

Über quadratische Erweiterungen étaler Algebren der Dimension Vier

Diplomarbeit von Laura Beltrametti

Betreut von Prof. Dr. Max-Albert Knus

Departement Mathematik
Eidgenössische Technische Hochschule Zürich

26. März 2006

Inhaltsverzeichnis

1	Einführung	3
1.1	Motivation	3
1.2	Γ -Mengen	4
1.3	Étale Algebren	7
1.3.1	Generisches Minimalpolynom, Norm und Spur	8
1.3.2	Konstruktionen auf étale Algebren	8
1.4	Minimale Idempotente	11
1.5	Galois-Algebren	11
1.6	Galois Kohomologie	13
1.7	Vorbereitung	14
2	Fälle mit $\Delta(S_0) = F \times F$	19
2.1	$\alpha_Y(\Gamma) = \mathfrak{A}_4$	19
2.2	$\alpha_Y(\Gamma) = \mathfrak{B}$	21
2.3	$\alpha_Y(\Gamma) = C_2 \subset \mathfrak{B}$	24
2.3.1	Fall $b_1 \neq b_2$	24
2.3.2	Fall $b_1 = b_2 \neq \sqrt{a}$	26
2.3.3	Fall $b_1 = b_2 = b = \sqrt{a}$	27
2.4	$\alpha(\Gamma) = \text{Id} \times C_3$	28
3	Fälle mit $\Delta(S_0) \neq F \times F$	29
3.1	$\alpha_Y(\Gamma) = \mathfrak{S}_4$	29
3.2	$\alpha_y(\Gamma) = D_4$	30
3.3	$\alpha_Y(\Gamma) = C_4$	33
3.4	$\alpha_Y(\Gamma) = C_2 \not\subset \mathfrak{B}$	35
3.5	$\alpha_Y(\Gamma) = C_2 \times C_2 \not\subset \mathfrak{B}$	36
3.5.1	$x \neq y$	37
3.5.2	$x = y =: c$	39
3.6	$\alpha_Y(\Gamma) = \text{Id} \times S_3$	40
4	Schlussfolgerungen	41
5	Zusammenhänge und Ausblicke	41
5.1	Quaternionen	41
5.1.1	Definition	41
5.1.2	Quaternionen-Algebren	45
5.2	Clifford-Algebren	46

1 Einführung

1.1 Motivation

Symmetrie ist vielleicht eines der faszinierendsten und wichtigsten Konzepte die es gibt. Schon die alten Griechen bewunderten die Symmetrien der Körper und verliehen ihnen mystische Bedeutungen. Plato beschrieb als erste die fünf reguläre Polyeder, die sogenannten platonische Körper, und diese wurden mit den «fünf Elementen» assoziiert. Diese sind der Tetraeder (Feuer), der Kubus (Erde), der Oktaeder (Luft), der Ikosaeder (Wasser) und der Dodekaeder (Himmel). Die charakterisierende Eigenschaft dieser Körper ist, dass sich alle Flächen unter demselben Winkel treffen, und dass sich in jeder Ecke die gleiche Anzahl Kanten unter demselben Winkel trifft. Das impliziert insbesondere, dass alle Flächen dasselbe reguläre Polygon sind. Es kann gezeigt werden, dass, in drei Dimensionen, die einzigen Polyedern mit dieser Eigenschaft genau die fünf platonischen Körper sind. Die Symmetrie eines Objektes wird mathematisch durch die Existenz von Symmetriegruppen beschrieben. Symmetriegruppen sind Gruppen, die aus der Menge aller Kongruenzabbildungen bestehen, die ein gewisses Objekt wieder auf sich selbst abbilden, zusammen mit der Verkettung von Abbildungen als Gruppenoperation. Eine Kongruenzabbildung ist dabei eine Abbildung, bei der Form und Grösse der abgebildeten Objekte gleich bleiben (die Entfernung zweier beliebiger Punkten bleibt erhalten). Zum Beispiel ist die Symmetriegruppe des dreidimensionalen Raumes die Drehgruppe SO_3 . Die Symmetriegruppen von dreidimensionalen Körper müssen dann Untergruppen von SO_3 sein. Es gibt nur fünf Untergruppen von SO_3 die endlich sind und sie sind alle Symmetriegruppen der platonischen Körper (vgl. [6], Kapitel 5.9). Gruppen wurden eigentlich ursprünglich erfunden, um die Symmetrien von Körpererweiterungen zu analysieren. Die Wörter Symmetrie und Automorphismus sind nahezu Synonym, man verwendet aber die Bezeichnung Symmetrie für eine Permutation die eine geometrische Struktur erhält, während die Bezeichnung Automorphismus sich auf eine Permutation einer Menge bezieht, die eine algebraische Struktur erhält. Der Zusammenhang zwischen geometrische und algebraische Interpretation wird im Galois-Kohomologie Formalismus besonders evident. Ein allgemeineres Konzept, das das der Symmetrie einschliesst, ist das der Operation einer Gruppe auf einer Menge. In dieser Arbeit wird die Operation der absoluten Galois Gruppe $\Gamma = \text{Gal}(F_{\text{sep}}/F)$ eines Körpers F der Charakteristik 0 auf der Menge der F -Algebra Homomorphismen von L nach F_{sep} untersucht, wobei L eine quadratische Erweiterung einer étalen Algebra der Dimension vier ist. Man wird sehen, dass das sich auf die Symmetrien eines Hyperkubus (das vierdimensionale Analogon des Kubus) zurückführen lässt. Diese werden am Besten in der Sprache der Quaternionen behandelt. Am Ende werden die Clifford-Algebren (eine Verallgemeinerung der Quaternionenalgebren) eingeführt und ein kurzer Ausblick auf der Triality der zentral-einfachen

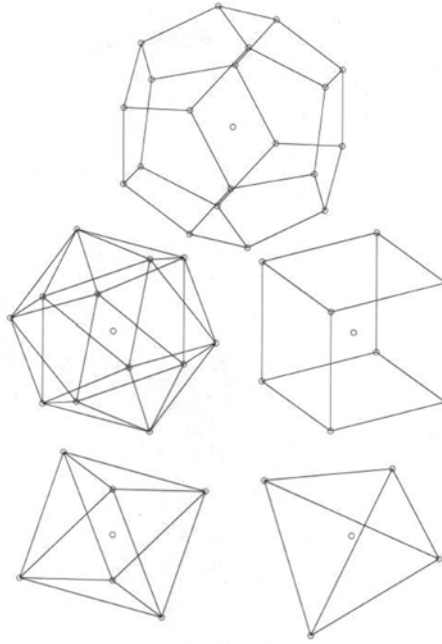


Abbildung 1: Platonische Körper

Algebren der Dimension acht gegeben.

1.2 Γ -Mengen

Sei Γ eine proendliche Gruppe.

Definition 1: Eine Γ -Menge ist eine endliche Menge, auf der eine stetige Γ -Operation definiert ist.

Γ -Mengen sind im folgenden aufgrund ihrer einfachen Struktur und der Existenz einer Antiäquivalenz zwischen ihrer Kategorie und der Kategorie der étalen Algebren wichtig.

Definition 2: Für eine Γ -Menge X mit n Elementen, d.h. $|X| = n$, definiere

$$\Sigma_k(X) := \{(\xi_1, \dots, \xi_k) \in X^k \mid \xi_i \neq \xi_j \text{ für } i \neq j\}, \quad k \in \mathbb{N}, \quad 0 < k \leq n\},$$

als die Menge der geordneten k -Tupel bestehend aus paarweise verschiedenen Elementen von X .

Es gilt:

$$|\Sigma_k(X)| = k! \binom{n}{k}.$$

Die Γ -Operation auf X induziert eine stetige Operation auf $\Sigma_k(X)$ das somit auch eine Γ -Menge ist. Im Folgenden wird man sich nur mit dem Fall $\Sigma_n(X)$, bei $|X| = n$ beschäftigen

so dass

$$|\Sigma_n(X)| = n! = |\mathfrak{S}_n|.$$

Man kann nun die Operation der alternierende Gruppe \mathfrak{A}_n auf $\Sigma_n(X)$ betrachten:

$$\begin{aligned} \theta : \mathfrak{A}_n &\longrightarrow \text{Aut}(\Sigma_n(X)), \\ \sigma &\longmapsto \theta(\sigma) : (\xi_1, \dots, \xi_n) \mapsto (\xi_{\sigma(1)}, \dots, \xi_{\sigma(n)}). \end{aligned} \tag{1}$$

Definiere

$$\Delta(X) := \Sigma_n(X)/\mathfrak{A}_n$$

als $\Delta(X)$ die Diskriminante von X . Klarerweise ist $|\Delta(X)| = 2$ für alle Γ -Mengen X und $\Delta(X)$ ist eine Γ -Menge mit der induzierten Operation. Γ operiert trivial auf $\Delta(X)$ genau dann wenn die Γ -Operation auf X durch \mathfrak{A}_n faktorisiert, d.h. genau dann, wenn es nur durch gerade Permutationen auf X operiert. $\Delta(X)$ verallgemeinert den Begriff der Diskriminante eines Polynoms: wenn $X = \{\alpha_1, \dots, \alpha_n\}$ die Menge der Nullstellen eines Polynoms $f(x) \in F[x]$ ist, so ist $\Delta(X) = \{\delta, -\delta\}$, wobei δ die positive Wurzel der gewöhnlichen Diskriminante von $f(x)$ bezeichnet:

$$\delta = \sqrt{\Delta} = \prod_{i < j} (\alpha_i - \alpha_j).$$

Definition 3: Für eine Γ -Menge X mit $|X| = n$ definiere

$$\Lambda_k(X) := \{\{\xi_1, \dots, \xi_k\} \subset X \mid \xi_i \neq \xi_j \text{ für } i \neq j\}$$

Definition 4: Für $n = 2m$ sei

$$\gamma_X : \Lambda_m(X) \rightarrow \Lambda_m(X)$$

die Abbildung, die zu jeder m -elementigen Teilmenge von X die jeweils komplementäre Teilmenge assoziiert. Offensichtlich gilt

$$\gamma_X^2 = \text{Id},$$

und γ_X induziert eine \mathfrak{S}_2 -Operation auf $\Lambda_m(X)$.

Eine andere wichtige Konstruktion, die das in der Theorie der Lösung polynomialer Gleichungen auftretende Konzept der Resolvente verallgemeinert, ist folgende:

Definition 5: Sei $|X| = 2m$ gerade. Betrachte die \mathfrak{S}_2 -Operation auf $\Lambda_m(X)$, die von der Abbildung $\gamma_X : \Lambda_m(X) \rightarrow \Lambda_m(X)$ induziert wird und definiere

$$\mathcal{R}(X) = \Lambda_m(X)/\mathfrak{S}_2$$

als die Menge der Partitionen von X in m -elementige Teilmengen.

Die Γ -Operation auf X induziert in natürlicher Weise eine Γ -Operation auf all diesen Konstruktionen. Bezeichne das Bild von Γ in \mathfrak{S}_X , $\mathfrak{S}_{\Delta(X)}$, $\mathfrak{S}_{\mathcal{R}(X)}$ mit $\alpha_X(\Gamma)$, $\alpha_{\Delta(X)}(\Gamma)$ und $\alpha_{\mathcal{R}(X)}(\Gamma)$.

Definition 6: Eine Γ -Überdeckung von Grad d ist ein Γ -äquivarianter Morphismus

$$Y \xleftarrow{\pi} Z$$

zwischen Γ -Mengen Y und Z , so dass $\forall y \in Y$ die Faser $\pi^{-1}(y) \subset Z$ genau d Elemente enthält.

Definition 7: Ein Morphismus zwischen zwei Γ -Überdeckungen

$$(Y_1 \xleftarrow{\pi_1} Z_1) \longrightarrow (Y_2 \xleftarrow{\pi_2} Z_2)$$

ist ein Paar von Γ -äquivalenten Morphismen

$$\sigma : Y_1 \rightarrow Y_2; \quad \tau : Z_1 \rightarrow Z_2,$$

die

$$\sigma \circ \pi_1 = \pi_2 \circ \tau$$

erfüllen.

Zwei Γ -Überdeckungen sind genau dann isomorph, wenn σ und τ Γ -Isomorphismen sind.

Definition 8: Für eine Γ -Überdeckung

$$Y \xleftarrow{\pi} Z$$

vom Grad d und $|Y| = n$, definiere die Menge der Schnitte von π durch

$$\Omega(Z/Y) = \{ \{ \xi_1, \dots, \xi_n \} \subset Z \mid \{ \pi(\xi_1), \dots, \pi(\xi_n) \} = Y \}.$$

Da jede Faser d Elemente enthält, gibt für jedes Element ξ_i es d Möglichkeiten; somit folgt

$$|\Omega(Z/Y)| = d^n.$$

Für den Fall $d = 2$ kann man eine Γ -equivariante Involution $\gamma_{Z/Y}$ auf Z/Y definieren, die die zwei Elemente in jeder Faser miteinander vertauscht und Y invariant lässt. Da $|Y| = n$, $|Z| = 2n$, induziert die Involution $\gamma_{Z/Y}$ eine Γ -verträgliche Involution auf $\Omega(Z/Y)$, die jedes Element $\{ \xi_1, \dots, \xi_n \} \subset Z$ in sein komplementäres $\{ \xi_1, \dots, \xi_n \}^c = \{ \gamma_{Z/Y}(\xi_1), \dots, \gamma_{Z/Y}(\xi_n) \}$ überführt. Diese Involution kann in natürlicher Weise als \mathfrak{S}_2 -Operation auf $\Omega(Z/Y)$ interpretiert werden. Definiere

$$S(Z/Y) = \Omega(Z/Y) / \mathfrak{S}_2,$$

so ist $S(Z/Y) \xleftarrow{\pi} \Omega(Z/Y)$ eine Γ -Überdeckung von Grad 2 mit $|S(Z/Y)| = 2^{n-1}$ und $|\Omega(Z/Y)| = 2^n$.

Für eine Γ -Menge X mit n Elementen sei $\mathfrak{S}_X = \mathfrak{S}_n$ die Gruppe der Permutationen von X . Jede Permutation von X induziert eine Permutation auf den oben definierten Konstruktionen $\Sigma_n(X)$, $\Lambda_k(X)$, $\Delta(X)$ und $\mathcal{R}(X)$, es existiert also ein kanonischer Gruppenhomomorphismus von \mathfrak{S}_X nach der Permutationsgruppe dieser Konstruktionen.

Bemerkung: Der Gruppenhomomorphismus $\mathfrak{S}_X \longrightarrow \mathfrak{S}_{\Delta(X)}$ ist nichts anderes als die Signatur-Abbildung, die jeder Permutation ihre Parität zuordnet.

Sei Y eine Menge mit n Elementen und Z/Y eine Überdeckung von Grad d . Die Gruppe der Automorphismen von Z/Y ist

$$\mathfrak{S}_{Z/Y} = \{(\sigma, \tau) \in \mathfrak{S}_Y \times \mathfrak{S}_Z \mid \pi \circ \tau = \sigma \circ \pi\}.$$

Man kann leicht sehen, dass diese Gruppe Ordnung $(d!)^n n!$ hat und zu $\mathfrak{S}_d^n \rtimes \mathfrak{S}_n$ isomorph ist. Die Automorphismen von Z/Y induzieren Permutationen auf der Menge der Schnitte $\Omega(Z/Y)$ und, falls $d = 2$, auch auf $\mathcal{S}(Z/Y)$. Bezeichne die zugehörigen Gruppenhomomorphismen mit

$$\omega_{Z/Y} : \mathfrak{S}_{Z/Y} \rightarrow \mathfrak{S}_{\Omega(Z/Y)}, \quad s_{Z/Y} : \mathfrak{S}_{Z/Y} \rightarrow \mathfrak{S}_{\mathcal{S}(Z/Y)}$$

Bemerkung: Der Kern von $s_{Z/Y}$ ist die zu \mathfrak{S}_2 isomorphe Untergruppe von $\mathfrak{S}_{Z/Y}$, deren einziges nicht triviales Element $\gamma_{Z/Y}$ ist.

1.3 Étale Algebren

Definition 9: Eine **Etale Algebra** über F ist eine endlichdimensionale, kommutative separable F -Algebra.

Definition 10: Sei L eine endlichdimensionale kommutative F -Algebra und F_{sep} ein separabler Abschluss von F . Definiere

$$X(L) := \text{Hom}_{F\text{-Alg}}(L, F_{\text{sep}}).$$

Theorem 1 *Sei L eine endlich dimensionale kommutative F -Algebra, dann sind die folgenden Aussagen äquivalent:*

- i) L ist separabel (und somit étale),
- ii) $L \simeq K_1 \times K_2 \times \cdots \times K_r$ für endliche separable Körpererweiterungen K_i/F ,
- iii) $L \otimes F_{\text{sep}} \simeq F_{\text{sep}} \times F_{\text{sep}} \times \cdots \times F_{\text{sep}}$,
- iv) $|X(L)| = \dim_F(L)$,
- v) Die Bilinearform $T : L \times L \rightarrow F$, die von der Spur durch

$$T(x, y) := \text{Tr}_L(xy) \quad \text{für } x, y \in L$$

induziert wird, ist nichtsingulär.

- vi) Falls F unendlich ist, so sind i)-v) äquivalent zu $L \simeq F[T]/(f)$ für ein separables Polynom $f \in F[T]$.

Referenzen:[3]: Théorème 4, S. V.34, für i) \Leftrightarrow ii) \Leftrightarrow iii); Corollaire, S. V.29, für iii) \Leftrightarrow iv); Proposition 1, S. V.47 und Proposition 3, S. V.36, für die Äquivalenz von v) und vi) zu den anderen Aussagen.

1.3.1 Generisches Minimalpolynom, Norm und Spur

Eine Algebra über F ist insbesondere ein F -Vektorraum. Sei $\{a_1, \dots, a_m\}$ eine Basis der m -dimensionalen F -Algebra A und setze $R = F[t_1, t_2, \dots, t_m]$ für m Variablen t_1, \dots, t_m (R ist der Polynomring in m Variablen über F). Sei K der Quotientenkörper von R .

Definition 11: Das **generische Element** von A ist definiert als

$$\gamma := \sum_{i=1}^m t_i a_i \in K \otimes A.$$

Da $K \otimes A$ ein endlichdimensionaler K -Vektorraum ist, gibt es ein nichttriviales, normiertes, minimales Polynom $P_{A,\gamma}(T) \in K(T)$, so dass $P_{A,\gamma}(\gamma) = 0$. Als Minimalpolynom von γ ist $P_{A,\gamma}(T)$ eindeutig und wird **generisches Minimalpolynom** von A genannt. Schreibe

$$P_{A,\gamma}(T) = T^d - s_1(\gamma)T^{d-1} + \dots + (-1)^{d-1}s_{d-1}(\gamma)T + (-1)^d s_d(\gamma)1.$$

Es kann gezeigt werden, vgl z.B. ([15]), dass die Koeffizienten $s_i(\gamma)$, $i \in \{1, \dots, d\}$, in R liegen. Man nennt $s_1(\gamma) =: t_A$ **generische Spur**, $s_d(\gamma) =: n_A$ **generische Norm** und d **Grad** von A .

Definition 12: Sei $a = \sum_{i=1}^m \alpha_i a_i \in A$ mit $\alpha_i \in F$ und

$$\begin{aligned} \tau_a : R[T] &\rightarrow F[T] \\ t_i &\mapsto \alpha_i \quad \forall i \in \{1, \dots, m\}. \end{aligned}$$

Das **charakteristische Polynom** von a ist definiert als das Bild von $P_{A,\gamma}(T)$ unter τ_a . Ähnlicherweise sind Spur $T_A(a)$ und Norm $N_A(a)$ von a die Bilder von $s_1(\gamma)$ bzw. $s_d(\gamma)$ unter τ_a .

