &= \gamma\left(\frac{ax}{x}\right). \end{aligned}$$

Sei jetzt speziell $x = 1$. Dann liegt b im Bild der durch den kanonischen Schnitt $S_n \hookrightarrow S_n \int \mu_m$ induzierten Abbildung $Z^1_{\mathrm{cont}}(G, S_n) \hookrightarrow Z^1_{\mathrm{cont}}(G, S_n \int \mu_m)$, und die behauptete Isomorphie folgt aus 2.28.

Die Operation, durch die das semidirekte Produkt definiert wird, ergibt sich aus dem folgenden Diagramm, welches offenbar kommutiert:

$$\begin{array}{ccccccccc} & \big(\sigma & , & (\zeta_\varphi)_{\varphi\in M}\big) & \longmapsto & (\zeta_{\sigma^{-1}\varphi})_{\varphi\in M} & & \\ [\varphi\mapsto\varphi a] & \mathrm{Aut}\,(M) & \times & \mu_m^n & \longrightarrow & \mu_m^n & & (\varphi x)_{\varphi\in M} \\ \uparrow & \uparrow & & \uparrow & & \uparrow & & \uparrow \\ & H^0(G,(S_n)_c) & \times & H^0(G,(\mu_m^n)_b) & \longrightarrow & H^0(G,(\mu_m^n)_b) & & \\ & \alpha\uparrow\wr & & \eta\uparrow\wr & & \eta\uparrow\wr & & \\ a & \mathrm{Aut}_k(L)^{\mathrm{opp}} & \times & \prod_{i=1}^r (L_i \cap \mu_m) & \longrightarrow & \prod_{i=1}^r (L_i \cap \mu_m) & & x \\ & \big(a & , & x\big) & \longmapsto & a^{-1}(x) & & \end{array}$$

q.e.d.

5.23 Bemerkung. Wir haben die Sequenzen (22) und (23) aus unserem allgemeinen Formalismus hergeleitet; wie Sładek und Wesołowski in [SW98, Theorem 1.3.] bzw. [Wes99, Theorem 3.3.] gezeigt haben, kann man sie auch elementar durch direktes Nachrechnen beweisen.

5.24 Beispiel. Sei speziell $n = 6$, $m = 3$, $k = \mathbb{F}_7$ (und also $K = \overline{\mathbb{F}_7}$).

Wie in 5.13 schreiben wir $\mathbb{F}_{49}$ als $\mathbb{F}_7(\alpha)$ mit $\alpha^2 + 5\alpha + 5 = 0$ und $\mathbb{F}_{2401}$ als $\mathbb{F}_7(\beta)$ mit $\beta^4 + 5\beta^3 + 4\beta^2 + \beta + 5 = 0$ und betrachten die durch das Paar $\left(\mathbb{F}_{2401} \times \mathbb{F}_{49}, (\frac{1}{\beta}, \frac{1}{\alpha^2})\right)$ gegebene Klasse $b \in H^1_{\text{cont}}(G, \mu_3 \int S_6)$.

Um $P_6^3\{b\}$ berechnen zu können, müssen wir zunächst einige Rechnungen in den Körpern $\mathbb{F}_{49}$ und $\mathbb{F}_{2401}$ durchführen, um die benötigten Spuren auszurechnen:

$$\alpha^7 = 6\alpha + 2 \implies \operatorname{Tr}_{\mathbb{F}_{49}/\mathbb{F}_7}(\alpha) = \alpha + \alpha^7 = 2,$$

$$\left.\begin{array}{rcl} \beta^7 & = & 3\beta^3 + 5\beta^2 + 2\beta + 3 \\ \beta^{49} & = & 2\beta^3 + \beta + 6 \\ \beta^{343} & = & 2\beta^3 + 2\beta^2 + 3\beta \end{array}\right\} \implies \operatorname{Tr}_{\mathbb{F}_{2401}/\mathbb{F}_7}(\beta) = 2,$$

$$\left.\begin{array}{rcl} (\beta^2)^7 & = & 3\beta^3 + \beta^2 + 4\beta \\ (\beta^2)^{49} & = & 3\beta^3 + 6\beta^2 + 3\beta + 2 \\ (\beta^2)^{343} & = & \beta^3 + 6\beta^2 + 1 \end{array}\right\} \implies \operatorname{Tr}_{\mathbb{F}_{2401}/\mathbb{F}_7}(\beta^2) = 3,$$

$$\left.\begin{array}{rcl} (\beta^3)^7 & = & 3\beta^3 + 2\beta^2 + 4\beta + 6 \\ (\beta^3)^{49} & = & 6\beta^3 + 1 \\ (\beta^3)^{343} & = & 4\beta^3 + 5\beta^2 + 3\beta + 2 \end{array}\right\} \implies \operatorname{Tr}_{\mathbb{F}_{2401}/\mathbb{F}_7}(\beta^3) = 2.$$

Bei der Berechnung von $P_6^3\{b\}$ wollen wir anstelle der Variablen $X_1^{(1)}, \ldots, X_4^{(1)}, X_1^{(2)}, X_2^{(2)}$ die Variablen a, b, c, d, x, y verwenden, weil dies kürzer und übersichtlicher ist. Als $\mathbb{F}_7$-Basis von $\mathbb{F}_{49}$ nehmen wir $\{1, \alpha\}$, und als $\mathbb{F}_7$-Basis von $\mathbb{F}_{2401}$ nehmen wir $\{1, \beta, \beta^2, \beta^3\}$. Damit ergibt sich:

$$\begin{array}{rcl} P_6^3\{b\} & = & \operatorname{Tr}_{\mathbb{F}_{2401}/\mathbb{F}_7}\left[\beta \cdot (a + \beta b + \beta^2 c + \beta^3 d)^3\right] + \operatorname{Tr}_{\mathbb{F}_{49}/\mathbb{F}_7}\left[\alpha^2 \cdot (x + \alpha y)^3\right] \\ & = & 2a^3 + 6a^2c + a^2d + 6ab^2 + 2abc + 4abd + 2ac^2 + 3acd + 6ad^2 \\ & & \quad + 5b^3 + 2b^2c + 5b^2d + 5bc^2 + 5bcd + 6bd^2 + 2c^3 + 6c^2d + cd^2 + d^3 \\ & & + y^3 + 4x^2y + 5y^3. \end{array}$$

5.25 Beispiele. Wir wollen die Beispiele aus 5.16 fortsetzen und zu den dort aufgelisteten Kohomologieklassen die zugehörigen Formen angeben:

(i) $k = \mathbb{R}$, $K = \mathbb{C}$, $n = 3$ und $m = 4$.

Die einzige endliche separable Körpererweiterung von $\mathbb{R}$ ist $\mathbb{C}$, und wir wählen $\{1, i\}$ als $\mathbb{R}$-Basis von $\mathbb{C}$. Die Spur von $\mathbb{C}$ über $\mathbb{R}$ drückt sich bezüglich dieser Basis wie folgt aus:

$$\operatorname{Tr}_{\mathbb{C}/\mathbb{R}}(a + ib) = (a + ib) + (a - ib) = 2a,$$

und wir erhalten (wobei wir die Unbestimmten der besseren Lesbarkeit willen mit $x, y, \ldots$ anstelle von $X_1^{(1)}, X_2^{(1)}, \ldots$ bezeichnen wollen):

b	$P_3^4\{b\}$
$\big(\mathbb{R}^3,(1,1,1)\big)$	$x^4+y^4+z^4$
$\big(\mathbb{R}^3,(1,1,-1)\big)$	$x^4+y^4-z^4$
$\big(\mathbb{R}^3,(1,-1,-1)\big)$	$x^4-y^4-z^4$
$\big(\mathbb{R}^3,(-1,-1,-1)\big)$	$-x^4-y^4-z^4$
$\big(\mathbb{C}\times\mathbb{R},(1,1)\big)$	$(2x^4-12x^2y^2+2y^4)+z^4$
$\big(\mathbb{C}\times\mathbb{R},(1,-1)\big)$	$(2x^4-12x^2y^2+2y^4)-z^4.$

(ii) $k=\mathbb{F}_5$, $K=\overline{\mathbb{F}_5}$, $n=4$ und $m=3$.

Wie in 5.16 gesagt, ist $\mathbb{F}_{25}=\mathbb{F}_5(\alpha)$ mit $\alpha^2+2\alpha+3=0$, und wir wollen $\{1,\alpha\}$ als $\mathbb{F}_5$-Basis von $\mathbb{F}_{25}$ wählen. Dann erhält man für die Spur:

$$\mathrm{Tr}_{\mathbb{F}_{25}/\mathbb{F}_5}(a+\alpha b)=2a+3b.$$

Den Körper $\mathbb{F}_{125}$ erhalten wir zum Beispiel, wenn wir γ mit $\gamma^3+4\gamma+3=0$ zu $\mathbb{F}_5$ adjungieren; wir können dann $\{1,\gamma,\gamma^2\}$ als $\mathbb{F}_5$-Basis von $\mathbb{F}_{125}$ nehmen und erhalten für die Spur:

$$\mathrm{Tr}_{\mathbb{F}_{125}/\mathbb{F}_5}(a+\gamma b+\gamma^2 c)=3a+4b+2c.$$

Wie schon erwähnt, gilt $\mathbb{F}_{625}=\mathbb{F}_5(\beta)$ mit $\beta^4+\beta^2+3\beta+3=0$. Wählen wir $\{1,\beta,\beta^2,\beta^3\}$ als $\mathbb{F}_5$-Basis von $\mathbb{F}_{625}$, so ergibt sich die folgende Formel für die Spur:

$$\mathrm{Tr}_{\mathbb{F}_{625}/\mathbb{F}_5}(a+\beta b+\beta^2 c+\beta^3 d)=4a+3c+d.$$

Mit Hilfe dieser Formeln können wir nun auch die Formen des Polynoms P_4^3 über $\mathbb{F}_5$ vollständig auflisten:

b	$P_4^3\{b\}$
$\big(\mathbb{F}_5^4,(1,1,1,1)\big)$	$x^3+y^3+z^3+u^3$
$\big(\mathbb{F}_{25}\times\mathbb{F}_5^2,(1,1,1)\big)$	$(2x^3+4x^2y+4xy^2)+z^3+u^3$
$\big(\mathbb{F}_{25}\times\mathbb{F}_5^2,(\alpha,1,1)\big)$	$(3x^3+4x^2y+y^3)+z^3+u^3$
$\big(\mathbb{F}_{25}^2,(1,1)\big)$	$(2x^3+4x^2y+4xy^2)+(2z^3+4z^2u+4zu^2)$
$\big(\mathbb{F}_{25}^2,(1,\alpha)\big)$	$(2x^3+4x^2y+4xy^2)+(3z^3+4z^2u+u^3)$
$\big(\mathbb{F}_{25}^2,(\alpha,\alpha)\big)$	$(3x^3+4x^2y+y^3)+(3z^3+4z^2u+u^3)$
$\big(\mathbb{F}_{125}\times\mathbb{F}_5,(1,1)\big)$	$(3x^3+xy^2+2x^2y+x^2z+2yz^2)+u^3$
$\big(\mathbb{F}_{625},1\big)$	$x^3+4xy^2+y^3+4x^2z+3x^2u+xyz+4xu^2+4yzu+yu^2$ $+3z^3+z^2u+zu^2+4u^3$
$\big(\mathbb{F}_{625},\beta\big)$	$4x^2y+3xy^2+3x^2z+4y^2u+4xzu+xu^2+4yz^2+yzu$ $+zu^2+2z^3+z^2u+2zu^2+3u^3$

6 Binäre kubische Formen

In diesem Kapitel wollen wir die Ergebnisse des letzten Kapitels auf den Spezialfall $n = 2$, $m = 3$ anwenden, d.h. auf den Fall der *binären kubischen Formen*. Dieser Fall ist besonders interessant, weil sich herausstellen wird, daß alle nicht-ausgearteten binären kubischen Formen getwistete Fermatgleichungen sind, und weil man in diesem Fall nicht nur ϑ^{-1}, sondern auch ϑ selbst explizit angeben. Dies bedeutet, daß man eine Formel hat, mit der man zu einer gegebenen nicht-ausgearteten binären kubischen Form Q das Paar $(L, x) = \vartheta[Q]$ berechnen kann.

Es seien k ein Körper mit $(\mathrm{char} k) \notin \{2, 3\}$ und K ein separabler algebraischer Abschluß von k.

6.1 Definition. Eine *binäre kubische Form (über k)* ist ein Objekt Q aus $\mathcal{F}_k^{2,3}$, d.h. ein homogenes Polynom vom Grad drei in zwei Unbestimmten über k.

Die *Diskriminante* einer binären kubischen Form $Q(X, Y) = aX^3 + bX^2Y + cXY^2 + dY^3$ ist definiert als

$$\Delta(Q) := -27a^2d^2 + 18abcd + b^2c^2 - 4b^3d - 4ac^3, \tag{24}$$

und Q heißt *nicht-ausgeartet*, falls $\Delta(Q) \neq 0$ gilt. Es sei $\mathcal{F} \subset \mathcal{F}_k^{2,3}$ die volle Unterkategorie der nicht-ausgearteten Formen. Insbesondere ist die *Fermat-Form* $P := P_2^3 = X^3 + Y^3$ nicht-ausgeartet, denn es gilt $\Delta(P) = -27$.

6.2 Bemerkung. In [GKZ94] wird allgemeiner jedem Polynom f von beliebigem Grad in beliebig vielen Unbestimmten eine Diskriminante $\Delta(f)$ zugeordnet, und die oben definierte Diskriminante einer binären kubischen Form Q ist dann gerade $\Delta(Q(1, X))$ im Sinne von [GKZ94].

Insbesondere folgt aus der allgemeinen Theorie, daß Q genau dann nicht-ausgeartet ist, wenn die zugehörige Hyperfläche $X(Q)$ in $\mathbb{P}_k^1$ glatt ist.

6.3 Lemma. Es sei $Q(X, Y)$ eine beliebige binäre kubische Form über k. Dann gilt:

(i) Ist $A = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \in \mathrm{GL}\,(2, k)$ beliebig, so gilt

$$\Delta\big(\underbrace{Q(rX + sY, tX + uY)}_{=:Q_A}\big) = \big[\det(A)\big]^6 \cdot \Delta(Q);$$

insbesondere induziert die Diskriminante also eine wohldefinierte Abbildung

$$\Big\{\text{Isomorphieklassen in } \mathcal{F}\Big\} \xrightarrow{\Delta} k^\times/k^{\times 6}.$$

(ii) In $K[X, Y]$ gelte $Q(X, Y) = a(X - \alpha Y)(X - \beta Y)(X - \gamma Y)$. Dann ist

$$\Delta(Q) = a^4(\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2.$$

(iii) Q ist genau dann eine K/k-Form der Fermat-Form P, wenn Q nicht-ausgeartet ist.

Beweis: Die Aussagen (i) und (ii) folgen sofort aus allgemeinen Eigenschaften der Diskriminanten, die in [GKZ94] behandelt werden. Wir können sie aber auch direkt durch einfaches, stures Ausmultiplizieren und Nachrechnen erhalten.

Aus (i) folgt dann, daß jede K/k-Form von P notwendig nicht-ausgeartet sein muß; gelte also $\Delta(Q) \neq 0$.

Die zu Q assoziierte Hyperfläche in $\mathbb{P}^1_K$ ist nulldimensional und besteht aus höchstens drei Punkten. Bekanntlich operiert $\mathrm{GL}\,(2,K)$ dreifach transitiv auf $\mathbb{P}^1_K$, d.h. wir finden eine reguläre 2×2-Matrix A, die alle Punkte der Hyperfläche auf von ∞ verschiedene Punkte in $\mathbb{P}^1_k$ abbildet. Dies bedeutet genau, daß das Polynom Q_A die Darstellung $a(X-\alpha Y)(X-\beta Y)(X-\gamma Y)$ mit $a \in K$ geeignet besitzt.

Weil wir Q als nicht-ausgeartet vorausgesetzt haben, folgt aus (ii), daß die Elemente α, β und γ paarweise verschieden sind. Benutzen wir erneut, daß $\mathrm{GL}\,(2,K)$ dreifach transitiv auf $\mathbb{P}^1_K$ operiert, so finden wir ein $B \in \mathrm{GL}\,(2,K)$, welches α, β und γ auf (-1), $(-\zeta)$ und $(-\zeta^2)$ abbildet, wobei $\zeta \in K$ eine primitive dritte Einheitswurzel bezeichne. Sei schließlich $C := \mathrm{diag}\,(\frac{1}{\sqrt[3]{a}}, \frac{1}{\sqrt[3]{a}})$. Dann erhalten wir:

$$Q_{CBA} = a \cdot \left(\frac{1}{\sqrt[3]{a}}\right)^3 \cdot (X+Y)(X+\zeta Y)(X+\zeta^2 Y) = P,$$

d.h. CBA definiert einen Isomorphismus von P nach Q in $\mathcal{F}^{2,3}_K$. **q.e.d.**

6.4 Definition. Für $\delta \in k^\times/k^{\times 2}$ definiere

$$L_\delta := \begin{cases} k \times k & \text{falls } \delta \in k^{\times 2}, \\ k(\sqrt{\delta}) & \text{sonst.} \end{cases}$$

Offenbar definiert $\delta \mapsto L_\delta$ eine Bijektion zwischen $k^\times/k^{\times 2}$ und den Isomorphieklassen von separablen k-Algebren vom Grad zwei über k.

Definiere schließlich noch $A_\delta := \mathrm{Aut}_k(L_\delta)$; der Erzeuger dieser zweielementigen Mengen werde stets mit τ bezeichnet, d.h. es gilt $\tau(x,y) = (y,x)$ für $\delta \in k^{\times 2}$ und $\tau(x + y\sqrt{\delta}) = x - y\sqrt{\delta}$ sonst.

6.5 Korollar. Wir haben eine kanonische Bijektion

$$\begin{array}{ccc} \coprod_{\delta \in k^\times/k^{\times 2}} \left[A_\delta \backslash \left(L_\delta^\times / L_\delta^{\times 3}\right)\right] & \longrightarrow & \left\{\text{Isomorphieklassen in } \mathcal{F}\right\} \\ (\delta, x) & \mapsto & P\left\{(L_\delta, x)\right\}. \end{array}$$

Beweis: Klar nach 5.11, 5.18 und 6.3(iii)! **q.e.d.**

6.6 Korollar. Es sei speziell $k = \mathbb{F}_q$ ein *endlicher* Körper, und es sei Q eine beliebige nicht-ausgeartete binäre kubische Form über k.

Wähle ein erzeugendes Element α der multiplikativen Gruppe von $k' := \mathbb{F}_{q^2}$, und setze $\beta := \alpha^{\frac{q+1}{2}}$ und $\delta := \beta^2 = N_{k'/k}(\alpha)$! Dann ist $[\alpha]$ ein Erzeuger von $k'^\times/k'^{\times 3}$, δ ein Erzeuger von $k^\times$, $[\delta]$ ein Erzeuger von $k^\times/k^{\times 3}$, und es gilt:

(i) Ist $q \equiv 1 \pmod 3$, d.h. enthält k die dritte Einheitswurzeln, so ist Q über k isomorph zu einer der folgenden neun getwisteten Fermatformen (wobei $\{1, \beta\}$ als Basis von L_δ und $\{(1,0),(0,1)\}$ als Basis von $L_1 = k \times k$ gewählt wurden):

$$\begin{array}{lcl}
P_2^3\{(L_1,(1,1))\} & = & X^3 + Y^3, \\
P_2^3\{(L_1,(1,\delta))\} & = & X^3 + \delta Y^3, \\
P_2^3\{(L_1,(1,\delta^2))\} & = & X^3 + \delta^2 Y^3, \\
P_2^3\{(L_1,(\delta,\delta))\} & = & \delta X^3 + \delta Y^3, \\
P_2^3\{(L_1,(\delta,\delta^2))\} & = & \delta X^3 + \delta^2 Y^3, \\
P_2^3\{(L_1,(\delta^2,\delta^2))\} & = & \delta^2 X^3 + \delta^2 Y^3, \\
P_2^3\{(L_\delta,1)\} & = & 2X^3 + 6\delta XY^2, \\
P_2^3\{(L_\delta,\alpha)\} & = & \mathrm{Tr}_{k'/k}(\alpha)X^3 + 3\mathrm{Tr}_{k'/k}(\alpha\beta)X^2Y \\
 & & \qquad +3\delta\mathrm{Tr}_{k'/k}(\alpha)XY^2 + \delta\mathrm{Tr}_{k'/k}(\alpha\beta)Y^3, \\
P_2^3\{(L_\delta,\alpha^2)\} & = & \mathrm{Tr}_{k'/k}(\alpha^2)X^3 + 3\mathrm{Tr}_{k'/k}(\alpha^2\beta)X^2Y \\
 & & \qquad +3\delta\mathrm{Tr}_{k'/k}(\alpha^2)XY^2 + \delta\mathrm{Tr}_{k'/k}(\alpha^2\beta)Y^3.
\end{array}$$

(ii) Ist $q \equiv 2 \pmod 3$, d.h. enthält k die dritten Einheitswurzeln *nicht*, so ist Q über k isomorph zu einer der folgenden drei getwisteten Fermatformen (wobei die Basen wie oben gewählt wurden):

$$\begin{array}{lcl}
P_2^3\{(L_1,(1,1))\} & = & X^3 + Y^3, \\
P_2^3\{(L_\delta,1)\} & = & 2X^3 + 6\delta XY^2 \\
P_2^3\{(L_\delta,\alpha)\} & = & \mathrm{Tr}_{k'/k}(\alpha)\cdot X^3 + 3\cdot\mathrm{Tr}_{k'/k}(\alpha\beta)\cdot X^2Y \\
 & & \qquad +3\delta\cdot\mathrm{Tr}_{k'/k}(\alpha)\cdot XY^2 + \delta\cdot\mathrm{Tr}_{k'/k}(\alpha\beta)\cdot Y^3.
\end{array}$$

Beweis: Als Erzeuger der multiplikativen Gruppe kann δ kein Quadrat in k sein, woraus folgt, daß α ein erzeugendes Element von $\mathbb{F}_{q^2}^\times$ ist. Es ist dann klar, daß $[\delta]$ und $[\alpha]$ die Gruppen $k^\times/k^{\times 3}$ bzw. $L_\delta^\times/L_\delta^{\times 3}$ erzeugen.

Als nächstes wollen wir die Operation von A_δ auf $H := L_\delta^\times/L_\delta^{\times 3}$ verstehen. Sei dazu zunächst $q \equiv 1 \pmod 3$, gelte etwa $q = 3t+1$ mit $t \in \mathbb{N}_+$. Dann ist

$$\tau[\alpha] = \alpha^q = \alpha^{3t+1} = \alpha\cdot(\alpha^t)^3,$$

d.h. A_δ läßt die Elemente von H fix, und es gibt drei Bahnen in H, repräsentiert von 1, α und α^2. Außerdem ist klar, daß es in $(k\times k)^\times/(k\times k)^{\times 3}$ genau neun Elemente und sechs Bahnen unter der Operation von A_1 gibt, repräsentiert durch $(1,1)$, $(1,\delta)$, $(1,\delta^2)$, (δ,δ), (δ,δ^2) und (δ^2,δ^2). Behauptung (i) folgt dann aus 6.5.

— Gelte jetzt $q \equiv 2 \pmod 3$, etwa $q = 3t+2$ mit $t \in \mathbb{N}_+$. Dann ist

$$\tau[\alpha] = \alpha^q = \alpha^{3t+2} = \alpha^2\cdot(\alpha^t)^3,$$

d.h. A_δ läßt das Element $[1] \in H$ fix und vertauscht $[\alpha]$ mit $[\alpha^2]$ (man beachte, daß $[1] \neq [\alpha]$, da $\mathbb{F}_{q^2}$ wegen $q^2 \equiv 2^2 \equiv 4 \equiv 1 \pmod 3$ die dritten Einheitswurzeln enthält). Es gibt also nur zwei Bahnen in H, repräsentiert durch 1 und α. Außerdem ist $k^\times \xrightarrow{3} k^\times$ wegen $\mu_3 \not\subseteq k^\times$ ein Isomorphismus, so daß $(k\times k)^\times/(k\times k)^{\times 3}$ überhaupt nur aus einem Element, repräsentiert durch $(1,1)$, besteht. Behauptung (ii) folgt dann wie (i) aus 6.5. **q.e.d.**

6.7 Lemma. Es sei $Q(X,Y)$ eine nicht-ausgeartete binäre kubische Form über k. Dann gibt es eine reguläre Matrix $A \in \mathrm{GL}(2,k)$ der Form $A = \left(\begin{smallmatrix} 1 & 0 \\ \rho & 1 \end{smallmatrix}\right)$ für ein $\rho \in k$, so daß

$$Q_A(X,Y) = a \cdot \left(X^3 + bX^2Y + cXY^2 + dY^3\right) \tag{25}$$

für geeignete a, b, c und d aus k mit $a \neq 0$ gilt. Sei f das Polynom $f(X) := \frac{1}{a} \cdot Q(X,1)$, und sei M der Zerfällungskörper von f. Dann verschwindet die Diskriminante von f nicht, und M ist unabhängig von der Wahl von A.

Beweis: Es sei $Q(X,Y) = a'X^3 + b'X^2Y + c'XY^2 + d'Y^3$. Ist $a' \neq 0$, so ist $Q(X,Y)$ schon von der Form (25), d.h. wir können $\rho = 0$ bzw. $A = \mathrm{id}$ wählen.

Sei also $a' = 0$. Die Elemente b', c' und d' können dann nicht alle zugleich null sein, da sonst die Form ausgeartet wäre. Weil der Körper k mehr als drei Elemente hat, gibt es also ein $\rho \in k$, für das $P(\rho) \neq 0$ gilt, wobei P das nicht-konstante Polynom $P(X) = d'X^3 + c'X^2 + b$ bezeichnet. Dann liefert $A = \left(\begin{smallmatrix} 1 & 0 \\ e & 1 \end{smallmatrix}\right)$

$$Q_A(X,Y) = \underbrace{(d'\rho^3 + c'\rho^2 + b'\rho)}_{P(\rho)\neq 0} X^3 + (b' + 2c'\rho' + 3d'\rho^2)X^2Y + (c' + 3d'\rho)XY^2 + d'Y^3$$

die gewünschte Form.

Es seien α_1, α_2 und α_3 die Nullstellen von f in K. Dann gilt

$$Q(X,Y) = a \cdot \prod_{i=1}^{3} \left(X - \alpha_i Y\right),$$

und da Q nach Voraussetzung nicht-ausgeartet ist, folgt aus 6.3(ii), daß die Wurzeln α_i paarweise verschieden sind, d.h. die Diskriminante von f verschwindet nicht.

Sei $B \in \mathrm{GL}(2,k)$ eine weitere Matrix, für die Q_B die Form (25) hat, sei etwa

$$Q_B = a' \cdot \left(X^3 + b'X^2Y + c'XY^2 + d'Y^3\right),$$

sei $g := \frac{1}{a'} \cdot Q(X,1)$, und sei $C := BA^{-1} = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$. Dann ergibt sich:

$$\begin{aligned} g(X) &= (Q_A)_C(X,1) \\ &= a \cdot \prod_{i=1}^{3} \Big((rX+s) - \alpha_i(tX+u) \Big) \\ &= a \cdot \prod_{i=1}^{3} \Big((r - \alpha_i t)X - (\alpha_i u - s) \Big) \\ &\overset{a'\neq 0}{=} \underbrace{\left(a \prod_{i=1}^{3} (r - \alpha_i t) \right)}_{=a'} \cdot \prod_{i=1}^{3} \Big(X - \frac{\alpha_i u - s}{r - \alpha_i t} \Big), \end{aligned}$$

d.h. die Nullstellen von g sind rationale Ausdrücke in den α_i mit Koeffizienten aus k, d.h. der Zerfällungskörper von g liegt in M. Aus Symmetriegründen müssen die beiden Körper dann gleich sein, so daß M also wirklich unabhängig von A ist. **q.e.d.**

6.8 Theorem. Es sei $Q(X,Y) = aX^3 + bX^2Y + cXY^2 + dY^3$ eine nicht-ausgeartete Form über k mit $a \neq 0$. [†] Setze

$$\boxed{\begin{array}{lcll} \delta & := & -\dfrac{\Delta(Q)}{27} & \in k^\times, \\ e & := & \dfrac{a}{2} - \dfrac{27a^2d + 2b^3 - 9abc}{2\Delta(Q)}\sqrt{\delta} & \in k(\sqrt{\delta})^\times, \end{array}}$$

wobei in der Formel für e die Wurzel von δ so zu wählen ist, daß $e \neq 0$ ist (man kann natürlich höchstens dann null erhalten, wenn δ ein Quadrat in $k^\times$ ist).
Dann gilt:

$$\boxed{Q \cong \begin{cases} P\left\{\left(L_\delta, \left(e, \dfrac{\sqrt{\delta}}{e}\right)\right)\right\} & \text{falls } \delta \in k^{\times 2}, \\ P\{(L_\delta, e)\} & \text{sonst.} \end{cases}}$$

Wir haben also bei binären kubischen Formen eine vollkommen explizite Beschreibung der Bijektion ϑ aus 5.18; im allgemeinen Fall kennen wir ja nur die Umkehrabbildung ϑ^{-1} dank 5.17 explizit.

6.9 Bemerkung. In der Arbeit [HM00] werden binäre kubische Formen über viel allgemeineren Grundringen R untersucht, und unser Resultat 6.5 ist nur ein Spezialfall der dortigen Ergebnisse. Auch die Formel $\delta = -\frac{\Delta(Q)}{27}$ wird dort hergeleitet, sie geht sogar auf klassische Resultate von Eisenstein zurück.
Interessant und neu ist jedoch die Invariante e in 6.8, die im Fall $R = k$ die explizite Berechnung von ϑ gestattet.

Bevor wir zum Beweis des Theorems kommen, schicken wir zunächst zwei Lemmata vorweg:

6.10 Lemma. Es sei $f \in k[X]$ ein (nicht notwendig irreduzibles) normiertes Polynom vom Grad drei über k mit Diskriminante $\Delta \neq 0$, ferner seien $\delta := -\frac{\Delta}{27}$, $L := k(\sqrt{\delta})$, M der Zerfällungskörper von f über k und ζ eine primitive dritte Einheitswurzel in K. Dann gilt:

(i) Es gibt ein $\varepsilon \in L^\times$ mit der Eigenschaft, daß ε in $M' := M(\zeta)$ dritte Potenz eines $u \in M'$ ist und daß $M' = L(\zeta, u)$ ist.

(ii) Ist $\varepsilon' \in L$ ein weiteres Element mit $M' = L(\zeta, u')$ für ein geeignetes $u' \in M'$ mit ${u'}^3 = \varepsilon'$, so gilt:

(1) Ist δ *kein* Quadrat in $k^\times$ und L also eine echte quadratische Erweiterung von k, und bezeichnet τ das nicht-triviale Element der Galoisgruppe von L/k, so existiert ein $\eta \in L^\times$ derart, daß entweder $\varepsilon' = \varepsilon\eta^3$ oder $\tau(\varepsilon') = \varepsilon\eta^3$ ist.

[†] Dies ist keine Einschränkung, weil wir im Falle $a = 0$ nach 6.7 stets eine isomorphe Form mit $a \neq 0$ finden können

(2) Ist δ ein Quadrat in $k^\times$ und also $L = k$, so existiert ein $\eta \in k^\times$ derart, daß entweder $\varepsilon' = \varepsilon\eta^3$ oder $\frac{1}{\varepsilon'} = \varepsilon\eta^3$ ist.

Beweis:

(i) Es sei $f = X^3 + bX^2 + cX + d$. Für jedes $a \in k$ hat dann das Polynom $f(X - a)$ dieselbe Diskriminante und denselben Zerfällungskörper wie f; setzen wir speziell $a = \frac{b}{3}$, so ist

$$f\left(X - \frac{b}{3}\right) = X^3 + \left(c - \frac{1}{3}b^2\right)X - \left(\frac{2}{27}b^3 - \frac{1}{3}bc + d\right).$$

Wir können also ohne Beschränkung der Allgemeinheit annehmen, daß $b = 0$ gilt. Setzen wir noch $p := \frac{c}{3}$ und $q := \frac{d}{2}$, so erhalten wir $f = X^3 + 3pX + 2q$.

Dann ist $\Delta = -4 \cdot 27 \cdot (p^3 + q^2)$, also $\delta = \frac{p^3+q^2}{4}$, und wir setzen

$$\varepsilon := -q - \sqrt{p^3 + q^2} = -q - \frac{1}{2}\sqrt{\delta}, \tag{26}$$

wobei wir die Wurzel so wählen, daß $\varepsilon \neq 0$ ist, was möglich ist, weil die Diskriminante ja nach Voraussetzung nicht verschwindet. Wählen wir eine beliebige dritte Wurzel $u \in K$ von ε, und setzen wir $v := -\frac{p}{u}$, so folgt nach den Cardanoschen Formeln ([Bos93, 6.1]) dann $f = (X - x_1)(X - x_2)(X - x_3)$ mit

$$\begin{aligned} x_1 &= u + v, \\ x_2 &= \zeta u + \zeta^2 v, \\ x_3 &= \zeta^2 u + \zeta v. \end{aligned}$$

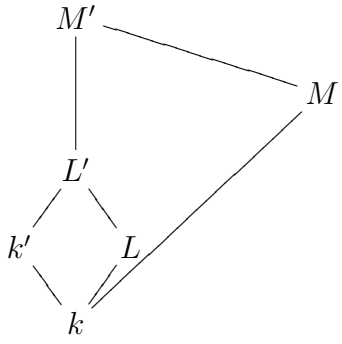
Also erhalten wir schon einmal $M' \subseteq L(\zeta, \varepsilon)$.

Wegen

$$\det \begin{pmatrix} 1 & 1 \\ \zeta & \zeta^2 \end{pmatrix} = \zeta^2 - \zeta = (-1 - \zeta) - \zeta = -1 - 2\zeta \neq 0$$

können wir die Gleichungen für x_1 und x_2 nach u und v auflösen und erhalten somit auch die umgekehrte Inklusion $L(\zeta, \varepsilon) \subseteq k'(x_1, x_2) = M'$.

(ii) Wir setzen $k' := k(\zeta)$, $L' := L(\zeta)$ und erhalten das folgende Hasse-Diagramm:



Bezeichne μ_3 die Gruppe der dritten Einheitswurzeln in k'. Die Inflations-Restriktions-Sequenzen in der Galoiskohomologie von μ_3 bezüglich der drei Körpertürme

$K/M'/L$, $K/M'/L'$ und $M'/L'/L$ liefern das folgende kommutative Diagramm von abelschen Gruppen mit exakten Zeilen und Spalten:

$$\begin{array}{ccccccc}
 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \\
 & & H^1(L'/L,\mu_3) & = & H^1(L'/L,\mu_3) & & \\
 & & \downarrow{\scriptstyle \inf} & & \downarrow{\scriptstyle \inf} & & \\
1 & \longrightarrow & H^1(M'/L,\mu_3) & \xrightarrow{\inf} & H^1(L,\mu_3) & \xrightarrow{\mathrm{res}} & H^1(M',\mu_3) \\
 & & \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \mathrm{res}} & & \| \\
1 & \longrightarrow & H^1(M'/L',\mu_3) & \xrightarrow{\inf} & H^1(L',\mu_3) & \xrightarrow{\mathrm{res}} & H^1(M',\mu_3)
\end{array}$$

Wegen $[L' : L] \leq 2$ und $(2,3) = 1$ gilt $H^1(L'/L,\mu_3) = 1$, und bekanntlich gilt für einen beliebigen Körper $N \subset K$, daß $H^1(N,\mu_3)$ isomorph zu $N^\times/N^{\times 3}$ ist. Tragen wir dies in obiges Diagramm ein, so erhalten wir:

$$\begin{array}{ccccccc}
 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & H^1(M'/L,\mu_3) & \xrightarrow{\inf} & L^\times/L^{\times 3} & \xrightarrow{\mathrm{res}} & M'^\times/M'^{\times 3} \\
 & & \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \mathrm{res}} & & \| \\
1 & \longrightarrow & H^1(M'/L',\mu_3) & \xrightarrow{\inf} & L'^\times/L'^{\times 3} & \xrightarrow{\mathrm{res}} & M'^\times/M'^{\times 3}
\end{array}$$

Betrachten wir die Elemente $[\varepsilon]$ und $[\varepsilon']$ aus $L^\times/L^{\times 3}$, so liegen sie im Kern der Restriktion nach $M'^\times/M'^{\times 3}$, stammen also von Kohomologieklassen aus $H^1(M'/L,\mu_3)$ ab, die wir ebenfalls mit $[\varepsilon]$ und $[\varepsilon']$ bezeichnen wollen.

