Friedrich Kasch

Die Galoissche Theorie für Schiefkörper

Verlag Reinhard Fischer

0. Einleitung

Die Galoissche Theorie für Schiefkörper wurde nach einer längeren Entwicklung, in der Spezialfälle behandelt wurden, fast gleichzeitig von Henri Cartan ([1], 1947) und von Nathan Jacobson ([2], 1947) in voller Allgemeinheit entwickelt. Allerdings führt die Arbeit von H. Cartan etwas weiter, da darin auch die Isomorphismen von Zwischenschiefkörpern untersucht werden.

Im Jahre 1955 erschien eine Note von J. Ninot ([4]), in der eine Bemerkung zum Beweis des Hauptsatzes im kommutativen Fall gemacht wird. Ich habe dann festgestellt ([3], 1955), daß man die Idee von J. Ninot auch zum Beweis des Hauptsatzes für Schiefkörper heranziehen kann. Damit kann man den Satz von Jacobson-Bourbaki, der in den Arbeiten von E. Cartan und N. Jacobson verwendet wird, durch eine ganz einfache Schlußweise ersetzen. Praktisch läuft es darauf hinaus, daß ein endlichdimensionaler Vektorraum und sein dualer Raum die gleiche Dimension haben. In meiner Note ([3]) habe ich dies nur angedeutet. Ein Vortrag, den ich darüber gehalten habe, hat mich veranlaßt, dies hier zusammen mit allen anderen Ergebnissen ausführlich darzustellen.

Literatur

[1] Cartan, Henri:
Théorie de Galois pour les corps non commutatifs.
Ann. École Norm. Sup. 64 (1947), 59-77.

[2] Jacobson, Nathan:
A note on division rings.
Amer. J. Math. 69 (1947), 27-36.

[3] Kasch, Friedrich
Bemerkung zum Hauptsatz der Galoisschen Theorie für Schiefkörper.
Arch. Math. 6 (1955), 420-422.

[4] Ninot, J.
Über den Hauptsatz der Galoisschen Theorie (Kommutative Körper).
Arch. Math. 6 (1955), 52-54.

Inhaltsverzeichnis

0.	Einleitung	Seite 1
1.	Lineare Hilfsmittel	Seite 3
	a. Minimale Elemente	Seite 3
	b. Schiefkörpererweiterungen als Vektorräume	Seite 4
2.	Fixkörper und Dualität	Seite 5
3.	Galoissche Erweiterungen und abgeschlossene Untergruppen	Seite 8
4.	Der Hauptsatz	Seite 16
5.	Fortsetzung von Isomorphismen	Seite 18

Bemerkung zur Indizierung

Ich mache großzügig von der Möglichkeit Gebrauch, Indizes umzubenennen. Ist z.B. I eine Indexmenge und ist $\emptyset \neq I_0 \subset I, I_0$ endlich, dann wird $\sum_{i \in I_0} \ldots$ durch $\sum_{i=1}^{m} \ldots$ ersetzt. Oder ist

$$h = \sum_{i=1}^{n} \alpha_i g_i$$

eine Basisdarstellung, dann ist es für unsere Zwecke oft bequem, die Indizierung so zu ändern, daß $\alpha_i \neq 0$ für $i = 1, \ldots, m$ und $\alpha_i = 0$ für $i > m$ gilt.

Wir machen solche Änderungen ohne dies jeweils ausdrücklich zu erwähnen.

1. Lineare Hilfsmittel

a. Minimale Elemente

Sei L ein Schiefkörper und sei ${}_LV$ ein Linksvektorraum über L. Mit $(v_i|i \in I)$ bezeichnen wir eine Basis von ${}_LV$ und für $a \in V$ sei

$$a = \sum_{i \in I} \alpha_i v_i$$

die Basisdarstellung von a (wobei rechts in der Summe nur jeweils endlich viele Summanden $\alpha_i v_i$ vorkommen).

1.1. Definition

(i) *Träger von* $a = \mathrm{tr}(a) := \{i | i \in I \wedge \alpha_i \neq 0\}$

(ii) *Gewicht von* $a = \mathrm{wt}(a) := |\mathrm{tr}(a)|$
(= Anzahl der Koeffizienten $\neq 0$ in der Basisdarstellung).

(iii) Sei $0 \neq U \subsetneq V$ und sei $a \in U$.
Minimal a *in* U
$:\Longleftrightarrow a \neq 0 \wedge \forall b \in U, b \neq 0[\mathrm{tr}(b) \subset \mathrm{tr}(a) \Longrightarrow \mathrm{tr}(b) = \mathrm{tr}(a)]$.

Man beachte, daß diese Begriffe von der Basis abhängen und daß gilt:

$$a = 0 \Longleftrightarrow \mathrm{tr}(a) = \emptyset \Longleftrightarrow \mathrm{wt}(a) = 0.$$

1.2. Hilfssatz

Seien $0 \neq U \subsetneq V$ und $a, b, u \in U$.

1) Minimal a in $U \wedge \lambda \in L, \lambda \neq 0 \Longrightarrow$ minimal λa in U.

2) Minimal a in $U \wedge \mathrm{tr}(b) = \mathrm{tr}(a) \Longrightarrow$ minimal b in $U \wedge \exists \lambda \in L, \lambda \neq 0[b = \lambda a]$.

3) Zu jedem $u \in U, u \neq 0$ gibt es ein minimales $a \in U$ mit $\mathrm{tr}(a) \subset \mathrm{tr}(u)$.

4) Die Menge der minimalen Elemente aus U ist eine Erzeugendenmenge von U (und enthält daher auch eine Basis von U).

Beweis

1) Klar, da $\mathrm{tr}(a) = \mathrm{tr}(\lambda a)$

2) Durch Umindizieren kann erreicht werden

$$a = \sum_{i=1}^{m} \alpha_i v_i \qquad , b = \sum_{i=1}^{m} \beta_i v_i$$

mit $\alpha_i \neq 0, \beta_i \neq 0, i = 1, \ldots, m$. Sei $c := b - \beta_1 \alpha_1^{-1} a = \sum_{i=2}^{m} (\beta_i - \beta_1 \alpha_1^{-1} \alpha_i) v_i \in U$;
dafür gilt dann $\mathrm{tr}(c) \subsetneq \mathrm{tr}(a)$. Da a minimal ist, folgt $c = 0$, also $b = \lambda a$ mit $\lambda = \beta_1 \alpha_1^{-1} \neq 0$. Dann ist b auch minimal.

3) Induktion nach $\mathrm{wt}(u)(\geqq 1)$.
Beginn: $\mathrm{wt}(u) = 1 \Longrightarrow u$ ist selbst minimal. Die Behauptung sei für $\mathrm{wt}(u) \leqq m-1$ richtig. Sei $u \in U$ mit $\mathrm{wt}(u) = m$. Ist u minimal, dann ist man fertig. Ist u nicht minimal, dann gibt es $0 \neq b \in U$ mit $\mathrm{tr}(b) \subsetneqq \mathrm{tr}(u)$. Daher muß $\mathrm{wt}(b) \leqq m-1$ sein. Also existiert ein minimales a mit $\mathrm{tr}(a) \subset \mathrm{tr}(b) \subset \mathrm{tr}(u)$.

4) Ebenfalls Induktion nach $\mathrm{wt}(u)$ mit Beginn wie in 3). Richtig für $\mathrm{wt}(u) \leqq m-1$. Sei $\mathrm{wt}(u) = m$. Nach 3) gibt es ein minimales $a \in U$ mit $\mathrm{tr}(a) \subset \mathrm{tr}(u)$. Seien (Umindizierung)

$$u = \sum_{i=1}^{m} \mu_i v_i \quad , \; a = \sum_{i=1}^{k} \alpha_i v_i \; (k \leqq m),$$

wobei $\alpha_1 \neq 0$ angenommen werden kann. Dann folgt

$$\mathrm{tr}(u - \mu_1 \alpha_1^{-1} a) \subsetneqq \mathrm{tr}(u).$$

Nach Induktionsvoraussetzung gibt es minimale Elemente $a_1, \ldots, a_t \in U$ und $\lambda_1, \ldots, \lambda_t \in L$ mit

$$u - \mu \alpha_1^{-1} a = \lambda_1 a_1 + \cdots + \lambda_t a_t.$$

Folglich ist u Linearkombination von minimalen Elementen.

Die folgenden Abschnitte enthalten mehrere Anwendungen der minimalen Elemente. Die damit erhaltenen Resultate bilden die Grundlage für den Hauptsatz.

b. Schiefkörpererweiterungen als Vektorräume

Sei L ein Schiefkörper, dann bezeichne E den Ring aller Endomorphismen von L als additive Gruppe ($= \mathbb{Z}$-Modul). E enthält zwei wichtige Teilmengen. Sei $\lambda \in L$, dann ist die Linksmultiplikation mit λ d.h.

$$\lambda' : \; L \ni \xi \mapsto \lambda\xi \in L$$

offensichtlich ein Element in E und

$$\Phi : \; L \ni \lambda \mapsto \lambda' \in E$$

ist ein Ringmonomorphismus. Sei $L' := \Phi(L)$, dann ist L' ein zu L isomorpher Unterschiefkörper von E.