Definition 13: Die **bilineare Spur-Form** auf A ist die Bilinearform die von der Spur durch

$$T_A(a, b) = T_A(ab) \quad \forall a, b \in A$$

induziert wird.

Bemerkung: Falls A isomorph zu einer Matrixalgebra $M_n(F)$ ist, so stimmt die obige Definition von Spur mit der üblichen Matrixspur überein.

1.3.2 Konstruktionen auf étale Algebren

Von nun an sei L eine étale Algebra. Die Galois-Gruppe der (nicht notwendigerweise endlichen) Galois-Erweiterung F_{sep}/F , auch absolute Galois-Gruppe genannt, ist definiert durch einen inversen Limes:

$$\Gamma = \text{Gal}(F_{\text{sep}}/F) = \varprojlim_{\alpha} \text{Gal}(F_{\alpha}/F)$$

wobei der Index α alle endlichen Galois-Erweiterungen F_α von F durchläuft. Die Gruppe Γ operiert in natürlicher Weise auf $X(L)$ durch

$$\gamma\xi = \gamma \circ \xi \quad \text{für } \gamma \in \Gamma \quad \text{und} \quad \xi \in X(L).$$

Da $|X(L)| = \dim(L) < \infty$, faktorisiert die Γ -Operation auf $X(L)$ durch einen endlichen Quotienten $\text{Gal}(F_\alpha/F)$ von Γ derart dass $\xi(L) \subset F_\alpha, \forall \xi \in X(L)$ gilt. Somit ist die Γ -Operation stetig und $X(L)$ eine Γ -Menge.

Für eine Γ -Menge X betrachte die F_{sep} -Algebra $\text{Map}(X, F_{\text{sep}})$ der Abbildungen $f : X \rightarrow F_{\text{sep}}$ mit punktweiser Addition und Multiplikation. Γ operiert auf dieser Algebra durch

$$\gamma f : \xi \mapsto \gamma f(\gamma^{-1}\xi).$$

Definition 14: Sei

$$M(X) = \text{Map}(X, F_{\text{sep}})^\Gamma = \{f \in \text{Map}(X, F_{\text{sep}}) \mid \gamma f = f \quad \forall \gamma \in \Gamma\}$$

die F -Algebra der Γ -invarianten Abbildungen in $\text{Map}(X, F_{\text{sep}})$.

Natürlich liegt ein $f \in \text{Map}(X, F_{\text{sep}})$ genau dann in $M(X)$ wenn

$$f(\sigma\xi) = \sigma \circ f(\xi) \quad \forall \sigma \in \Gamma \quad \text{und} \quad \forall \xi \in X.$$

Bemerkung: Die Algebra $M(X)$ ist étale, da nach Galois-descent gilt:

$$M(X) \otimes_F F_{\text{sep}} = \text{Map}(X, F_{\text{sep}})^\Gamma \otimes_F F_{\text{sep}} \simeq \text{Map}(X, F_{\text{sep}}) \simeq F_{\text{sep}} \times \dots \times F_{\text{sep}}.$$

Die Konstruktionen $X(L)$ und $M(X)$ sind beide funktoriell:

- Jeder F -Algebra Homomorphismus von étale Algebren $f : L_1 \rightarrow L_2$ induziert eine Γ -äquivalente Abbildung

$$X(f) : X(L_2) \rightarrow X(L_1),$$

definiert durch

$$X(f)(\xi) := \xi \circ f \quad \text{für } \xi \in X(L_2).$$

- Jede Γ -equivariante Abbildung von Γ -Mengen $g : X_1 \rightarrow X_2$ induziert einen F -Algebra Homomorphismus

$$M(g) : \text{Map}(X_2, F_{\text{sep}})^\Gamma \rightarrow \text{Map}(X_1, F_{\text{sep}})^\Gamma,$$

definiert durch

$$(M(g)(f))(\xi) = f(g\xi) \quad \text{für } f \in \text{Map}(X_2, F_{\text{sep}})^\Gamma \quad \text{und} \quad \xi \in X_1.$$

Die Abbildungen $X : L \rightarrow X(L)$ und $M : X \rightarrow M(X)$ sind also kontravariante Funktoren zwischen der Kategorie Sets_Γ der Γ -Mengen und der Kategorie Et_F der étale Algebren über F .

Theorem 2 Die Funktoren X und M definieren eine Antiäquivalenz von Kategorien

$$\text{Et}_F \equiv \text{Sets}_\Gamma,$$

und es gilt:

i) Falls $X \simeq X(L)$ und $L \simeq M(X)$ so gilt $\dim_F L = |X|$,

ii)

$$X(L_1 \times \dots \times L_r) = X(L_1) \sqcup \dots \sqcup X(L_r),$$

iii)

$$X(L_1 \otimes \dots \otimes L_r) = X(L_1) \times \dots \times X(L_r).$$

mit der diagonalen Γ -Operation auf der rechten Seite.

Mittels dieser Antiäquivalenz kann man Konstruktionen auf Γ -Mengen in äquivalente Konstruktionen auf étale Algebren überführen.

Definition 15: Sei L eine étale Algebra der Dimension n über F . Definiere

$$\Sigma(L) = \text{Map}(\Sigma(X(L)), F_{\text{sep}})^\Gamma,$$

$$\Delta(L) = \text{Map}(\Delta(X(L)), F_{\text{sep}})^\Gamma = \Sigma(L)^{A_n},$$

$$\mathcal{R}(L) = \text{Map}(\mathcal{R}(X(L)), F_{\text{sep}})^\Gamma.$$

Aus der Definition von $\Delta(X(L))$ folgt, dass der Kern der Γ -Operation auf $\Delta(X(L))$ diejenige Untergruppe $\Gamma_0 \subset \Gamma$ ist, die durch gerade Permutationen auf $X(L)$ operiert. Dann gilt

$$\Delta(L) \simeq \begin{cases} F \times F & \text{falls } \Gamma_0 = \Gamma, \\ (F_{\text{sep}})^{\Gamma_0} & \text{falls } \Gamma_0 \neq \Gamma. \end{cases}$$

Man nennt die Diskriminante $\Delta(X)$ bzw. $\Delta(L)$ *trivial*, falls Γ trivial auf $\Delta(X)$ operiert bzw. falls $\Delta(L) \simeq F \times F$.

Bemerkung: Wenn $L = F[T]/(f)$ für ein separables Polynom $f(T) \in F[T]$ von Grad n ist und $\text{Char}(F) \neq 2$, so gilt

$$\Delta(L) \simeq F[T]/(T^2 - d)$$

für die gewöhnliche Diskriminante d von f

$$d = \prod_{1 \leq i < j \leq n} (x_i - x_j)^2 \in F$$

mit x_1, \dots, x_n die n paarweise verschiedene Nullstellen von f in F_{sep} .

Allgemeiner gilt:

Theorem 3 Sei L eine étale Algebra über der Körper F mit $\text{Char}(F) \neq 2$. Dann

$$\Delta(L) \simeq F[t]/(t^2 - d)$$

wobei $d \in F^\times$ die Determinante der bilineare Spur-Form T bezeichnet.

Beweis. Siehe [1], Prop. 18.24, S. 293

□

1.4 Minimale Idempotente

Der kanonische Isomorphismus $L \simeq M(X(L))$ definiert eine Korrespondenz zwischen den Idempotenten von L und den charakteristischen Funktionen von Γ -Untermengen von $X(L)$. Erinnerung: die Charakteristische Funktion f_{char} einer Untergruppe Y von X durch

$$f_{\text{char}}(x) = \begin{cases} 1 & \text{falls } x \in Y, \\ 0 & \text{falls } x \in X \setminus Y \end{cases}$$

definiert ist.

Falls $e \in L$ das idempotente Element ist, der zu der charakteristische Funktion von $Y \subset X(L)$ korrespondiert, so ist $X(eL) = Y$ und $X((1-e)L) = X \setminus Y$. Für $L = F^n$ sind die Elemente von $X(L) = \{\xi_1, \dots, \xi_n\}$ und die minimale Idempotente von L zueinander dual:

$$\xi_i(e_j) = \begin{cases} 1 & \text{falls } i = j, \\ 0 & \text{falls } i \neq j. \end{cases}$$

Der Idempotent, der zu einer Untergruppe $Y = \{\xi_i | i \in I\}$ von $X(F^n)$ korrespondiert, ist dann die Summe $\sum_{i \in I} e_i$.

Für eine beliebige étale Algebra L der Dimension n , bezeichne mit $s_k^L \in L^{\otimes k}$, $1 \leq k \leq n$, der zu

$$\Sigma_k(X(L)) = \{(\xi_1, \dots, \xi_k) | \xi_i \neq \xi_j \text{ für } i \neq j\} \subset X(L)^k = X(L^{\otimes k})$$

korrespondierende Idempotent. Dann $\Sigma_k(L) = s_k^L L^{\otimes k}$ und $X(\Sigma_k(L)) = \Sigma_k(X(L))$. Für $\Lambda_k(L)$ und $\Delta(L)$ gilt

$$\Lambda_k(L) = \Sigma_k(L)^{\mathfrak{S}_k} = s_k^L (L^{\otimes k})^{\mathfrak{S}_k}, \quad \Delta(L) = \Sigma_n(L)^{\mathfrak{A}_n} = s_n^L (L^{\otimes n})^{\mathfrak{A}_n}.$$

Falls B/A eine Erweiterung von étalen Algebren von Grad d ist, dann korrespondiert die Inklusion $A \xrightarrow{i} B$ unter der Antiäquivalenz $\text{Et}_F \equiv \text{Sets}_\Gamma$ zu der Überdeckung $X(A) \xleftarrow{\pi} X(B)$ von Grad d . Sei A von der Dimension n und s_n^A der zu $\Sigma_n(A)$ gehörige Idempotent. Dann kann $\Omega(B/A)$ folgenderweise definiert werden (vgl. [2], S.11)

$$\Omega(B/A) = i^{\otimes n}(s_n(A)) \cdot (B^{\otimes n})^{\mathfrak{S}_n}.$$

1.5 Galois-Algebren

Die spezielle Struktur der oben definierten Algebren (sie lassen sich als Produkt von separablen Körpererweiterungen schreiben) legt es nahe, die gewöhnliche Galois-Theorie für Körpererweiterungen auf Algebren zu verallgemeinern. Man betrachtet eine étale F -Algebra L , auf der eine endliche Gruppe G durch F -Automorphismen operiert. Eine solche Algebra mit G -Operation nennt man **G -Algebra**; die Unter algebra der G -invarianten Elementen bezeichnet man mit L^G . Die Antiäquivalenz $\text{Et}_F \equiv \text{Sets}_\Gamma$ definiert einen Gruppenisomorphismus

$$\text{Aut}_F(L) \simeq \text{Aut}_{\text{Sets}_\Gamma}(X(L)).$$

Theorem 4 $L^G = F$ genau dann, wenn G auf $X(L)$ transitiv operiert.

Der Beweis findet man z.B. in [1], S.287.

Definition 16: Eine G -Algebra L über F heisst **Galois** falls

$$\dim_F(L) = |G| \quad \text{und} \quad L^G = F.$$

Falls E eine étale F -Algebra der Dimension n ist, so ist $\Sigma_n(E)$ eine Galois \mathfrak{S}_n -Algebra. In der Tat ist $|\Sigma_n(E)| = n! = |\mathfrak{S}_n|$ und \mathfrak{S}_n operiert transitiv auf $\Sigma_n(E)$. Es gibt n Einbettungen $\varepsilon_i : E \rightarrow \Sigma_n(E)$ die, unter der Antiäquivalenz $\text{Et}_F \equiv \text{Sets}_\Gamma$, zu den n Projektionen $\Pi_i : \Sigma_n(X(E)) \rightarrow X(E)$ korrespondieren. Explizit sind diese Einbettungen gegeben durch

$$\varepsilon_i(x) = s_n^E \cdot (1 \otimes \dots \otimes x \otimes \dots \otimes 1)$$

mit $x \in E$ an der i -ten Stelle. Klarerweise ist $\sigma(\varepsilon_i(x)) = \varepsilon_{\sigma(i)}(x)$ für alle $\sigma \in \mathfrak{S}_n$. $\Sigma_n(E)$ zusammen mit den Einbettungen ε_i heisst *Galois-Abschluss* von E .

Für eine Erweiterung B/A von étale F -Algebren kann ein Galois-Abschluss folgenderweise definiert werden: ist B/A eine Erweiterung von Grad d und $\dim_F(A) = n$, so betrachte zuerst B als A -Algebra der Dimension d ; sei $s_d^{B/A}$ der zur charakteristischen Funktion von der n -elementige Teilmenge

$$\{(\xi_1, \dots, \xi_d) \mid \xi_i \neq \xi_j \text{ für } i \neq j \text{ und } \pi(\xi_i) = \pi(\xi_j) \text{ für } i = 1, \dots, d\} \subset X(B^{\otimes_A d})$$

korrespondierende Idempotent. Dann ist

$$\Sigma_d^A(B) = s_d^{B/A} \cdot B^{\otimes_A d}$$

der \mathfrak{S}_d -Galois Abschluss von B als A -Algebra. Da $\Sigma_d^A(B)$ eine A -Algebra ist, gibt es eine kanonische Einbettung $j : A \rightarrow \Sigma_d^A(B)$. Definiere

$$\Sigma(B/A) = j^{\otimes n}(s_n^A) \cdot \Sigma_d^A(B)^{\otimes n}.$$

$\Sigma(B/A)/\Sigma_n(A)$ ist dann eine Erweiterung von Grad $(d!)^n$, so dass $|\Sigma(B/A)| = (d!)^n n! = |\mathfrak{S}_d^n \times \mathfrak{S}_n|$. Es existieren nd kanonische Einbettungen $\varepsilon_{ij} : B \rightarrow \Sigma(B/A)$ mit $1 \leq i \leq d$ und $1 \leq j \leq n$, so dass das Diagramm

$$\begin{array}{ccc} \Sigma_n(A) & \longrightarrow & \Sigma(B/A) \\ \varepsilon_j \uparrow & & \uparrow \varepsilon_{ij} \\ A & \longrightarrow & B \end{array}$$

für alle i, j kommutiert.

Es gilt ferner

$$\Omega(B/A) = \Sigma(B/A)^{\mathfrak{S}_{d-1}^n \times \mathfrak{S}_n}.$$

Falls $d = 2$, so definieren die kanonischen Einbettungen ε_1^A und $\varepsilon_2^A = \varepsilon_1^A \circ \gamma_{B/A}$ einen Isomorphismus $B \simeq \Sigma_2^A(B)$, und

$$\Omega(B/A) = \Sigma(B/A)^{\mathfrak{S}_n}.$$

In diesem Fall werden die kanonischen Einbettungen $\varepsilon_{ij} : B \rightarrow \Sigma(B/A)$ explizit durch

$$\begin{aligned} \varepsilon_{11}(b) &= s_n^A \cdot (b \otimes 1 \otimes \dots \otimes 1) =: b_1, & \varepsilon_{21}(b) &= s_n^A \cdot (\bar{b} \otimes 1 \otimes \dots \otimes 1) =: b'_1 \\ \varepsilon_{12}(b) &= s_n^A \cdot (1 \otimes b \otimes \dots \otimes 1) =: b_2, & \varepsilon_{22}(b) &= s_n^A \cdot (1 \otimes \bar{b} \otimes \dots \otimes 1) =: b'_2 \\ & \vdots & & \vdots \\ \varepsilon_{1n}(b) &= s_n^A \cdot (1 \otimes 1 \otimes \dots \otimes b) =: b_n, & \varepsilon_{2n}(b) &= s_n^A \cdot (1 \otimes 1 \otimes \dots \otimes \bar{b}) =: b'_n \end{aligned}$$

für $b \in B$ definiert.

Definition 17: Sei

$$\omega : B \rightarrow \Omega(B/A)$$

die lineare Abbildung die durch

$$b \mapsto \omega(b) = b_1 + b_2 + \dots + b_n \in \Omega(B/A) = \Sigma(B/A)^{\mathfrak{S}_n},$$

für alle $b \in B$ definiert ist.

Diese Abbildung wird im Abschnitt über Clifford-Algebren eine wichtige Rolle spielen. Dort wird insbesondere gezeigt, dass $\omega(B)$ die Algebra $\Omega(B/A)$ über F erzeugt.

1.6 Galois Kohomologie

Für eine Γ -Menge G definiere

$$H^0(\Gamma, G) := G^\Gamma = \{g \in G \mid \sigma g = g \quad \forall \sigma \in \Gamma\}$$

Sei G eine Γ -Gruppe. Ein *1-Kozykel* von Γ mit Werten in G ist eine stetige Abbildung $\alpha : \Gamma \rightarrow G$, so dass

$$\alpha(\sigma\tau) = \alpha(\sigma) \cdot \sigma\alpha(\tau)$$

für alle $\sigma, \tau \in \Gamma$. Die Menge aller Kozykeln von Γ mit Werten in G wird mit $Z'(\Gamma, G)$ bezeichnet. Falls G eine abelsche Γ gruppe ist, so ist auch $Z'(\Gamma, G)$ eine abelsche Gruppe mit der Multiplikation

$$\alpha\beta(\sigma) = \alpha(\sigma) \cdot \beta(\sigma).$$

Auf $Z'(\Gamma, G)$ ist eine Äquivalenzrelation \sim durch

$$\alpha \sim \alpha' \Leftrightarrow \exists g \in G \quad \text{so dass} \quad \alpha'(\sigma) = g \cdot \alpha(\sigma) \cdot \sigma g^{-1} \quad \forall \sigma \in \Gamma \quad (2)$$

definiert. Die erste Kohomologiegruppe von Γ mit Werten in G ist definiert als

$$H^1(\Gamma, G) = Z^1(\Gamma, G) / \sim.$$

Falls Γ trivial auf G operiert, so folgt aus (2), dass zwei Kozykeln α und α' genau dann äquivalent sind, wenn $\alpha' = \text{Int}(g) \circ \alpha$ für ein $g \in G$ gilt, das heisst genau dann wenn $\alpha'(\sigma) = g\alpha(\sigma)g^{-1}$ für alle $\sigma \in \Gamma$ gilt. Sei $f : A \rightarrow B$ ein Homomorphismus von Γ -Mengen. Falls ein Element von A unter Γ fixiert bleibt, so bleibt auch sein Bild in B fixiert und f lässt sich zu einer Abbildung $f_0 : H^0(\Gamma, A) \rightarrow H^0(\Gamma, B)$ einschränken.