Angenommen, $[\varepsilon]$ oder $[\varepsilon']$ wäre die triviale Klasse, gelte ohne Beschränkung der Allgemeinheit etwa $[\varepsilon] = 1$. Dann muß $\mathrm{res}([\varepsilon])$ trivial in $L'^\times/L'^{\times 3}$ sein, d.h. die dritten Wurzeln u, ζu und $\zeta^2 u$ von ε liegen schon in L'. Nach Voraussetzung gilt aber $M' = L'(u)$, d.h. in diesem Fall folgt $L' = M'$. Wegen $L' = M' = L'(u')$ muß dann aber auch $\varepsilon' = u'^3$ eine dritte Potenz in L' sein, d.h. auch $\mathrm{res}([\varepsilon'])$ ist trivial. Wir wissen aber schon, daß die Restriktion injektiv ist, es folgt also $[\varepsilon'] = 1 = [\varepsilon]$, d.h. die Aussage des Lemmas ist in diesem Fall bewiesen.

Seien also $[\varepsilon]$ und $[\varepsilon']$ beide *nicht* trivial. Wäre $[\varepsilon'] = [\varepsilon]$, so wäre die Aussage ebenfalls bewiesen. Wir müssen also nur den Fall betrachten, daß $[\varepsilon]$ und $[\varepsilon']$ verschiedene, nicht-triviale Klassen sind.

Wegen $\mu_3 \subset L'$ operiert $G_{M'/L'} := \mathrm{Gal}\,(M'/L')$ trivial auf μ_3, d.h. es ist

$$H^1(M'/L',\mu_3) = \mathrm{Hom}\,(G_{M'/L'},\mu_3).$$

Weiter ist $[M' : L'] \in \{1,3\}$, weil M' nach Voraussetzung der Zerfällungskörper des Polynoms $g := X^3 - \varepsilon \in L'[X]$ ist und g wegen $\mu_3 \subset L'$ entweder irreduzibel oder Produkt von drei Linearfaktoren sein muß. Im Falle $M' = L'$ folgte aber wie oben sofort $[\varepsilon] = [\varepsilon']$, und diesen Fall hatten wir ja ausgeschlossen. Also ist M'/L' eine Galoiserweiterung vom Grad drei mit Galoisgruppe A_3 und daher $H^1(M'/L',\mu_3)$

dreielementig. Da die Untergruppe $H^1(M'/L, \mu_3)$ die nicht-trivialen, verschiedenen Elemente $[\varepsilon]$ und $[\varepsilon']$ enthält, muß sie ebenfalls dreielementig sein, und es muß

$$[\varepsilon'] = [\varepsilon]^2 = [\varepsilon^2]$$

gelten. Insbesondere ist also der Quotient $\frac{\varepsilon'}{\varepsilon^2}$ eine dritte Potenz in L, und wir können für den Beweis des Lemmas ohne Beschränkung der Allgemeinheit $\varepsilon' = \varepsilon^2$ annehmen. Dann gilt

$$\frac{1}{\varepsilon'} = \frac{1}{\varepsilon^2} = \varepsilon \cdot \left(\frac{1}{\varepsilon}\right)^3,$$

d.h. Teil (2) des Lemmas ist bewiesen.

Sei jetzt also δ *kein* Quadrat in L. Wir müssen dann beweisen, daß $\frac{\tau(\varepsilon')}{\varepsilon} = \frac{\tau(\varepsilon^2)}{\varepsilon}$ eine dritte Potenz in L ist oder äquivalent, daß $\tau(\varepsilon) \cdot \varepsilon$ eine dritte Potenz in L ist:

$$\frac{\tau(\varepsilon^2)}{\varepsilon} = \eta^3 \;\Leftrightarrow\; \frac{\varepsilon^2}{\tau(\varepsilon)} = \big(\tau(\eta)\big)^3 \;\Leftrightarrow\; \frac{\tau(\varepsilon)}{\varepsilon^2} = \left(\frac{1}{\tau(\eta)}\right)^3 \;\Leftrightarrow\; \tau(\varepsilon)\cdot\varepsilon = \left(\frac{\varepsilon}{\tau(\eta)}\right)^3.$$

Setzen wir die explizite Formel (26) ein und beachten wir, daß $\tau(\sqrt{\delta}) = -\sqrt{\delta}$ gilt, weil δ kein Quadrat in k ist, so erhalten wir:

$$\tau(\varepsilon)\cdot\varepsilon = \left(-q - \frac{1}{2}\sqrt{\delta}\right)\left(-q + \frac{1}{2}\sqrt{\delta}\right) = q^2 - \frac{\delta}{4} = q^2 - (p^3 + q^2) = (-p)^3.$$

Damit ist das Lemma vollständig bewiesen.

q.e.d.

6.11 Lemma. Es seien alle Bezeichnungen wie in 6.8, weiter sei M der Zerfällungskörper von $f := \frac{1}{a} \cdot Q(X, 1)$ wie in 6.7, und es sei $M' := M(\zeta)$ wie in 6.10. Setze $\varepsilon' := e \cdot \sqrt{\delta}$. Dann ist ε' dritte Potenz eines $u' \in M'$, und es gilt $M' = k(\sqrt{\delta}, \zeta, u')$.

Beweis: Es sei g das normierte Polynom

$$g(X) := \frac{1}{a} \cdot f\left(X - \frac{b}{3a}\right) = X^3 + 3\underbrace{\left(\frac{3ac - b^2}{9a^2}\right)}_{=:p} X + 2\underbrace{\left(\frac{27a^2d + 2b^3 - 9abc}{54a^3}\right)}_{=:q}.$$

Bezeichnen Δ_f und Δ_g die Diskriminanten von$f$ bzw. g, so folgt aus 6.3(ii):

$$\begin{aligned} \Delta(Q) &= a^4 \cdot \Delta_f = a^4 \cdot \Delta_g = -a^4 \cdot 4 \cdot 27 \cdot (p^3 + q^2), \\ \sqrt{\delta} &= \sqrt{-\tfrac{\Delta(Q)}{27}} = \sqrt{4a^4(p^3 + q^2)} = 2a^2\sqrt{p^3 + q^2}. \end{aligned}$$

Einsetzen ergibt:

$$\begin{aligned} \varepsilon' &= \left(\frac{a}{2} - \frac{27a^2d + 2b^3 - 9abc}{2\Delta(Q)}\sqrt{\delta}\right) \cdot \sqrt{\delta} \\ &= \frac{a}{2}\sqrt{\delta} - \frac{54a^3q \cdot 4a^4(p^3 + q^2)}{-2a^4 \cdot 4 \cdot 27 \cdot (p^3 + q^2)} \\ &= a^3\sqrt{p^3 + q^2} + a^3q \\ &= a^3 \cdot (q + \sqrt{p^3 + q^2}) \\ &= (-a)^3 \cdot (-q - \sqrt{p^3 + q^2}). \end{aligned}$$

Werfen wir nun einen Blick zurück in den Beweis von 6.10(i), so sehen wir, daß zu dem dort konstruierten ε der Zusammenhang $\varepsilon' = (-a)^3 \cdot \varepsilon$ besteht. Weil ε die geforderten Eigenschaften hat, gilt dasselbe auch für unser ε', und das Lemma ist bewiesen. **q.e.d.**

Beweis des Theorems: Zunächst wollen wir zeigen, daß die Klasse (L_δ, e) bzw. $(L_\delta, (e, \frac{\sqrt{\delta}}{e}))$ aus $H^1_{\text{cont}}(G, S_2 \int \mu_3)$ nur von der Isomorphieklasse $[Q]$ von Q abhängt. Dazu stellen wir zuerst einmal fest, daß das Bild von δ in $k^\times/k^{\times 2}$ und damit die Isomorphieklasse von L_δ wegen 6.3 tatsächlich nur von $[Q]$ abhängen.

Sei nun $Q'(X,Y) = a'X^3 + b'X^2Y + c'XY^2 + d'Y^3$ eine weitere Form aus $[Q]$ mit $a' \neq 0$, und seien δ' und e' die zugehörigen Invarianten. Gemäß 5.11 müssen wir zeigen, daß es ein $a \in A_\delta$ und ein $y \in L_\delta^\times$ gibt mit $e' = a[ey^3]$ bzw. $(e', \frac{\sqrt{\delta'}}{e'}) = a[(e, \frac{\sqrt{\delta}}{e})y^3]$.

Seien alle Bezeichnungen wie in 6.10, und sei zunächst δ *kein* Quadrat in k. Nach 6.10 und 6.11 gibt es ein $\eta \in L(\sqrt{\delta})^\times = L_\delta^\times$, für das entweder $\sqrt{\delta'}e' = \sqrt{\delta}e\eta^3$ oder $\tau(\sqrt{\delta'}e') = \sqrt{\delta}e\eta^3$ gilt. Nach 6.3(i) ist $\frac{\delta'}{\delta}$ eine sechste Potenz in $k^\times$, gelte etwa $\frac{\delta'}{\delta} = \nu^6$. Dann können wir im ersten Fall $a := \mathrm{id}$ und $y := \frac{\eta}{\nu}$ und im zweiten Fall $a := \tau$ und $y := -\frac{\eta}{\nu}$ setzen (wobei man beachte, daß $\tau(\sqrt{\delta}) = -\sqrt{\delta}$ und $\tau(\nu) = \nu$ gilt):

$$\begin{aligned}
\underline{\text{1. Fall}}: \quad a[ey^3] &= e\left(\frac{\eta}{\nu}\right)^3 = e\eta^3 \cdot \frac{\sqrt{\delta}}{\sqrt{\delta'}} = e', \\
\underline{\text{2. Fall}}: \quad a[ey^3] &= \tau\left[e\left(-\frac{\eta}{\nu}\right)^3\right] = \tau\left[e\eta^3 \cdot \left(-\frac{\sqrt{\delta}}{\sqrt{\delta'}}\right)\right] = \frac{\tau\left[\sqrt{\delta}e\eta^3\right]}{\sqrt{\delta'}} = e'.
\end{aligned}$$

Sei jetzt δ ein Quadrat in k. Dann gibt es — wieder nach 6.10 und 6.11 — ein $\eta \in k^\times$, für das entweder $\sqrt{\delta'}e' = \sqrt{\delta}e\eta^3$ oder $\frac{1}{\sqrt{\delta'}e'} = \sqrt{\delta}e\eta^3$ gilt. Setze dann im ersten Fall $a := \mathrm{id}$ und $y := (\frac{\eta}{\nu}, \frac{\nu^2}{\eta})$ und im zweiten Fall $a := \tau$ und $y := (\frac{\sqrt{\delta'}\eta}{\nu}, \frac{\nu^2}{\sqrt{\delta'}\eta})$:

$$\begin{aligned}
\underline{\text{1. Fall}}: \quad a\left[\left(e, \tfrac{\sqrt{\delta}}{e}\right)y^3\right] &= \left(e\eta^3 \cdot \frac{\sqrt{\delta}}{\sqrt{\delta'}}, \sqrt{\delta'} \cdot \frac{\sqrt{\delta'}}{\sqrt{\delta}} \cdot \frac{1}{e\eta^3}\right) = \left(e', \frac{\sqrt{\delta'}}{e'}\right), \\
\underline{\text{2. Fall}}: \quad a\left[\left(e, \tfrac{\sqrt{\delta}}{e}\right)y^3\right] &= \tau\left(\delta'\sqrt{\delta}e\eta^3, \frac{1}{\sqrt{\delta\delta'}e\eta^3}\right) = \left(e', \frac{\sqrt{\delta'}}{e'}\right).
\end{aligned}$$

Damit haben wir bewiesen, daß die Q zugeordnete Form der Fermatgleichung nur von der Isomorphieklasse $[Q]$ abhängt. Es bleibt zu zeigen, daß die zugeordnete Form wieder isomorph zu Q ist. Wir wissen aber schon aus 6.5, daß es eine Form $P := P_2^3\{(L'_\delta, x)\}$ gibt, die isomorph zu Q ist. Wir müssen also nur zeigen, daß P sich selbst zugeordnet wird.

Seien also $\delta' \in k^\times$ und $x \in L_{\delta'}$ beliebig. Gelte zunächst $\delta \notin k^{\times 2}$ und $x = y + z\alpha$ mit $\alpha^2 = \delta'$. Dann erhalten wir nach 5.17 bezüglich der Basis $\{1, \alpha\}$ von $L_{\delta'}$:

$$\begin{aligned}
P &:= P_2^3\{(\delta', x)\} \\
&= \mathrm{Tr}_{L_{\delta'}/k}\left[(y + z\alpha) \cdot (X + \alpha Y)^3\right] \\
&= \mathrm{Tr}_{L_{\delta'}/k}\left[(y + z\alpha)X^3 + (3y\alpha + 3\delta' z)X^2Y + (3\delta' y + 3\delta' z\alpha)XY^2 + (\delta'^2 z + \delta' y\alpha)Y^3\right] \\
&= (2y)X^3 + (6\delta' z)X^2Y + (6\delta' y)XY^2 + (2\delta'^2 z)Y^3.
\end{aligned}$$

Also gilt $a = 2y$, $b = 6\delta' z$, $c = 6\delta' y$ und $d = 2\delta'^2 z$.

1. Fall: $y \neq 0$,
dann ist $a \neq 0$, und wir können uns direkt daran machen, die Invarianten zu berechnen:

$$\begin{aligned} \Delta(P) &= -1728\,\delta'^3(y^2 - \delta' z^2)^2 = (-27\delta') \cdot \left[8\delta'(y^2 - \delta' z^2)\right]^2, \\ \delta &= \delta' \cdot \left[8\delta'(y^2 - \delta' z^2)\right]^2, \\ e &= y - \frac{\delta'^2(y^2 - \delta' z^2)z}{\delta'^2(y^2 - \delta' z^2)} \cdot \alpha = y - z\alpha = \tau[y + z\alpha] = \tau[x]. \end{aligned}$$

2. Fall: $y = 0$,
wegen $x \neq 0$ muß dann $z \neq 0$ sein, und wir können zu P_A für $A := \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ übergehen:

$$P_A = (2\delta'^2 z)X^3 + (6\delta' y)X^2 Y + (6\delta' z)XY^2 + (2y)Y^3.$$

Wegen $\det(A) = -1$ und 6.3(i) ist $\Delta(P_A) = \Delta(P)$, d.h. auch δ ist dasselbe wie oben, und für e ergibt sich

$$e = \delta'^2 z - \frac{\delta'^4 z^2 y - \delta'^3 y^3}{\delta'^2(y^2 - \delta_1 z^2)} \cdot \alpha = \delta'^2 z + \delta' y\alpha = (y + \alpha z) \cdot \alpha^3 = x \cdot \alpha^3.$$

— In beiden Fällen ist die Aussage damit gezeigt.

Es bleibt der Fall, daß δ' ein Quadrat in k ist. Sei $x = (y, z)$, dann erhalten wir nach 5.17 bezüglich der Basis $\{(1,0),(0,1)\}$ die Darstellung

$$P := P_2^3\{(\delta', x)\} = yX^3 + zY^3,$$

d.h. $a = y$, $b = c = 0$ und $d = z$. Wegen $y, z \in k^\times$ benötigen wir diesmal glücklicherweise keine Fallunterscheidung:

$$\begin{aligned} \Delta(P) &= -27y^2 z^2, \\ \delta &= y^2 z^2 = (yz)^2, \\ e &= \frac{y}{2} - \frac{27y^2 z}{-54y^2 z^2} \cdot (\pm yz) = \frac{y}{2} \pm \frac{y}{2} = y, \end{aligned}$$

weil wir ja die Wurzel von $y^2 z^2$ so wählen sollen, daß $e \neq 0$ ist. Dann ist

$$(e, \frac{\sqrt{\delta}}{e}) = (y, \frac{yz}{y}) = (y, z) = x,$$

und auch in diesem Fall ist die Behauptung gezeigt. Damit ist das Theorem vollständig bewiesen. **q.e.d.**

6.12 Beispiel. Zu welcher Form $P_2^3\{b\}$ ist die binäre kubische Form $Q(X,Y) := X^2Y + XY^2$ über $\mathbb{Q}$ isomorph?

Zunächst berechnen wir mit (24) die Diskriminante und erhalten $\Delta(Q) = 0 + 0 + 1^2 \cdot 1^2 - 0 - 0 = 1$; insbesondere ist Q also nicht-ausgeartet.

Leider ist der Koeffizient von X^3 null, so daß wir Q zunächst mit Hilfe von 6.7 transformieren müssen. Mit den Bezeichnungen aus dem Beweis von 6.7 müssen wir ein $\rho \in \mathbb{Q}$

mit $P(\rho) = \rho^2 + \rho \neq 0$ suchen — nehmen wir zum Beispiel $\rho := 1$. Dann ist $A = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$, und wir erhalten die isomorphe Form

$$Q_A(X, Y) = Q(X, X + Y) = 2X^3 + 3X^2Y + XY^2,$$

also $a = 2$, $b = 3$, $c = 1$ und $d = 0$.

Nun können wir die Invarianten δ und e berechnen, wobei wir beachten, daß wegen 6.3(i) die Diskriminante von Q_A wegen $\det(A) = 1$ gleich $\Delta(Q)$ ist:

$$\begin{aligned} \delta &= -\frac{1}{27}, \\ e &= \frac{2}{2} - \frac{0 + 2 \cdot 3^3 - 9 \cdot 2 \cdot 3 \cdot 1}{2 \cdot 1}\sqrt{-\frac{1}{27}} = 1. \end{aligned}$$

Also ist $L_\delta = \mathbb{Q}\left(\sqrt{-\frac{1}{27}}\right) = \mathbb{Q}(\sqrt{-3})$, und wir erhalten $\boxed{Q \cong P_2^3\left\{\left(\mathbb{Q}(\sqrt{-3}), 1\right)\right\}}$.

7 Formen der Fermatgleichung in $\widetilde{\mathcal{F}_k^{n,m}}$

Es seien wieder $m, n \geq 1$ natürliche Zahlen, k ein Körper mit $(\operatorname{char} k) \nmid m!$, $K := \bar{k}$ ein separabler algebraischer Abschluß von k, $G := \operatorname{Gal}(K/k)$ die absolute Galoisgruppe und $P_n^m := X_1^m + \ldots + X_n^m \in k[X_i]$. — Diesmal wollen wir P_n^m aber in erster Linie als ein Objekt aus $\widetilde{\mathcal{F}_k^{n,m}}$ auffassen! — Wie wir in der Einleitung erläutert haben, ist dies die natürlichere Sicht, wenn wir P_n^m als „Gleichung“ sehen und (nur) an der Anzahl der Lösungen dieser Gleichung interessiert sind.

In diesem Kapitel werden wir untersuchen, wie man die Ergebnisse aus dem fünften Kapitel modifizieren muß, um die K/k-Formen der Fermatgleichung in $\widetilde{\mathcal{F}_k^{n,m}}$ zu verstehen.

7.1 Satz/ Definition. Die Gruppe μ_m bettet sich diagonal in die Gruppe μ_m^n und damit in das Kranzprodukt von S_n mit μ_m ein, wo sie im Zentrum liegt und also ein Normalteiler ist; bezeichne $\tilde{A} := \tilde{A_n^m}$ den Quotienten:

$$\tilde{A} := \tilde{A_n^m} := \left(S_n \int \mu_m\right) / \mu_m.$$

Dann induziert die in 5.1 definierte Einbettung $S_n \int \mu_m \hookrightarrow \mathrm{GL}(n, K)$ eine Einbettung $\tilde{A} \hookrightarrow \mathrm{PGL}(n, K)$:

$$\begin{array}{ccc} S_n \int \mu_m & \hookrightarrow & \mathrm{GL}(n,K) \\ \downarrow & = & \downarrow \\ \tilde{A} & \hookrightarrow & \mathrm{PGL}(n,K), \end{array}$$

und bezüglich dieser Einbettung ist $\tilde{A}$ eine Untergruppe der Automorphismengruppe von P_n^m in $\widetilde{\mathcal{F}_K^{n,m}}$. Ist $m \geq 3$, so gilt sogar Gleichheit, d.h. in diesem Fall haben wir

$$A(P_n^m) := \operatorname{Aut}_{\widetilde{\mathcal{F}_K^{n,m}}}(P_n^m) = \tilde{A}.$$

Beweis:

- *wohldefiniert:* Klar!
- *Einbettung:* Seien $\overline{(\zeta_i)_i \cdot \sigma}$ und $\overline{(\xi_i)_i \cdot \tau}$ zwei Elemente aus $\tilde{A}$, die in $\mathrm{PGL}(n, K)$ auf dasselbe Element abgebildet werden, d.h. die Bilder von $(\zeta_i)_i \cdot \sigma$ und $(\xi_i)_i \cdot \tau$ in $\mathrm{GL}(n, K)$ unterscheiden sich nur um ein Skalar $c \in K^\times$. Dann folgt aber sofort, daß $\sigma = \tau$ und $\zeta_i = c \cdot \xi_i$ für alle $i \in \{1, \ldots, n\}$ gilt, daß also $c \in \mu_m$ ist und damit $\overline{(\zeta_i)_i \cdot \sigma} = \overline{(\xi_i)_i \cdot \tau}$.
- *Untergruppe von $A(P_n^m)$:* Klar nach Definition von $A(P_n^m)$!
- *Gleichheit im Fall $m \geq 3$:* Sei also $m \geq 3$, und sei $\bar{B} \in \mathrm{PGL}(n, K)$ ein K-Automorphismus von P_n^m, repräsentiert durch $B \in \mathrm{GL}(n, K)$. Nach Definition von Morphismen in der Kategorie $\widetilde{\mathcal{F}_K^{n,m}}$ gibt es dann ein $c \in K^\times$ mit $P_n^m(BX) = c \cdot P_n^m$. Sei $d \in K^\times$ eine m-te Wurzel von c, und sei $B' \in \mathrm{GL}(n, K)$ die Matrix $\frac{1}{d}B$. Es folgt

  $$P_n^m(B'X) = P_n^m(\tfrac{1}{d}BX) = \left(\tfrac{1}{d}\right)^m \cdot P_n^m(BX) = P_n^m,$$

  d.h. B' ist ein K-Automorphismus von P_n^m in der Kategorie $\mathcal{F}_K^{n,m}$. Nach 5.2 ist B' dann ein Element aus $S_n \int \mu_m$, und die Behauptung folgt, da natürlich $\bar{B'} = \bar{B}$ in $\mathrm{PGL}(n, K)$ gilt.

q.e.d.

7.2 Lemma/ Definition. Die Gruppe S_n operiert via

$$^{\sigma}\overline{(\zeta_1,\ldots,\zeta_n)} := \overline{(\zeta_{\sigma^{-1}(1)},\ldots,\zeta_{\sigma^{-1}(n)})}$$

von links auf der Gruppe μ_m^n/μ_m (wobei μ_m wieder diagonal in μ_m^n eingebettet sei), und die offensichtliche Abbildung

$$\begin{array}{rcccc} \tilde{A} & = & (\mu_m^n \rtimes S_n)/\mu_m & \longrightarrow & (\mu_m^n/\mu_m) \rtimes S_n \\ & & \overline{(\zeta_i)_i \cdot \sigma} & \mapsto & \overline{(\zeta_i)_i} \cdot \sigma \end{array}$$

ist ein Isomorphismus. In Zukunft wollen wir die Gruppe $\tilde{A}$ auf diese Weise mit der Gruppe $(\mu_m^n/\mu_m) \rtimes S_n$ identifizieren!

Beweis: Klar! **q.e.d.**

7.3 Lemma. Durch

$$^{s}\big(\overline{(\zeta_i)_i} \cdot \sigma\big) := \big(\overline{(^{s}\zeta_i)_i} \cdot \sigma\big) \qquad (\text{für } s \in G,\ \zeta_1,\ldots,\zeta_n \in \mu_m \text{ und } \sigma \in S_n \text{ beliebig}) \qquad (27)$$

wird auf $\tilde{A}$ eine stetige Links-G-Operation definiert, die den Normalteiler $(\mu_m^n/\mu_m) \trianglelefteq \tilde{A}$ invariant läßt.
Ist $m \geq 3$ (und also $\tilde{A} = \mathrm{Aut}_K(P_n^m)$ nach 7.1), so stimmt diese Operation mit der in Beispiel 1.6(v) definierten und nach Beispiel 3.5(ii) stetigen Operation überein.

Beweis:

- *diskrete G-Gruppen-Struktur:* Die Gruppe $S_n \int \mu_m$ ist nach 2.16 eine diskrete G-Gruppe, und man sieht sofort, daß der Normalteiler $\mu_m \trianglelefteq S_n \int \mu_m$ invariant unter der G-Operation ist. Nach 2.11 ist dann auch der Quotient $\tilde{A}$ eine diskrete G-Gruppe, und Formel (27) ergibt sich sofort aus 2.11 und 7.2.
  Diese Operation auf $\tilde{A}$ ist offenbar auch die (für $S = G$, $T = S_n$ und $A = \mu_m^n/\mu_n$) durch 2.14 definierte, woraus insbesondere folgt, daß der Normalteiler $\mu_m^n/\mu_n \trianglelefteq \tilde{A}$ invariant ist, eine Tatsache, die man natürlich auch direkt aus (27) ablesen kann.
- *Übereinstimmung im Fall $m \geq 3$:* Für jede Operation von G auf $\tilde{A}$ muß $^{s}\overline{(\mu_i)_i} \cdot \sigma) = \overline{^{s}(\mu_i)_i} \cdot {}^{s}\sigma$ gelten, und nach Gleichung (4) operiert G auf $\mathrm{PGL}(n,K)$ durch Operation auf den Einträgen einer repräsentierenden Matrix, woraus $\overline{^{s}(\mu_i)_i} = \overline{(^{s}\mu_i)_i}$ und ${}^{s}\sigma = \sigma$ folgt, da man das Bild von σ in $\mathrm{PGL}(n,K)$ durch eine Permutationsmatrix mit Einträgen aus $\{0,1\}$, also insbesondere aus k, repräsentieren kann und σ demnach fix unter der Galois-Operation ist.

q.e.d.

7.4 Lemma/ Definition. Von nun an bezeichne $p : S_n \int \mu_m \twoheadrightarrow \tilde{A}$ die kanonische Projektion. Folgendes Diagramm ist dann kommutativ in der Kategorie der diskreten G-Gruppen, und alle Zeilen und Spalten sind exakt:

$$\begin{array}{ccccccccc}
 & & & & 1 & & 1 & & \\
 & & & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mu_m & \longrightarrow & \mu_m^n & \longrightarrow & \mu_m^n/\mu_m & \longrightarrow & 1 \\
 & & \| & = & \downarrow & = & \downarrow & & \\
1 & \longrightarrow & \mu_m & \longrightarrow & S_n \int \mu_m & \xrightarrow{p} & \tilde{A} & \longrightarrow & 1 \\
 & & & & \downarrow & = & \downarrow & & \\
 & & & & S_n & = & S_n & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 1 & & 1 & &
\end{array} \tag{28}$$

Beweis: Klar! **q.e.d.**

7.5 Lemma. Der Morphismus von Koeffizientenerweiterungen aus 3.11(iv) induziert nach 3.4, 3.5(ii) und 3.10 das folgende Diagramm in der Kategorie der punktierten Mengen, wobei die Abbildung φ *surjektiv* ist:

$$\begin{array}{ccc}
E_{\mathcal{F}_k^{n,m}}(K/k, P_n^m) & \xrightarrow[[Q] \mapsto [Q]]{\varphi} & E(K/k, P_n^m) \\
\vartheta \downarrow & = & \downarrow \vartheta \\
H^1_{\mathrm{cont}}(G, A_{\mathcal{F}_k^{n,m}}(P_n^m)) & \xrightarrow[\psi]{(a_s) \mapsto (\bar{a}_s)} & H^1_{\mathrm{cont}}(G, A(P_n^m)).
\end{array}$$

Beweis: Sei Q eine beliebige Form von P_n^m in der Kategorie $\widetilde{\mathcal{F}_k^{n,m}}$. Es gibt also einen Isomorphismus $\bar{A} \in \mathrm{PGL}\,(n, K)$ von Y nach P_n^m. Wird $\bar{A}$ durch eine reguläre Matrix A repräsentiert, so bedeutet das nach Definition, daß es ein $\lambda \in K^\times$ gibt mit $P_n^m(AX) = \lambda \cdot Q$. Setzt man demnach $A' := \frac{1}{\sqrt[m]{\lambda}} \cdot A$, so gilt

$$P_n^m(A'X) = \left(\frac{1}{\sqrt[m]{\lambda}}\right)^m \cdot P_n^m(AX) = \frac{1}{m} \cdot m \cdot Q = Q,$$

d.h. A' definiert einen Isomorphismus von Q nach P_n^m in $\mathcal{F}_k^{n,m}$. Das Polynom Q ist also auch dort eine Form von P_n^m, und die Surjektivität von φ ist bewiesen. **q.e.d.**

7.6 Korollar. Ist $m \geq 3$, so ist das Bild von $E_{\widetilde{\mathcal{F}_k^{n,m}}}(K/k, P_n^m)$ unter ϑ gleich dem Bild von $H^1_{\mathrm{cont}}(G, \mathrm{Aut}_{\mathcal{F}_k^{n,m}}(P_n^m))$ unter ψ, d.h. es gilt:

$$\boxed{E(K/k, P_n^m) \xrightarrow{\sim} \mathrm{Im}\left(H^1_{\mathrm{cont}}(G, S_n \int \mu_m) \xrightarrow{H^1_{\mathrm{cont}}(p)} H^1_{\mathrm{cont}}(G, \tilde{A})\right)}$$

Beweis: Klar nach 5.2, 5.18, 7.1 und 7.5! **q.e.d.**

7.7 Satz. Zwei Klassen aus $H^1_{\mathrm{cont}}(G, S_n \int \mu_m)$, gemäß 5.11 gegeben durch Paare (L, x) und (L', x'), werden genau dann unter $H^1_{\mathrm{cont}}(p)$ in $H^1_{\mathrm{cont}}(G, \tilde{A})$ auf dieselbe Klasse abgebildet, wenn es ein $\lambda \in k^\times$ gibt mit $(L', x') = (L, \lambda x) \in H^1_{\mathrm{cont}}(G, S_n \int \mu_m)$.

Beweis: Wir bezeichnen den durch (L, x) definierten 1-Kozykel von G in $S_n \int \mu_m$ mit $b = (b_s)$, twisten die untere kurze exakte Sequenz aus Diagramm (28) mit b, gehen zur langen exakten Kohomologiesequenz über (vgl. 2.27!) und erhalten:

$$H^1(G, \mu_{m,b}) \longrightarrow H^1(G, (S_n \int \mu_m)_b) \xrightarrow{H^1_{\mathrm{cont}}(p)} H^1(G, \tilde{A}_b)$$

ist exakt.

Wie man leicht sieht, liegt der Normalteiler μ_m im *Zentrum* von $S_n \int \mu_m$, d.h. nach 2.24 gilt $\mu_{m,b} = \mu_m$. Wir haben also den wohlbekannten Kummerisomorphismus

$$\begin{array}{ccc} k^\times/(k^\times)^m & \xrightarrow{\sim} & H^1_{\mathrm{cont}}(G, \mu_{m,b}) \\ \lambda & \mapsto & \left(\frac{s\sqrt[m]{\lambda}}{\sqrt[m]{\lambda}}\right)_s . \end{array}$$

Nach 2.33 hat die durch (L', x') gegebene Klasse genau dann dasselbe Bild wie b in $H^1_{\mathrm{cont}}(G, \tilde{A})$, wenn sie durch einen 1-Kozykel der Form $(a_s \cdot b_s)$ gegeben wird für eine Klasse (a_s) aus $H^1_{\mathrm{cont}}(G, \mu_{m,b})$. Nach obiger Überlegung sind dies genau die Klassen $\left(\frac{s\sqrt[m]{\lambda}}{\sqrt[m]{\lambda}} \cdot b_s\right)$ mit $\lambda \in k^\times$. Einsetzen der expliziten Formel für (b_s) aus 5.11 liefert (wobei (c_s) den durch L definierten 1-Kozykel von G in S_n bezeichne):

$$\left(\frac{s\sqrt[m]{\lambda}}{\sqrt[m]{\lambda}} \cdot b_s\right) = \left(\left(\frac{s\sqrt[m]{\lambda} \cdot s\sqrt[m]{s^{-1}\varphi x}}{\sqrt[m]{\lambda} \cdot \sqrt[m]{\varphi x}}\right)_\varphi \cdot c_s\right)_s = \left(\left(\frac{s\sqrt[m]{s^{-1}\varphi(\lambda x)}}{\sqrt[m]{\varphi(\lambda x)}}\right)_\varphi \cdot c_s\right)_s = (L, \lambda x).$$

(Für die letzte Gleichheit beachte man, daß alle $s \in G$ und alle $\varphi \in M$ nach Definition k-Morphismen sind, also λ auf sich selbst abbilden!)

Insgesamt erhalten wir, daß die Klasse (L', x') genau dann dasselbe Bild wie (L, x) in $H^1_{\mathrm{cont}}(G, \tilde{A})$ hat, wenn sie von der Form $(L, \lambda x)$ für ein geeignetes $\lambda \in k^\times$ ist — und dies ist gerade die Behauptung, der Satz ist also bewiesen. **q.e.d.**

7.8 Korollar. Für eine separable k-Algebra L wollen wir zwei Klassen $[x], [x']$ aus der Menge $\mathrm{Aut}_k(L)\backslash(L^\times/L^{\times m})$, repräsentiert durch Elemente $x, x' \in L^\times$, *äquivalent* nennen, wenn es ein $\lambda \in k^\times$ gibt mit $[x] = [\lambda x']$, d.h. mit $(L, x) = (L, \lambda x') \in H^1_{\mathrm{cont}}(G, S_n \int \mu_m)$. — Nach 5.11 ist $(L, x) = (L, \lambda x')$ äquivalent dazu, daß es ein $y \in L^\times$ und ein $a \in \mathrm{Aut}_k(L)$ gibt mit $x = \psi(a[\lambda x' y^m])$.

Die Menge der Äquivalenzklassen werde mit $\mathrm{Aut}_k(L)\backslash(L^\times/L^{\times m})/k^\times$ bezeichnet. Wir haben dann das folgende kommutative Diagramm von punktierten Mengen:

$$\begin{array}{ccc} \coprod_{[L]} \mathrm{Aut}_k(L)\backslash(L^\times/L^{\times m}) & \xrightarrow{\quad\mathrm{can}\quad} & \coprod_{[L]} \mathrm{Aut}_k(L)\backslash(L^\times/L^{\times m})/k^\times \\ \big\downarrow \wr & = & \big\downarrow \frown \\ H^1_{\mathrm{cont}}(G, S_n \int \mu_m) & \xrightarrow[H^1_{\mathrm{cont}}(p)]{} & H^1_{\mathrm{cont}}(G, \tilde{A}) \end{array}$$

Dabei laufen die disjunkten Vereinigungen über alle k-Isomorphieklassen von endlichen, separablen k-Algebren L vom Grad n, und die ausgezeichneten Elemente sind die durch $(k^n, 1)$ gegebenen.