Mit $\mathfrak{Aut}(L)$ wird die Gruppe aller Automorphismen von L bezeichnet. Für $g \in \mathfrak{Aut}(L)$, $\xi, \eta \in L$ gilt dann

$$g(\xi + \eta) = g\xi) + g(\eta) \; , \; g(\xi\eta) = g(\xi)g(\eta).$$

Offensichtlich ist $\mathfrak{Aut}(L) \subset \mathfrak{E}$. Für $g \in \mathfrak{Aut}(L), \lambda, \xi \in L$ folgt dann

$$(g\lambda')(\xi) = g(\lambda\xi) = g(\lambda)g(\xi) = (g(\lambda)'g)(\xi),$$

d.h.

$$g\lambda' = g(\lambda)'g$$

Wir wollen jetzt das Element $\lambda' \in E$ wieder mit λ und $L' \subset E$ wieder mit L bezeichnen. Dann ist also L selbst Unterschiefkörper von E und E kann als L-Links- und L-Rechtsvektorraum betrachtet werden (also ${}_LE$ bzw. E_L). Eine Gefahr der Fehlinterpretation besteht nur in Bezug auf die Produktregel $g\lambda' = g(\lambda)'g$, die jetzt
Produktregel: $g\lambda = g(\lambda)g$
lautet. Es ist also das Produkt $g\lambda$ in E von $g(\lambda)$ zu unterscheiden.

Sei jetzt K ein Unterschiefkörper von L. Dann ist L Links- und Rechtsvektorraum über K. Der Endomorphismenring $\mathrm{End}(L_K)$ ist Unterring von E und enthält $L(= L')$. $\mathrm{End}(L_K)$ ist also auch beidseitiger L- Vektorraum.

1.3. Hilfssatz

Sei K Unterschiefkörper von L.

(i) $K = \{\kappa | \kappa \in L \wedge \forall f \in \mathrm{End}(L_K), \xi \in L[f(\xi\kappa) = f(\xi)\kappa]\}$

(ii) Gilt $\dim(L_K) = n \Longrightarrow \dim({}_L\mathrm{End}(L_K)) = n$.

Beweis:

(i) Bezeichnen wir die Menge auf der rechten Seite von (i) mit K_1, dann gilt $K \subset K_1$. Sei jetzt $\lambda \notin K$, dann existiert eine Basis von L_K der Form $(1, \lambda, \lambda_j | j \in J)$. Definiere $f \in \mathrm{End}(L_K)$ durch

$$f(1) := 1\ ,\ f(\lambda) := 0\ ,\ f(\lambda_j) = 0 \text{ für } j \in J.$$

Dann folgt

$$f(1)\lambda = \lambda \neq f(\lambda) = f(1 \cdot \lambda) = 0,$$

also $\lambda \notin K_1$. Daher gilt $K = K_1$.

(ii) Sei $\lambda_1, \ldots, \lambda_n$ eine Basis von L_K, dann definiert man $d_i \in \mathrm{End}(L_K), i = 1, \ldots, n$ durch

$$d_i(\lambda_j) = \begin{cases} 0 & \text{für } i \neq j \\ 1 & \text{für } i = j \end{cases} \qquad i, j = 1, \ldots, n.$$

Dann ist $d_1, \ldots, d_n$ eine Basis von ${}_L\mathrm{End}(L_K)$.

2. Fixkörper und Dualität

Zu einer Untergruppe $\mathfrak{G} \subsetneq \mathfrak{Aut}(L)$ definiert man den Fixkörper

$$K = \mathrm{Fix}(\mathfrak{G}) := \{\kappa | \kappa \in L \wedge \forall g \in \mathfrak{G}[g(\kappa) = \kappa]\}$$

dann ist K ein Unterschiefkörper von L.
Für $g \in \mathfrak{G}$, $\xi \in L$, $\kappa \in K$ gilt:

$$g(\xi\kappa) = g(\xi)g(\kappa) = g(\xi)\kappa,$$

d.h. g ist ein Endomorphismus von L_K. Also gilt $\mathfrak{G} \subset \mathrm{End}(L_K)$. Da auch $L \subset \mathrm{End}(L_K)$, folgt

$$L\mathfrak{G} \subset \mathrm{End}(L_K).$$

Dies ist nicht nur ein Unterraum von ${}_L\mathrm{End}(L_K)$, sondern wegen der Produktregel $g\lambda = g(\lambda)g$ sogar ein Unterring. Wir wollen zeigen, daß bei endlicher Dimension von L_K sogar $L\mathfrak{G} = \mathrm{End}(L_K)$ gilt. Dazu brauchen wir eine Bezeichnung. Für $\alpha \in L$ betrachten wir die Abbildung

$$\sigma_\alpha : L\mathfrak{G} \ni f \mapsto f(\alpha) \in L.$$

Dies ist eine lineare Abbildung von ${}_LL\mathfrak{G}$ nach ${}_LL$, also ein Element aus dem dualen Vektorraum von ${}_LL\mathfrak{G}$, der mit

$$({}_LL\mathfrak{G})^* := \mathrm{Hom}_L(L\mathfrak{G}, L)$$

bezeichnet wird.

Allgemein ist für einen Linksvektorraum ${}_LV$ der duale Raum $({}_LV)^* := \mathrm{Hom}_L(V, L)$ ein Rechtsvektorraum über L.

Für $\sigma \in ({}_LL\mathfrak{G})^*$ und $f \in L\mathfrak{G}$ bezeichne $f\sigma$ das Bild von f bei σ.

2.1. Lemma.

Sei $\mathfrak{G} \subsetneq \mathfrak{Aut}(L)$, $K := \mathrm{Fix}(\mathfrak{G})$ und sei $(\lambda_j | j \in J)$ eine Familie von $\lambda_j \in L$, dann sind die folgenden Bedingungen (i) und (ii) äquivalent:

(i) die Familie $(\lambda_j | j \in J)$ ist linear abhängig über K in L_K ;
(ii) die Familie $(\sigma_{\lambda_j} | j \in J)$ ist linear abhängig über L in ${}_L(L\mathfrak{G})^*_L$.

Beweis $(i) \Longrightarrow (ii)$: Sei (nach Umindizierung)

$$\sum_{j=1}^{m} \lambda_j\kappa_j = 0 \quad , \quad \kappa_j \in K, \kappa_j \neq 0 \quad ,$$

dann folgt für $g \in \mathfrak{G}$

$$g\sum_{j=1}^{m} \sigma_{\lambda_j}\kappa_j = \sum_{j=1}^{m} g(\lambda_j)\kappa_j$$
$$= \sum_{j=1}^{m} g(\lambda_j\kappa_j) = g(\sum_{j=1}^{m} \lambda_j\kappa_j) = g(0) = 0.$$

Da $\mathfrak{G}$ eine Erzeugendenmenge von $L\mathfrak{G}$ ist, folgt $\sum_{j=1}^{m} \sigma_{\lambda_j} \kappa_j = 0$, d.h. es gilt (ii).

$(ii) \Longrightarrow (i)$: In $L_L^{(J)}$ betrachten wir den Unterraum U der (β_j) mit

$$\sum_{j \in J} \sigma_{\lambda_j} \beta_j = 0.$$

Nach Voraussetzung ist $U \neq 0$. Sei (α_j) ein minimales Element in U; Dann gilt nach Umindizierung und Normierung

$$\sum_{j=1}^{m} \sigma_{\lambda_j} \alpha_j = 0 \ , \alpha_1 = 1, \alpha_j \neq 0 \text{ für } j = 1, \ldots, m.$$

Für $f \in L\mathfrak{G}$ folgt

$$f \sum_{j=1}^{m} \sigma_{\lambda_j} \alpha_j = \sum_{j=1}^{m} f(\lambda_j) \alpha_j = 0.$$

Darauf wird $g \in \mathfrak{G}$ angewendet:

$$g\Big(\sum_{j=1}^{m} f(\lambda_j)\alpha_j\Big) = \sum_{j=1}^{m} gf(\lambda_j) g(\alpha_j) = gf \sum_{j=1}^{m} \sigma_{\lambda_j} g(\alpha_j) = g(0) = 0.$$

Da g in dem Ring $L\mathfrak{G}$ invertierbar ist, durchläuft mit f auch gf alle Elemente aus $L\mathfrak{G}$. Daraus folgt, daß auch

$$\sum_{j=1}^{m} \sigma_{\lambda_j} g(\alpha_j) = 0$$

gilt. Daher ist mit $(\alpha_1, \ldots, \alpha_m)$ auch $\big(g(\alpha_1), \ldots, g(\alpha_m)\big)$ ein minimales Element in U. Also existiert ein $\lambda \in L, \lambda \neq 0$ mit

$$\alpha_j \lambda = g(\alpha_j) \qquad , j = 1, \ldots, m.$$

Wegen $\alpha_1 = 1$ gilt $\lambda = g(1) = 1$, also

$$\alpha_j = g(\alpha_j) \qquad , j = 1, \ldots, m.$$

Da dies für alle $g \in \mathfrak{G}$ gilt, folgt $\alpha_j \in K = \mathrm{Fix}(\mathfrak{G})$. Für $f = 1_L \in L\mathfrak{G}$ ergibt sich dann

$$1_L \sum_{j=1}^{m} \sigma_{\lambda_j} \alpha_j = \sum_{j=1}^{m} \lambda_j \alpha_j = 0,$$

also sind $\lambda_1, \ldots, \lambda_m$ linear abhängig über K.

