Werk

Titel: Bericht über Fastkörper.

Autor: Wähling, Heinz

PURL: https://resolver.sub.uni-goettingen.de/purl?37721857X_0076|log7

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

Klass. 12 K 05
Jber. Deutsch. Math.-Verein
76 (1974) 41 – 103

Bericht über Fastkörper

Von HEINZ WÄHLING in Hamburg

Inhalt

Einleitung 41
§ 1. Grundlegende Definitionen und vorbereitende Ergebnisse 42
§ 2. Fastkörperpaare 50
§ 3. Endliche Untergruppen der multiplikativen Gruppe eines Fastkörpers. Endliche Fastkörper 58
§ 4. Automorphismen Dicksonscher Fastkörperpaare 64
§ 5. Ein Zassenhauskriterium für unendliche Fastkörper 70
§ 6. Normale Fastkörper 73
§ 7. Normale Fastkörper mit kommutativer bzw. zweiseitiger Inzidenzgruppe 77
§ 8. Kern und Zentrum eines Dicksonschen Fastkörpers 81
§ 9. Fastkörperkonstruktionen 88
Literaturverzeichnis 100

Einleitung

Die ersten echten Fastkörper (Definition 1.1) stammen von L. E. Dickson [14]*) aus einer Arbeit, in der er die Unabhängigkeit eines gewissen Axiomensystems für endliche Körper untersuchte. Durch die Konstruktion einer unendlichen Familie echter endlicher Fastkörper (in [14] „endliche Algebren" genannt) gelang ihm der Nachweis, daß keines der Distributivgesetze entbehrlich ist. 30 Jahre später wurde H. Zassenhaus [66] durch das Studium gewisser endlicher Permutationsgruppen erneut auf Fastkörper geführt. Jede endliche, scharf zweifach transitive Permutationsgruppe ist zu der Gruppe aller injektiven Transformationen $x \to ax + b$ eines endlichen Fastkörpers isomorph (vgl. Satz (1.3)). Zassenhaus verstand unter einem Fastkörper – er führte in [66] diesen Namen ein – allgemeinere Strukturen als es heute üblich ist. Fastkörper in unserem Sinne nannte er vollständig. In [67] löste er das von Dickson aufgeworfene Problem, alle endlichen Fastkörper zu bestimmen. Mit Ausnahme von 7 Typen lassen sie sich sämtlich nach einer auf Dickson zurückgehenden Methode aus Körpern durch Abänderung der Multiplikation mittels geeigneter Körperautomorphismen ableiten (§ 3). H. Karzel [31] axiomatisierte und ver-

*) Zahlen in eckigen Klammern beziehen sich auf das Literaturverzeichnis am Ende des Berichts.

allgemeinerte dieses sog. Dicksonsche Verfahren (§ 2) und konstruierte damit eine Reihe neuer unendlicher Fastkörper. Meines Wissens sind alle bisher entdeckten unendlichen Fastkörper in diesem Sinne „Dicksonsch", d. h. mit Hilfe des Dicksonschen Verfahrens zu gewinnen.

Da projektive Fastkörper (Definition 1.7) zur Konstruktion projektiver Ebenen herangezogen werden können (vgl. etwa [46] und [13]), wird das Interesse an Fastkörpern u. a. durch das augenblicklich sehr intensive Studium projektiver Ebenen wachgehalten. Eine weitere Verbindung zur Geometrie schufen E. Ellers und H. Karzel [16] mit der Einführung der projektiven Inzidenzgruppen, d. s. Kollineationsgruppen projektiver Räume, die auf den Punkten regulär operieren. Die desarguesschen projektiven Inzidenzgruppen einer Dimension $\geqslant 2$ lassen sich mit Hilfe der ebenfalls in [16] eingeführten normalen Fastkörper algebraisch beschreiben (§ 6). Dieser Zusammenhang wird in § 7 weiter verfolgt.

Das Zassenhauskriterium in § 5 sagt aus, daß ein Fastkörper Dicksonsch ist, sofern seine multiplikative Gruppe einen Normalteiler mit gewissen dort aufgeführten Eigenschaften besitzt. Dieses Ergebnis ist insofern von Bedeutung, als das Dicksonsche Verfahren zusätzliche Information über den Fastkörper liefert. Beispielsweise sind die Automorphismengruppen Dicksonscher Fastkörper in vielen Fällen überschaubar (§ 4), und über das Zentrum und den Kern läßt sich wesentlich mehr aussagen als im allgemeinen Fall (§ 8).

Ausgeklammert haben wir alle Fragen, die Topologien, Ordnungen und Bewertungen von Fastkörpern betreffen. Für topologische Fastkörper sei auf [25], [28], [43] und [61] verwiesen; geordnete Fastkörper sind von W. Kerby ([36], [38]), bewertete Fastkörper von H. Wefelscheid ([62], [63]) untersucht worden.

§ 1. Grundlegende Definitionen und vorbereitende Ergebnisse

In diesem Paragraphen werden zahlreiche für spätere Untersuchungen erforderliche Begriffe eingeführt und einige ihrer Eigenschaften beschrieben. Soweit die angegebenen Resultate bekannt oder aber leicht zu bestätigen sind, wird auf ihre Beweise verzichtet.

Ausgangspunkt ist die folgende

Definition 1: Eine binäre Doppelstruktur $F(+,\cdot)$ heißt *Fastkörper*[1]), wenn die folgenden Bedingungen erfüllt sind:

[1]) Genauer: *Linksfastkörper.* In einem *Rechtsfastkörper* wird an Stelle von (F 3) das rechtsseitige Distributivgesetz $(a+b)\cdot c = a\cdot c + b\cdot c$ gefordert. Aus einem Linksfastkörper $F(+,\cdot)$ entsteht durch Übergang zur „dualen" Multiplikation $*$ (d. h. $a * b = b\cdot a$ für alle $a,b \in F$) ein Rechtsfastkörper $F(+,*)$ u. u. Die hier erklärten Strukturen nennt H. Zassenhaus [67] *vollständige Fastkörper* (vgl. auch [5]).

(F 1) $F(+)$ ist eine Gruppe (mit neutralem Element 0).
(F 2) $F^*(\cdot)$ ist eine Gruppe (mit neutralem Element 1)[2]).
(F 3) $a \cdot (b + c) = a \cdot b + a \cdot c$ für alle $a,b,c \in F$.
(F 4) $0 \cdot a = 0$ für alle $a \in F$.

Eine binäre Doppelstruktur $F(+,\cdot)$ wird *Fastring* genannt[3]), wenn sie den Axiomen (F 1) und (F 3) genügt.

Bemerkungen:

a) Die Operationen $+$ und $\cdot$ in F werden wie üblich *Addition* und *Multiplikation* genannt.

b) Wir werden durchweg ab an Stelle von $a \cdot b$ schreiben.

c) Offenbar ist jeder (nicht notwendig kommutative) Körper ein Fastkörper. Es gibt andererseits Fastkörper, die keine Körper sind (vgl. z. B. § 3 und § 9). Wir sprechen dann von *echten* Fastkörpern. In ihnen ist das rechtsseitige Distributivgesetz nicht gültig.

Die nächsten Eigenschaften lassen sich leicht mit Hilfe des Distributivgesetzes (F 3) verifizieren (vgl. etwa [32]):

(1.1) *In einem Fastkörper $F(+,\cdot)$ gilt für beliebige $a,b \in F$:*

a) $a \cdot 0 = 0$
b) $a \cdot (-b) = -(ab)$
c) $(-1)^2 = 1$.

Nicht trivial sind die folgenden, in [32] bewiesenen Aussagen (vgl. auch [44] und [69]), von denen wir ohne besondere Erwähnung fortlaufend Gebrauch machen werden:

(1.2) *In einem Fastkörper $F(+,\cdot)$ gilt:*

a) $a^2 = 1$ *ist nur für* $a = 1$ *und* $a = -1$ *erfüllt.*
b) -1 *liegt im Zentrum von* $F^*(\cdot)$.
c) $F(+)$ *ist kommutativ.*

Im Gegensatz zu (1.1)a) ist (F 4) nicht aus (F 1), (F 2) und (F 3) beweisbar, wie die folgende einfache Überlegung zeigt: Man gehe von einem beliebigen Fastkörper $F(+,\cdot)$ und einem von der Nullabbildung $x \to 0$ verschiedenen Endomorphismus τ der Gruppe $F(+)$ aus (etwa $\tau : x \to ax$, wobei $a \in F^*$), und setze

$$a * b = \begin{cases} ab, & \text{wenn } a \neq 0 \\ b^{\tau}, & \text{wenn } a = 0^{4}). \end{cases}$$

Dann erfüllt $F(+,*)$ die Axiome (F 1), (F 2) und (F 3), aber nicht (F 4). Andererseits bedeutet (F 4) insofern keine Einschränkung, als jede Doppelstruktur $F(+,*)$, die den Bedingungen (F 1), (F 2) und (F 3) genügt, durch die Abänderung

---

[2]) Für jede Teilmenge A eines Fastkörpers wird $A^* := \{a \in A | a \neq 0\}$ gesetzt.

[3]) Vgl. z. B. [52].

[4]) Wir bevorzugen bei Abbildungen die Exponentenschreibweise $\tau : a \to a^{\tau}$ und bezeichnen dementsprechend die zusammengesetzte Abbildung $a \to (a^{\sigma})^{\tau}$ mit $\sigma\tau$.

$$a \cdot b = \begin{cases} a * b, & \text{wenn } a \neq 0 \\ 0, & \text{wenn } a = 0 \end{cases}$$

der Multiplikation $*$ in einen Fastkörper $F(+,\cdot)$ übergeht.

Fordert man neben (F1), (F2) und (F3) die Assoziativität der Operation $\cdot$ in ganz F (und nicht nur in F^*), so erhält man einen Fastkörper oder eine Struktur, die sich von dem Körper GF(2) mit zwei Elementen nur durch die Beziehung $0 \cdot 1 = 1$ (statt $0 \cdot 1 = 0$) unterscheidet.

Der in der Einleitung erwähnte Zusammenhang zwischen scharf zweifach transitiven endlichen Permutationsgruppen und Fastkörpern wird durch das folgende Ergebnis erweitert (vgl. etwa [21], Theorem 20.7.1):

(1.3) a) *Es sei $G(\cdot)$ eine auf der Menge F scharf zweifach transitiv operierende Permutationsgruppe mit der Eigenschaft* (**E**)*: „F ist endlich, oder es gibt zu je zwei Elementen $a, b \in F$ höchstens eine fixelementfreie Permutation $\gamma \in G$ mit $a^\gamma = b$". Dann bilden die fixelementfreien Permutationen aus G zusammen mit der Identität einen abelschen Normalteiler A von $G(\cdot)$, und $G(\cdot)$ ist isomorph zur Gruppe aller linearen Transformationen $x \to ax + b$ (mit $a \neq 0$) eines geeigneten Fastkörpers $F(+,\cdot)$.*

b) *Die linearen Transformationen $x \to ax + b$ (mit $a \neq 0$) eines Fastkörpers $F(+,\cdot)$ bilden eine auf F scharf zweifach transitiv operierende Permutationsgruppe. Wenn die Gleichung $ax - x = b$ für jedes $a \neq 1$ und alle $b \in F$ eine Lösung in F besitzt, ist* (**E**) *erfüllt.*

Die Frage, ob im Teil a) auf die Bedingung (**E**) verzichtet werden kann, ist noch offen. An die Stelle der Fastkörper treten dann die von H. Karzel in [33] eingeführten sog. *Fastbereiche*. Das soeben angeschnittene Problem ist daher äquivalent mit der folgenden Frage: Ist jeder Fastbereich ein Fastkörper? Für die bisher erzielten Ergebnisse sei auf [33], [35], [40] und [41] verwiesen. An dieser Stelle wollen wir nur anmerken, daß ein Fastbereich genau dann einen Fastkörper bildet, wenn seine Addition kommutativ ist.

Im folgenden bezeichnet $F(+,\cdot)$ einen Fastkörper.

Definition 2: Eine Teilmenge $H \neq \emptyset$ von F heißt *Teilfastring* von $F(+,\cdot)$, wenn mit a und b auch stets $a - b$ und ab in H enthalten sind. Wenn die Unterstruktur $H(+,\cdot)$ darüberhinaus ein Fastkörper (bzw. Körper) ist – sie ist in jedem Fall ein Fastring, der (F4) genügt –, wird H ein *Teilfastkörper* (bzw. *Teilkörper*) von $F(+,\cdot)$ genannt.

Definition 3: A und B seien Teilmengen von F.

a) Es bezeichnen

$N_F(A) = \{x \in F \mid Ax = xA\}$ [5]) den *Normalisator* von A,

[5]) Für $A, B \subset F$ sowie $x \in F$ wird $AB = \{ab \mid a \in A, b \in B\}$, $xB = \{x\} \cdot B$ und $Ax = A \cdot \{x\}$ gesetzt.

$Z_F(A) = \{x \in F | ax = xa \text{ für alle } a \in A\}$ den *Zentralisator* von A und
$Z_F := Z_F(F)$ das *Zentrum* von $F(+,\cdot)$.
b) B heißt *A-invariant*, wenn $A \subset N_F(B)$. Statt F-invariant sagen wir kurz *invariant*.

Weil das rechtsseitige Distributivgesetz in $F(+,\cdot)$ nicht zu gelten braucht, erweist sich außerdem die Einführung des folgenden Begriffs als nützlich (vgl. [56]):

Definition 4: Für jede Teilmenge A von F wird die Menge

$$K_F(A) = \{x \in F | (a + a')x = ax + a'x \quad \text{für alle} \quad a,a' \in A\}$$

der *A-Kern* von $F(+,\cdot)$ genannt.
$K_F := K_F(F)$ heißt der *Kern* von $F(+,\cdot)$ (vgl. [2]).

Wir verzichten auf die sehr einfachen Beweise der nächsten Feststellungen.

(1.4) *Für jede Teilmenge A von F gilt:*
a) *$K_F(A)$ ist eine Untergruppe von $F(+)$. (Genauer: $(K_F(A))(+)$ ist ein Rechtsvektorraum über $K_F(+,\cdot)$).*
b) *$K_F(A)$ ist ein Teilfastkörper von $F(+,\cdot)$, wenn $K_F(A) \subset N_F(A)$. Das ist insbesondere der Fall, wenn A invariant ist.*
c) *K_F ist ein Teilkörper von $F(+,\cdot)$.*

(1.4c) rechtfertigt die

Definition 5: Die Charakteristik des Kerns $K_F(+,\cdot)$ wird die *Charakteristik* von $F(+,\cdot)$ genannt und mit *Char* $F(+,\cdot)$ oder – wenn keine Zweideutigkeit vorliegt – mit *Char* F abgekürzt.

Des häufigen Gebrauchs wegen sei schließlich ein für allemal festgelegt:

Definition 6: a) Für jedes $a \in F^*$ ist i_a die Abbildung

$$\begin{cases} F \to F \\ x \to a^{-1}xa. \end{cases}$$

b) $A(F,+,\cdot)$ bezeichnet die Automorphismengruppe von $F(+,\cdot)$.
i_a ist zwar immer ein Automorphismus von $F(\cdot)$, i.a. jedoch kein Automorphismus der additiven Gruppe $F(+)$. Es gibt vielmehr:

(1.5) a) *Für jede Unterhalbgruppe H von $F(+)$ ist*

$$(K_F(H))^* = \{x \in F^* | i_x | H \textit{ ist ein Isomorphismus von } H(+) \textit{ in } F(+)\}^{6})$$

---

[6]) Für jede Abbildung $\tau: A \to B$ und jede Teilmenge X von A bedeutet $\tau|X$ die Restriktion von τ auf X.

b) *Für jeden Teilfastkörper H von $F(+,\cdot)$ gilt*

$K_F(H)\backslash H = \{x \in F\backslash H \mid H^{ix}$ *und* $H^{i(x+1)}$ *sind Untergruppen von* $F(+)\}$[7]).

c) *Es gilt genau dann $K_F(H) = F$ für einen Teilfastkörper $H \neq F$ von $F(+,\cdot)$, wenn H^{ix} für jedes $x \in F\backslash H$ eine Untergruppe von $F(+)$ ist.*

Der Beweis der Aussage a) bereitet keine Schwierigkeiten, und c) ist ein Korollar zu a) und b)[8]). Aufgrund von a) braucht außerdem nur eine Richtung der Behauptung b) bewiesen zu werden: Wenn H^{ix} und $H^{i(x+1)}$ für $x \in F\backslash H$ Untergruppen von $F(+)$ sind, ist x in $K_F(H)$ enthalten.

Die Begründung ist im wesentlichen mit dem Beweis des Satzes 2 aus [56] identisch:

Zu jedem $h \in H$ gibt es nach Voraussetzung Elemente h_1 und h_2 aus H derart, daß $(x+1)^{-1}(h+1)(x+1) - 1 = (x+1)^{-1}h_1(x+1)$, d. h.

$$\text{(I)} \qquad (h+1)(x+1) = h_1(x+1) + (x+1),$$

sowie $x^{-1}(h+1)x - 1 = x^{-1}h_2x$, d. h.

$$\text{(II)} \qquad (h+1)x = h_2x + x.$$

Aus (I) und (II) gewinnt man die Gleichung

$h_1(x+1) + (x+1) = (h+1)x + (h+1) = (h_2x + x) + (h+1)$, d. h.

$h_1x - h_2x = h - h_1$. Demnach gilt

$$\text{(III)} \qquad x(x^{-1}h_1x - x^{-1}h_2x) = h - h_1.$$

Aufgrund der Voraussetzungen gibt es ein Element $h_3 \in H$ mit $x^{-1}h_1x - x^{-1}h_2x = x^{-1}h_3x$, so daß

$$\text{(IV)} \qquad h_3x = h - h_1.$$

Diese Gleichung hat wegen $x \notin H$ offenbar $h = h_1$ zur Folge. Der Beziehung (III) entnimmt man daher $h = h_2$, und die Behauptung folgt aus (II). | [9])

Wir fügen zwei einfache Folgerungen an:

(1.6) *Es seien H ein Teilfastkörper von $F(+,\cdot)$ und L eine Unterhalbgruppe von $F(+)$ mit $1 \in L$ und $L \not\subset H$. Wenn H L-invariant ist, liegt L im H-Kern von $F(+,\cdot)$: $L \subset K_F(H)$.*

---

[7]) $A\backslash B$ bezeichnet die Differenz der Mengen A und B.

[8]) Bei diesem Nachweis wird – wie auch mehrfach an späteren Stellen – die folgende Feststellung ausgenutzt:

Wenn $G(\cdot)$ eine Gruppe, H eine Unterhalbgruppe und U, V Untergruppen von $G(\cdot)$ sind, folgt aus $H \subset U \cup V$ stets $H \subset U$ oder $H \subset V$.

[9]) Das Zeichen | deutet das Ende eines Beweises an.

Insbesondere gilt $K_F(H) = F$ für jeden invarianten Teilfastkörper $H \neq F$ von $F(+,\cdot)$. (Vgl. [56], Satz 1).

H^{ix} und $H^{i(x+1)}$ sind nämlich für jedes $x \in L\backslash\{0, -1\}$ Untergruppen von $F(+)$, so daß $L \subset K_F(H) \cup H$ nach (1.5b). Wegen $L \not\subset H$ folgt daraus der erste Teil der Aussage. Die zweite Behauptung ist der Spezialfall $L = F$. |

(1.7) *R sei ein invarianter Teilfastring $\neq F$ des Fastkörpers $F(+,\cdot)$. Dann ist $\bar{R} := \{r^{-1}s | r \in R^*, s \in R\}$ ein Teilfastkörper von $F(+,\cdot)$, und es gilt $\bar{R} = F$ oder $K_F(\bar{R}) = F$.*

Der erste Teil dieser Aussage kann sehr schnell direkt bestätigt werden. Der zweite Teil folgt unmittelbar aus (1.6), weil $\bar{R}$ invariant ist.