Wenn A, B Γ -Gruppen sind, und f ein Gruppenhomomorphismus, so induziert f einen Homomorphismus

$$f^1 : H^1(\Gamma, A) \rightarrow H^1(\Gamma, B).$$

Für eine Γ -Menge X mit n Elementen betrachte man noch den Gruppenhomomorphismus

$$\Gamma \rightarrow \mathfrak{S}_X \simeq \mathfrak{S}_n.$$

Da $\mathfrak{S}_X \simeq \mathfrak{S}_n$ von der Indizierung der Elementen in X abhängt, wird der Homomorphismus $\Gamma \rightarrow \mathfrak{S}_n$ von X nur bis auf Konjugation mit einem Element in \mathfrak{S}_n eindeutig bestimmt. Betrachtet man \mathfrak{S}_n als Menge mit trivialer Γ -Operation, so erhält man eine kanonische bijektive Korrespondenz zwischen der Menge der Isomorphieklassen von Γ -Mengen mit n Elementen und der ersten Kohomologie-Gruppe $H^1(\Gamma, \mathfrak{S}_n)$. Zusammen mit der Antiäquivalenz $\text{Sets}_\Gamma \equiv \text{Ét}_F$ ergibt dies eine bijektive Korrespondenz

$$\Gamma\text{-Mengen mit } n \text{ Elementen} \longleftrightarrow \text{étale Algebren der Dimension } n \longleftrightarrow H^1(\Gamma, \mathfrak{S}_n).$$

Analog kann man eine Korrespondenz zwischen den Γ -Mengen die aus X konstruiert wurden und der ersten Kohomologie-Gruppe von Γ mit Werten in der jeweils zugehörigen Permutationsgruppe definieren. Man hat zum Beispiel eine bijektive Korrespondenz zwischen den Isomorphieklassen von Γ -Überdeckungen Z/Y von Grad d mit $|Y| = n$ und den Elementen der ersten Kohomologie-Gruppe $H^1(\Gamma, \mathfrak{S}_d^n \times \mathfrak{S}_n)$. Galois-Kohomologie dient allgemeiner zur Klassifizierung von Algebren, neben étale Algebren können insbesondere auch zentral-einfache Algebren durch Kohomologie-Gruppen klassifiziert werden (vgl.[1], 29.B, S. 395).

1.7 Vorbereitung

Sei F ein Körper der Charakteristik 0. Im folgenden werden quadratische Erweiterungen $S_0 \subset S$ von étalen Algebren S_0 der Dimension 4 über F betrachtet, mit der zusätzlichen Annahme, dass $\Delta(S) = F \times F$ ist. S ist eine étale Algebra der Dimension 8 über F . Setze:

$$Z = X(S) \quad \text{und} \quad Y = X(S_0).$$

Es gilt $|Z| = 8$, $|Y| = 4$, und $Y \leftarrow Z$ ist eine Γ -Überdeckung vom Grad 2. Es gibt eine schöne geometrische Deutung dieser Situation, man kann nämlich die Menge Z mit der Menge der Zellen eines Hyperkubus identifizieren; Y entspricht dann der Menge der Paare entgegengesetzter Zellen (siehe Abbildung 2):

$$Z = \{A, \bar{A}, B, \bar{B}, C, \bar{C}, D, \bar{D}\},$$

$$Y = \{(A, \bar{A}), (B, \bar{B}), (C, \bar{C}), (D, \bar{D})\}.$$

Da sich in jeder Ecke 4 paarweise verschiedene, nicht entgegengesetzte Zellen treffen, kann man die Menge der Schnitte $\Omega(Z/Y)$ mit den 16 Ecken des Hyperkubus identifizieren

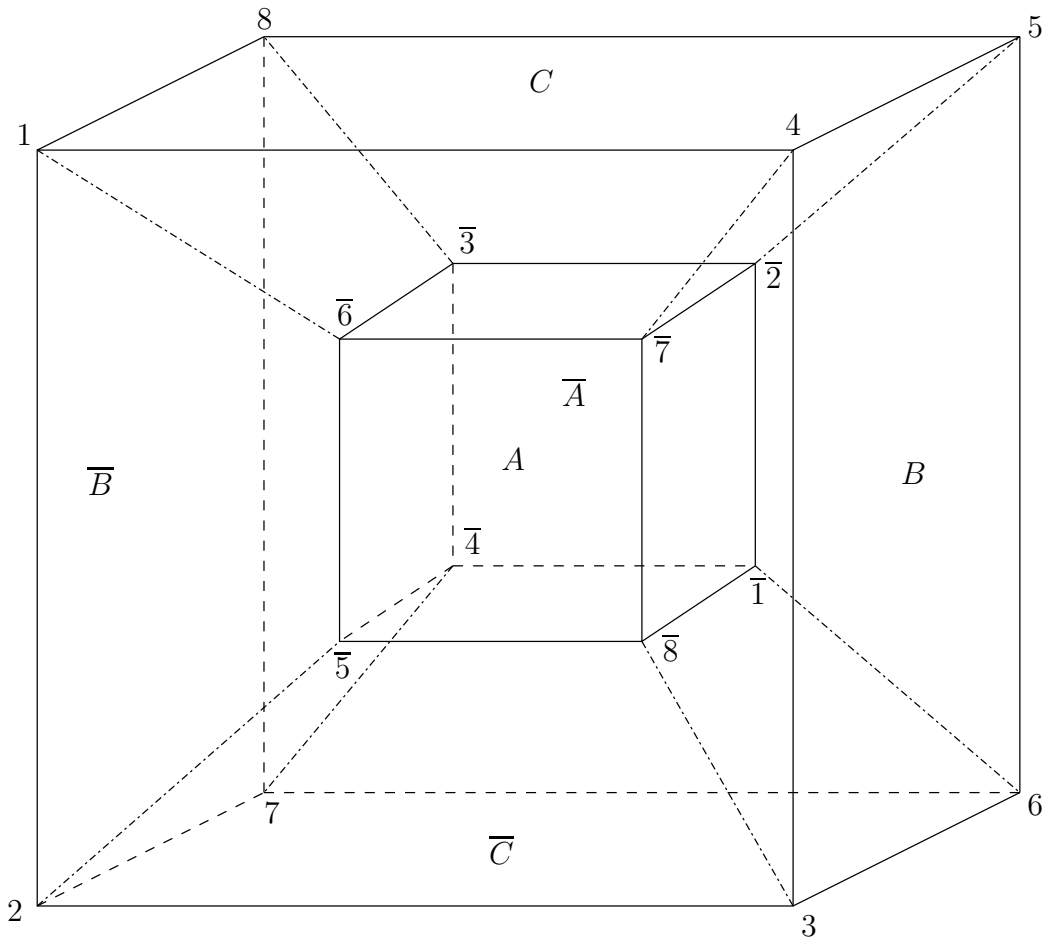


Abbildung 2: Hyperkubus

$$\begin{array}{llll}
1 = (A, \overline{B}, C, D) & \overline{1} = (\overline{A}, B, \overline{C}, \overline{D}) & 2 = (A, \overline{B}, \overline{C}, D) & \overline{2} = (\overline{A}, B, C, \overline{D}) \\
3 = (A, B, \overline{C}, D) & \overline{3} = (\overline{A}, \overline{B}, C, \overline{D}) & 4 = (A, B, C, D) & \overline{4} = (\overline{A}, \overline{B}, \overline{C}, \overline{D}) \\
5 = (\overline{A}, B, C, D) & \overline{5} = (A, \overline{B}, \overline{C}, \overline{D}) & 6 = (\overline{A}, B, \overline{C}, D) & \overline{6} = (A, \overline{B}, C, \overline{D}) \\
7 = (\overline{A}, \overline{B}, \overline{C}, D) & \overline{7} = (A, B, C, \overline{D}) & 8 = (\overline{A}, \overline{B}, C, D) & \overline{8} = (A, B, \overline{C}, \overline{D}).
\end{array}$$

Die Voraussetzung $\Delta(S) = F \times F$ bedeutet, dass Γ nur durch gerade Permutationen auf Z operiert. Die von den Involutionsen $i_W : W \rightarrow \overline{W}$ für $W \in \{A, B, C, D\}$ erzeugten Permutationen, sind die einzigen Permutationen von Z , die eine nicht-triviale Permutation auf $\Omega(Z/Y)$ induzieren.

Bemerkung: Jede Permutation auf Y induziert eine gerade Permutation auf Z (eine Transposition in Y induziert zwei Transpositionen in Z). Daher kann die Bedingung $\Delta(Z)$ trivial erfüllt sein, auch wenn Γ auf $\Delta(Y)$ nicht trivial operiert.

Jede Involution i_W entspricht einer Bewegung der Ecken des Hyperkubus längs einer Verbindungskante zwischen W und \overline{W} . Da aber Γ durch gerade Permutationen auf Z operiert, wird nur eine gerade Anzahl solcher Involutionsen auftreten, und somit können nur Ecken mit geradem Abstand (in Kanten gemessen) in derselben Bahn von Γ liegen. Mit der Numerierung der Ecken bedeutet dies, dass die Γ -Operation nur gerade in gerade und ungerade in ungerade Ecken überführen kann. Daher kann man die Menge $\Omega(Z/Y)$ in zwei Γ -Untermengen zerlegen:

$$\Omega(Z/Y) = Z' \sqcup Z'',$$

mit

$$Z' = \{1, \overline{1}, 3, \overline{3}, 5, \overline{5}, 7, \overline{7}\} \quad , \quad Z'' = \{2, \overline{2}, 4, \overline{4}, 6, \overline{6}, 8, \overline{8}\}.$$

Da die auf $\Omega(Z/Y)$ durch Komplementbildung definierte Involution eine Ecke x in der entgegengesetzte Ecke \overline{x} überführt, kann man auch $S(Z/Y)$ folgenderweise zerlegen:

$$S(Z/Y) = Y' \sqcup Y'',$$

mit

$$Y' = \{(1, \overline{1}), (3, \overline{3}), (5, \overline{5}), (7, \overline{7})\} \quad ; \quad Y'' = \{(2, \overline{2}), (4, \overline{4}), (6, \overline{6}), (8, \overline{8})\}.$$

Bemerke, dass $|Z'| = |Z''| = |Z| = 8$, $|Y'| = |Y''| = |Y| = 4$ und Z'/Y' ; Z''/Y'' sind wie Z/Y ebenfalls Γ -Überdeckungen von Grad 2. Betrachte jetzt die Menge $\Omega(Z'/Y')$ der Schnitte von Z'/Y' mit Involution gegeben durch Komplementbildung. Definiere $S(Z'/Y')$ analog wie $S(Z/Y)$ so, dass $S(Z'/Y') \leftarrow \Omega(Z'/Y')$ eine Γ -Überdeckung vom Grad 2 ist. Erinnere, dass jedes Element von $\Omega(Z'/Y')$ vier paarweise verschiedenen nicht entgegengesetzten Ecken in Z' entspricht, und somit eindeutig eine Zelle in Z (falls 0, 2 oder 4 Ecken auf den kleinen Kubus liegen) oder eine Ecke in Z'' (falls eine ungerade Anzahl von Ecken auf der kleine Kubus liegt) entspricht. Zum Beispiel $\{1, 3, 5, 7\} \in \Omega(Z'/Y')$ bestimmt die Zelle D , $\{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ die Zelle \overline{D} , $\{1, 3, 5, 7\}$ bestimmt die Ecke $6 \in Z''$ und $\{1, \overline{3}, \overline{5}, \overline{7}\}$ die Ecke $\overline{6}$. Es ist einfach zu sehen, dass falls ein Element $\omega \in \Omega(Z'/Y')$ eine Zelle (bzw. eine Ecke) bestimmt, so bestimmt auch jedes andere Element

in der Γ -Bahn von ω eine Zelle (bzw. eine Ecke). Man kann daher die Menge $\Omega(Z'/Y')$ schreiben als

$$\Omega(Z'/Y') = Z \sqcup Z''.$$

Da die Involution durch Komplementbildung auf $\Omega(Z'/Y')$ die natürliche, ursprünglich definierte Involution auf Z und Z'' induziert, gilt wieder

$$S(Z'/Y') = Y \sqcup Y''.$$

Durch diese Konstruktion auf Z'/Y' findet man somit wieder die Γ -Überdeckungen Z/Y und Z''/Y'' . Aus Symmetriegründen ist es einfach zu sehen, dass dieselbe Konstruktion, auf Z''/Y'' angewandt, die Γ -Überdeckungen Z/Y und Z'/Y' wiedergibt. Anders gesagt assoziiert diese Konstruktion eindeutig jedem Element von Z_1 ein Element in $\Omega(Z_2/Y_2)$ und ein Element in $\Omega(Z_3/Y_3)$, wobei $Z_i/Y_i \in \{Z/Y, Z'/Y', Z''/Y''\}$ und $Z_i/Y_i \neq Z_j/Y_j$ für $i \neq j$. Mit der früheren Bezeichnung der Elemente dieser Überdeckungen findet man folgende Korrespondenzen:

$$\begin{aligned} A &\leftrightarrow \{1, 3, \bar{5}, \bar{7}\} \leftrightarrow \{2, 4, \bar{6}, \bar{8}\}, & 1 &\leftrightarrow \{A, \bar{B}, C, D\} \leftrightarrow \{2, 4, \bar{6}, 8\}, \\ B &\leftrightarrow \{\bar{1}, 3, 5, \bar{7}\} \leftrightarrow \{\bar{2}, 4, 6, \bar{8}\}, & 3 &\leftrightarrow \{A, B, \bar{C}, D\} \leftrightarrow \{2, 4, 6, \bar{8}\}, \\ C &\leftrightarrow \{1, \bar{3}, 5, \bar{7}\} \leftrightarrow \{\bar{2}, 4, \bar{6}, 8\}, & 5 &\leftrightarrow \{\bar{A}, B, C, D\} \leftrightarrow \{\bar{2}, 4, 6, 8\}, \\ D &\leftrightarrow \{1, 3, 5, 7\} \leftrightarrow \{2, 4, 6, 8\}, & 7 &\leftrightarrow \{\overline{A, B, C}, D\} \leftrightarrow \{2, \bar{4}, 6, 8\}, \end{aligned} \quad (3)$$

$$2 \leftrightarrow \{A, \bar{B}, \bar{C}, D\} \leftrightarrow \{1, 3, \bar{5}, 7\},$$

$$4 \leftrightarrow \{A, B, C, D\} \leftrightarrow \{1, 3, 5, \bar{7}\},$$

$$6 \leftrightarrow \{\bar{A}, B, \bar{C}, D\} \leftrightarrow \{\bar{1}, 3, 5, 7\},$$

$$8 \leftrightarrow \{\overline{A, B}, C, D\} \leftrightarrow \{1, \bar{3}, 5, 7\}.$$

Hierbei werden die Korrespondenzen für die dazu transponierten Elementen durch Komplementbildung (d.h. die auf $\Omega(Z_i/Y_i)$ definierte Involution) gefunden.

Betrachte jetzt die Gruppe $\mathfrak{S}_{Z/Y} \simeq \mathfrak{S}_2^4 \rtimes \mathfrak{S}_4$ der Automorphismen von Z/Y . Jede Kopie von \mathfrak{S}_2 entspricht der Faser eines Elementes in Y . Setze $\mathfrak{S}_2 = \{1, -1\}$, wobei 1 die Identität ist und -1 die Vertauschung der zwei Elemente in der Faser entspricht. Falls Γ nur durch geraden Permutationen auf Z operiert, so liegt $\alpha_{Z/Y}(\Gamma)$ in der Untergruppe der gerade Permutationen in $\mathfrak{S}_2^4 \rtimes \mathfrak{S}_4$. Diese ist isomorph zu $\mathfrak{S}_2^3 \rtimes \mathfrak{S}_4$. In der Tat sind alle Elemente dieser Untergruppe von der Form $((\xi_1, \xi_2, \xi_3, \xi_4 = \xi_1\xi_2\xi_3), \sigma)$, mit $\xi_i \in \{1, -1\}$ für $i \in \{1, 2, 3\}$ und $\sigma \in \mathfrak{S}_4$. Man hat somit einen Gruppenhomomorphismus

$$\alpha_{Z/Y} : \Gamma \rightarrow \mathfrak{S}_2^3 \rtimes \mathfrak{S}_4.$$

Die oben definierte Konstruktion permutiert zyklisch $\alpha_{Z/Y}(\Gamma)$, $\alpha_{Z'/Y'}(\Gamma)$ und $\alpha_{Z''/Y''}(\Gamma)$, das heisst sie entspricht einen Automorphismus $\rho : \mathfrak{S}_2^3 \rtimes \mathfrak{S}_4 \rightarrow \mathfrak{S}_2^3 \rtimes \mathfrak{S}_4$ der Ordnung 3

($\rho^3 = \text{Id}$). Ziel dieser Arbeit ist es, diese Konstruktion besser zu verstehen, indem man sie für verschiedene S/S_0 durchführt. Eine interessante Frage ist zum Beispiel: "Wann gilt $Z/Y \simeq Z'/Y' \simeq Z''/Y''$?".

Das gilt zum Beispiel, wenn

$$\begin{array}{ccccccc} S/S_0 & = & F(\sqrt{a}) & \times & F(\sqrt{a}) & \times & F(\sqrt{a}) & \times & F(\sqrt{a}) \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ & & F & \times & F & \times & F & \times & F \end{array}$$

wobei $a \in F$ quadratfrei ist.

In diesem Fall sind die Elementen von

$$Z = X(S) = X(F(\sqrt{a})) \sqcup X(F(\sqrt{a})) \sqcup X(F(\sqrt{a})) \sqcup X(F(\sqrt{a})) \simeq X(F(\sqrt{a}))$$

eindeutig durch ihre Wirkung auf \sqrt{a} bestimmt. Das einzige nichttriviale Element in Z ist somit $\gamma : \sqrt{a} \rightarrow -\sqrt{a}$ so dass Γ nur durch den kanonischen Involuntionen $\gamma_{Z/Y}, \gamma_{Z'/Y'}, \gamma_{Z''/Y''}$ auf $Z/Y, Z'/Y', Z''/Y''$ operiert.

Betrachte die Involuntionen von $S \otimes_F F_{\text{sep}}$, die $S_0 \otimes_F F_{\text{sep}} \subset S \otimes_F F_{\text{sep}}$ invariant lassen, das heisst, diejenige für die gilt $-|_{S_0 \otimes_F F_{\text{sep}}} = \text{Id}|_{S_0 \otimes_F F_{\text{sep}}}$. Diese sind genau die Involuntionen, die auf $Z = \text{Hom}_F(S, F_{\text{sep}})$ eine Abbildung induzieren, die von den $i_W : W \rightarrow \overline{W}$ mit $W \in \{A, B, C, D\}$ erzeugt wird. Bezeichne mit $i_{\{WW'\}}$ die Komposition $i_W \circ i_{W'}$.

$Z/Y, Z'/Y'$ und Z''/Y'' können nur als Γ -Überdeckungen isomorph sein, wenn Y, Y' und Y'' als Γ -Mengen isomorph sind; und das ist nur der Fall, wenn die einzige mögliche Involution von $S \otimes_F F_{\text{sep}}$ die $S_0 \otimes_F F_{\text{sep}}$ invariant lässt, gerade die ist, die zu $i_{\{ABCD\}} = \gamma_{Z/Y} \in \text{End}(Z/Y)$ korrespondiert (jede andere Involution würde Y invariant lassen, aber auf Y' und Y'' eine nicht triviale Permutation induzieren, vgl. Bemerkung am Ende von Abschnitt 1.1). Diese Situation tritt genau dann ein, wenn die quadratische Erweiterung $S_0 \subset S$ durch Adjunktion desselben Elementes auf jeden Faktor der étale Algebra S_0 erfolgt. Dieses Element kann Ordnung 2 oder 4 über F haben.

Nimm jetzt an, dass die Γ -Operation ein Element von Y (z.B. (D, \overline{D})) invariant lässt; das heisst S_0 sei von der Form

$$S_0 = F \times L,$$

für eine étale Algebra L der Dimension 3 über F . In diesem Fall muss die quadratische Erweiterung $S_0 \subset S$ durch Adjunktion eines Elementes der Ordnung 2 über F erfolgen. Die einzigen noch möglichen Permutationen auf Z , werden dann durch die elementaren Transpositionen $(AB)(\overline{AB}), (AC)(\overline{AC})$ und $(BC)(\overline{BC})$ erzeugt. Schreibe nur noch A für $(A, \overline{A}), (AB)$ für $(AB)(\overline{AB})$ u.s.w. Betrachtet man noch die Korrespondenzen (3), so sieht man dass

$$(AB) \leftrightarrow (15) \leftrightarrow (26).$$

$$(AC) \leftrightarrow (35) \leftrightarrow (28)$$

$$(BC) \leftrightarrow (13) \leftrightarrow (68)$$

Mit den Identifizierungen

$$A \equiv 5 \equiv 2$$

$$B \equiv 1 \equiv 6$$

$$C \equiv 3 \equiv 8$$

$$D \equiv 7 \equiv 4$$

sind Z/Y , Z'/Y' und Z''/Y'' für jede mögliche Operation von Γ auf $\{A, B, C\}$ isomorph als Γ -Mengen.