2.2. Folgerung

Sei $\mathfrak{G} \subsetneq \mathfrak{Aut}(L)$ und sei $K := \mathrm{Fix}(\mathfrak{G})$, dann gilt:

$$\dim(L_K) = n \Longleftrightarrow \dim({}_L L\mathfrak{G}) = n$$
$$\Rightarrow L\mathfrak{G} = \mathrm{End}(L_K).$$

Beweis: Aus 2.1. folgt

$$\dim(L_K) = n \Longrightarrow \dim\big(({}_L L\mathfrak{G})^*_L\big) \geq n.$$

Da nach 1.3.(ii) $\dim\big({}_L\mathrm{End}(L_K)\big) = n$ ist und $L\mathfrak{G} \subset \mathrm{End}(L_K)$ gilt, folgt $\dim({}_L L\mathfrak{G}) \leq n$. Dies impliziert

$$\dim({}_L L\mathfrak{G}) = \dim\big(({}_L L\mathfrak{G})^*_L\big) \leqq n.$$

Zusammen folgt

$$\dim\big(({}_L L\mathfrak{G})^*_L\big) = n = \dim({}_L L\mathfrak{G}) = \dim\big({}_L\mathrm{End}(L_K)\big).$$

Da ${}_L L\mathfrak{G}$ ein Unterraum von ${}_L\mathrm{End}(L_K)$ ist, folgt das wichtige Resultat $L\mathfrak{G}$ $= \mathrm{End}(L_K)$. Damit haben wir alles gezeigt bis auf: $\dim({}_L L\mathfrak{G}) = n \Longrightarrow \dim(L_K) = n$. Aus $\dim({}_L L\mathfrak{G}) = n$ folgt $\dim\big(({}_L L\mathfrak{G})^*_L\big) = n$ und 2.1. impliziert $\dim(L_K) \leqq n$. Wegen $L\mathfrak{G} \subsetneq \mathrm{End}(L_K)$ und $\dim({}_L L\mathfrak{G}) = n$ folgt andererseits nach 1.3.(ii)

$$\dim(L_K) = \dim\big({}_L\mathrm{End}(L_K)\big) \geq n,$$

also zusammen $\dim(L_K) = n$.

Das Resultat $L\mathfrak{G} = \mathrm{End}(L_K)$ ist die Grundlage für alle weiteren Überlegungen. Dadurch kann die Gruppeneigenschaft von $\mathfrak{G}$ optimal ausgenutzt werden.

Als unmittelbare Folge aus 2.1. und 2.2. erwähnen wir noch ein bemerkenswertes Resultat.

2.3. Folgerung

Sei $\mathfrak{G} \subsetneq \mathfrak{Aut}(L)$ und sei $K := \mathrm{Fix}(\mathfrak{G})$, dann gilt:
Ist $\lambda_1, \ldots, \lambda_n$ eine Basis von L_K, dann ist $\sigma_{\lambda_1}, \ldots, \sigma_{\lambda_n}$ eine Basis von $\big({}_L\mathrm{End}(L_K)\big)^*_L$.

3. Galoissche Erweiterungen und abgeschlossene Untergruppen

Wir beginnen damit, den von kommutativen Körpern bekannten Begriff der Galoisschen Erweiterung nun für Schiefkörper zu definieren.

3.1. Definition

1) Sei K ein Unterschiefkörper des Schiefkörpers L. L heißt Galoissche Erweiterung von K und K Galoisscher Unterschiefkörper von L, kurz Galoissch $L/K :\Longleftrightarrow$ es existiert eine Untergruppe $\mathfrak{G} \subsetneq \mathfrak{Aut}(L))$ mit

$$K = \mathrm{Fix}(\mathfrak{G}) \wedge \dim(L_K) < \infty.$$

2) Ist Galoissch L/K, dann heißt

$$\mathfrak{Fix}(K) := \{g | g \in \mathfrak{Aut}(L) \wedge \forall \kappa \in K[g(\kappa) = \kappa]\}.$$

die Galoisgruppe von L/K.

Zunächst ist klar, daß $\mathfrak{Fix}(K)$ eine Untergruppe von $\mathfrak{Aut}(L)$ ist und zwar eine solche, die jedes $\mathfrak{G}$ mit $K = \mathrm{Fix}(\mathfrak{G})$ enthält. Im kommutativen Fall ist $\mathfrak{G} = \mathfrak{Fix}(K)$, jedoch im allgemeinen nicht bei Schiefkörpern! Damit ergibt sich die Frage, wie man $\mathfrak{Fix}(K)$ aus $\mathfrak{G}$ gewinnen kann. Ferner möchte man in der Definition der Galoisschen Erweiterung die Bedingung $\dim(L_K) < \infty$ durch eine Bedingung über $\mathfrak{G}$ allein ersetzen. Auf diese Fragen wird im Folgenden eingegangen. Dabei spielen innere Automorphismen eine wesentliche Rolle. Wir müssen daher zunächst einige Eigenschaften von inneren Automorphismen erwähnen.

Sei wie bisher L ein Schiefkörper und sei $0 \neq \lambda \in L$. Mit

$$t_\lambda : L \ni \xi \mapsto \lambda^{-1}\xi\lambda \in L$$

wird der durch λ erzeugte innere Automorphismus von L bezeichnet (beachte $t_\lambda(\xi) = \lambda^{-1}\xi\lambda$ und nicht $\lambda\xi\lambda^{-1}$, was auch möglich wäre!). Die folgenden Eigenschaften sind leicht zu bestätigen. Dabei sei Z das Zentrum von L.

3.2. Bemerkung

Seien $\kappa, \lambda \in L, \kappa \neq 0, \lambda \neq 0, g \in \mathfrak{Aut}(L)$, dann gilt

(i) $t_\kappa t_\lambda = t_{\lambda\kappa}$ $\quad, t_\kappa^{-1} = t_{\kappa^{-1}}$

(ii) $t_\kappa = t_\lambda \Longleftrightarrow \exists z \in Z[\lambda = z\kappa]$

(iii) $gt_\kappa = t_{g(\kappa)}g$ $\quad, gt_\kappa g^{-1} = t_{g(\kappa)}$

(iv) Die inneren Automorphismen von L bilden einen Normalteiler $\mathfrak{T}$ von $\mathfrak{Aut}(L)$ und es gilt $\mathfrak{T} \cong L^*/Z^*$ $(L^* = L \setminus \{0\}, Z^* = Z \setminus \{0\})$.

Sei $\mathfrak{G} \subsetneq \mathfrak{Aut}(L)$, dann bezeichne

$$\mathfrak{J}(\mathfrak{G}) := \mathfrak{G} \cap \mathfrak{T}.$$

Nach 3.2.(iii) ist $\mathfrak{J}(\mathfrak{G})$ Normalteiler von $\mathfrak{G}$ und mit $g \in \mathfrak{G}, t_\lambda \in \mathfrak{J}(\mathfrak{G})$ gilt auch $t_{g(\lambda)} \in \mathfrak{J}(\mathfrak{G})$. Ferner sei

$$T(\mathfrak{G}) := \{\lambda | \lambda \in L \wedge t_\lambda \in \mathfrak{G}\}.$$

Dies ist offenbar eine bei Produkten, Inversenbildung und Anwendung von Automorphismen aus $\mathfrak{G}$ abgeschlossene Teilmenge von L^*, die Z^* enthält.
Spezialfall: Ist $\mathfrak{J}(\mathfrak{G}) = \{t_1\}$, dann ist $T(\mathfrak{G}) = Z^*$.