Entsprechend leicht beweist man

(1.8) *R sei ein Teilfastring des Fastkörpers $F(+,\cdot)$. Genau dann ist $\bar{R} = \{r^{-1}s | r \in R^*, s \in R\}$ der von R erzeugte Teilfastkörper von $F(+,\cdot)$, wenn es zu beliebigen $r, s \in R^*$ zwei Elemente $r_0, s_0 \in R^*$ mit $s_0 r = r_0 s$ gibt. (Existenz gemeinsamer Linksvielfachen).* |

Die nächsten Aussagen betreffen den Zusammenhang zwischen Zentralisatoren und Kernen von Teilfastkörpern. Wir beginnen mit

(1.9) a) *Für jede Unterhalbgruppe A von $F(+)$ ist $Z_F(A)$ Teilmenge von $K_F(A)$. Insbesondere ist das Zentrum des Fastkörpers $F(+,\cdot)$ in dessen Kern enthalten.*

b) *Für $A \subset F$ ist $Z_F(A)$ ein Teilfastkörper von $F(+,\cdot)$, falls $A \subset K_F(Z_F(A))$. Das ist insbesondere der Fall, wenn A in K_F enthalten ist.*

c) *Wenn H ein Teilfastkörper, aber kein Teilkörper von $F(+,\cdot)$ ist, gilt $Z_F(H) = \bigcap_{h \in H^*} (K_F(H))^{ih}$; d. h. $Z_F(H)$ ist die größte H-invariante Teilmenge von $K_F(H)$.*

Während a) und b) sehr leicht zu bestätigen sind, ist c) in [56] (Satz 6) bewiesen worden. Man vergleiche auch [4] und [13] (5.2.3).

Bemerkungen:

a) Aufgrund von (1.9)a) ist Z_F in einem kommutativen Teilkörper von $F(+,\cdot)$, nämlich im Zentrum des Körpers $K_F(+,\cdot)$, enthalten. (Vgl. [33], Satz 5.6.)

b) (1.9)c) ist ohne die Voraussetzung, daß $H(+,\cdot)$ kein Körper ist, nicht richtig, wie jeder nichtkommutative Körper $H = F$ deutlich macht.

Zwei weitere Ergebnisse aus [56] ergänzen die vorausgegangenen Feststellungen:

(1.10) a) *H und L seien zwei Teilfastkörper des Fastkörpers $F(+,\cdot)$, und H sei nicht in L enthalten. Dann folgt aus $H \subset N_F(L)$ stets $L \cap K_F(H) \subset Z_F(H)$. Insbesondere gilt $L \cap K_F \subset Z_F$ für jeden von F verschiedenen invarianten Teilfastkörper L von $F(+,\cdot)$.*

b) *H und L seien zwei einander nicht enthaltende Teilfastkörper von $F(+,\cdot)$. Aus $H \subset N_F(L)$ und $L \subset N_F(H)$ folgt $H \subset Z_F(L)$ (und damit auch $L \subset Z_F(H)$). Insbesondere sind zwei voneinander und von F verschiedene invariante Teilfastkörper von $F(+,\cdot)$ elementweise miteinander vertauschbar.*

Aus dem Teil a) geht unmittelbar hervor, daß Kern und Zentrum eines echten Fastkörpers $F(+,\cdot)$ genau dann übereinstimmen, wenn der Kern invariant ist, und daß der *Primkörper* von $F(+,\cdot)$ – das ist der Primkörper des Kerns $K_F(+,\cdot)$ – genau dann im Zentrum von $F(+,\cdot)$ liegt, wenn $F(+,\cdot)$ mindestens einen invarianten Teilfastkörper $\neq F$ besitzt (vgl. [36], Satz 4.3). Es sei angemerkt, daß der Primkörper eines Fastkörpers nicht in dessen Zentrum enthalten zu sein braucht. Beispiele dazu findet man in § 3 und § 9.

(1.11) a) *H sei ein Teilfastkörper von $F(+,\cdot)$ und $k \in K_F(H) \backslash Z_F(H)$. Dann ist H in dem von der Menge $\{k^{ih} | h \in H^*\}$ erzeugten Teilfastkörper L von $F(+,\cdot)$ enthalten.*

b) *Die Menge $\{k^{ix} | x \in F^*\}$ der Konjugierten eines Elements $k \in K_F \backslash Z_F$ erzeugen F als Fastkörper.*

Beweis: Für jedes $a \in H^* \backslash \{-1\}$ gilt

$$ak + k = (a+1)k = k^{i(a+1)^{-1}} \cdot (a+1) = ak^{i(a+1)^{-1} \cdot a} + k^{i(a+1)^{-1}}, \text{ d. h.}$$
$$a(k - k^{i(a+1)^{-1} \cdot a}) = k^{i(a+1)^{-1}} - k.$$

Im Fall $a \notin L$ folgt daraus offenbar $k = k^{i(a+1)^{-1}} = k^{i(a+1)^{-1} \cdot a}$, insbesondere also $ak = ka$. Daher ist H in $L \cup Z_F(\{k\})$ enthalten. Aus $H \not\subset L$ ergäbe sich $H \subset Z_F(\{k\})$ im Widerspruch zur Voraussetzung $k \notin Z_F(H)$. |

Die in (1.3)b) auftretende Bedingung

(P) „Die Gleichung $ax - x = b$ besitzt für alle $a \neq 1$ und b aus F eine Lösung in F"

erlaubt folgende geometrische Interpretation:

Ein Fastkörper ist genau dann Koordinatenbereich einer affinen oder projektiven Ebene, wenn **(P)** erfüllt ist; denn genau unter dieser Voraussetzung bildet $F(+,\cdot)$ zusammen mit der durch $T(a,b,c) = ab + c$ in F erklärten ternären Operation T einen ternären Ring (vgl. etwa [37]). Man überzeugt

sich sofort, daß es ausreicht, an Stelle von (**P**) die Eigenschaft (**P'**) zu verlangen:

(**P'**) „Die Gleichung $ax - x = 1$ besitzt für alle $a \neq 1$ eine Lösung in F".

Definition 7: Ein Fastkörper $F(+,\cdot)$, der der Bedingung (**P**) (bzw. (**P'**)) genügt, heißt *planar* ([68]) oder *projektiv* ([37]).

In [69] und [37] wurde die Existenz nicht-planarer Fastkörper nachgewiesen. Die Dimension $[F : K_F]_r$ des Rechtsvektorraums (F, K_F)[10]) ist dann notwendig unendlich, weil die Abbildung $x \to ax - x$ für jedes $a \neq 1$ ein injektiver Endomorphismus von (F, K_F) ist. Wir fassen die Sätze 3 und 4 aus [37] zusammen:

(1.12) a) *Es gibt nicht-planare Fastkörper, und es gibt echte planare Fastkörper, deren Rechtsrang über ihrem Kern unendlich ist.*
b) *Ein Fastkörper mit endlichem Rechtsrang über seinem Kern ist planar.*

Infolge der Äquivalenz von (**P**) und (**P'**) läßt sich (1.12) b) verallgemeinern zu

b') *Ein über seinem Kern rechts-algebraischer Fastkörper ist planar.*

Dabei nennen wir $F(+,\cdot)$ *rechts-algebraisch* über $K_F(+,\cdot)$, wenn der von a und K_F erzeugte Teilfastkörper von $F(+,\cdot)$ für jedes $a \in F$ endlichen Rechtsrang über $K_F(+,\cdot)$ hat.

Eine Ergänzung zu (1.12) ist in (6.7) enthalten.

Wir beschließen diesen Abschnitt mit einem Ergebnis von P. M. Cohn [10], das diejenigen Gruppen kennzeichnet, die als multiplikative Gruppe eines Fastkörpers auftreten:

(1.13) *$G(\cdot)$ bezeichne eine Gruppe mit dem neutralen Element 1 und mit $G^* := G \setminus \{1\} \neq \emptyset$. Es seien e ein Element aus G und $\varepsilon : G^* \to G^*$ eine Abbildung mit den folgenden Eigenschaften:*

(I)	$x^{\varepsilon^2} = x$	*für alle* $x \in G^*$
(II)	$(x^{-1})^\varepsilon = x^{-1} x^\varepsilon e$	*für alle* $x \in G^*$
(III)	$(y^{-1}x)^\varepsilon = (y^{-1})^\varepsilon ((y^\varepsilon)^{-1} x^\varepsilon)^\varepsilon$	*für alle* $x, y \in G^*$ *mit* $x \neq y$.

Dann gibt es genau einen Fastkörper $F(+,\cdot)$, dessen multiplikative Gruppe mit $G(\cdot)$ übereinstimmt und für den $e = -1$ und $x^\varepsilon = 1 - x$ für alle $x \in G^*$.
Wenn $F(+,\cdot)$ andererseits ein Fastkörper mit $|F| > 2$ ist, genügen $G(\cdot) = F^*(\cdot)$ sowie $e = -1$ und

---

[10]) Offenbar ist $F(+)$ genau dann Rechtsvektorraum über einem Teilkörper $H(+,\cdot)$ von $F(+,\cdot)$ (mit $\cdot$ als skalarer Verknüpfung), wenn H im Kern von $F(+,\cdot)$ liegt.

$$\varepsilon: \begin{cases} F^*\setminus\{1\} \to F^*\setminus\{1\} \\ x \quad \to 1 - x \end{cases}$$

den Bedingungen (I), (II) *und* (III).

Die in [10] zusätzlich auftretende Bedingung (IV) entspricht gerade dem rechtsseitigen Distributivgesetz.

§ 2. Fastkörperpaare

L. E. Dickson [14] konstruierte 1905 die ersten (endlichen) echten Fastkörper durch Abänderung der Multiplikation von Körpern mit Hilfe geeigneter Körperautomorphismen. Dieses sog. *Dicksonsche Verfahren* wurde von E. Ellers und H. Karzel [15] axiomatisiert und später in verschiedenen Richtungen vor allem von F. Pokropp [47], [48], [49], W. Kerby [36], [37], [38] und J. Timm [52], [53] verallgemeinert und ausgebaut. Mit Ausnahme von sieben (endlichen), bereits Dickson bekannten Beispielen, die im nächsten Paragraphen beschrieben werden, lassen sich alle bisher entdeckten Fastkörper mit dem Dicksonschen Verfahren gewinnen. Wir beginnen mit seiner Darstellung, beschränken uns aber von vornherein auf eine unseren Zwecken angepaßte spezielle Form. In der Bezeichnungsweise schließen wir uns dabei weitgehend [49] und [53] an.

$F(+,\cdot)$ bezeichne wiederum einen vorgegebenen Fastkörper.

Definition 1: Eine Abbildung

$$\varphi: \begin{cases} F^* \to A(F,+,\cdot) \\ a \quad \to a_\varphi \end{cases}$$

heißt *gekoppelt* oder eine *Dickson-Abbildung* von $F(+,\cdot)$, wenn die „Kopplungsgleichung"

(I) $$a_\varphi b_\varphi = (b a^{b\bullet})_\varphi \quad \text{für alle} \quad a,b \in F^*$$

erfüllt ist.

Die Menge aller gekoppelten Abbildungen von $F(+,\cdot)$ wird mit $\mathfrak{K}(F,+,\cdot)$ bezeichnet.

Jeder Fastkörper besitzt gekoppelte Abbildungen: Die triviale Abbildung $\begin{cases} F^* \to A(F,+,\cdot) \\ a \quad \to 1_F \end{cases}$ [11]) genügt der Kopplungsgleichung (I).

(I) ist gleichwertig mit

---

[11]) 1_F ist die identische Abbildung von F.

(II) $$(a^{b\varphi^{-1}})_\varphi b_\varphi = (ba)_\varphi \quad \text{für alle} \quad a,b \in F^* .$$

Jede gekoppelte Abbildung φ von $F(+,\cdot)$ ermöglicht es, in F durch die Vorschrift

(III) $$\left.\begin{cases} a \circ b = ab^{a\varphi}, & \text{wenn} \quad a \in F^* \\ 0 \circ b = 0 \end{cases}\right\} \quad (\text{für jedes } b \in F)$$

eine weitere binäre Operation $\circ$ einzuführen, und es gilt (vgl. etwa [31]:

(2.1) *$F(+,\circ)$ ist ein Fastkörper.*

Definition 2: $F(+,\cdot)$ sei ein Fastkörper, φ eine gekoppelte Abbildung von $F(+,\cdot)$, und $\circ$ bedeute die durch (III) eingeführte (von φ abhängige) binäre Operation in F. Wir schreiben diesen Sachverhalt kurz in der Form $F(+,\cdot) \xrightarrow{\varphi} F(+,\circ)$ oder $F(+,\circ) = F^\varphi(+,\cdot)$.

a) Der Fastkörper $F^\varphi(+,\cdot) = F(+,\circ)$ heißt die *φ-Ableitung* von $F(+,\cdot)$ und wird aus $F(+,\cdot)$ *ableitbar* genannt. Das geordnete Paar $(F(+,\cdot),F(+,\circ))$ – im folgenden kurz (F,F^φ) oder $F(+,\cdot,\circ)$ geschrieben – bezeichnet man als ein *Fastkörperpaar*.

b) Gilt überdies $F(+,\circ) \xrightarrow{\psi} F(+,\cdot)$ mit einer geeigneten gekoppelten Abbildung ψ von $F(+,\circ)$, so heißen $F(+,\cdot)$ und $F(+,\circ)$ *äquivalent*, i. Z. $F(+,\cdot) \leftrightarrow F(+,\circ)$.

c) Ein Fastkörperpaar $F(+,\cdot,\circ)$ wird *regulär* oder ein *Dicksonsches Fastkörperpaar* (kurz *D-Fastkörperpaar*) genannt, wenn $F(+,\cdot)$ ein Körper ist. Auch $F(+,\circ)$ heißt in diesem Fall ein *regulärer* oder *Dicksonscher Fastkörper (D-Fastkörper)* [12]).

Ein Fastkörper ist also genau dann Dicksonsch, wenn er aus einem Körper ableitbar ist.

Bemerkung: In [31] und [47] wird eine Relation „gekoppelt an" eingeführt: Ein Fastkörper $F'(+,\circ)$ heißt an einen Fastkörper $F(+,\cdot)$ *gekoppelt*, i. Z. $F'(+,\circ) \llcorner F(+,\cdot)$, wenn $F'(+,\circ)$ zu einem aus $F(+,\cdot)$ ableitbaren Fastkörper $F^\varphi(+,\cdot) = F(+,\circ)$ isomorph ist. Überträgt man die Operation $\cdot$ in F mit Hilfe des zugrunde liegenden Isomorphismus π zwischen $F(+,\circ)$ und $F'(+,\circ)$ von F auf F', d. h. setzt man $a^\pi \cdot b^\pi = (a \cdot b)^\pi$ für alle $a,b \in F$, so sind $F(+,\cdot)$ und $F'(+,\cdot)$ isomorph, und $F'(+,\circ)$ ist die ψ-Ableitung von $F'(+,\cdot)$ für

$$\psi: \begin{cases} F'^* \to A(F',+,\cdot) \\ a^\pi \to (a_\varphi)^{i\pi} = \pi^{-1} a_\varphi \pi , \end{cases}$$

wie man sich sofort überzeugt. Es sei auch auf [47] (Satz 9) verwiesen. In diesem Sinne ist die Relation $\llcorner$ nicht allgemeiner als $\to$, und die z. B. in [31] gegebene Definition des Begriffs „D-Fastkörper" ist zu der unsrigen äquivalent.

---

[12]) Vgl. [13] (Seite 33) und [17] (dort wird $F(+,\circ)$ noch als *Dickson-Veblenscher Fastkörper* bezeichnet).

Es ist zweckmäßig, einige abkürzende Bezeichnungen einzuführen:

Definition 3: Es seien φ eine gekoppelte Abbildung des Fastkörpers $F(+,\cdot), F(+,\circ)$ die φ-Ableitung von $F(+,\cdot)$ und A eine Teilmenge von F. Dann setzen wir:

a) $A_\varphi = \{a_\varphi | a \in A^*\}$;
$\Gamma_\varphi := F_\varphi$ heißt die *Dicksongruppe* (*D-Gruppe*) von φ oder von $F(+,\cdot,\circ)$.
b) $U_\varphi(A) = \{x \in F^* | x_\varphi | A = 1_A\}$;
$U_\varphi := U_\varphi(F)$ (Der „Kern" von φ);
c) $V_\varphi(A) = \{x \in F^* | x_\varphi | A = i_x | A\}$;
$V_\varphi := V_\varphi(F)$;
d) $P_\varphi(A) = \{x \in F | x^{a_\varphi} = x \quad \text{für alle} \quad a \in A^*\}$;
$P_\varphi := P_\varphi(F)$ (Die Fixmenge von Γ_φ);
e) $Q_\varphi(A) = \{x \in F | x^{a_\varphi} = x^{i_a} \text{ für alle } a \in A^*\}$;
$Q_\varphi := Q_\varphi(F)$.

Die Einführung der Mengen $V_\varphi(A)$ und $Q_\varphi(A)$, die nur bei D-Fastkörperpaaren eine Rolle spielen, wird durch die folgende leicht zu bestätigende Feststellung nahegelegt:

(2.2) *$F(+,\cdot,\circ) = (F, F^\varphi)$ sei ein D-Fastkörperpaar, und $*$ bezeichne die zu $\cdot$ duale Operation in F: $a * b = ba$ für alle $a,b \in F$.*
Dann ist

$$\psi: \begin{cases} F \to A(F,+,*) \\ a \to a_\varphi i_a^{-1} \end{cases}$$

eine gekoppelte Abbildung von $F(+,*)$ und $F(+.*) \overset{\psi}{\to} F(+,\circ)$. Ferner gelten $U_\psi(A) = V_\varphi(A), V_\psi(A) = U_\varphi(A), P_\psi(A) = Q_\varphi(A)$ sowie $Q_\psi(A) = P_\varphi(A)$ für jede Teilmenge A von F.

Ohne Mühe lassen sich die nächsten Aussagen (2.3) – (2.7) beweisen, in denen $F(+,\cdot,\circ) = (F, F^\varphi)$ ein Fastkörperpaar und A eine Teilmenge von F bezeichnen.

(2.3) *φ ist ein Antihomomorphismus von $F^*(\circ)$ in $A(F,+,\cdot)$:*
(IV) $a_\varphi b_\varphi = (b \circ a)_\varphi$ *für alle* $a,b \in F^*$.

(2.4) a) $U_\varphi(A) = \{x \in F^* | x \circ a = xa \quad \text{für alle} \quad a \in A\}$;
$V_\varphi(A) = \{x \in F^* | x \circ a = ax \quad \text{für alle} \quad a \in A\}$;
b) $U_\varphi(A) < F^*(\circ), V_\varphi(A) < F^*(\circ)$[13])
$U_\varphi \lhd F^*(\circ), V_\varphi \lhd F^*(\circ)$[14])

---

[13]) D. h. $U_\varphi(A)$ und $V_\varphi(A)$ sind Untergruppen von $F^*(\circ)$.
[14]) D. h. U_φ und V_φ sind Normalteiler von $F^*(\circ)$.

c) $U_\varphi < F^*(\cdot)$, $V_\varphi < F^*(\cdot)$,
$-1 \in U_\varphi \cap V_\varphi$.

d) $U_\varphi(A) \cup \{0\}$ *ist ein Teilfastkörper von* $F(+,\circ)$, *wenn* $A \subset K_F(U_\varphi(A))$[15] *und wenn* $F(+,\cdot)$ *ein Körper ist.*

e) $V_\varphi(A) \cup \{0\}$ *ist ein Teilfastkörper von* $F(+,\circ)$, *wenn* $A \subset K_F(V_\varphi(A))$.

f) *Wenn* A *gleichzeitig Untergruppe von* $F^*(\circ)$ *und* $F^*(\cdot)$ *ist, gilt:*
$\alpha)$ $A \subset N_F(U_\varphi(A))$, $A \subset N_F(V_\varphi(A))$[15],
$\beta)$ $(U_\varphi(A))^{a_\varphi} = (U_\varphi(A))^{i_a}$, $(V_\varphi(A))^{a_\varphi} = V_\varphi(A)$ *für alle* $a \in A^*$.
Insbesondere ist U_φ *genau dann Normalteiler von* $F^*(\cdot)$, *wenn* $U_\varphi^{a_\varphi} = U_\varphi$ *für alle* $a \in F^*$.

g) $a_\varphi = (ua)_\varphi$ *für alle* $u \in U_\varphi$ *und alle* $a \in F^*$;
$a_\varphi = b_\varphi$ gilt genau dann, wenn $U_\varphi a = U_\varphi b$.