Beweis: Klar nach 5.11 und 7.7! **q.e.d.**

7.9 Korollar. Es sei $m \geq 3$. Dann induziert die Abbildung ϑ eine Bijektion von punktierten Mengen

$$\boxed{E(K/k, P_n^m) \xrightarrow{\sim} \coprod_{[L]} \mathrm{Aut}_k(L)\backslash(L^\times/L^{\times m})/k^\times}$$

Die Umkehrabbildung schickt ein Paar (L, x) auf die Isomorphieklasse von $P_n^m\{(L, x)\}$.

Beweis: Klar nach 7.6 und 7.8! **q.e.d.**

Als Anwendung werden wir nun nicht-ausgeartete binäre kubische Formen über einem endlichen Körper k bis auf Isomorphie in $\widetilde{\mathcal{F}_k^{2,3}}$ klassifizieren:

7.10 Korollar. Es sei speziell k ein *endlicher* Körper, und es sei Q eine beliebige nicht-ausgeartete binäre kubische Form über k.

Seien alle Bezeichnungen wie in 6.6, dann gilt:

(i) Enthält k die dritte Einheitswurzeln, so ist Q in $\widetilde{\mathcal{F}_k^{2,3}}$ isomorph zu einer der folgenden drei getwisteten Fermatformen (wobei wieder $\{1, \beta\}$ als Basis von L_δ und $\{(1,0), (0,1)\}$ als Basis von $L_1 = k \times k$ gewählt wurden):

$$\boxed{\begin{array}{lcl} P_2^3\{(L_1, (1,1))\} & = & X^3 + Y^3, \\ P_2^3\{(L_1, (1,\delta))\} & = & X^3 + \delta Y^3, \\ P_2^3\{(L_\delta, 1)\} & = & 2X^3 + 6\delta XY^2. \end{array}}$$

(ii) Enthält k die dritten Einheitswurzeln *nicht*, so ist Q in $\widetilde{\mathcal{F}_k^{2,3}}$ isomorph zu einer der folgenden drei getwisteten Fermatformen (wobei die Basen wie oben gewählt wurden):

$$\begin{array}{lcl} P_2^3\{(L_1,(1,1))\} & = & X^3+Y^3, \\ P_2^3\{(L_\delta,1)\} & = & 2X^3+6\delta XY^2 \\ P_2^3\{(L_\delta,\alpha)\} & = & \mathrm{Tr}_{k'/k}(\alpha)\cdot X^3+3\cdot\mathrm{Tr}_{k'/k}(\alpha\beta)\cdot X^2Y \\ & & \quad +3\delta\cdot\mathrm{Tr}_{k'/k}(\alpha)\cdot XY^2+\delta\cdot\mathrm{Tr}_{k'/k}(\alpha\beta)\cdot Y^3. \end{array}$$

Beweis: Es sei $k=\mathbb{F}_q$.

(i) Es ist $(\delta,\delta)=\delta\cdot(1,1)$, $(\delta^2,\delta^2)=\delta^2\cdot(1,1)$ und $(1,\delta^2)=\tau[\delta^2\cdot(\delta,1)]$, ferner $(\delta,\delta^2)=\delta\cdot(1,\delta)$. Aus 7.8 folgt dann, daß sowohl die Klassen $(L_1,(1,1))$, $(L_1,(\delta,\delta))$ und $(L_1,(\delta^2,\delta^2))$ als auch die Klassen $(L_1,(1,\delta))$, $(L_1,(1,\delta^2))$ und $(L_1,(\delta,\delta^2))$ äquivalent sind. Außerdem sieht man leicht, daß $(L_1,(1,1))$ und $(L_1,(1,\delta))$ nicht äquivalent sein können.

Um zu beweisen, daß auch die Klassen $(L_\delta,1)$, (L_δ,α) und (L_δ,α^2) äquivalent sind, schreiben wir q als $3s+1$ mit $s\in\mathbb{N}_+$; dann gilt

$$\begin{aligned} \overbrace{(\alpha^{s+1})^3}^{\in L_\delta^{\times 3}}\cdot 1\cdot\frac{1}{\delta} &= \alpha^{(3s+3)-(3s+1+1)}=\alpha, \\ \underbrace{\left(\frac{1}{\alpha^s}\right)^3}_{\in L_\delta^{\times 3}}\cdot 1\cdot\delta &= \alpha^{-3s+(3s+1+1)}=\alpha^2. \end{aligned}$$

(ii) Wir müssen uns nur überlegen, daß $(L_\delta,1)$ und (L_δ,α) nicht äquivalent sind. Schreibe q als $3s+2$ mit einem $s\in\mathbb{N}_+$! Wären $(L_\delta,1)$ und (L_δ,α) äquivalent, dann gäbe es nach 7.8 Zahlen $u,v\in\mathbb{N}_0$ mit $\alpha=(\alpha^u)^3\cdot 1\cdot\delta^v$ oder $\alpha^q=(\alpha^u)^3\cdot 1\cdot\delta^v$. Das kann aber nicht sein, da zwar

$$(\alpha^u)^3\cdot 1\cdot\delta^v=\alpha^{3u+(3s+2+1)v}=(\alpha^{u+(s+1)v})^3$$

eine dritte Potenz ist, α und α^q aber offenbar nicht.

q.e.d.

7.11 Beispiele. Wir wollen die Beispiele 5.16 und 5.25 fortsetzen und die $\mathbb{C}/\mathbb{R}$-Formen von P_3^4 sowie die $\overline{\mathbb{F}_5}/\mathbb{F}_5$-Formen von P_4^3 berechnen:

(i) Nach 7.7 definieren $\big(\mathbb{R}^3,(1,1,1)\big)$ und $\big(\mathbb{R}^3,(-1,-1,-1)\big)$ dieselbe Klasse, ebenso $\big(\mathbb{R}^3,(1,1,-1)\big)$ und $\big(\mathbb{R}^3,(1,-1,-1)\big)$ sowie $\big(\mathbb{C}^2\times\mathbb{R},(1,1)\big)$ und $\big(\mathbb{C}^2\times\mathbb{R},(1,-1)\big)$. Also folgt, daß es genau drei $\mathbb{C}/\mathbb{R}$-Formen von P_3^4 gibt, nämlich

$$E(\mathbb{C}/\mathbb{R},P_3^4)=\{x^4+y^4+z^4,\ x^4+y^4-z^4,\ 2x^4-12x^2y^2+2y^4+z^4\}.$$

(ii) Wie schon bemerkt, ist das Nehmen der dritten Potenz in $\mathbb{F}_5$ *bijektiv*, d.h. für jede k-Algebra L (die separabel und endlich vom Grad vier über $\mathbb{F}_5$ ist) gilt $k^\times \subseteq (L^\times)^3$. Deswegen haben wir offenbar

$$\mathrm{Aut}_{\mathbb{F}_5}\backslash(L^\times/(L^\times)^3)/\mathbb{F}_5^\times = \mathrm{Aut}_{\mathbb{F}_5}\backslash(L^\times/(L^\times)^3),$$

und wir sehen, daß alle neun in 5.25 aufgelisteten Formen auch in der Kategorie $\widetilde{\mathcal{F}^{4,3}}$ paarweise nicht-isomorph bleiben.

8 Spezialisierung

Es seien $n, m \in \mathbb{N}_+$ positive natürliche Zahlen, A ein Dedekind-Ring, K der Quotientenkörper von A und $\mathfrak{p} \subset A$ ein maximales Primideal mit zugehöriger diskreter Bewertung $v_\mathfrak{p} : K \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$ und Restklassenkörper $\kappa(\mathfrak{p})$. Ferner sei L/K eine Galoiserweiterung mit Galoisgruppe G, B der ganze Abschluß von A in L und $\mathfrak{P} \subset B$ ein maximales Primideal von B, das über $\mathfrak{p}$ liegt, mit Restklassenkörper $\kappa(\mathfrak{P})$. Wir setzen voraus, daß die Restklassenkörpererweiterung $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ separabel ist.

In diesem Kapitel werden wir die *Spezialisierung*, d.h. die Reduktion modulo $\mathfrak{p}$, sowohl für Objekte P aus $\widetilde{\mathcal{F}_K^{n,m}}$ als auch für Kohomologieklassen aus $H^1_{\mathrm{cont}}(G, A(P))$ definieren und insbesondere zeigen, daß diese beiden Reduktionen miteinander verträglich sind. Wir werden dann speziell den Fall der Fermatgleichung P_n^m betrachten und untersuchen, wie sich die Spezialisierung in Termen der Charakterisierung von Kohomologieklassen durch Paare (L, x) ausdrücken läßt.

8.1 Lemma/ Definition. Für eine Matrix $M = (m_{ij})_{ij} \in \mathrm{End}\,(K^n)$ setze $v_\mathfrak{p}(M) := \min_{i,j} v_\mathfrak{p}(m_{ij}) \in \mathbb{Z} \cup \{\infty\}$.

Sei nun $\bar{M} \in \mathrm{PGL}\,(n, K)$, repräsentiert durch $M \in \mathrm{GL}\,(n, K)$. Dann gilt:

(i) $v_\mathfrak{p}(\det M) \geq n \cdot v_\mathfrak{p}(M)$,

(ii) $v_\mathfrak{p}(\det M) = n \cdot v_\mathfrak{p}(M) \quad \Leftrightarrow \quad \bar{M} \in \mathrm{PGL}\,(n, A_\mathfrak{p})$.

Beweis: Fixiere ein $\pi \in A$ mit $v_\mathfrak{p}(\pi) = 1$!

- *(i):* Klar, weil die Determinante ein homogenes Polynom vom Grad n in den Koeffizienten von M ist!

- *(ii)⇐:* Es gebe also ein $M' \in \mathrm{GL}\,(n, A_\mathfrak{p})$ und ein $c \in K^\times$ mit $M = cM'$. Aus $\det M' \in A_\mathfrak{p}^\times$ folgt zunächst $v_\mathfrak{p}(\det M') = 0$. Außerdem gilt offenbar $v_\mathfrak{p}(M') \geq 0$.

  Angenommen, es wäre $v_\mathfrak{p}(M') > 0$. Dann folgte $\frac{1}{\pi}M' \in \mathrm{End}\,(n, A_\mathfrak{p})$, aber es ist $\det \frac{1}{\pi}M' = \frac{1}{\pi^n}\det(M')$, d.h. $v_\mathfrak{p}(\det \frac{1}{\pi}M') = -n < 0$, so daß $\det \frac{1}{\pi}M' \notin A_\mathfrak{p}^\times$ — Widerspruch!

  Also gilt $v_\mathfrak{p}(M') = 0$, und es ergibt sich:

$$\begin{aligned} v_\mathfrak{p}(\det M) = v_\mathfrak{p}(\det cM') = v_\mathfrak{p}(c^n \det M') &= n \cdot v_\mathfrak{p}(c) + \underbrace{v_\mathfrak{p}(\det M')}_{=0} \\ = n \cdot v_\mathfrak{p}(c) = n \cdot (v_\mathfrak{p}(c) + \underbrace{v_\mathfrak{p}(M')}_{=0}) &= n \cdot v_\mathfrak{p}(c) = n \cdot v_\mathfrak{p}(cM') = n \cdot v_\mathfrak{p}(M). \end{aligned}$$

- *(ii)⇒:* Setze $M' := \pi^{-v_\mathfrak{p}(M)}M$. Dann gilt $v_\mathfrak{p}(M') = -v_\mathfrak{p}(M) + v_\mathfrak{p}(M) = 0$, d.h. $M' \in \mathrm{End}\,(n, A_\mathfrak{p})$, und

$$v_\mathfrak{p}(\det M') = v_\mathfrak{p}(\pi^{-n \cdot v_\mathfrak{p}(M)} \cdot \det M) = -n \cdot v_\mathfrak{p}(M) + v_\mathfrak{p}(\det M) \overset{\text{Vor.}}{=} 0.$$

  Die Matrix M', die ja ebenfalls ein Repräsentant von $\bar{M}$ ist, liegt also in $\mathrm{GL}\,(n, A_\mathfrak{p})$.

q.e.d.

8.2 Korollar.

$$\mathrm{PGL}\,(n, B_{\mathfrak{P}}) \cap \mathrm{PGL}\,(n, K) = \mathrm{PGL}\,(n, A_{\mathfrak{p}}) \qquad (\text{in } \mathrm{PGL}\,(n, L)!)$$

Beweis:

- $\supseteq$*:* Klar!
- $\subseteq$*:* Sei $\bar{M} \in \mathrm{PGL}\,(n, B_{\mathfrak{P}}) \cap \mathrm{PGL}\,(n, K)$ gegeben, repräsentiert durch eine Matrix $M \in \mathrm{GL}\,(n, K)$. Nach Voraussetzung wird $\bar{M}$ auch durch eine Matrix aus $\mathrm{GL}\,(n, B_{\mathfrak{P}})$ repräsentiert; deren endlich viele Koeffizienten liegen schon in einer endlichen Galoiserweiterung von K, so daß wir ohne Beschränkung der Allgemeinheit annehmen dürfen, daß L/K *endlich* ist; insbesondere ist dann B wieder ein Dedekind-Ring, die zugehörige diskrete Bewertung werde mit $v_{\mathfrak{P}}$ bezeichnet. Sei $e := e(\mathfrak{P}/\mathfrak{p}) \in \mathbb{N}$ der Verzweigungsindex, dann folgt:

$$e \cdot v_{\mathfrak{p}}(\det M) = v_{\mathfrak{P}}(\det M) \overset{8.1}{=} n \cdot v_{\mathfrak{P}}(M) = n \cdot e \cdot v_{\mathfrak{p}}(M)$$
$$\Rightarrow \quad v_{\mathfrak{p}}(\det M) = n \cdot v_{\mathfrak{p}}(M) \quad \overset{8.1}{\Rightarrow} \quad \bar{M} \in \mathrm{PGL}\,(n, Ap).$$

q.e.d.

8.3 Lemma/ Definition. Es seien P und Q Objekte aus $\widetilde{\mathcal{F}_K^{n,m}}$ (d.h. also von Null verschiedene homogene Polynome vom Grad m in n Variablen über K) mit $[Q] \in E(L/K, P)$ (d.h. also, daß Q eine L/K-Form von P ist).
Das Polynom Q (oder genauer die K-Isomorphieklasse $[Q]$ von Q) heißt $\mathfrak{p}$-*reduzible Form von* P, wenn es einen Isomorphismus $\bar{M} : Q_L \xrightarrow{\sim} P_L \in \mathrm{PGL}\,(n, L)$ mit $\bar{M} \in \mathrm{PGL}\,(n, B_{\mathfrak{P}})$ gibt.
Diese Definition hängt nicht von der Wahl des Primideals $\mathfrak{P}$ über $\mathfrak{p}$ ab.

Beweis: Sei Q $\mathfrak{p}$-reduzibel bezüglich $\mathfrak{P}$, und sei $\mathfrak{P}'$ ein weiteres maximales Primideal von B, das über $\mathfrak{p}$ liegt. Wir haben zu zeigen, daß Q dann auch $\mathfrak{p}$-reduzibel bezüglich $\mathfrak{P}'$ ist.

Sei also ein $M \in \mathrm{GL}\,(n, B_{\mathfrak{P}})$ gegeben, das einen Isomorphismus $\bar{M} : Q_L \xrightarrow{\sim} P_L$ repräsentiert. Wähle einen Zwischenkörper $\tilde{K}$ der Erweiterung L/K, der endlich und galoissch ist und alle Koeffizienten von M enthält! Bezeichnet $\tilde{A}$ den ganzen Abschluß von A in $\tilde{K}$, und setzt man $\tilde{\mathfrak{P}} := \mathfrak{P} \cap \tilde{A}$ und $\tilde{\mathfrak{P}}' := \mathfrak{P}' \cap \tilde{A}$, so folgt aus 8.2, angewandt auf die Erweiterung $L/\tilde{K}$ und die Primideale $\mathfrak{P}|\tilde{\mathfrak{P}}$, daß $\bar{M}$ in $\mathrm{PGL}\,(n, \tilde{A}_{\tilde{\mathfrak{P}}})$ liegt; wir dürfen also ohne Beschränkung der Allgemeinheit annehmen, daß M schon aus $\mathrm{GL}\,(n, \tilde{A}_{\tilde{\mathfrak{P}}})$ ist.

Weil $\tilde{K}/K$ endlich und galoissch ist, gibt es ein $\tilde{s} \in \mathrm{Gal}\,(\tilde{K}/K)$ mit ${}^{\tilde{s}}\tilde{\mathfrak{P}} = \tilde{\mathfrak{P}}'$. Wähle eine Fortsetzung $s \in \mathrm{Gal}\,(L/K)$ von $\tilde{s}$ auf L! Dann ist auch $\overline{{}^{s}M} \in \mathrm{PGL}\,(n, L)$ ein Isomorphismus von Q_L nach P_L, und

$${}^{s}M = {}^{\tilde{s}}M \in \mathrm{GL}\,(n, \tilde{A}_{\tilde{s}\tilde{\mathfrak{P}}}) = \mathrm{GL}\,(n, \tilde{A}_{\tilde{\mathfrak{P}}'}) \subseteq \mathrm{GL}\,(n, B_{\mathfrak{P}'}),$$

d.h. Q ist auch $\mathfrak{p}$-reduzibel bezüglich des Primideals $\mathfrak{P}'$. **q.e.d.**

8.4 Definition. Für ein Objekt P aus $\widetilde{\mathcal{F}_K^{n,m}}$ definiere die punktierte Menge

$$E(L/K,P)(\mathfrak{p}) := \{[Q] \in E(L/K,P) \,|\, \exists Q' \in [Q] \,:\, Q' \text{ ist } \mathfrak{p}\text{-reduzible Form von } P\}.$$

8.5 Lemma/ Definition. Für ein beliebiges Objekt $P = \sum \alpha_{i_1,\ldots,i_n} X_1^{i_1} \cdot \ldots \cdot X_n^{i_n}$ aus $\widetilde{\mathcal{F}_K^{n,m}}$ setze $v_\mathfrak{p}(P) := \min_{i_1,\ldots,i_n} v_\mathfrak{p}(\alpha_{i_1,\ldots,i_n}) \in \mathbb{Z}$.
Ist dann $M \in \mathrm{GL}\,(n, A_\mathfrak{p})$ beliebig, so gilt $v_\mathfrak{p}(P(MX)) = v_\mathfrak{p}(P)$.

Beweis: Das folgende Diagramm kommutiert:

$$\begin{array}{ccc} A_\mathfrak{p}[X_1,\ldots,X_n] & \xrightarrow[\sim]{M} & A_\mathfrak{p}[X_1,\ldots,X_n] \\ \downarrow & = & \downarrow \\ \kappa(\mathfrak{p})[X_1,\ldots,X_n] & \xrightarrow[M \bmod \mathfrak{p}]{\sim} & \kappa(\mathfrak{p})[X_1,\ldots,X_n]. \end{array}$$

Gelte zunächst $v_\mathfrak{p}(P) = 0$. Dann ist also $P \bmod \mathfrak{p} \neq 0$, wird also auch unter $M \bmod \mathfrak{p}$ auf ein von Null verschiedenes Polynom abgebildet, woraus aus der Kommutativität des Diagramms folgt, daß $v_\mathfrak{p}(P(MX)) = 0$ sein muß.

Im allgemeinen Fall wähle man wieder ein $\pi \in A_\mathfrak{p}$ mit $v_\mathfrak{p}(\pi) = 1$ und betrachte das Polynom $\tilde{P} := \pi^{-v_\mathfrak{p}(P)} P$; offenbar gilt $v_\mathfrak{p}(\tilde{P}) = 0$ und damit

$$\begin{aligned} v_\mathfrak{p}(P(MX)) = v_\mathfrak{p}(\pi^{v_\mathfrak{p}(P)} \tilde{P}(MX)) &= v_\mathfrak{p}(P) + v_\mathfrak{p}(\tilde{P}(MX)) \\ &= v_\mathfrak{p}(P) + v_\mathfrak{p}(\tilde{P}) = v_\mathfrak{p}(\pi^{v_\mathfrak{p}(P)} \tilde{P}) = v_\mathfrak{p}(P). \end{aligned}$$

q.e.d.

8.6 Lemma/ Definition. Definiere zunächst die Abbildung

$$\begin{array}{rcl} \mathrm{Ob}\,(\widetilde{\mathcal{F}_K^{n,m}}) & \longrightarrow & \mathrm{Ob}\,(\widetilde{\mathcal{F}_{\kappa(\mathfrak{p})}^{n,m}})/\text{Homothetie} \\ P & \mapsto & [P(\mathfrak{p})] := [(\pi^{-v_\mathfrak{p}(P)} P) \bmod \mathfrak{p}], \end{array}$$

wobei $\pi \in A_\mathfrak{p}$ ein beliebiges Element mit $v_\mathfrak{p}(\pi) = 1$ sei, und sei jetzt $P \in \mathrm{Ob}\,(\widetilde{\mathcal{F}_K^{n,m}})$ ein Objekt mit der Eigenschaft, daß die Automorphismengruppe $\mathrm{Aut}_L(P)$ in $\mathrm{PGL}\,(n, B_\mathfrak{P})$ liegt. Dann haben wir die folgende wohldefinierte *Spezialisierungsabbildung*:

$$\begin{array}{rcl} s_\mathfrak{p} : \; E(L/K,P)(\mathfrak{p}) & \longrightarrow & E\big(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}), P(\mathfrak{p})\big) \\ [Q] & \mapsto & [Q'(\mathfrak{p})] \quad (\text{für eine } \mathfrak{p}\text{-reduzible Form } Q' \in [Q] \text{ von } P), \end{array}$$

wobei man beachte, daß die Menge $E(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}), P(\mathfrak{p}))$ nur von der Isomorphieklasse von $P(\mathfrak{p})$ und also nicht von der Wahl von π abhängt!

Beweis:

- *Wohldefiniertheit von $P \mapsto P(\mathfrak{p})$:* Ist P ein Objekt aus $\widetilde{\mathcal{F}_K^{n,m}}$, so ist $v_\mathfrak{p}(\pi^{-v_\mathfrak{p}(P)}P) = 0$, d.h. die Reduktion modulo $\mathfrak{p}$ ist nicht das Nullpolynom und also ein Objekt aus $\widetilde{\mathcal{F}_{\kappa(\mathfrak{p})}^{n,m}}$.

- *Unabhängigkeit von π:* Ist auch $\pi' \in A_\mathfrak{p}$ ein Element mit $v_\mathfrak{p}(\pi') = 1$, so gilt $\frac{\pi}{\pi'} \in {A_\mathfrak{p}}^\times$, d.h. die Polynome $\pi^{-v_\mathfrak{p}(P)}P$ und $\pi'^{-v_\mathfrak{p}(P)}P$ unterscheiden sich modulo $\mathfrak{p}$ nur um ein Element aus $\kappa(\mathfrak{p})^\times$, d.h. um eine Homothetie.

- *Wohldefiniertheit von $s_\mathfrak{p}$:* Wir zeigen zunächst: Ist Q' eine $\mathfrak{p}$-reduzible Form von P, so ist $Q'(\mathfrak{p})$ eine $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$-Form von $P(\mathfrak{p})$. Sei hierzu $\pi \in B$ mit $v_\mathfrak{P}(\pi) = 1$, und sei $e := e(\mathfrak{P}/\mathfrak{p})$ der Verzweigungsindex. Offenbar gilt:

$$\begin{aligned} P(\mathfrak{p}) &= (\pi^{-ev_\mathfrak{p}(P)}P_L) \bmod \mathfrak{P} \quad \text{und} \\ Q'(\mathfrak{p}) &= (\pi^{-ev_\mathfrak{p}(Q')}Q'_L) \bmod \mathfrak{P}. \end{aligned}$$

  Nach Voraussetzung gibt es ein $M \in \mathrm{GL}\,(n, B_\mathfrak{P})$ und ein $\lambda \in L^\times$ mit $P_L(MX) = \lambda \cdot Q'_L$, woraus folgt:

$$\begin{aligned} (\pi^{-ev_\mathfrak{p}(P)}P_L)(MX) = \pi^{-ev_\mathfrak{p}(P)} \cdot \lambda \cdot Q'_L &= (\pi^{-ev_\mathfrak{p}(P)} \cdot \lambda \cdot \pi^{ev_\mathfrak{p}(Q')}) \cdot (\pi^{-ev_\mathfrak{p}(Q')}Q'_L) \\ &= \underbrace{(\pi^{e[v_\mathfrak{p}(Q')-v_\mathfrak{p}(P)]}\lambda)}_{=:\lambda'} \cdot (\pi^{-ev_\mathfrak{p}(Q')}Q'_L), \end{aligned}$$

  d.h.

$$P(\mathfrak{p})(\bar{M}X) \equiv \lambda' \cdot Q'(\mathfrak{p}) \pmod{\mathfrak{P}}. \tag{29}$$

  Außerdem gilt:

$$\begin{aligned} & v_\mathfrak{P}(P_L) \overset{8.5}{=} v_\mathfrak{P}(P_L(MX)) = v_\mathfrak{P}(\lambda \cdot Q'_L) = v_\mathfrak{P}(\lambda) + v_\mathfrak{P}(Q'_L) \\ \Longrightarrow \quad & v_\mathfrak{P}(\lambda) = v_\mathfrak{P}(P_L) - v_\mathfrak{P}(Q'_L) = e[v_\mathfrak{p}(P) - v_\mathfrak{p}(Q')] \\ \Longrightarrow \quad & v_\mathfrak{P}(\lambda') = 0. \end{aligned}$$

  Also liegt $\bar{\lambda'}$ in $\kappa(\mathfrak{P})^\times$, womit aus Gleichung (29) folgt, daß die Reduktion $\bar{M}$ von M modulo $\mathfrak{P}$ einen Isomorphismus von $(Q'(\mathfrak{p}))_{\kappa(\mathfrak{P})}$ nach $(P(\mathfrak{p}))_{\kappa(\mathfrak{P})}$ definiert.

  Jetzt müssen wir noch die Unabhängigkeit von der Wahl der $\mathfrak{p}$-reduziblen Form Q' zeigen. Sei also Q'' eine weitere $\mathfrak{p}$-reduzible Form von P. Wir haben dann nach Voraussetzung Isomorphismen $Q'_L \xrightarrow{M'} P_L$, $Q''_L \xrightarrow{M''} P_L$ und $Q' \xrightarrow{N} Q''$ mit $M', M'' \in \mathrm{PGL}\,(n, B_\mathfrak{P})$ und $N \in \mathrm{PGL}\,(n, K)$. Setzen wir $O := M''N_LM'^{-1}$, so erhalten wir das folgende kommutative Diagramm in der Kategorie $\widetilde{\mathcal{F}_L^{n,m}}$:

$$\begin{array}{ccc} Q'_L & \xrightarrow[\sim]{M'} & P_L \\ {\scriptstyle N_L}\downarrow & = & \downarrow{\scriptstyle O} \\ Q''_L & \xrightarrow[M'']{\sim} & P_L. \end{array}$$

  Der Morphismus O ist also ein Automorphismus von P_L, d.h. nach Voraussetzung an P ein Element aus $\mathrm{PGL}\,(n, B_\mathfrak{P})$. Dann muß aber auch N in $\mathrm{PGL}\,(n, B_\mathfrak{P})$ liegen, d.h.

$$N \in \mathrm{PGL}\,(n, B_\mathfrak{P}) \cap \mathrm{PGL}\,(n, K) \overset{8.2}{=} \mathrm{PGL}\,(n, A_\mathfrak{p}).$$

  Die Reduktion von N modulo $\mathfrak{p}$ definiert also einen $\kappa(\mathfrak{p})$-Isomorphismus von $Q'_\mathfrak{p}$ nach $Q''_\mathfrak{p}$, d.h. $Q'_\mathfrak{p}$ und $Q''_\mathfrak{p}$ definieren in $E(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}), P_\mathfrak{p})$ dasselbe Element.

q.e.d.

8.7 Lemma. Es sei P ein Objekt aus $\widetilde{\mathcal{F}_K^{n,m}}$ mit $\mathrm{Aut}_L(P) \leq \mathrm{PGL}\,(n, B_{\mathfrak{P}})$ und Q eine L/K-Form von P. Dann gilt:
Q ist genau dann $\mathfrak{p}$-reduzible Form von P, wenn alle Isomorphismen $Q_L \xrightarrow{\sim} P_L$ in $\mathrm{PGL}\,(n, B_{\mathfrak{P}})$ liegen.

Beweis:

- $\Leftarrow$*:* Klar nach Definition von „$\mathfrak{p}$-reduzibel“!
- $\Rightarrow$*:* Ist Q eine $\mathfrak{p}$-reduzible Form von P, so gibt es einen Isomorphismus $Q_L \xrightarrow{M} P_L$ mit $M \in \mathrm{PGL}\,(n, B_{\mathfrak{P}})$. Ist nun $Q_L \xrightarrow{M'} P_L$ ein beliebiger Isomorphismus, so ist $M'M^{-1}$ ein Automorphismus von P_L und also nach Voraussetzung ein Element von $\mathrm{PGL}\,(n, B_{\mathfrak{P}})$. Dann muß aber auch M' in $\mathrm{PGL}\,(n, B_{\mathfrak{P}})$ liegen.

q.e.d.

8.8 Lemma. Ist $m \geq 3$, enthält L die m-ten Einheitswurzeln, und bezeichnet $P_n^m \in \mathrm{Ob}\,(\widetilde{\mathcal{F}_K^{n,m}})$ die Fermatgleichung, so gilt

$$\mathrm{Aut}_L(P_n^m) \overset{7.1}{=} (S_n \textstyle\int \mu_m)/\mu_m \leq \mathrm{PGL}\,(n, B) \leq \mathrm{PGL}\,(n, B_{\mathfrak{P}}).$$

Beweis: Klar, da die m-ten Einheitswurzeln ganz über $\mathbb{Z}$, also insbesondere auch ganz über A sind und damit in B liegen! **q.e.d.**

8.9 Beispiel. Es sei speziell $n := 2$, $m := 3$, $A := \mathbb{Z}$ (also $K = \mathbb{Q}$) und $L := \mathbb{Q}(\sqrt{3})$, also $B = \mathcal{O}_L = \mathbb{Z}[\sqrt{3}]$. Betrachte das Polynom $P := X^3 + Y^3 \in \mathrm{Ob}\,(\widetilde{\mathcal{F}_{\mathbb{Q}}^{2,3}})$. Weil L die dritten Einheitswurzeln nicht enthält, gilt offenbar

$$\mathrm{Aut}_L(P) = \underbrace{\mathrm{Aut}_{\bar{\mathbb{Q}}}(P)}_{=(S_2 \int \mu_3)/\mu_3} \cap \mathrm{PGL}\,(2, L) = S_2 \leq \mathrm{PGL}\,(2, B),$$

d.h. für alle maximalen Primideale $\mathfrak{P}$ von B liegt $\mathrm{Aut}_L(P)$ in $\mathrm{PGL}\,(2, B_{\mathfrak{P}})$. Setze $M := \begin{pmatrix} 1 & \sqrt{3} \\ 1 & -\sqrt{3} \end{pmatrix} \in \mathrm{GL}\,(2, L)$ und $Q := \frac{5}{9}X^3 + 5XY^2 \in \mathrm{Ob}\,(\widetilde{\mathcal{F}_{\mathbb{Q}}^{2,3}})$. Es gilt:

$$\begin{aligned} P(MX) &= (X + \sqrt{3}Y)^3 + (X - \sqrt{3}Y)^3 \\ &= X^3 + 3\sqrt{3}X^2Y + 9XY^2 + 3\sqrt{3}Y^3 + X^3 - 3\sqrt{3}X^2Y + 9XY^2 - 3\sqrt{3}Y^3 \\ &= 2X^3 + 18XY^2 \\ &= \tfrac{18}{5} \cdot Q. \end{aligned}$$

Die Matrix M, aufgefaßt als Element von $\mathrm{PGL}\,(2, L)$, definiert also einen Isomorphismus von Q_L nach P_L, d.h. Q ist eine $L/\mathbb{Q}$-Form von P.
Die Determinante von M ist $(-2\sqrt{3})$, und wir erhalten (unter Berücksichtigung der wohlbekannten Tatsache, daß $L/\mathbb{Q}$ genau bei 2 und 3 verzweigt ist):

- $v_{\mathfrak{P}}(M) = 0$ für alle maximalen Primideale $\mathfrak{P}$ von B.
- $v_{\mathfrak{P}}(\det M) = \begin{cases} 2 & , \text{ falls } \mathfrak{P}|2 \\ 1 & , \text{ falls } \mathfrak{P}|3 \\ 0 & \text{sonst.} \end{cases}$

Wegen 8.1 und 8.7 folgt hieraus für eine Primzahl p, daß Q genau dann (p)-reduzible Form von P ist, wenn $p \geq 5$ gilt. Zum Beispiel erhalten wir für $p = 5$ und $p = 11$:

$$\begin{array}{rclcl} s_{(5)}Q & = & [\frac{1}{9}X^3 + XY^2 \bmod 5] & = & [4X^3 + XY^2] \quad \in \quad E(\mathbb{F}_{25}/\mathbb{F}_5, X^3 + Y^3), \\ s_{(11)}Q & = & [\frac{5}{9}X^3 + 5XY^2 \bmod 11] & = & [3X^3 + 5XY^2] \quad \in \quad E(\mathbb{F}_{11}/\mathbb{F}_{11}, X^3 + Y^3). \end{array}$$

(Hierbei beachte man, daß (5) unzerlegt und (11) vollzerlegt ist!)

8.10 Lemma/ Definition. Es sei wieder ein Objekt P aus $\widetilde{\mathcal{F}_K^{n,m}}$ gegeben mit $\mathrm{Aut}_L(P) \leq \mathrm{PGL}\,(n, B_{\mathfrak{P}})$. Wir haben dann eine offensichtliche Abbildung $\mathrm{Aut}_L(P) \xrightarrow{f} \mathrm{Aut}_{\kappa(\mathfrak{P})}(P(\mathfrak{p}))$, die einen Repräsentanten M aus $\mathrm{PGL}\,(n, B_{\mathfrak{P}})$ auf die Klasse von M mod $\mathfrak{P}$ abbildet.
Bezeichne $G_{\mathfrak{P}} \leq G$ die Zerlegungsgruppe von $\mathfrak{P}$ in G und $I_{\mathfrak{P}} \trianglelefteq G_{\mathfrak{P}}$ die Trägheitsgruppe, und definiere $H^1_{\mathrm{cont}}(G, \mathrm{Aut}_L(P))(\mathfrak{P})$, die *Menge der $\mathfrak{P}$-reduziblen Kohomologieklassen*, als die punktierte Teilmenge der Kohomologieklassen in der punktierten Menge $H^1_{\mathrm{cont}}(G, \mathrm{Aut}_L(P))$, die unter $H^1_{\mathrm{cont}}(f)$ in den Kern der Restriktion von G auf $I_{\mathfrak{P}}$ abgebildet werden. Nach Satz 2.36 erhalten wir dann die folgende *Spezialisierungsabbildung*, die wir mit $s_{\mathfrak{P}}$ bezeichnen wollen:

$$\begin{aligned} H^1_{\mathrm{cont}}(G, \mathrm{Aut}_L(P))(\mathfrak{P}) &\xrightarrow{H^1_{\mathrm{cont}}(f)} H^1_{\mathrm{cont}}(G, \mathrm{Aut}_{\kappa(\mathfrak{P})}(P(\mathfrak{p}))) \\ &\xrightarrow{\mathrm{res}} H^1_{\mathrm{cont}}\big(G_{\mathfrak{P}}, \mathrm{Aut}_{\kappa(\mathfrak{P})}(P(\mathfrak{p}))\big) \xrightarrow{\mathrm{inf}^{-1}} H^1_{\mathrm{cont}}\big(G_{\mathfrak{P}}/I_{\mathfrak{P}}, \mathrm{Aut}_{\kappa(\mathfrak{P})}(P(\mathfrak{p}))\big), \end{aligned}$$

wobei wir beachten, daß $G_{\mathfrak{P}}/I_{\mathfrak{P}} = \mathrm{Gal}\,(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})) =: G(\mathfrak{P})$ gilt.