Schließlich brauchen wir

$$Q(\mathfrak{G}) := \text{der von } T(\mathfrak{G}) \text{ erzeugte Unterschiefkörper von } L.$$

Wegen $g\big(T(\mathfrak{G})\big) = T(\mathfrak{G})$, $g \in \mathfrak{G}$ ist auch $g\big(Q(\mathfrak{G})\big) = Q(\mathfrak{G})$.

Es folgt eine letzte Bezeichnung. Zu einem Unterschiefkörper H von L sei

$$\mathfrak{T}(H) := \{t_\eta | 0 \neq \eta \in H\}.$$

Dies ist offenbar eine Gruppe von inneren Automorphismen und es gilt $\mathfrak{T} = \mathfrak{T}(L)$.

3.3. Definition

Sei $\mathfrak{G} \subsetneq \mathfrak{Aut}(L)$.

(i) $\mathfrak{G}$ heißt abgeschlossen $:\Longleftrightarrow T(\mathfrak{G}) = Q(\mathfrak{G})^*$

(ii) Die von $\mathfrak{G}$ und $\mathfrak{T}\big(Q(\mathfrak{G})\big)$ erzeugte Untergruppe von $\mathfrak{Aut}(L)$ heißt der Abschluß von $\mathfrak{G}$, bezeichnet mit $\widehat{\mathfrak{G}}$.

3.4. Hilfssatz

Sei $\mathfrak{G} \subsetneq \mathfrak{Aut}(L)$.

(i) $\mathfrak{G}$ ist abgeschlossen $\Longleftrightarrow \mathfrak{G} = \widehat{\mathfrak{G}}$.

(ii) $\widehat{\mathfrak{G}}$ ist die kleinste $\mathfrak{G}$ enthaltende abgeschlossene Untergruppe von $\mathfrak{Aut}(L)$ und es gilt $Q(\mathfrak{G}) = Q(\widehat{\mathfrak{G}})$.

(iii) Die Abbildung
$\mathfrak{G}|\mathfrak{J}(\mathfrak{G}) \ni \mathfrak{J}(\mathfrak{G})g \mapsto \mathfrak{J}(\widehat{\mathfrak{G}})g \in \widehat{\mathfrak{G}}/\mathfrak{J}(\widehat{\mathfrak{G}})$
ist ein Gruppenisomorphismus.

Beweis:

(i) $\Longrightarrow$: Wegen $T(\mathfrak{G}) = Q(\mathfrak{G})^*$ folgt $\mathfrak{T}\big(Q(\mathfrak{G})\big) = \mathfrak{J}(\mathfrak{G}) \subsetneq \mathfrak{G} \Longrightarrow \mathfrak{G} = \widehat{\mathfrak{G}}$.

(i) $\Longleftarrow$: Wegen $\mathfrak{G} = \widehat{\mathfrak{G}} \Longrightarrow \mathfrak{T}\big(Q(\mathfrak{G})\big) \subsetneq \mathfrak{G} \Longrightarrow T(\mathfrak{G}) = Q(\mathfrak{G})^* \Longrightarrow \mathfrak{G}$ abgeschlossen.

(ii) : Wegen $\mathfrak{T}\big(Q(\mathfrak{G})\big) \subset \widehat{\mathfrak{G}}$ folgt

$$Q(\mathfrak{G})^* \subset T(\widehat{\mathfrak{G}}) \tag{1}$$

Für $g \in \mathfrak{G}, t_\lambda \in \mathfrak{T}\big(Q(\mathfrak{G})\big)$ gilt

(2) $$gt_\lambda = t_{g(\lambda)}g \qquad \text{mit } t_{g(\lambda)} \in \mathfrak{T}(Q(\mathfrak{G}))$$

Nach dem Untergruppenkriterium sind die Elemente aus $\widehat{\mathfrak{G}}$ endliche Produkte von Elementen aus $\mathfrak{G}$ und aus $\mathfrak{T}(Q(\mathfrak{G}))$. Durch sukzessive Anwendung von (2) (Durchschieben von Faktoren aus $\mathfrak{G}$ nach rechts), kann man diese in der Form

(3) $$t_\beta g \quad , g \in \mathfrak{G} \quad , t_\beta \in \mathfrak{T}(Q(\mathfrak{G}))$$

schreiben. Sei nun $t_\lambda \in \mathfrak{J}(\widehat{\mathfrak{G}})$ und sei

$$t_\lambda = t_\beta g \quad , g \in \mathfrak{G} \quad , t_\beta \in \mathfrak{T}(Q(\mathfrak{G})),$$

dann folgt $g = t_{\lambda\beta^{-1}} \in \mathfrak{J}(\mathfrak{G})$, also $\lambda\beta^{-1} \in T(\mathfrak{G}) \subset Q(\mathfrak{G})$. Folglich gilt $\lambda \in Q(\mathfrak{G})$, also $T(\widehat{\mathfrak{G}}) \subset Q(\mathfrak{G})$. Zusammen mit (1) folgt

$$T(\widehat{\mathfrak{G}}) = Q(\mathfrak{G})^*.$$

Da somit $T(\widehat{\mathfrak{G}}) \cup \{0\}$ bereits ein Schiefkörper und zwar $Q(\mathfrak{G})$ ist, ist auch

$$Q(\widehat{\mathfrak{G}})^* = T(\widehat{\mathfrak{G}}) = Q(\mathfrak{G})^*.$$

Also ist $\widehat{\mathfrak{G}}$ abgeschlossen und $Q(\mathfrak{G}) = Q(\widehat{\mathfrak{G}})$. Sei nun $\mathfrak{H} \subsetneq \mathfrak{Aut}(L), \mathfrak{H}$ abgeschlossen und $\mathfrak{G} \subsetneq \mathfrak{H}$. Folglich muß $Q(\mathfrak{G}) \subset Q(\mathfrak{H}) = T(\mathfrak{H}) \cup \{0\}$ und daher auch $\mathfrak{T}(Q(\mathfrak{G})) \subset \mathfrak{J}(\mathfrak{H})$ gelten. Dies impliziert $\widehat{\mathfrak{G}} \subsetneq \mathfrak{H}$.

(iii) Wegen $\mathfrak{J}(\mathfrak{G}) \subset \mathfrak{J}(\widehat{\mathfrak{G}})$ handelt es sich um einen Gruppenhomomorphismus, der wegen (3) surjektiv ist. Wegen $\mathfrak{J}(\widehat{\mathfrak{G}}) \cap \mathfrak{G} = \mathfrak{J}(\mathfrak{G})$ ist er auch injektiv.

Unser nächstes Ziel ist es zu zeigen, daß für eine Galoissche Erweiterung L/K mit $K = \mathrm{Fix}(\mathfrak{G})$ die Galoisgruppe $\mathfrak{Fix}(K) = \widehat{\mathfrak{G}}$ ist und daß

$$\dim(L_K) = \mathrm{Ord}(\mathfrak{G}/\mathfrak{J}(\mathfrak{G}))\dim({}_Z Q(\mathfrak{G}))$$

gilt.

3.5. Hilfssatz

Seien $h, g_1, \ldots, g_m \in \mathfrak{Aut}(L)$, seien $g_1, \ldots, g_m$ linear unabhängig über L(in ${}_L E$) und es gelte

(4) $$h = \sum_{j=1}^{m} \alpha_j g_j \quad , \ 0 \neq \alpha_j \in L, j = 1, \ldots, m$$

Dann folgt

(5) $$h = t_{\alpha_j^{-1}} g_j \quad , \ j = 1, \ldots, m$$

Ist $h = t_\beta, 0 \neq \beta \in L$ ein innerer Automorphismus, dann sind alle g_j (beachte $\alpha_j \neq 0$!) innere Automorphismen und es gilt

$$g_j = t_{\beta\alpha_j} \quad , \; j = 1, \ldots, m \tag{6}$$

Beweis: Wegen der Produktregel in E

$$g\xi = g(\xi)g \quad , \xi \in L \; , \; g \in \mathfrak{Aut}(L)$$

folgt aus (4)

$$h(\xi)^{-1} h\xi = h = h(\xi)^{-1} \sum_{j=1}^{m} \alpha_j g_j(\xi) g_j. \tag{7}$$

Da die $g_1, \ldots, g_m$ linear unabhängig sind, ist die Darstellung (4) eindeutig. Also folgt aus (4) und (7)

$$\alpha_j = h(\xi)^{-1} \alpha_j g_j(\xi) \quad , \xi \in L, j = 1, \ldots, m.$$

und daher gilt

$$h(\xi) = \alpha_j g_j(\xi) \alpha_j^{-1} = (t_{\alpha_j^{-1}} g_j)(\xi)$$

also (5). Ist $h = t_\beta$, dann impliziert (5)

$$g_j = t_{\alpha_j} t_\beta = t_{\beta\alpha_j} \quad , \; j = 1, \ldots, m,$$

also (6).