(2.5) a) $P_\varphi(A) = \{x \in F \mid a \circ x = ax$ *für alle* $a \in A\}$
$Q_\varphi(A) = \{x \in F \mid a \circ x = xa$ *für alle* $a \in A\}$

b) $P_\varphi(A)$ *ist ein Teilfastkörper von* $F(+,\cdot)$.
$(Q_\varphi(A))^*$ *ist Untergruppe von* $F^*(\cdot)$; $Q_\varphi(A)$ *ist Teilfastkörper von* $F(+,\cdot)$, *wenn* $F(+,\cdot)$ *ein Körper ist.*
P_φ *ist ein Teilfastkörper von* $F(+,\circ)$.
Q_φ^* *ist Untergruppe von* $F^*(\circ)$; Q_φ *ist Teilfastkörper von* $F(+,\circ)$, *wenn* $F(+,\cdot)$ *ein Körper ist.*

c) *Für jede Unterhalbgruppe* A *von* $F(+)$ *gilt:*
$Q_\varphi(A) \subset K_F(A)$;
$P_\varphi(A) \subset K_F(A)$, *wenn* $F(+,\cdot)$ *ein Körper ist.*

d) $P_\varphi(A) \subset Z_F(A)$ *ist äquivalent mit* $P_\varphi(A) \subset V_\varphi(A)$;
$Q_\varphi(A) \subset Z_F(A)$ *ist äquivalent mit* $Q_\varphi(A) \subset U_\varphi(A)$.

(2.6) *Aus* $B^* < F^*(\circ)$ *folgen* $B_\varphi < A(F,+,\cdot)$ *sowie*
$B_\varphi \simeq B^*/(U_\varphi \cap B) \simeq (U_\varphi \circ B^*)/U_\varphi$ *(bezüglich* $\circ$*).*

(2.7) a) $a^{\overline{-1}} = (a^{-1})^{a_{\bar\varphi}^{-1}} = (a^{a_{\bar\varphi}^{-1}})^{-1}$ [16],
$a^{-1} = (a^{\overline{-1}})^{a_\varphi} = (a^{(a^{-1})_{\bar\varphi}^{-1}})^{\overline{-1}}$
für alle $a \in F^*$.

b) $x^{a_\varphi} = a^{-1}(a \circ x)$ *für alle* $a, x \in F^*$.

In den Anwendungen treten besonders häufig gekoppelte Abbildungen mit einer der folgenden zusätzlichen Eigenschaften auf:

---

[15]) Wenn $F(+,\cdot,\circ)$ ein Fastkörperpaar ist, bezeichnen auch später $K_F(B)$, $Z_F(B)$ und $N_F(B)$ der Reihe nach Kern, Zentralisator und Normalisator der Teilmenge B von F in dem abgeleiteten Fastkörper $F(+,\circ)$.

[16]) Wir bezeichnen die n-te Potenz von $a \in F^*$ bez. der Operation $\cdot$ mit a^n und bez. der Operation $\circ$ mit $a^{\underline{n}}$.

Definition 4: a) Eine gekoppelte Abbildung φ eines Fastkörpers $F(+,\cdot)$ wird ein *gekoppelter Homomorphismus* (bzw. *Antihomomorphismus*) genannt, wenn φ ein Homomorphismus (bzw. Antihomomorphismus) von $F^*(\cdot)$ in $A(F,+,\cdot)$ ist, d. h. wenn $(ab)_\varphi = a_\varphi b_\varphi$ (bzw. $(ab)_\varphi = b_\varphi a_\varphi$) für alle $a,b \in F^*$.

b) (Dual zu a)) Eine gekoppelte Abbildung φ von $F(+,\cdot)$ heißt *gekoppelter d-Homomorphismus* (bzw. *d-Antihomomorphismus*), wenn $(ab)_\varphi = b_\varphi(i_b^{-1} a_\varphi i_b) = b_\varphi a_\varphi^{i_{(i_b)}}$ (bzw. $(ab)_\varphi = a_\varphi i_{a^{-1}} b_\varphi i_{b^{-1}ab}$) für alle $a,b \in F^*$.

Bemerkung: Ein gekoppelter Antihomomorphismus wird in [31], [47], [48], [49] gekoppelter Homomorphismus bzw. *stark gekoppelte Abbildung* genannt. Man beachte dabei den Unterschied in der Schreibweise zusammengesetzter Abbildungen.

In den nächsten beiden Kriterien sind einige brauchbare Kennzeichnungen gekoppelter Homomorphismen und Antihomomorphismen zusammengestellt:

(2.8) a) *φ sei eine gekoppelte Abbildung des Fastkörpers $F(+,\cdot)$. Dann sind die folgenden Aussagen äquivalent:*
α) φ ist ein gekoppelter Homomorphismus
β) $(b^{a_\varphi})_\varphi = (b_\varphi)^{i_{a_\varphi}} = a_\varphi^{-1} b_\varphi a_\varphi$ für alle $a,b \in F^*$;
γ) $b^{a_\varphi i_a^{-1}} \in U_\varphi b$ für alle $a,b \in F^*$;
δ) $U_\varphi \lhd F^*(\cdot)$, und $(F^*/U_\varphi)(\cdot), (F^*/U_\varphi)(\circ)$ sind dual zueinander, d. h. $(a\,U_\varphi)(b\,U_\varphi) = (b \circ U_\varphi) \circ (a \circ U_\varphi)$ für alle $a,b \in F^*$.
b) *Ein Homomorphismus φ von $F^*(\cdot)$ in $A(F,+,\cdot)$ mit dem Kern U_φ, der eine der Bedingungen β), γ) erfüllt, ist eine gekoppelte Abbildung von $F(+,\cdot)$.*

(2.9) (Vgl. etwa [31], Satz 3)
a) *φ sei eine gekoppelte Abbildung des Fastkörpers $F(+,\cdot)$. Dann sind die folgenden Aussagen äquivalent:*
α) φ ist ein gekoppelter Antihomomorphismus;
β) $(b^{a_\varphi})_\varphi = b_\varphi$ für alle $a,b \in F^*$;
γ) $b^{a_\varphi} \in U_\varphi b$ für alle $a,b \in F^*$;
δ) $U_\varphi \lhd F^*(\cdot)$, und $(F^*/U_\varphi)(\cdot), (F^*/U_\varphi)(\circ)$ sind identisch, d. h. $(a\,U_\varphi)(b\,U_\varphi) = (a \circ U_\varphi) \circ (b \circ U_\varphi)$ für alle $a,b \in F^*$.
b) *Ein Antihomomorphismus φ von $F^*(\cdot)$ in $A(F,+,\cdot)$ mit dem Kern U_φ, der einer der Bedingungen β), γ) genügt, ist eine gekoppelte Abbildung von $F(+,\cdot)$.*

Gekoppelte Homomorphismen und Antihomomorphismen lassen sich bemerkenswert besser handhaben als gekoppelte Abbildungen ohne derartige

zusätzliche Eigenschaften. Daher ist das folgende, von H. Karzel [31] (14) stammende Resultat von Interesse:

Eine gekoppelte Abbildung φ des Fastkörpers $F(+,\cdot)$ ist ein gekoppelter Homomorphismus (und Antihomomorphismus), wenn $U_\varphi \lhd F^*(\cdot)$ und wenn $|\Gamma_\varphi|$ eine Primzahl ist[17]).

Wir wollen diese Aussage etwas erweitern:

(2.10) *$(F,F^\varphi) = F(+,\cdot,\circ)$ sei ein Fastkörperpaar und es gelte:*
a) $U_\varphi \lhd F^*(\cdot)$;
b) $|\Gamma_\varphi| = p_1 \dots p_n$ *mit verschiedenen Primzahlen* $p_1,\dots,p_n$ *(d.h. $|\Gamma_\varphi|$ ist quadratfrei) und* $p_i \nmid p_j - 1$ *für* $i,j = 1,\dots,n$.
Dann ist φ ein gekoppelter Homomorphismus (und Antihomomorphismus) von $F(+,\cdot)$.

Beweis: Wegen (b) sind Γ_ψ und $(F^*/U_\varphi)(\cdot)$ zyklisch (vgl. [70]), insbesondere also direkte Produkte ihrer p_i-Sylowgruppen Z_{p_i} bzw. Z'_{p_i}:

$$\Gamma_\varphi = Z_{p_1} \times \dots \times Z_{p_n} \quad \text{und} \quad (F^*/U_\varphi)(\cdot) = Z'_{p_1} \times \dots \times Z'_{p_n}.$$

Jedes $\gamma \in \Gamma_\varphi$ induziert einen Automorphismus

$$\bar{\gamma}: \begin{cases} F^*/U_\varphi \to F^*/U_\varphi \\ U_\varphi x \to U_\varphi x^\gamma \end{cases}$$

von $(F^*/U_\varphi)(\cdot)$ (vgl. (2.4)f), wonach $U_\varphi x^\gamma = U_\varphi^\gamma x^\gamma = (U_\varphi x)^\gamma$), und die Abbildung $\gamma \to \bar{\gamma}$ von Γ_φ in $\mathrm{Aut}(F^*/U_\varphi,\cdot)$ ist ein Homomorphismus. Da die Sylowgruppen von $(F^*/U_\varphi)(\cdot)$ charakteristisch sind, induziert $\bar{\gamma}$ Automorphismen $\bar{\gamma}_i$ in $Z'_{p_i}(\cdot)$ für $i = 1,\dots,n$. Wegen $|\mathrm{Aut}(Z'_{p_i},\cdot)| = p_i - 1$ ist die Ordnung von $\bar{\gamma}_i$ ein Teiler von $p_i - 1$.

Andererseits ist die Ordnung von $\bar{\gamma}_i$ ein Teiler der Ordnung von γ, d. h. von $p_1 \dots p_n$. Aus der Voraussetzung b) folgt $\bar{\gamma}_i = 1_{Z'_{p_i}}$ für $i = 1,\dots,n$, so daß $\bar{\gamma} = 1_{F^*/U_\varphi}$. Daher gilt $U_\varphi x = U_\varphi x^\gamma$ für alle $x \in F^*$ und alle $\gamma \in \Gamma_\varphi$. Das ist nach (2.9)$\gamma$) gerade die Behauptung. |

Mit den in der Definition 4 eingeführten Begriffen lassen sich die Symmetrie- und Transitivitätseigenschaften der Relation $\to$ beschreiben (vgl. etwa [47]):

(2.11) *Wenn φ eine gekoppelte Abbildung des Fastkörpers $F(+,\cdot)$ ist und $F(+,\circ)$ die φ-Ableitung von $F(+,\cdot)$ bezeichnet, sind die folgenden Aussagen äquivalent:*
a) $F(+,\cdot) \leftrightarrow F(+,\circ)$;
b) $\varphi^{-1}: a \to a_\varphi^{-1}$ *ist eine gekoppelte Abbildung von* $F(+,\circ)$;

[17]) $|X|$ bezeichnet die Kardinalzahl der Menge X.

c) $\Gamma_\varphi \subset A(F,+,\circ)$;
d) φ *ist ein gekoppelter Homomorphismus.*

(2.12) *Es seien* $F(+,\cdot,\circ) = (F,F^\varphi)$ *und* $F(+,\circ,*) = (F^\varphi,(F^\varphi)^\psi)$ *Fastkörperpaare, d. h.* $F(+,\cdot) \xrightarrow{\varphi} F(+,\circ)$ *und* $F(+,\circ) \xrightarrow{\psi} F(+,*)$ *mit* $\varphi \in \mathscr{K}(F,+,\cdot)$ *und* $\psi \in \mathscr{K}(F,+,\circ)$. *Dann sind die folgenden Aussagen äquivalent:*

a) $F(+,\cdot) \to F(+,*)$;
b) $\Gamma_\psi \subset A(F,+,\cdot)$;
c) $(b^{a_\psi})_\varphi = (b_\varphi)^{i_{a_\psi}} = a_\psi^{-1} b_\varphi a_\psi$ *für alle* $a,b \in F^*$.

Die beiden letzten Ergebnisse legen es nahe, die durch

$$\text{(V)} \qquad \varphi * \psi : \begin{cases} F^* \to A(F,+,\cdot) \\ a \to a_{\varphi*\psi} := a_\varphi a_\psi \end{cases}, \quad (\varphi,\psi \in \mathscr{K}(F,+,\cdot)),$$

erklärte Produktbildung $*$ zu untersuchen. Gibt es Teilmengen von $\mathscr{K}(F,+,\cdot)$, die gegenüber $*$ abgeschlossen sind und Gruppen bilden? Eine Teilantwort gibt der nächste Satz.

(2.13) a) *Es seien* $F(+,\cdot)$ *ein Fastkörper,* G *eine nichtleere Teilmenge von* $\mathscr{K}(F,+,\cdot)$, *und* G *sei gegenüber* $*$ *(vgl.* (V)*) abgeschlossen. Wenn* $\psi \in \mathscr{K}(F^\varphi)$ *für alle* $\varphi,\psi \in G$ *erfüllt ist, gelten*

(α) $(b^{a_\varphi})_\psi = b_\psi$ *und*
(β) $a_\psi b_\varphi = b_\varphi a_\psi$

für alle $a,b \in F^*$ *und alle* $\varphi,\psi \in G$.
Insbesondere ist jedes $\varphi \in G$ *sowohl ein gekoppelter Homomorphismus als auch Antihomomorphismus von* $F(+,\cdot)$.
b) $F(+,\cdot)$ *sei ein Fastkörper und* $M \subset \mathscr{K}(F,+,\cdot)$. *Es gelte*

(α) $(b^{a_\varphi})_\psi = b_\psi$ *und*
(β) $a_\psi b_\varphi = b_\varphi a_\psi$

für alle $a,b \in F^*$ *und alle* $\varphi,\psi \in M$.
Dann gibt es eine M *enthaltende Teilmenge* G *von* $\mathscr{K}(F,+,\cdot)$ *mit den Eigenschaften:*
(A) G *ist abgeschlossen gegenüber* $*$, *und* $G(*)$ *bildet eine Gruppe.*
(B) $\psi \in \mathscr{K}(F^\varphi)$ *für alle* $\varphi,\psi \in G$.

Insbesondere ist φ^n für jedes $n \in \mathbb{Z}$ in $\mathscr{K}(F,+,\cdot)$ enthalten, wenn φ ein gekoppelter Homomorphismus mit abelscher D-Gruppe Γ_φ ist.

Beweis: a) Es seien φ und ψ in G enthalten. Aus $\psi \in \mathscr{K}(F^\varphi)$ folgt nach (2.12):

$$\text{(VI)} \qquad (b^{a_\psi})_\varphi = (b_\varphi)^{i_{a_\psi}} \quad \text{für alle} \quad a,b \in F^*.$$

Insbesondere ist φ ein gekoppelter Homomorphismus von $F(+,\cdot)$. Infolge $\psi * \varphi \in G$ gilt außerdem

$$(ab^{a_{\psi*\varphi}})_{\psi*\varphi} = b_{\psi*\varphi}a_{\psi*\varphi}, \quad \text{d. h.}$$
$$(ab^{a_\psi a_\varphi})_\psi (ab^{a_\psi a_\varphi})_\varphi = b_\psi b_\varphi a_\psi a_\varphi, \quad \text{und somit}$$
$$(b^{a_\psi a_\varphi a_{\psi*\varphi}^{-1}})_\psi a_\psi (b^{a_\psi})_\varphi a_\varphi = b_\psi b_\varphi a_\psi a_\varphi \quad \text{für alle} \quad a,b \in F^*.$$

Diese Gleichung vereinfacht sich mit Rücksicht auf (VI) zu

(VII) $$(b^{a_\psi a_\varphi a_\psi^{-1}})_\psi = b_\psi, \quad \text{gültig für alle} \quad a,b \in F^*.$$

Setzt man hierin $\psi = \varphi$:

(VIII) $$(b^{a_\varphi})_\varphi = b_\varphi \quad \text{für alle} \quad a,b \in F^*,$$

so erkennt man nach (2.9), daß φ ein gekoppelter Antihomomorphismus ist.

Wir ersetzen ψ in (VI) durch φ und beachten (VIII):

$$b_\varphi = (b^{a_\varphi})_\varphi = (b_\varphi)^{i_{a_\varphi}} = a_\varphi^{-1} b_\varphi a_\varphi, \quad \text{d. h.}$$

(IX) $$a_\varphi b_\varphi = b_\varphi a_\varphi, \quad \text{gültig für alle} \quad a,b \in F^*.$$

Γ_φ ist daher abelsch für jedes $\varphi \in G$.

Mehrfaches Anwenden der Gleichung (VI) auf (VII) führt aufgrund von (IX) zu

$$b_\psi = (b^{a_\psi a_\varphi a_\psi^{-1}})_\psi = a_\psi (a_\varphi^{-1}(a_\psi^{-1} b_\psi a_\psi) a_\varphi) a_\psi^{-1} = a_\psi a_\varphi^{-1} b_\psi a_\varphi a_\psi^{-1}.$$

Wir multiplizieren von links mit a_ψ^{-1}, von rechts mit a_ψ, und erhalten infolge (IX) die Beziehung $b_\psi = a_\varphi^{-1} b_\psi a_\varphi$, d. h.

(β) $$a_\varphi b_\psi = b_\psi a_\varphi \quad \text{für alle} \quad a,b \in F^*.$$

Aus (IV) und (β) folgt schließlich (α).

b) Wir zeigen zunächst, daß $\varphi^{-1} \in \mathscr{K}(F,+,\cdot)$ für jedes $\varphi \in M$, wobei $\varphi^{-1} : x \to (x_\varphi)^{-1}$: Nach ($\alpha$) und ($\beta$) gilt $(ab^{a_\varphi^{-1}})_{\varphi^{-1}} = \{(ab^{(a_\varphi)^{-1}})_\varphi\}^{-1} =$
$= \{(b^{(a_\varphi)^{-2}})_\varphi a_\varphi\}^{-1} = (a_\varphi)^{-1}(b_\varphi)^{-1} = (b_\varphi)^{-1}(a_\varphi)^{-1} = b_{\varphi^{-1}} a_{\varphi^{-1}}$.

Offenbar sind die Beziehungen (α) und (β) für beliebige Elemente φ,ψ aus $M \cup \{\chi^{-1} | \chi \in M\}$ erfüllt, so daß wir o.B.d.A. voraussetzen dürfen, daß mit φ auch immer φ^{-1} in M enthalten ist.