Beweis: Klar, wenn man beachtet, daß $I_{\mathfrak{P}}$ trivial auf $\mathrm{Aut}_{\kappa(\mathfrak{P})}(P(\mathfrak{p}))$ operiert, so daß also

$$\mathrm{Aut}_{\kappa(\mathfrak{P})}(P(\mathfrak{p}))^{I_{\mathfrak{P}}} = \mathrm{Aut}_{\kappa(\mathfrak{P})}(P(\mathfrak{p}))$$

gilt! **q.e.d.**

8.11 Satz. Es seien alle Voraussetzungen wie in 8.10, und es gelte zusätzlich, daß m teilerfremd zur Charakteristik von $\kappa(\mathfrak{p})$ ist und daß $\mathfrak{p}$ unzerlegt in L ist. Dann induziert die Inflation einen Isomorphismus von punktierten Mengen

$$H^1_{\mathrm{cont}}\big(G(\mathfrak{P}), \mathrm{Aut}_{\kappa(\mathfrak{P})}(P(\mathfrak{p}))\big) \xrightarrow{\sim} H^1_{\mathrm{cont}}\big(G, \mathrm{Aut}_L(P)\big)(\mathfrak{P}).$$

Beweis: Offenbar ist der Gruppenhomomorphismus f aus 8.10 wegen $(m, \mathrm{char}\,(\kappa(\mathfrak{p}))) = 1$ ein Isomorphismus, und aus der Unzerlegtheit von $\mathfrak{p}$ in L folgt $G_{\mathfrak{P}} = G$. Also ist $H^1_{\mathrm{cont}}\big(G, \mathrm{Aut}_L(P)\big)(\mathfrak{P})$ per definitionem der Kern von

$$H^1_{\mathrm{cont}}\big(G, \mathrm{Aut}_{\kappa(\mathfrak{P})}(P(\mathfrak{p}))\big) \xrightarrow{\mathrm{res}} H^1_{\mathrm{cont}}\big(I_{\mathfrak{P}}, \mathrm{Aut}_{\kappa(\mathfrak{P})}(P(\mathfrak{p}))\big),$$

und nach 2.36 identifiziert sich dieser Kern über die Inflation mit

$$H^1_{\mathrm{cont}}\big(G/I_{\mathfrak{P}}, \mathrm{Aut}_{\kappa(\mathfrak{P})}(P(\mathfrak{p}))\big).$$

q.e.d.

8.12 Lemma/ Definition. Es sei speziell A *vollständig* und *lokal*, d.h. A ist ein vollständiger diskreter Bewertungsring mit Quotientenkörper K, maximalem Ideal $\mathfrak{p}$ und Restklassenkörper $\kappa(\mathfrak{p})$.
Dann haben wir eine Kategorienäquivalenz

$$\begin{aligned} F_1 : \{&\text{unverzweigte, kommutative, separable } K\text{-Algebren vom Grad } n \text{ über } K\} \\ &\tilde{\rightsquigarrow} \{\text{kommutative, separable } \kappa(\mathfrak{p})\text{-Algebren vom Grad } n \text{ über } \kappa(\mathfrak{p})\}. \end{aligned}$$

Ist Λ ein Objekt der linken Seite, $\Lambda = \prod_{i=1}^t \Lambda_i$ mit Körpern Λ_i, und bezeichnet C_i den ganzen Abschluß von A in Λ_i, so wird $F_1\Lambda$ explizit durch

$$F_1\Lambda := \prod_{i=1}^t \big(C_i \otimes_A \kappa(\mathfrak{p})\big)$$

gegeben.

Ist umgekehrt $\lambda = \prod_{j=1}^u \lambda_j$ ein Objekt der rechten Seite mit Körpern λ_j, so werden die λ_j nach dem Hauptsatz der Galoistheorie durch offene Untergruppen $V_j \leq G_{\kappa(\mathfrak{p})}$ der absoluten Galoisgruppe $G_{\kappa(\mathfrak{p})}$ von $\kappa(\mathfrak{p})$ gegeben. Bezeichne G_K die absolute Galoisgruppe von K sowie $I \trianglelefteq G_K$ die Trägheitsgruppe und $p : G_K \twoheadrightarrow G_{\kappa(\mathfrak{p})}$ die kanonische Projektion mit Kern I. Für $j \in \{1, \ldots, u\}$ sei Λ_j die zur offenen Untergruppe $p^{-1}(V_j)$ von G_K korrespondierende endliche, separable Körpererweiterung von K. Dann wird ein Quasiinverses F_2 zu F_1 durch

$$F_2\lambda := \prod_{j=1}^u \Lambda_j$$

definiert.

Beweis: Siehe [Mil80, I.4.4, S.34] und [Mil80, I.5.2.(c), S.41]! **q.e.d.**

8.13 Satz. Es seien wieder speziell A vollständig und lokal und $L = \bar{K}$ ein separabler algebraischer Abschluß von K, und es gelte wieder $(m, \mathrm{char}\,(\kappa(\mathfrak{p})) = 1$. Dann ist $G(\mathfrak{P}) = G$ die absolute Galoisgruppe von K, und es bezeichne $p : G \twoheadrightarrow G_{\kappa(\mathfrak{p})}$ die kanonische Projektion.
Wir betrachten die Fermatgleichung $P := P_n^m = X_1^m + \ldots + X_n^m$. Dann haben wir nach

8.11 einen kanonischen, durch die Inflation induzierten, Isomorphismus von punktierten Mengen

$$\alpha : H^1_{\mathrm{cont}}\big(G_{\kappa(\mathfrak{p})}, \mathrm{Aut}_{\kappa(\mathfrak{P})}(P(\mathfrak{p}))\big) \xrightarrow{\sim} H^1_{\mathrm{cont}}\big(G, \mathrm{Aut}_{\bar{K}}(P)\big)(\mathfrak{P}).$$

Ein Element der Quelle von α wird gemäß 7.9 durch ein Paar $(\lambda, \bar{x})$ gegeben, wobei λ eine kommutative, separable $\kappa(\mathfrak{p})$-Algebra vom Grad n über $\kappa(\mathfrak{p})$ ist und $\bar{x}$ ein Element aus $\lambda^\times$.

Bezeichne $\Lambda := \prod_{j=1}^u \Lambda_j := F_2\lambda$ die zu λ über die Kategorienäquivalenz aus 8.12 korrespondierende kommutative, separable, *unverzweigte*, K-Algebra vom Grad n über K. Ist $\bar{x} = (\bar{x}_1, \ldots, \bar{x}_u)$ mit $\bar{x}_j \in \lambda_j^\times$, so wähle für jedes $j \in \{1, \ldots, j\}$ im ganzen Abschluß C_j von A in Λ_j ein x_j, dessen Reduktion gleich $\bar{x}_j$ ist, und setze $x := (x_1, \ldots, x_t) \in \Lambda^\times$.

Dann wird das Bild von $(\lambda, \bar{x})$ unter α durch das Paar (Λ, x) gegeben.

Ist umgekehrt $(\prod_{i=1}^t \Lambda_i, x)$ ein Repräsentant eines Elements aus dem Ziel von α mit der Eigenschaft, daß alle Λ_i/K *unverzweigt* sind und daß $\varphi(x)$ für alle $\varphi \in \mathrm{Hom}_K(\Lambda, \bar{K})$ eine Einheit in $B_{\mathfrak{P}}$ ist[†], und bezeichnet C_i den ganzen Abschluß von A in Λ_i, so wird ein Urbild des Paares $(\prod \Lambda_i, x)$ unter α durch das Paar $(\prod_i C_i/\mathfrak{p}, x \bmod \mathfrak{p})$ repräsentiert.

Beweis: Es sei also $(\lambda, \bar{x})$ ein Repräsentant eines Elements der Quelle von α und (Λ, x) wie oben konstruiert. Es sei C_i der ganze Abschluß von A in Λ_i, und die kanonischen Projektionen $C_i \twoheadrightarrow \lambda_i$ sowie $\prod C_i \twoheadrightarrow \lambda$ mögen alle mit p bezeichnet werden. Wir müssen zeigen, daß $\alpha(\lambda, \bar{x}) = (\Lambda, x)$ gilt.

Es seien $M := \mathrm{Hom}_K(\Lambda, \bar{K})$ und $\bar{M} := \mathrm{Hom}_{\kappa(\mathfrak{p})}(\lambda, \overline{\kappa(\mathfrak{p})})$. Wir haben wegen 8.12 eine kanonische Bijektion

$$\beta : \left\{ \begin{array}{ccc} M & \longrightarrow & \bar{M} \\ \varphi & \mapsto & \big(p(y) \mapsto p(\varphi y)\big) \end{array} \right\}$$

Nach 5.11 wird die Klasse $(\lambda, \bar{x})$ durch den 1-Kozykel

$$\left(\left(\frac{\bar{s}\, \sqrt[m]{\bar{s}^{-1}\bar{\varphi}\bar{x}}}{\sqrt[m]{\bar{\varphi}\bar{x}}} \right)_{\bar{\varphi} \in \bar{M}} \cdot [\bar{\varphi} \mapsto \bar{s} \circ \bar{\varphi}] \right)_{\bar{s} \in G_{\kappa(\mathfrak{p})}}$$

repräsentiert.

Sei $\bar{s} \in G_{\kappa(\mathfrak{p})}$ beliebig, sei $s \in G$ ein Urbild von $\bar{s}$, und sei $\varphi \in M$ beliebig. Dann gilt

$$p(\varphi x) = \beta(\varphi)\bar{x} \quad \text{und} \quad p(s^{-1}\varphi x) = \bar{s}^{-1}[\beta(\varphi)]\bar{x},$$

und wegen $(m, \mathrm{char}\, \kappa(\mathfrak{p})) = 1$ können wir nach Hensels Lemma zu vorgegebenen $\sqrt[m]{\beta(\varphi)\bar{x}}$ bzw. $\sqrt[m]{\bar{s}^{-1}[\beta(\varphi)]\bar{x}}$ Elemente $\sqrt[m]{\varphi x}$ und $\sqrt[m]{s^{-1}\varphi x}$ wählen mit

$$p(\sqrt[m]{\varphi x}) = \sqrt[m]{\beta(\varphi)\bar{x}} \quad \text{und} \quad p(\sqrt[m]{s^{-1}\varphi x}) = \bar{s}^{-1}[\beta(\varphi)]\bar{x}.$$

Mit diesen Wahlen folgt dann

$$p\left(\frac{s\, \sqrt[m]{s^{-1}\varphi x}}{\sqrt[m]{\varphi x}} \right) = \frac{\bar{s}\, \sqrt[m]{\bar{s}^{-1}[\beta(\varphi)]\bar{x}}}{\sqrt[m]{\beta(\varphi)\bar{x}}},$$

[†]Wir werden in 8.17 sehen, daß es einen Repräsentanten mit diesen Eigenschaften stets gibt.

und dies zeigt die Behauptung, wenn wir $\mathrm{Aut}_{\bar{K}}(P_n^m)$ via

$$\begin{array}{ccc} \left\{\zeta \in \bar{K} \,|\, \zeta^m = 1\right\}^M \ltimes \mathrm{Aut}\,(M) & \longrightarrow & \left\{\bar{\zeta} \in \overline{\kappa(\mathfrak{p})} \;\middle|\; \bar{\zeta}^m = 1\right\}^{\bar{M}} \ltimes \mathrm{Aut}\,(\bar{M}) \\ (\zeta_\varphi)_\varphi \cdot [\varphi \mapsto \sigma(\varphi)] & \mapsto & (p(\zeta_{\beta^{-1}\bar{\varphi}}))_{\bar{\varphi}} \cdot [\bar{\varphi} \mapsto \beta\sigma\beta^{-1}\bar{\varphi}] \end{array}$$

mit $\mathrm{Aut}_{\overline{\kappa(\mathfrak{p})}}(P_n^m)$ identifizieren (dies ist der Gruppenhomomorphismus f aus 8.10 und dem Beweis von 8.11).

Nun müssen wir noch die im Satz behauptete explizite Beschreibung von α^{-1} beweisen. Diese folgt aber sofort aus der Beschreibung des Funktors F_1 aus 8.12 und der soeben bewiesenen Beschreibung von α. **q.e.d.**

8.14 Satz. Es sei wieder ein Objekt P aus $\widetilde{\mathcal{F}_K^{n,m}}$ gegeben mit $\mathrm{Aut}_L(P) \leq \mathrm{PGL}\,(n, B_{\mathfrak{P}})$. Dann bildet die Abbildung $E(L/K, P) \xrightarrow{\vartheta} H^1_{\mathrm{cont}}(G, \mathrm{Aut}_L(P))$ aus 3.1 bzw. 3.4 eine $\mathfrak{p}$-reduzible L/K-Form von P auf eine $\mathfrak{P}$-reduzible Kohomologieklasse ab, und das folgende Diagramm von punktierten Mengen ist kommutativ:

$$\begin{array}{ccc} E(L/K,P)(\mathfrak{p}) & \xrightarrow{\quad s_{\mathfrak{p}} \quad} & E(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}), P(\mathfrak{p})) \\ \downarrow \vartheta & = & \downarrow \vartheta \\ H^1_{\mathrm{cont}}(G, \mathrm{Aut}_L(P))(\mathfrak{P}) & \xrightarrow[s_{\mathfrak{P}}]{} & H^1_{\mathrm{cont}}(G(\mathfrak{P}), \mathrm{Aut}_{\kappa(\mathfrak{P})}(P(\mathfrak{p}))). \end{array}$$

Beweis: Es sei Q eine $\mathfrak{p}$-reduzible Form von P und $M : Q \xrightarrow{\sim} P$ ein Isomorphismus mit $M \in \mathrm{PGL}\,(n, B_{\mathfrak{P}})$. Ist dann $s \in I_{\mathfrak{P}}$, so gilt nach Definition der Trägheitsgruppe ${}^sM \equiv M \pmod{\mathfrak{P}}$, d.h. der 1-Kozykel $(M^s(M^{-1}))_s$, eingeschränkt auf $I_{\mathfrak{P}}$, ist trivial modulo $\mathfrak{P}$, und dies zeigt die erste Behauptung.

Die Kommutativität des Diagramms folgt aus der Tatsache, daß $M \bmod \mathfrak{P}$ einen Isomorphismus von $Q(\mathfrak{p})$ nach $P(\mathfrak{p})$ definiert, wie wir im Beweis von 8.6 gesehen haben. **q.e.d.**

8.15 Satz. Es sei wieder ein Objekt P aus $\widetilde{\mathcal{F}_K^{n,m}}$ gegeben mit $\mathrm{Aut}_L(P) \leq \mathrm{PGL}\,(n, B_{\mathfrak{P}})$. Wir betrachten die Erweiterung der Lokalisierungen[†] $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ von L und K bezüglich der durch $\mathfrak{P}$ und $\mathfrak{p}$ gegebenen Bewertungen; die Galoisgruppe dieser Erweiterung identifiziert sich mit der Zerlegungsgruppe $G_{\mathfrak{P}}$ (vgl. [Neu92, II.9, S.179]).

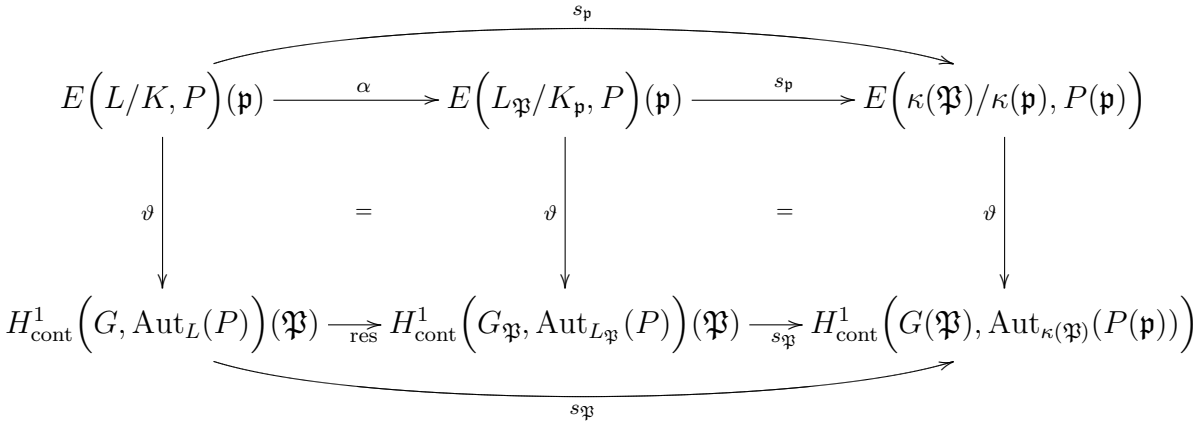
Wir fassen P auch als Objekt von $\widetilde{\mathcal{F}_{K_{\mathfrak{p}}}^{n,m}}$ auf und haben dann eine offensichtliche Abbildung

$$\alpha : E\big(L/K, P\big) \longrightarrow E\big(L_{\mathfrak{P}}/K_{\mathfrak{p}}, P\big),$$

die eine L/K-Form von P auf sich selbst, aufgefaßt als Polynom über $K_{\mathfrak{p}}$, schickt. Wir wollen noch zusätzlich voraussetzen, daß $\mathrm{Aut}_{L_{\mathfrak{P}}}(P) \leq \mathrm{PGL}\,(n, \widehat{B_{\mathfrak{P}}})$ gilt.

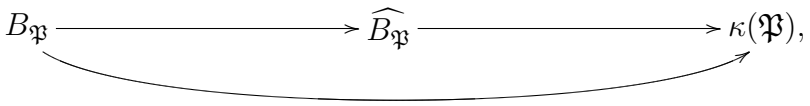
[†]Wir folgen hier Neukirch ([Neu92, II.8, S.168]) und definieren $L_{\mathfrak{P}}$ als die *Vervollständigung* von L bezüglich $\mathfrak{P}$, falls L/K *endlich* ist, und sonst als $\bigcup_i (L_i)_{(L_i \cap \mathfrak{P})}$, wobei die Vereinigung über alle endlichen Teilerweiterungen L_i/K von L/K läuft.

Dann erhalten wir das folgende kommutative Diagramm in der Kategorie der punktierten Mengen:



Beweis: Die Abbildung α ist wohldefiniert, weil wegen $\mathrm{PGL}\,(n,B_{\mathfrak{P}}) \leq \mathrm{PGL}\,(n,\widehat{B_{\mathfrak{P}}})$ eine $\mathfrak{p}$-reduzible Form unter α wieder auf eine $\mathfrak{p}$-reduzible Form abgebildet wird, und die Abbildungen ϑ sind nach 8.14 wohldefiniert, da nach Voraussetzung $\mathrm{Aut}_L(P) \leq \mathrm{PGL}\,(n,B_{\mathfrak{P}})$ bzw. $\mathrm{Aut}_{L_{\mathfrak{P}}}(P) \leq \mathrm{PGL}\,(n,\widehat{B_{\mathfrak{P}}})$ gilt.

Die Kommutativität des oberen Kreissegments ist klar, die des unteren folgt aus der Definition der Spezialisierungsabbildung in 8.10 und aus der Kommutativität von



die Kommutativität des linken Quadrates ist wegen $\mathrm{PGL}\,(n,B_{\mathfrak{P}}) \leq \mathrm{PGL}\,(n,\widehat{B_{\mathfrak{P}}})$ klar nach Definition von ϑ, und die Kommutativität des rechten Quadrates schließlich folgt aus 8.14. **q.e.d.**

8.16 Beispiel. Es seien alle Bezeichnungen wie in Beispiel 8.9! Die Erweiterung L/K ist unverzweigt und unzerlegt bei $\mathfrak{p} := (5)$ — sei $\mathfrak{P}$ das Primideal in B über $\mathfrak{p}$, und bezeichne f den arithmetischen Frobenius in $\kappa(\mathfrak{P}) = \mathbb{F}_{25}$! Der $\mathbb{Q}$-Automorphismus s von L, der $a+b\sqrt{3}$ auf $a-b\sqrt{3}$ abbildet, liegt in $G_{\mathfrak{P}}$ und ist unter $G_{\mathfrak{P}} \twoheadrightarrow G_{\mathfrak{P}}/I_{\mathfrak{P}}$ ein Urbild von f. Es ist

$$M^s(M^{-1}) = \left(\begin{smallmatrix} 1 & \sqrt{3} \\ 1 & -\sqrt{3} \end{smallmatrix}\right) \cdot {}^s\left(\begin{smallmatrix} 1 & \sqrt{3} \\ 1 & -\sqrt{3} \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & \sqrt{3} \\ 1 & -\sqrt{3} \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 1 & -\sqrt{3} \\ 1 & \sqrt{3} \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right),$$

d.h. $s_{\mathfrak{P}} \circ \theta(Q)$ ist die Klasse des 1-Kozykels, der f auf $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \in \mathrm{PGL}\,(2,\mathbb{F}_{25})$ abbildet. Aus Satz 8.14 folgt, daß dies auch gerade $\vartheta(4X^3+XY^2)$ ist.

8.17 Theorem. Es sei speziell $L = \bar{K}$ ein separabler algebraischer Abschluß von K und $m \geq 3$ mit $(m, \mathrm{char}\,(\kappa(\mathfrak{p}))) = 1$. Betrachte die Fermatgleichung $P_n^m = X_1^m + \ldots + X_n^m$, und sei $[Q]$ eine $\bar{K}/K$-Form von P_n^m.

Dann sind die folgenden drei Bedingungen äquivalent:

(1) Die $\bar{K}/K$-Form $[Q]$ von P_n^m ist $\mathfrak{p}$-reduzibel.

(2) Die Kohomologieklasse $\vartheta[Q]$ ist $\mathfrak{P}$-reduzibel.

(3) Die Kohomologieklasse $\vartheta[Q]$ besitzt einen Repräsentanten (Λ, x) im Sinne von 7.9, wobei Λ ein Produkt $\prod_{i=1}^t \Lambda_i$ mit Teilkörpern Λ_i von $\bar{K}$ ist und x in $\Lambda^\times$ liegt, so daß die folgenden beiden Bedingungen erfüllt sind:

   (i) Für jedes $i \in \{1, \ldots, t\}$ ist $\mathfrak{p}$ unverzweigt in Λ_i.

   (ii) Für jedes $\varphi \in M := \mathrm{Hom}_K(\Lambda, \bar{K})$ ist $\varphi(x)$ eine Einheit in $B_{\mathfrak{P}}$.

Sind diese Bedingungen erfüllt, ist (Λ, x) ein Repräsentant von $\vartheta[Q]$ wie in (3) mit $\Lambda = \prod \Lambda_i$, und bezeichnet C_i den ganzen Abschluß von $A_{\mathfrak{p}}$ in Λ_i, so wird die Spezialisierung $s_{\mathfrak{p}}[Q]$ gemäß 7.9 durch das Paar $\boxed{\left(\prod_{i=1}^t (C_i/\mathfrak{p}), x \bmod \mathfrak{p}\right)}$ gegeben.

Beweis:

- *(1) ⇒ (2):* Dies ist gerade die erste Aussage von Satz 8.14.

- *(2) ⇒ (3):* In dem Spezialfall, daß A *vollständig* und *lokal* ist, wissen wir nach 8.13, daß wir einen Repräsentanten (Λ, x) der gewünschten Form haben.

  Sei jetzt A beliebig, sei $(\Lambda, \tilde{x})$ irgendein Repräsentant von $\vartheta[Q]$, und sei $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ die Erweiterung der Lokalisierungen wie in 8.15. Fassen wir P als Objekt von $\widetilde{\mathcal{F}^{n,m}_{K_{\mathfrak{p}}}}$ und $[Q]$ als $L_{\mathfrak{P}}/K_{\mathfrak{p}}$-Form von P auf, so wird $\vartheta[Q]$ nach nach 5.20 und 8.15 durch das Paar $(\Lambda \otimes_K K_{\mathfrak{p}}, \tilde{x} \otimes 1)$ repräsentiert.

  Es ist $\Lambda = \prod_{i=1}^t \Lambda_i$ mit Teilkörpern Λ_i von $\bar{K}$. Sei C_i der ganze Abschluß von $A_{\mathfrak{p}}$ in Λ_i, und seien $\mathfrak{q}_1^{(i)}, \ldots, \mathfrak{q}_{m_i}^{(i)}$ die Primideale von C_i, die über $\mathfrak{p}$ liegen. Dann gilt (vgl. [Neu92, II.8, S.173]):

$$\Lambda_i \otimes_K K_{\mathfrak{p}} = \prod_{j=1}^{m_i} \underbrace{(\Lambda_i)_{\mathfrak{q}_j^{(i)}}}_{=:\Lambda_{ij}}, \quad \text{und also} \quad \Lambda \otimes_K K_{\mathfrak{p}} = \prod_{i,j} \Lambda_{ij}.$$

  Nach dem schon bewiesenen Spezialfall wissen wir, daß die Λ_{ij} unverzweigt sind (denn die Eigenschaft, unverzweigt zu sein, ist invariant unter $K_{\mathfrak{p}}$-Isomorphismen), und es folgt, daß die Λ_i unverzweigt bei $\mathfrak{p}$ sind (vgl. [Neu92, II.9, S.179]).

  Sei C_{ij} der ganze Abschluß von $\widehat{A_{\mathfrak{p}}}$ in Λ_{ij}. Bezeichne $(\tilde{x}_{ij})$ das Bild von $\tilde{x}$ in $\prod \Lambda_{ij}$. Aus dem Spezialfall wissen wir, daß es $\hat{x}_{ij} \in C_{ij}^\times$ gibt, so daß $\left(\prod \Lambda_{ij}, (\tilde{x}_{ij})\right)$ und $\left(\prod \Lambda_{ij}, (\hat{x}_{ij})\right)$ dieselbe Kohomologieklasse repräsentieren. Also gibt es nach 7.8 ein $\lambda \in K_{\mathfrak{p}}$, ein $a \in \mathrm{Aut}_{K_{\mathfrak{p}}}(\prod \Lambda_{ij})$ und ein $y = (y_{ij}) \in \prod \Lambda_{ij}^\times$, so daß

$$\hat{x} = a[\lambda(\tilde{x} \otimes 1)y^m]$$

  gilt. Nach Ersetzen von $\hat{x}$ durch $a^{-1}\hat{x}$ dürfen wir also ohne Beschränkung der Allgemeinheit annehmen, daß $\hat{x}_{ij} = \lambda \tilde{x}_{ij} y_{ij}^m$ für alle i und j gilt.

  Sei $v : L_{\mathfrak{P}} \to \mathbb{Q} \cup \{\infty\}$ die eindeutig bestimmte Fortsetzung der Bewertung $v_{\mathfrak{p}}$, sei $c := v(\lambda)$, und sei $c_{ij} := v(y_{ij})$ für alle i und j. Weil alle $\Lambda_{ij}/K_{\mathfrak{p}}$ unverzweigt sind,

sind c und alle c_{ij} *ganze* Zahlen. Wähle mit Hilfe des Approximationssatzes ([Neu92, II.3, S.122]) ein $\tilde{\lambda} \in A_\mathfrak{p}$ und $\tilde{y}_i \in C_i$ mit

$$\tilde{\lambda} \in \mathfrak{p}^c \setminus \mathfrak{p}^{c+1} \quad \text{und} \quad \tilde{y}_i \in (\mathfrak{q}_j^{(i)})^{c_{ij}} \setminus (\mathfrak{q}_j^{(i)})^{c_{ij}+1},$$

und setze $\tilde{y} := (\tilde{y}_i)$ und $x := \tilde{\lambda}\tilde{x}\tilde{y}^m$. Bezeichnet (x_{ij}) das Bild von x in $\prod \Lambda_{ij}$, so gilt nach Konstruktion $v(x_{ij}) = v(\hat{x}_{ij}) = 0$ für alle i und j. Dies ist äquivalent dazu, daß $\varphi(x)$ für alle $\varphi \in M$ eine Einheit in $B_\mathfrak{P}$ ist. Also ist (Λ, x) ein Repräsentant von $\vartheta[Q]$, der die Bedingungen (i) und (ii) erfüllt.

- *(3) ⇒ (1):* Sei also (Λ, x) ein Repräsentant von $\vartheta[Q]$, der die Bedingungen (i) und (ii) erfüllt. Sei $x = (x_1, \ldots, x_t)$ mit $x_i \in \Lambda_i^\times$, sei $i \in \{1, \ldots, t\}$ beliebig, und seien wieder $\mathfrak{q}_1^{(i)}, \ldots, \mathfrak{q}_{m_i}^{(i)}$ die Primideale von C_i, die über $\mathfrak{p}$ liegen. Weil $C_i/A_\mathfrak{p}$ nach Voraussetzung unverzweigt ist, gilt dann also $\mathfrak{p}C_i = \prod_{j=1}^{m_i} \mathfrak{q}_j^{(i)}$, und nach dem Chinesischen Restsatz folgt, daß wir einen kanonischen Isomorphismus

$$C_i/\mathfrak{p} \xrightarrow{\sim} \prod_{j=1}^{m_i} C_i/\mathfrak{q}_j^{(i)} = \prod_{j=1}^{m_i} \kappa(\mathfrak{q}_j^{(i)}) \tag{30}$$

haben. Wähle für jedes $j \in \{1, \ldots, m_i\}$ eine $\kappa(\mathfrak{p})$-Basis $\{\bar{e}_1^{ij}, \ldots, \bar{e}_{f_{ij}}^{ij}\}$ von $\kappa(\mathfrak{q}_j^{(i)})$ und lifte die $\bar{e}_k^{ij}$ zu Elementen e_k^{ij} aus C_i; dann impliziert das Nakayama-Lemma, daß C_i von den e_k^{ij} als $A_\mathfrak{p}$-Modul erzeugt wird. Weil $A_\mathfrak{p}$ als diskreter Bewertungsring insbesondere ein *Hauptidealring* ist, wissen wir, daß C_i ein *freier* $A_\mathfrak{p}$-Modul vom Rang n_i ist, und somit folgt aus der Formel $n_i := [\Lambda_i : K] = \sum_{j=1}^{m_i} f_{ij}$ (hier geht wieder die Unverzweigtheit ein!), daß die e_k^{ij} eine $A_\mathfrak{p}$-Basis von C_i bilden und damit insbesondere auch eine K-Basis von Λ_i. — Bilde mit Hilfe dieser Basis die Matrix

$$E_i := \left(\varphi e_k^{ij}\right)_{\varphi \in M_i, (j,k) \in \{(j,k) \,|\, j \in \{1,\ldots,m_i\},\, k \in \{1,\ldots,f_{ij}\}\}},$$

wobei wir $M_i := \mathrm{Hom}_K(\Lambda_i, \bar{K})$ setzen. Bekanntlich (vgl. [Ser79, S.50]!) gilt

$$(\det E_i)^2 = \mathfrak{d}_{C_i/A_\mathfrak{p}},$$

die Diskriminante von $C_i/A_\mathfrak{p}$. Wegen der Unverzweigtheit wissen wir aber $\mathfrak{d}_{C_i/A_\mathfrak{p}} = A_\mathfrak{p}$, und es folgt $E_i \in \mathrm{GL}\,(n_i, B_\mathfrak{P})$.

Setze

$$H_i := \underbrace{\mathrm{diag}\left(\frac{1}{\sqrt[m]{\varphi x_i}}\right)_{\varphi \in M_i}}_{=:\, F_i} \cdot E_i.$$

Weil alle φx_i Einheiten in $B_\mathfrak{P}$ sind, gilt dasselbe auch für die $\frac{1}{\sqrt[m]{\varphi x_i}}$, d.h. auch die Matrizen F_i und H_i liegen in $\mathrm{GL}\,(n_i, B_\mathfrak{P})$ und definieren also insbesondere ein Element in $\mathrm{PGL}\,(n, B_\mathfrak{P})$.

Werfen wir einen Blick zurück in den Beweis von 5.17, so sehen wir, daß die Matrizen H_i die Rolle der dort auftretenden B_i spielen, und es folgt, daß die Matrix $H := \mathrm{diag}\,(H_i)_{i \in \{1,\ldots,t\}}$ [†] einen $\bar{K}$-Isomorphismus von $P_n^m(\Lambda, x)$ nach P_n^m definiert. — Wegen $H \in \mathrm{GL}\,(n, B_\mathfrak{P})$ folgt hieraus per definitionem, daß $P_n^m(\Lambda, x)$ eine $\mathfrak{p}$-reduzible Form von P_n^m ist.

[†] Die entsprechende Matrix wurde im Beweis von 5.17 mit B bezeichnet.

- Es bleibt zu zeigen, daß $s_{\mathfrak{p}}[Q]$ gerade durch das Paar $(\prod_{i=1}^{t}(C_i/\mathfrak{p}), x \bmod \mathfrak{p})$ gegeben wird, wenn die Bedingungen (1), (2) und (3) erfüllt sind.

  Wegen 5.20, 8.13 und 8.15 müssen wir dazu nur zeigen, daß

$$\inf^{-1}(\Lambda \otimes_K K_{\mathfrak{p}}, x \otimes 1) = \left(\prod_{i=1}^{t}(C_i/\mathfrak{p}), x \bmod \mathfrak{p}\right)$$

  gilt. Seien dazu wie oben $\mathfrak{q}_j^{(i)}$ die Primideale von C_i über $\mathfrak{p}$ und C_{ij} der ganze Abschluß von $\widehat{A_{\mathfrak{p}}}$ in $\Lambda_{ij} := (\Lambda_i)_{\mathfrak{q}_j^{(i)}}$. Dann gilt (vgl. [Neu92, II.8, S.174]):

$$C_i \otimes_{A_{\mathfrak{p}}} \widehat{A_{\mathfrak{p}}} \cong \prod_j C_{ij},$$

  und es folgt

$$C_i/\mathfrak{p} = C_i \otimes_{A_{\mathfrak{p}}} (A_{\mathfrak{p}}/\mathfrak{p}) = C_i \otimes_{A_{\mathfrak{p}}} \widehat{A_{\mathfrak{p}}} \otimes_{\widehat{A_{\mathfrak{p}}}} (\widehat{A_{\mathfrak{p}}}/\mathfrak{p}\widehat{A_{\mathfrak{p}}}) = \prod_j C_{ij}/\mathfrak{p}\widehat{A_{\mathfrak{p}}}.$$

  Damit folgt die Behauptung mit Hilfe der expliziten Beschreibung von $\inf^{-1}$ in 8.13, und das Theorem ist vollständig bewiesen.

q.e.d.

8.18 Beispiel. Es sei speziell $K = \mathbb{Q}$, $n = 4$, $m = 3$, $\mathfrak{p} = (5)$, $\Lambda = \Lambda_1 \times \Lambda_2 = \mathbb{Q}(\sqrt[3]{2}) \times \mathbb{Q}$ und $x = (x_1, x_2) = (5\sqrt[3]{2}, 10)$.

Setze $\vartheta := \sqrt[3]{2}$; dann ist $\{1, \vartheta, \vartheta^2\}$ eine $\mathbb{Q}$-Basis von Λ_1, und wenn wir $Q = P_4^3(\Lambda, x)$ mit Hilfe dieser Basis berechnen, erhalten wir

$$\begin{aligned}
Q &= \mathrm{Tr}_{\Lambda_1/\mathbb{Q}}\left[\tfrac{1}{5\vartheta}\cdot(x+\vartheta y+\vartheta^2 z)^3\right] + \left[\tfrac{1}{10}u^3\right] \\
&= \mathrm{Tr}_{\Lambda_1/\mathbb{Q}}\big[\tfrac{1}{5\vartheta}\cdot\big(x^3+3\vartheta x^2y+3\vartheta^2x^2z+3\vartheta^2xy^2+12xyz+6\vartheta xz^2 \\
&\qquad +2y^3+6\vartheta y^2z+6\vartheta^2yz^2+4z^3\big)\big] + \left[\tfrac{1}{10}u^3\right] \\
&= \mathrm{Tr}_{\Lambda_1/\mathbb{Q}}\big[\tfrac{1}{5\vartheta}x^3+\tfrac{3}{5}x^2y+\tfrac{3\vartheta}{5}x^2z+\tfrac{3\vartheta}{5}xy^2+\tfrac{12}{5\vartheta}xyz+\tfrac{6}{5}xz^2 \\
&\qquad +\tfrac{2}{5\vartheta}y^3+\tfrac{6}{5}y^2z+\tfrac{6\vartheta}{5}yz^2+\tfrac{4}{5\vartheta}z^3\big] + \left[\tfrac{1}{10}u^3\right] \\
&=^{\dagger} \tfrac{9}{5}x^2y+\tfrac{18}{5}xz^2+\tfrac{18}{5}y^2z+\tfrac{1}{10}u^3.
\end{aligned}$$

Bekanntlich ist $\mathcal{O}_{\Lambda_1} = \mathbb{Z}[\vartheta]$, und $\Lambda_1/\mathbb{Q}$ ist nur bei (2) und (3) verzweigt, d.h. Bedingung (i) aus 8.17 ist erfüllt.