3.6. Hilfssatz

Seien $\beta, \lambda_1, \ldots, \lambda_m \in L \; \beta \neq 0$. Dann sind die folgenden Bedingungen (i) und (ii) äquivalent:

(i) $\lambda_1, \ldots, \lambda_m$ sind linear unabhängig über Z in ${}_Z L$ und

$$\beta = \sum_{j=1}^{m} z_j \lambda_j \quad , \; z_j \in Z. \tag{8}$$

(ii) $t_{\lambda_1}, \ldots, t_{\lambda_m}$ sind linear unabhängig über L in ${}_L E$ und

$$t_\beta = \sum_{j=1}^{m} \alpha_j t_{\lambda_j} \quad , \; \alpha_j \in L. \tag{9}$$

Beweis

(i) $\Longrightarrow$ (9) : Aus (8) folgt unmittelbar (nachrechnen)

$$t_\beta = \beta^{-1} \sum z_j \lambda_j t_{\lambda_j},$$

also gilt (9) mit

$$\alpha_j = \beta^{-1} z_j \lambda_j \qquad , j = 1, \ldots, m.$$

(ii) $\Longrightarrow$ (8) : Nach (6) gilt für $j = 1, \ldots, m$ mit $\alpha_j \neq 0$

$$t_{\lambda_j} = t_{\beta\alpha_j}.$$

Folglich gibt es $z_j \in Z$ mit $z_j\lambda_j = \beta\alpha_j$ wobei im Falle $\alpha_j = 0$ $z_j = 0$ zu setzen ist. Wendet man (9) auf $1 \in L$ an, so ergibt sich

$$1 = \sum_{j=1}^{m} \alpha_j$$

Multiplikation dieser Gleichung mit β und Einsetzen von $z_j\lambda_j = \beta\alpha_j$ liefert (8). Wir kommen nun zum Beweis der restlichen Behauptungen.
(i) $\Longrightarrow$ $t_{\lambda_1}, \ldots, t_{\lambda_m}$ sind linear unabhängig über L: Beweis indirekt. Angenommen, diese wären linear abhängig. Sei die Indizierung so, daß
$t_{\lambda_1}, \ldots, t_{\lambda_k}$ mit $k < m$ eine maximale linear unabhängige Teilmenge ist. Dann läßt sich t_{λ_m} als Linearkombination der $t_{\lambda_1}, \ldots, t_{\lambda_k}$ (oder weniger) mit Koeffizienten in L schreiben. Da schon (ii) $\Longrightarrow$ (8) gezeigt ist, wäre λ_m Linearkombination der $\lambda_1, \ldots, \lambda_k$ mit Koeffizienten in Z. *Widerspruch!* Analog zeigt man, daß (ii) die lineare Unabhängigkeit von $\lambda_1, \ldots, \lambda_m$ impliziert.

Bei den weiteren Überlegungen brauchen wir zu einem Unterschiefkörper K von L den Zentralisator von K in L, bezeichnet mit $\mathrm{Za}(K)$. bekanntlich ist

$$\mathrm{Za}(K) := \{\beta | \beta \in L \wedge \forall \kappa \in K[\kappa\beta = \beta\kappa]\}.$$

Dies ist offentsichtlich ein Z enthaltender Unterschiefkörper von L. Für $\beta \neq 0$ ist die Bedingung $\kappa\beta = \beta\kappa$ äquivalent mit

$$\beta^{-1}\kappa\beta = t_\beta(\kappa) = \kappa \tag{10}$$

Sei jetzt $\mathfrak{G} \subset \mathfrak{Aut}(L)$ und seien

$$K := \mathrm{Fix}(\mathfrak{G}) \qquad , \ \mathfrak{K} := \mathfrak{Fix}(K),$$

dann folgt $\mathfrak{G} \subset \mathfrak{K}$ und wegen (10) gilt

$$\mathrm{Za}(K)^* = T(\mathfrak{K}) = Q(\mathfrak{K})^* \tag{11}$$

Wir können nun die im Anschluß an 3.1 aufgeworfenen Fragen beantworten.

3.7. Satz

Sei Galoissch L/K und $K = \mathrm{Fix}(\mathfrak{G})$ mit $\mathfrak{G} \subset \mathfrak{Aut}(L)$. Dann gilt
(i) $\widehat{\mathfrak{G}} = \mathfrak{Fix}(K) = \mathfrak{K}$

(ii) $T(\mathfrak{G})$ enthält eine Basis von $\mathrm{Za}(K)$ über Z

12) $$\wedge \qquad Q(\mathfrak{G})^* = \mathrm{Za}(K)^* = T\wedge(\mathfrak{G})$$

(iii) Ist $\lambda_1, \ldots, \lambda_k$ eine Basis von $\mathrm{Za}(K)$ über Z und ist $g_1, \ldots, g_m$ ein Repräsentantensystem von $\mathfrak{G}/\mathfrak{J}(\mathfrak{G})$, dann ist

13) $$\{t_{\lambda_i} g_j | i = 1, \ldots, k \qquad , j = 1, \ldots, m\}$$

eine Basis von $L\mathfrak{G} =_L \mathrm{End}(L_K)$. Folglich gilt

14) $$\dim(L_K) = \dim(Za(K)_Z)\mathrm{Ord}(\mathfrak{G}/\mathfrak{J}(\mathfrak{G}))$$

Beweis:

(i), (ii): Zur Abkürzung setzen wir $\mathfrak{K} := \mathfrak{Fix}(K)$. Dann gilt offensichtlich

$$T(\mathfrak{K}) = \mathrm{Za}(K)^* = Q(\mathfrak{K})^*$$

Also ist $\mathfrak{K}$ abgeschlossen. Ausgangspunkt für die weiteren Überlegungen ist die Situation

$$\mathfrak{G} \subsetneq \mathfrak{K} \subset L\mathfrak{G} = \mathrm{End}(L_K).$$

In ${}_L L\mathfrak{G}$ betrachten wir eine Basis von Elementen aus $\mathfrak{G}$, in der wir die inneren Automorphismen an den Anfang schreiben:

(15) $$\{t_{\lambda_1}, \ldots, t_{\lambda_k}, h_1, \ldots, h_l\}.$$

Falls nur innere Automorphismen vorhanden sind, gibt es keine h_j. Hingegen gibt es immer mindestens einen inneren Automorphismus in (15) (Folgt aus 3.5 für $\beta = 1 \in L$). In (15) sind $\lambda_1, \ldots, \lambda_k \in \mathrm{Za}(K)$ und nach 3.6 sind diese Elemente linear unabhängig über Z. Da für jedes $\beta \in \mathrm{Za}(K), \beta \neq 0$ folgt $t_\beta \in \mathfrak{K} \subset L\mathfrak{G}$, läßt sich nach 3.5 t_β als Linearkombination der $t_{\lambda_i}, i = 1, \ldots k$ schreiben. Nach 3.5 ist dann β Linearkombination der $\lambda_1, \ldots, \lambda_k$ mit Koeffizienten in Z. Also ist dies eine Basis von ${}_Z\mathrm{Za}(K)$ und zwar mit Elementen aus $T(\mathfrak{G})$. Daraus folgt

$$\mathrm{Za}(K) \subset Q(\mathfrak{G}).$$

Da andererseits

$$Q(\mathfrak{G})^* \subset Q(\mathfrak{K})^* = \mathrm{Za}(K)^* = T(\mathfrak{K})$$

gilt, folgt

$$Q(\mathfrak{G})^* = Q(\mathfrak{K})^* = \mathrm{Za}(K)^* = T(\mathfrak{K}).$$

Da $\widehat{\mathfrak{G}}$ die durch $\mathfrak{G}$ und $\mathfrak{T}(Q(\mathfrak{G}))$ erzeugte Gruppe ist und beide in $\mathfrak{K}$ liegen, ist $\widehat{\mathfrak{G}} \subsetneq \mathfrak{K}$. Sei jetzt $h \in \mathfrak{K}$, dann folgt wegen $h \in L\mathfrak{G}$ nach (5)

$$h = t_{\alpha_j^{-1}} g_j$$

mit g_j aus der Basis (15), also $g_j \in \mathfrak{G} \subsetneq \mathfrak{K}$ und $t_{\alpha_j^{-1}} \in \mathfrak{K}$, also $\alpha_j^{-1} \in \mathrm{Za}(K) = Q(\mathfrak{G})$. folglich gilt auch $\mathfrak{K} \subset \widehat{\mathfrak{G}}$. Damit haben wir $\widehat{\mathfrak{G}} = \mathfrak{K} = \mathfrak{Fix}(K)$.
(iii): Wir zeigen zuerst, daß (13) eine linear unabhängige Menge ist. Beweis indirekt. Dann kann man eines der Elemente aus (13) als Linearkombination von gewissen anderen darstellen. Die Indizierung sei so, daß

$$t_{\lambda_k} g_m = \sum_{i=1}^{k_\circ} \sum_{j=1}^{m_\circ} \alpha_{ij} t_{\lambda_i} g_j$$

mit $k_\circ \leq k, m_\circ \leq m, (k_\circ, m_\circ) \neq (k, m)$ und die Menge $\{t_{\lambda_i} g_j | i = 1, \ldots, k_\circ, j = 1, \ldots, m_\circ\}$ linear unabhängig sei. Nach (5) folgt für $\alpha_{ij} \neq 0$

$$t_{\lambda_m} g_m = t_{\alpha_{ij}^{-1}} t_{\lambda_i} g_j, \quad \begin{matrix} i = 1, \ldots, k_\circ \\ j = 1, \ldots, m_\circ \end{matrix} \tag{16}$$