Wir setzen – unter dieser Annahme –

$$G := \{\varphi_1 * \ldots * \varphi_n | \varphi_1, \ldots, \varphi_n \in M; n \in \mathbb{N}\}.$$

Zum Beweis der Aussage (A) braucht offenbar nur $G \subset \mathscr{K}(F,+,\cdot)$ nachgewiesen zu werden. Da (α) und (β) für alle $a,b \in F^*$ und alle $\varphi,\psi \in G$ gültig sind, reicht es dazu wiederum aus, die folgende Aussage zu beweisen: Wenn (α) und (β) für $\varphi,\psi \in \mathscr{K}(F,+,\cdot)$ und alle $a,b \in F^*$ erfüllt sind, ist $\varphi * \psi$ in $\mathscr{K}(F,+,\cdot)$ enthalten. Unter diesen Voraussetzungen folgt aber

$(ab^{a_{\varphi*\psi}})_{\varphi*\psi} = (ab^{a_\varphi a_\psi})_\varphi (ab^{a_\varphi a_\psi})_\psi =$
$= (b^{a_\varphi a_\psi a_{\bar\varphi}^{-1}})_\varphi a_\varphi (b^{a_\varphi})_\psi a_\psi = b_\varphi a_\varphi b_\psi a_\psi = (b_\varphi b_\psi)(a_\varphi a_\psi) = b_{\varphi*\psi} a_{\varphi*\psi}$

für beliebige $a,b \in F^*$.

Es bleibt (B) zu beweisen. Es seien $\varphi,\psi \in G$, und es werde $a \circ b := ab^{a_\varphi}$ gesetzt (für $a,b \in F^*$). Da

$$(a \circ b)^{x_\psi} = (ab^{a_\varphi})^{x_\psi} = a^{x_\psi} b^{a_\varphi x_\psi} = a^{x_\psi} \circ b^{a_\varphi x_\psi (a^{x_\psi})_{\bar\varphi}^{-1}} = a^{x_\psi} \circ b^{x_\psi}$$

für alle $x \in F^*$, ist Γ_ψ in $A(F,+,\circ)$ enthalten. Schließlich ist $(a \circ b^{a_\psi})_\psi =$
$= (ab^{a_\psi a_\varphi})_\psi = (b^{a_\psi a_\varphi a_\psi^{-1}})_\psi a_\psi = b_\psi a_\psi$, so daß $\psi \in \mathscr{K}(F^\varphi)$. |

§ 3. Endliche Untergruppen der multiplikativen Gruppe eines Fastkörpers. Endliche Fastkörper

Die endlichen Fastkörper sind nach H. Zassenhaus [67] (vgl. auch [45] und [65]) vollständig klassifiziert. Bis auf 7 Typen, die wir am Ende dieses Paragraphen aufführen, sind sie sämtlich Dicksonsch. Wir beginnen mit der Beschreibung und Konstruktion der endlichen Dicksonschen Fastkörper und stellen einige ihrer Eigenschaften zusammen. Anschließend wenden wir uns allgemeiner den endlichen Untergruppen der multiplikativen Gruppe beliebiger Fastkörper zu.

Unser Ausgangspunkt ist der (leicht abgeänderte) Satz 14 aus [49]:

(3.1) *Es seien $F(+,\cdot)$ ein Körper mit p^m Elementen — p eine Primzahl — und Γ eine Untergruppe der Ordnung n von $A(F,+,\cdot)$. Folgende Aussagen sind äquivalent:*

a) *Es existiert ein $\varphi \in \mathscr{K}(F,+,\cdot)$ mit $\Gamma_\varphi = \Gamma$.*

b) *Ist $\sigma: \begin{cases} F \to F \\ x \to x^q \end{cases}$ ein erzeugendes Element von Γ, so ist $\left\{1, \dfrac{q^2-1}{q-1}, \ldots, \dfrac{q^n-1}{q-1}\right\}$ ein Repräsentantensystem* mod n *und $n \Big| \dfrac{q^n-1}{q-1}$.*

c) *Es gibt genau $\Phi(n)$ verschiedene gekoppelte Abbildungen von $F(+,\cdot)$ auf Γ. Dabei bezeichnet Φ die Eulersche Funktion. Wenn q minimal gewählt wird, gilt $|K_F| = q$ und $|F| = q^n$, d. h. $[F:K_F] = n = |F^*/U_\varphi|$.*

Die folgende Abkürzung (vgl. [17]) ermöglicht eine kurze Formulierung der wichtigsten Konsequenz:

Definition 1: Ein geordnetes Paar (q,n) natürlicher Zahlen q und n heißt *Dicksonsches Zahlenpaar* (kurz *D-Zahlenpaar*)[18]), wenn gilt:

[18]) In [17] *Dickson-Veblensches Zahlenpaar* genannt.

(1) q ist eine Primzahlpotenz
(2) Jeder Primteiler von n ist Teiler von $q-1$
(3) Im Fall $q \equiv 3 \bmod n$ gilt $4 \nmid n$.

Die endlichen Dicksonschen Fastkörper lassen sich damit folgendermaßen beschreiben (vgl. [17], (Satz 2) und [42]):

(3.2) *Ist (q,n) ein D-Zahlenpaar, q eine Potenz der Primzahl p, so gibt es bis auf Isomorphie genau $\Phi(n)\cdot i^{-1}$ D-Fastkörper mit q^n Elementen, deren Zentren jeweils aus q Elementen bestehen. Dabei ist Φ wieder die Eulersche Funktion, und i ist die Ordnung von $p (\bmod n)$. Weitere endliche D-Fastkörper existieren nicht.*

Die Klasse aller D-Fastkörper mit q^n Elementen, deren Zentren q Elemente enthalten, wird mit $DF(q^n,q)$[19]) (bzw. $N(n,q)$[20]) bezeichnet.

Zusatz *(vgl. etwa [17]): Die multiplikativen Gruppen je zweier Fastkörper aus $DF(q^n,q)$ sind isomorph.*

Wir schildern ganz kurz die Konstruktion: Es seien (q,n) ein D-Zahlenpaar, $F(+,\cdot)$ ein Körper mit q^n Elementen, w ein erzeugendes Element der Gruppe $F^*(\cdot)$, und es bezeichnen U die Untergruppe $(F^*)^n = \langle w^n\rangle$ vom Index n in $F^*(\cdot)$, σ den Automorphismus $x \to x^q$ von $F(+,\cdot)$ und $\Gamma = \langle\sigma\rangle$ die von σ erzeugte Untergruppe von $A(F,+,\cdot)$. Dann bilden die Zahlen $\left\{1, \frac{q^2-1}{q-1}, \ldots, \frac{q^n-1}{q-1}\right\}$ ein Repräsentantensystem mod n (vgl. etwa [17] oder [67]), d. h. $F^*/U = \left\{U w, U w^{\frac{q^2-1}{q-1}}, \ldots, U w^{\frac{q^n-1}{q-1}}\right\}$. Wenn λ die Abbildung $\begin{cases} F^*/U \to \Gamma \\ U w^{\frac{q^\alpha-1}{q-1}} \to \sigma^\alpha \end{cases}$ und $\varkappa$ den kanonischen Homomorphismus von F^* auf F^*/U bedeuten, ist $\varphi := \varkappa\lambda$ eine gekoppelte Abbildung von $F(+,\cdot)$ auf Γ; und $F^\varphi(+,\cdot)$ ist ein Fastkörper, dessen Kern genau q Elemente enthält und mit dem Fixkörper P_φ von φ identisch ist.

Es folgen einige wichtige Eigenschaften endlicher D-Fastkörperpaare.

(3.3) *Wenn $F(+,\cdot,\circ) = (F,F^\varphi)$ ein endliches D-Fastkörperpaar ist, stimmen der Kern K_F und das Zentrum Z_F von $F(+,\circ)$ sowie der Fixkörper P_φ von φ überein.*

Anmerkung: Im allgemeinen ist das Zentrum eines Fastkörpers echt in seinem Kern enthalten. Beispiele dazu liefern die nicht-regulären endlichen

[19]) Nach H. Karzel [29] (Seite 127).
[20]) Nach P. Dembowski [13] (Seite 34).

Fastkörper vom Typ I, II, V und VI (s. u.) und die unendlichen Kalscheuerschen Fastkörper (vgl. § 9 (B)).

(3.4) (Vgl. [47] (1.13)). *$F(+,\cdot,\circ) = (F,F^\varphi)$ sei ein endliches D-Fastkörperpaar mit $F(+,\circ) \in DF(q^n,q)$. Genau dann ist φ ein gekoppelter Homomorphismus, wenn $n|q-1$.*

Auskunft über die Automorphismengruppen der endlichen D-Fastkörper gibt der Satz 18 aus [67]:

(3.5) *$F(+,\cdot,\circ)$ sei ein endliches D-Fastkörperpaar mit $F(+,\circ) \in DF(q^n,q) \neq DF$ (9,3). Die Automorphismengruppe $A(F,+,\circ)$ von $F(+,\circ)$ ist zyklisch von der Ordnung $\frac{l}{g}$, wobei l die Dimension von $F(+,\cdot)$ über dem Primkörper $GF(p)$ und g die Ordnung von $p \pmod n$ bedeuten. Jeder Automorphismus von $F(+,\circ)$ ist auch ein Automorphismus von $F(+,\cdot)$: $A(F,+,\circ) \subset A(F,+,\cdot)$. Die Automorphismengruppe jedes „Ausnahmefastkörpers" $F(+,\circ) \in DF$ (9,3) ist isomorph zur symmetrischen Gruppe vom Grad 3 und scharf transitiv auf $F \setminus K_F$.*

Eine Verallgemeinerung des wichtigsten Teils dieser Aussage ist in (4.9) enthalten.

Die Struktur der multiplikativen Gruppe der endlichen D-Fastkörper ist ebenfalls vollständig bekannt und folgt aus Eigenschaften, die allen endlichen Untergruppen der multiplikativen Gruppe $F^*(\cdot)$ eines beliebigen Fastkörpers $F(+,\cdot)$ gemeinsam sind. Da die Abbildung $a \to a_l: \begin{cases} F \to F \\ x \to ax \end{cases}$ ein Isomorphismus von $F^*(\cdot)$ auf eine fixpunktfreie Gruppe linearer Abbildungen des Rechtsvektorraums $F(+)$ über $K_F(+,\cdot)$ ist, läßt sich der folgende Hilfssatz (5.8.12) aus [23] anwenden:

> *Sei V ein Rechtsvektorraum über dem Körper $K(+,\cdot)$ und A eine endliche Gruppe linearer Abbildungen von V auf sich. Es sei A fixpunktfrei, d. h. für $1_V \neq \gamma \in A$ und $0 \neq v \in V$ sei stets $v^\gamma \neq v$.*
> a) *Ist $|A| = pq$ mit (nicht notwendig verschiedenen) Primzahlen p und q, so ist A zyklisch.*
> b) *Die p-Sylowgruppen von A sind zyklisch für $p \neq 2$; sie sind zyklisch oder verallgemeinerte Quaternionengruppen für $p = 2$.*
> c) *Es ist $|A| \neq \operatorname{Char} K$.*

Der Teil c) folgt aus dem dortigen Beweis.

Dieser Hilfssatz führt in Verbindung mit Theorem 9.4.3 aus [21] zu den Aussagen

(3.6) *G sei eine endliche Untergruppe der multiplikativen Gruppe $F^*(\cdot)$ eines (beliebigen) Fastkörpers $F(+,\cdot)$. Dann gilt:*

a) *Ist* $|G| = pq$ *mit (nicht notwendig verschiedenen) Primzahlen* p *und* q, *so ist* $G(\cdot)$ *zyklisch.*
b) *Die Sylowgruppen von* $G(\cdot)$ *sind zyklisch oder verallgemeinerte Quaternionengruppen.*
c) $G(\cdot)$ *ist metazyklisch, wenn die 2-Sylowgruppen von* $G(\cdot)$ *zyklisch sind oder wenn eine 2-Sylowgruppe direkter Faktor von* $G(\cdot)$ *ist.*
d) *Es ist* $|G| \neq \operatorname{Char} F(+,\cdot)$.

Zusatz (vgl. [1], Theorem 1 und die Lemmata 1, 2, 3):
Wenn $G(\cdot)$ *metazyklisch ist, besitzt* $G(\cdot)$ *zwei Erzeugende* a *und* b, *die den Relationen*

$$\text{Ordnung } a = m, b^n = a^t, bab^{-1} = a^q$$

genügen, wobei die natürlichen Zahlen m, n, q *und* t *die folgenden Bedingungen erfüllen:*
α) $st = m$; *dabei ist* $s = (q-1, m)$, *und im Fall* $q = 1$ *ist* $n = s = 1$ *zu setzen.*
β) $q^\nu \not\equiv 1 \bmod m$ *für* $1 \leq \nu < n$ *und* $q^n \equiv 1 \bmod m$.
γ) $(n,t) = (q-1,t) \leq 2$.
Die Ordnung von $G(\cdot)$ *ist* mn, *die Kommutatorgruppe* G' *von* $G(\cdot)$ *wird von* a^s *und das Zentrum von* a^t *erzeugt.*
Die Sylowgruppen von $G(\cdot)$ *sind genau dann zyklisch, wenn* $(n,t) = 1$. *Es gilt dann* $(s,t) = 1$ *und* t *ist ungerade.*
Die 2-Sylowgruppen von $G(\cdot)$ *sind genau dann verallgemeinerte Quaternionengruppen, wenn es ungerade Zahlen* m', s', n' *und eine Zahl* $\alpha \geq 2$ *derart gibt, daß*
$n = 2n'$, $m = 2^\alpha m'$, $s = 2s'$, $(n,t) = (s,t) = 2$ *sowie* $q \equiv -1 (\bmod 2^\alpha)$.

Berücksichtigt man die folgende, von H. Zassenhaus [67] stammende und später (vgl. (7.10)) verallgemeinerte Kennzeichnung der endlichen D-Fastkörper in der Menge aller endlichen Fastkörper:

(3.7) *Ein endlicher Fastkörper ist genau dann Dicksonsch, wenn seine multiplikative Gruppe metazyklisch ist,*

so erhält man aus (3.6) und (3.2) den Satz

(3.8) (Vgl. [67] und [17] (Satz 1)).
Die multiplikative Gruppe $F^*(\cdot)$ *des endlichen D-Fastkörpers* $F(+,\cdot) \in DF(q^n, q)$ *ist metazyklisch. Sie besitzt zwei Erzeugende* a *und* b, *die den Relationen*

$$a^m = 1,\ b^n = a^t,\ bab^{-1} = a^q$$

genügen, wobei für die Zahlen m, n, t und q die folgenden Bedingungen gelten:

a) $(q-1)t = m > 0$

b) $q^\nu \not\equiv 1 \bmod m$ *für* $1 \leq \nu < n$ *und* $q^n \equiv 1 \bmod m$

c) $(n,t) = (q-1,t) \leq 2$.

Eine weitere einfache Konsequenz von (3.6) ist

(3.9) *Jede endliche nilpotente Untergruppe G der multiplikativen Gruppe $F^*(\cdot)$ eines Fastkörpers $F(+,\cdot)$ ist metazyklisch, und $G(\cdot)$ ist zyklisch, wenn die 2-Sylowgruppen zyklisch sind. Insbesondere ist jede abelsche endliche Untergruppe von $F^*(\cdot)$ zyklisch.*

Damit erhöht sich die Anwendungsmöglichkeit des folgenden Resultats aus [17] (Satz 4):

(3.10) a) *Es sei $F(+,\cdot,\circ) = (F, F^\varphi)$ ein endliches D-Fastkörperpaar mit $F^\varphi(+,\cdot) = F(+,\circ) \notin DF(9,3)$. Die zyklischen Normalteiler von $F^*(\circ)$ stimmen mit den Untergruppen von U_φ überein, und sie sind charakteristisch in $F^*(\circ)$.*

b) *Im Fall $F(+,\circ) \in DF(9,3)$ ist $F^*(\circ)$ eine Quaternionengruppe, und jedes Element aus F^* erzeugt einen (zyklischen) Normalteiler von $F^*(\circ)$.*

Eine für spätere Zwecke nützliche Ergänzung ist der Satz (vgl. [59])

(3.11) *Es bezeichne $F(+,\cdot,\circ) = (F, F^\varphi)$ ein D-Fastkörperpaar.*

a) *Wenn G eine endliche Untergruppe von $F^*(\circ)$ mit quadratfreier Ordnung ist und $G_\varphi = \{a_\varphi | a \in G\}$ keine inneren Automorphismen von $F(+,\cdot)$ enthält, liegt G in U_φ, und $G(\circ)$ ist zyklisch.*

b) *Jedes Element $a \in F^*$ mit $a^3 = 1$ ist in $U_\varphi \cup V_\varphi$ enthalten.*

Dieses Ergebnis ist bis auf den letzten Teil der Aussage a) in [59] (§ 3, Hilfssatz) bewiesen worden. Die noch zu bestätigende Behauptung folgt aus Cor. 5 von [1], wonach G als Untergruppe der multiplikativen Gruppe $F^*(\cdot)$ des Körpers $F(+,\cdot)$ mit quadratfreier Ordnung zyklisch ist.

Im Fall eines endlichen D-Fastkörperpaares $F(+,\cdot,\circ) = (F, F^\varphi)$ ist jede Untergruppe G von $F^*(\cdot)$ als Untergruppe einer zyklischen Gruppe charakteristisch und daher auch Untergruppe von $F^*(\circ)$. Wegen $a \circ b = ab^{a_\varphi}$ gilt allgemeiner $a \circ G = aG^{a_\varphi} = aG$ für alle $a \in F^*$:

(3.12) (Vgl. [13], Seite 229).

$F(+,\cdot,\circ)$ sei ein endliches D-Fastkörperpaar.

Dann ist jede Untergruppe G von $F^*(\cdot)$ auch Untergruppe von $F^*(\circ)$, und die Linksnebenklassen von G stimmen in beiden Fällen überein.

Insbesondere ist jeder Teilkörper von $F(+,\cdot)$ ein Teilfastkörper von $F(+,\circ)$. Wie wir in (4.15)b) erfahren werden, ist die Menge der Teilkörper von $F(+,\cdot)$ sogar mit der der Teilfastkörper von $F(+,\circ)$ identisch.

In [52] (3.10) und [50] wurde gezeigt, daß jeder endliche Fastkörper von einem Element erzeugt wird. Genauer:

(3.13) *$F(+,\cdot)$ sei ein endlicher Fastkörper mit $[F:K_F]_r = n$. Dann existiert ein Element a in F mit den folgenden Eigenschaften:*
a) *$\{1,a,a^2,\ldots,a^{n-1}\}$ bildet eine Basis des Rechtsvektorraumes (F,K_F).*
b) *$F(+,\cdot)$ wird von a als Fastring erzeugt.*

Nach H. Zassenhaus [67] (vgl. auch [45] und [65]) gibt es neben den Dicksonschen endlichen Fastkörpern bis auf Isomorphie genau 7 weitere endliche Beispiele. Sie enthalten jeweils p^2 Elemente, wobei p eine der Primzahlen 5, 7, 11, 23, 29, 59 ist, und unter ihnen existieren zwei nichtisomorphe Typen mit 11^2 Elementen. Es sind überhaupt die einzigen bis jetzt bekannten nicht-regulären Fastkörper. Späterer Anwendungen wegen geben wir eine kurze Übersicht. Wir halten uns dabei an die Bezeichnungsweisen und Reihenfolge von Zassenhaus [67] und Dembowski [13] (Seite 230–231).

Jeder nicht-reguläre Fastkörper $F(+,\cdot)$ mit p^2 Elementen ist ein Rechtsvektorraum der Dimension 2 über seinem Kern $K_F(+,\cdot)$. Da die Linksmultiplikation $a_l: \begin{cases} F \to F \\ x \to ax \end{cases}$ für jedes $a \in F^*$ ein Automorphismus dieses Vektorraumes ist, läßt sich die multiplikative Gruppe $F^*(\cdot)$ vollständig durch eine zu ihr isomorphe Gruppe $G(\cdot)$ zweireihiger quadratischer regulärer Matrizen über $K_F = \mathrm{GF}(p)$ beschreiben. Im folgenden wird jeweils eine Menge von Erzeugenden angegeben. Eines der erzeugenden Elemente ist in jedem der 7 Fälle $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ mit $A^4 = E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$; ein zweites Element B hat in allen Fällen die Ordnung 3 und – wie A – die Determinante 1.