Wegen $N_{\Lambda_1/\mathbb{Q}}(\vartheta) = 2$ ist ϑ eine Einheit in $B_{\mathfrak{P}}$, und es folgt, daß das zu (Λ, x) äquivalente Paar $(\Lambda, \frac{1}{5}x)$ ein Repräsentant von $\vartheta[Q]$ ist, der die Bedingungen (i) und (ii) aus 8.17(3) erfüllt. Theorem 8.17 impliziert also, daß $[Q]$ (5)-reduzibel ist, daß also $s_{(5)}[Q]$ definiert ist. Man kann sich leicht überlegen, daß schon das oben berechnete Polynom Q eine (5)-reduzible Form von P_4^3 ist, d.h. $s_{(5)}[Q]$ ist die Klasse des Polynoms

$$Q_{(5)} \quad =^{\ddagger} \quad 4x^2y+3xz^2+3y^2z+3u^3. \tag{31}$$

[†]Hierbei beachte man, daß $\mathrm{Tr}(\vartheta) = \mathrm{Tr}(\frac{1}{\vartheta}) = 0$ und $\mathrm{Tr}(1) = 3$ gilt!

Andererseits wissen wir nach 8.17 aber auch, daß $s_{(5)}[Q]$ durch das Paar

$$\Big((C_1/5)\times(C_2/5),\big(5^{-1}\cdot(5\vartheta,10)\big) \bmod 5\Big) \quad = \quad \Big(\mathcal{O}_{\Lambda_1}/5\times\mathbb{F}_5,(\vartheta,2) \bmod 5\Big)$$

gegeben wird. Modulo fünf zerfällt das Polynom X^3-2 in die beiden irreduziblen Faktoren $(X+2)$ und (X^2+3X+4), d.h. der Isomorphismus (30) nimmt die folgende Gestalt an:

$$C_1/5 \xrightarrow{\sim} \mathbb{F}_5[\bar\vartheta]/(\bar\vartheta^2+3\bar\vartheta+4)\times\mathbb{F}_5, \quad \vartheta\mapsto(\bar\vartheta,3).$$

Stellen wir $\mathbb{F}_{25}$ wie in 5.16 und 5.25 als $\mathbb{F}_5(\alpha)$ dar, wobei α die Gleichung $\alpha^2+2\alpha+3=0$ erfüllt, so können wir $\bar\vartheta = 2\alpha+3 = \alpha^{14}$ wählen. Dann wird $s_{(5)}[Q]$ also durch das Paar $\big(\mathbb{F}_{25}\times\mathbb{F}_5,(\alpha^{14},3)\big)$ gegeben. Weil 14 nicht durch drei teilbar ist, ist α^{14} keine dritte Potenz in $\mathbb{F}_{25}$, und es folgt aus unseren Überlegungen in 5.16, daß $\big(\mathbb{F}_{25}\times\mathbb{F}_5,(\alpha^{14},3)\big)$ die gleiche Kohomologieklasse wie $\big(\mathbb{F}_{25}\times\mathbb{F}_5,(\alpha,1)\big)$ definiert; aus unserer Liste in 5.16 lesen wir also ab:

$$\boxed{s_{(5)}[Q] \quad = \quad 3x^3+4x^2y+y^3+z^3+u^3} \tag{32}$$

Aufgrund unserer theoretischen Überlegungen wissen wir, daß die beiden Polynome aus (31) und (32) schon über $\mathbb{F}_5$ isomorph sein, d.h. durch eine lineare Koordinatensubstitution auseinander hervorgehen müssen; und tatsächlich gilt: Die Matrix $\left(\begin{smallmatrix}0&4&4&0\\3&3&3&0\\4&3&1&0\\0&0&0&3\end{smallmatrix}\right)\in \mathrm{GL}\,(4,\mathbb{F}_5)$ definiert einen $\mathbb{F}_5$-Isomorphismus

$$(3x^3+4x^2y+y^3+z^3+u^3) \qquad \xrightarrow{\sim} \qquad (4x^2y+3xz^2+3y^2z+3u^3).$$

Ist speziell K ein Zahlkörper, so können wir mit Hilfe von 8.17 jetzt eine zahlentheoretische Interpretation der getwisteten Fermatgleichungen geben und erhalten dadurch eine weitere Motivation, die Zetafunktionen solcher Gleichungen zu studieren:

8.19 Beispiel. Es sei Λ/K eine Erweiterung von Zahlkörpern vom Grad n, $\mathfrak{p}$ ein in Λ/K unverzweigtes Primideal von K, x ein Element aus $\mathcal{O}_\Lambda$ mit $\mathfrak{p}\nmid\big(N_{\Lambda/K}(x)\big)$ und $m\geq 3$ eine natürliche Zahl.
Wir betrachten die Abbildung

$$f:\Lambda\longrightarrow K,\ \ a\mapsto \mathrm{Tr}_{\Lambda/K}(xa^m)$$

und interessieren uns für die Frage: *Wenn a alle ganzen Zahlen von Λ durchläuft, wie oft ist dann das ganze Hauptideal $(f(a))$ durch $\mathfrak{p}$ teilbar?*

Um dies präziser zu formulieren, beobachten wir zunächst, daß für $a\in\mathcal{O}_\Lambda$ die Restklasse von $f(a)$ (mod $\mathfrak{p}$) nur von der Restklasse von a modulo $\mathfrak{p}\mathcal{O}_\Lambda$ abhängt, weil die Spur ja eine K-lineare Abbildung ist. Genauer lautet unsere Frage dann:

Wieviele der Restklassen aus $\mathcal{O}_\Lambda/\mathfrak{p}\mathcal{O}_\Lambda$ werden unter f nach $\mathfrak{p}$ abgebildet?

Es sei $\{\omega_1,\dots,\omega_n\}$ eine $\mathcal{O}_{K,\mathfrak{p}}$-Basis von $\mathcal{O}_{\Lambda,\mathfrak{p}}:=\mathcal{O}_\Lambda\otimes_{\mathcal{O}_K}\mathcal{O}_{K,\mathfrak{p}}$, dem ganzen Abschluß von $\mathcal{O}_{K,\mathfrak{p}}$ in Λ, und sei $R\subseteq\mathcal{O}_K$ ein Repräsentantensystem von $\mathcal{O}_K/\mathfrak{p}$. Wegen $\mathcal{O}_\Lambda/\mathfrak{p}\mathcal{O}_\Lambda\xrightarrow{\sim}\mathcal{O}_{\Lambda,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{\Lambda,\mathfrak{p}}$ ist dann die Menge

$$S:=\{\textstyle\sum_{i=1}^n x_i\omega_i \mid x_i\in R\}$$

[‡]Wir wählen einfach $\pi=5$.

ein Repräsentantensystem von $\mathcal{O}_\Lambda/\mathfrak{p}\mathcal{O}_\Lambda$, d.h. wir können uns genauso gut fragen, wieviele Elemente aus S nach $\mathfrak{p}$ abgebildet werden; die Anzahl sei N.

Sei P der bezüglich $\{\omega_i\}$ gebildete Repräsentant der Form $P_n^m\{(\Lambda, x)\}$ von P_n^m, d.h.

$$P = \mathrm{Tr}_{\Lambda[X_i]/K[X_i]}\left[\frac{1}{x}\left(\sum_{i=1}^n \omega_i X_i\right)^m\right].$$

Offenbar gilt dann

$$\forall (x_1, \ldots, x_n) \in K: \; P(x_1, \ldots, x_n) = f\left(\textstyle\sum_{i=1}^n x_i\omega_i\right),$$

d.h.

$$N = \#\left\{\textstyle\sum_{i=1}^n x_i\omega_i \in S \mid P(x_1, \ldots, x_n) \equiv 0 \pmod{\mathfrak{p}}\right\}. \tag{33}$$

Nach Voraussetzung[†] ist x eine Einheit in $\mathcal{O}_{\Lambda,\mathfrak{p}}$, dann sind auch alle Konjugierten φx für ein φ aus $\mathrm{Hom}_K(\Lambda, \overline{Q})$ Einheiten in $\mathcal{O}_{\Lambda,\mathfrak{p}}$. Weil $\mathfrak{p}$ als unverzweigt vorausgesetzt wurde, folgt dann wie im Beweis von 8.17, daß P eine $\mathfrak{p}$-reduzible Form von P_n^m ist.

Betrachten wir die Spezialisierung $P_\mathfrak{p}$! Es ist $v_\mathfrak{p}(P) \overset{8.5}{=} v_\mathfrak{p}(P_n^m) = 0$, d.h. $P_\mathfrak{p} = P \pmod{\mathfrak{p}}$. Also gilt:

$$N \overset{(33)}{=} \#\left\{(\bar{x}_1, \ldots, \bar{x}_n) \in \kappa(\mathfrak{p})^n \mid P_\mathfrak{p}(\bar{x}_1, \ldots, \bar{x}_n) = 0\right\} = \#P_\mathfrak{p}(\kappa(\mathfrak{p})). \tag{34}$$

Es sei $\mathfrak{p}\mathcal{O}_\Lambda = \prod_{i=1}^r \mathfrak{P}_i$ die Primfaktorzerlegung von $\mathfrak{p}$ in Λ (man beachte, daß die $\mathfrak{P}_i$ paarweise verschieden sind, da $\mathfrak{p}$ als unverzweigt vorausgesetzt wurde), und es seien $f_i := [\kappa(\mathfrak{P}_i) : \kappa(\mathfrak{p})]$ die Trägheitsgrade; ferner sei $q := \#\kappa(\mathfrak{p})$. Dann gilt

$$\mathcal{O}_{\Lambda,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_\Lambda \cong \prod_{i=1}^r \mathcal{O}_{\Lambda,\mathfrak{p}}/\mathfrak{P}_i \cong \prod_{i=1}^r \kappa(\mathfrak{P}_i) \cong \prod_{i=1}^r \mathbb{F}_{q^{f_i}}. \tag{35}$$

Bezeichne x_i das Bild von x unter $\mathcal{O}_\Lambda \twoheadrightarrow \mathcal{O}_\Lambda/\mathfrak{P}_i \xrightarrow{\sim} \mathbb{F}_{q^{f_i}}$. Dann folgt aus (34) und (35) mittels 8.17:

$$\boxed{N = \#P_n^m\left\{\left(\textstyle\prod_{i=1}^r \mathbb{F}_{q^{f_i}}\right), (x_1, \ldots, x_r)\right\}(\mathbb{F}_q).}$$

Wir sehen also: Die Frage nach der Anzahl der $\mathbb{F}_q$-rationalen Punkte einer $\overline{\mathbb{F}}_q/\mathbb{F}_q$-Form von P_n^m hängt eng zusammen mit der Frage nach der Verteilung von Spuren m-ter Potenzen ganzer algebraischer Zahlen.

[†]Nach Voraussetzung ist $N := N_{\Lambda/K}(x)$ eine Einheit in $\mathcal{O}_{K,\mathfrak{p}}$, also ist $\frac{1}{x} = \frac{1}{N}\prod_{\varphi\neq\iota}\varphi x$, wobei φ alle K-Einbettungen von Λ nach $\overline{\mathbb{Q}}$ durchläuft und ι die identische Einbettung bezeichnet, und dies ist dann offenbar eine ganze Zahl.

9 Kohomologie der Fermathyperfläche

In diesem Kapitel werden wir die Kohomologie von getwisteten Fermathyperflächen studieren und berechnen, welchen Isomorphismus auf der mittleren Kohomologie der Fermathyperfläche $\mathcal{X}_n^m$ ein Isomorphismus von $\mathcal{X}_n^m$ induziert. Wir beschränken uns dabei auf die mittlere Kohomologie, weil diese für Hyperflächen die einzig interessante ist — die anderen werden einfach von den Potenzen der Klasse eines Hyperebenenschnittes erzeugt.

Es seien $n, m \in \mathbb{N}_+$ mit $n \geq 2$, P_n^m die in den Kapiteln 5 und 7 betrachtete Fermatgleichung, $\tilde{A}$ die in 7.1 bzw. 7.2 definierte Gruppe $(\mu_m^n/\mu_m) \rtimes S_n$ und $k = \mathbb{F}_q$ ein endlicher Körper der Charakteristik $p > \max(m, 2)$ mit (separablen) algebraischem Abschluß $K = \bar{k}$. Ferner sei $l \neq p$ eine Primzahl mit $l \equiv 1 \pmod{m}$.

9.1 Lemma/ Definition. Sei $\mathcal{X} := \mathcal{X}_n^m$ die unter dem Funktor F_k zu P_n^m assoziierte $(n-2)$-dimensionale Fermathyperfläche (vgl. 3.11!). Sei A die endliche abelsche Gruppe μ_m^n/μ_m (so daß also $\tilde{A} = A \rtimes S_n$ ist), sei $\zeta \in \mathbb{C}$ die primitive m-te Einheitswurzel $\mathrm{e}^{\frac{2\pi i}{m}}$, und wähle eine Einbettung $\mu_m \hookrightarrow \mathbb{Q}(\zeta)$. Dann ist $\check{A}$, das Dual von A, isomorph zu

$$\left\{ \boldsymbol{a} = (a_1, \ldots, a_n) \in (\mathbb{Z}/m\mathbb{Z})^n \;\middle|\; \sum_{i=1}^{n} a_i = 0 \in \mathbb{Z}/m\mathbb{Z} \right\}$$

mittels der Paarung

$$(\boldsymbol{a}, \underbrace{[(\zeta_1, \ldots, \zeta_n)]}_{\in A}) \mapsto \prod_{i=1}^{n} \zeta_i^{a_i}.$$

Die Operation von S_n aus 4.1 übersetzt sich dabei in die natürliche Operation

$${}^s(a_1, \ldots, a_n) = (a_{s^{-1}(1)}, \ldots, a_{s^{-1}(n)}).$$

Außerdem operiert offenbar auch $(\mathbb{Z}/m\mathbb{Z})^\times$ auf $\check{A}$ via $\boldsymbol{a} \mapsto t\boldsymbol{a} := (ta_1, \ldots, ta_n)$ für $t \in (\mathbb{Z}/m\mathbb{Z})^\times$ beliebig. Bezeichne den Orbit von $\boldsymbol{a}$ unter der Operation von S_n mit $[\boldsymbol{a}]$ und den Orbit unter der Operation von $(\mathbb{Z}/m\mathbb{Z})^\times$ mit $\langle \boldsymbol{a} \rangle$.

Definiere

$$A_n^m := \left\{ \boldsymbol{a} \in \check{A} \mid \forall i \in \{1, \ldots, n\} \;:\; a_i \neq 0 \in \mathbb{Z}/m\mathbb{Z} \right\}.$$

Setze $\bar{\mathcal{X}} := \mathcal{X} \times_k \bar{k}$ und $V := \mathrm{H}_{\text{ét}}^{n-2}(\bar{\mathcal{X}}, \mathbb{Q}_l)$. Gemäß Beispiel 4.7(ii) erhalten wir eine kanonische Zerlegung von V als $\mathbb{Q}_l$-Vektorraum

$$V = \bigoplus_{\chi \in \check{A}} V_\chi,$$

die sogar eine Zerlegung als $\mathbb{Q}_l$-G_k-Darstellung ist, wenn $\tilde{A}$ mit dem Frobenius vertauscht, was genau dann der Fall ist, wenn k die m-ten Einheitswurzeln enthält, d.h. wenn $q \equiv 1 \pmod{m}$ gilt. Insbesondere sind also für $\boldsymbol{a} \in A_n^m$ die $\mathbb{Q}_l$-Vektorräume (bzw. $\mathbb{Q}_l$-G_k-Darstellungen) $V_{\boldsymbol{a}}$ definiert. Wir setzen ferner (vgl. 4.6!):

$$V_{[\boldsymbol{a}]} := \bigoplus_{\boldsymbol{b} \in [\boldsymbol{a}]} V_{\boldsymbol{b}}, \quad V_{\langle \boldsymbol{a} \rangle} := \bigoplus_{\boldsymbol{b} \in \langle \boldsymbol{a} \rangle} V_{\boldsymbol{b}}.$$

Beweis: Vgl. [GY95]! **q.e.d.**

Bevor wir das in der Einleitung erwähnte Resultat von Deligne über die Frobeniusoperation auf V formulieren können, müssen wir zunächst definieren, was eine *Jacobisumme* ist.

9.2 Definition. Es sei κ ein endlicher Körper, der die m-ten Einheitswurzeln enthält. Dann kann man einen multiplikativen Charakter χ von κ wählen, der genau Ordnung m hat:

$$\chi : \kappa^\times \twoheadrightarrow \mu_m \hookrightarrow \mathbb{Q}(\zeta) \hookrightarrow \mathbb{Q}_l.$$

Für $\boldsymbol{a} \in A_n^m$ definiere die *Jacobisumme der Dimension* $(n-2)$ *vom Grad* m *zu* $\boldsymbol{a}$ (bezüglich κ und χ und der Einbettung $\mu_m \hookrightarrow \mathbb{Q}(\zeta) \hookrightarrow \mathbb{Q}_l$) als

$$\mathcal{J}_\kappa^m(\boldsymbol{a}) := \mathcal{J}(\boldsymbol{a}) := (-1)^n \sum_{\substack{(v_2,\ldots,v_n)\in\kappa^\times\times\ldots\times\kappa^\times \\ 1+v_2+\ldots+v_n=0}} \chi(v_2)^{a_2} \cdot \chi(v_3)^{a_3} \cdot \ldots \cdot \chi(v_n)^{a_n} \in \mathbb{Q}(\zeta) \subseteq \mathbb{Q}_l.$$

Wir können $\mathcal{J}(\boldsymbol{a})$ also sowohl als Element von $\mathbb{Q}(\zeta)$ als auch als Element von $\mathbb{Q}_l$ auffassen.

9.3 Lemma. Ist m *ungerade*, und enthält k die m-ten Einheitswurzeln, so gilt für alle $\boldsymbol{a} \in A_2^m$:

$$\mathcal{J}_k^m(\boldsymbol{a}) = 1.$$

Beweis: Nach Definition gilt $\mathcal{J}_k^m(\boldsymbol{a}) = \chi(-1)$. Nun hat aber (-1) Ordnung 2 in $k^\times$, d.h. es muß $\chi(-1) \in \{-1, 1\} \cap \mu_m = \{1\}$ gelten. **q.e.d.**

9.4 Definition. Es sei L ein Zahlkörper, $\mathfrak{m} \neq 0$ ein ganzes Ideal von L und $I_\mathfrak{m}$ die Gruppe der zu $\mathfrak{m}$ teilerfremden gebrochenen Ideale von L. Dann heißt ein Gruppenhomomorphismus $\varphi : I_\mathfrak{m} \to \mathbb{C}^\times$ ein *Größencharakter von* L *mit Erklärungsmodul* $\mathfrak{m}$, wenn es ganze Zahlen n_σ für alle $\sigma \in \mathrm{Hom}_\mathbb{Q}(L, \mathbb{C})$ gibt, so daß für alle Hauptideale $(a) \in I_\mathfrak{m}$ mit $a \equiv 1 \pmod{\mathfrak{m}}$ und a total positiv gilt: $\varphi\big((a)\big) = \prod_\sigma (\sigma a)^{n_\sigma}$. In diesem Fall heißt das Tupel $(n_\sigma)_\sigma$ der *Unendlichtyp* des Größencharakters φ.

9.5 Satz. Es sei wieder $\zeta = \mathrm{e}^{\frac{2\pi i}{m}}$, es sei $\mathfrak{p}$ ein Primideal von $\mathbb{Q}(\zeta)$, das teilerfremd zu m ist, und es bezeichne $\kappa_\mathfrak{p}$ den Restklassenkörper von $\mathfrak{p}$. Dann ist $\kappa_\mathfrak{p}$ ein endlicher Körper, der die m-ten Einheitswurzeln enthält, und wir können einen multiplikativen Charakter $\chi : \kappa^\times \to \mu_m$ der Ordnung m durch die Vorschrift

$$\forall x \in \kappa^\times \,:\, x^{\frac{|\kappa|-1}{m}} \equiv \chi(x) \pmod{\mathfrak{p}}$$

definieren. Für $\boldsymbol{a} \in A_n^m$ setze $\mathbf{J}_{\boldsymbol{a}}(\mathfrak{p}) := \mathcal{J}_{\kappa_\mathfrak{p}}^m(\boldsymbol{a})$, wobei die Jacobisumme bezüglich des soeben definierten Charakters χ gebildet werde. Man setze $\mathbf{J}_{\boldsymbol{a}}$ multiplikativ auf die Gruppe $I_{(m)}{=}I_{(m^2)}$ fort zu einem Gruppenhomomorphismus

$$\mathbf{J}_{\boldsymbol{a}} : I_{(m^2)} \longrightarrow \mathbb{C}^\times.$$

Dann gilt: $\mathbf{J}_{\boldsymbol{a}}$ ist ein Größencharakter zum Erklärungsmodul (m^2).

Beweis: Siehe [Wei52]! **q.e.d.**

9.6 Lemma/ Definition. Es sei hier $n \geq 4$, und $r, s \in \mathbb{N}$ seien natürliche Zahlen mit $r, s \geq 3$ und $r + s = n + 2$. Man setze

$$A^m_{r,s} := \{(\boldsymbol{b}, \boldsymbol{c}) \in A^m_r \times A^m_s \mid b_r + c_s = 0\}$$

und betrachte die Abbildungen

$$\begin{array}{lllllll} A^m_{r,s} & \xrightarrow{\sharp} & A^m_n, & (\boldsymbol{b}, \boldsymbol{c}) & \mapsto & \boldsymbol{b} \sharp \boldsymbol{c} & := & (b_1, \ldots, b_{r-1}, c_1, \ldots, c_{s-1}) \quad \text{und} \\ A^m_{r-1} \times A^m_{s-1} & \xrightarrow{*} & A^m_n, & (\boldsymbol{b'}, \boldsymbol{c'}) & \mapsto & \boldsymbol{b'} * \boldsymbol{c'} & := & (b'_1, \ldots, b'_{r-1}, c'_1, \ldots, c'_{s-1}). \end{array}$$

Dann ist die Abbildung $A^m_{r,s} \coprod \left(A^m_{r-1} \times A^m_{s-1}\right) \xrightarrow{\sharp \sqcup *} A^m_n$ eine Bijektion.

Beweis: Vgl. [Shi79]! **q.e.d.**

9.7 Satz. Es gelte $q \equiv 1 \pmod{m}$, d.h. k enthält die m-ten Einheitswurzeln, und wir können Jacobisummen bezüglich k betrachten. Dann haben wir die folgenden Regeln für das Rechnen mit Jacobisummen:

(i) Es seien $\boldsymbol{a} \in A^m_n$ und $t \in (\mathbb{Z}/m\mathbb{Z})^\times$ beliebig, und bezeichne σ den durch $\zeta \mapsto \zeta^t$ definierten Automorphismus von $\mathbb{Q}(\zeta)$. Dann gilt:

$$\mathcal{J}^m_k(t\boldsymbol{a}) = \sigma\left(\mathcal{J}^m_k(\boldsymbol{a})\right).$$

(ii) Sei $\psi : (k, +) \longrightarrow \mathbb{C}^\times$ der durch $\psi(x) := \exp\left(\frac{\mathrm{Tr}_{k/\mathbb{F}_p}(x)}{p}\right)$ gegebene Charakter der additiven Gruppe von k und $\xi : k^\times \longrightarrow \mathbb{C}^\times$ ein nichttrivialer Charakter der multiplikativen Gruppe von k. Definiere die *Gaußsche Summe*

$$G(\xi) := \sum_{x \in k^\times} \xi(x)\psi(x).$$

Dann gilt $G(\xi)\overline{G(\xi)} = q$ und $G(\bar{\xi}) = \xi(-1)\overline{G(\xi)}$, und für $\boldsymbol{a} \in A^m_n$ haben wir die Produktdarstellung

$$\mathcal{J}(\boldsymbol{a}) = \frac{(-1)^n}{q} \cdot G(\chi^{a_1}) \cdot \ldots \cdot G(\chi^{a_n}).$$

Man beachte, daß insbesondere $\mathcal{J}(\boldsymbol{a})$ nur von $[\boldsymbol{a}]$ abhängt!

(iii) Sei $n \geq 4$, und seien $r, s \in \mathbb{N}$ mit $r, s \geq 3$ und $r+s = n+2$. Dann gilt für $(\boldsymbol{b}, \boldsymbol{c}) \in A^m_{r,s}$ und $(\boldsymbol{b'}, \boldsymbol{c'}) \in A^m_{r-1} \times A^m_{s-1}$:

$$\begin{array}{lcl} \mathcal{J}(\boldsymbol{b} \sharp \boldsymbol{c}) & = & \chi(-1)^{b_r} \cdot \mathcal{J}(\boldsymbol{b}) \cdot \mathcal{J}(\boldsymbol{c}) \quad \text{und} \\ \mathcal{J}(\boldsymbol{b'} * \boldsymbol{c'}) & = & q \cdot \mathcal{J}(\boldsymbol{b'}) \cdot \mathcal{J}(\boldsymbol{c'}). \end{array}$$

Beweis: Vergleiche [Wei49] und [GY95, S.13ff]!

Gouvêa und Yui zeigen (i), Weil zeigt die Formel $G(\xi)\overline{G(\xi)} = q$ und die Produktdarstellung der Jacobisumme aus (ii). Man berechnet leicht:

$$G(\bar{\xi}) = \sum_{x\in k^\times} \overline{\xi(x)}\psi(x) = \sum_{x\in k^\times} \overline{\xi(-x)}\psi(-x) = \xi(-1)\sum_{x\in k^\times} \overline{\xi(x)\psi(x)} = \xi(-1)\overline{G(\xi)}.$$

Wir wollen rasch die Formeln in (iii) nachrechnen:

$$\begin{array}{rcl}
\mathcal{J}(\boldsymbol{b}\sharp\boldsymbol{c}) & \overset{(ii)}{=} & \frac{(-1)^n}{q}\cdot G(\chi^{b_1})\cdot\ldots\cdot G(\chi^{b_{r-1}})\cdot G(\chi^{c_1})\cdot\ldots\cdot G(\chi^{c_{s-1}}) \\
& = & \frac{(-1)^n}{q}\cdot\big[(-1)^r\cdot q\cdot G(\chi^{b_r})^{-1}\mathcal{J}(\boldsymbol{b})\big]\cdot[(-1)^s\cdot q\cdot G(\chi^{c_s})^{-1}\mathcal{J}(\boldsymbol{c})] \\
& = & \underbrace{(-1)^{n+r+s}}_{=(-1)^{2n+2}=1}\cdot\mathcal{J}(\boldsymbol{b})\cdot\mathcal{J}(\boldsymbol{c})\cdot q^2/[\quad \underbrace{G(\chi^{b_r})\cdot G(\overline{\chi^{b_r}})}_{\begin{array}{l}=\ G(\chi^{b_r})\cdot\chi(-1)^{b_r}\cdot\overline{G(\chi^{b_r})}\\ =\ q\chi(-1)^{b_r}\end{array}}\quad], \\
\mathcal{J}(\boldsymbol{b'}*\boldsymbol{c'}) & \overset{(ii)}{=} & \frac{(-1)^n}{q}\cdot G(\chi^{b'_1})\cdot\ldots\cdot G(\chi^{b'_{r-1}})\cdot G(\chi^{c'_1})\cdot\ldots\cdot G(\chi^{c'_{s-1}}) \\
& = & \frac{(-1)^n}{q}\cdot[(-1)^{r-1}\cdot q\cdot\mathcal{J}(\boldsymbol{b'})]\cdot[(-1)^{s-1}\cdot q\cdot\mathcal{J}(\boldsymbol{c'})] \\
& = & \underbrace{(-1)^{n+r+s-2}}_{=(-1)^{2n}=1}\cdot q\cdot\mathcal{J}(\boldsymbol{b'})\cdot\mathcal{J}(\boldsymbol{c'}).
\end{array}$$

q.e.d.

9.8 Beispiel. Es sei $n = 6$, $m = 3$ und $p = q = 7$. Setze $\boldsymbol{a} := (1,1,1,2,2,2) \in A_6^3$ und $\boldsymbol{b} := (1,1,1,1,1,1) \in A_6^3$. Man überlegt sich leicht, daß dann $A_6^3 = [\boldsymbol{a}] \sqcup \{\boldsymbol{b}\} \sqcup \{2\boldsymbol{b}\}$ gilt. In $\mathbb{F}_7$ ist 3 erzeugendes Element der multiplikativen Gruppe; der Charakter χ kann also durch $\chi(3) := \zeta$ definiert werden. Wir wollen $\mathcal{J}(\boldsymbol{a})$, $\mathcal{J}(\boldsymbol{b})$ und $\mathcal{J}(2\boldsymbol{b})$ berechnen. Zunächst gilt $(2,1,2,1,2,1) \in [\boldsymbol{a}]$ und $(2,1,2,1,2,1) = (2,1,2,1)\sharp(1,2,1,2) = [(2,1)*(2,1)]\sharp[(1,2)*(1,2)]$, und es ist:

$$\mathcal{J}(1,2) = \mathcal{J}(2,1) = (-1)^2\cdot\chi(6)^1 = 1.$$

Also folgt

$$\mathcal{J}(\boldsymbol{a}) \overset{9.7(ii)}{=} \chi(-1)^1\cdot[7\cdot1\cdot1]\cdot[7\cdot1\cdot1] = 49.$$

Wegen $\boldsymbol{b} = (1,1,1)*(1,1,1)$ berechnen wir nun zunächst $\mathcal{J}(1,1,1)$, wobei wir beachten, daß die Gleichung $1+\zeta+\zeta^2 = 0$ gilt:

$$\begin{array}{rcl}
\mathcal{J}(1,1,1) & = & (-1)^3\cdot[\chi(1)\chi(5)+\chi(2)\chi(4)+\chi(3)\chi(3)+\chi(4)\chi(2)+\chi(5)\chi(1)] \\
& = & -[\chi(5)+\chi(8)+\chi(9)+\chi(8)+\chi(5)] \ = \ -[2\chi(3^5)+2+\chi(3^2)] \\
& = & -[2\zeta^2+2+\zeta^2] \ = \ -2-3\zeta^2 \ = \ -2-3(-1-\zeta) \\
& = & 1+3\zeta.
\end{array}$$

Damit ergibt sich dann

$$\mathcal{J}(\boldsymbol{b}) \overset{9.7(ii)}{=} 7\cdot(1+3\zeta)^2 = 7\cdot(1+6\zeta+9\zeta^2) = 7\cdot(-8-3\zeta) = -56-21\zeta.$$

Wir wollen nun noch $\mathcal{J}(2\boldsymbol{b})$ mit Hilfe von 9.7(i) berechnen. Dazu betrachten wir den Automorphismus σ von $\mathbb{Q}(\zeta)$, der durch $\zeta \mapsto \zeta^2 = -1-\zeta$ gegeben wird. Mit seiner Hilfe folgt:

$$\mathcal{J}(2\boldsymbol{b}) \overset{9.7(i)}{=} \sigma\big(\mathcal{J}(\boldsymbol{b})\big) = \sigma(-56-21\zeta) = -56-21(-1-\zeta) = -35+21\zeta.$$

Jetzt kommen wir zu dem angekündigten Resultat von Deligne:

9.9 Satz. Für $V = \mathrm{H}^{n-2}_{\text{ét}}(\bar{\mathcal{X}}, \mathbb{Q}_l)$ gilt:

$$V = \underbrace{\left(\bigoplus_{\boldsymbol{a} \in A^m_n} V_{\boldsymbol{a}} \right)}_{=:V^m_{n,\mathrm{prim}} =: V_{\mathrm{prim}}} \oplus \begin{cases} 0 & \text{, falls } n \text{ ungerade,} \\ \mathbb{Q}_l(-\frac{n-2}{2}) & \text{, falls } n \text{ gerade,} \end{cases}$$

und die $V_{\boldsymbol{a}}$ sind eindimensionale $\mathbb{Q}_l$-Vektorräume. Weil $\mathcal{X}$ eine Hyperfläche ist, gilt außerdem für $i \in \{0, 1, \ldots, 2n-4\} \setminus \{n-2\}$:

$$\mathrm{H}^i_{\text{ét}}(\bar{\mathcal{X}}, \mathbb{Q}_l) = \begin{cases} 0 & \text{, falls } i \text{ ungerade,} \\ \mathbb{Q}_l(-\frac{i}{2}) & \text{, falls } i \text{ gerade.} \end{cases}$$

Gilt zusätzlich $q \equiv 1 \pmod m$ (so daß also k die m-ten Einheitswurzeln enthält), so respektiert der geometrische Frobenius obige Zerlegung von V_{prim} und operiert auf den $V_{\boldsymbol{a}}$ per Multiplikation mit der Jacobisumme $\mathcal{J}(\boldsymbol{a})$.

Beweis: Siehe [Del82, I., §7]! **q.e.d.**

Der Fall, daß k die m-ten Einheitswurzeln *nicht* enthält, wird in keiner der in der Einleitung erwähnten Arbeiten von Weil, Deligne, Shioda oder Gouvêa/ Yui behandelt. Wir untersuchen jetzt, wie der Frobenius in diesem Fall operiert:

9.10 Satz. Es sei $\boldsymbol{a} \in A^m_n$ beliebig, und bezeichne F den geometrischen Frobenius auf $\mathcal{X}$. Dann bildet F^* den Raum $V_{\boldsymbol{a}}$ nach $V_{q\boldsymbol{a}}$ ab (wobei wir q als Element von $(\mathbb{Z}/m\mathbb{Z})^\times$ auffassen). Insbesondere ist also $V_{\langle \boldsymbol{a} \rangle}$ invariant unter der Frobenius-Operation und folglich eine $\mathbb{Q}_l$-G_k-Darstellung, d.h. wir erhalten eine Zerlegung von V_{prim} in $\mathbf{Rep}^{G_k}_{\mathbb{Q}_l}$ als

$$V_{\mathrm{prim}} = \bigoplus_{\langle \boldsymbol{a} \rangle \in A^m_n/(\mathbb{Z}/m\mathbb{Z})^\times} V_{\langle \boldsymbol{a} \rangle}.$$

Sei $d := \mathrm{ggT}\,(m, a_1, \ldots, a_n)$, $m' := m/d$, $\boldsymbol{a'} := (a_1/d, \ldots, a_n/d)$ und e die Ordnung von q in $(\mathbb{Z}/m'\mathbb{Z})^\times$ (d.h. $\mathbb{F}_{q^e}$ ist der kleinste Körper der Charakteristik p, der die m'-ten Einheitswurzeln enthält). Dann ist $\langle \boldsymbol{a} \rangle = \{q^i \boldsymbol{a} \,|\, i \in \{0, \ldots, e-1\}\}$, wobei die $q^i\boldsymbol{a}$ paarweise verschieden sind. Insbesondere gilt also $e = \#\langle \boldsymbol{a} \rangle$.