Im allgemeinen Fall, (aber immer noch unter der Voraussetzung $S = S_0(\sqrt{a})$ für $a \in F$, $a \notin F^{\times 2}$), können alle Elemente untereinander permutiert werden, das heisst es kommen noch die folgende möglichen elementaren Transpositionen hinzu

$$(AD) \leftrightarrow (5\bar{7}) \leftrightarrow (6\bar{8}),$$

$$(BD) \leftrightarrow (1\bar{7}) \leftrightarrow (2\bar{8}),$$

$$(CD) \leftrightarrow (3\bar{7}) \leftrightarrow (2\bar{6})$$

Daraus erkennt man, dass die obigen Identifizierungen immer noch einen Isomorphismus von Γ -Mengen zwischen Z/Y und Z'/Y' definieren. Dieser Isomorphismus kann aber nicht mehr auf Z''/Y'' erweitert werden.

Nach diesen Überlegungen und Voraussagen betrachtet man nun verschiedene konkrete Fälle.

2 Fälle mit $\Delta(S_0) = F \times F$

2.1 $\alpha_Y(\Gamma) = \mathfrak{A}_4$

Dann ist

$$S/S_0 = N(\sqrt{a})/N,$$

für eine separable Erweiterung N von Grad 4 über F , deren Galois Abschluss eine zu \mathfrak{A}_4 isomorphe Galois-Gruppe besitzt.

Bemerkung: Falls F unendlich und L der Zerfällungskörper eines irreduziblen Polynoms $f(x)$ vierten Grades mit Koeffizienten in F ist, so gilt $\text{Gal}(L/F) = \mathfrak{A}_4$ genau dann, wenn die Determinante von $f(x)$ eine Quadratwurzel in F besitzt.

Sei also $f(x)$ separabel mit Nullstellen x_1, x_2, x_3, x_4 in L . Setze $N = F(x_1)$. Da $f(x)$ das Minimalpolynom von x_1 über F ist, ist $F \subset N$ eine Erweiterung von Grad vier mit Galois Abschluss $L = F(x_1, x_2, x_3, x_4)$. Die Elemente von $Z = X(S) = \text{Hom}_{F\text{-Alg}}(F(x_1, \sqrt{a}), F_{\text{sep}})$ sind durch das Bild von x_1 und \sqrt{a} in F_{sep} bestimmt. Für $v = (x_1, \sqrt{a})$ setze:

$$\begin{aligned}
A &= \xi_1(v) = (x_1, \sqrt{a}), & \bar{A} &= \bar{\xi}_1(v) = (x_1, -\sqrt{a}), \\
B &= \xi_2(v) = (x_2, \sqrt{a}), & \bar{B} &= \bar{\xi}_2(v) = (x_2, -\sqrt{a}), \\
C &= \xi_3(v) = (x_3, \sqrt{a}), & \bar{C} &= \bar{\xi}_3(v) = (x_3, -\sqrt{a}), \\
D &= \xi_4(v) = (x_4, \sqrt{a}), & \bar{D} &= \bar{\xi}_4(v) = (x_4, -\sqrt{a}).
\end{aligned}$$

Da $\alpha_Y(\Gamma) = \mathfrak{A}_4$, ist die Γ -Operation auf Z/Y durch die Elemente $\alpha = (ABC)(\overline{ABC})$, $\beta = (AB)(CD)(\overline{AB})(\overline{CD})$, und durch die natürliche Involution von Z/Y , $i = (A\bar{A})(B\bar{B})(C\bar{C})(D\bar{D})$ erzeugt. Mit der Zerlegung $\Omega(Z/Y)/S(Z/Y) = Z'/Y' \sqcup Z''/Y''$, und Numerierung der Elemente wie früher, findet man die folgende Tabelle

Tabelle 1:

$\phi(\Gamma)$	$\alpha(\Gamma)$	$\alpha'(\Gamma)$	$\alpha''(\Gamma)$
(x_1, x_2, x_3)	$(ABC)(\overline{ABC})$	$(135)(\overline{135})$	$(268)(\overline{268})$
$(x_1, x_2)(x_3, x_4)$	$(AB)(CD)(\overline{AB})(\overline{CD})$	$(15)(\overline{15})(37)(\overline{37})$	$(2\bar{2})(4)(6\bar{6})(8)$
$(\sqrt{a}, -\sqrt{a})$	$(A\bar{A})(B\bar{B})(C\bar{C})(D\bar{D})$	$(1\bar{1})(3\bar{3})(5\bar{5})(7\bar{7})$	$(2\bar{2})(4\bar{4})(6\bar{6})(8\bar{8})$,

wobei $\phi(\Gamma)$ das Bild von Γ in $\text{Aut}_F(L \otimes_F F_{\text{sep}})$ bezeichnet.

Mit den Korrespondenzen $A \leftrightarrow 5$, $B \leftrightarrow 1$, $C \leftrightarrow 3$, $D \leftrightarrow \bar{7}$ sind Z/Y und Z'/Y' isomorph als Γ -Mengen und damit auch

$$S/S_0 \simeq S'/S'_0.$$

Aus der vierten Spalte von Tabelle 2.1 sieht man sofort, dass das Element $(4, \bar{4}) \in Y''$ unter der Γ -Operation fixiert bleibt. Die übrigen drei Elemente werden dagegen zyklisch miteinander permutiert. Wenn man die Nullstellen der kubischen Resolvente und deren Wurzeln betrachtet, so sieht man, dass sie als Γ -Mengen isomorph zu $\{(2, \bar{2}); (6, \bar{6}); (8, \bar{8})\} \subset Y''$ bzw. $\{2, \bar{2}, 6, \bar{6}, 8, \bar{8}\} \subset Z''$ sind. Erinnerung, dass die Nullstellen der kubischen Resolvente aus den Nullstellen von $f(x)$ folgenderweise berechnet werden können

$$\begin{aligned}
z_1 &= (x_1 + x_2)(x_3 + x_4), \\
z_2 &= (x_1 + x_3)(x_2 + x_4), \\
z_3 &= (x_2 + x_3)(x_1 + x_4)
\end{aligned}$$

Wegen der Relation $x_1 + x_2 + x_3 + x_4 = 0$ findet man für die Wurzeln folgende Identitäten

$$\begin{aligned}
\sqrt{-z_1} &= (x_1 + x_2), & -\sqrt{-z_1} &= (x_3 + x_4), \\
\sqrt{-z_2} &= (x_1 + x_3), & -\sqrt{-z_2} &= (x_2 + x_4), \\
\sqrt{-z_3} &= (x_2 + x_3), & -\sqrt{-z_3} &= (x_1 + x_4)
\end{aligned}$$

Die Γ -Operation auf diesen Elementen ist somit:

Tabelle 2:

$\phi(\Gamma)$	$\phi_{\mathcal{R}^{1/2}}(\Gamma)$
(x_1, x_2, x_3)	$(\sqrt{-z_1}, \sqrt{-z_3}, \sqrt{-z_2})(-\sqrt{-z_1}, -\sqrt{-z_3}, -\sqrt{-z_2})$
$(x_1, x_2)(x_3, x_4)$	$(\sqrt{-z_2}, -\sqrt{-z_2})(\sqrt{-z_3}, -\sqrt{-z_3})$

Man sieht hier, dass die Korrespondenzen

$$\begin{array}{cccc} 4 \leftrightarrow \sqrt{a} & 8 \leftrightarrow \sqrt{-z_1}\sqrt{a} & 6 \leftrightarrow \sqrt{-z_2}\sqrt{a} & 2 \leftrightarrow \sqrt{-z_3}\sqrt{a} \\ \bar{4} \leftrightarrow -\sqrt{a} & \bar{8} \leftrightarrow -\sqrt{-z_1}\sqrt{a} & \bar{6} \leftrightarrow -\sqrt{-z_2}\sqrt{a} & \bar{2} \leftrightarrow -\sqrt{-z_3}\sqrt{a} \end{array}$$

einen Isomorphismus von Γ -Mengen definieren, das heisst

$$\begin{array}{ccc} S''/S_0'' \simeq F(\sqrt{a}) \times F(\sqrt{-z_1}) & & \\ \downarrow & \times & \downarrow \\ F & & F(z_1) \end{array}$$

2.2 $\alpha_Y(\Gamma) = \mathfrak{B}$

Die Klein'sche Vierergruppe \mathfrak{B} auf $\{1, 2, 3, 4\}$ ist

$$\mathfrak{B} = \{\text{Id}, (12)(34), (13)(24), (14)(23)\}$$

Setze

$$\begin{array}{c} S/S_0 = F(\sqrt{a}, \sqrt{b}, \sqrt{c}) \quad a, b, c \in F \setminus F^{\times 2} \\ \downarrow \\ F(\sqrt{a}, \sqrt{b}) \end{array}$$

Da die Erweiterung $F \subset F(\sqrt{a}, \sqrt{b})$ als separabel angenommen wird, kann man den Satz vom primitiven Element anwenden und

$$F(\sqrt{a}, \sqrt{b}) = F(\sqrt{a} + \sqrt{b})$$

schreiben. Die Elemente in $X(S) = \text{Hom}_{F\text{-Alg}}(S, F_{\text{sep}})$ sind bestimmt durch ihre Wirkung auf $v := (\sqrt{a} + \sqrt{b}, \sqrt{c})$ und werden folgenderweise mit den 8 Zellen des Hyperkubus auf folgende Weise identifiziert

$$\begin{array}{ll} A = \xi_1(v) = (-\sqrt{a} + \sqrt{b}, \sqrt{c}) & \bar{A} = \bar{\xi}_1(v) = (-\sqrt{a} + \sqrt{b}, -\sqrt{c}) \\ B = \xi_2(v) = (\sqrt{a} - \sqrt{b}, \sqrt{c}) & \bar{B} = \bar{\xi}_2(v) = (\sqrt{a} - \sqrt{b}, -\sqrt{c}) \\ C = \xi_3(v) = (-\sqrt{a} - \sqrt{b}, \sqrt{c}) & \bar{C} = \bar{\xi}_3(v) = (-\sqrt{a} - \sqrt{b}, -\sqrt{c}) \\ D = \xi_4(v) = (\sqrt{a} + \sqrt{b}, \sqrt{c}) & \bar{D} = \bar{\xi}_4(v) = (\sqrt{a} + \sqrt{b}, -\sqrt{c}) \end{array}$$

Die Γ -Operation auf S/S_0 ist durch die Elemente

$$\gamma_1 : \sqrt{a} \rightarrow -\sqrt{a} \quad ; \quad \gamma_2 : \sqrt{b} \rightarrow -\sqrt{b} \quad ; \quad \gamma_3 : \sqrt{c} \rightarrow -\sqrt{c}$$

Tabelle 3:

$\phi(\Gamma)$	$\phi''(\Gamma)$
$\gamma_1 : \sqrt{a} \rightarrow -\sqrt{a}$	$\sqrt{x_3} \rightarrow -\sqrt{x_3} ; \sqrt{x_1 x_2 x_3} \rightarrow -\sqrt{x_1 x_2 x_3}$
$\gamma_2 : \sqrt{b} \rightarrow -\sqrt{b}$	$\sqrt{x_1} \rightarrow -\sqrt{x_1} ; \sqrt{x_1 x_2 x_3} \rightarrow -\sqrt{x_1 x_2 x_3}$
$\gamma_3 : \sqrt{c} \rightarrow -\sqrt{c}$	$\sqrt{x_1} \rightarrow -\sqrt{x_1} ; \sqrt{x_3} \rightarrow -\sqrt{x_3} ; \sqrt{x_1 x_2 x_3} \rightarrow -\sqrt{x_1 x_2 x_3}$

Daraus folgt

$$\begin{aligned}
\sqrt{x_1} &= \sqrt{bc}, \\
\sqrt{x_2} &= \sqrt{c}, \\
\sqrt{x_3} &= \sqrt{ac}, \\
\sqrt{x_4} &= \sqrt{abc},
\end{aligned} \tag{4}$$

und

$$\begin{array}{cccc}
S''/S_0'' = F(\sqrt{c}) \times F(\sqrt{bc}) \times F(\sqrt{ac}) \times F(\sqrt{abc}) . \\
\begin{array}{cccc}
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
F & \times & F & \times & F & \times & F
\end{array}
\end{array}$$

Auch dieses Resultat kann mit den Nullstellen der kubischen Resolvente des Minimalpolynoms $f(x)$ von $\sqrt{a} + \sqrt{b}$ über F in Verbindung gebracht werden. Die Nullstellen von $f(x)$ sind

$$y_1 = \sqrt{a} + \sqrt{b} \quad ; \quad y_2 = -\sqrt{a} + \sqrt{b} \quad ; \quad y_3 = -\sqrt{a} - \sqrt{b} \quad ; \quad y_4 = \sqrt{a} - \sqrt{b}.$$

Die der kubischen Resolvente von $f(x)$ sind also

$$\begin{aligned}
z_1 &= (y_1 + y_2)(y_3 + y_4) = -4b, \\
z_2 &= (y_1 + y_3)(y_2 + y_4) = 0, \\
z_3 &= (y_2 + y_3)(y_1 + y_4) = -4a,
\end{aligned}$$

und die Wurzeln davon

$$\begin{aligned}
\sqrt{-z_1} &= (y_1 + y_2) = 2\sqrt{b}, & -\sqrt{-z_1} &= (y_3 + y_4) = -2\sqrt{b}, \\
\sqrt{-z_2} &= (y_1 + y_3) = 0, & -\sqrt{-z_2} &= (y_2 + y_4) = 0, \\
\sqrt{-z_3} &= (y_2 + y_3) = 2\sqrt{a}, & -\sqrt{-z_3} &= (y_1 + y_4) = -2\sqrt{a}.
\end{aligned}$$

Dann stimmen die Resultate (4) mit

$$\sqrt{x_1} = \frac{1}{2}\sqrt{-z_1}\sqrt{c} \quad ; \quad \sqrt{x_3} = \frac{1}{2}\sqrt{-z_3}\sqrt{c} \quad ; \quad \sqrt{x_4} = \frac{1}{4}\sqrt{z_1 z_3}\sqrt{c}$$

überein.

und

$$S''/S_0'' = F(\sqrt{x'}, \sqrt{y_1'}) \times F(\sqrt{x'}, \sqrt{y_2'})$$

$$\begin{array}{ccc} & | & \\ & F(\sqrt{x'}) & \times & F(\sqrt{x'}) \\ & | & & | \end{array}$$

schreiben. Setze

$$1 = (\sqrt{x}, \sqrt{y_1}) \quad \bar{1} = (\sqrt{x}, -\sqrt{y_1})$$

$$3 = (\sqrt{x}, \sqrt{y_2}) \quad \bar{3} = (\sqrt{x}, -\sqrt{y_2})$$

$$5 = (-\sqrt{x}, \sqrt{y_1}) \quad \bar{5} = (\sqrt{x}, -\sqrt{y_1})$$

$$7 = (-\sqrt{x}, \sqrt{y_2}) \quad \bar{7} = (\sqrt{x}, -\sqrt{y_2})$$

$$2 = (\sqrt{x'}, \sqrt{y_1'}) \quad \bar{2} = (\sqrt{x'}, -\sqrt{y_1'})$$

$$4 = (\sqrt{x'}, \sqrt{y_2'}) \quad \bar{4} = (\sqrt{x'}, -\sqrt{y_2'})$$

$$6 = (-\sqrt{x'}, \sqrt{y_1'}) \quad \bar{6} = (\sqrt{x'}, -\sqrt{y_1'})$$

$$8 = (-\sqrt{x'}, \sqrt{y_2'}) \quad \bar{8} = (\sqrt{x'}, -\sqrt{y_2'})$$

Durch Vergleich mit 2.3.1 erhält man die folgende Tabelle für die Γ -Operation auf S'/S_0' und S''/S_0'' :

Tabelle 5: -

$\phi(\Gamma)$	$\phi'(\Gamma)$	$\phi''(\Gamma)$
$(\sqrt{a} \leftrightarrow -\sqrt{a})$	$(\sqrt{x} \leftrightarrow -\sqrt{x}); (\sqrt{y_2} \leftrightarrow -\sqrt{y_2})$	$(\sqrt{y_1'} \leftrightarrow -\sqrt{y_1'})$
$(\sqrt{b_1} \leftrightarrow -\sqrt{b_1})$	$(\sqrt{x} \leftrightarrow -\sqrt{x})$	$(\sqrt{x'} \leftrightarrow -\sqrt{x'})$
$(\sqrt{b_2} \leftrightarrow -\sqrt{b_2})$	$(\sqrt{x} \leftrightarrow -\sqrt{x});$ $(\sqrt{y_1} \leftrightarrow -\sqrt{y_1});$ $(\sqrt{y_2} \leftrightarrow -\sqrt{y_2})$	$(\sqrt{x'} \leftrightarrow -\sqrt{x'});$ $(\sqrt{y_1'} \leftrightarrow -\sqrt{y_1'});$ $(\sqrt{y_2'} \leftrightarrow -\sqrt{y_2'})$

Daraus folgt:

$\sqrt{x} = \sqrt{ab_1b_2}$	$\sqrt{x'} = \sqrt{b_1b_2}$
$\sqrt{y_1} = \sqrt{b_2}$	$\sqrt{y_1'} = \sqrt{ab_2}$
$\sqrt{y_2} = \sqrt{ab_2}$	$\sqrt{y_2'} = \sqrt{b_2}$

2.3.2 Fall $b_1 = b_2 \neq \sqrt{a}$

Setze $b_1 = b_2 =: b$. Die Γ -Operation auf S/S_0 ist hier durch die Elemente $\sqrt{a} \leftrightarrow -\sqrt{a}$ und $\sqrt{b} \leftrightarrow -\sqrt{b}$ erzeugt. Es gilt

$$Z = X(S) = X(F(\sqrt{a}, \sqrt{b})) \sqcup X(F(\sqrt{a}, \sqrt{b})) = X_1 \sqcup X_2.$$

Mit $A, B \in X_1, C, D \in X_2$ und

$$\begin{aligned} A &= C = (\sqrt{a}, \sqrt{b}) & \bar{A} &= \bar{C} = (\sqrt{a}, -\sqrt{b}) \\ B &= D = (-\sqrt{a}, \sqrt{b}) & \bar{B} &= \bar{D} = (-\sqrt{a}, -\sqrt{b}) \end{aligned}$$

findet man die folgende Tabelle

Tabelle 6:

$\phi(\Gamma)$	$\alpha(\Gamma)$	$\alpha'(\Gamma)$	$\alpha''(\Gamma)$
$\sqrt{a} \leftrightarrow -\sqrt{a}$	$(AB)(CD)(\bar{A}\bar{B})(\bar{C}\bar{D})$	$(15)(\bar{1}\bar{5})(3\bar{7})(\bar{3}\bar{7})$	$(2\bar{2})(4)(6\bar{6})(8)$
$\sqrt{b} \leftrightarrow -\sqrt{b}$	$(A\bar{A})(B\bar{B})(C\bar{C})(D\bar{D})$	$(1\bar{1})(3\bar{3})(5\bar{5})(7\bar{7})$	$(2\bar{2})(4\bar{4})(6\bar{6})(8\bar{8})$

daraus folgt

$$S'/S'_0 \simeq S/S_0$$

und

$$S''/S''_0 = \underset{\substack{| \\ F}}{F(\sqrt{y_1})} \times \underset{\substack{| \\ F}}{F(\sqrt{y_2})} \times \underset{\substack{| \\ F}}{F(\sqrt{y_3})} \times \underset{\substack{| \\ F}}{F(\sqrt{y_4})}.$$