Typ I: $p = 5$, $G = \langle A,B\rangle =: M(2,3)$, wobei $B = \begin{pmatrix} 1 & -2 \\ -1 & -2 \end{pmatrix}$.

$A(F,+,\cdot)$ ist zyklisch von der Ordnung 4. Wenn τ ein erzeugender Automorphismus ist, gilt $\tau^2 = i_2$. (Vgl. die Def. (1.6)).

Typ II: $p = 11$, $G = \langle A,B,C\rangle$, wobei $B = \begin{pmatrix} 1 & 5 \\ -5 & -2 \end{pmatrix}$ und $C = \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}$.
Es ist $G \cong \langle A,B\rangle \times \langle C\rangle$ auflösbar und $\langle A,B\rangle \cong M(2,3)$.
$A(F,+,\cdot)$ hat die Ordnung 2.

Typ III: $p = 7$, $G = \langle A,B\rangle = :G_3$, wobei $B = \begin{pmatrix} 1 & 3 \\ -1 & -2 \end{pmatrix}$.
$A(F,+,\cdot) = \langle i_2\rangle$ hat die Ordnung 3.

Typ IV: $p = 23$, $G = \langle A,B,C\rangle$, wobei $B = \begin{pmatrix} 1 & -6 \\ 12 & -2 \end{pmatrix}$ und $C = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$.
Es gilt $G \cong \langle A,B\rangle \times \langle C\rangle$ mit $\langle A,B\rangle \cong G_3$. G ist auflösbar und $A(F,+,\cdot)$ ist trivial.

Typ V: $p = 11$, $G = \langle A,B\rangle \cong \mathrm{SL}_2(5)$, wobei $B = \begin{pmatrix} 2 & 4 \\ 1 & -3 \end{pmatrix}$.
Es gilt $G/Z(G) \cong A_5$. G ist nicht auflösbar, und $A(F,+,\cdot) = \langle i_2\rangle$ hat die Ordnung 5.

Typ VI: $p = 29$, $G = \langle A,B,C\rangle$, wobei $B = \begin{pmatrix} 1 & -7 \\ -12 & -2 \end{pmatrix}$ und $C = \begin{pmatrix} -13 & 0 \\ 0 & -13 \end{pmatrix}$.
Es gilt $G \cong \langle A,B\rangle \times \langle C\rangle$ mit $\langle A,B\rangle \cong \mathrm{SL}_2(5)$, und $A(F,+,\cdot) = \langle i_2\rangle$ hat die Ordnung 2.

Typ VII: $p = 59$, $G = \langle A,B,C\rangle$, wobei $B = \begin{pmatrix} 9 & 15 \\ -10 & -10 \end{pmatrix}$ und $C = \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}$.
Es gilt $G \cong \langle A,B\rangle \times \langle C\rangle$ mit $\langle A,B\rangle \cong \mathrm{SL}_2(5)$, und $A(F,+,\cdot)$ ist trivial.

In den Fällen I, III und V ist $Z_F = \{0,1,-1\}$; in allen anderen Fällen gilt $Z_F = \{0\} \cup \langle C\rangle \cup \{-\langle C\rangle\}$, d. h. $Z_F = K_F$ bei den Typen II, IV und VII und $[K_F^* : Z_F^*] = 2$ beim Typ VI.

Die Automorphismengruppen sind von D. A. Foulser [19] bestimmt worden.

§ 4. Automorphismen Dicksonscher Fastkörperpaare

In diesem Abschnitt werden im wesentlichen die Resultate über Isomorphismen und Antiisomorphismen zwischen D-Fastkörperpaaren aus [59] beschrieben. Sie enthalten insbesondere eine Verallgemeinerung des Zassenhausschen Kriteriums (3.5), eine Ausdehnung des Hauptsatzes der Galoistheorie auf D-Fastkörperpaare mit „kleiner" D-Gruppe und Aussagen über die Fortsetzbarkeit von Isomorphismen.

Definition 1: Unter einem *Isomorphismus* (bzw. *Antiisomorphismus*) von einem Fastkörperpaar $F(+,\cdot,\circ)$ auf ein zweites Paar $F'(+,\cdot,\circ)$ verstehen wir eine bijektive Abbildung von F auf F', die gleichzeitig ein Isomorphismus (bzw. Antiisomorphismus) von $F(+,\cdot)$ auf $F'(+,\cdot)$ und ein Isomorphismus zwischen $F(+,\circ)$ und $F'(+,\circ)$ ist. Im Fall $F = F'$ sprechen wir von *Automorphismen* bzw. *Antiautomorphismen*. Die Gruppe der Automorphismen und Antiautomorphismen eines Fastkörpers $F(+,\cdot)$ wird im folgenden mit $\bar{A}(F,+,\cdot)$ bezeichnet.

Die Unsymmetrie, die in dieser Definition des Antiisomorphismus hinsichtlich der Verknüpfungen $\cdot$ und $\circ$ besteht, wird durch unser Interesse an D-Fastkörperpaaren und die folgende Bemerkung verständlich:

Wenn es einen Antiisomorphismus zwischen zwei (Links-)Fastkörpern gibt, sind sie beide Körper.

A) Vorbereitende Ergebnisse

Wir beginnen mit einer leichten Verallgemeinerung des Satzes 9 aus [31]:

(4.1) *$F(+,\cdot,\circ) = (F, F^{\varphi})$ sei ein Fastkörperpaar. Wenn $F(+,\circ)$ ein Körper ist, gilt $K_F = P_{\varphi}$ oder $K_F = Q_{\varphi} = F$. Im zweiten Fall sind die Verknüpfungen $\cdot$ und $\circ$ dual zueinander.* (Dabei bezeichnet K_F den Kern von $F(+,\cdot)$.)

Der Beweis ist eine Modifikation der in [31] benutzten Schlußweise: Für beliebige $x, y \in F$ mit $x \neq 0, -1$ gilt $(x+1)\circ y = x \circ y + y$, d. h.

$$(x+1)y^{(x+1)_{\varphi}} = xy^{x_{\varphi}} + y. \tag{I}$$

Es sei $k \in K_F$ und es werde $z = k^{(x+1)\bar{\varphi}^1}$ gesetzt.

Wir ersetzen y in (I) durch yz:

$$(x+1)y^{(x+1)_{\varphi}} z^{(x+1)_{\varphi}} = xy^{x_{\varphi}} z^{x_{\varphi}} + yz,$$

multiplizieren die Gleichung (I) von rechts mit $k = z^{(x+1)_{\varphi}} \in K_F$:

$$(x+1)y^{(x+1)_{\varphi}} z^{(x+1)_{\varphi}} = xy^{x_{\varphi}} z^{(x+1)_{\varphi}} + yz^{(x+1)_{\varphi}},$$

und erhalten durch einen Vergleich die Beziehung

$$xy^{x_{\varphi}} z^{x_{\varphi}} + yz = xy^{x_{\varphi}} z^{(x+1)_{\varphi}} + yz^{(x+1)_{\varphi}}, \quad \text{d. h.}$$

$$xy^{x_{\varphi}}(z^{x_{\varphi}} - z^{(x+1)_{\varphi}}) = y(z^{(x+1)_{\varphi}} - z). \tag{II}$$

Schließlich setzen wir den aus (II) durch die Spezialisierung $y = 1$ hervorgehenden Ausdruck $z^{x_{\varphi}} - z^{(x+1)_{\varphi}} = x^{-1}(z^{(x+1)_{\varphi}} - z)$ in (II) ein und erhalten

$$xy^{x_{\varphi}} x^{-1}(z^{(x+1)_{\varphi}} - z) = y(z^{(x+1)_{\varphi}} - z), \tag{III}$$

gültig für alle $x, y \in F$ mit $x \neq 0, -1$ und alle $z \in F$ mit $z^{(x+1)_{\varphi}} \in K_F$. Es seien x und z Elemente aus F mit $x \notin \{0, -1\}, z^{(x+1)_{\varphi}} \in K_F$ sowie $z^{(x+1)_{\varphi}} \neq z$. Aus (III) folgt $y^{x_{\varphi}} = y^{ix}$ für alle $y \in F$, d. h. $x \in V_{\varphi}$.

Für jedes $x \in F^* \setminus V_{\varphi}$ gilt daher $z^{(x+1)_{\varphi}} = z = z^{x_{\varphi}}$ (vgl. (II)), falls $z^{(x+1)_{\varphi}} \in K_F$, also $k = k^{(x+1)\bar{\varphi}^1} = k^{(x+1)\bar{\varphi}^1 x_{\varphi}}$ für alle $k \in K_F$, d. h. $x \in U_{\varphi}(K_F)$. Da V_{φ} und $U_{\varphi}(K_F)$ Untergruppen von $F^*(\circ)$ sind, tritt notwendig einer der Fälle $F^* = V_{\varphi}$, d. h. aber $K_F = F = Q_{\varphi}$, oder $F^* = U_{\varphi}(K_F)$, d. h. $K_F \subset P_{\varphi}$, ein.

Das beweist die Behauptung, weil P_{φ} offenbar in K_F enthalten ist. |

Die nächsten Ergebnisse stammen im wesentlichen von F. Pokropp, der in [48] erstmals Isomorphismen zwischen Gruppenpaaren und Fastkörperpaaren untersuchte.

(4.2) *Es seien $F(+,\cdot)$ und $F'(+,\cdot)$ zwei Fastkörper. Jeder Isomorphismus (bzw. Antiisomorphismus) π von $F(+,\cdot)$ auf $F'(+,\cdot)$ induziert eine Bijektion $\hat{\pi}: \varphi \to \varphi^{\hat{\pi}}$ von $\mathscr{K}(F,+,\cdot)$ auf $\mathscr{K}(F',+,\cdot)$, wobei $\varphi^{\hat{\pi}}$ die durch*

$$(*) \qquad x^{\pi} \to (x_{\varphi})^{i_{\pi}} = \pi^{-1} x_{\varphi} \pi$$

(bzw.

$$(**) \qquad x^{\pi} \to (x_{\varphi} i_{x^{-1}})^{i_{\pi}} = (x_{\varphi})^{i_{\pi}} i_{x^{\pi}} = \pi^{-1} x_{\varphi} i_{x^{-1}} \pi)$$

$(x \in F^*)$ erklärte Abbildung von F'^* in $A(F',+,\cdot)$ ist.
Wenn $F''(+,\cdot)$ ein dritter Fastkörper und τ ein Isomorphismus bzw. Antiisomorphismus von $F'(+,\cdot)$ auf $F''(+,\cdot)$ sind, gilt $\widehat{\pi\tau} = \hat{\pi}\hat{\tau}$.

Der Übergang von φ zu $\varphi^{\hat{\pi}}$ bedeutet ein Übertragen der Verknüpfung $\circ$ von F auf F' mit Hilfe der Bijektion π, d. h. es gilt $(x \circ y)^{\pi} = x^{\pi} \circ y^{\pi}$ für alle $x, y \in F$, wenn $F(+,\circ) = F^{\varphi}(+,\cdot)$ und $F'(+,\circ) = F'^{\varphi^{\hat{\pi}}}(+,\cdot)$ gesetzt wird.

(4.3) *Es seien $F(+,\cdot,\circ) = (F, F^{\varphi})$ und $F'(+,\cdot,\circ) = (F', F'^{\psi})$ zwei Fastkörperpaare und π ein Isomorphismus oder Antiisomorphismus von $F(+,\cdot)$ auf $F'(+,\cdot)$ (bzw. ein Isomorphismus von $F(+,\circ)$ auf $F'(+,\circ)$). Genau dann ist π ein Isomorphismus zwischen $F(+,\circ)$ und $F'(+,\circ)$ (bzw. ein Isomorphismus oder Antiisomorphismus zwischen $F(+,\cdot)$ und $F'(+,\cdot)$), wenn $\psi = \varphi^{\hat{\pi}}$ nach (*) oder (**).*

Aus (4.2) und (4.3) folgt unmittelbar

(4.4) *Für jeden Fastkörper $F(+,\cdot)$ ist die Abbildung*

$$\begin{cases} \bar{A}(F,+,\cdot) \times \mathscr{K}(F,+,\cdot) \to \mathscr{K}(F,+,\cdot) \\ (\pi, \varphi) \to \varphi^{\hat{\pi}} \end{cases}$$

eine äußere Operation, und die Gruppe der Automorphismen und Antiautomorphismen von (F, F^{φ}) ist der Stabilisator von φ.

(4.5) *Die D-Gruppen zweier isomorpher Fastkörperpaare sind isomorph.*

Es sei π ein Isomorphismus von $F(+,\circ) = F^{\varphi}$ auf $F'(+,\circ) = F'^{\psi}$.

Aufgrund der beiden Sätze (4.2) und (4.3) gilt $(x_{\varphi})^{i_{\pi}} = (x^{\pi})_{\psi}$ bzw. $(x_{\varphi})^{i_{\pi}} = (x^{\pi})_{\psi}(i_{x^{\pi}})^{-1}$, wenn π ein Isomorphismus bzw. Antiisomorphismus von $F(+,\cdot)$ auf $F'(+,\cdot)$ ist. Insbesondere ist dann $(\Gamma_{\varphi})^{i_{\pi}}$ in der Automorphismengruppe $A(F',+,\cdot)$ von $F'(+,\cdot)$ enthalten. Der nächste Satz (vgl. [59], Satz 1) besagt u. a., daß diese Bedingung im Fall von D-Fastkörperpaaren auch hinreichend ist:

(4.6) *$(F, F^{\varphi}) = F(+,\cdot,\circ)$ und $(F', F'^{\psi}) = F'(+,\cdot,\circ)$ seien zwei D-Fastkörperpaare. Ein Isomorphismus π von $F(+,\circ)$ auf $F'(+,\circ)$ ist ein Isomorphismus oder Antiisomorphismus zwischen $F(+,\cdot)$ und $F'(+,\cdot)$, wenn eine der folgenden Bedingungen erfüllt ist:*

a) $\pi^{-1}\Gamma_{\varphi}\pi \subset \bar{A}(F', +,\cdot)$

b) $\pi\Gamma_{\psi}\pi^{-1} \subset \bar{A}(F, +.\cdot)$.

Anmerkung: Nach [7] (Th. 1.15 auf Seite 37) ist (a) (bzw. (b)) aus (4.6) schon dann erfüllt, wenn

$$(a'^{-1})^{\pi^{-1}a_{\varphi}\pi} = (a'^{\pi^{-1}a_{\varphi}\pi})^{-1} \quad \text{(bzw. } (a^{-1})^{\pi a'_{\psi}\pi^{-1}} = (a^{\pi a'_{\psi}\pi^{-1}})^{-1}\text{)}$$

für alle $a \in F^*$ und $a' \in F'^*$.

B) Isomorphismen und Antiisomorphismen zwischen D-Fastkörperpaaren

Das erste Resultat ist die angekündigte Verallgemeinerung des Kriteriums (3.5) von H. Zassenhaus (vgl. [59], Satz 2):

(4.7) *$F(+,\cdot,\circ) = (F, F^{\varphi})$ und $F'(+,\cdot,\circ) = (F', F'^{\psi})$ seien zwei D-Fastkörperpaare, und es gelte $F(+,\circ) \notin DF(9,3)$.*

a) *Wenn $|\Gamma_{\varphi}| < |F|$ und $|\Gamma_{\psi}| < |F|$ (bzw. $|F^*/V_{\varphi}| < |F|$ und $|F'^*/V_{\psi}| < |F|$) erfüllt sind, ist jeder Isomorphismus von $F(+,\circ)$ auf $F'(+,\circ)$ ein Isomorphismus zwischen $F(+,\cdot)$ und $F'(+,\cdot)$.*

b) *Wenn $|\Gamma_{\varphi}| < |F|$ und $|F'^*/V_{\psi}| < |F|$ (bzw. $|F^*/V_{\varphi}| < |F|$ und $|\Gamma_{\psi}| < |F|$) erfüllt sind, ist jeder Isomorphismus von $F(+,\circ)$ auf $F'(+,\circ)$ ein Antiisomorphismus zwischen $F(+,\cdot)$ und $F'(+,\cdot)$.*

Die Anwendung dieses Satzes auf die identische Abbildung von F führt unmittelbar zu dem Korollar

(4.8) *$F(+,\cdot) \xrightarrow{\varphi} F(+,\circ)$ und $F(+,*) \xrightarrow{\psi} F(+,\circ)$ seien D-Fastkörperpaare mit $F(+,\circ) \notin DF(9,3)$.*

a) *Aus $|\Gamma_{\varphi}| < |F|$ und $|\Gamma_{\psi}| < |F|$ (bzw. $|F^*/V_{\varphi}| < |F|$ und $|F^*/V_{\psi}| < |F|$) folgt $F(+,\cdot) = F(+,*)$, d. h. die Operationen $\cdot$ und $*$ stimmen in F überein.*

b) *Unter den Voraussetzungen $|\Gamma_{\varphi}| < |F|$ und $|F^*/V_{\psi}| < |F|$ (bzw. $|F^*/V_{\varphi}| < |F|$ und $|\Gamma_{\psi}| < |F|$) sind die Operationen $\cdot$ und $*$ dual zueinander, d. h. es gilt $ab = b * a$ für alle $a, b \in F$.*

Mit Rücksicht auf (2.12) gewinnt man aus (4.7) außerdem sofort die folgende Transitivitätseigenschaft der Fastkörperableitung $\rightarrow$:

(4.9) a) $(F,F^{\varphi}) = F(+,\cdot,\circ)$ *sei ein D-Fastkörperpaar, und es gelte* $F(+,\circ) \notin DF(9,3)$ *sowie* $|\Gamma_{\varphi}| < |F|$ *(bzw.* $|F^*/V_{\varphi}| < |F|$*). Dann ist jeder aus* $F(+,\circ)$ *ableitbare Fastkörper auch aus* $F(+,\cdot)$ *ableitbar.*
b) *Wenn die Automorphismengruppe eines Körpers* $F(+,\cdot)$ *eine kleinere Mächtigkeit hat als* F *selbst und* $|F| \neq 9$ *gilt, ist jeder aus* $F(+,\cdot)$ *durch wiederholtes Ableiten entstehende Fastkörper aus* $F(+,\cdot)$ *(in einem Schritt) ableitbar.*

(4.7) besitzt ein Gegenstück in der folgenden Aussage (vgl. [59], Satz 3):

(4.10) $F(+,\cdot,\circ) = (F,F^{\varphi})$ *und* $F'(+,\cdot,\circ) = (F',F'^{\psi})$ *seien zwei Fastkörperpaare mit* $F(+,\cdot) \notin DF(9,3)$ *und* $|\Gamma_{\varphi}| < |F|, |\Gamma_{\psi}| < |F'|$. *Wenn* $F(+,\circ)$ *und* $F'(+,\circ)$ *Körper sind, ist jeder Isomorphismus von* $F(+,\cdot)$ *auf* $F'(+,\cdot)$ *ein Isomorphismus zwischen* $F(+,\circ)$ *und* $F'(+,\circ)$.

Daraus gewinnt man eine Symmetrieeigenschaft der Fastkörperableitung $\rightarrow$:

(4.11) *Es sei* $F(+,\cdot,\circ) = (F,F^{\varphi})$ *ein Fastkörperpaar mit* $|\Gamma_{\varphi}| < |F|$. *Wenn* $F(+,\circ)$ *ein Körper ist, sind* $F(+,\cdot)$ *und* $F(+,\circ)$ *äquivalent. Insbesondere ist* $F(+,\cdot)$ *dann ein Dicksonscher Fastkörper.*

Bemerkungen:

a) Auf die Einschränkung $F(+,\circ) \notin DF(9,3)$ kann in (4.7), (4.8) und (4.9) nicht verzichtet werden: Es gibt vier verschiedene gekoppelte Abbildungen für jedes $F(+,\circ) \in DF(9,3)$. Die drei nichttrivialen unter ihnen führen zu drei verschiedenen (natürlich isomorphen) Körpern, so daß (4.9) nicht gültig ist; die zugehörigen D-Gruppen haben die Ordnung 2.

b) Auch die Bedingung $|\Gamma_{\varphi}| < |F|$ darf in (4.7), (4.8) und (4.10) nicht weggelassen werden.