Sei $v \in V_{\boldsymbol{a}} \setminus \{0\}$ beliebig, und man setze $v_i := (F^*)^i v \in V_{q^i\boldsymbol{a}} \setminus \{0\}$ für $i \in \{0, \ldots, e-1\}$. Bezüglich der Basis $\{v = v_0, v_1, \ldots, v_{e-1}\}$ von $V_{\langle \boldsymbol{a} \rangle}$ besitzt dann F^* die folgende Matrixdarstellung:

$$\left(\begin{array}{ccc|c} 0 & \cdots & 0 & \mathcal{J}^{m'}_{\mathbb{F}_{q^e}}(\boldsymbol{a'}) \\ \hline 1 & & 0 & 0 \\ & \ddots & & \vdots \\ 0 & & 1 & 0 \end{array} \right)$$

Beweis: Fasse $\bar{\mathcal{X}}$ als k-Varietät auf. Dann ist der arithmetische Frobenius f ein Automorphismus von $\bar{\mathcal{X}}$, und wir erhalten durch $1 \mapsto f$ eine Operation von $\mathbb{Z}$ auf $\bar{\mathcal{X}}$. Sei $(\zeta_1, \ldots, \zeta_n) \in A$ beliebig. Offenbar ist dann das folgende Diagramm kommutativ:

$$\begin{array}{ccc}
 & \lambda\in K \longmapsto \lambda & \\
 & X_i \longmapsto \zeta_i X_i & \\
K[X_i] & \longrightarrow & K[X_i] \\
\lambda\in K \;\; X_i \\ \downarrow \;\; \downarrow \\ \lambda^q \;\; X_i & = & X_i \;\; \lambda\in K \\ & & \downarrow \;\; \downarrow \\ & & X_i \;\; \lambda^q \\
K[X_i] & \longrightarrow & K[X_i] \\
 & X_i \longmapsto \zeta_i^q X_i & \\
 & \lambda\in K \longmapsto \lambda &
\end{array}$$

Es folgt, daß auch das folgende induzierte Diagramm kommutiert:

$$\begin{array}{ccc}
\bar{\mathcal{X}} & \xleftarrow{(\zeta_1,\ldots,\zeta_n)} & \bar{\mathcal{X}} \\
f \uparrow & = & \uparrow f \\
\bar{\mathcal{X}} & \xleftarrow[(\zeta_1^q,\ldots,\zeta_n^q)]{} & \bar{\mathcal{X}}
\end{array}$$

Lassen wir also $\mathbb{Z}$ auf A operieren via $1 \mapsto \big[(\zeta_1, \ldots, \zeta_n) \mapsto (\zeta_1^{-q}, \ldots, \zeta_n^{-q})\big]$, (wobei man beachte, daß q eine Einheit modulo m ist), so erhalten wir eine wohldefinierte Operation von $A \rtimes \mathbb{Z}$ von links auf $\bar{\mathcal{X}}$.

Sei nun $\boldsymbol{\mathcal{M}}$ die Kategorie der $\mathbb{Q}_l$-Vektorräume und $M := V_{\text{prim}}$; wir erhalten eine induzierte Operation von $A \rtimes \mathbb{Z}$ von rechts auf M (vgl. 4.7(ii)!), wobei $s := -1$ gerade als der geometrische Frobenius operiert. Die gemäß 4.1 induzierte Operation von $\mathbb{Z}$ auf $\check{A}$ wird gerade durch $1 \mapsto [\boldsymbol{a} \mapsto q\boldsymbol{a}]$ gegeben, d.h. F^* operiert via $\boldsymbol{a} \mapsto q^{-1}\boldsymbol{a}$. Auf diese Situation können wir nun 4.5 anwenden und erhalten, daß F^* den Vektorraum $V_{q^{-1}\boldsymbol{a}}$ nach $V_{\boldsymbol{a}}$ abbildet. Es folgt, daß $V_{\boldsymbol{a}}$ nach $V_{q\boldsymbol{a}}$ abgebildet wird, womit der erste Teil des Satzes gezeigt ist.

Als nächstes wollen wir zeigen, daß tatsächlich $\langle \boldsymbol{a} \rangle = \{q^i \boldsymbol{a} \,|\, i \in \{0, \ldots, e-1\}\}$ und $e = \#\langle \boldsymbol{a} \rangle$ gilt. Wir haben gerade gesehen, daß $\langle \boldsymbol{a} \rangle = \{q^i \boldsymbol{a} \,|\, i \in \mathbb{N}_0\}$ ist. Für $\tilde{e} := \#\langle \boldsymbol{a} \rangle$ haben wir $q^{\tilde{e}}\boldsymbol{a} = \boldsymbol{a}$, und man überlegt sich sofort, daß dann auch $q^{\tilde{e}} d \equiv d \pmod{m}$ sein muß, woraus $q^{\tilde{e}} \equiv 1 \pmod{m'}$ folgt. Damit erhalten wir $e | \tilde{e}$. Umgekehrt gilt für $j \in \{1, \ldots, n\}$, daß $q^e(a_j/d) \equiv (a_j/d) \pmod{m'}$ ist, woraus $q^e a_j \equiv a_j \pmod{m}$ folgt und also $\tilde{e} | e$.

Insbesondere ist jetzt klar, daß die v_i eine Basis von $V_{\langle a \rangle}$ bilden. Zum Beweis der Matrixdarstellung von F^* bleibt nun offenbar nur noch zu zeigen, daß $(F^*)^e v = \mathcal{J}^{m'}_{\mathbb{F}_{q^e}}(\boldsymbol{a'})v$ gilt.

Setze dazu $B := \mu_{m'}^n/\mu_{m'}$ und definiere den Gruppenepimorphismus $\varphi : A \twoheadrightarrow B, (\zeta_i) \mapsto (\zeta_i^d)$. Wir erhalten das folgende kommutative Diagramm von endlichen abelschen Gruppen mit exakten Zeilen:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mu_d^n/\mu_d & \longrightarrow & A & \xrightarrow{\varphi} & \mu_{m'}^n/\mu_{m'} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle -q} & & \downarrow{\scriptstyle -q} & & \downarrow{\scriptstyle -q} & & \\
0 & \longrightarrow & \mu_d^n/\mu_d & \longrightarrow & A & \xrightarrow[\varphi]{} & \mu_{m'}^n/\mu_{m'} & \longrightarrow & 0
\end{array}$$

und sehen also, daß φ ein $\mathbb{Z}$-äquivarianter Morphismus ist, so daß wir $A \rtimes \mathbb{Z} \xrightarrow{\varphi_*} B \rtimes \mathbb{Z}$ erhalten (vgl. 4.10!).

Sei $\mathcal{Y} := \mathcal{X}_n^{m'}$ und $\bar{\mathcal{Y}} := \mathcal{Y} \times_k \bar{k}$, dann operiert B auf $\bar{\mathcal{Y}}$ genauso wie A auf $\bar{\mathcal{X}}$. Außerdem lassen wir $\mathbb{Z}$ auf $\bar{\mathcal{Y}}$ auch mit dem arithmetischen Frobenius f operieren und erhalten so eine $B \rtimes \mathbb{Z}$-Operation von links auf $\bar{\mathcal{Y}}$. Betrachte den folgenden endlichen, dominanten Morphismus g, von dem man sich leicht überlegt, daß er $A \rtimes \mathbb{Z}$-äquivariant ist:

$$g : \bar{\mathcal{X}} \longrightarrow \bar{\mathcal{Y}}, \quad [x_1 : \ldots : x_n] \mapsto [x_1^d, \ldots, x_n^d].$$

Sei $\boldsymbol{\mathcal{M}}$ wieder die Kategorie der $\mathbb{Q}_l$-Vektorräume, und setze $N := V_{\text{prim}}$ und $M := V' := \mathrm{H}^{n-2}_{\text{ét}}(\bar{\mathcal{Y}}, \mathbb{Q}_l)$. Dann erfüllen M, N und g^*, zusammen mit den Operationen von $B \rtimes \mathbb{Z}$ bzw. $A \rtimes \mathbb{Z}$, die Voraussetzungen von 4.10. Beachtet man noch, daß $\varphi^*\chi = \boldsymbol{a'} \in A_n^{m'}$ gilt, so folgt, daß g^* den eindimensionalen $\mathbb{Q}_l$-Vektorraum $V'_{a'}$ nach V_a abbildet und daß $V'_{\langle a' \rangle} \xrightarrow{g^*} V_{\langle a \rangle}$ sogar $A \rtimes \mathbb{Z}$-äquivariant, insbesondere also $\mathbb{Z}$-invariant, d.h. ein Morphismus von $\mathbb{Q}_l$-G_k-Darstellungen ist.

Weil g endlich und dominant ist, ist g^* injektiv. Wegen $\#\langle \boldsymbol{a} \rangle = \#\langle \boldsymbol{a'} \rangle = e$ folgt, daß $g^*|V'_{\langle a' \rangle}$ sogar ein Isomorphismus von $\mathbb{Q}_l$-G_k-Darstellungen ist. Bezeichnen wir auch den geometrischen Frobenius auf $\bar{\mathcal{Y}}$ mit F, so genügt es also zu zeigen, daß $(F^*)^e$ auf $V'_{a'}$ Multiplikation mit $\mathcal{J}^{m'}_{\mathbb{F}_{q^e}}(\boldsymbol{a'})$ ist. Dies folgt aber aus 9.9, weil $\mathbb{F}_{q^e}$ die m'-ten Einheitswurzeln enthält! Der Satz ist also vollständig bewiesen. **q.e.d.**

9.11 Beispiel. Es sei speziell $m := n := 3$ und $q := p \geq 5$ eine Primzahl mit $p \equiv 2 \pmod 3$, d.h. $k = \mathbb{F}_p$ enthält die dritten Einheitswurzeln *nicht*.

Man sieht sofort, daß $A_3^3 = \{(1,1,1), (2,2,2)\}$, d.h. es gilt $V_{\text{prim}} = V_{\langle (1,1,1) \rangle}$. Bezeichne $\mathcal{J}$ die Jacobisumme $\mathcal{J}^3_{\mathbb{F}_{p^2}}(1,1,1)$. Dann folgt aus 9.10, daß V_{prim} eine Basis besitzt, bezüglich der der Frobenius F^* die Matrixdarstellung $\left(\begin{smallmatrix} 0 & \mathcal{J} \\ 1 & 0 \end{smallmatrix}\right)$ besitzt.

9.12 Lemma. Die Operation der Gruppe $\tilde{A}$ auf $V_{(0,\ldots,0)}$ ist trivial.

Beweis: Ist n ungerade, so gilt nach Satz 9.9, daß $V_{(0,\ldots,0)} = 0$ ist, und die Behauptung ist trivial. Sei also n gerade!

Betrachten wir zunächst den Fall $n = 2$: Wegen $\dim \mathcal{X} = 0$ ist V eine $\mathbb{Q}_l$-Algebra, d.h. es liegt ein zu $\mathbb{Q}_l$ isomorpher Unterring R in V, auf dem alle Automorphismen von $\mathcal{X}$ trivial operieren; insbesondere operieren also alle Elemente aus A trivial, d.h. $R \subseteq V_{(0,0)}$. Nun ist nach Satz 9.9 der Raum $V_{(0,0)}$ eindimensional, so daß $R = V_{(0,0)}$ folgt.

Sei nun $n \geq 4$. Bezeichne $[H]$ die Klasse des glatten Hyperebenenschnittes $\{x_n = 0\}$ in $\mathrm{CH}^1_{\mathbb{Q}}(\mathcal{X})$ und $\gamma \in \mathrm{H}^2_{\text{ét}}(\bar{\mathcal{X}}, \mathbb{Q}_l(1))$ die zugehörige Kohomologieklasse. Nach dem Starken Satz von Lefschetz induziert Multiplikation mit γ^{n-2} einen Isomorphismus $\mathrm{H}^0_{\text{ét}}(\bar{\mathcal{X}}, \mathbb{Q}_l) \xrightarrow{\sim} \mathrm{H}^{2n-4}_{\text{ét}}(\bar{\mathcal{X}}, \mathbb{Q}_l(n-2))$, so daß also insbesondere $[\gamma(-1)]^{\frac{n-2}{2}} \neq 0 \in V$ folgt. Offenbar gilt für alle Automorphismen $s \in \tilde{A}$, daß $s^*[H] = H$, so daß $\tilde{A}$ also trivial auf dem eindimensionalen Unterraum $\left\langle [\gamma(-1)]^{\frac{n-2}{2}} \right\rangle \subseteq V$ operiert. Insbesondere operiert also A trivial, so daß mit Satz 9.9 folgt, daß dieser Unterraum schon gleich $V_{(0,\ldots,0)}$ ist. Die Aussage des Lemmas folgt. **q.e.d.**

Wir wollen untersuchen, wie $\tilde{A}$ auf V operiert. Da wir die Operation von $\mu_m^n/\mu_m \trianglelefteq \tilde{A}$ auf V_{prim} schon im vierten Kapitel bestimmt haben, müssen wir jetzt „nur“ noch verstehen, wie S_n auf V operiert.

9.13 Lemma. Sei $\tau \in S_n$ eine Transposition und $\boldsymbol{a} \in A_n^m$ beliebig mit ${}^\tau\boldsymbol{a} \neq \boldsymbol{a}$. Dann gilt ${}^\tau({}^\tau\boldsymbol{a}) = \boldsymbol{a}$, und wegen Korollar 4.5 induziert τ deshalb eine $\mathbb{Q}_l$-lineare Involution τ^* von $V_{\boldsymbol{a}} \oplus V_{{}^\tau\boldsymbol{a}}$. Diese hat Spur null.

Beweis: Nach Satz 9.9 sind $V_{\boldsymbol{a}}$ und $V_{{}^\tau\boldsymbol{a}}$ eindimensionale $\mathbb{Q}_l$-Vektorräume. Sei $v \in V_{\boldsymbol{a}} \setminus \{0\}$ beliebig. Wegen $\tau^*\tau^* = 1$ muß $\tau^*(v) \neq 0 \in V_{{}^\tau\boldsymbol{a}}$ gelten. Also ist $\{v, \tau^*(v)\}$ eine Basis von $V_{\boldsymbol{a}} \oplus V_{{}^\tau\boldsymbol{a}}$. Die Matrix von τ^* bezüglich dieser Basis ist aber (wegen Korollar 4.5) offenbar

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

hat also tatsächlich Spur null. **q.e.d.**

Der Beweis der folgenden Aussage, die das Schlüsselergebnis zur Berechnung der Operation von S_n auf V ist, erweist sich als erstaunlich schwierig und ist das eigentliche Herzstück der vorliegenden Arbeit.

9.14 Satz. Sei $\tau \in S_n$ eine Transposition und $\boldsymbol{a} \in A_n^m$ beliebig mit ${}^\tau\boldsymbol{a} = \boldsymbol{a}$. Wegen Korollar 4.5 induziert τ deshalb eine $\mathbb{Q}_l$-lineare Involution von $V_{\boldsymbol{a}}$. Diese ist gerade Multiplikation mit (-1).

Beweis: Ohne Beschränkung der Allgemeinheit dürfen wir offenbar $\tau = [12]$ annehmen, daß heißt es gilt $a_1 = a_2$. Wir zeigen die Behauptung der Reihe nach für die drei Fälle $n = 2$, $n = 3$ und $n \geq 4$:

- $\underline{n = 2}$*:* Ist m ungerade, so ist A_2^m leer und demnach nichts zu zeigen. Sei also m gerade! Dann muß $\boldsymbol{a} = (\frac{m}{2}, \frac{m}{2})$ gelten. Der Automorphismus τ operiert fixpunktfrei auf $\bar{\mathcal{X}}$, denn $[0:1], [0:1] \notin \bar{\mathcal{X}}(K)$, und wäre $[1:y]$ Fixpunkt mit $y \in K^\times$, also $[1:y] = [y:1]$, so folgte $y^2 = 1$ und damit

  $$1^m + y^m = 1 + (y^2)^{\frac{m}{2}} = 2 \overset{p>m\geq 3}{\neq} 0$$

  im Widerspruch zu $[1:y] \in \bar{\mathcal{X}}(K)$.

  Es gilt

  $$V = V_{(0,0)} \oplus V_{(\frac{m}{2},\frac{m}{2})} \oplus \underbrace{\bigoplus_{0<j<\frac{m}{2}} \left(V_{(j,m-j)} \oplus V_{(m-j,j)}\right)}_{=:V'}.$$

  Nach Lemma 9.12 ist τ^* auf $V_{(0,0)}$ die Identität, hat also dort Spur eins. Aus Lemma 9.13 wissen wir, daß die Spur von τ^* auf V' null ist. Die Lefschetzsche Spurformel ergibt also:

  $$0 = \operatorname{Tr}(\tau^*) = 1 + \operatorname{Tr}(\tau^*|V_{(\frac{m}{2},\frac{m}{2})}) + 0 \implies \operatorname{Tr}(\tau^*|V_{(\frac{m}{2},\frac{m}{2})}) = -1.$$

  Weil $V_{(\frac{m}{2},\frac{m}{2})}$ eindimensional ist, folgt die Behauptung.

- $\underline{n=3}$*:* Wieder berechnen wir zunächst die Zahl der Fixpunkte von τ, d.h. das Schnittprodukt $(\Delta_{\bar{\mathcal{X}}}, \Gamma_\tau)$; sei $[x:y:z] \in \bar{\mathcal{X}}(K)$ ein solcher Fixpunkt, d.h. gelte $[x:y:z] = [y:x:z]$. Wir können annehmen, daß $x \in \{0,1\}$ gilt.

  - $\underline{\text{1. Fall: } x=0}$
    Dann folgt $y = 0$, also $z \neq 0$ und damit $x^m + y^m + z^m = 0 + 0 + z^m \neq 0$. Widerspruch!
  - $\underline{\text{2. Fall: } x=1,\ y=1}$
    Dann folgt $1^m + 1^m + z^m = 0$, also $z^m = -2 \neq 0$ (wegen $p > 2$). Es gibt also m verschiedene Fixpunkte dieser Gestalt.
  - $\underline{\text{3. Fall: } x=1,\ y \notin \{0,1\}}$

    $$[1:y:z] = [y:1:z] \implies zy = z \overset{y\neq 1}{\implies} z = 0,\ y = -1 \overset{p>2}{\neq} 1.$$

    Wir erhalten also $[x:y:z] = [1:-1:0]$. Ist m gerade, so gilt

    $$1^m + (-1)^m + 0^m = 2 \neq 0 \ \text{— Widerspruch!}$$

    Ist m hingegen ungerade, so liegt $[1:-1:0]$ tatsächlich in $\bar{\mathcal{X}}(K)$, ist also wirklich ein Fixpunkt.

  Der Automorphismus τ hat also m Fixpunkte, wenn m gerade ist, und $(m+1)$ Fixpunkte, wenn m ungerade ist. Nach der Lefschetzschen Spurformel gilt:

  $$(\Delta_{\bar{\mathcal{X}}}, \Gamma_\tau) = \underbrace{\operatorname{Tr}\left(\tau^* | \mathrm{H}^0_{\text{ét}}(\bar{\mathcal{X}}, \mathbb{Q}_l)\right)}_{=:t_0} - \underbrace{\operatorname{Tr}\left(\tau^* | \mathrm{H}^1_{\text{ét}}(\bar{\mathcal{X}}, \mathbb{Q}_l)\right)}_{=:t_1} + \underbrace{\operatorname{Tr}\left(\tau^* | \mathrm{H}^2_{\text{ét}}(\bar{\mathcal{X}}, \mathbb{Q}_l)\right)}_{=:t_2}. \tag{36}$$

  Bezeichne wieder R den zu $\mathbb{Q}_l$ isomorphen Unterring von $\mathrm{H}^*_{\text{ét}}(\bar{\mathcal{X}}, \mathbb{Q}_l)$, der diesem Kohomologiering die Struktur einer $\mathbb{Q}_l$-Algebra verleiht. Weil $\bar{\mathcal{X}}$ irreduzibel ist, gilt $R = \mathrm{H}^0_{\text{ét}}(\bar{\mathcal{X}}, \mathbb{Q}_l)$. Also ist τ^* auf $\mathrm{H}^0_{\text{ét}}(\bar{\mathcal{X}}, \mathbb{Q}_l)$ die Identität, d.h. $t_0 = 1$. Mittels Poincaré-Dualität folgt dann, daß τ^* auch auf $\mathrm{H}^2_{\text{ét}}(\bar{\mathcal{X}}, \mathbb{Q}_l)$ die Identität ist, d.h. es gilt auch $t_2 = 1$. Damit folgt aus Gleichung (36):

  $$t_1 = 2 - (\Delta_{\bar{\mathcal{X}}}, \Gamma_\tau). \tag{37}$$

  Als nächstes fragen wir uns, für wie viele Elemente $\boldsymbol{a}$ aus A_3^m die Bedingung $a_1 = a_2$ erfüllt ist; diese Anzahl wollen wir mit N bezeichnen:

  - $\underline{\text{1. Fall: } m \text{ ungerade}}$
    Dann gilt $a_1 + a_2 = 2a_1 \not\equiv 0 \pmod m$ für alle $a_1 \in \mathbb{Z}/m\mathbb{Z} \setminus \{0\}$, so daß es also $N = (m-1)$ Möglichkeiten gibt.
  - $\underline{\text{2. Fall: } m \text{ gerade}}$
    In diesem Fall muß $a_1 \not\equiv \frac{m}{2} \pmod m$ gelten, weil sonst $a_3 \equiv 0 \pmod m$ wäre. Hier gibt es also nur $N = (m-2)$ Möglichkeiten.

  Es gilt

  $$\begin{aligned} t_1 &= \operatorname{Tr}(V) \overset{9.9}{=} \operatorname{Tr}\Big(\tau^* \Big| \bigoplus_{a \in A_n^m} V_{\boldsymbol{a}}\Big) \\ &= \sum_{(a_1,a_1,a_3) \in A_n^m} \underbrace{\operatorname{Tr}\left(\tau^* | V_{(a_1,a_1,a_3)}\right)}_{\in \{-1,1\}} \\ &+ \frac{1}{2} \sum_{\substack{(a_1,a_2,a_3) \in A_n^m \\ a_1 \neq a_2}} \underbrace{\operatorname{Tr}\left(\tau^* | V_{(a_1,a_2,a_3)} \oplus V_{(a_2,a_1,a_3)}\right)}_{\overset{9.13}{=} 0}. \end{aligned}$$

Es folgt $t_1 \in [-N, N]$, und $t_1 = -N$ genau dann, wenn die Behauptung des Lemmas für alle $\boldsymbol{a} \in A_n^m$ mit $a_1 = a_2$ gilt.

– 1. Fall: m ungerade

$$t_1 \overset{(37)}{=} 2 - (\Delta_{\bar{\mathcal{X}}}, \Gamma_\tau) = 2 - (m+1) = 1 - m = -N.$$

– 2. Fall: m gerade

$$t_1 \overset{(37)}{=} 2 - (\Delta_{\bar{\mathcal{X}}}, \Gamma_\tau) = 2 - m = -N.$$

Damit ist das Lemma auch für den Fall $n = 3$ bewiesen.

- $n \geq 4$: Sei also jetzt $n \geq 4$, dann ist $\mathcal{X}$ mindestens zweidimensional. Seien r und s natürliche Zahlen mit $r, s \geq 3$ und $r + s = n + 2$. Dann haben wir nach [Shi79, S.179] das folgende kommutative Diagramm:

$$\begin{array}{ccccccc}
\beta^{-1}(Y) & \xhookrightarrow{j'} & Z_{r,s}^m & \xrightarrow{\pi} & Z_{r,s}^m/\mu_m & & \\
\downarrow{\scriptstyle \beta'} & \square & \downarrow{\scriptstyle \beta} & \searrow^{\psi} & \downarrow{\scriptstyle \bar{\psi}} & & \\
Y := \mathcal{X}_{r-1,K}^m \times \mathcal{X}_{s-1,K}^m & \xhookrightarrow[j]{} & \mathcal{X}_{r,K}^m \times \mathcal{X}_{s,K}^m & \overset{\varphi}{\dashrightarrow} & \bar{\mathcal{X}} & \xhookleftarrow[i]{} & \mathcal{X}_{r-1,K}^m \coprod \mathcal{X}_{s-1,K}^m
\end{array}$$

Dabei sind die verschiedenen Abbildungen wie folgt definiert:

$$\begin{array}{lcl}
\varphi & : & \text{rationale Abbildung, definiert durch} \\
 & & ([x_1 : \ldots : x_r], [y_1 : \ldots : y_s]) \mapsto \\
 & & \qquad [x_1 y_s : \ldots : x_{r-1} y_s : \varepsilon x_r y_1 : \ldots : \varepsilon x_r y_{s-1}] \text{ (mit } \varepsilon^m = -1), \\
j & : & ([x_1 : \ldots : x_{r-1}], [y_1 : \ldots : y_{s-1}]) \mapsto ([x_1 : \ldots : x_{r-1}, 0], [y_1 : \ldots : y_{s-1}, 0]), \\
i & = & i_1 \coprod i_2 : \begin{cases} i_1([x_1 : \ldots : x_{r-1}]) = [x_1 : \ldots : x_{r-1} : 0 : \ldots : 0] \\ i_2([y_1 : \ldots : y_{s-1}]) = [0 : \ldots : 0 : y_1 : \ldots : y_{s-1}] \end{cases}, \\
\beta & : & \text{Aufblasung von } \mathcal{X}_{r,K}^m \times \mathcal{X}_{s,K}^m \text{ entlang } Y, \\
\beta' & : & \text{Einschränkung von } \beta \text{ auf } \beta^{-1}(Y), \\
j' & : & \text{Einbettung}, \\
\pi & : & \text{Quotientenmorphismus}, \\
\bar{\psi} & : & \text{Aufblasung von } \bar{\mathcal{X}} \text{ entlang } \mathcal{X}_{r-1,K}^m \coprod \mathcal{X}_{s-1,K}^m, \\
\psi & = & \varphi \circ \beta = \bar{\psi} \circ \pi.
\end{array}$$

Shioda zeigt, daß man mit Hilfe dieses Diagramms einen Isomorphismus

$$\left[V_{r,\text{prim}}^m \otimes V_{s,\text{prim}}^m\right]^{\mu_m} \oplus \left[V_{r-1,\text{prim}}^m \otimes V_{s-1,\text{prim}}^m\right](-1) \xrightarrow[\sim]{\psi_*(\beta^* \oplus j'_* \beta'^*)} V_{\text{prim}} \quad (38)$$

von $\mathbb{Q}_l$-G-Darstellungen erhält, der außerdem A-äquivariant ist. Dabei ist die Operation von A auf der linken Seite wie folgt erklärt: Zunächst operiert $(\mu_m^r/\mu_m) \times (\mu_m^s/\mu_m)$ offenbar auf $\left[V_{r,\text{prim}}^m \otimes V_{s,\text{prim}}^m\right]$. Mit Hilfe der folgenden kurzen exakten Sequenz erhält man die Operation auf dem ersten Summanden:

$$\begin{array}{ccccccccc}
0 & \to & \mu_m & \to & (\mu_m^r/\mu_m) \times (\mu_m^s/\mu_m) & \to & A & \to & 0 \\
 & & \zeta & \mapsto & ([\zeta,\ldots,\zeta,1],[\zeta,\ldots,\zeta,1]) & & & & \\
 & & & & ([\zeta_1,\ldots,\zeta_{r-1},1],[\xi_1,\ldots,\xi_{s-1},1]) & \mapsto & [\zeta_1,\ldots,\zeta_{r-1},\xi_1,\ldots,\xi_{s-1}] & &
\end{array}$$

Die Operation auf dem zweiten Summanden erhält man mit Hilfe des Gruppenhomomorphismusses

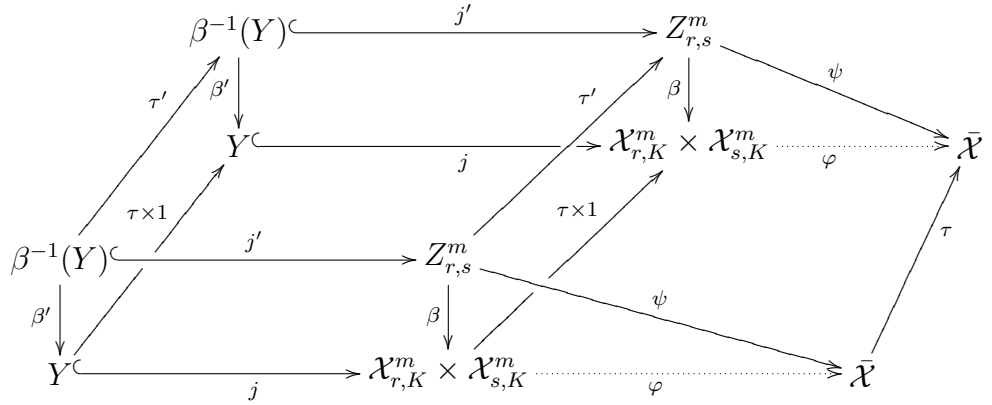
$$\begin{array}{ccc} A & \longrightarrow & (\mu_m^{r-1}/\mu_m) \times (\mu_m^{s-1}/\mu_m) \\ {\scriptstyle [\zeta_1,\ldots,\zeta_n]} & \mapsto & {\scriptstyle ([\zeta_1,\ldots,\zeta_{r-1}],[\zeta_r,\ldots,\zeta_n])} \end{array}$$

und der offensichtlichen Operation von $(\mu_m^{r-1}/\mu_m) \times (\mu_m^{s-1}/\mu_m)$ auf dem zweiten Summanden.

Seien nun $(\boldsymbol{b}, \boldsymbol{c}) \in A_{r,s}^m$ und $(\boldsymbol{b'}, \boldsymbol{c'}) \in A_{r-1}^m \times A_{s-1}^m$ beliebig. Gleichung (38) induziert Isomorphismen (vgl. [Shi79] und [Shi82]!)

$$V_{\boldsymbol{b}} \otimes V_{\boldsymbol{c}} \xrightarrow[\sim]{\psi_*\beta^*} V_{\boldsymbol{b} \sharp \boldsymbol{c}} \qquad \text{und} \qquad V_{\boldsymbol{b'}} \otimes V_{\boldsymbol{c'}}(-1) \xrightarrow[\sim]{\psi_* {j'}_* {\beta'}^*} V_{\boldsymbol{b'} * \boldsymbol{c'}}.$$

Wähle nun speziell $r = 3$ und $s = n + 2 - r$, und man betrachte das folgende Diagramm:



Der Morphismus $\tau \times 1$ bildet Y isomorph auf Y ab, wodurch ein eindeutiges τ' auf der Aufblasung induziert wird, daß mit $\tau \times 1$ kommutiert. Außerdem rechnet man sofort nach, daß $(\tau \times 1) \circ j = j \circ (\tau \times 1)$ und $\tau \circ \varphi = \varphi \circ (\tau \times 1)$ gilt, so daß das Diagramm also kommutiert.

Wegen

$$\tau^* \psi_* \beta^* = (\tau_* \psi_*) \beta^* = (\psi_* {\tau'}_*) \beta^* = \psi_* (\tau'^* \beta^*) = \psi_* \beta^* (\tau \times 1)^*$$

und

$$\tau^* \psi_* {j'}_* {\beta'}^* = (\tau_* \psi_* {j'}_*) {\beta'}^* = (\psi_* {j'}_* {\tau'}_*) {\beta'}^* = \psi_* {j'}_* (\tau'^* {\beta'}^*) = \psi_* {j'}_* {\beta'}^* (\tau \times 1)^*$$

(wobei man beachte, daß für Involutionen $\tilde{\tau}$ bekanntlich $\tilde{\tau}_* = \tilde{\tau}^*$ gilt) folgt, daß auch die folgenden Diagramme kommutieren, wenn $\boldsymbol{b}$ bzw. $\boldsymbol{b'}$ fix unter der Transposition τ sind:

$$\begin{array}{ccc} V_{\boldsymbol{b}} \otimes V_{\boldsymbol{c}} & \xrightarrow[\sim]{\psi_*\beta^*} & V_{\boldsymbol{b} \sharp \boldsymbol{c}} \\ {\scriptstyle (\tau\times 1)^*}\downarrow\wr & & \wr\downarrow{\scriptstyle \tau^*} \\ V_{\boldsymbol{b}} \otimes V_{\boldsymbol{c}} & \xrightarrow[\sim]{\psi_*\beta^*} & V_{\boldsymbol{b} \sharp \boldsymbol{c}} \end{array} \qquad \begin{array}{ccc} V_{\boldsymbol{b'}} \otimes V_{\boldsymbol{c'}}(-1) & \xrightarrow[\sim]{\psi_* {j'}_* {\beta'}^*} & V_{\boldsymbol{b'} * \boldsymbol{c'}} \\ {\scriptstyle (\tau\times 1)^*}\downarrow\wr & & \wr\downarrow{\scriptstyle \tau^*} \\ V_{\boldsymbol{b'}} \otimes V_{\boldsymbol{c'}}(-1) & \xrightarrow[\sim]{\psi_* {j'}_* {\beta'}^*} & V_{\boldsymbol{b'} * \boldsymbol{c'}} \end{array}$$

Wegen 9.6 ist $\boldsymbol{a}$ entweder von der Form $\boldsymbol{b} \sharp \boldsymbol{c}$ oder von der Form $\boldsymbol{b'} * \boldsymbol{c'}$, wobei nach Voraussetzung $b_1 = b_2$ bzw. $b'_1 = b'_2$ gilt. Da wir die Fälle „$n = 2$“ und „$n = 3$“ schon behandelt haben, ist dann aber $(\tau \times 1)^*$ Multiplikation mit (-1), und die Behauptung folgt aus der Kommutativität des entsprechenden Diagrammes.

Damit gilt die Behauptung also für alle $n \geq 2$, und das Lemma ist bewiesen. **q.e.d.**

Jetzt verfügen wir über alle Informationen, die wir benötigen, um die Existenz einer Basis $\{v_b\}$ von V_{prim} (mit $v_b \in V_{\boldsymbol{b}}$) zu beweisen, bezüglich der wir die Operation von S_n explizit angeben können.

9.15 Korollar. Sei $\boldsymbol{a} \in A_n^m$ beliebig. Dann gibt es $v_b \in V_{\boldsymbol{b}} \setminus \{0\}$ für alle $\boldsymbol{b} \in [\boldsymbol{a}]$ derart, daß

$$\forall \sigma \in S_n \; \forall \boldsymbol{b} \in [\boldsymbol{a}] : \; \sigma^*(v_b) = \operatorname{sgn}(\sigma) \cdot v_{\sigma^{-1}b}.$$

Beweis: Wähle zunächst $v \in V_{\boldsymbol{a}} \setminus \{0\}$ beliebig. Für $\boldsymbol{b} \in [\boldsymbol{a}]$ wähle $\sigma \in S_n$ mit $\sigma^{-1}(\boldsymbol{a}) = \boldsymbol{b}$. Setze $v_b := \operatorname{sgn}(\sigma) \cdot \sigma^* v$. Da σ^* Automorphismus von $V_{[\boldsymbol{a}]}$ ist mit $\sigma^*(V_{\boldsymbol{a}}) = V_{\boldsymbol{b}}$ (nach 4.5 und 4.6), gilt offenbar $v_b \in V_{\boldsymbol{b}} \setminus \{0\}$.