Mit

$$\begin{aligned} 2 &\leftrightarrow \sqrt{y_1} & \bar{2} &\leftrightarrow -\sqrt{y_1} \\ 4 &\leftrightarrow \sqrt{y_2} & \bar{4} &\leftrightarrow -\sqrt{y_2} \\ 6 &\leftrightarrow \sqrt{y_3} & \bar{6} &\leftrightarrow -\sqrt{y_3} \\ 8 &\leftrightarrow \sqrt{y_4} & \bar{8} &\leftrightarrow -\sqrt{y_4} \end{aligned}$$

sieht man aus Tabelle 2.3.2, dass

Tabelle 7: -

$\phi(\Gamma)$	$\alpha''(\Gamma)$
$\sqrt{a} \leftrightarrow -\sqrt{a}$	$\sqrt{y_1} \leftrightarrow -\sqrt{y_1}; \sqrt{y_3} \leftrightarrow -\sqrt{y_3}$
$\sqrt{b} \leftrightarrow -\sqrt{b}$	$\sqrt{y_1} \leftrightarrow -\sqrt{y_1}; \sqrt{y_2} \leftrightarrow -\sqrt{y_2}$
	$\sqrt{y_3} \leftrightarrow -\sqrt{y_3}; \sqrt{y_4} \leftrightarrow -\sqrt{y_4}$

und somit

$$\sqrt{y_1} = \sqrt{y_3} = \sqrt{ab} \quad ; \quad \sqrt{y_2} = \sqrt{y_4} = \sqrt{b}.$$

2.3.3 Fall $b_1 = b_2 = b = \sqrt{a}$

$$\begin{array}{ccc} S/S_0 = F(\sqrt{a}, \sqrt[4]{a}) \times F(\sqrt{a}, \sqrt[4]{a}) & & \\ \left| \quad \quad \quad \right. & & \left| \quad \quad \quad \right. \\ F(\sqrt{a}) & \times & F(\sqrt{a}) \end{array}$$

In diesem Fall gilt

$$Z = X(S) = X_1 \sqcup X_2$$

wobei

$$X_1 = X_2 = X(F(\sqrt{a}, \sqrt[4]{a})).$$

Setze

$$\begin{array}{ll} A = (\sqrt{a}, \sqrt[4]{a}), & \bar{A} = (\sqrt{a}, -\sqrt[4]{a}), \\ B = (-\sqrt{a}, i\sqrt[4]{a}), & \bar{B} = (-\sqrt{a}, -i\sqrt[4]{a}), \\ C = (\sqrt{a}, -\sqrt[4]{a}), & \bar{C} = (\sqrt{a}, \sqrt[4]{a}), \\ D = (-\sqrt{a}, -i\sqrt[4]{a}), & \bar{D} = (-\sqrt{a}, i\sqrt[4]{a}). \end{array}$$

$\phi(\Gamma)$ ist durch $\sqrt[4]{a} \leftrightarrow -\sqrt[4]{a}$ und $\sqrt[4]{a} \leftrightarrow i\sqrt[4]{a}$ erzeugt.

Bemerkung: $\sqrt[4]{a} \leftrightarrow i\sqrt[4]{a}$ impliziert automatisch $\sqrt{a} \leftrightarrow -\sqrt{a}$

Die Tabelle der Γ -Operation lautet dann

Tabelle 8: -

$\phi(\Gamma)$	$\alpha(\Gamma)$	$\alpha'(\Gamma)$	$\alpha''(\Gamma)$
$\sqrt[4]{a} \leftrightarrow -\sqrt[4]{a}$	$(A\bar{A})(B\bar{B})(C\bar{C})(D\bar{D})$	$(1\bar{1})(3\bar{3})(5\bar{5})(7\bar{7})$	$(2\bar{2})(4\bar{4})(6\bar{6})(8\bar{8})$
$\sqrt[4]{a} \leftrightarrow i\sqrt[4]{a}$	$(A\bar{B}\bar{A}B)(C\bar{D}\bar{C}D)$	$(13\bar{1}\bar{3})(57\bar{5}\bar{7})$	$(46\bar{4}\bar{6})(82\bar{8}\bar{2})$

Daraus sieht man dass

$$Z/Y \simeq Z'/Y' \simeq Z''/Y''$$

und somit

$$S/S_0 \simeq S'/S'_0 \simeq S''/S''_0.$$

2.4 $\alpha(\Gamma) = \text{Id} \times C_3$

Erinnere, dass der Fall

$$\begin{array}{ccc} S = F(\sqrt{y}) & \times & F(\sqrt[6]{x}\sqrt{y}) \\ \downarrow & & \downarrow \\ F & \times & F(\sqrt[3]{x}) \end{array}$$

schon in Abschnitt 3.1 begegnet wurde. Wenn man die gewöhnliche Konstruktion anwendet, so findet man

$$\begin{array}{c} S'/S'_0 \simeq S''/S''_0 = (\sqrt[4]{a}, \sqrt{b}) \\ \downarrow \\ F(\sqrt[4]{a}) \end{array}$$

Wir betrachten also den Fall

$$\begin{array}{ccc} S = F(\sqrt{b_1}) & \times & F(\sqrt[3]{a}, \sqrt{b_2}) \\ \downarrow & & \downarrow \\ F & \times & F(\sqrt[3]{a}) \end{array}$$

Wobei F eine primitive dritte Einheitswurzel σ enthält. Mit $v_1 = \sqrt{b_1}$ und $v_2 = (\sqrt[3]{a}, \sqrt{b_2})$ setze

$$\begin{array}{ll} D = \xi_4(v_1) = \sqrt{b_1} & \overline{D} = \overline{\xi_4}(v_1) = -\sqrt{b_1} \\ A = \xi_1(v_2) = (\sqrt[3]{a}, \sqrt{b_2}) & \overline{A} = \overline{\xi_1}(v_2) = (\sqrt[3]{a}, -\sqrt{b_2}) \\ B = \xi_2(v_2) = (\sigma\sqrt[3]{a}, \sqrt{b_2}) & \overline{B} = \overline{\xi_2}(v_2) = (\sigma\sqrt[3]{a}, -\sqrt{b_2}) \\ C = \xi_3(v_2) = (\sigma^2\sqrt[3]{a}, \sqrt{b_2}) & \overline{C} = \overline{\xi_3}(v_2) = (\sigma^2\sqrt[3]{a}, -\sqrt{b_2}) \end{array}$$

Die étale Algebra S besitzt zwei Involutionen, $i_1 : \sqrt{b_1} \rightarrow \sqrt{b_1}$ auf $F(\sqrt{b_1})$ und $i_2 : \sqrt{b_2} \rightarrow \sqrt{b_2}$ auf $F(\sqrt[3]{a}, \sqrt{b_2})$. Da aber per Voraussetzung Γ nur durch gerade Permutationen auf Z operiert, und i_2 auf Y die ungerade Permutation $(A\overline{A})(B\overline{B})(C\overline{C})$ auf Z induziert, müssen die beide Involutionen immer gleichzeitig auftreten und somit muss $\sqrt{b_1} = \sqrt{b_2} = \sqrt{b}$ gelten. Die Γ -Operation auf S/S_0 ist dann durch

$$\gamma : \sqrt[3]{a} \rightarrow \sigma\sqrt[3]{a} \quad \text{und} \quad i : \sqrt{b} \leftrightarrow -\sqrt{b}.$$

erzeugt. Die Tabelle der Γ -Operation auf Z/Y , Z'/Y' , Z''/Y'' ist dann

Tabelle 9:

$\phi(\Gamma)$	$\alpha(\Gamma)$	$\alpha'(\Gamma)$	$\alpha''(\Gamma)$
γ	$(ABC)(\overline{ABC})$	$(135)(\overline{135})$	$(268)(\overline{268})$
i	$(A\overline{A})(B\overline{B})(C\overline{C})(D\overline{D})$	$(1\overline{1})(3\overline{3})(5\overline{5})(7\overline{7})$	$(2\overline{2})(4\overline{4})(6\overline{6})(8\overline{8})$

Die Korrespondenzen

$$\begin{array}{ll}
 A \longleftrightarrow 5 \longleftrightarrow 2 & \bar{A} \longleftrightarrow \bar{5} \longleftrightarrow \bar{2} \\
 B \longleftrightarrow 1 \longleftrightarrow 6 & \bar{B} \longleftrightarrow \bar{1} \longleftrightarrow \bar{6} \\
 C \longleftrightarrow 3 \longleftrightarrow 8 & \bar{C} \longleftrightarrow \bar{3} \longleftrightarrow \bar{8} \\
 D \longleftrightarrow 7 \longleftrightarrow 4 & \bar{D} \longleftrightarrow \bar{7} \longleftrightarrow \bar{4}
 \end{array}$$

definieren die Isomorphismen der Γ -Mengen

$$Z/Y \simeq Z'/Y' \simeq Z''/Y'' \simeq Z/Y$$

und mit der Antiäquivalenz $\text{Et}_F \equiv \text{Sets}_\Gamma$ erhält man also

$$S/S_0 \simeq S'/S'_0 \simeq S''/S''_0 \simeq S/S_0.$$

3 Fälle mit $\Delta(S_0) \neq F \times F$

3.1 $\alpha_Y(\Gamma) = \mathfrak{S}_4$

Setze

$$S/S_0 = N(\sqrt{a})/N$$

für eine separable Erweiterung N von Grad 4 über F deren Galois Abschluss eine zu \mathfrak{S}_4 isomorphe Galois-Gruppe besitzt.

Bemerkung: Falls F unendlich und L der Zerfällungskörper eines irreduziblen Polynoms $f(x)$ vierten Grades mit Koeffizienten in F ist, so gilt $\text{Gal}(L/F) = \mathfrak{S}_4$ genau dann, wenn die Determinante von $f(x)$ keine Quadratwurzel in F besitzt.

Für x_1 Nullstelle eines Polynoms $f(x)$ wie in der Bemerkung, setze $N = F(x_1)$; es sei $L = F(x_1, x_2, x_3, x_4)$ der Galois-Abschluss von N . Für $v = (x_1, \sqrt{a})$ setze

$$\begin{array}{ll}
 A = \xi_1(v) = (x_1, \sqrt{a}), & \bar{A} = \bar{\xi}_1(v) = (x_1, -\sqrt{a}), \\
 B = \xi_2(v) = (x_2, \sqrt{a}), & \bar{B} = \bar{\xi}_2(v) = (x_2, -\sqrt{a}), \\
 C = \xi_3(v) = (x_3, \sqrt{a}), & \bar{C} = \bar{\xi}_3(v) = (x_3, -\sqrt{a}), \\
 D = \xi_4(v) = (x_4, \sqrt{a}), & \bar{D} = \bar{\xi}_4(v) = (x_4, -\sqrt{a}).
 \end{array}$$

Man findet folgende Tabelle für die Γ -Operation:

Tabelle 10:

$\phi(\Gamma)$	$\alpha(\Gamma)$	$\alpha'(\Gamma)$	$\alpha''(\Gamma)$
(x_1, x_2, x_3, x_4)	$(ABCD)(\overline{ABCD})$	$(13\overline{7}5)(\overline{13}7\overline{5})$	$(2\overline{8}28)(6\overline{6})$
(x_1, x_2)	$(AB)(\overline{AB})$	$(15)(\overline{15})$	$(26)(\overline{26})$
(x_1, x_3)	$(AC)(\overline{AC})$	$(35)(\overline{35})$	$(28)(\overline{28})$
(x_2, x_3)	$(BC)(\overline{BC})$	$(13)(\overline{13})$	$(68)(\overline{68})$
(x_3, x_4)	$(CD)(\overline{CD})$	$(3\overline{7})(\overline{37})$	$(2\overline{6})(\overline{26})$
(x_2, x_4)	$(BD)(\overline{BD})$	$(1\overline{7})(\overline{17})$	$(2\overline{8})(\overline{28})$
(x_1, x_4)	$(AD)(\overline{AD})$	$(5\overline{7})(\overline{57})$	$(6\overline{8})(\overline{68})$
$(\sqrt{a}, -\sqrt{a})$	$(AA)(BB)(C\overline{C})(D\overline{D})$	$(1\overline{1})(3\overline{3})(5\overline{5})(7\overline{7})$	$(2\overline{2})(4\overline{4})(6\overline{6})(8\overline{8})$

Mit $A \leftrightarrow 5, B \leftrightarrow 1, C \leftrightarrow 3, D \leftrightarrow \overline{7}$ sind Z/Y und Z'/Y' isomorph. $\alpha_{Y''}(\Gamma)$ fixiert das Element $(4, \overline{4}) \in Y''$ und operiert wie \mathfrak{S}_3 auf $(2, \overline{2}), (6, \overline{6}), (8, \overline{8})$, somit setzt man

$$S''/S_0'' = F(\sqrt{a}) \times F(\sqrt{z}\sqrt{a}).$$

$$\begin{array}{ccc} & \downarrow & \downarrow \\ & F & \times & F(z) \end{array}$$

Man kann $z = z_1$ als Wurzel der kubischen Resolvente von $f(x)$ interpretieren. Dann ist $z = (x_1 + x_2)(x_3 + x_4)$ und

$$(x_1 + x_2) = \sqrt{-z} \quad ; \quad (x_3 + x_4) = -\sqrt{-z}.$$

Seien z_2, z_3 die übrigen Nullstellen der kubischen Resolvente

$$z_2 = (x_1 + x_3)(x_2 + x_4)$$

$$z_3 = (x_2 + x_3)(x_1 + x_4)$$

Setze:

$$4 = \sqrt{a} \quad \overline{4} = -\sqrt{a}$$

$$8 = \sqrt{-z_1}\sqrt{a} = (x_1 + x_2)\sqrt{a} \quad \overline{8} = -\sqrt{-z_1}\sqrt{a} = (x_3 + x_4)\sqrt{a}$$

$$6 = \sqrt{-z_2}\sqrt{a} = (x_1 + x_3)\sqrt{a} \quad \overline{6} = -\sqrt{-z_2}\sqrt{a} = (x_2 + x_4)\sqrt{a}$$

$$2 = \sqrt{-z_3}\sqrt{a} = (x_2 + x_3)\sqrt{a} \quad \overline{2} = -\sqrt{-z_3}\sqrt{a} = (x_1 + x_4)\sqrt{a}$$

Es ist leicht nachzuprüfen, dass diese Korrespondenzen einen Isomorphismus von Γ -Mengen definieren.

3.2 $\alpha_y(\Gamma) = D_4$

Dies ist ein Spezialfall des vorangehenden Fall, indem man $f(x)$ von der Form

$$f(x) = (x^2 - a)^2 - b \quad \text{mit} \quad b > a^2$$

wählt. In diesem Fall sind die Nullstellen von $f(x)$ von der Form

$$x_1 = -x_3 = \sqrt{a + \sqrt{b}} \quad ; \quad x_2 = -x_4 = \sqrt{a - \sqrt{b}}.$$

Definiere

$$\alpha := \sqrt{a + \sqrt{b}} \quad ; \quad \beta := \sqrt{a - \sqrt{b}}.$$

Für i eine primitive vierte Einheitswurzel und F so, dass $i \notin F$ setze

$$\begin{array}{c} S/S_0 = F(\alpha, \sqrt{c}) . \\ | \\ F(\alpha) \end{array}$$

$F(\alpha)$ hat Galois Abschluss $L = F(\alpha, \beta)$ und $|\text{Gal}(L/F)| = [L : F] = 8$. Da $\text{Gal}(L/F) \subset \mathfrak{S}_4$ und die einzigen Untergruppen von \mathfrak{S}_4 der Ordnung 8 isomorph zu D_4 sind, folgt dass

$$\phi_Y(\Gamma) = \text{Gal}(L/F) \simeq D_4.$$

Bemerkung: Die Symmetriegruppe \mathfrak{S}_4 enthält nur 3 Untergruppen der Ordnung 8; diese sind zur Diedergruppe D_4 isomorph. Es sind genau die Untergruppen, die eine Partition von $\{A, B, C, D\}$ in zweielementige Untermengen erhalten. Will man zum Beispiel erreichen, dass die Partition $\{AC\}\{BD\}$ erhalten bleibt, so sieht die zu D_4 isomorphe Untergruppe von \mathfrak{S}_4 folgendermassen aus:

$$\begin{aligned} U_{\{AC\}\{BD\}} = \\ \{\text{Id}; (AC); (BD); (AB)(CD); (AC)(BD); (AD)(BC); (ABCD); (ADCB)\} \simeq D_4 \end{aligned}$$

Als erzeugende Elemente kann man $\tau = (AC)$ und $\sigma = (ABCD)$ wählen, so dass

$$D_4 = \langle \sigma, \tau \rangle = \{\text{Id}, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}.$$

Mit $v = (\alpha, \sqrt{c})$ setze

$$\begin{aligned} A &= \xi_1(v) = (\alpha, \sqrt{c}) \quad ; \quad \bar{A} = \bar{\xi}_1(v) = (\alpha, -\sqrt{c}) \\ B &= \xi_2(v) = (\beta, \sqrt{c}) \quad ; \quad \bar{B} = \bar{\xi}_2(v) = (\beta, -\sqrt{c}) \\ C &= \xi_3(v) = (-\alpha, \sqrt{c}) \quad ; \quad \bar{C} = \bar{\xi}_3(v) = (-\alpha, -\sqrt{c}) \\ D &= \xi_4(v) = (-\beta, \sqrt{c}) \quad ; \quad \bar{D} = \bar{\xi}_4(v) = (-\beta, -\sqrt{c}) \end{aligned}$$

Die erzeugenden Elemente von $\phi_Y(\Gamma)$ sind dann

$$\begin{array}{ll} \sigma : \alpha \mapsto \beta \quad , & \tau : \alpha \mapsto -\alpha . \\ & \beta \mapsto -\alpha \quad \quad \beta \mapsto \beta \end{array}$$

Für die Γ -Operation ergibt sich die folgende Tabelle:

Tabelle 11:

$\phi(\Gamma)$	$\alpha(\Gamma)$	$\alpha'(\Gamma)$	$\alpha''(\Gamma)$
σ	$(ABCD)(\overline{ABCD})$	$(13\overline{75})(\overline{1375})$	$(2\overline{828})(6\overline{6})$
σ^2	$(AC)(BD)(\overline{AC})(\overline{BD})$	$(1\overline{7})(\overline{17})(35)(\overline{35})$	$(2\overline{2})(8\overline{8})$
σ^3	$(ADCB)(\overline{ADCB})$	$(15\overline{73})(\overline{1573})$	$(28\overline{28})(6\overline{6})$
τ	$(AC)(\overline{AC})$	$(35)(\overline{35})$	$(28)(\overline{28})$
$\sigma\tau$	$(AD)(BC)(\overline{AD})(\overline{BC})$	$(13)(\overline{13})(5\overline{7})(\overline{57})$	$(8\overline{8})(6\overline{6})$
$\sigma^2\tau$	$(BD)(\overline{BD})$	$(1\overline{7})(\overline{17})$	$(2\overline{8})(\overline{28})$
$\sigma^3\tau$	$(AB)(CD)(\overline{AB})(\overline{CD})$	$(15)(\overline{37})(\overline{15})(\overline{37})$	$(2\overline{2})(6\overline{6})$
$\sqrt{c} \rightarrow -\sqrt{c}$	$(A\overline{A})(B\overline{B})(C\overline{C})(D\overline{D})$	$(1\overline{1})(3\overline{3})(5\overline{5})(7\overline{7})$	$(2\overline{2})(4\overline{4})(6\overline{6})(8\overline{8})$