C) Teilfastkörperpaare

Für das Studium von Fastkörperpaaren $F(+,\cdot,\circ)$ ist es besonders nützlich, eine Übersicht über sämtliche Teilfastkörperpaare zu gewinnen (d. s. Teilmengen von F, die Teilfastkörper von $F(+,\cdot)$ und $F(+,\circ)$ sind). Der nächste Satz sagt aus, daß diese unter geeigneten Voraussetzungen mit den Teilfastkörpern von $F(+,\circ)$ übereinstimmen (vgl. Satz 4 aus [59]).

(4.12) a) $F(+,\cdot,\circ)$ *sei ein D-Fastkörperpaar mit kommutativer Verknüpfung* $\cdot$. *Dann ist ein endlicher Teilfastkörper* E *von* $F(+,\circ)$ *gleichzeitig Teilkörper von* $F(+,\cdot)$, *oder es ist* $\operatorname{Char} F = p = 2^{p'} - 1$ *eine Mersennesche Primzahl und* $|E| = p^2$.

b) *Jeder endliche Teilfastkörper eines D-Fastkörpers ist Dicksonsch.*

c) *Es seien* $F(+,\cdot,\circ) = (F,F^{\varphi})$ *ein unendliches D-Fastkörperpaar und E ein in einem kommutativen Teilkörper von* $F(+,\cdot)$ *enthaltener Teilfastkörper von* $F(+,\circ)$. *Es gelte* $|\Gamma_{\varphi}|^2 < |E|$, *und* $U := E \cap U_{\varphi}$ *sei algebraisch über einem in E liegenden Teilkörper* L_0 *von* $F(+,\cdot)$, *d. h. jedes Element aus U sei algebraisch über* $L_0(+,\cdot)$.

Dann ist E ein Teilkörper von $F(+,\cdot)$.

d) *Bei jedem endlichen D-Fastkörperpaar* $F(+,\cdot,\circ)$ *stimmt die Menge der Teilfastkörper von* $F(+,\circ)$ *mit der der Teilkörper von* $F(+,\cdot)$ *überein.*

Die Aussage d) ist auch von Frl. S. Dancs in [11] und [12] bewiesen worden.

Anmerkung: Ein Teilkörper von $F(+,\cdot)$ braucht kein Teilfastkörper von $F(+,\circ)$ zu sein, wenn $F(+,\cdot,\circ)$ ein unendliches D-Fastkörperpaar ist. Diese Feststellung werden wir später (vgl. die Folgerung (g) in § 9, Abschnitt C) mit Beispielen belegen.

D) Galoistheorie

Die Ergebnisse der beiden vorhergehenden Abschnitte erlauben es, wesentliche Teile der Galoistheorie kommutativer Körper auf eine Klasse Dicksonscher Fastkörper zu übertragen.

Definition 2: a) Wir nennen einen Fastkörper $F(+,\cdot)$ *galoissch* über einem Teilfastkörper H (und H *galoissch* in $F(+,\cdot)$), wenn H die Fixmenge einer Untergruppe von $A(F,+,\cdot)$ ist.

b) Die Gruppe aller Automorphismen eines Fastkörpers $F(+,\cdot)$, die einen gegebenen Teilfastkörper H elementweise festlassen, wird als die *volle Galoisgruppe* von $F(+,\cdot)$ über H bezeichnet.

Eine Anwendung von (4.7) und (4.12) auf den Hauptsatz der Galoistheorie in kommutativen Körpern liefert den folgenden Satz (vgl. Satz 5 in [59]):

(4.13) *Es bezeichne* $F(+,\cdot,\circ) = (F,F^{\varphi})$ *ein D-Fastkörperpaar mit* $|\Gamma_{\varphi}| < |F|$, *und* $F(+,\circ)$ *sei galoissch über dem Teilfastkörper H. Dann ist H ein galoisscher Teilkörper von* $F(+,\cdot)$. *Wenn* $F(+,\cdot)$ *außerdem kommutativ und über H algebraisch ist, stimmt die volle Galoisgruppe* $\mathfrak{G}(H)$ *von* $F(+,\circ)$ *über H im Fall* $F(+,\circ) \notin DF(9,3)$ *mit der vollen Galoisgruppe von* $F(+,\cdot)$ *über H überein; die Menge* $\mathfrak{F}$ *aller H enthaltenden Teilkörper von* $F(+,\cdot)$ *ist identisch mit der Menge aller H umfassenden Teilfastkörper von* $F(+,\circ)$, *und die Abbildung* $E \to \mathfrak{G}(E) =$

$\{\gamma \in \mathfrak{G}(H) | e^\gamma = e$ für alle $e \in E\}$ stellt eine Bijektion von $\mathfrak{F}$ auf die Menge $\mathfrak{A}$ aller (bezüglich der endlichen Topologie) abgeschlossenen Untergruppen von $\mathfrak{G}(H)$ mit der Inversen $\mathfrak{H} \to \{a \in F | a^\gamma = a$ für alle $\gamma \in' \mathfrak{H}\}$ von $\mathfrak{A}$ in $\mathfrak{F}$ dar. H ist genau dann galoissch in $E(+,\circ) \in \mathfrak{F}$, wenn $\mathfrak{G}(E)$ einen Normalteiler in $\mathfrak{G}(H)$ bildet, und die Galoisgruppen von $E(+,\circ)$ über H ist dann isomorph zu $\mathfrak{G}(H)/\mathfrak{G}(E)$, falls $E(+,\circ) \notin DF(9,3)$.

Aus (4.13) und (3.5) gewinnt man sofort das Korollar

(4.14) *Es sei $F(+,\cdot,\circ) \in DF(q^n,q)$. Genau dann ist $F(+,\circ)$ über jedem Teilfastkörper galoissch, wenn* Char $F \equiv 1 \bmod n$.

Der Hauptsatz (4.13) ermöglicht außerdem Aussagen über die Fortsetzbarkeit von Isomorphismen (vgl. [59], Satz 6):

(4.15) *Es bezeichne $F(+,\cdot,\circ) = (F, F^\varphi)$ ein D-Fastkörperpaar mit $|\Gamma_\varphi| < |F|$, und $F(+,\circ)$ sei galoissch über dem Teilfastkörper H. Wenn $F(+,\cdot)$ kommutativ und über H algebraisch ist, bildet jeder H enthaltende Teilfastkörper E von $F(+,\circ)$ einen Teilkörper von $F(+,\cdot)$, und im Fall $E(+,\circ) \notin DF(9,3)$ stimmen die H elementweise festlassenden Isomorphismen von $E(+,\circ)$ in $F(+,\circ)$ mit denen von $E(+,\cdot)$ in $F(+,\cdot)$ überein. Jeder dieser Isomorphismen kann zu einem Automorphismus von $F(+,\cdot,\circ)$ fortgesetzt werden.*

§ 5. Ein Zassenhauskriterium für unendliche Fastkörper

In [67] gelang H. Zassenhaus eine vollständige Klassifizierung der endlichen Fastkörper in reguläre und nichtreguläre. Es stellt sich die Frage nach einer Verallgemeinerung auf beliebige Fastkörper. Ein wichtiger Schritt bei ihrer Beantwortung wäre die Lösung des Problems, die D-Fastkörper in der Klasse aller Fastkörper intern zu kennzeichnen. Eine solche Lösung liefe auf eine Ausdehnung des Kriteriums (3.7) hinaus und wäre auch insofern interessant, als die Körperstruktur $F(+,\cdot)$ eines D-Fastkörperpaars $F(+,\cdot,\circ)$ wichtige Aufschlüsse über die Fastkörperstruktur $F(+,\circ)$ liefern kann. Wir werden in diesem Abschnitt in dem Satz (5.1) hinreichende Bedingungen angeben und dann nachweisen, daß eine umfangreiche Klasse Dicksonscher Fastkörper – in der alle dem Autor bekannten Beispiele enthalten sind – diesen Bedingungen genügt.

(5.1) (Vgl. [58], Satz 1) a) *Die multiplikative Gruppe $F^*(\circ)$ eines Fastkörpers $F(+,\circ)$ enthalte einen Normalteiler A mit den folgenden Eigenschaften:*
(I) $-1 \in A$

(II) *Aus* $\sum_{i=1}^{n} a_i = 0$ *mit* $a_1,\ldots,a_n \in A$ *folgt* $\sum_{i=1}^{n} (a_i \circ x) = 0$ *für jedes* $x \in A$.

(III) *F wird von A als Fastring erzeugt.*

Dann ist $F(+,\circ)$ ein Dicksonscher Fastkörper.

Genauer: Es gilt $F = \left\{ \sum_{i=1}^{n} a_i | a_1,\ldots,a_n \in A; n \in \mathbb{N} \right\}$; *durch* $x \cdot \left(\sum_{i=1}^{n} a_i \right) = \sum_{i=1}^{n} (a_i \circ x)$ *(mit $x \in F$ und $a_1,\ldots,a_n \in A$) wird eine Verknüpfung $\cdot$ in F definiert, und $F(+,\cdot,\circ) = (F(+,\cdot),F(+,\circ))$ ist ein D-Fastkörperpaar.*

b) *Wenn A ein abelscher Normalteiler von $F^*(\circ)$ ist, der $F(+,\circ)$ als Fastring erzeugt, so erfüllt der (abelsche) Normalteiler $\bar{A} = A \cup (-A)$ die Bedingungen (I), (II) und (III).*

Bemerkungen:

1. Die Bedingung (II) kann durch die folgende Forderung ersetzt werden:

(II') Für beliebige $a_1,\ldots,a_n \in A$ mit $\sum_{i=1}^{n} a_i = 0$ ist der von

$$\left\{ \sum_{i=1}^{n} (x^{-1} \circ a_i \circ x) | x \in F^* \right\}$$

erzeugte Teilfastkörper von $F(+,\circ)$ echt in F enthalten.

2. An Stelle von $\cdot$ kann in F natürlich auch die duale Operation eingeführt werden.

3. $F(+,\cdot)$ ist genau dann kommutativ, wenn A abelsch ist.

Der folgende Zusatz zu (5.1) kann ohne Schwierigkeiten verifiziert werden:

(5.2) *Der Normalteiler A der multiplikativen Gruppe $F^*(\circ)$ des Fastkörpers $F(+,\circ)$ erfülle die Bedingungen (I), (II) und (III) aus* (5.1), *die binäre Operation $\cdot$ werde wie dort eingeführt, und es sei $F(+,\cdot) \to F(+,\circ)$. Dann gilt:*

a) $U_\varphi = (Z_F(A))^*$ [15].

b) $V_\varphi \cup \{0\} = \left\{ \sum_{i=1}^{n} a_i | a_1,\ldots,a_n \in A; n \in \mathbb{N};\ \sum_{i=1}^{n} (a_i \circ a) = \left(\sum_{i=1}^{n} a_i \right) \circ a \right.$ *für alle* $\left. a \in A \right\}$.

c) $P_\varphi = K_F \cap \left\{ \sum_{i=1}^{n} a_i | a_1,\ldots,a_n \in A; n \in \mathbb{N};\ \sum_{i=1}^{n} (a_i \circ a) = \sum_{i=1}^{n} (a \circ a_i) \right.$ *für alle* $\left. a \in A \right\}$.

d) $Q_\varphi = K_F$.

e) *Wenn $A(\circ)$ abelsch ist, gilt $U_\varphi = V_\varphi = (Z_F(A))^*$, d. h. $U_\varphi = V_\varphi$ ist ein maximaler abelscher Normalteiler von $F^*(\circ)$.*

Mit Hilfe des Zornschen Lemmas gewinnt man außerdem sofort den Hilfssatz

(5.3) *Zu jedem die Bedingungen (I), (II) und (III) aus* (5.1) *erfüllenden Normalteiler A der multiplikativen Gruppe eines Fastkörpers $F(+,\circ)$ gibt es einen A enthaltenden maximalen Normalteiler dieser Art.*

(5.4) *A sei ein den Bedingungen (I), (II) und (III) aus* (5.1) *genügender Normalteiler der multiplikativen Gruppe $F^*(\circ)$ eines Fastkörpers $F(+,\circ)$, und hinsichtlich dieser Eigenschaft maximal. Dann läßt sich in F eine binäre Operation $\cdot$ derart einführen, daß $F(+,\cdot,\circ) = (F,F^\varphi)$ ein D-Fastkörperpaar ist und $U_\varphi = A$ (oder auch $V_\varphi = A$) gilt.*

Die Behauptung folgt aus (5.1)a), (5.2)b), der Möglichkeit, zur dualen Struktur überzugehen, und der folgenden, leicht zu bestätigenden Aussage, mit der wir uns der Frage zuwenden, unter welchen Voraussetzungen die Bedingungen des Satzes (5.1) notwendig sind:

(5.5) *Wenn $F(+,\cdot,\circ) = (F,F^\varphi)$ ein D-Fastkörperpaar ist, erfüllen die Normalteiler U_φ und V_φ von $F^*(\circ)$ die Bedingungen (I) und (II) aus* (5.1).

Weitere Information enthält

(5.6) a) *A und A' seien zwei die Bedingungen (I), (II) und (III) aus* (5.1) *erfüllende Normalteiler der multiplikativen Gruppe $F^*(\circ)$ eines Fastkörpers $F(+,\circ)$, und sie seien hinsichtlich dieser Eigenschaft maximal. Wenn $|F^*/A| < |F|, |F^*/A'| < |F|$ sowie $|F| \neq 9$ gelten, stimmen A und A' überein.*

b) *$F(+,\cdot,\circ) = (F,F^\varphi)$ sei ein D-Fastkörperpaar mit $|\Gamma_\varphi| < |F|$ (bzw. $|F^*/V_\varphi| < |F|$), sowie $|F| \neq 9$. Dann ist jeder den Bedingungen (I), (II) und (III) aus* (5.1) *sowie $|F^*/A| < |F|$ genügende Normalteiler A von $F^*(\circ)$ in U_φ (bzw. V_φ) enthalten.*

Beweis: a) Nach (5.4) lassen sich Operationen $\cdot$ und $*$ in F derart einführen, daß $F(+,\cdot,\circ) = (F,F^\varphi)$ und $F(+,*,\circ) = (F,F^\psi)$ D-Fastkörperpaare und $A = U_\varphi$ sowie $A' = U_\psi$ erfüllt sind. Wegen $\Gamma_\varphi \cong (F^*/U_\varphi)(\circ)$ und $\Gamma_\psi \cong (F^*/U_\psi)(\circ)$ stimmen $\cdot$ und $*$ nach (4.8) überein, so daß $A = U_\varphi = U_\psi = A'$.

b) Infolge (5.3) gibt es einen A enthaltenden Normalteiler A' von $F^*(\circ)$, der (I), (II) und (III) erfüllt und hinsichtlich dieser Eigenschaft maximal ist. Die Behauptung folgt damit aus (5.4) und (4.8). |

Der Hilfssatz (5.5) legt die Frage nahe, unter welchen Voraussetzungen wenigstens einer der Normalteiler U_φ, V_φ von $F^*(\circ)$ die Eigenschaft (III) besitzt. Eine Teilantwort ist in dem folgenden Satz (vgl. [59], Satz 2) ent-

halten, der damit Aussagen über den Anwendungsbereich des Satzes (5.1) liefert:

(5.7) *$(F,F^{\varphi}) = F(+,\cdot,\circ)$ sei ein D-Fastkörperpaar. Die Bedingungen (I), (II) und (III) aus* (5.1) *werden zumindest von einem der Normalteiler U_{φ}, V_{φ} von $F^*(\circ)$ erfüllt, wenn φ eine der folgenden Eigenschaften hat:*

a) *φ ist ein gekoppelter Homomorphismus oder Antihomomorphismus (bzw. d-Homomorphismus oder d-Antihomomorphismus), und $F(+,\circ)$ ist algebraisch über U_{φ} (bzw. V_{φ}).*

b) *$(F^*/U_{\varphi})(\circ)$ (bzw. $(F^*/V_{\varphi})(\circ)$) ist abelsch, $F(+,\circ)$ algebraisch über U_{φ} (bzw. V_{φ}), und $\langle U_{\varphi}\rangle$ (bzw. $\langle V_{\varphi}\rangle$) ist kein invarianter Teilkörper von $F(+,\circ)$ mit $[F:\langle U_{\varphi}\rangle]_l = 2$ (bzw. $[F:\langle V_{\varphi}\rangle]_l = 2$). (Dabei bezeichnet $\langle U_{\varphi}\rangle$ (bzw. $\langle V_{\varphi}\rangle$) den von U_{φ} (bzw. V_{φ}) erzeugten Teilfastkörper von $F(+,\circ)$).*

c) *$|\Gamma_{\varphi}| < |F|$ (bzw. $|F^*/V_{\varphi}| < |F|$), und $F(+,\circ)$ ist algebraisch über U_{φ} (bzw. V_{φ}).*

Das ist insbesondere der Fall, wenn Γ_{φ} (bzw. F^*/V_{φ}) endlich ist.

Anmerkung: b) kann mit Hilfe der Ergebnisse aus § 7 weiter verschärft werden.

§ 6. Normale Fastkörper

E. Ellers und H. Karzel führten in [16] den Begriff des normalen Fastkörpers ein.

Definition 1: a) Wenn H ein invarianter Teilfastkörper $\neq F$ eines Fastkörpers $F(+,\cdot)$ ist, wird das geordnete Paar $(F(+,\cdot), H(+,\cdot))$ – im folgenden kurz (F,H) geschrieben – ein *normaler Fastkörper* genannt[21]). Die Dimension des Linksvektorraums F über H (vgl. (1.6)) heißt der *Rang* von (F,H) und wird $[F:H]$ geschrieben. Jeder Teilfastkörper von $F(+,\cdot)$, der H enthält, wird als *Zwischenfastkörper* von (F,H) bezeichnet.

b) Zwei normale Fastkörper (F,H) und (F',H') heißen *isomorph*, wenn es einen Isomorphismus τ von $F(+,\cdot)$ auf $F'(+,\cdot)$ mit $H^{\tau} = H'$ gibt.

Bemerkung: Es ist $i_a|H: \begin{cases} H \to H \\ h \to a^{-1}ha \end{cases}$ für jedes $a \in F^*$ ein Automorphismus des Körpers $H(+,\cdot)$, wie man sofort bestätigt. Daher stellt die Linksmultiplikation $a_l: \begin{cases} F \to F \\ x \to ax \end{cases}$ für jedes $a \in F^*$ eine bijektive semilineare Transformation des Linksvektorraums (F,H) dar.

[21]) Die in [16] zusätzlich geforderte Bedingung „$(\alpha+\beta)a = \alpha a + \beta a$ für alle $a \in F$ und $\alpha,\beta \in H$" ist nach (1.6) überflüssig.

Ellers und Karzel [16] wiesen nach, daß normale Fastkörper das geeignete Hilfsmittel sind, um die ebenfalls von ihnen eingeführten und untersuchten projektiven Inzidenzgruppen algebraisch zu beschreiben.

Definition 2: a) Eine Struktur $G(\cdot,\pi)$ wird *projektive Inzidenzgruppe* genannt[22]), wenn G eine Menge, $\cdot$ eine binäre Operation in G und π eine Teilmenge der Potenzmenge von G mit den folgenden Eigenschaften sind:

(IG 1) $G(\cdot)$ ist eine Gruppe

(IG 2) $G(\pi)$ ist ein projektiver Raum

(IG 3) Für jedes $a \in G$ ist die Linkstranslation $a_l: x \to ax$ von $G(\cdot)$ ein Automorphismus von $G(\pi)$.