Nach Wahl der g_j (in verschiedenen Restklassen von $\mathfrak{G}$ mod $\mathfrak{J}(\mathfrak{G})$), kann $\alpha_{ij} \neq 0$ nur für $j = m$ gelten. Also folgt $m_\circ = m$ und (16) hat die Form

$$t_{\lambda_k} g_m = \sum_{i=1}^{k_\circ} \alpha_{im} t_{\lambda_i} g_m.$$

Dies impliziert

$$t_{\lambda_k} = \sum_{i=1}^{k_\circ} \alpha_{im} t_{\lambda_i}. \tag{17}$$

Wegen $m_\circ = m$ muß $k_\circ < k$ gelten. Dann steht (17) aber im Widerspruch zur linearen Unabhängigkeit der $t_{\lambda_1}, \ldots, t_{\lambda_k}$, die nach 3.6 gegeben ist.

Schließlich zeigen wir, daß (13) eine Erzeugendenmenge von ${}_L L\mathfrak{G}$ ist. Es genügt zu zeigen, daß sich jedes $g \in \mathfrak{G}$ damit darstellen läßt. Sei g in der gleichen Restklasse von $\mathfrak{G}/\mathfrak{J}(\mathfrak{G})$ wie etwa g_1 und sei $g = t_\beta g_1$ mit $\beta \in \mathrm{Za}(K)$. Ist $\beta = \sum_{i=1}^{k} z_i \lambda_i$, $z_i \in Z$ die Basisdarstellung, dann folgt

$$t_\beta = \beta^{-1} \sum_{i=1}^{k} z_i \lambda_i t_{\lambda_i},$$

also

$$g = t_\beta g_1 = \sum_{i=1}^{k} \beta^{-1} z_i \lambda_i t_{\lambda_i} g_1.$$

Damit ist der Beweis vollständig.

4. Der Hauptsatz

Wir brauchen zunächst eine weitere Anwendung der minimalen Elemente.

Sei $\emptyset \neq \mathfrak{G} \subset \mathfrak{Aut}(L)$ ($\mathfrak{G}$ braucht nur Teilmenge von $\mathfrak{Aut}(L)$ zu sein), dann sei $L\mathfrak{G}$ wie bisher der durch $\mathfrak{G}$ erzeugte Unterraum von ${}_LE$. Für $g \in \mathfrak{G}, \lambda \in L$ gilt die Produktregel $g\lambda = g(\lambda)g$ in E. Daher ist $L\mathfrak{G}$ auch L- Rechtsvektorraum.

4.1. Definition

Voraussetzungen wie zuvor. Sei $\emptyset \neq R \subset L\mathfrak{G}$. R heißt Bi-Unterraum von $L\mathfrak{G} :\Longleftrightarrow$

$$LR = R \qquad \wedge \qquad RL = R.$$

4.2. Lemma

Ist $0 \neq R$ Bi-Unterraum von $L\mathfrak{G}$, dann gibt es $\mathfrak{H} \subset R \cap \mathfrak{Aut}(L)$ mit $R = L\mathfrak{H}$. Zu $h \in \mathfrak{H}$ gibt es $\lambda \in L, g \in \mathfrak{G}$ mit $h = t_\lambda g$.

Beweis: Sei $(g_j | j \in J)$ eine Basis von ${}_LL\mathfrak{G}$ mit $g_j \in \mathfrak{G}$. Sei

$$f = \sum_{j=1}^{m} \alpha_j g_j \ , \alpha_1 = 1 \ \alpha_j \neq 0 \ , j = 1, \ldots, m$$

ein minimales Element in R, R betrachtet als Unterraum von ${}_LL\mathfrak{G}$. Dann ist für $0 \neq \xi \in L$ auch $f\xi \in R$ und

$$f\xi = \sum_{j=1}^{m} \alpha_j g_j(\xi) g_j$$

ist ebenfalls ein minimales Element aus R, denn $\mathrm{tr}(f) = \mathrm{tr}(f\xi)$. Also existiert ein $\lambda \in L, \lambda \neq 0$ mit

$$\lambda \alpha_j = \alpha_j g_j(\xi) \qquad , j = 1, \ldots, m.$$

Wegen $\alpha_1 = 1$ folgt $\lambda = g_1(\xi)$ sowie

$$f(\xi) = \sum_{j=1}^{m} \alpha_j g_j(\xi) = g_1(\xi) \sum_{j=1}^{m} \alpha_j, \tag{18}$$

(beachte: $f(\xi)$, nicht $f\xi$.)
Wegen $f \neq 0$ (da f minimales Element) existiert ein $\xi_\circ \in L$ mit $f(\xi_\circ) \neq 0$, also muß $\alpha := \sum_{j=1}^{m} \alpha_j \neq 0$ gelten und dann folgt aus (18)

$$\alpha^{-1} f(\xi) = (t_\alpha g_1)(\xi),$$

also

$$h := t_\alpha g_1 \in R \cap \mathfrak{Aut}(L), g_1 \in \mathfrak{G}$$

und

$$f = \alpha h.$$

Da die minimalen Elemente R erzeugen, ist auch

$$\mathfrak{H} := R \cap \mathfrak{Aut}(L)$$

Erzeugendenmenge von ${}_L R$.

4.3. Folgerung

Ist L/K Galoissch und ist H ein Schiefkörper mit $K \subsetneq H \subsetneq L$, dann ist L/H Galoissch.

Beweis:

Es ist offensichtlich

$$\mathrm{End}(L_H) \subset \mathrm{End}(L_K) = L\mathfrak{G}$$

und $\mathrm{End}(L_H)$ ist ein Bi-Unterraum von $L\mathfrak{G}$. Folglich gibt es nach 4.2 $\mathfrak{H} \subset \mathrm{End}(L_H) \cap \mathfrak{Aut}(L)$ mit $\mathrm{End}(L_H) = L\mathfrak{H}$. Da $\mathrm{End}(L_H)$ ein Ring ist und mit jedem Automorphismus auch den inversen enthält, kann $\mathfrak{H}$ als Gruppe angenommen werden. Seien $\xi \in L, \eta \in H$, dann gilt für $h \in \mathfrak{H} (\subset \mathrm{End}(L_H)!)$

$$h(\xi\eta) = h(\xi)h(\eta) = h(\xi)\eta.$$

Für $\xi = 1$ folgt $h(\eta) = \eta$. Also gilt $H \subset \mathrm{Fix}(\mathfrak{H})$. Sei $\lambda \in L, \lambda \notin H$, dann existiert nach 1.3.(i) ein $\xi \in L$ und ein

$$f = \sum_{j=1}^{m} \alpha_j h_j \in L\mathfrak{H} \qquad , h_j \in \mathfrak{H}$$

mit

$$f(\xi\lambda) = \sum_{j=1}^{m} \alpha_j h_j(\xi\lambda) = \sum_{j=1}^{m} \alpha_j h_j(\xi) h_j(\lambda)$$

$$\neq f(\xi)\lambda = \sum_{j=1}^{m} \alpha_j h_j(\xi)\lambda$$

Daher kann nicht $h_j(\lambda) = \lambda$ für alle h_j gelten. Also folgt $\lambda \notin \mathrm{Fix}(\mathfrak{H})$, d.h. $H = \mathrm{Fix}(\mathfrak{H})$.