Wir zeigen zunächst, daß v_b nicht von der Wahl von σ abhängt. Sei $\tilde{\sigma} \in S_n$ eine weitere Permutation mit $\tilde{\sigma}^{-1}(\boldsymbol{a}) = \boldsymbol{b}$. Es folgt, daß $\boldsymbol{b}$ fix unter $\omega := \sigma^{-1}\tilde{\sigma}$ ist. Nach eventueller Umnumerierung der Koordinaten läßt sich ω wie folgt in elementfremde Zykel zerlegen:

$$\omega = [1, \ldots, k_1] \cdot [k_1 + 1, \ldots, k_2] \cdot \ldots \cdot [k_{s-1} + 1, \ldots, n].$$

Es folgt:

$$b_1 = b_2 = \ldots = b_{k_1}, \; b_{k_1+1} = \ldots = b_{k_2}, \; b_{k_{s-1}+1} = \ldots = b_n.$$

Schreibt man nun jeden dieser Zykel als Produkt von Transpositionen, die nur Elemente vertauschen, die auch der entsprechende Zykel vertauscht, so halten diese Transpositionen $\boldsymbol{b}$ offenbar auch fest. Also läßt sich ω als Produkt von Transpositionen schreiben, die $\boldsymbol{b}$ festhalten. Es folgt aus Lemma 9.14, daß ω^* in $V_{\boldsymbol{b}}$ Multiplikation mit $\operatorname{sgn}(\omega)$ ist. Damit ergibt sich:

$$\begin{aligned} \operatorname{sgn}(\tilde{\sigma}) \cdot \tilde{\sigma}^* v = \operatorname{sgn}(\sigma\omega) \cdot (\sigma\omega)^* v = \operatorname{sgn}(\sigma\omega) \cdot \omega^*\sigma^* v \\ = \operatorname{sgn}(\sigma\omega) \cdot \operatorname{sgn}(\omega) \cdot \sigma^* v = \operatorname{sgn}(\sigma) \cdot \sigma^* v = v_b. \end{aligned}$$

Damit haben wir gezeigt, daß v_b tatsächlich unabhängig von der Wahl von σ ist. Wir zeigen nun, daß die so definierten v_b die gewünschte Eigenschaft haben. Seien dazu $\sigma \in S_n$ und $\boldsymbol{b} \in [\boldsymbol{a}]$ beliebig. Wähle ein $\omega \in S_n$ mit $\omega^{-1}(\boldsymbol{a}) = \boldsymbol{b}$. Nach obiger Überlegung gilt:

$$\begin{aligned} v_b &= \operatorname{sgn}(\omega) \cdot \omega^* v, \\ v_{\sigma^{-1}b} &= v_{(\omega\sigma)^{-1}a} = \operatorname{sgn}(\omega\sigma) \cdot (\omega\sigma)^* v. \end{aligned}$$

Es folgt also:

$$\begin{aligned} \sigma^* v_b &= \sigma^*(\operatorname{sgn}(\omega) \cdot \omega^* v) = \operatorname{sgn}(\omega) \cdot \sigma^*\omega^* v \\ &= \operatorname{sgn}(\omega) \cdot \underbrace{\operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\sigma)}_{=1} \cdot (\omega\sigma)^* v = \operatorname{sgn}(\sigma) \cdot \underbrace{\operatorname{sgn}(\omega\sigma) \cdot (\omega\sigma)^* v}_{=v_{\sigma^{-1}b}} = \operatorname{sgn}(\sigma) \cdot v_{\sigma^{-1}b}. \end{aligned}$$

q.e.d.

9.16 Korollar. Es sei $\boldsymbol{a} \in A_n^m$ beliebig und $(S_n)\boldsymbol{a} \leq S_n$ die Standgruppe von $\boldsymbol{a}$ unter der Operation von S_n auf A_n^m. Ferner bezeichne $\mathbf{sgn} : (S_n)\boldsymbol{a} \longrightarrow \mathbb{Q}_l^\times = \mathrm{Aut}\,(V_{\boldsymbol{a}})$ den Charakter, der durch das *Signum* einer Permutation gegeben wird. Dann wird die Operation von S_n auf $V_{[\boldsymbol{a}]}$ durch **sgn** induziert, d.h. es gilt:

$$\boxed{\left[\begin{array}{ccc} S_n & \longrightarrow & \mathrm{Aut}\,(V_{[\boldsymbol{a}]}) \\ \sigma & \mapsto & \sigma^* \end{array}\right] \quad \cong \quad \mathrm{ind}_{(S_n)_a}^{S_n}\,[\mathbf{sgn}]}. \tag{39}$$

Insbesondere folgt für beliebiges $\sigma \in S_n$:

$$\mathrm{Tr}\,\left(\sigma^* \,|\, V_{[\boldsymbol{a}]}\right) = \mathrm{sgn}\,(\sigma) \cdot \frac{\#\{\tau \in S_n \,|\, \tau\sigma\tau^{-1} \in (S_n)\boldsymbol{a}\}}{\#(S_n)\boldsymbol{a}} = \mathrm{sgn}\,(\sigma) \cdot \#\{\boldsymbol{b} \in [\boldsymbol{a}] \,|\, \sigma \in (S_n)_{\boldsymbol{b}}\}.$$

Beweis: Die erste Aussage ist klar nach 9.15 und der Definition der induzierten Darstellung.

Die Formel für die Spur folgt dann aus folgender allgemeinen Formel für den Charakter einer induzierten Darstellung: Sei G eine endliche Gruppe, $S \leq G$ eine Untergruppe, g ein Charakter auf S und g^G der induzierte Charakter auf G. Dann gilt (vgl. [Lan93, XVIII,§6,S.686]!)

$$g^G(\sigma) = \frac{1}{\#S} \sum_{\tau \in G} g(\tau\sigma\tau^{-1}) \qquad (\text{mit } g(\tau) := 0 \text{ für } \tau \notin S).$$

Wegen $\mathrm{sgn}\,(\tau\sigma\tau^{-1}) = \mathrm{sgn}\,(\sigma)$ folgt daraus die erste Gleichung. Die zweite Gleichung folgt hieraus aus der Bahngleichung für die Operation von S_n auf $[\boldsymbol{a}]$ oder auch direkt aus 9.15. **q.e.d.**

9.17 Korollar. Sei $s := (\zeta_1, \ldots, \zeta_n) \cdot \sigma \in \tilde{A}$ beliebig und $\boldsymbol{a} \in \check{A}$ beliebig. Ist $\boldsymbol{a} = (0, \ldots, 0)$, so operiert s trivial auf $V_{[\boldsymbol{a}]} = V_{(0,\ldots,0)}$. Ist $\boldsymbol{a} \in A_n^m$ und $\{v_b\}_{b \in [a]}$ eine Basis von $V_{[\boldsymbol{a}]}$ wie in Korollar 9.15, so gilt für $\boldsymbol{b} \in [\boldsymbol{a}]$:

$$\boxed{s^* v_b = (\zeta_1^{b_{\sigma(1)}} \cdot \ldots \cdot \zeta_n^{b_{\sigma(n)}}) \cdot \mathrm{sgn}\,(\sigma) \cdot v_{\sigma^{-1}b}}.$$

Insbesondere liegt $s^*|V_{[\boldsymbol{a}]}$ also in der Untergruppe

$$(\pm\mu_m)^{\sharp[a]} \rtimes S([\boldsymbol{a}]) \hookrightarrow \mathrm{Aut}_{\mathbb{Q}_l - G_k}\,(V_{[\boldsymbol{a}]}),$$

wobei $(\pm\mu_m)$ die Gruppe $\{\pm\xi \,|\, \xi^m = 1\}$ und $S([\boldsymbol{a}])$ die Gruppe der Permutationen der Menge $[\boldsymbol{a}]$ bezeichne.

Beweis: Klar nach 9.1, 9.12 und 9.15! **q.e.d.**

9.18 Beispiel. Es sei speziell $m = 3$, $n = 6$, $s = (\zeta, 1, 1, 1, \zeta^2, 1) \cdot [1234][56]$ und $\boldsymbol{a} = [1, 1, 1, 2, 2, 2]$. Dann ist

$$\begin{aligned}[\boldsymbol{a}] \;=\; \{\; & \underbrace{[1,1,1,2,2,2]}_{=a=:b_1}, \underbrace{[1,1,2,1,2,2]}_{=:b_2}, \underbrace{[1,1,2,2,1,2]}_{=:b_3}, \underbrace{[1,1,2,2,2,1]}_{=:b_4}, \underbrace{[1,2,1,1,2,2]}_{=:b_5}, \\ & \underbrace{[1,2,1,2,1,2]}_{=:b_6}, \underbrace{[1,2,1,2,2,1]}_{=:b_7}, \underbrace{[1,2,2,1,1,2]}_{=:b_8}, \underbrace{[1,2,2,1,2,1]}_{=:b_9}, \underbrace{[1,2,2,2,1,1]}_{=:b_{10}}, \\ & \underbrace{[2,1,1,1,2,2]}_{=:b_{11}}, \underbrace{[2,1,1,2,1,2]}_{=:b_{12}}, \underbrace{[2,1,1,2,2,1]}_{=:b_{13}}, \underbrace{[2,1,2,1,1,2]}_{=:b_{14}}, \underbrace{[2,1,2,1,2,1]}_{=:b_{15}}, \\ & \underbrace{[2,1,2,2,1,1]}_{=:b_{16}}, \underbrace{[2,2,1,1,1,2]}_{=:b_{17}}, \underbrace{[2,2,1,1,2,1]}_{=:b_{18}}, \underbrace{[2,2,1,2,1,1]}_{=:b_{19}}, \underbrace{[2,2,2,1,1,1]}_{=:b_{20}} \;\}. \end{aligned}$$

Sei $\{v_1, \ldots, v_{20}\}$ eine Basis von $V_{[\boldsymbol{a}]}$ wie in 9.15 mit $v_i \in V_{b_i}$. Bezüglich dieser Basis hat $s^*|V_{[\boldsymbol{a}]}$ dann die folgende Matrixdarstellung:

$$\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \zeta^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\zeta^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \zeta^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \zeta^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \zeta^2 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & \zeta^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \zeta & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \zeta & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \zeta & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \zeta & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \zeta \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \zeta & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}$$

und ist als Element von $(\pm\mu_m)^{\sharp[a]} \rtimes S([\boldsymbol{a}])$ gleich

$$\begin{aligned}&(\zeta^2, \zeta^2, 1, \zeta^2, \zeta^2, 1, \zeta^2, 1, \zeta^2, 1, 1, \zeta, 1, \zeta, 1, \zeta, \zeta, 1, \zeta, \zeta) \\ &\qquad\qquad \cdot [1, 2, 5, 11][3, 9, 17, 13][4, 8, 18, 12][6, 15][7, 14][10, 20, 19, 16].\end{aligned}$$

Dabei beachte man, daß $\operatorname{sgn}(\underbrace{[1234][56]}_{=[14]\circ[13]\circ[12]\circ[56]}) = 1$ gilt!

9.19 Bemerkung. Enthält k die m-ten Einheitswurzeln, so können wir mit Hilfe von (16), 9.9 und 9.17 die Frobeniusoperation auf der Kohomologie einer beliebigen getwisteten Fermathyperfläche über k explizit berechnen.

Enthält k die m-ten Einheitswurzeln *nicht*, so können wir mittels 9.10 dasselbe erreichen,

wenn es keine $\boldsymbol{a} \in A_n^m$, $\sigma \in S_n \backslash \{\mathrm{id}\}$ und $t \in (Z/mZ)^\times \backslash \{1\}$ mit $t\boldsymbol{a} = {}^\sigma\boldsymbol{a}$ gibt, denn offenbar können wir genau dann die Basen auf V_{prim} aus 9.10 und 9.15 unabhängig voneinander wählen. Ein solcher „gutartiger“ Fall liegt zum Beispiel für $m = n = 3$ vor, denn es ist $A_3^3 = \{(1,1,1),(2,2,2)\}$, und S_3 operiert trivial auf A_3^3, während $(\mathbb{Z}/3\mathbb{Z})^\times$ die beiden Charaktere vertauscht.

„Bösartig“ sind zum Beispiel die Fälle $m = 3$, $n = 2$ und $m = 3$, $n = 4$, und diese werden wir im letzten Kapitel exemplarisch untersuchen.

10 Berechnung der Zetafunktion

In diesem Kapitel definieren wir zunächst die *Zetafunktion* eines Objektes aus $\mathcal{F}_k^{n,r}$ (für einen endlichen Körper k) und leiten dann eine explizite Formel her, mit der sie sich unter der Voraussetzung, daß k die r-ten Einheitswurzeln enthält, mittels der Ergebnisse des neunten Kapitels berechnen läßt.

10.1 Definition. Es seien $n \geq 2$ und $r \geq 1$ natürliche Zahlen, $k = \mathbb{F}_q$ ein endlicher Körper der Charakteristik p und P ein beliebiges Objekt aus $\mathcal{F}_k^{n,r}$ mit assoziierter Varietät $X := F_k P$ (vgl. 1.6(iv) und 3.11(i)!). Die *Zetafunktion von* P werde definiert als die Zetafunktion von X, d.h. (vgl. [Mil80, S.286]!):

$$\zeta(P,t) := \zeta(X,t) := \exp\left(\sum_{i=1}^{\infty} \frac{\nu_X^{(i)}}{i} t^i\right) \in \mathbb{Q}[[t]],$$

wobei $\nu_X^{(i)}$ die Anzahl der $\mathbb{F}_{q^i}$-rationalen Punkte von X bezeichne. Nach den (von Dwork und Deligne bewiesenen) Weil-Vermutungen gilt, daß $\zeta(P,t)$ sogar schon in $\mathbb{Q}(t)$ liegt.

Mit Hilfe der Lefschetzschen Spurformel kann man die Zetafunktion leicht berechnen, wenn man die Frobeniusoperation auf der l-adischen Kohomologie von X kennt:

10.2 Satz. Die Bezeichnungen seien wie in 10.1, und es gelte, daß X *regulär* ist (was also zum Beispiel erfüllt ist, wenn P eine Form von P_n^m für ein $m < p$ ist). Dann gilt

$$\zeta(P,t) = Q(P,t)^{\left[(-1)^{n+1}\right]} \prod_{i \in \{0,\ldots,n-2\} \setminus \{\frac{n-2}{2}\}} \frac{1}{1-q^i t},$$

wobei $Q(P,t)$ ein normiertes Polynom mit ganzzahligen Koeffizienten ist, das sich in $\bar{\mathbb{Q}}[t]$ zerlegen läßt als $Q(P,t) = \prod(1 - a_j t)$ mit ganzen algebraischen Zahlen a_j, die unter jeder komplexen Einbettung den Betrag $q^{(n-2)/2}$ haben. Ist $l \neq p$ eine Primzahl, $K = \bar{k}$ ein (separabler) algebraischer Abschluß von k, $\bar{X} := X \times_k \bar{k}$ und $F : \bar{X} \to \bar{X}$ der geometrische Frobenius, so gilt

$$Q(P,t) = \det\left(1 - F^* t \,|\, \mathrm{H}_{\text{ét}}^{n-2}(\bar{X}, \mathbb{Q}_l)\right)$$

und

$$\forall i \in \mathbb{N}_+ \,:\, \nu_X^{(i)} = \left(\sum_{j \in \{0,\ldots,n-2\} \setminus \{\frac{n-2}{2}\}} q^j\right) + (-1)^n \cdot \mathrm{Tr}\left((F^*)^i \,\middle|\, \mathrm{H}_{\text{ét}}^{n-2}(\bar{X}, \mathbb{Q}_l)\right). \qquad (40)$$

Beweis: Siehe [Del73] und [Mil80, Lemma 2.7.,S.186]! **q.e.d.**

10.3 Lemma/ Definition. Es seien $r, s \in \mathbb{N}_+$ natürliche Zahlen. Definiere die Mengen

$$\Pi_r^s := \{(n_1, \ldots, n_s) \in \mathbb{N}_0^s | \sum_{i=1}^s n_i = r\} \text{ und}$$
$$B_r^s := \{1, \ldots, s\}^r.$$

Die symmetrische Gruppe S_r operiert auf B_r^s durch Permutation der Einträge. Ist $\pi = (n_i) \in \Pi_r^s$ beliebig, so definiere

$$B_r^s(\pi) := S_r \cdot (\underbrace{1, \ldots, 1}_{n_1}, \underbrace{2, \ldots, 2}_{n_2}, \ldots, \underbrace{s, \ldots, s}_{n_s}) \subseteq B_r^s \text{ und}$$
$$D := D(\pi) := \tfrac{r}{\mathrm{ggT}\,(n_1, \ldots, n_s)}.$$

Wir haben eine Operation von $\mathbb{Z}$ auf $B_r^s(\pi)$ via $\mathbb{Z} \xrightarrow{1 \mapsto [12 \ldots r]} S_r$. Die Anzahl der Elemente eines Orbits unter dieser Operation ist natürlich ein Teiler von r, und für einen solchen Teiler e von r bezeichne $N(e) := N_r^s(\pi, e)$ die Anzahl der Orbiten mit genau e Elementen. Sei schließlich $\mu : \mathbb{N}_+ \to \{-1, 0, 1\}$ die *Möbius-Funktion*, die wie folgt für eine natürliche Zahl c mit Primfaktorzerlegung $c = p_1^{m_1} \cdot \ldots \cdot p_u^{m_u}$ definiert ist:

$$\mu(c) = \begin{cases} (-1)^u & \text{falls } m_i \leq 1 \text{ für alle } i, \\ 0 & \text{sonst.} \end{cases}$$

Dann gilt folgende Formel:

$$\boxed{N_r^s(\pi, e) = \frac{1}{e} \cdot \sum_{D|d|e} \mu\left(\frac{e}{d}\right) \cdot \frac{d!}{\prod_{i=1}^s \left(n_i \cdot \frac{d}{r}\right)!}}. \tag{41}$$

Seien jetzt $n, h \in \mathbb{N}_+$ und $r_1, \ldots, r_h \in \mathbb{N}_+$ mit $r_1 + \ldots + r_h = n$. Definiere

$$\Pi_n^s(\pi; r_1, \ldots, r_h) := \left\{ \left(\pi^{(i)} = (n_1^{(i)}, \ldots, n_s^{(i)})\right)_i \in \Pi_{r_1}^s \times \ldots \times \Pi_{r_h}^s \,|\, \forall_{j=1,\ldots,s} \sum_{i=1}^h n_j^{(i)} = n_j \right\}.$$

Ist $(\pi^{(1)}, \ldots, \pi^{(h)}) \in \Pi_n^s(\pi; r_1, \ldots, r_h)$ beliebig, so definiere

$$B_n^s(\pi^{(1)}, \ldots, \pi^{(h)}) := B_{r_1}^s(\pi^{(1)}) \times \ldots \times B_{r_h}^s(\pi^{(h)}) \in B_{r_1}^s \times \ldots \times B_{r_h}^s = B_n^s.$$

Offenbar gilt:

$$B_n^s(\pi) = \coprod_{(\pi^{(i)}) \in \Pi_n^s(\pi; r_1, \ldots, r_h)} B_n^s(\pi^{(1)}, \ldots, \pi^{(h)}). \tag{42}$$

Sei $\sigma(r_1, \ldots, r_h)$ der Zykel $[12 \ldots r_1][(r_1+1) \ldots (r_1+r_2)] \ldots [(n-r_h+1) \ldots n]$ aus S_n. Dann operiert $\mathbb{Z}$ vermöge $\mathbb{Z} \xrightarrow{1 \mapsto \sigma(r_1, \ldots, r_h)} S_n$ auf $B_n^s(\pi^{(1)}, \ldots, \pi^{(h)})$. Für eine natürliche Zahl e definiere

$$E(e; r_1, \ldots, r_h) := \left\{(e_1, \ldots, e_h) \in \mathbb{N}_+^h \mid e_1 | r_1, \ldots, e_h | r_h, \mathrm{kgV}\,(e_1, \ldots, e_h) = e\right\}$$

und bezeichne für $(e_i) \in E(e; r_i)$ mit $\tilde{N}_n^s(\pi^i, e_i)$ die Zahl der Orbiten, in denen die ersten r_1 Elemente unter $[1 \ldots r_1]$ in einem Orbit der Länge e_1 liegen, die nächsten r_2 Element unter $[(r_1 + 1) \ldots (r_1 + r_2)]$ in einem Orbit der Länge e_2 liegen und so weiter. Dann gilt die folgende Formel:

$$\boxed{\tilde{N}_n^s(\pi^{(i)}, e_i) = \mathrm{ggT}\,(e_1, \ldots, e_h) \cdot \prod_{i=1}^h N_{r_i}^s(\pi^{(i)}, e_i)}. \tag{43}$$

Beweis: Wenn $(a_1, \ldots, a_r)$ in einem Orbit der Länge e liegt, muß gelten:

$$\begin{array}{ccccccccc} a_1 & = & a_{1+e} & = & a_{1+2e} & = & \ldots & = & a_{1+(r/e-1)e}, \\ a_2 & = & a_{2+e} & = & a_{2+2e} & = & \ldots & = & a_{2+(r/e-1)e}, \\ \vdots & & \vdots & & \vdots & & \vdots & & \\ a_e & = & a_{2e} & = & a_{3e} & = & \ldots & = & a_r. \end{array}$$

In jeder Zeile stehen r/e Elemente, d.h. die Zahl r/e muß jedes der n_i, also auch D teilen. Dies ist äquivalent zu $D|e$.

Für eine natürliche Zahl d bezeichne $k(d)$ die Zahl der Elemente aus $B_r^s(\pi)$, die eine durch d teilbare Ordnung unter der Operation von $\mathbb{Z}$ haben. Diese Ordnung muß natürlich auch r und damit (r, d) teilen. Außerdem haben wir gerade gesehen, daß sie von D geteilt werden muß, d.h. für $k(d) > 0$ ist $D|d$ notwendig.

Wie groß ist $k(d)$, wenn $D|d$ gilt? Offenbar hat ein (a_i) aus $B_r^s(\pi)$ genau dann durch d teilbare Ordnung, wenn für $e := (r, d)$ obige Gleichungen erfüllt sind. Alle a_i werden dann schon durch $a_1, \ldots, a_e$ bestimmt, und von diesen müssen genau $n_1 \cdot r/e$ Stück gleich 1 sein, $n_2 \cdot r/e$ Stück gleich 2 und so weiter. Also gilt:

$$k(d) = \begin{cases} \dfrac{(r,d)!}{\left(n_1 \cdot \frac{r}{(r,d)}\right)! \cdot \ldots \cdot \left(n_s \cdot \frac{r}{(r,d)}\right)!} & \text{falls } D|d, \\ 0 & \text{sonst.} \end{cases} \tag{44}$$

Offenbar gilt andererseits:

$$k(e) = \sum_{d|e} d \cdot N(d) \quad (\text{wobei } N(d) := 0 \text{ für } d \not| r).$$

Wir können die *Möbiussche Umkehrformel* (vgl. [Lan93, S.254]!) anwenden und erhalten:

$$e \cdot N(e) = \sum_{d|e} \mu\left(\frac{e}{d}\right) \cdot k(d).$$

Ist e ein *Teiler* von r, so folgt (41) aus (44), wenn man beachtet, daß dann für $d|e$ schon $(r, d) = d$ gilt.

Die Gleichung (42) ist klar. Es bleibt also Gleichung (43) zu zeigen: Einer der $\tilde{N}$-vielen Orbits ist dadurch bestimmt, daß zunächst die zugehörigen Orbiten aus $B_{r_1}^s(\pi^{(1)}, e_1), \ldots,$ $B_{r_h}^s(\pi^{(h)}, e_h)$ angegeben werden (dies liefert den zweiten Faktor) und dann die Stellung dieser Orbiten zueinander, was den Faktor $\frac{e_1 \cdot \ldots \cdot e_h}{e} = \text{ggT}\,(e_1, \ldots, e_h)$ liefert. **q.e.d.**

10.4 Beispiel. Wähle $r = 108$, $s = 3$ und $\pi = (24, 36, 48)$. Wie viele Orbiten der Länge 54 gibt es? — Zunächst ist $D = 108/12 = 9$. Die Formel (41) ergibt dann:

$$\begin{aligned} N(54) &= \frac{1}{54} \cdot \sum_{d \in \{9,18,27,54\}} \mu\left(\frac{54}{d}\right) \frac{d!}{(24 \cdot d/108)! \cdot (36 \cdot d/108)! \cdot (48 \cdot d/108)!} \\ &= \frac{1}{54}\left(\mu(6)\frac{9!}{2!3!4!} + \mu(3)\frac{18!}{4!6!8!} + \mu(2)\frac{27!}{6!9!12!} + \mu(1)\frac{54!}{12!18!24!}\right) \\ &= \frac{1}{54}\left(\frac{9!}{2!3!4!} - \frac{18!}{4!6!8!} - \frac{27!}{6!9!12!} + \frac{54!}{12!18!24!}\right) \\ &= 2.246.676.834.410.732.596.320 \end{aligned}$$

10.5 Lemma. Es sei R ein kommutativer Ring mit Eins, $n \in \mathbb{N}_+$ eine natürliche Zahl und $a_1, \ldots, a_n \in R$ beliebig. Sei A die Matrix

$$\left(\begin{array}{cccc|c} 0 & 0 & \cdots & 0 & a_n \\ \hline a_1 & 0 & \cdots & 0 & 0 \\ 0 & a_2 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & a_{n-1} & 0 \end{array}\right)$$

über R. Dann gilt

$$\det(1 - At) = 1 - \left(\prod_{i=1}^{n} a_i\right) t^n.$$

Ist insbesondere R ein Körper, dessen Charakteristik n nicht teilt, und sind die a_i alle ungleich null, so ist A halbeinfach.

Beweis: Wir entwickeln die Determinante nach der ersten Zeile:

$$\det(1 - At) = \det \left(\begin{array}{cccc|c} 1 & 0 & \cdots & 0 & -a_n t \\ \hline -a_1 t & 1 & \cdots & 0 & 0 \\ 0 & -a_2 t & \ddots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & -a_{n-1} t & 1 \end{array}\right)$$

$$= \begin{vmatrix} 1 & 0 & \cdots & 0 & 0 \\ -a_2 t & 1 & \cdots & 0 & 0 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \ddots & 1 & 0 \\ 0 & 0 & \cdots & -a_{n-1} t & 1 \end{vmatrix} + (-1)^n a_n t \cdot \begin{vmatrix} -a_1 t & 1 & \cdots & 0 & 0 \\ 0 & -a_2 t & \ddots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & -a_{n-2} t & 1 \\ 0 & 0 & \cdots & 0 & -a_{n-1} \end{vmatrix}$$

$$= 1 + (-1)^n a_n t \cdot (-1)^{n-1} a_1 \cdot \ldots a_{n-1} \cdot t^{n-1}$$

$$= 1 + \underbrace{(-1)^{2n-1}}_{=(-1)} a_1 \cdot \ldots \cdot a_n \cdot t^n.$$

q.e.d.

10.6 Lemma/ Definition. Seien k, p, l, χ, n und m wie in Kapitel 5. Sei ferner $s \in (\mu_m^n/\mu_m) \rtimes S_n$ beliebig; nach eventueller Umnumerierung ist s von der Gestalt $s = (\zeta_1, \ldots, \zeta_n) \cdot \underbrace{\sigma(r_1, \ldots, r_h)}_{=:\sigma}$, setze

$$\begin{aligned} \xi_1 &:= \zeta_1 \cdot \ldots \cdot \zeta_{r_1}, \\ \xi_2 &:= \zeta_{r_1+1} \cdot \ldots \cdot \zeta_{r_1+r_2}, \\ &\cdots \\ \xi_h &:= \zeta_{n-r_h+1} \cdot \ldots \cdot \zeta_n. \end{aligned}$$

Sei nun $\boldsymbol{a} \in A_n^m$ beliebig. Dadurch wird ein $\pi_a \in \Pi_n^{m-1}$ definiert vermöge $n_i := \sharp\{j | a_j = i\}$. Dann gilt:

$$\begin{aligned}\Phi(s,\boldsymbol{a},t) &:= \det\left(1 - s^* t | V_{[\boldsymbol{a}]}\right) \\ &= (\operatorname{sgn}\sigma)^{\sharp[a]} \prod_{\substack{(\pi_a^{(i)}) \in \Pi_n^{m-1}(\pi_a; r_i), \\ e \in \mathbb{N}_+, \\ (e_i) \in E(e; r_i)}} \left[1 - \chi\left(\prod_{i=1}^{h} \xi_i^{\frac{e}{r_i}\sum_{j=1}^{m-1} j \cdot n_j^{(i)}}\right) t^e\right]^{\tilde{N}_n^{m-1}(\pi_a^{(i)}, e_i)}\end{aligned}$$

Beweis: Folgt sofort aus 9.17, 10.3 und 10.5! **q.e.d.**

10.7 Beispiel. Es sei speziell $m = 3$, $n = 6$, $s = (\zeta, 1, 1, 1, \zeta^2, 1) \cdot [1234][56]$, $\boldsymbol{a} = [1, 1, 1, 2, 2, 2]$ und $\boldsymbol{b} = [1, 1, 1, 1, 1, 1]$ (vgl. 9.8!). Dann ist also $\pi_a = (3, 3)$, $\pi_b = (6, 0)$, $\pi_{2b} = (0, 6)$, $h = 2$, $r_1 = 4$, $r_2 = 2$, $\xi_1 = \zeta$ und $\xi_2 = \zeta^2$. Weiter gilt:

$$\Pi_6^2((3,3); 4, 2) = \{((3,1),(0,2)), ((2,2),(1,1)), ((1,3),(2,0))\}$$

und

$$\begin{aligned} E(1; ((3,1),(4,2))) &= \{(1,1)\}, \\ E(2; ((3,1),(4,2))) &= \{(1,2),(2,1),(2,2)\}, \\ E(4; ((3,1),(4,2))) &= \{(4,1),(4,2)\} \end{aligned}$$

sowie

$$\begin{aligned} N_4^2((3,1),1) &= 0, & N_4^2((3,1),2) &= 0, & N_4^2((3,1),4) &= 1, \\ N_4^2((2,2),1) &= 0, & N_4^2((2,2),2) &= 1, & N_4^2((2,2),4) &= 1, \\ N_4^2((1,3),1) &= 0, & N_4^2((1,3),2) &= 0, & N_4^2((1,3),4) &= 1, \\ N_2^2((0,2),1) &= 1, & N_2^2((0,2),2) &= 0, \\ N_2^2((1,1),1) &= 0, & N_2^2((1,1),2) &= 1, \\ N_2^2((2,0),1) &= 1, & N_2^2((2,0),2) &= 0, \end{aligned}$$

so daß nur folgende $\tilde{N}$ ungleich null sind:

$$\begin{aligned} \tilde{N}_4^2(((3,1),(0,2)),(4,1)) &= (4,1) \cdot N_4^2((3,1),4) \cdot N_2^2((0,2),1) = 1, \\ \tilde{N}_4^2(((2,2),(1,1)),(2,2)) &= (2,2) \cdot N_4^2((2,2),2) \cdot N_2^2((1,1),2) = 2, \\ \tilde{N}_4^2(((2,2),(1,1)),(4,2)) &= (4,2) \cdot N_4^2((2,2),4) \cdot N_2^2((1,1),2) = 2, \\ \tilde{N}_4^2(((1,3),(2,0)),(4,1)) &= (4,1) \cdot N_4^2((1,3),4) \cdot N_2^2((2,0),1) = 1. \end{aligned}$$

Es folgt:

$$\begin{aligned} \Phi(s,\boldsymbol{a},t) &= 1^{20} \cdot \left[1 - \zeta^{1\cdot 5 + 2\cdot 2\cdot 4} t^4\right]^1 \left[1 - \zeta^{6/2 + 2\cdot 1\cdot 3} t^2\right]^2 \left[1 - \zeta^{1\cdot 6 + 2\cdot 2\cdot 3} t^4\right]^2 \left[1 - \zeta^{1\cdot 7 + 2\cdot 2\cdot 2} t^4\right]^1 \\ &= \left[1 - \zeta^{21} t^4\right] \cdot \left[1 - \zeta^9 t^2\right]^2 \cdot \left[1 - \zeta^{18} t^4\right]^2 \cdot \left[1 - \zeta^{15} t^4\right] \\ &= \left[1 - t^4\right] \cdot \left[1 - t^2\right]^2 \cdot \left[1 - t^4\right]^2 \cdot \left[1 - t^4\right] \\ &= \left[1 - t^4\right]^4 \cdot \left[1 - t^2\right]^2 \end{aligned}$$

Außerdem ergibt sich leicht:

$$\begin{aligned}\Phi(s,\boldsymbol{b},t) &= 1^1\cdot\left[1-\zeta^{1+2}t\right]^1 &= 1-t,\\ \Phi(s,2\boldsymbol{b},t) &= 1^2\cdot\left[1-\zeta^{2+4}t\right]^1 &= 1-t.\end{aligned}$$

10.8 Theorem. Mit den Bezeichnungen aus den Kapiteln 4 und 5 seien $m,n\in\mathbb{N}$ natürliche Zahlen mit $m\geq 1$ und $n\geq 2$ und $k=\mathbb{F}_q$ ein endlicher Körper der Charakteristik p, der die m-ten Einheitswurzeln enthält, sowie $b\in H^1_{\mathrm{cont}}(G_k,S_n\int\mu_m)$ beliebig. Bezeichne F den geometrischen Frobenius auf $\mathcal{X}^m_{n,K}$, und sei s das Bild des arithmetischen Frobenius $f\in G_k$ unter dem 1-Kozykel b. Die Zetafunktion des getwisteten Fermatpolynoms $P^m_n\{b\}$ wird dann gegeben durch:

$$\boxed{Q(P^m_n\{b\},t)=\prod_{[a]\in(\mu_m^{\check{n}}/\mu_m)/S_n}\det\left(1-s^*F^*t\,|\,V_{[a]}\right)}$$

mit

$$\boxed{\begin{aligned}&\det\left(1-s^*F^*t\,|\,V_{\{0,\dots,0\}}\right) &=& \begin{cases}1-q^{\frac{n-2}{2}}t & \text{falls } n \text{ gerade},\\ 1 & \text{sonst}\end{cases}\\ \text{und}\quad&\det\left(1-s^*F^*t\,|\,V_{[\boldsymbol{a}]}\right) &=& \Phi(s,\boldsymbol{a},\mathcal{J}(\boldsymbol{a})\cdot t)\qquad\qquad \text{für } \boldsymbol{a}\in A^m_n.\end{aligned}}$$

Beweis: Die erste Gleichung ist klar wegen (16), 4.6, 7.3 und 10.2, der Rest folgt aus 9.9, 9.12 und 10.6. **q.e.d.**

10.9 Beispiel. Sei $m=3$, $n=6$, $k=\mathbb{F}_7$ und $b\in H^1_{\mathrm{cont}}(G_{\mathbb{F}_7},\mu_3\int S_6)$ wie in 5.13 und 5.24. Wir wollen die Zetafunktion des Polynoms $P:=P^3_6\{b\}$ berechnen (vgl. 5.13, 5.24, 9.8, 9.18 und 10.7!). Es ist

$$\begin{aligned}Q(P,t) &= \det\left(1-s^*F^*t\,|\,V_{\{0,0,0,0,0,0\}}\right)\cdot\det\left(1-s^*F^*t\,|\,V_{\{1,1,1,1,1,1\}}\right)\\ &\quad\cdot\det\left(1-s^*F^*t\,|\,V_{[1,1,1,2,2,2]}\right)\cdot\det\left(1-s^*F^*t\,|\,V_{\{2,2,2,2,2,2\}}\right)\\ &= (1-7^2t)\cdot[1-(-56-21\zeta)t]\cdot[1-(49t)^4]^4[1-(49t)^2]^2\\ &\qquad\cdot[1-(-35+21\zeta)t]\\ &= (1+91t+7^4t^2)(1-7^2t)(1-7^4t^2)^2(1-7^8t^4)^4.\end{aligned}$$

Also

$$\zeta(P,t)=\frac{1}{1-t}\cdot\frac{1}{1-7t}\cdot\frac{1}{(1+91t+7^4t^2)(1-7^2t)(1-7^4t^2)^2(1-7^8t^4)^4}\cdot\frac{1}{1-7^3t}\cdot\frac{1}{1-7^4t}.$$

Logarithmieren ergibt:

$$\zeta(P,t)=\exp\left(\frac{2710}{1}t+\frac{5897984}{2}t^2+\frac{13881660703}{3}t^3+\frac{33246893493864}{4}t^4+\dots\right).$$

11 Kubische getwistete Fermatgleichungen

In diesem Kapitel wollen wir den Spezialfall von getwisteten kubischen Fermatgleichungen in zwei und in vier Variablen betrachten. Dies sind zwei „bösartige“ Fälle gemäß 9.19.