$G(\cdot,\pi)$ heißt *desarguessch*, wenn $G(\pi)$ desarguessch ist, *abelsch*, wenn $G(\cdot)$ abelsch ist, und *zweiseitig*, wenn auch die Rechtstranslation $a_r: x \to xa$ von $G(\cdot)$ für jedes $a \in G$ ein Automorphismus von $G(\pi)$ ist. Die Dimension von $G(\pi)$ wird auch die *Dimension* von $G(\cdot,\pi)$ genannt. Eine Teilmenge U von G heißt *Inzidenzuntergruppe* von $G(\cdot,\pi)$, wenn sie Untergruppe von $G(\cdot)$ und projektiver Teilraum von $G(\pi)$ ist.

b) Zwei projektive Inzidenzgruppen $G(\cdot,\pi)$ und $G'(\cdot,\pi')$ werden *isomorph* genannt, wenn es eine Bijektion τ von G auf G' gibt, die ein Isomorphismus sowohl von $G(\cdot)$ auf $G'(\cdot)$ als auch von $G(\pi)$ auf $G'(\pi')$ ist.

Der erwähnte Zusammenhang zwischen normalen Fastkörpern und projektiven Inzidenzgruppen wird in den nächsten beiden Sätzen präzisiert. (Vgl. [16] oder [32] (Sätze 1, 2, 3, 4).)

(6.1) a) *Jedem normalen Fastkörper (F,H) ist eine projektive desarguessche Inzidenzgruppe F^*/H^* (die sog. Inzidenzgruppe von (F,H)) zugeordnet: Ihre Gruppenstruktur ist die der Faktorgruppe $(F^*/H^*)(\cdot)$ und ihre projektive Struktur die durch den Linksvektorraum (F,H) gegebene.*

b) *Jedem Zwischenfastkörper L von (F,H) entspricht die Inzidenzuntergruppe L^*/H^* von F^*/H^*.*

c) *Die Inzidenzgruppen zweier normaler Fastkörper (F,H) und (F',H') mit $[F:H] \geqslant 3$ sind genau dann isomorph, wenn (F,H) und (F',H') isomorph sind.*

(6.2) a) *Zu jeder desarguesschen projektiven Inzidenzgruppe $G(\cdot,\pi)$ einer Dimension $\geqslant 2$ gibt es bis auf Isomorphie genau einen normalen Fastkörper (F,H), dessen Inzidenzgruppe F^*/H^* zu $G(\cdot,\pi)$ isomorph ist.*

Es gilt $[F:H] = \dim G(\cdot,\pi) + 1$, und $H(+,\cdot)$ ist isomorph zum Koordinatenkörper von $G(\pi)$.

b) *Zu jeder Inzidenzuntergruppe U von $G(\cdot,\pi)$ gibt es genau einen Zwischenfastkörper L von (F,H), dessen Inzidenzgruppe L^*/H^* der*

[22]) Genauer: *Links-Inzidenzgruppe.*

Gruppe $U(\cdot,\pi)$ bei dem Isomorphismus zwischen $G(\cdot,\pi)$ und F^*/H^* entspricht.

Anmerkung: Projektive Inzidenzgruppen der Dimension 1 sind in [64] untersucht worden.

Während die kommutativen und zweiseitigen Inzidenzgruppen Gegenstand des nächsten Paragraphen sind, sei im folgenden kurz geschildert, wie nach E. Ellers und H. Karzel [17] alle endlichen desarguesschen projektiven Inzidenzgruppen einer Dimension $\geqslant 2$ ermittelt werden können. Aufgrund der Darstellungssätze (6.1) und (6.2) ist diese Aufgabe gleichwertig mit der Bestimmung aller endlichen normalen Fastkörper (F,H) mit $[F:H] \geqslant 3$. Wir fassen die wichtigsten Resultate aus [17] zusammen.

(6.3) *Es seien $F(+,\cdot,\circ) = (F,F^\varphi)$ ein endliches D-Fastkörperpaar mit $F(+,\circ) \in DF(q^n,q)$ und $a \in F^*$ ein erzeugendes Element von $U_\varphi(\circ)$. Dann gilt:*

a) *Jeder invariante Teilfastkörper $L \neq F$ von $F(+,\circ)$ ist in $U_\varphi \cup \{0\}$ enthalten. $|L^*|$ ist daher ein Teiler von $\dfrac{q^n-1}{n}$, und $L^*(\circ)$ wird von a^s erzeugt, wobei $s = \dfrac{q^n-1}{n\cdot|L^*|}$.*

(Vgl. auch die Verallgemeinerung (8.3).)

b) *Ist $p^\sigma - 1, (p = \operatorname{Char} F)$, ein Teiler von $\dfrac{q^n-1}{n}$, so gibt es genau einen invarianten Teilfastkörper L von $F(+,\circ)$ mit $|L| = p^\sigma$.*

Eine kurze Formulierung erlaubt der folgende Begriff:

Definition 3: Das Tripel $(p^{\tau n}, p^\tau, p^\sigma)$ mit einer Primzahl p und natürlichen Zahlen τ, n und σ heißt *normales Zahlentripel*, wenn (p^τ, n) ein Dicksonsches Zahlenpaar ist, und wenn $p^\sigma - 1 \Big| \dfrac{p^{\tau n}-1}{n}$.

Damit folgt aus (6.3) und (3.2):

(6.4) *Für jeden endlichen normalen Fastkörper (F,H) ist $(|F|, |K_F|, |H|)$ ein normales Zahlentripel. Ist umgekehrt $(p^{\tau n}, p^\tau, p^\sigma)$ ein normales Zahlentripel, so gibt es bis auf Isomorphie genau einen normalen Fastkörper (F,H) mit $|F| = p^{\tau n}, |H| = p^\sigma, |K_F| = p^\tau$ und regulärem $F(+,\cdot)$.*

Man beachte, daß die nichtregulären Fastkörper $F(+,\cdot)$ vom Typ II, IV und VII drei normale Fastkörper $(F,K_F) = (F,Z_F)$ liefern.

Eine Folgerung aus (6.4) (vgl. [17], (19)) ist

(6.5) *Es sei H ein invarianter Teilfastkörper $\neq F$ des endlichen Fastkörpers $F(+,\cdot)$. Aus $K_F \subset H$ folgt $K_F = H = Z_F$.*

Der Satz von Cartan-Brauer-Hua[23]) legt die Vermutung nahe, daß jeder normale Fastkörper (F,H) mit $F \neq H$ sogar zentral ist im Sinne der

Definition 4: Ein Teilfastkörper H eines Fastkörpers $F(+,\cdot)$ heißt *zentral*, wenn $H \subset Z_F$. Wir nennen (F,H) dann einen *zentralen Fastkörper*.

Es gibt jedoch (sogar endliche) Gegenbeispiele:

(6.6) ([17], Satz 7): *Ein endlicher normaler Fastkörper (F,H) mit dem normalen Zahlentripel $(p^{\tau n},p^{\tau},p^{\sigma})$ ist genau dann zentral, wenn $\sigma|\tau$ gilt.*

Wir beenden diesen Paragraphen mit einer angekündigten Ergänzung zu (1.12):

(6.7) a) *Es sei (F,H) ein normaler Fastkörper mit periodischer Inzidenzgruppe F^*/H^*. Dann ist $F(+,\cdot)$ projektiv.*

b) *$F(+,\cdot,\circ) = (F,F^{\varphi})$ sei ein Fastkörperpaar mit periodischer Dicksongruppe. Wenn $F(+,\cdot)$ projektiv ist, dann auch $F(+,\circ)$.*

Der Beweis wird mit dem folgenden Hilfssatz vorbereitet:

(6.8) *a sei ein Element $\neq 1$ eines Fastkörpers $F(+,\cdot)$.*

a) *Zu jedem $n \in \mathbb{N}$ und jedem $x \in F$ gibt es ein $y \in F$ mit $a^n x - x = ay - y$.*

b) *Wenn es eine natürliche Zahl $n \geqslant 1$ mit $a^n = 1$ gibt, ist die Gleichung $ax - x = b$ für jedes $b \in F$ in F lösbar.*

Beweis: a) Für $y := x + ax + a^2x + \cdots + a^{n-1}x$ gilt $ay - y = a^n x - x$, wie man sofort nachrechnet.

b) n sei die kleinste natürliche Zahl $\geqslant 1$ mit $a^n = 1$.

Nach (3.7)d) ist n nicht durch die Charakteristik von $F(+,\cdot)$ teilbar. Für beliebiges $x \in F$ ist $x_0 := x + ax + a^2x + \cdots + a^{n-1}x = 0$, denn $ax_0 = x_0$ und $a \neq 1$. Wenn τ die Abbildung $x \to \sum_{\nu=0}^{n-1} \{a^{\nu}x \cdot (\nu+1)\}$ von F in sich bezeichnet (dabei ist $y \cdot \nu = \sum_{i=1}^{\nu} y_i$ mit $y_i = y$ für $i = 1,\ldots,\nu$), gilt $ax^{\tau} = x^{\tau} + x \cdot n - x_0 = x + x \cdot n$, d. h. $ax^{\tau} - x^{\tau} = x \cdot n$, wie man sich leicht überzeugt.

Wegen Char $F \nmid n$ gibt es zu jedem $b \in F$ ein $x_b \in F$ mit $x_b \cdot n = b$, und es folgt $ax_b^{\tau} - x_b^{\tau} = b$. |

Beweis zu (6.7):

a) Für jedes $a \in H\backslash\{1\}$ und alle $b \in F$ ist $ax - x = (a-1)x = b$ in F

[23]) Er besagt, daß jeder invariante Teilkörper $\neq F$ eines Körpers $F(+,\cdot)$ in dessen Zentrum Z_F liegt.

lösbar. Aus den Voraussetzungen und (6.8) gewinnt man unmittelbar die Behauptung.

b) Für jedes $a \in U_\varphi \backslash \{1\}$ und alle $b \in F$ ist $a \circ x - x = ax - x = b$ lösbar in F. Wieder folgt die Behauptung aus (6.8). |

Anmerkung: Aus (6.8) folgt allgemein: Wenn es zu jedem Element $a \in F$ unendlicher Ordnung (bez. $\cdot$) eine natürliche Zahl n derart gibt, daß $a^n x - x = 1$ eine Lösung in F hat, ist $F(+,\cdot)$ projektiv.

§ 7. Normale Fastkörper mit kommutativer bzw. zweiseitiger Inzidenzgruppe

Nachdem die Bestimmung der endlichen, desarguesschen projektiven Inzidenzgruppen mit den in § 6 geschilderten Ergebnissen von E. Ellers und H. Karzel abgeschlossen ist, wenden wir uns in diesem Abschnitt den Klassen der kommutativen und zweiseitigen projektiven Inzidenzgruppen zu. H. Karzel bewies in den drei Noten [26], [27] und [29], daß ein normaler Fastkörper (F,H) im Fall $[F:H] \geqslant 3$ genau dann eine kommutative Inzidenzgruppe F^*/H^* hat, wenn $F(+,\cdot)$ ein kommutativer Körper ist; und in [55] wurde gezeigt, daß ein normaler Fastkörper (F,H) mit $[F:H] \geqslant 3$ genau dann eine zweiseitige Inzidenzgruppe besitzt, wenn $F(+,\cdot)$ ein Körper ist. In der Note [60], die diesem Paragraphen zugrunde liegt, wurden beide Ergebnisse verschärft und ihre Beweise vereinfacht[24]). Danach ist die folgende Aussage gültig ([60], Satz 1):

(7.1) *Es seien (F,H) ein normaler Fastkörper mit $[F:H] \geqslant 3$ und a ein Element aus $F \backslash H$. Wenn aH^* und $(a+1)H^*$ im Zentrum von F^*/H^* liegen, d. h. wenn $[x,a] \in H^*$ und $[x,a+1] \in H^*$[25]) für alle $x \in F^*$, sind a und $a+1$ im Zentrum Z_F von $F(+,\cdot)$ enthalten.*

Ein Korollar ist der erwähnte Satz von H. Karzel:

(7.2) *Die Inzidenzgruppe F^*/H^* eines normalen Fastkörpers (F,H) mit $[F:H] \geqslant 3$ ist genau dann kommutativ, wenn $F(+,\cdot)$ ein kommutativer Körper ist.*

Zur Verschärfung des Ergebnisses aus [55] ist es zweckmäßig, den Begriff der Zweiseitigkeit algebraisch zu deuten (vgl. [16], Satz 3):

Es sei $G(\cdot,\pi) = F^*/H^*$ die Inzidenzgruppe eines normalen Fastkörpers (F,H). Die Abbildung $a_r: H^*x \to (H^*x)\cdot(H^*a)$ von G in sich ist für

---

[24]) Inzwischen hat Herr Bröcker in seiner Habilitationsschrift einen kurzen Beweis des Hauptsatzes aus [55] angegeben. Er stützt sich dabei jedoch – wie [55] – wesentlich auf den Satz von H. Karzel sowie Satz 6 aus [30].

[25]) $[u,v] = uvu^{-1}v^{-1}$ bezeichnet den Kommutator von $u,v \in F^*$.

$a \in F^*$ genau dann eine Kollineation von $G(\pi)$, wenn $(x + y) \cdot a \in H^* xa + H^* ya$ für alle $x, y \in F$.

Es bezeichne $H(a)$ den kleinsten Teilfastkörper von $F(+,\cdot)$, der a und H enthält. Dann läßt sich der folgende Satz ([60], Satz 2) aussprechen:

(7.3) *Es seien (F,H) ein normaler Fastkörper und a ein Element aus $F \setminus H$.*

a) *Wenn $H(a) \neq F$ und $(x + y)c \in H^* xc + H^* yc$ für $c = a$ und $c = a + 1$ sowie alle $x, y \in F$ erfüllt sind, ist a im Kern K_F von $F(+,\cdot)$ enthalten.*

b) *Wenn $[F : H] \geqslant 3, H(a) = F$ sowie $(x + y)c \in H^* xc + H^* yc$ für alle $x, y \in F$ und alle $c \in H + Ha = \{\alpha + \beta a | \alpha, \beta \in H\}$ gelten, ist $F(+,\cdot)$ ein kommutativer Körper.*

Eine einfache Anwendung dieses Resultats führt zu dem Hauptsatz der Note [55]:

(7.4) *Es sei (F,H) ein normaler Fastkörper mit $[F : H] \geqslant 3$. Gilt das verallgemeinerte rechtsseitige Distributivgesetz $(a + b) \cdot c \in H^* ac + H^* bc$ für alle $a, b, c \in F$, so ist $F(+,\cdot)$ ein Körper.*

Eine ganz andere Situation findet man im Fall $[F : H] = 2$ vor. In jedem normalen Fastkörper (F,H) vom Rang $[F : H] = 2$ ist die Bedingung aus (7.3)a) für alle $c \in F$ erfüllt: Mit x und y sind auch xc und yc für jedes $c \in F^*$ linear unabhängig über H, so daß $Hxc + Hyc = F$; und wenn $x \in F^*$ und $y \in F$ linear abhängig über H sind, gibt es ein $\gamma \in H$ mit $y = \gamma x$, so daß $(x + y)c = (x + \gamma x)c = (1 + \gamma)xc = xc + \gamma xc = xc + yc$ für jedes $c \in F$. Dem Satz (6.4) entnimmt man, daß es unendlich viele (sogar endliche) echte normale Fastkörper vom Rang 2 gibt; dabei nennen wir einen normalen Fastkörper (F,H) *echt*, wenn $F(+,\cdot)$ kein Körper ist.

Die Frage, wie Satz (7.1) modifiziert werden muß, wenn die Voraussetzung „$[F : H] \geqslant 3$" durch „$[F : H] = 2$" ersetzt wird, ist nur zum Teil beantwortet. Bisher sind zwei echte normale Fastkörper (vom Rang 2) mit kommutativer Inzidenzgruppe bekannt:

a) Das Zentrum Z_F jedes Fastkörpers $F(+,\cdot)$ aus $DF(9,3)$ ist ein invarianter Teilfastkörper, und die Faktorgruppe $(F^*/Z_F^*)(\cdot)$ ist eine Kleinsche Vierergruppe.

b) Jeder Fastkörper $F(+,\cdot)$ aus $DF(64,4)$ enthält einen nichtzentralen, invarianten Teilfastkörper H derart, daß $(F^*/H^*)(\cdot)$ zyklisch ist.

Die ersten Teilantworten zu dem aufgeworfenen Problem gab H. Karzel in [29] (Satz 1 und Satz 2):

(I) *Ist (F,H) ein endlicher normaler Fastkörper mit $[F:H]=2$ und kommutativer Inzidenzgruppe F^*/H^*, so ist $F(+,\cdot)$ entweder ein kommutativer Körper oder in $DF(9,3)$ bzw. $DF(64,4)$ enthalten.*

(II) *Ist (F,H) ein zentraler Fastkörper mit $[F:H]=2$ und kommutativer Inzidenzgruppe F^*/H^*, so ist $F(+,\cdot)$ entweder ein kommutativer Körper oder in $DF(9,3)$ enthalten.*

Eine Verallgemeinerung wurde in [60] bewiesen. Wenn (F,H) ein normaler Fastkörper ist, bezeichne j_x für jedes $x\in F^*$ den Automorphismus $\alpha\to x^{-1}\alpha x$ des Körpers $H(+,\cdot)$, und $J_{(F,H)}$ sei die Automorphismengruppe $\{j_x|x\in F^*\}$ von $H(+,\cdot)$. Dann gilt ([60], Satz 3):

(7.5) *(F,H) sei ein normaler Fastkörper vom Rang $[F:H]=2$ mit kommutativer Inzidenzgruppe F^*/H^*, und es gelte $|J_{(F,H)}|<|F|$. Dann ist $F(+,\cdot)$ entweder ein kommutativer Körper oder in $DF(9,3)$ bzw. $DF(64,4)$ enthalten.*

Nach [60] (§ 2, Hilfssatz 1) stimmt der Kern K_F unter den Voraussetzungen dieses Satzes mit dem Zentrum überein, und $H\cap Z_F$ ist offenbar der Fixkörper der Automorphismengruppe $J_{(F,H)}$. Wenn $H(+,\cdot)$ kommutativ und $[H:(H\cap K_F)]$ endlich sind, folgt aus dem Hauptsatz der Galoistheorie, daß $|J_{(F,H)}|=[H:(H\cap K_F)]<|F|$. Daher besitzt (7.5) das Korollar

(7.6) *(F,H) sei ein normaler Fastkörper vom Rang $[F:H]=2$ mit kommutativer Inzidenzgruppe F^*/H^*. Wenn $H(+,\cdot)$ kommutativ und $[H:(H\cap K_F)]$ endlich sind, ist $F(+,\cdot)$ entweder ein kommutativer Körper oder in $DF(9,3)$ bzw. $DF(64,4)$ enthalten.*

(I) und (II) sind offenbar Spezialfälle dieses Korollars.

Unter gewissen Zusatzbedingungen ist ein normaler Fastkörper vom Rang 2 mit kommutativer Inzidenzgruppe notwendig Dicksonsch ([60], Satz 5):

(7.7) *(F,H) sei ein normaler Fastkörper mit $[F:H]=2$ und kommutativer Inzidenzgruppe F^*/H^*. Wenn es ein Element $a\in F\setminus H$ mit $a^2\in H$ gibt, ist $F(+,\cdot)$ Dicksonsch.*

Anmerkung: Die Bedingung „$a^2\in H$" kann ersetzt werden durch die Forderung „Char $H\neq 2$, $a^2=\mu a+\nu$ mit $\mu,\nu\in H$ und $\mu a\nu^{-1}a=a^2\nu^{-1}\mu$".