4.4. Der Hauptsatz der Galoisschen Theorie

Sei L/K Galoissch mit der Galoisgruppe $\mathfrak{K}$. Bezeichne $ZS(L/K)$ die Menge der Schiefkörper zwischen K und L und $\mathfrak{UU}(\mathfrak{K})$ die Menge der abgeschlossenen Untergruppen von $\mathfrak{K}$. Dann ist

$$\mathfrak{Fix} : ZS(L/K) \ni H \mapsto \mathfrak{Fix}(H) \in \mathfrak{UU}(\mathfrak{K})$$

eine bijektive Abbildung mit der Umkehrabbildung

$$\mathrm{Fix} : \mathfrak{AU}(\mathfrak{K}) \ni \mathfrak{H} \mapsto \mathrm{Fix}(\mathfrak{H}) \in ZS(L/K).$$

Beweis:

Zum Beweis genügt es zu zeigen, daß die Hintereinanderausführung Fix$\mathfrak{Fix}$ die Identität von $ZS(L/K)$ und $\mathfrak{Fix}$Fix die Identität von $\mathfrak{AU}(\mathfrak{K})$ ist. Sei $H \in ZS(L/K)$, dann gibt es, wie zuvor gezeigt, eine Gruppe $\mathfrak{H} \subsetneq \mathfrak{Aut}(L)$ mit $H = \mathrm{Fix}(\mathfrak{H})$. Nach 3.7. ist $\mathfrak{Fix}(H) = \widehat{\mathfrak{H}}$ abgeschlossen und wegen $\mathfrak{H} \subsetneq \widehat{\mathfrak{H}}$ gilt auch

$$H = \mathrm{Fix}(\widehat{\mathfrak{H}}) = \mathrm{Fix}\mathfrak{Fix}(H).$$

Wegen $K \subsetneq H$ ist selbstverständlich auch $\mathfrak{Fix}(H) \subsetneq \mathfrak{K} = \mathfrak{Fix}(K)$, also $\mathfrak{Fix}(H) \in \mathfrak{AU}(\mathfrak{K})$. Sei nun $\mathfrak{H} \in \mathfrak{AU}(\mathfrak{K})$, dann ist

$$K \subsetneq \mathrm{Fix}(\mathfrak{H}) \subsetneq L$$

und nach 3.7. gilt

$$\mathfrak{Fix}(\mathrm{Fix}(\mathfrak{H})) = \widehat{\mathfrak{H}}.$$

Da $\mathfrak{H}$ abgeschlossen ist, ist aber $\mathfrak{H} = \widehat{\mathfrak{H}}$. Damit ist der Hauptsatz bewiesen.

Wie im kommutativen Fall, kehren die Abbildungen Fix und $\mathfrak{Fix}$ Inklusionen um.

Enthält $\mathfrak{K}$ nur den inneren Automorphismus $t_1 (1 \in L)$, dann gilt für jede Untergruppe $\mathfrak{H} \subsetneq \mathfrak{K} : T(\mathfrak{H}) = Z$. Also ist jetzt jede Untergruppe abgeschlossen, wie im kommutativen Fall.

Sind hingegen alle Automorphismen aus $\mathfrak{K}$ innere, dann ist

$$ZS(L/K) \ni H \mapsto \mathfrak{Fix}(H) \mapsto Q(\mathfrak{Fix}(H)) \in ZS(\mathrm{Za}(K)/Z)$$

eine bijektive Abbildung zwischen $ZS(L/K)$ und den Zwischenschiefkörpern zwischen dem Zentrum Z von L und dem Zentralisator $\mathrm{Za}(K)$ von K in L. Berücksichtigt man noch $Q(\mathfrak{Fix}(H)) = \mathrm{Za}(H)$, so erhält man eine Bijektion, die jedem $H \in ZS(L/K)$ ihren Zentralisator zuordnet. Das ergibt die „innere Galoissche Theorie".

5. Fortsetzung von Isomorphismen

5.1. Definition

Seien $K \subsetneq H \subsetneq L$ Schiefkörper. Ein Schiefkörperhomomorphismus

$$h : H \longrightarrow L$$

heißt ein Isomorphismus von H in L über $K :\Longleftrightarrow \forall \kappa \in K[h(\kappa) = \kappa]$.

Wegen $h(1) = 1, 1 \in K$ ist h ein Monomorphismus. Genau genommen besteht der Isomorphismus nur zwischen H und $h(H)$. Wir halten uns aber an die übliche Bezeichnung und nennen h einen Isomorphismus.

5.2. Satz

Ist L/K Galoissch mit der Galoisgruppe $\mathfrak{K}$, dann wird jeder Isomorphismus eines Zwischenschiefkörpers H zwischen K und L in L über K von einem Element aus $\mathfrak{K}$ induziert.

Beweis:

Sei $h : H \longrightarrow L$ ein solcher Isomorphismus, dann kann h (auf vielfältige Weise) zu einem Element $f \in \mathrm{End}(L_K)$ fortgesetzt werden: Sei $\eta_1, \ldots, \eta_l$ eine Basis von H/K und

$$\eta_1, \ldots, \eta_l, \lambda_1, \ldots, \lambda_m$$

eine Verlängerung zu einer Basis von L_K. Dann setze man (z.B.)

$$\begin{aligned} f(\eta_i) &:= \quad h(\eta_i) \qquad , i = 1, \ldots, l \\ f(\lambda_j) &:= \quad 0 \qquad\quad , j = 1, \ldots, m \end{aligned}$$

Damit haben wir eine solche Fortsetzung. In $L\mathfrak{K} = \mathrm{End}(L_K)$ legen wir eine Basis

$$g_1, \ldots, g_n \qquad , g_i \in \mathfrak{K}$$

zugrunde. Unter allen Fortsetzungen von h zu Elementen aus $L\mathfrak{K}$ betrachten wir jetzt eine solche, bei der möglichst wenig Koeffizienten in der Basisdarstellung $\neq 0$ sind; sei dies bei entsprechender Numerierung

$$f = \sum_{i=1}^{m} \alpha_i g_i \qquad , \alpha_i \neq 0, i = 1, \ldots, m. \tag{19}$$

Für $\xi, \eta \in H$ folgt dann

$$\begin{aligned} h(\xi\eta) &= h(\xi)h\lambda) = h(\xi)f(\eta) \\ &= \sum_{i=1}^{m} h(\xi)\alpha_i g_i(\eta), \end{aligned} \tag{20}$$

sowie

$$h(\xi\eta) = f(\xi\eta) = \sum_{i=1}^{m} \alpha_i g_i(\xi) g_i(\eta) \tag{21}$$

Wir unterscheiden nun zwei Fälle.

1.Fall: Für alle $\xi \in H$ gilt

$$h(\xi)\alpha_1 = \alpha_1 g_1(\xi).$$

Dann folgt

$$h(\xi) = t_{\alpha_1^{-1}} g_1(\xi).$$

Für $\kappa \in K$ ergibt sich

$$\kappa = h(\kappa) = \alpha_1 g_1(\kappa)\alpha_1^{-1} = \alpha_1 \kappa \alpha_1^{-1},$$

also $t_{\alpha_1^{-1}} \in \mathfrak{K}$. Folglich wird jetzt h durch $t_{\alpha_1^{-1}} g_1 \in \mathfrak{K}$ induziert.

2. Fall: Es gibt ein $\xi_\circ \in H$ mit

22) $$h(\xi_\circ)\alpha_1 \neq \alpha_1 g_1(\xi_\circ).$$

Seien dann

23) $$\begin{cases} f_1 := h(\xi_\circ) f \\ f_2 := \sum_{i=1}^{m} \alpha_i g_i(\xi_\circ) g_i \ , \end{cases}$$

so folgt wegen (20) und (21) für alle $\eta \in H$

24) $$(f_1 - f_2)(\eta) = h(\xi_\circ \eta) - h(\xi_\circ \eta) = 0.$$

Wegen (22) kann

$$F := f - \alpha_1 \big(h(\xi_\circ)\alpha_1 - \alpha_1 g_1(\xi_\circ)\big)^{-1}(f_1 - f_2)$$

definiert werden. Wegen (23) gilt $F(\eta) = f(\eta) = h(\eta)$ für alle $\eta \in H$, d.h. auch F ist eine Fortsetzung von h. Aber (19) und (23) liefern die Basisdarstellung

$$F = \sum_{i=2}^{m} \beta_i g_i \qquad , \beta_i \in L \ ,$$

wobei die explizite Form von β_i nicht interessiert. Dies wäre eine Fortsetzung von h mit weniger Koeffizienten $\neq 0$ als f. *Widerspruch!* Es kann also nur der 1. Fall gültig sein.

Es ist nach diesem Satz klar, daß genau alle Isomorphismen von H nach L über K durch ein Repräsentantensystem für die Klassen von $\mathfrak{K}$ modulo $\mathfrak{Fix}(H)$ geliefert werden.

Es ist nach dem Hauptsatz klar, daß L über jedem Zwischenschiefkörper H zwischen K und L Galoissch ist. Bleibt die Frage, wann H über K wieder Galoissch ist. Diese Frage ist nicht so leicht zu beantworten wie im kommutativen Fall, wo dies genau dann gilt, wenn $\mathfrak{Fix}(H) \lhd \mathfrak{K}$($\lhd$ bedeutet Normalteiler).