Mit den Korrespondenzen $A \leftrightarrow 5$, $B \leftrightarrow 1$, $C \leftrightarrow 3$, $D \leftrightarrow \overline{7}$ sieht man, dass

$$Z/Y \simeq Z'/Y' \not\simeq Z''/Y'',$$

und somit auch

$$S/S_0 \simeq S'/S'_0 \not\simeq S''/S''_0.$$

Die Γ -Operation auf Y'' lässt die Elemente $(6, \overline{6})$ und $(4, \overline{4})$ fix, so dass

$$S''_0 = F \times F \times F(\sqrt{x}).$$

Ausserdem operiert Γ auf den Elementen $2, 8, \overline{2}, \overline{8}$ wie D_4 und erhält die Partition $\{2, \overline{2}\}\{8, \overline{8}\}$. Setze $\alpha' = 8$, $-\alpha' = \overline{8}$, $\beta' = 2$, $-\beta' = \overline{2}$ und

$$\begin{aligned} \sigma' : \alpha' &\mapsto \beta' & \tau' : \alpha' &\mapsto -\alpha' \\ \beta' &\mapsto -\alpha' & \beta' &\mapsto \beta' \end{aligned}$$

Dann liest man aus Tabelle 3.2, dass σ und τ die Operationen σ' und $\sigma'^3\tau'$ auf S'' induzieren:

$$\begin{aligned} \tau &= (\alpha, -\alpha) \Rightarrow \sigma'^3\tau' = (\alpha', \beta')(-\alpha', -\beta') . \\ \sigma^2\tau &= (\beta, -\beta) \Rightarrow \sigma'\tau' = (\alpha', -\beta')(-\alpha', \beta') \\ \sigma\tau &= (\alpha, -\beta)(-\alpha, \beta) \Rightarrow \tau' = (\alpha', -\alpha') \\ \sigma^3\tau &= (\alpha, \beta)(-\alpha, -\beta) \Rightarrow \sigma'^2\tau' = (\beta', -\beta') \end{aligned}$$

Betrachtet man wie früher die Nullstellen der kubischen Resolvente von $f(x)$, so sieht man dass

$$\begin{aligned} z_1 &= (x_1 + x_2)(x_3 + x_4) = -(\alpha + \beta)^2 \\ z_2 &= (x_1 + x_3)(x_2 + x_4) = 0 \\ z_3 &= (x_2 + x_3)(x_1 + x_4) = -(\alpha - \beta)^2 \end{aligned}$$

und

$$\begin{aligned}\sqrt{-z_1} &= \alpha + \beta & -\sqrt{-z_1} &= -\alpha - \beta \\ \sqrt{-z_2} &= \alpha - \alpha & -\sqrt{-z_2} &= \beta - \beta \\ \sqrt{-z_3} &= -\alpha + \beta & -\sqrt{-z_3} &= \alpha - \beta.\end{aligned}$$

Γ induziert dann die folgende Operation auf diesen Elementen

$$\begin{aligned}\sigma &\rightarrow (\sqrt{-z_1}, \sqrt{-z_3}, -\sqrt{-z_1}, -\sqrt{-z_3}) \quad , \quad (\sqrt{-z_2}, -\sqrt{-z_2}) \\ \tau &\rightarrow (\sqrt{-z_1}, \sqrt{-z_3})(-\sqrt{-z_1}, -\sqrt{-z_3}).\end{aligned}$$

Bemerkung: Da $z_2 = 0$ ist, kann man die kubische Resolvente durch z dividieren, so dass dann z_1 und z_3 von Grad 2 über F sind. Man unterscheidet aber auch in diesem Fall zwischen positiver und negativer Wurzel von $-z_2$. Die nicht triviale Permutation $(\sqrt{-z_2}, -\sqrt{-z_2})$ ist durch (α, β) induziert, oder in äquivalenter Weise durch $(\sqrt{b}, -\sqrt{b})$.

Die Korrespondenzen

$$\begin{aligned}4 &= \sqrt{c} & \bar{4} &= -\sqrt{c} \\ 6 &= \sqrt{bc} & \bar{6} &= -\sqrt{bc} \\ 2 &= \sqrt{-z_3}\sqrt{c} & \bar{2} &= -\sqrt{-z_3}\sqrt{c} \\ 8 &= \sqrt{-z_1}\sqrt{c} & \bar{8} &= -\sqrt{-z_1}\sqrt{c}\end{aligned}$$

definieren einen Isomorphismus von Γ -Mengen, und man kann

$$\begin{array}{ccccc}S''/S_0'' \simeq & F(\sqrt{c}) & \times & F(\sqrt{bc}) & \times & F(\sqrt{-z_1}\sqrt{c}) \\ & \downarrow & & \downarrow & & \downarrow \\ & F & \times & F & \times & F(z_1)\end{array}$$

schreiben.

3.3 $\alpha_Y(\Gamma) = C_4$

Nimm an, dass F eine primitive vierte Einheitswurzel i enthält und setze

$$\begin{array}{c}S/S_0 = F(\sqrt[4]{a}, \sqrt{b}) \\ \downarrow \\ F(\sqrt[4]{a})\end{array}$$

Die zyklische Operation auf Y ist durch $\rho : \sqrt[4]{a} \mapsto i \cdot \sqrt[4]{a}$ erzeugt. Setze

$$\begin{aligned} A &= (\sqrt[4]{a}, \sqrt{b}) \quad ; \quad \bar{A} = (\sqrt[4]{a}, -\sqrt{b}) \\ B &= (i\sqrt[4]{a}, \sqrt{b}) \quad ; \quad \bar{B} = (i\sqrt[4]{a}, -\sqrt{b}) \\ C &= (-\sqrt[4]{a}, \sqrt{b}) \quad ; \quad \bar{C} = (-\sqrt[4]{a}, -\sqrt{b}) \\ D &= (-i\sqrt[4]{a}, \sqrt{b}) \quad ; \quad \bar{D} = (-i\sqrt[4]{a}, -\sqrt{b}) \end{aligned}$$

dann hat man

Tabelle 12:

$\phi(\Gamma)$	$\alpha(\Gamma)$	$\alpha'(\Gamma)$	$\alpha''(\Gamma)$
ρ	$(ABCD)(\bar{A}\bar{B}\bar{C}\bar{D})$	$(13\bar{7}5)(\bar{1}\bar{3}\bar{7}\bar{5})$	$(2\bar{8}\bar{2}8)(6\bar{6})$
ρ^2	$(AC)(\bar{A}\bar{C})(BD)(\bar{B}\bar{D})$	$(1\bar{7})(\bar{1}\bar{7})(35)(\bar{3}\bar{5})$	$(2\bar{2})(8\bar{8})$
ρ^3	$(ADCB)(\bar{A}\bar{D}\bar{C}\bar{B})$	$(15\bar{7}3)(\bar{1}\bar{5}\bar{7}\bar{3})$	$(2\bar{8}\bar{2}8)(6\bar{6})$
$\sqrt{b} \leftrightarrow -\sqrt{b}$	$(A\bar{A})(B\bar{B})(C\bar{C})(D\bar{D})$	$(1\bar{1})(3\bar{3})(5\bar{5})(7\bar{7})$	$(2\bar{2})(4\bar{4})(6\bar{6})(8\bar{8})$

Daraus sieht man, dass

$$Z/Y \simeq Z'/Y' \not\simeq Z''/Y''$$

und somit auch

$$S/S_0 \simeq S'/S'_0 \not\simeq S''/S''_0$$

gilt. Weiter kann man bemerken, dass Γ trivial auf den Elementen $(4, \bar{4}), (6, \bar{6}) \in Y''$ operiert und $2, \bar{8}, \bar{2}, 8$ zyklisch permutiert. Daher schreibt man

$$\begin{array}{c} S''/S''_0 = F(\sqrt{\alpha}) \times F(\sqrt{\beta}) \times F(\sqrt[4]{x}) \\ \quad \quad \quad \downarrow \quad \quad \quad \downarrow \quad \quad \quad \downarrow \\ \quad \quad \quad F \quad \times \quad F \quad \times \quad F(\sqrt{x}). \end{array}$$

Mit

$$\begin{aligned} 4 &= \sqrt{\alpha} & \bar{4} &= -\sqrt{\alpha} \\ 6 &= \sqrt{\beta} & \bar{6} &= -\sqrt{\beta} \\ 2 &= i\sqrt[4]{x} & \bar{2} &= -i\sqrt[4]{x} \\ 8 &= \sqrt[4]{x} & \bar{8} &= -\sqrt[4]{x} \end{aligned}$$

ergeben sich aus Tabelle 3.3 folgende Relationen:

$$\begin{aligned} \sqrt{\alpha} &= \sqrt{b} \\ \sqrt{\beta} &= \sqrt{ab} \\ \sqrt[4]{x} &= \sqrt[4]{a}\sqrt{b}. \end{aligned}$$

Somit ist

$$S''/S_0'' = F(\sqrt{b}) \times F(\sqrt{ab}) \times F(\sqrt[4]{a}\sqrt{b})$$

$$\begin{array}{ccc} \downarrow & & \downarrow \\ F & \times & F \\ & & \downarrow \\ & & F(\sqrt{a}). \end{array}$$

Auch in diesem Fall kann man die Γ -Operation auf S''/S_0'' auf eine Operation auf den Nullstellen der kubischen Resolvente von $f(x) = x^4 - a$ zurückführen. Es gilt

$$\begin{aligned} z_1 &= -\sqrt{a}(1+i)^2, \\ z_2 &= 0, \\ z_3 &= -\sqrt{a}(1-i)^2 \end{aligned}$$

und

$$\begin{aligned} \sqrt{-z_1} &= \sqrt[4]{a}(1+i), & -\sqrt{-z_1} &= -\sqrt[4]{a}(1+i), \\ \sqrt{-z_2} &= \sqrt[4]{a} - \sqrt[4]{a}, & -\sqrt{-z_2} &= i\sqrt[4]{a} - i\sqrt[4]{a}, \\ \sqrt{-z_3} &= i\sqrt[4]{a}(1+i), & -\sqrt{-z_3} &= -i\sqrt[4]{a}(1+i) \end{aligned}$$

Da $i \in F$, ist auch $(1+i) \in F$, und somit

$$F(\sqrt{a}(1+i)^2) \simeq F(\sqrt{a}) \quad ; \quad F(\sqrt[4]{a}(1+i)) \simeq F(\sqrt[4]{a}).$$

Man kann also den Faktor $(1+i)$ wegdividieren; mit $t' = t/(1+i)$ setze:

$$\begin{aligned} 2 &= \sqrt{-z_3'}\sqrt{b} = i\sqrt[4]{a}\sqrt{b} & \bar{2} &= -\sqrt{-z_3'}\sqrt{b} = -i\sqrt[4]{a}\sqrt{b} \\ 8 &= \sqrt{-z_1'}\sqrt{b} = \sqrt[4]{a}\sqrt{b} & \bar{8} &= -\sqrt{-z_1'}\sqrt{b} = -\sqrt[4]{a}\sqrt{b} \end{aligned}$$

Was mit dem früheren Resultat übereinstimmt.

3.4 $\alpha_Y(\Gamma) = C_2 \not\subset \mathfrak{B}$

Man betrachtet hier nur den Fall, in dem S durch Adjunktion eines einzigen Elementes \sqrt{b} zu S_0 entsteht. Andere Fälle treten während der Berechnung von $\alpha_Y(\Gamma) = C_2 \times C_2 \not\subset \mathfrak{B}$, D_4 und C_4 auf. Es ist also:

$$S/S_0 = (F(\sqrt{b}) \times F(\sqrt{b}) \times F(\sqrt{a}, \sqrt{b})).$$

$$\begin{array}{ccc} \downarrow & & \downarrow \\ F & \times & F \\ & & \downarrow \\ & & F(\sqrt{a}) \end{array}$$

$$S''/S_0'' = F(\sqrt{\alpha'}, \sqrt{\beta'}) \times F(\sqrt{\gamma'}, \sqrt{\delta'}) \cdot$$

$$\begin{array}{ccc} & | & | \\ & F(\sqrt{\alpha}) & \times & F(\sqrt{\gamma}) \end{array}$$

Mit den Korrespondenzen

$$\begin{aligned} 1 &= (\sqrt{\alpha}, \sqrt{\beta}), & \bar{1} &= (\sqrt{\alpha}, -\sqrt{\beta}), \\ 3 &= (\sqrt{\gamma}, \sqrt{\delta}), & \bar{3} &= (\sqrt{\gamma}, -\sqrt{\delta}), \\ 5 &= (-\sqrt{\alpha}, \sqrt{\beta}), & \bar{5} &= (-\sqrt{\alpha}, -\sqrt{\beta}), \\ 7 &= (-\sqrt{\gamma}, \sqrt{\delta}), & \bar{7} &= (-\sqrt{\gamma}, -\sqrt{\delta}), \\ \\ 2 &= (\sqrt{\alpha'}, \sqrt{\beta'}), & \bar{2} &= (\sqrt{\alpha'}, -\sqrt{\beta'}), \\ 4 &= (\sqrt{\gamma'}, \sqrt{\delta'}), & \bar{4} &= (\sqrt{\gamma'}, -\sqrt{\delta'}), \\ 6 &= (-\sqrt{\alpha'}, \sqrt{\beta'}), & \bar{6} &= (-\sqrt{\alpha'}, -\sqrt{\beta'}), \\ 8 &= (-\sqrt{\gamma'}, \sqrt{\delta'}), & \bar{8} &= (-\sqrt{\gamma'}, -\sqrt{\delta'}), \end{aligned}$$

findet man aus Tabelle 3.5.1

Tabelle 15:

$\phi(\Gamma)$	$\phi'(\Gamma)$	$\phi''(\Gamma)$
$\gamma_1 : \sqrt{a} \leftrightarrow -\sqrt{a}$	$\sqrt{\alpha} \leftrightarrow -\sqrt{\alpha}$	$\sqrt{\alpha'} \leftrightarrow -\sqrt{\alpha'}$
$\gamma_2 : \sqrt{b} \leftrightarrow -\sqrt{b}$	$\sqrt{\gamma} \leftrightarrow -\sqrt{\gamma}$ $\sqrt{\delta} \leftrightarrow -\sqrt{\delta}$	$\sqrt{\alpha'} \leftrightarrow -\sqrt{\alpha'}$ $\sqrt{\beta'} \leftrightarrow -\sqrt{\beta'}$
$\gamma'_1 : \sqrt{x} \leftrightarrow -\sqrt{x}$	$\sqrt{\alpha} \leftrightarrow -\sqrt{\alpha}$ $\sqrt{\gamma} \leftrightarrow -\sqrt{\gamma}$	$\sqrt{\alpha'} \leftrightarrow -\sqrt{\alpha'}$ $\sqrt{\gamma'} \leftrightarrow -\sqrt{\gamma'}$
$\gamma'_2 : \sqrt{y} \leftrightarrow -\sqrt{y}$	$\sqrt{\alpha} \leftrightarrow -\sqrt{\alpha}$ $\sqrt{\beta} \leftrightarrow -\sqrt{\beta}$ $\sqrt{\gamma} \leftrightarrow -\sqrt{\gamma}$ $\sqrt{\delta} \leftrightarrow -\sqrt{\delta}$	$\sqrt{\alpha'} \leftrightarrow -\sqrt{\alpha'}$ $\sqrt{\beta'} \leftrightarrow -\sqrt{\beta'}$ $\sqrt{\gamma'} \leftrightarrow -\sqrt{\gamma'}$ $\sqrt{\delta'} \leftrightarrow -\sqrt{\delta'}$

und

$$\begin{aligned}\Lambda_2(Y) &= \\ &= \left\{ \{\sqrt{a}, -\sqrt{a}\}, \{\sqrt{b}, -\sqrt{b}\}, \{\sqrt{a}, \sqrt{b}\}, \{-\sqrt{a}, -\sqrt{b}\}, \{-\sqrt{a}, \sqrt{b}\}, \{\sqrt{a}, -\sqrt{b}\} \right\} \\ &= \{\sqrt{-z_1}, -\sqrt{-z_1}, \sqrt{-z_2}, -\sqrt{-z_2}, \sqrt{-z_3}, -\sqrt{-z_3}\}\end{aligned}$$

sieht man leicht, dass $\{(2, \bar{2}), (6, \bar{6}), (8, \bar{8})\} \subset Y'' \simeq \mathcal{R}(Y)$ und $\{2, \bar{2}, 6, \bar{6}, 8, \bar{8}\} \subset Z'' \simeq \Lambda_2(Y)$.

3.6 $\alpha_Y(\Gamma) = \text{Id} \times S_3$

$$\begin{array}{ccc} S/S_0 & = & F(\sqrt{b}) \times F(\alpha, \sqrt{b}) \\ & & \downarrow \quad \quad \downarrow \\ & & F \quad \times \quad F(\alpha) \end{array}$$

wobei α Nullstelle eines separablen irreduziblen Polynoms $f(x)$ vom Grad 3 mit Koeffizienten in F ist und F keine primitive dritte Einheitswurzel enthält.

Bemerkung: Der Fall

$$\begin{array}{ccc} S/S_0 & = & F(\sqrt{a}) \times F(\alpha, \sqrt{b}) \\ & & \downarrow \quad \quad \downarrow \\ & & F \quad \times \quad F(\alpha) \end{array}$$

mit $a \neq b$, ist wegen der Bedingung $\Delta(S) = F \times F$ ausgeschlossen.