11.1 Lemma. Es sei $p \geq 5$ eine Primzahl mit $p \equiv 2 \pmod 3$. Dann gilt:

(i) $\left(\frac{-3}{p}\right) = -1$.

(ii) $\ker\left(\mathbb{F}_{p^2} \xrightarrow{\mathrm{Tr}} \mathbb{F}_p\right) = \{a\sqrt{-3} \mid a \in \mathbb{F}_p\}$.

(iii) $\ker\left(\mathbb{F}_{p^2} \xrightarrow{\mathrm{Tr}} \mathbb{F}_p\right) \subseteq (\mathbb{F}_{p^2})^3$.

Beweis:

(i) Es ist $\frac{1}{2}(-1+\sqrt{-3})$ eine primitive dritte Einheitswurzel in $\overline{\mathbb{Q}}$, d.h. $\mathbb{Q}(\sqrt{-3})$ ist der dritte (und der sechste) Kreisteilungskörper. Also enthielte der Körper $\mathbb{F}_p$ die dritten Einheitswurzeln, wenn er $\sqrt{-3}$ enthielte, was aber wegen $p \equiv 2 \pmod 3$ nicht der Fall ist.

(ii) Wegen (i) liegt $\sqrt{-3}$ nicht in $\mathbb{F}_p$, d.h. $\left(\sqrt{-3}\right)^p = -\sqrt{-3}$, also $\mathrm{Tr}\left(\sqrt{-3}\right) = \sqrt{-3} - \sqrt{-3} = 0$, so daß „$\supseteq$“ folgt.

Umgekehrt folgt aus der Surjektivität der Spur, daß die folgende Sequenz von $\mathbb{F}_p$-Vektorräumen exakt ist.

$$0 \longrightarrow \ker(\mathrm{Tr}) \longrightarrow \mathbb{F}_{p^2} \xrightarrow{\mathrm{Tr}} \mathbb{F}_p \longrightarrow 0.$$

Also ist der Kern der Spur ein eindimensionaler $\mathbb{F}_p$-Vektorraum, enthält also genau p Elemente, und die Gleichheit der beiden Mengen folgt, weil sie gleiche Kardinalität haben.

(iii) Weil $\mathbb{F}_p$ die dritten Einheitswurzeln nicht enthält, kann man aus jedem Element von $\mathbb{F}_p$ (eindeutig) die dritte Wurzel ziehen. Wegen (ii) ist also nur zu zeigen, daß $\sqrt{-3}$ dritte Potenz in $\mathbb{F}_{p^2}$ ist, oder äquivalent, daß (-3) sechste Potenz ist.

Sei $a \in \mathbb{F}_p$ das Element mit $a^3 = -3$. Dann liegt $\sqrt{a}$ in $\mathbb{F}_{p^2}$, und es gilt $\left(\sqrt{a}\right)^6 = a^3 = -3$.

q.e.d.

Zunächst berechnen wir die auftretenden Jacobisummen.

11.2 Lemma. Es sei $\zeta \in \mathbb{C}$ eine primitive dritte Einheitswurzel und $K := \mathbb{Q}(\zeta)$. Dann ist die Strahlklassengruppe $Cl_K^{(3)}$ trivial, d.h. jedes gebrochene, zu (3) teilerfremde Ideal von K ist ein Hauptideal (a) mit $a \equiv 1 \pmod 3$. †

†Eigentlich muß man auch noch fordern, daß a *total positiv* ist, d.h. positiv unter jeder Einbettung $K \hookrightarrow \mathbb{R}$. In unserem Fall gibt es eine solche Einbettung jedoch offensichtlich nicht, so daß die Bedingung leer ist (vgl. [Neu92, S.381]!).

Beweis: Zunächst beachte man, daß $\mathcal{O}_K = \mathbb{Z}[\zeta]$ euklidisch bezüglich der Funktion

$$d : \mathbb{Z}[\zeta] \setminus \{0\} \longrightarrow \mathbb{N}_+,\ x \mapsto |x|^2 = N_{K/\mathbb{Q}}(x)$$

ist. Insbesondere ist $\mathbb{Z}[\zeta]$ also ein Hauptidealring, d.h. $Cl_K^{(3)}$ wird als abelsche Gruppe von Klassen von Hauptidealen (π) zu Primelementen $\pi \nmid 3$ erzeugt. Sei also ein solches $\pi \in \mathbb{Z}[\zeta]$ vorgegeben. Wir müssen zeigen, daß es dann ein $\xi \in \mathbb{Z}[\zeta]^\times$ mit $\pi \equiv \xi \pmod 3$ gibt (denn dann folgt $(\pi) = (\xi^{-1}\pi)$ und $\xi^{-1}\pi \equiv 1 \pmod 3$). Wegen $(1-\zeta)(2+\zeta) = 3$ und $\pi \nmid 3$ gilt

$$\pi \not\equiv 0, (1+2\zeta) \text{ und } (2+\zeta) \pmod 3.$$

Es folgt

$$\pi \equiv 1, (1+\zeta), \zeta, 2\zeta, 2 \text{ oder } (2+2\zeta) \pmod 3.$$

Nun gilt

$$\begin{array}{llllll} (-\zeta)^0 = 1 \equiv 1 \pmod 3, & & (-\zeta)^1 = -\zeta \equiv 2\zeta \pmod 3, \\ (-\zeta)^2 = \zeta^2 \equiv 2+2\zeta \pmod 3, & & (-\zeta)^3 = -1 \equiv 2 \pmod 3, \\ (-\zeta)^4 = \zeta \equiv \zeta \pmod 3, & & (-\zeta)^5 = -\zeta^2 \equiv 1+\zeta \pmod 3, \end{array}$$

d.h. für jede der sechs Möglichkeiten finden wir ein $n \in \{0,1,2,3,4,5\}$ mit $\pi \equiv (-\zeta)^n \pmod 3$. **q.e.d.**

11.3 Satz. Es sei ζ die primitive dritte Einheitswurzel $\mathrm{e}^{\frac{2\pi i}{3}}$, und $I_{(3)}$ bezeichne die Gruppe der zu 3 teilerfremden gebrochenen Ideale von $\mathbb{Q}(\zeta)$. Ist $\mathfrak{a} \in I_{(3)}$ ein ganzes Ideal, so finden wir nach 11.2 eine ganze Zahl $a \in \mathbb{Q}(\zeta)$ mit $\mathfrak{a} = (a)$ und $a \equiv 1 \pmod 3$. Mit diesem a gilt dann für den in 9.5 definierten Charakter $\mathbf{J}_{(1,1,1)} : I_{(3)} \to \mathbb{C}^\times$:

$$\mathbf{J}_{(1,1,1)}(\mathfrak{a}) = a.$$

Beweis: Es seien $\iota, \tau : \mathbb{Q}(\zeta) \hookrightarrow \mathbb{C}$ die beiden, durch $\iota(\zeta) := \zeta$ und $\tau(\zeta) := \zeta^2 = \bar{\zeta}$ gegebenen Einbettungen von $\mathbb{Q}(\zeta)$ in $\mathbb{C}$. Nach 9.5 ist $\mathbf{J}_{(1,1,1)}$ ein Größencharakter mit Erklärungsmodul (9). Für den Beweis unseres Satzes ist zu zeigen, daß man als Erklärungsmodul sogar (3) wählen kann und daß der Unendlichtyp $(n_\iota = 1, n_\tau = 0)$ ist.

Zunächst stellen wir die folgende Tabelle auf, wobei wir die letzte Spalte durch stures Einsetzen in Definition 9.2 berechnen:

i	ϖ_i	$\varpi_i \pmod{(9)}$	$N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\varpi_i)$	$\mathbf{J}_{(1,1,1)}\big((\varpi_i)\big)$
1	$1+9\zeta$	1	73	$1+9\zeta$
2	$1+3\zeta$	$1+3\zeta$	7	$1+3\zeta$
3	$1-3\zeta$	$1+6\zeta$	13	$1-3\zeta$
4	$4+9\zeta$	4	61	$4+9\zeta$
5	$4+3\zeta$	$4+3\zeta$	13	$4+3\zeta$
6	$4-3\zeta$	$4+6\zeta$	37	$4-3\zeta$
7	$7+9\zeta$	7	67	$7+9\zeta$
8	$7+3\zeta$	$7+3\zeta$	37	$7+3\zeta$
9	$-2-3\zeta$	$7+6\zeta$	7	$-2-3\zeta$

Weil $\varpi_1 \equiv 1 \pmod{(9)}$ ist, folgt aus der ersten Zeile der Tabelle:

$$\varpi_1 = \mathbf{J}_{(1,1,1)}\big((\varpi_1)\big) \overset{9.5}{=} \varpi_1^{n_\iota} \cdot \overline{\varpi_1}^{n_\tau} \quad \overset{\substack{\mathbb{Z}[\zeta] \text{ faktoriell,} \\ \varpi_1,\, \overline{\varpi_1} \text{ Primelemente}}}{\Longrightarrow} \quad (n_\iota, n_\tau) = (1,0),$$

d.h. wir wissen jetzt, daß Hauptideale (a) mit $a \in \mathbb{Z}[\zeta]$ und $a \equiv 1 \pmod{(9)}$ unter $\mathbf{J}_{(1,1,1)}$ auf a abgebildet werden.

Sei jetzt $\mathfrak{a} \in I_{(3)}$ ein beliebiges ganzes Ideal von $\mathbb{Q}(\zeta)$, und sei $a \in \mathbb{Z}[\zeta]$ mit $\mathfrak{a} = (a)$ und $a \equiv 1 \pmod{(3)}$. Dann ist a modulo (9) kongruent zu einem der ϖ_i aus der Tabelle. Es gilt:

i	j	$\varpi_i \cdot \varpi_j$	$\varpi_i\varpi_j \pmod{(9)}$
1	1	$-80-63\zeta$	1
2	3	$10+9\zeta$	1
4	7	$-53+18\zeta$	1
5	9	$1-9\zeta$	1
6	8	37	1

Also sind die ϖ_i Einheiten des Rings $\mathbb{Z}[\zeta]/(9)$, d.h. wir finden ein $j \in \{1,\dots,9\}$ mit $a \cdot \varpi_j \equiv 1 \pmod{9}$. Wie wir uns oben überlegt haben, folgt hieraus

$$\mathbf{J}_{(1,1,1)}\big((a \cdot \varpi_j)\big) = a \cdot \varpi_j.$$

Aus der ersten Tabelle wissen wir, daß $\mathbf{J}_{(1,1,1)}\big((\varpi_j)\big) = \varpi_j$ gilt, und wir erhalten:

$$\mathbf{J}_{(1,1,1)}\big(\mathfrak{a}\big) = \frac{\mathbf{J}_{(1,1,1)}\big(\mathfrak{a} \cdot (\varpi_j)\big)}{\mathbf{J}_{(1,1,1)}\big((\varpi_j)\big)} = \frac{\mathbf{J}_{(1,1,1)}\big((a \cdot \varpi_j)\big)}{\mathbf{J}_{(1,1,1)}\big((\varpi_j)\big)} = \frac{a \cdot \varpi_j}{\varpi_j} = a.$$

Dies ist gerade die Behauptung; unser Satz ist also bewiesen. **q.e.d.**

11.4 Lemma. Es sei $p \geq 5$ eine Primzahl mit $p \equiv 2 \pmod 3$. Dann gilt für die Jacobisummen der Dimensionen 0, 1 und 2 vom Grad 3 zu $(1,2)$, $(1,1,1)$ bzw. $(1,1,2,2)$ (unabhängig vom verwendeten Charakter $\chi : \mathbb{F}_{p^2}^\times \twoheadrightarrow \mu_3$):

$$\begin{aligned}
\mathcal{J}^3_{\mathbb{F}_{p^2}}(1,2) &= 1, \\
\mathcal{J}^3_{\mathbb{F}_{p^2}}(1,1,1) &= -p, \\
\mathcal{J}^3_{\mathbb{F}_{p^2}}(1,1,2,2) &= p^2.
\end{aligned}$$

Beweis:

- Dies ist ein bloßer Spezialfall von 9.3.
- Legt man zur Berechnung der Jacobisummen zwei verschiedene Charaktere χ zugrunde, so sind die Ergebnisse offenbar konjugiert zueinander. Wenn wir also zeigen können, daß die Jacobisumme für irgendein χ in $\mathbb{Q}$ liegt, so hat sie für alle anderen χ denselben Wert.

  Wegen $p \equiv 2 \pmod 3$ ist p träge in $\mathbb{Q}(\zeta)$, d.h. (p) ist ein Primideal mit Restklassenkörper $\mathbb{F}_{p^2}$, so daß wir erhalten:

$$\mathcal{J}^3_{\mathbb{F}_{p^2}}(1,1,1) = \mathbf{J}_{(1,1,1)}\big((p)\big) = \mathbf{J}_{(1,1,1)}\big((-p)\big) \overset{11.3}{=} -p \quad \text{da } (-p) \equiv 1 \pmod 3.$$

•

$$\mathcal{J}^3_{\mathbb{F}_{p^2}}(1,1,2,2) \overset{9.7(ii)}{=} \mathcal{J}^3_{\mathbb{F}_{p^2}}(1,2,1,2) = \mathcal{J}^3_{\mathbb{F}_{p^2}}\Big((1,2)*(1,2)\Big)$$
$$\overset{9.7(iii)}{=} p^2 \cdot \big(\mathcal{J}^3_{\mathbb{F}_{p^2}}(1,2)\big)^2 = p^2 \cdot 1^2 = p^2.$$

q.e.d.

Jetzt können wir die Frobeniusoperation auf der l-adischen Kohomologie der null- und zwei-dimensionalen Fermathyperfläche bezüglich der Basis aus 9.15 mit einigen Mühen explizit bestimmen und dadurch insbesondere die Zetafunktion einer beliebigen nicht-ausgearteten binären kubischen Form über einem endlichen Körper berechnen.

11.5 Korollar. Es seien k ein *endlicher* Körper, $\mathcal{X} := \mathcal{X}^3_2$ die nulldimensionale kubische Fermathyperfläche über k, $V := \mathrm{H}^0_{\text{ét}}(\mathcal{X}_{\bar{k}}, \mathbb{Q}_l)$ die Kohomologie von $\mathcal{X}$ und V_{prim} wie in 9.9 der primitive Teil der Kohomologie von $\mathcal{X}$.
Setze $\boldsymbol{a} := (1,2) \in A^3_2$, und sei $\{v_b\}_{b\in\{(1,2),(2,1)\}}$ eine Basis von $V_{[\boldsymbol{a}]}$ wie in 9.15. Dann gilt $V_{\text{prim}} = V_{[\boldsymbol{a}]}$, und der geometrische Frobenius $F^*_{\mathcal{X}}$ operiert auf V_{prim} durch

$$\boxed{\forall \boldsymbol{b} \in [\boldsymbol{a}] \,:\, F^*_{\mathcal{X}}(v_b) = \begin{cases} v_b & \text{falls } \mu_3 \subseteq k, \\ -v_{2b} & \text{sonst.} \end{cases}}$$

Beweis: Zuerst überlegt man sich sofort, daß $A^3_2 = [\boldsymbol{a}]$ gilt, d.h. $V_{\text{prim}} = V_{[\boldsymbol{a}]}$ ist klar. — Enthält k die dritten Einheitswurzeln, so folgt sofort nach 9.3 und 9.9, daß der Frobenius trivial auf V operiert.

Enthalte also k die dritten Einheitswurzeln *nicht*. Sei k' die eindeutig bestimmte Erweiterung vom Grad zwei von k. Es ist kein Problem, $(F^*_{\mathcal{X}})^2$ zu berechnen, da k' die dritten Einheitswurzeln enthält: Für beliebiges $\boldsymbol{b} \in \{(1,2),(2,1)\}$ ergibt sich

$$(F^*_{\mathcal{X}})^2(v_b) \overset{9.9}{=} \mathcal{J}^3_{k'}(\boldsymbol{b}) \cdot v_b \overset{9.3}{=} v_b.$$

Nach 9.10 folgt also $F^*_{\mathcal{X}}(v_b) = \varepsilon(\boldsymbol{b}) \cdot v_{2b}$ für $\varepsilon(\boldsymbol{b}) \in \{-1,1\}$, und wir müssen beweisen, daß $\varepsilon(\boldsymbol{b}) = -1$ gilt. Der erste Schritt hierzu ist, einzusehen, daß $\varepsilon(\boldsymbol{b})$ nicht von $\boldsymbol{b}$ abhängt, d.h. es gilt $\varepsilon(\boldsymbol{b}) = \varepsilon(\boldsymbol{a}) =: \varepsilon$. Sei dazu $\sigma \in S_2$ die Permutation mit $\sigma^*\boldsymbol{a} = \boldsymbol{b}$. Offenbar vertauschen $F^*_{\mathcal{X}}$ und σ^*, und wir erhalten

$$F^*_{\mathcal{X}}(v_b) = F^*_{\mathcal{X}}(\sigma^* v_a) = \sigma^* F^*_{\mathcal{X}}(v_a) = \varepsilon \cdot \sigma^*(v_{2a}) = \varepsilon \cdot v_{2b}.$$

Wir wollen nun das getwistete Fermat-Polynom $P' := P^3_2\{(k',1)\}$ und die zugehörige projektive Hyperfläche $\mathcal{Y} \subseteq \mathbb{P}^1_k$ betrachten: Bezeichne s die Transposition $(12) \in S_2$. Nach (16) und (40) gilt dann

$$\#\mathcal{Y}(\mathbb{F}_p) = \mathrm{Tr}\left(s^* F^*_{\mathcal{X}} \,\middle|\, V\right),$$

und bezüglich der Basis $\{v_{(1,2)}, v_{(2,1)}\}$ von V_{prim} besitzt $s^*F^*_{\mathcal{X}}|V_{\text{prim}}$ die Darstellung

$$\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & \varepsilon \\ \varepsilon & 0 \end{pmatrix} = \begin{pmatrix} -\varepsilon & 0 \\ 0 & -\varepsilon \end{pmatrix}$$

Daraus folgt

$$\mathrm{Tr}\left(s^*F_{\mathcal{X}}^* \,\middle|\, V_{\mathrm{prim}}\right) = -2\varepsilon$$

und damit

$$\#\mathcal{Y}(\mathbb{F}_p) = \mathrm{Tr}\left(s^*F_{\mathcal{X}}^* \,\middle|\, \mathbb{Q}_l\right) + \mathrm{Tr}\left(s^*F_{\mathcal{X}}^* \,\middle|\, V_{\mathrm{prim}}\right) = 1 - 2\varepsilon.$$

Diese Zahl darf als Kardinalität einer (endlichen) Menge natürlich nicht negativ sein, so daß nur $\varepsilon = -1$ in Frage kommt. **q.e.d.**

11.6 Korollar. Es seien k ein *endlicher* Körper und Q eine nicht-ausgeartete binäre kubische Form über k.

(i) Enthält k die dritten Einheitswurzeln, so ist Q in $\widetilde{\mathcal{F}_k^{2,3}}$ isomorph zu einer der drei Formen aus 7.10(i), und wir können die zugehörige Zetafunktion angeben:

Q	$\zeta(Q,t)^{-1}$
$P\{(L_1,(1,1))\}$	$(1-t)^3$
$P\{(L_1,(1,\delta))\}$	$(1-t)(1+t+t^2)$
$P\{(L_\delta,1)\}$	$(1-t)(1+t^2)$

(ii) Enthält k die dritten Einheitswurzeln *nicht*, so ist Q in $\widetilde{\mathcal{F}_k^{2,3}}$ isomorph zu einer der drei Formen aus 7.10(ii), und auch dann können wir die zugehörige Zetafunktion angeben:

Q	$\zeta(Q,t)^{-1}$
$P\{(L_1,(1,1))\}$	$(1-t)^2(1+t)$
$P\{(L_\delta,1)\}$	$(1-t)^3$
$P\{(L_\delta,\alpha)\}$	$(1-t)(1+t+t^2)$

Beweis: Dies folgt durch simples Einsetzen in unsere Resultate aus (16), 5.14, 9.15, 10.2 und 11.5. **q.e.d.**

11.7 Bemerkung. Insbesondere sehen wir, daß die Zetafunktion binäre kubische Formen über einem endlichen Körper k bis auf Isomorphie in $\widetilde{\mathcal{F}_k^{2,3}}$ klassifiziert.

11.8 Satz. Es sei $p \geq 5$ eine Primzahl mit $p \equiv 2 \pmod 3$, $\mathcal{X} := \mathcal{X}_4^3$ die kubische Fermathyperfläche über $\mathbb{F}_p$ und V_{prim} wie in 9.9 der primitive Teil der mittleren Kohomologie von $\mathcal{X}$. Setze $\boldsymbol{a} := (1,1,2,2) \in A_4^3$, und sei $\{v_b\}_{b\in[a]}$ eine Basis von $V_{[\boldsymbol{a}]}$ wie in 9.15. Dann gilt $V_{\mathrm{prim}} = V_{[\boldsymbol{a}]}$, und der geometrische Frobenius $F_{\mathcal{X}}^*$ operiert auf V_{prim} durch

$$\boxed{\forall \boldsymbol{b} \in [\boldsymbol{a}] \;:\; F_{\mathcal{X}}^*(v_b) = p \cdot v_{2b}.}$$

Beweis: Wir gehen vollkommen analog zum Beweis von 11.5 vor, müssen uns diesmal aber ein klein wenig mehr anstrengen:

Wieder überlegt man sich sofort, daß $A_4^3 = [\boldsymbol{a}]$ gilt, d.h. $V_{\text{prim}} = V_{[\boldsymbol{a}]}$ ist klar. Des weiteren ist es kein Problem, $(F_{\mathcal{X}}^*)^2$ zu berechnen, da $\mathbb{F}_{p^2}$ die dritten Einheitswurzeln enthält: Für beliebiges $\boldsymbol{b} \in [\boldsymbol{a}]$ ergibt sich

$$(F_{\mathcal{X}}^*)^2 (v_b) \overset{9.9}{=} \mathcal{J}^3_{\mathbb{F}_{p^2}}(\boldsymbol{b}) \cdot v_b \overset{9.7(ii)}{=} \mathcal{J}^3_{\mathbb{F}_{p^2}}(\boldsymbol{a}) \cdot v_b \overset{11.4}{=} p^2 \cdot v_b.$$

Nach 9.10 folgt also $F_{\mathcal{X}}^* (v_b) = \varepsilon(\boldsymbol{b}) p \cdot v_{2b}$ für $\varepsilon(\boldsymbol{b}) \in \{-1, 1\}$, und wir müssen beweisen, daß $\varepsilon(\boldsymbol{b}) = 1$ gilt. Der erste Schritt hierzu ist wieder, einzusehen, daß $\varepsilon(\boldsymbol{b})$ nicht von $\boldsymbol{b}$ abhängt, d.h. es gilt $\varepsilon(\boldsymbol{b}) = \varepsilon(\boldsymbol{a}) =: \varepsilon$. Wählt man eine Permutation $\sigma \in S_4$ mit $\sigma^* \boldsymbol{a} = \boldsymbol{b}$, so folgt dies aber genau wie in 11.5.

Wir wollen nun das getwistete Fermat-Polynom $P' := P_4^3\{(\mathbb{F}_{p^2} \times \mathbb{F}_{p^2}, 1)\}$ und die zugehörige projektive Hyperfläche $\mathcal{Y} \subseteq \mathbb{P}^3_{\mathbb{F}_p}$ betrachten und dann auf zwei verschiedene Weisen die Anzahl der $\mathbb{F}_p$-rationalen Punkte $\#\mathcal{Y}(\mathbb{F}_p)$ berechnen. Der Vergleich der beiden Zahlen wird dann $\varepsilon = 1$ zeigen.

Die „erste Weise“ ist dieselbe wie im Beweis von 11.5: Bezeichne s die Permutation $(12)(34) \in S_4$. Nach (16) und (40) gilt dann

$$\#\mathcal{Y}(\mathbb{F}_p) = 1 + p^2 + \operatorname{Tr}\left(s^* F_{\mathcal{X}}^* \,\middle|\, \mathrm{H}^{n-2}_{\text{ét}}(\mathcal{X}_{\overline{\mathbb{F}}_p}, \mathbb{Q}_l)\right),$$

und bezüglich der Basis $\{v_{(1,1,2,2)}, v_{(1,2,1,2)}, v_{(1,2,2,1)}, v_{(2,1,1,2)}, v_{(2,1,2,1)}, v_{(2,2,1,1)}\}$ von V_{prim} besitzt $s^* F_{\mathcal{X}}^*$ die Darstellung

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & \varepsilon p \\ 0 & 0 & 0 & 0 & \varepsilon p & 0 \\ 0 & 0 & 0 & \varepsilon p & 0 & 0 \\ 0 & 0 & \varepsilon p & 0 & 0 & 0 \\ 0 & \varepsilon p & 0 & 0 & 0 & 0 \\ \varepsilon p & 0 & 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & \varepsilon p \\ 0 & \varepsilon p & 0 & 0 & 0 & 0 \\ 0 & 0 & \varepsilon p & 0 & 0 & 0 \\ 0 & 0 & 0 & \varepsilon p & 0 & 0 \\ 0 & 0 & 0 & 0 & \varepsilon p & 0 \\ \varepsilon p & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Daraus folgt

$$\operatorname{Tr}\left(s^* F_{\mathcal{X}}^* \,\middle|\, V_{\text{prim}}\right) = 4\varepsilon p$$

und damit

$$\begin{aligned} \#\mathcal{Y}(\mathbb{F}_p) = 1 + p^2 + \operatorname{Tr}\left(s^* F_{\mathcal{X}}^* \,\middle|\, \mathbb{Q}_l(-1)\right) + \operatorname{Tr}\left(s^* F_{\mathcal{X}}^* \,\middle|\, V_{\text{prim}}\right) \\ = 1 + p^2 + p + 4\varepsilon p = 1 + (1 + 4\varepsilon)p + p^2. \quad (45) \end{aligned}$$

Im Gegensatz zu der Situation aus 11.5 sind wir jetzt noch nicht fertig, weil dieser Ausdruck (zumindest für hinreichend große p) unabhängig von ε stets positiv ist. Wir haben aber zum Glück noch eine andere Möglichkeit, $\#\mathcal{Y}(\mathbb{F}_p)$ zu berechnen, wir können nämlich 3.15 benutzen. Sei dazu $\widetilde{\mathcal{Y}} \subseteq \mathbb{A}^4_{\mathbb{F}_p}$ die durch P' definierte affine dreidimensionale Hyper-

fläche. Dann liefert 3.15:

$$\begin{aligned}
\#\widetilde{\mathcal{Y}}(\mathbb{F}_p) &= \#\Big\{(x,y,z,u)\in\widetilde{\mathcal{Y}}(\bar{\mathbb{F}}_p)\;\Big|\;(x,y,z,u)=(y^p,x^p,u^p,z^p)\Big\}\\
&= \#\Big\{(x,x^p,z,z^p)\in\widetilde{\mathcal{Y}}(\bar{\mathbb{F}}_p)\;\Big|\;\Big(x^{(p^2)}=x\Big)\wedge\Big(z^{(p^2)}=z\Big)\Big\}\\
&= \#\Big\{(x,x^p,z,z^p)\in\widetilde{\mathcal{Y}}(\mathbb{F}_{p^2})\Big\}\\
&= \#\Big\{(x,z)\in\mathbb{F}_{p^2}^2\;\Big|\;(x^3+z^3)+(x^3+z^3)^p=0\Big\}\\
&= \#\Big\{(x,z)\in\mathbb{F}_{p^2}^2\;\Big|\;\mathrm{Tr}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(x^3+z^3)=0\Big\}\\
&= \#\Big\{(x,z,t)\in\mathbb{F}_{p^2}^3\;\Big|\;\Big(\mathrm{Tr}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(t)=0\Big)\wedge(x^3+z^3=t)\Big\}.
\end{aligned}\tag{46}$$

Setze

$$A:=\#\Big\{(x,z)\in\mathbb{F}_{p^2}^2\;\Big|\;x^3+z^3=0\Big\}\quad\text{und}\quad B:=\#\Big\{(x,z)\in\mathbb{F}_{p^2}^2\;\Big|\;x^3+z^3=1\Big\},$$

Dann folgt aus 11.1(ii),(iii) und (46)

$$\#\widetilde{\mathcal{Y}}(\mathbb{F}_p)=A+(p-1)B.\tag{47}$$

Wir berechnen zuerst A:

$$\begin{aligned}
A &= 1+(p^2-1)\cdot\#\Big\{(x:z)\in\mathbb{P}^1_{\mathbb{F}_p}(\mathbb{F}_{p^2})\;\Big|\;x^3+z^3=0\Big\}\\
&\overset{(40)}{=} 1+(p^2-1)\cdot(1+\mathcal{J}^3_{\mathbb{F}_{p^2}}(1,2)+\mathcal{J}^3_{\mathbb{F}_{p^2}}(2,1))\overset{11.4}{=}1+(p^2-1)\cdot 3=3p^2-2.
\end{aligned}\tag{48}$$

Bevor wir uns an die Berechnung von B machen, berechnen wir zunächst

$$\begin{aligned}
C &:= \#\Big\{(x:z:w)\in\mathbb{P}^1_{\mathbb{F}_p}(\mathbb{F}_{p^2})\;\Big|\;x^3+z^3=w^3\Big\}\\
&= \#\Big\{(x:z:w)\in\mathbb{P}^1_{\mathbb{F}_p}(\mathbb{F}_{p^2})\;\Big|\;x^3+z^3+w^3=0\Big\}\\
\text{und}\quad D &:= \#\Big\{(x,z,w)\in\mathbb{F}_{p^2}^3\;\Big|\;x^3+z^3=w^3\Big\}.
\end{aligned}$$

Wegen $A_3^3=\{(1,1,1),(2,2,2)\}$, 11.4 und (40) erhalten wir

$$\begin{aligned}
C &= 1+p^2-\Big(\mathcal{J}^3_{\mathbb{F}_{p^2}}(1,1,1)+\mathcal{J}^3_{\mathbb{F}_{p^2}}(2,2,2)\Big)=p^2+2p+1\\
&\Longrightarrow D=1+(p^2-1)C=1+(p^2-1)(p^2+2p+1)=p^4+2p^3-2p
\end{aligned}\tag{49}$$

und damit

$$B=\frac{D-A}{p^2-1}=\frac{p^4+2p^3-3p^2-2p+2}{p^2-1}=p^2+2p-2.\tag{50}$$

Einsetzen von (48) und (50) in (47) liefert schließlich das Ergebnis

$$\#\mathcal{Y}(\mathbb{F}_p)=\frac{\#\widetilde{\mathcal{Y}}(\mathbb{F}_p)-1}{p-1}=\frac{1+(3p^2-2)+(p-1)(p^2+2p-2)}{p-1}=p^2+5p+1,$$

und der Vergleich mit (45) zeigt $\varepsilon=1$, womit der Satz vollständig bewiesen ist. **q.e.d.**

Wie man sieht, ist es uns also auch in zwei „bösartigen“ Fällen gelungen, die Frobeniusoperation auf der l-adischen Kohomologie getwisteter Fermathyperflächen explizit zu bestimmen. Im Prinzip sollte es möglich sein, dieselbe Methode auch auf andere Grade und Dimensionen anzuwenden.

Literatur

[Bos93] Siegfried Bosch. *Algebra*. Springer, Berlin, Heidelberg, New York, 1993.

[Brü98] Lars Brünjes. Fast-étale Überlagerungen und Faltings' Reinheitssatz in den Dimensionen eins und zwei. Diplomarbeit, Universität zu Köln, 1998.

[Del73] P. Deligne. *Groupes de Monodromie en Géométrie Algébrique (SGA 7 II)*, volume 340 of *Lecture Notes in Mathematics*, chapter XI - Cohomologie des intersections complète, pages 39–61. Springer, Berlin, Heidelberg, New York, 1973.

[Del82] P. Deligne. *Hodge Cycles, Motives and Shimura Varieties*, volume 900 of *Lecture Notes in Mathematics*. Springer, Berlin, Heidelberg, New York, 1982.

[GKZ94] Israel M. Gelfand, Mikhail M. Kapranov, and Andrei V. Zelevinsky. *Discriminants, Resultants and Multidimensional Determinants*. Mathematics: Theory & Applications. Birkhäuser, Boston, Basel, Berlin, 1994.

[Gro71] A. Grothendieck. *SGA 1*, volume 224 of *Lecture Notes in Mathematics*, chapter VIII - Déscente Fidelment plat. Springer, New York, Berlin, Heidelberg, 1971.

[GY95] Fernando Q. Gouvêa and Noriko Yui. *Arithmetic of Diagonal Hypersurfaces over Finite Fields*, volume 209 of *London Mathematical Society, Lecture Note Series*. Cambridge University Press, Cambridge, 1995.

[Har93] Robin Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer, New York, Berlin, Heidelberg, 1993.

[HM00] J. William Hoffman and Jorge Morales. Arithmetic of Binary Cubic Forms. *L'Enseignement Mathématique*, 46:61–94, 2000.

[Kna92] Anthony W. Knapp. *Elliptic Curves*. Princeton University Press, Princeton, New Jersey, 1992.

[Lan93] Serge Lang. *Algebra*. Addison-Wesley Publishing Company, Reading (Massachusetts), Menlo Park (California), New York, 1993.

[Mil80] J. S. Milne. *Étale Cohomology*. Princeton University Press, Princeton, New Jersey, 1980.

[Mum94] David Mumford. *The Red Book of Varieties and Schemes*, volume 1358 of *Lecture Notes in Mathematics*. Springer, New York, Berlin, Heidelberg, 1994.

[Neu92] Jürgen Neukirch. *Algebraische Zahlentheorie*. Springer, New York, Berlin, Heidelberg, 1992.

[Rup96] Christopher Rupprecht. Kohomologische Invarianten für Formen höheren Grades. Diplomarbeit, Universität zu Köln, 1996.

[Ser79] Jean-Pierre Serre. *Local Fields*, volume 67 of *Graduate Texts in Mathematics*. Springer, New York, Berlin, Heidelberg, 1979.

[Ser97] Jean-Pierre Serre. *Galois Cohomology*. Springer, New York, Berlin, Heidelberg, 1997.

[Shi79] Tetsuji Shioda. The Hodge conjecture for Fermat Varieties. *Math. Ann.*, 245, 1979.

[Shi82] Tetsuji Shioda. Geometry of Fermat Varieties. *Number Theory Related to Fermat's Last Theorem, Progress in Math.*, 26, 1982.

[Shi83] Tetsuji Shioda. What is known about the Hodge Conjecture? *Advanced Studies in Pure Mathematics, Algebraic varieties and analytic varieties, Proc. Symp., Tokyo 1981*, 1:55–68, 1983.

[Shi87] Tetsuji Shioda. Some Observations on Jacobi Sums. *Advanced Studies in Pure Mathematics 12, Galois Representations and Arithmetic Algebraic Geometry*, pages 119–135, 1987.

[Shi88] Tetsuji Shioda. Arithmetic and geometry of Fermat curves. In *Algebraic Geometry Seminar, Singapore, 1987*, pages 95–102. World Sci. Publishing, Singapore, 1988.

[SK79] Tetsuji Shioda and Toshiyuki Katsura. On Fermat Varieties. *Tôhoku Math. Journ.*, 31:97–115, 1979.

[SW98] Andrzej Składek and Adam Wesołowski. Clifford-Littlewood-Eckmann groups as orthogonal groups of forms of higher degree. *Annales Mathematicae Silesianae*, 12:93–103, 1998.

[Tam94] Günter Tamme. *Introduction to Étale Cohomology.* Universitext. Springer, New York, Berlin, Heidelberg, 1994.

[Wei49] André Weil. Numbers of Solutions of Equations in Finite Fields. *Bulletin of the American Mathematical Society*, 55(1):497–508, 1949.

[Wei52] André Weil. Jacobi Sums as "Größencharaktere". *Transactions of the American Mathematical Society*, 73:487–495, 1952.

[Wes99] Adam Wesołowski. Automorphism and similarity groups of forms determined by the characteristic polynomial. *Communications in Algebra*, 27(7):3109–3116, 1999.