Zur Beantwortung brauchen wir

$$\mathfrak{K}^H := \{g | g \in \mathfrak{K} \wedge g(H) = H\}$$

Dafür gilt:

$$\mathfrak{K}^H \subsetneq \mathfrak{K} \qquad , \mathfrak{Fix}(H) \lhd \mathfrak{K}^H.$$

Die erste Bedingung ist klar, denn $g_1, g_2 \in \mathfrak{K}^H$ impliziert $g_2^{-1} \in \mathfrak{K}^H$ und $g_1 g_2^{-1} \in \mathfrak{K}^H$. Für die zweite seien $h \in \mathfrak{Fix}(H), g \in \mathfrak{K}^H, \eta \in H$, dann gilt

$$(g^{-1}hg)(\eta) = g^{-1}(h(g(\eta))) = g^{-1}g(\eta) = \eta,$$

also $g^{-1}hg \in \mathfrak{Fix}(H)$.

Es ist nach 5.2 klar, daß die Elemente aus $\mathfrak{K}^H$ alle Automorphismen von H über K indizieren und daß $\mathfrak{K}^H/\mathfrak{Fix}(H)$ isomorph zur Gruppe aller Automorphismen von H über K ist (auch wenn H über K nicht Galoissch ist).

5.4. Satz

Sei L/K Galoissch mit der Galoisgruppe $\mathfrak{K} = \mathfrak{Fix}(K)$ und sei H ein Zwischenkörper zwischen K und L. Dann gilt

(i) Galoissch $H/K \iff \widehat{\mathfrak{K}^H} = \mathfrak{K}$

(ii) Galoissch $H/K \implies \mathfrak{K}^H/\mathfrak{Fix}(H)$ ist isomorph zur Galoisgruppe von H/K.

(iii) $\mathfrak{Fix}(H) \lhd \mathfrak{K} \iff \mathfrak{K}^H = \mathfrak{K}$ ($\implies$ GaloisschH/K)

Beweis:

(i) $\implies$: Wegen 5.2 wird jeder Automorphismus von H/K durch ein Element aus $\mathfrak{K}^H$ induziert. Ist H/K Galoissch, so muß also $\mathrm{Fix}(\mathfrak{K}^H) = K$ gelten. Nach 3.7.(i) folgt $\widehat{\mathfrak{K}^H} = \mathfrak{K}$.

(i) $\impliedby$: Sei $K_1 := \mathrm{Fix}(\mathfrak{K}^H)$, dann ist L/K_1 Galoissch mit der Galoisgruppe $\widehat{\mathfrak{K}^H}$. Nach Voraussetzung gilt $\widehat{\mathfrak{K}^H} = \mathfrak{K}$, also folgt $K_1 = K$. Daher ist H/K Galoissch.

(ii): Die Elemente der Galoisgruppe von H/K werden durch die Elemente von $\mathfrak{K}^H$ induziert. Zwei Elemente aus $\mathfrak{K}^H$ induzieren genau dann den gleichen Automorphismus von H/K, wenn sie sich durch einen Faktor aus $\mathfrak{Fix}(H)$ unterscheiden. Also gilt (ii).

(iii) $\implies$: Seien $g \in \mathfrak{K}, h \in \mathfrak{Fix}(H)$, dann existiert nach Voraussetzung ein $h' \in \mathfrak{Fix}(H)$ mit

$$hg = gh'$$

Folglich gilt für $\eta \in H$

$$hg(\eta) = gh'(\eta) = g(\eta),$$

also

$$g(\eta) \in \mathrm{Fix}\mathfrak{Fix}(H) = H$$

und dies bedeutet $\mathfrak{K}^H = \mathfrak{K}$.

(iii) $\Longleftarrow$: Seien $g \in \mathfrak{K}, h \in \mathfrak{Fix}(H), \eta \in H$, dann folgt $g(\eta) \in H$ aus $\mathfrak{K}^H = \mathfrak{K}$. Damit ergibt sich

$$g^{-1}hg(\eta) = g^{-1}g(\eta) = \eta,$$

also $g^{-1}hg \in \mathfrak{Fix}(H)$, d.h. $\mathfrak{Fix}(H) \lhd \mathfrak{K}$.

Als Anwendung wollen wir zum Schluß ein klassisches Resultat beweisen und zwar den Satz von Wedderburn: Jeder endliche Schiefkörper ist ein Körper. Dazu sind einige Feststellungen notwendig, die auch an sich von Interesse sind.

Sei zunächst L ein beliebiger Schiefkörper mit dem Zentrum Z. Für ein Element $\lambda \in L$ betrachten wir den durch Z und λ erzeugten Unterkörper $Z(\lambda)$ von L. Sei $\mathfrak{U}_\lambda$ die Menge aller Unterkörper von L, die $Z(\lambda)$ enthalten. In $\mathfrak{U}_\lambda$ ist die Inklusion eine Ordnung. Für eine nichtleere, total geordnete Teilmenge ist ihre Vereinigung offensichtlich wieder ein Element in $\mathfrak{U}_\lambda$. Also gibt es in $\mathfrak{U}_\lambda$ ein maximales Element, etwa K_λ. Dann ist K_λ nicht nur maximal in $\mathfrak{U}_\lambda$, sondern K_λ ist ein maximaler Unterkörper von L. Daraus folgt insbesondere, daß L gleich der Vereinigung von maximalen Unterkörpern ist.

Sei jetzt $\dim(L_Z) < \infty$, dann ist L/Z Galoissch mit der Galoisgruppe $\mathfrak{T}(L) =$ Gruppe aller durch die Elemente $\neq 0$ von L erzeugten inneren Automorphismen. Selbstverständlich ist $\mathrm{Fix}((\mathfrak{T}(L)) = Z$ und $\mathfrak{T}(L)$ ist abgeschlossen (denn $T(\mathfrak{T}(L)) = L^*$).

Sei jetzt K ein maximaler Unterkörper von L, dann ist der Zentralisator von K in L gleich K, also $\mathrm{Za}(K) = K$. Die Galoisgruppe $\mathfrak{F}(K)$ von L/K ist dann gleich $\mathfrak{T}(K)$. Sei $\dim(K_Z) = m$, dann folgt nach (14) $\dim(L_K) = m$ (da $\mathfrak{G} = \mathfrak{J}(\mathfrak{G})$) und folglich ist

$$\dim(L_Z) = \dim(L_K)\dim(K_Z) = m^2.$$

Da $\dim(L_Z)$ nicht von K abhängt, gilt $\dim(K_Z) = m$ für jeden maximalen Unterkörper von L.

Sei jetzt L endlich und sei $|K| = q$ (= Elementezahl von K), dann folgt $|L| = q^m$ (wegen $\dim(L_K) = m$). Also gilt auch $|K| = q$ für jeden maximalen Unterkörper von L. Ist umgekehrt H ein Z enthaltender Unterkörper von L mit $\dim(H_Z) = m$, dann ist H maximaler Unterkörper von L (da H in einem solchen enthalten ist).

Wir benutzen nun die folgende Tatsache: Sind K_1 und K_2 zwei endliche Körper gleicher Elementezahl q mit dem gemeinsamen Unterkörper Z, dann sind K_1 und K_2 isomorph über Z (Isomorphie von Zerfällungskörpern über Z).

Wir fassen zusammen: Jedes Element des endlichen Schiefkörpers L liegt in einem maximalen Unterkörper und alle maximalen Unterkörper von L sind isomorph über Z, also sind alle zu einem von ihnen über Z isomorph, etwa zu K. Es gibt höchstens so viele maximale Unterkörper, wie es Isomorphismen von K in L über Z gibt. Wie nach Satz 5.2. am Ende des Beweises festgestellt, ist diese Anzahl gleich dem Index

der Galoisgruppe von $L/K = \mathfrak{T}(K) \cong K^*/Z^*$ in der Galoisgruppe von $L/Z = \mathfrak{T}(L) \cong L^*/Z^*$. Also ist dieser Index gleich

$$\frac{|L^*|}{|K^*|} = \frac{q^m - 1}{q - 1}$$

Die Vereinigungsmenge V aller zu K über Z isomorphen Körper hat daher höchstens

$$\frac{q^m - 1}{q - 1} q \qquad (q = |K|)$$

Elemente. Allerdings haben wir dabei die Elemente 0 und 1 (sogar alle Elemente aus Z), die in allen diesen Körpern enthalten sind, zu oft gezählt. Zählt man 0 und 1 nur einmal, so erhält man die bessere obere Schranke

$$\frac{q^m - 1}{q - 1}(q - 2) + 2 = q^m - \frac{q^m - 1}{q - 1} + 1$$

Diese Zahl ist für $m < 1$ (da stets $q > 1$) echt kleiner als $q^m = |L|$. Dies steht im Widerspruch zu der Tatsache, daß nach den vorhergehenden Feststellungen $V = L$ ist. Also muß $m = 1$, d.h. $L = Z$ sein.