Sei L der Zerfällungskörper von $f(x)$ und $\alpha_2, \alpha_3 \in L$ die zu $\alpha = \alpha_1$ konjugierten Nullstellen von f . Für $Z = X(S)$ gilt

$$Z = X(S) = X(F(\sqrt{b})) \sqcup X(F(\alpha_1, \sqrt{b})).$$

Die Elemente von Z sind also durch die Bilder von $v_1 = \sqrt{b}$ und $v_2 = (\alpha_1, \sqrt{b})$ in F_{sep} bestimmt. Setze

$$\begin{aligned} A &= \xi_1(v_2) = (\alpha_1, \sqrt{b}), & \bar{A} &= \bar{\xi}_1(v_2) = (\alpha_1, -\sqrt{b}), \\ B &= \xi_2(v_2) = (\alpha_2, \sqrt{b}), & \bar{B} &= \bar{\xi}_2(v_2) = (\alpha_2, -\sqrt{b}), \\ C &= \xi_3(v_2) = (\alpha_3, \sqrt{b}), & \bar{C} &= \bar{\xi}_3(v_2) = (\alpha_3, -\sqrt{b}), \\ D &= \xi_4(v_1) = \sqrt{b}, & \bar{D} &= \bar{\xi}_4(v_1) = -\sqrt{b}. \end{aligned}$$

Erzeugende Elemente der Γ -Operation auf Z sind zum Beispiel

$$\gamma_1 = (\alpha_1 \alpha_2), \quad \gamma_2 = (\alpha_1 \alpha_2 \alpha_3), \quad i : \sqrt{b} \rightarrow -\sqrt{b},$$

und es ergibt sich die Tabelle

Tabelle 17:

$\phi(\Gamma)$	$\alpha(\Gamma)$	$\alpha'(\Gamma)$	$\alpha''(\Gamma)$
$\gamma_1 = (\alpha_1\alpha_2)$	$(AB)(\overline{AB})$	$(15)(\overline{15})$	$(26)(\overline{26})$
$\gamma_2 = (\alpha_1\alpha_2\alpha_3)$	$(ABC)(\overline{ABC})$	$(135)(\overline{135})$	$(268)(\overline{268})$
$i : \sqrt{b} \rightarrow -\sqrt{b}$	$(A\overline{A})(B\overline{B})(C\overline{C})(D\overline{D})$	$(1\overline{1})(3\overline{3})(5\overline{5})(7\overline{7})$	$(2\overline{2})(4\overline{4})(6\overline{6})(8\overline{8})$

Mit den Korrespondenzen

$$\begin{array}{ll}
 A \longleftrightarrow 5 \longleftrightarrow 2, & \overline{A} \longleftrightarrow \overline{5} \longleftrightarrow \overline{2}, \\
 B \longleftrightarrow 1 \longleftrightarrow 6, & \overline{B} \longleftrightarrow \overline{1} \longleftrightarrow \overline{6}, \\
 C \longleftrightarrow 3 \longleftrightarrow 8, & \overline{C} \longleftrightarrow \overline{3} \longleftrightarrow \overline{8}, \\
 D \longleftrightarrow 7 \longleftrightarrow 4, & \overline{D} \longleftrightarrow \overline{7} \longleftrightarrow \overline{4},
 \end{array}$$

sieht man, dass

$$Z/Y \simeq Z'/Y' \simeq Z''/Y'' \simeq Z/Y$$

und damit auch

$$S/S_0 \simeq S'/S'_0 \simeq S''/S''_0 \simeq S/S_0.$$

4 Schlussfolgerungen

Nach den obigen Berechnungen folgt, dass es grundsätzlich zwei Situationen gibt, in denen S/S_0 , S'/S'_0 und S''/S''_0 isomorph sind. Die eine tritt auf, wenn zumindest ein Element von $Y = X(S_0)$ unter Γ -Operation fixiert bleibt und S durch Adjunktion desselben Elementes (vom Grad zwei über F) zu jedem Faktor von S_0 entsteht. Die andere tritt auf, wenn S durch Adjunktion desselben Elementes von Grad 4 über F zu jedem Faktor von S_0 entsteht. Aus Dimensionsgründen kann letztere Situation nur auftreten, wenn $S_0 = K \times K$, wobei K eine quadratische Erweiterung von F bezeichnet.

5 Zusammenhänge und Ausblicke

5.1 Quaternionen

5.1.1 Definition

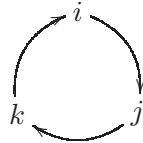
Die Quaternionen, mit \mathbb{H} bezeichnet, sind eine Verallgemeinerung der komplexen Zahlen. Sie wurden 1843 von Sir W.R. Hamilton eingeführt, weswegen sie auch Hamilton-Zahlen genannt werden. Die Menge der Quaternionen bildet eine nicht kommutative vierdimensionale normierte Divisionsalgebra über dem Körper der reellen Zahlen \mathbb{R} . Als Algebra

entsteht sie aus \mathbb{C} durch Adjunktion eines Elementes j , das $j^2 = -1$ und $ij = -ji$ erfüllt. Als reeller Vektorraum besitzt sie die vier Basiselemente $\{1, i, j, k\}$, welche folgende Multiplikationsregeln erfüllen:

$$i^2 = j^2 = k^2 = -1,$$

$$ij = k = -ji \quad ; \quad ki = j = -ik \quad ; \quad jk = i = -kj.$$

Dabei bezeichnet 1 wie gewöhnlich die multiplikative Einheit. Diese Multiplikationsregeln können am einfachsten mit Hilfe dieses Kreises erinnert werden



wobei Multiplikation zweier Elemente im Uhrzeigersinn (bzw. im Gegenuhrzeigersinn) jeweils das nachfolgende Element (bzw. minus das Nachfolgende Element) ergibt. Analog zu den komplexen Zahlen ist die Konjugation eines Quaternions $q = a + bi + cj + dk$ durch

$$\bar{q} = a - bi - cj - dk$$

definiert. Die Norm wird folgenderweise definiert:

$$|q|^2 = q\bar{q} = \bar{q}q = a^2 + b^2 + c^2 + d^2,$$

und das multiplikativ Inverse von $q \neq 0$ ist

$$q^{-1} = \bar{q}/|q|^2.$$

Die Quaternionen mit Norm 1 bilden unter Multiplikation eine Gruppe, die mit der speziellen unitären Gruppe $SU(2)$ identifiziert werden kann. Via Konjugation operieren diese Elemente auf den dreidimensionalen Raum der rein imaginären Quaternionen wie Drehungen, und man erhält einen surjektiven Homomorphismus von $SU(2)$ nach $SO(3)$ dessen Kern $\{1, -1\} \subset SU(2)$ ist ($SU(2)$ bildet eine doppelte Überdeckung von $SO(3)$). Zur Darstellung der Quaternionen bieten sich viele Möglichkeiten. Zum Beispiel können sie als Summe eines Skalars (der Realteil) und eines Vektors in \mathbb{R}^3 interpretiert werden:

$$q = q_0 + q_1i + q_2j + q_3k = q_0 + \vec{v} = (q_0, \vec{v}); \quad \text{mit} \quad \vec{v} = (q_1, q_2, q_3).$$

In dieser Vektor-Notation ist die Multiplikation gegeben durch

$$(q_0, \vec{v})(q'_0, \vec{v}') = (q_0q'_0 - \vec{v} \cdot \vec{v}', q_0\vec{v}' + q'_0\vec{v} + \vec{v} \times \vec{v}').$$

Als Matrizen können die Quaternionen durch komplexe 2×2 Matrizen oder durch reelle 4×4 Matrizen dargestellt werden. Erwähne zuerst dass die komplexe Zahlen folgendermaßen als reelle 2×2 Matrizen interpretiert werden können:

$$z \equiv \begin{pmatrix} \operatorname{Re}(z) & \operatorname{Im}(z) \\ -\operatorname{Im}(z) & \operatorname{Re}(z) \end{pmatrix}$$

mit $|z| = \sqrt{\det(z)}$. Bemerke dann, dass

$$q = a + bi + cj + dk = (a + bi) + (c + di)j = z + wj \quad \text{mit } z, w \in \mathbb{C}.$$

Somit kann man analog zu den komplexen Zahlen vorgehen und die Quaternionen in folgender Form darstellen

$$q \equiv \begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix} = \begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix}$$

mit $|q| = \sqrt{\det(q)}$. Die Basiselementen sind in diesem Fall

$$1 \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \quad i \equiv \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}; \quad j \equiv \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}; \quad k \equiv \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Bemerkung: Diese Äquivalenzen definieren eine zweidimensionale Matrixdarstellung der nichtkommutativen Quaternionengruppe $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ auf den komplexen Vektorraum $\mathbb{C} \times \mathbb{C}$, das heißt sie definieren einen Gruppenhomomorphismus $\rho : Q \rightarrow GL_2(\mathbb{C})$.

Man hat früher gesehen, dass die Quaternionen sich als ein vier dimensionaler reeller Vektorraum mit Basiselementen $\{1, i, j, k\}$ auffassen lassen. Die Elementen $\{1, i, j, k\}$ operieren dann durch Linksmultiplikation als Endomorphismen auf diesen Vektorraum, und ihre Matrixdarstellung (in der Basis $1 \equiv [1, 0, 0, 0], i \equiv [0, 1, 0, 0], j \equiv [0, 0, 1, 0], k \equiv [0, 0, 0, 1]$) lautet:

$$1 \equiv \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}; \quad i \equiv \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}; \quad j \equiv \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}$$

$$k \equiv \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Definition 18: Ein **Hurwitz-Quaternion** ist ein Quaternion deren Komponenten entweder alle ganze Zahlen oder alle halbe ganze Zahlen sind. Die Menge der Hurwitz-Quaternionen wird mit H bezeichnet:

$$H = \{a + bi + cj + dk \in \mathbb{H} \mid \text{entweder } a, b, c, d \in \mathbb{Z} \text{ oder } a, b, c, d \in \mathbb{Z} + 1/2\}.$$

H ist geschlossen bezüglich Multiplikation und Addition der Quaternionen und ist somit ein Unterring von \mathbb{H} . Als Gruppe ist H frei abelsch mit erzeugenden Elementen $\{1/2(1 + i + j + k), i, j, k\}$ und definiert somit ein Gitter in \mathbb{R}^4 .

Die Untergruppe der Hurwitz-Quaternionen der Norm 1 ist eine nichtabelsche Gruppe der Ordnung 24 (binäre Tetraedergruppe). Sie enthält die 8-elementige Quaternionengruppe $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ sowie die 16 Elemente $\{1/2(\pm 1 \pm i \pm j \pm k)\}$, wobei die Vorzeichen beliebig gewählt werden können. Diese 16 Elemente entsprechen den Ecken eines Hyperkubus in \mathbb{R}^4 . Diese Gruppe tritt oft in Zusammenhang mit dem Begriff der Trialität auf. Der Begriff der Trialität, analog zu den der Dualität, bezeichnet eine Korrespondenz, die drei verschiedene Objekten als äquivalent erklärt. Die frühere geometrische Konstruktion kann in der Sprache der Quaternionen folgendermassen interpretiert werden. Die 8 Zellen entsprechen den 8 Elementen von $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ (das heisst den vier Richtungen von \mathbb{R}^4 mit Orientierung ± 1)

$$\begin{aligned} A &\equiv i \equiv e_1, & \bar{A} &\equiv -i \equiv -e_1, \\ B &\equiv j \equiv e_2, & \bar{B} &\equiv -j \equiv -e_2, \\ C &\equiv k \equiv e_3, & \bar{C} &\equiv -k \equiv -e_3, \\ D &\equiv 1 \equiv e_4, & \bar{D} &\equiv -1 \equiv -e_4. \end{aligned}$$

Die 8 ungeraden und geraden Ecken entsprechen den Elementen der Form $1/2(\pm 1 \pm i \pm j \pm k)$ mit einer ungeraden bzw. geraden Anzahl von Minuszeichen:

$$\begin{aligned} 1 &\equiv \frac{1}{2}(1 + i - j + k) \equiv \frac{1}{2}(1, 1, -1, 1) & \bar{1} &\equiv \frac{1}{2}(-1 - i + j - k) \equiv \frac{1}{2}(-1, -1, 1, -1) \\ 3 &\equiv \frac{1}{2}(1 + i + j - k) \equiv \frac{1}{2}(1, 1, 1, -1) & \bar{3} &\equiv \frac{1}{2}(-1 - i - j + k) \equiv \frac{1}{2}(-1, -1, -1, 1) \\ 5 &\equiv \frac{1}{2}(1 - i + j + k) \equiv \frac{1}{2}(1, -1, 1, 1) & \bar{5} &\equiv \frac{1}{2}(-1 + i - j - k) \equiv \frac{1}{2}(-1, 1, -1, -1) \\ 7 &\equiv \frac{1}{2}(1 - i - j - k) \equiv \frac{1}{2}(1, -1, -1, -1) & \bar{7} &\equiv \frac{1}{2}(-1 + i + j + k) \equiv \frac{1}{2}(-1, 1, 1, 1) \end{aligned}$$

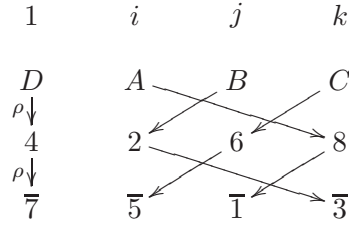
und

$$\begin{aligned} 2 &\equiv \frac{1}{2}(1 + i - j - k) \equiv \frac{1}{2}(1, 1, -1, -1) & \bar{2} &\equiv \frac{1}{2}(-1 - i + j + k) \equiv \frac{1}{2}(-1, -1, 1, 1) \\ 4 &\equiv \frac{1}{2}(1 + i + j + k) \equiv \frac{1}{2}(1, 1, 1, 1) & \bar{4} &\equiv \frac{1}{2}(-1 - i - j - k) \equiv \frac{1}{2}(-1, -1, -1, -1) \\ 6 &\equiv \frac{1}{2}(1 - i + j - k) \equiv \frac{1}{2}(1, -1, 1, -1) & \bar{6} &\equiv \frac{1}{2}(-1 + i - j + k) \equiv \frac{1}{2}(-1, 1, -1, 1) \\ 8 &\equiv \frac{1}{2}(1 - i - j + k) \equiv \frac{1}{2}(1, -1, -1, 1) & \bar{8} &\equiv \frac{1}{2}(-1 + i + j - k) \equiv \frac{1}{2}(-1, 1, 1, -1) \end{aligned}$$

Die zyklische Permutation von Z/Y , Z'/Y' und Z''/Y'' kann dann in Zusammenhang mit der Drehung die von der Multiplikation mit $-1/2(1+i+j+k)$ definiert wird gebracht werden. Die zu $-1/2(1+i+j+k)$ äquivalente reelle 4×4 Matrix ist

$$\rho = \frac{1}{2} \begin{pmatrix} -1 & 1 & 1 & 1 \\ -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & 1 \\ -1 & 1 & -1 & -1 \end{pmatrix}.$$

Am Ende der Vorbereitung hatte man gesehen, dass die Elemente von Z/Y , Z'/Y' und Z''/Y'' , im Fall wo $(D, \overline{D}) \in Y$ fixiert bleibt, identifiziert werden können. Aus den Spalten von ρ sieht man, dass D auf $\overline{4}$, A auf 8 , B auf 2 und C auf 6 abgebildet werden. $\rho^{-1} = \rho^t$ bildet dann D auf $\overline{7}$, A auf $\overline{1}$, B auf $\overline{3}$ und C auf $\overline{5}$ ab. Im Vergleich zu den früheren Identifizierungen, entspricht das einer zyklischen Permutation von i, j, k :



5.1.2 Quaternionen-Algebren

Definition 19: Sei F ein beliebiger Körper und $a, b \in F^\times$. Definiere eine 4-dimensionale F -Algebra $(a, b)_F$ mit der Basis $1, e_1, e_2, e_3$, so dass

$$e_1 e_2 = e_3, \quad e_2 e_1 = -e_3, \quad e_1^2 = a, \quad e_2^2 = b, \quad e_3^2 = ab = ba.$$

Eine solche Algebra $(a, b)_F$ wird **Quaternionen-Algebra** genannt.

Der Unterraum $e_1 F + e_2 F + e_3 F$ von $(a, b)_F = (a, b)$ wird mit $(a, b)_0$ bezeichnet, und seine Elemente werden reine Quaternionen genannt. Mit dieser Notation kann (a, b) als direkte Summe geschrieben werden:

$$(a, b) = F \cdot 1 \oplus (a, b)_0.$$

Für $x = x_0 + x_1$ mit $x_0 \in F$ und $x_1 \in (a, b)_0$ definiere das konjugierte Element durch $\overline{x} = x_0 - x_1$. Die Abbildung

$$\overline{} : (a, b) \rightarrow (a, b), \quad x \mapsto \overline{x}$$

wird auch kanonische Involution genannt.

Definition 20: Eine **Involution** auf einer zentral-einfachen Algebra A über F ist eine Abbildung $\sigma : A \rightarrow A$, die $\forall x, y \in A$ folgendes erfüllt:

- i) $\sigma(x + y) = \sigma(x) + \sigma(y)$,
- ii) $\sigma(xy) = \sigma(y)\sigma(x)$,
- iii) $\sigma^2(x) = x$.

Diese Abbildung muss nicht notwendigerweise F -linear sein, aber die Bedingung ii) impliziert, dass $F = Z(A)$ von σ wieder auf sich abgebildet wird. Die Restriktion von σ auf F kann daher entweder die Identität sein (und somit σ F -linear) oder Ordnung 2 haben. Eine Involution σ heisst **von erstem Typ**, falls sie $\sigma|_F = \text{Id}_F$ erfüllt, **von zweitem Typ**, falls $\sigma|_F \neq \text{Id}_F$, $\sigma|_F^2 = \text{Id}_F$.

Quaternionenalgebren spielen eine wichtige Rolle in der Theorie der quadratische Formen und in der Klassifikation zentral-einfacher Algebren. Man kann zum Beispiel zeigen dass alle zentral-einfache Algebren der Dimension vier isomorph zu einer Quaternionen-Algebra sind.

5.2 Clifford-Algebren

Clifford-Algebren entstehen als natürliche Verallgemeinerung der Quaternionenalgebren für grössere Dimensionen. Sie sind besonders wichtig in der Theorie der quadratischen Formen und finden unzählige Anwendungen in verschiedenen Gebiete, insbesondere in der Physik, Chemie, Robotik und der Computerprogrammierung (ein schönes Buch über die Anwendungen von Clifford-Algebren ist zum Beispiel [9]). Sie wurden zuerst 1878 von William Clifford definiert ([10]). Man sagt, eine F -Algebra A sei mit der quadratische Form q über V genau dann verträglich, wenn es eine lineare Abbildung $\varphi : V \rightarrow A$ gibt, die $\phi(v)^2 = q(v) \cdot 1_A$ für alle $v \in V$ erfüllt. Die Idee ist, für einen gegebenen quadratischen Raum (V, q) über F eine F -Algebra C zu konstruieren, die mit q via $\varepsilon : V \rightarrow C$ verträglich ist und so, dass für jede andere Algebra A , die mit q via $\varphi : V \rightarrow A$ verträglich ist, ein eindeutiger Algebra-Homomorphismus $\hat{\varphi} : C \rightarrow A$ existiert, der das Diagramm

$$\begin{array}{ccc} V & \xrightarrow{\varepsilon} & C \\ & \searrow \varphi & \downarrow \hat{\varphi} \\ & & A \end{array}$$

kommutieren lässt (universelle Eigenschaft der Clifford-Algebra).

Definition 21: Sei (V, q) ein quadratischer Raum über F und $T(V) = \bigoplus \{V^{\otimes n} : n \in \mathbb{N}\}$ die zugehörige Tensoralgebra. Sei $I(q)$ das zweiseitige Ideal von $T(V)$, das von den Elementen $\{x \otimes x - q(x)|x \in V\}$ erzeugt wird. Dann ist

$$C(V, q) = T(V)/I(q)$$

die Clifford-Algebra von (V, q) .

Man kann leicht zeigen, dass in der Tat die obige Definition die universelle Eigenschaft der Clifford-Algebra erfüllt ([4] S. 329). Die Clifford-Algebra erbt die $\mathbb{Z}/2\mathbb{Z}$ -Graduierung von $T(V)$. Erinnere dass eine $(\mathbb{Z}/2\mathbb{Z})$ Graduierung einer F -Algebra A eine Zerlegung von A in eine direkte Summe $A = A_0 \oplus A_1$ ist, so dass $F = F \cdot 1_A \subset A_0$ und $A_0 A_0 \subset A_0$, $A_0 A_1 = A_1 A_0 \subset A_1$, $A_1 A_1 \subset A_0$. Ein Unterraum B von A heisst graduiert, wenn $B = B_0 \oplus B_1$ für $B_0 = B \cap A_0$ und $B_1 = B \cap A_1$.

Die Tensoralgebra $T(V) = T(V)_0 \oplus T(V)_1$ mit

$$T(V)_0 = \bigoplus_{n \text{ gerade}} V^{\otimes n}; \quad T(V)_1 = \bigoplus_{n \text{ ungerade}} V^{\otimes n}$$

ist in natürlicher Weise eine graduierte Algebra. Da die erzeugende Elementen von $I(q)$ in $T(V)_0$ liegen, ist $I(q) = I(q)_0 \oplus I(q)_1$ graduiert und mit

$$C_0(V, q) = T(V)_0/I(V)_0; \quad C_1(V, q) = T(V)_1/I(V)_1$$

ist auch

$$C(V, q) = C_0(V, q) \oplus C_1(V, q)$$

graduiert. Für F der Charakteristik verschieden von zwei und V von gerader Dimension wird in [4], Theorem 9.2.10, S. 332, folgendes Strukturtheorem bewiesen:

Theorem 5 *Sei $\text{Char}(F) \neq 2$ und (V, q) ein regulärer quadratischer Raum der Dimension $n = 2m$ über F . Dann ist die Clifford-Algebra $C(V, q)$ von (V, q) zentral-einfach über F und isomorph zu einem Tensorprodukt von Quaternionenalgebren. Für das Zentrum $Z(C_0(V, q)) =: Z$ der geraden Clifford-Algebra gilt:*

$$Z(C_0(V, q)) \simeq F[T]/(T^2 - \delta)$$

wobei δ ein Representant der Diskriminante von q ist. Die gerade Clifford-Algebra $C_0(V, q)$ ist zentral-einfach über Z , insbesondere falls $\delta \notin F^{\times 2}$ so ist sie zentral-einfach über $F(\sqrt{\delta}) \simeq F \times F$.

Im Folgenden wird man mit einer anderen Definition arbeiten, die der verallgemeinerten gerade Clifford-Algebra. Zuerst will man noch ein Paar Definitionen erinnern.

Definition 22: Eine Algebra A über dem Körper F heisst **zentral-einfach** oder **Brauer-Algebra**, wenn ihr Zentrum $Z(A)$ mit F übereinstimmt (zentral) und sie keine nicht-trivialen zweiseitigen Ideale enthält (einfach).

Für eine zentral-einfache Algebra gilt:

Theorem 6 (Skolem-Noether) *Sei A zentral-einfach. Dann ist jeder Automorphismus φ von A ein innerer Automorphismus, das heisst von der Form*

$$\begin{aligned} \varphi : A &\rightarrow A \\ x &\mapsto \alpha x \alpha^{-1} \end{aligned}$$

für ein invertierbares Element $\alpha \in A$.

Theorem 7 (Wedderburn) *Für eine F -Algebra A sind folgende Bedingungen äquivalent:*

- A ist zentral-einfach
- Es existiert eine Körpererweiterung K von F , so dass

$$A \otimes_F K \simeq M_n(K) \quad \text{für ein } n \in \mathbb{N}.$$

Man nennt K einen Zerfällungskörper von A .

- Falls K algebraisch abgeschlossen und $F \subset K$ ist, so ist

$$A \otimes_F K \simeq M_n(K) \quad \text{für ein } n \in \mathbb{N}.$$

Anders gesagt, ist jeder algebraisch abgeschlossener Körper K , der F enthält, ein Zerfällungskörper von A .

- *Es existiert eine endlichdimensionale zentrale Divisionsalgebra D über F und eine Zahl $r \in \mathbb{N}$, so dass*

$$A \simeq M_r(D).$$

Ausserdem sind alle einfachen links- A -Moduln isomorph, und D ist bis auf Algebra-Isomorphismus eindeutig bestimmt als $D = \text{End}_A(M)$ für ein einfaches links- A -Modul.

Insbesondere gilt für eine zentral-einfache Algebra A über F , dass $\dim_F(A) = n^2$; $n \in \mathbb{N}$ heisst *Grad* von A .

Definition 23: Eine Involution σ vom ersten Typ auf einer zentral-einfachen F -Algebra A der Dimension n^2 über F heisst **orthogonal**, falls $\dim(A^+) = 1/2n(n+1)$; **symplektisch**, falls $\dim(A^+) = 1/2n(n-1)$, wobei $A^+ = \{x \in A \mid \sigma(x) = x\}$ der Unterraum der symmetrischen Elemente bezeichnet.

(Für mehr über die Klassifikation der Involutionen auf einfachen Algebren siehe [4], 300-304.)

Definition 24: Sei A eine zentral-einfache Algebra vom Grad n über F . Ein **quadratisches Paar** über A ist ein Paar (σ, f) , wobei σ eine Involution vom ersten Typ auf A ist und $f : \text{Sym}(A, \sigma) \rightarrow F$ eine lineare Abbildung, so dass

- i) $\dim_F \text{Sym}(A, \sigma) = 1/2n(n+1)$ und $T_A(\text{Skew}(A, \sigma)) = \{0\}$,
- ii) $f(x + \sigma(x)) = \text{Trd}_A(x)$ für alle $x \in A$.

Da man $\text{Char}(F) \neq 2$ vorausgesetzt hatte, ist die Bedingung $T_A(\text{Skew}(A, \sigma)) = \{0\}$ für alle Involutionen σ vom ersten Typ automatisch erfüllt. Bedingung i) bedeutet dann einfach, dass σ orthogonal sein muss und die Abbildung f durch $f(x) = 1/2T_A(x)$, für alle $x \in \text{Sym}(A, \sigma)$ definiert ist. Gegeben ein quadratischer Raum (V, q) , kann man ein quadratisches Paar (σ_q, f_q) über der zentral-einfachen Algebra $\text{End}_F(V)$ konstruieren, das sogenannte zu q assoziierte quadratische Paar (vgl.[1], S.58, Prop.5.11).

Sei A eine zentral-einfache Algebra über F und (σ, f) ein quadratisches Paar über A . Eine (verallgemeinerte gerade) Clifford-Algebra $C(A, \sigma, f)$ ist eine Algebra, die so definiert ist, dass für alle (nicht-singuläre) quadratischen Räume (V, q) ,

$$C(\text{End}_F(V), \sigma_q, f_q) \simeq C_0(V, q)$$

gilt. Für die explizite Definition wird auf [1], S.91, verwiesen. Wenn man das Struktur-Theorem 5 anwendet, so findet man (siehe [1], Theorem 8.10, S. 94):

Theorem 8 *Sei F mit $\text{Char}(F) \neq 2$, A eine zentral-einfache F -Algebra vom Grad $n = 2m$ und (σ, f) ein quadratisches Paar über A . Bezeichne mit Z das Zentrum von $C(A, \sigma, f)$. Dann gilt*

$$Z \simeq F[T]/(T^2 - \delta)$$

für δ mit $\delta \cdot F^{\times 2} = \text{disc}(\sigma, f) = \text{disc}(\sigma) \in F^{\times}/F^{\times 2}$. Falls $Z \simeq F \times F$, dann lässt sich $C(A, \sigma, f)$ als direktes Produkt von zwei zentral-einfachen F -Algebren vom Grad 2^{m-1} schreiben.

Bezeichne mit \underline{A} die Algebra A als F -Vektorraum. Es gibt eine kanonische Abbildung

$$c : A \rightarrow C(A, \sigma, f)$$

gegeben durch

$$A \rightarrow \text{End}_F(A) \simeq \underline{A} \otimes \underline{A} \hookrightarrow T_0(\underline{A}) \twoheadrightarrow C(A, \sigma, f).$$

In [1], Lemma 8.14, wird gezeigt, dass $\ker(c) = \ker(f) \subset \text{Sym}(A, \sigma)$. Insbesondere folgt für F mit $\text{char}(F) \neq 2$ dass $\ker(c) = \ker(T_A)$. In 8.18 wird ausserdem gezeigt, dass für F der Charakteristik verschieden von 2, $c(A)$ als direkte Summe

$$c(A) = F \oplus c_0(A)$$

mit $c_0(A) = \text{Skew}(A, \sigma)$ geschrieben werden kann.

Man ist jetzt bereit, den Zusammenhang mit den früheren Betrachtungen zu erklären. Sei wie früher S/S_0 eine quadratische Erweiterung von étalen F -Algebren mit $\dim(S) = 2m$, $\dim(S_0) = m$ und $\Delta(S) = F \times F$. S kann in einer zentral-einfachen F -Algebra A von Grad $2m$ ($\dim(A) = 64$) eingebettet werden, $\varphi : S \hookrightarrow A$. Nach skalare Erweiterung zu F_{sep} sei $A_{F_{\text{sep}}} = \text{End}_{F_{\text{sep}}}(V)$ für ein m -dimensionaler F_{sep} -Vektorraum V . Sei σ eine orthogonale Involution auf A , so dass die Einschränkung von σ auf $S \subset A$ mit der kanonischen Involution von S/S_0 übereinstimmt. Nimm ausserdem an, dass die Elemente von $S_{F_{\text{sep}}} \subset A_{F_{\text{sep}}} = \text{End}(V)$ eine Zerlegung von V als Summe von hyperbolischen Ebenen erhalten (vgl. [1] 8.20). Da für $\text{Char}(F) \neq 2$ die Abbildung f im quadratischen Paar (σ, f) eindeutig durch $f(s) = \frac{1}{2}T_A(s)$ definiert wird, schreibt man von nun an $C(A, \sigma)$ statt $C(A, \sigma, f)$. Aus [1] 8.18 und 8.21 folgt, dass $c(S)$ eine kommutative Unter algebra von $C(A, \sigma)$ erzeugt. Man wird jetzt sehen, den Überlegungen von J.-P. Tignol folgend, dass diese Algebra zu $\Omega(S/S_0)$ isomorph ist. Zuerst braucht man

Lemma 1 $\omega(S)$ erzeugt $\Omega(S/S_0)$ als F -Algebra.

Beweis. Erinnerung dass $\omega : S \rightarrow \Omega(S/S_0)$ die in Definition 17 definierte Abbildung ist. OBDA sei F ein Zerfällungskörper von S so dass $S = F^{2m}$. Seien f_i, f'_i für $1 \leq i \leq m$ die minimale Idempotente von S und $\sigma(f_i) = f'_i$ für alle $i \in \{1, \dots, m\}$. Die minimale Idempotente von $\Omega(S/S_0)$ sind von der Form

$$g_I = \sum_{\mathfrak{S}_m} f''_1 \otimes f''_2 \otimes f''_3 \otimes f''_4$$

für $I \subset \{1, \dots, m\}$ und

$$f''_i = \begin{cases} f_i & \text{falls } i \notin I, \\ f'_i & \text{falls } i \in I. \end{cases}$$

Im Beweis von [2], S.33, Prop.4.15, werden die Koeffizienten von $\omega(b)$ als Linearkombination der g_I 's gefunden. Daraus kann man folgern dass:

$$\omega(f_i) = \sum_{I \not\ni i} g_I \quad \text{und} \quad \omega(f'_i) = \sum_{I \ni i} g_I.$$

Somit können alle minimale Idempotente g_I von $\Omega(S/S_0)$ aus den $\omega(f_i)$'s und $\omega(f'_i)$'s durch die Formel

$$g_I = \prod_{i \notin I} \omega(f_i) \prod_{i \in I} \omega(f'_i) \quad (5)$$

gefunden werden und die Behauptung ist bewiesen. \square

Lemma 2 $\ker(c \circ \varphi) = \ker(\omega)$

Beweis. Mit [1] 8.14 findet man

$$\ker(c \circ \phi) = \{x \in S_0 \mid T_{S_0/F}(x) = 0\}.$$

Da $\omega(s) = T_{S_0/F}$ für alle $s \in S_0$, folgt bereits die Inklusion $\ker(c \circ \phi) \subset \ker(\omega)$. Dann ist für $s = \sum_{i=1}^m (s_i f_i + s'_i f'_i) \in S$

$$\omega(s) = \sum_I \left(\sum_{i \notin I} s_i + \sum_{i \in I} s'_i \right) g_I$$

und daher kann $\omega(s) = 0$ sein, nur wenn $s_i = s'_i$ für alle i (alle Koeffizienten müssen verschwinden) und $\sum_{i=1}^m s_i = 0$. Die erste Bedingung bedeutet dass $s \in S_0$; die zweite dass $T_{S_0/F} = 0$, das heisst $\ker(\omega) \subset \ker(c \circ \phi)$. \square

Aus diesem Lemma folgt die Existenz einer linearen Abbildung $\tilde{\varphi} : \omega(S) \rightarrow c(S)$, so dass

$$\tilde{\varphi}(\omega(s)) = c(s) \quad \text{für alle } s \in S.$$

Theorem 9 *Es existiert eine Einbettung*

$$\hat{\varphi} : \Omega(S/S_0) \hookrightarrow C(A, \sigma)$$

die durch die Bedingung

$$\hat{\varphi}(\omega(s)) = c(s) \quad \text{für alle } s \in S$$

eindeutig definiert ist.

Für den Beweis kann man zuerst annehmen, dass S über F zerfällt. Die Behauptung für den allgemeinen Fall folgt dann aus:

Proposition 1 *Seien Ω und C F -Algebren und $U \subset \Omega$ ein F -Unterraum, der Ω als F -Algebra erzeugt. Sei $f : U \rightarrow C$ eine lineare Abbildung. Wenn eine Körpererweiterung K/F existiert, so dass $f \otimes \text{Id}_K : U \otimes_F K \rightarrow C \otimes_F K$ sich auf ein K -Algebra Homomorphismus $\hat{f}_K \otimes \text{Id}_K : \Omega \otimes_F K \rightarrow C \otimes_F K$ erweitern lässt, dann lässt sich auch f zu einem F -Algebra Homomorphismus $\hat{f} : \Omega \rightarrow C$ erweitern.*

Beweis von Theorem 9. Nimm an dass $S = F^{2m}$. Dann ist $A = \text{End}_F(V)$, σ hyperbolisch und $S \subset \text{End}(V)$ erhält eine Zerlegung von V in hyperbolischen Ebenen. Identifiziere $A = V \otimes V$ wie in [1] 5.1. Aus einer orthogonalen Basis e_1, e_2, \dots, e_{2m} von V findet man wie im Beweis von [1] 8.21 eine Basis $h_1, \dots, h_m, h_1^2, \dots, h_m^2$ von S über F mit:

$$h_i = \frac{1}{2}(e_{2i-1} \otimes e_{2i} - e_{2i} \otimes e_{2i-1}) \quad \text{und} \quad h_i^2 = \frac{1}{2}(e_{2i-1} \otimes e_{2i-1} - e_{2i} \otimes e_{2i})$$

h_1^2, \dots, h_m^2 sind primitive Idempotente von S_0 und

$$f_i = \frac{1}{2}(h_i^2 + h_i), \quad f'_i = \frac{1}{2}(h_i^2 - h_i)$$

für $i = 1, \dots, m$ sind primitive Idempotente von S . Es gilt

$$c(f_i) = \frac{1}{2}(1 + e_{2i-1}e_{2i}), \quad c(f'_i) = \frac{1}{2}(1 - e_{2i-1}e_{2i})$$

und $c(f_i), c(f'_i)$ sind orthogonale Idempotente. Für $I \subset \{1, \dots, m\}$ definiere analog zu (5)

$$k_I = \prod_{i \notin I} c(f_i) \prod_{i \in I} c(f'_i) \in C(A, \sigma). \quad (6)$$

Die k_I 's sind orthogonale Idempotente (da $c(f_i)$ und $c(f'_i)$ es sind) und verschieden von 0 für alle $I \in \{1, \dots, m\}$. Ausserdem folgt aus $c(f_i) + c(f'_i) = c(f_i + f'_i) = 1$ für alle i , dass $\sum_I k_I = 1$. Der injektive Algebra-Homomorphismus $\Omega(S/S_0) \hookrightarrow C(A, \sigma)$, der durch

$$g_I \mapsto k_I$$

definiert wird, erweitert die lineare Abbildung $\tilde{\varphi} : \omega(S) \rightarrow c(S)$, und dank Proposition 1 ist Theorem 9 bewiesen. \square

Für $m = 4$ hat man $\text{deg}(A) = 8$ und S/S_0 ist eine der früher betrachteten quadratische Erweiterungen von étalen Algebren der Dimension vier. Aus 8 folgt dass $C(A, \sigma) \simeq (B, \sigma') \times (C, \sigma'')$ für zwei zentral-einfachen Algebren B und C von Grad 8 über F .

Definition 25: Seien A, B und C zentral-einfache F -Algebren von Grad 8 mit orthogonale Involution, so dass es ein Isomorphismus

$$\vartheta_A : (C(A, \sigma_A), \bar{\sigma}) \xrightarrow{\sim} (B, \sigma_B) \times (C, \sigma_C)$$

gibt. Dann heisst (A, B, C) ein trialitäres Tripel (vgl. [1] 42.A).

Bemerkung: Zentral-einfache F -Algebren der Dimension 8 mit orthogonale Involution werden von $H^1(\Gamma, \mathbf{P}\mathbf{G}\mathbf{O}_8)$ klassifiziert, wobei $\mathbf{P}\mathbf{G}\mathbf{O}_8$ die projektive orthogonale Gruppe in 8 Dimensionen bezeichnet. Insbesondere werden zentral-einfache Algebren der Dimension 8 mit orthogonale Involution und triviale Discriminante durch die Untergruppe $H^1(\Gamma, \mathbf{P}\mathbf{G}\mathbf{O}_8^+) \subset H^1(\Gamma, \mathbf{P}\mathbf{G}\mathbf{O}_8)$ klassifiziert. Dabei bezeichnet $\mathbf{P}\mathbf{G}\mathbf{O}_8^+ \subset \mathbf{P}\mathbf{G}\mathbf{O}_8$ die Untergruppe der Orientierungs erhaltende Elemente.

Aus $Z(C(A, \sigma)) = F \times F$ und [1], Prop. 8.12, S.95, folgt, dass, falls σ orthogonal ist, auch σ' und σ'' orthogonal sind. Das Tripel (A, B, C) ist somit ein *trialitäres Tripel*. Nach Theorem 9 kann $\Omega(S/S_0)$ in $C(A, \sigma)$ eingebettet werden so dass

$$\begin{array}{ccccccc} (A, \sigma) & \longrightarrow & C(A, \sigma) & \simeq & (B, \sigma') & \times & (C, \sigma'') . \\ \cup & & \cup & & \cup & & \cup \\ S & \longrightarrow & \Omega(S/S_0) & \simeq & S' & \times & S'' \end{array}$$

und die, von der früheren Konstruktion induzierte, Permutation von S, S' und S'' hängt somit mit der Trialität von A, B und C zusammen.

Literatur

- [1] M.-A. Knus, A.S. Merkurjev, M. Rost, J.-P. Tignol, *The book of Involutions*, AMS Coll. Pub.44, 1998.
- [2] M.-A. Knus, J.-P. Tignol, *Quartic Exercises*, Proc. of the 2001 Fes conference
- [3] N. Bourbaki, *Éléments de mathématique*, Masson, Paris, 1981, Algèbre. Chapitres 4 à 7.
- [4] W. Scharlau, *Quadratic and Hermitian Forms*, Springer-Verlag, 1985.
- [5] S.Bosch, *Algebra*, Springer-Verlag, 2003.
- [6] M. Artin, *Algebra*, Birkhäuser, 1998.
- [7] W.C. Waterhouse, *Introduction to affine group schemes*, Graduate Texts in Mathematics, vol.66, Springer-Verlag, 1979.
- [8] L.C. Grove, *Classical Groups and Geometric Algebra*, Graduate Studies in Mathematics, vol.39, Amer. Math. Soc.
- [9] R. Ablamowicz, G. Sobczyk, *Lectures on Clifford (geometric) Algebras and Applications*, Birkhäuser, 2004.
- [10] W.K. Clifford, *Applications of Grassmann's Extensive Algebra*, Amer. J. Math. 1, 1878, 350-358.
- [11] J.H. Conway, D.A. Smith, *On quaternions and octonions*, AK Peters, 2003.
- [12] N. Jacobson, *Basic Algebra I*, W. H. Freeman and company, 1974.
- [13] E. Artin, *Geometric Algebra*, Interscience Pub., New York, 1957.
- [14] O. Villa, *On Quadratic Quaternion Forms and Triality*, Diss.ETH No.14453.
- [15] S. Garibaldi, *The characteristic polynomial and determinant are not ad hoc constructions*, Amer.Math.Mon. 111, no. 9, 2004.