Da sich die Körpermultiplikation $\cdot$ unter diesen Voraussetzungen durchweg als kommutativ herausstellt (vgl. (8.4) mit Anmerkung), gewinnt der folgende Satz an Interesse ([60], Satz 4):

(7.8) *Es seien $F(+,\cdot,\circ)$ ein Dicksonsches Fastkörperpaar und H ein invarianter Teilfastkörper von $F(+,\circ)$ mit den Eigenschaften.*

α) $F(+,\cdot)$ *ist kommutativ*
β) $[F:H] = 2$
γ) $(F^*/H^*)(\circ)$ *ist kommutativ*
δ) $|K_F \cap H| > 3$ *(Das ist insbesondere dann der Fall, wenn* $|K_F| \neq 2,3,4,9$.*)*
Dann stimmen die Operationen $\cdot$ *und* $\circ$ *in* F *überein.*

Eine Ergänzung ist

(7.9) *H sei ein Teilfastkörper $\neq F$ des Fastkörpers $F(+,\cdot)$, und* Char $F \neq 2$. *Wenn die Quadrate aller Elemente aus F in H liegen, ist $F(+,\cdot)$ in $DF(9,3)$ enthalten.*

Diese Ergebnisse lassen sich auf den Satz (5.1) anwenden und führen zu einer weiteren Verallgemeinerung des Zassenhauskriteriums (3.7) (vgl. [60], Korollar zum Satz 1):

(7.10) *Die multiplikative Gruppe $F^*(\cdot)$ eines Fastkörpers $F(+,\cdot)$ enthalte einen abelschen Normalteiler A mit den folgenden Eigenschaften:*
a) $(F^*/A)(\cdot)$ *ist abelsch;*
b) $F(+,\cdot)$ *ist algebraisch über* $\bar{A} = A \cup (-A)$.
Dann ist $F(+,\cdot)$ Dicksonsch (und sogar aus einem kommutativen Körper ableitbar), oder F ist unendlich und enthält einen invarianten, kommutativen Teilkörper H, der den Bedingungen genügt:
α) $[F:H] = 2$
β) $(F^*/H^*)(\cdot)$ *ist kommutativ*
γ) $|J_{(F,H)}| = |\{j_x | x \in F^*\}| = |F|$
δ) $x \notin H \Rightarrow x^2 \notin H$.
Wegen (γ) ist dann insbesondere $[H:(Z_F \cap H)]$ *unendlich.*

Ganz entsprechend gewinnt man aus (7.4) und (5.1) die Aussage

(7.11) *Die multiplikative Gruppe $F^*(\cdot)$ des Fastkörpers $F(+,\cdot)$ enthalte einen abelschen Normalteiler A mit den folgenden Eigenschaften:*
a) $(x+y)z \in xz \cdot R^* + yz \cdot R^*$ *für alle* $x,y,z \in F$; *dabei bezeichne* $R = \left\{ \sum_{i=1}^{n} a_i | a_1,\ldots,a_n \in A; n \in \mathbb{N} \right\}$ *den von A erzeugten Teilfastring von $F(+,\cdot)$.*
b) $F(+,\cdot)$ *ist algebraisch über A.*
Dann ist $F(+,\cdot)$ ein D-Fastkörper, oder R ist ein invarianter, kommutativer Teilkörper von $F(+,\cdot)$ mit $[F:R] = 2$.

§ 8. Kern und Zentrum eines Dicksonschen Fastkörpers

In diesem Abschnitt bezeichnen durchgehend $F(+,\cdot,\circ) = (F,F^{\varphi})$ ein D-Fastkörperpaar und A eine Teilmenge von F.

Unser Interesse gilt den Beziehungen zwischen $K_F(A), Z_F(A)$ (im Fastkörper $F(+,\circ)$) sowie $P_{\varphi}(A)$ und $Q_{\varphi}(A)$. Eine erste Auskunft gab (2.5):

Wenn A eine Unterhalbgruppe von $F(+)$ ist, sind $P_{\varphi}(A)$ und $Q_{\varphi}(A)$ in $K_F(A)$ enthalten.

Es wird sich herausstellen, daß unter geeigneten Voraussetzungen auch eine der umgekehrten Inklusionen gültig ist. Wir beginnen mit einigen vorbereitenden Hilfssätzen.

Hs. 1: *Es seien* $a,b,c \in F$ *und* $a \neq 0,-1$. *Wenn* $(a+1)\circ x = a\circ x + x$ *für alle* $x \in \{b,c,bc\}$ *erfüllt ist, gilt* α): $b^{a^{\varphi}} = b^{i_a}, b^{(a+1)^{\varphi}} = b^{i_{(a+1)}}$, oder β): $c^{a^{\varphi}} = c^{(a+1)^{\varphi}} = c$.

Beweis: Wir setzen zur Abkürzung

$$b^{a^{\varphi}} = b_1, b^{(a+1)^{\varphi}} = b_2, c^{a^{\varphi}} = c_1 \quad \text{und} \quad c^{(a+1)^{\varphi}} = c_2 .$$

Nach Voraussetzung gilt

$$(a+1)b_2 = (a+1)\circ b = a\circ b + b = ab_1 + b, \quad \text{d. h.}$$

(I) $(a+1)b_2 = ab_1 + b$.

Ganz entsprechend folgen

(II) $(a+1)c_2 = ac_1 + c$ und

(III) $(a+1)b_2c_2 = ab_1c_1 + bc$.

Aus (I) und (III) gewinnt man

$$ab_1c_2 + bc_2 = (a+1)b_2c_2 = ab_1c_1 + bc,$$

d. h. – mit Rücksicht auf (II) –

$$ab_1(c_2 - c_1) = b(c - c_2) = ba(c_2 - c_1).$$

Es folgt $c_1 = c_2 = c$ oder $b_1 = a^{-1}ba = b^{i_a}$ und – nach (I) – $b_2 = b^{i_{(a+1)}}$. |

Ein einfaches Korollar ist

(8.1) *H sei eine das Einselement* 1 *enthaltende Unterhalbgruppe von* $F(\circ)$. *Dann folgt aus* $b,c,bc \in K_F(H)$ *stets* $b \in Q_{\varphi}(H)$ *oder* $c \in P_{\varphi}(H)$.

Beweis: Die Voraussetzungen zum Hs. 1 sind für alle $a \in H^* \setminus \{-1\}$ erfüllt. Daher gilt $c^{a^{\varphi}} = c$ oder $b^{a^{\varphi}} = b^{i_a}$ für alle $a \in H^*$, d. h. $H^* \subset M \cup N$, wenn $M = \{a \in F^* | c^{a^{\varphi}} = c\}$ und $N = \{a \in F^* | b^{a^{\varphi}} = b^{i_a}\}$ gesetzt wird. Die

Behauptung ist offenbar mit dem Nachweis bestätigt, daß M und N Untergruppen von $F^*(\circ)$ sind. Er enthält keine Schwierigkeiten. |

Folgerung: Wenn H eine Unterhalbgruppe von $F(\circ)$ mit $1 \in H$ bezeichnet, ist $x \in F^*$ also insbesondere dann in $P_\varphi(H) \cup Q_\varphi(H)$ enthalten, wenn eine der Bedingungen

$$\text{(a)} \quad x, x^{-1} \in K_F(H), \qquad \text{(b)} \quad x, x^2 \in K_F(H)$$

erfüllt ist.

Hs. 2: *B sei eine Unterhalbgruppe von $F(\cdot)$. Für $a \in F \setminus \{0, -1\}$ gilt genau dann $(a+1) \circ b = a \circ b + b$ für alle $b \in B$, wenn $a, a+1 \in U_\varphi(B)$ oder $a, a+1 \in V_\varphi(B)$.*

Beweis: Offenbar muß nur eine Richtung der Behauptung bewiesen werden. Es gelte also $(a+1) \circ b = a \circ b + b$ für alle $b \in B$.

Dem Hs. 1 entnimmt man, daß B in $M \cup N$ enthalten ist, wenn M und N die Mengen $M = \{b \in F^* | b^{a_\varphi} = b\}$ und $N = \{b \in F^* | b^{a_\varphi} = b^{i_a}\}$ bezeichnen. Da M und N Untergruppen von $F^*(\cdot)$ sind, folgt $B \subset M$ oder $B \subset N$. |

Eine direkte Konsequenz ist

(8.2) *Es seien H eine Unterhalbgruppe von $F(\circ)$ mit $1 \in H$ und B eine in $K_F(H)$ enthaltene Unterhalbgruppe von $F(\cdot)$.*
Dann gilt $B \subset P_\varphi(H)$ oder $B \subset Q_\varphi(H)$, d. h. $H^* \subset U_\varphi(B)$ oder $H^* \subset V_\varphi(B)$.

Beweis: Infolge (8.1) ist B in $P_\varphi(H) \cup Q_\varphi(H)$ enthalten, so daß die Behauptung aus der Feststellung folgt, daß $(P_\varphi(H))^*$ und $(Q_\varphi(H))^*$ Untergruppen von $F^*(\cdot)$ sind. |

Ein wichtiger Spezialfall ist

(8.3) *Es sei H eine Unterhalbgruppe von $F(\circ)$ mit $1 \in H$. Aus $K_F(H) = F$ folgt $H^* \subset U_\varphi$ oder $H^* \subset V_\varphi$. Insbesondere ist jeder invariante Teilfastkörper $\neq F$ von $F(+, \circ)$ in $U_\varphi \cup \{0\}$ oder in $V_\varphi \cup \{0\}$ enthalten.*

Aus (8.3) und (6.2)a) gewinnt man die Aussage:
Wenn $F(+, \cdot)$ kommutativ ist, ist jeder invariante Teilfastkörper $H \neq F$ von $F(+, \circ)$ kommutativ, F^*/H^* also eine Pappossche Inzidenzgruppe.

Wir ergänzen und verallgemeinern sie mit dem Satz

(8.4) *Es seien $F(+, \cdot, \circ) = (F, F^\varphi)$ ein D-Fastkörperpaar und H ein invarianter Teilfastkörper von $F(+, \circ)$.*

a) *H ist im Zentrum C von $F(+,\cdot)$ enthalten, wenn eine der folgenden Bedingungen erfüllt ist:*

α) U_φ und V_φ sind Normalteiler von $F^*(\cdot)$.

β) Γ_φ oder F^*/V_φ ist endlich, und H ist unendlich.

b) *H ist in C oder in Z_F enthalten, wenn eine der folgenden Bedingungen gilt:*

α) φ ist ein gekoppelter Antihomomorphismus (bzw. d-Antihomomorphismus).

β) U_φ (bzw. V_φ) ist Normalteiler von $F^*(\cdot)$, und Γ_φ (bzw. $(F^*/V_\varphi)(\circ)$) ist abelsch.

Beweis: a) Unter der Voraussetzung α) liegt H^* nach (8.3) in U_φ oder in V_φ. Im Fall $H^* \subset U_\varphi$ ist U_φ bez. $\cdot$ im Normalisator von H^* enthalten, denn es gilt $uHu^{-1} = u \circ H \circ u^{-1} \subset H$ für jedes $u \in U_\varphi$. Ganz entsprechend sieht man ein, daß V_φ im Fall $H^* \subset V_\varphi$ im Normalisator von H^* enthalten ist. Die Behauptung folgt daher aus [22] (Theorem 3).

Es sei β) vorausgesetzt.

Da die beiden Bedingungen in β) dual zueinander sind, können wir etwa von der Voraussetzung ausgehen, daß Γ_φ endlich ist.

1. Fall (vgl. (8.3)): $H^* \subset U_\varphi$.

Es ist $\{H^{i_a} | a \in F^*\}$ nach [18] (Theorem 3) eine unendliche Menge, wenn H nicht im Zentrum C von $F(+,\cdot)$ liegt. Unter dieser Annahme wäre daher auch Γ_φ unendlich, weil $H^{a\varphi} = H^{i_a}$ für jedes $a \in F^*$: Es ist $a \circ h \circ a^{-1} = a \circ (ha^{-1}) = ah^{a\varphi}a^{-1}$ für alle $a \in F^*$ und $h \in H$.

2. Fall: $H^* \subset V_\varphi$.

Angenommen H ist nicht in C enthalten. Nach [51] (Lemma) gilt $|H^*/(C \cap H)^*| = |H|$, so daß $|\{i_h | h \in H^*\}| = |H|$. Wegen $\{i_h = h_\varphi | h \in H\} \subset \Gamma_\varphi$ widerspricht das den Voraussetzungen.

b) folgt direkt aus dem Beweis zum Teil a) (α) – wenn H in U_φ liegt, ist H nach [22] Teilmenge von C, weil U_φ Normalteiler von $F^*(\cdot)$ ist – und dem

Hs. 3: *$F(+,\cdot,\circ) = (F, F^\varphi)$ sei ein D-Fastkörperpaar, das der Bedingung ($*$) „$\{v_\varphi | v \in V_\varphi\}$ ist im Zentrum von Γ_φ enthalten" genügt. Dann liegt jede Unterhalbgruppe L von $F(+)$ mit $1 \in L \subset V_\varphi$ in C oder in Z_F.*
($*$) ist insbesondere dann erfüllt, wenn Γ_φ kommutativ oder wenn φ ein gekoppelter Antihomomorphismus ist.

Beweis: a) Wenn φ ein gekoppelter Antihomomorphismus ist, gilt für beliebige $v \in V_\varphi$ und $x \in F^*$: $x_\varphi v_\varphi = (v \circ x)_\varphi = (xv)_\varphi = v_\varphi x_\varphi$, d. h. v_φ liegt im Zentrum von Γ_φ.

b) Es sei (*) vorausgesetzt.

Für beliebige $v \in V_\varphi$ und $x \in F^*$ gilt $x_\varphi^{-1} v_\varphi^{-1} x_\varphi v_\varphi = 1_F$, d. h. $v \circ x \circ v^{-1} \circ x^{-1} \in U_\varphi$, sowie $v \circ (x \circ v^{-1} \circ x^{-1}) \in V_\varphi$.

Andererseits ist

$$v \circ x \circ v^{-1} \circ x^{-1} = \{x \circ (x^{-1} v^{-1})\} v = x(x^{-1})^{x_\varphi} \cdot (v^{x_\varphi})^{-1} v = (v^{x_\varphi})^{-1} v$$

und $U_\varphi \cap V_\varphi \subset C$. Damit ist gezeigt:

(I) Zu jedem $v \in V_\varphi$ und jedem $x \in F^*$ gibt es ein $c \in C$ mit $v^{x_\varphi} = cv$.

Es seien L eine Unterhalbgruppe von $F(+)$ mit $1 \in L \subset V$ und $v \in L$. Infolge (I) existieren zu jedem $x \in F^*$ Elemente $c, c' \in C$ mit $v^{x_\varphi} = cv$ und $(v + 1)^{x_\varphi} = c'(v + 1)$, d. h.

$$c'v + c' = v^{x_\varphi} + 1 = cv + 1, \quad \text{so daß} \quad (c' - c)v = 1 - c'.$$

Wenn v nicht in C enthalten ist, folgt $c = c' = 1$, insbesondere also $v^{x_\varphi} = v$. L ist demnach Teilmenge von $C \cup P_\varphi$.

Da C und P_φ Untergruppen von $F(+)$ sind, ist L notwendig in C oder in P_φ enthalten. Das beweist die Behauptung, da $V_\varphi \cap P_\varphi \subset Z_F$. |

Anmerkung: Mit Rücksicht auf (8.3) ist $H(+,\cdot)$ unter jeder der Bedingungen aus (8.4) kommutativ, die Inzidenzgruppe F^*/H^* von $(F(+,\circ), H(+,\circ))$ nach (6.2)a) also Pappossch.

Den Hilfssätzen (2.5)c) und (8.2) entnimmt man die Aussage

(8.5) *Wenn H ein Teilfastring von $F(+,\circ)$ mit $1 \in H$ ist, sind $P_\varphi(H)$ und $Q_\varphi(H)$ die einzig möglichen maximalen, in $K_F(H)$ enthaltenen Unterhalbgruppen von $F(\cdot)$.*

I.a. sind $K_F(H)$ und $P_\varphi(H)$ voneinander verschieden, wie jeder nichtkommutative Körper $H(+,\cdot) = F(+,\cdot)$ und die gekoppelte Abbildung $\varphi: a \to i_a$ demonstrieren: $F^\varphi(+,\cdot) = F(+,\circ)$ ist der zu $F(+,\cdot)$ duale Körper und $P_\varphi = Z_F \neq F$, während $K_F = F$.

Ebensowenig braucht $K_F(H) = Q_\varphi(H)$ zu gelten: Wenn $H(+,\cdot) = F(+,\cdot)$ ein nichtkommutativer Körper und φ die triviale Kopplung sind, gilt $F^\varphi(+,\cdot) = F(+,\circ)$ sowie $Q_\varphi = Z_F \neq K_F = F$.

Offen bleibt jedoch die Frage, ob immer einer der Fälle $K_F(H) = P_\varphi(H)$ oder $K_F(H) = Q_\varphi(H)$ eintritt. Unser nächstes Ziel ist der Nachweis, daß diese Vermutung unter geeigneten Voraussetzungen zumindest im Fall $H = F$ zutrifft. Ein erstes, für die Praxis allerdings wenig brauchbares Ergebnis ist

(8.6) *H sei ein Teilfastring von $F(+,\circ)$ mit $1 \in H$.*

a) *Es gilt genau dann $K_F(H) = P_\varphi(H)$ oder $K_F(H) = Q_\varphi(H)$, wenn $K_F(H)$ Unterhalbgruppe von $F(\cdot)$ ist.*

b) (Vgl. [36], Satz 41). *Es gilt genau dann* $K_F(H) = P_\varphi(H)$, *wenn* $(a+1)_\varphi|K_F(H) = a_\varphi|K_F(H)$ *für alle* $a \in H^*\backslash\{-1\}$.

c) *Es gilt genau dann* $K_F = P_\varphi$ *oder* $K_F = Q_\varphi$, *wenn* $K_F^{x_\varphi} = K_F$ *für alle* $x \in K_F^*$.

Beweis: a) folgt unmittelbar aus (2.5) und (8.5).

b) Nur eine der beiden Richtungen braucht bewiesen zu werden: Es gelte $(a+1)_\varphi|K_F(H) = a_\varphi|K_F(H)$ für alle $a \in H^*\backslash\{-1\}$. Dann gilt für beliebige $a \in H^*\backslash\{-1\}$ und $k \in K_F(H)$:
$(a+1)k^{a_\varphi} = (a+1)k^{(a+1)_\varphi} = (a+1) \circ k = a \circ k + k = ak^{a_\varphi} + k$, d. h. $k^{a_\varphi} = k$.

c) Wegen $xy = x \circ y^{x\bar{\varphi}^1}$ ist K_F genau dann Unterhalbgruppe von $F^*(\cdot)$, wenn $K_F^{x_\varphi} = K_F$ für alle $x \in K_F^*$. Das beweist mit Rücksicht auf Teil a) die Behauptung. |

Um für die Anwendungen handlichere Kriterien zu gewinnen, erweist es sich als vorteilhaft, die von U_φ und V_φ erzeugten Teilfastkörper $\langle U_\varphi\rangle$ und $\langle V_\varphi\rangle$ von $F(+,\circ)$ in die Betrachtungen einzubeziehen. $U_\varphi(K_F) \cup \{0\}$ und $V_\varphi(K_F) \cup \{0\}$ sind nach (2.4)d),e) Teilfastkörper von $F(+,\circ)$, die U_φ bzw. V_φ enthalten. Damit ist die folgende Bemerkung bestätigt:
Aus $\langle U_\varphi\rangle = F$ (bzw. $\langle V_\varphi\rangle = F$) folgt $K_F = P_\varphi$ (bzw. $K_F = Q_\varphi$).

Auf diese Feststellung ist (5.9) anwendbar und führt zu folgenden Aussagen:

(8.7) $F(+,\cdot,\circ) = (F, F^\varphi)$ *sei ein D-Fastkörperpaar, und* $F(+,\circ)$ *sei kein Körper.*

a) *Es gilt* $K_F = P_\varphi$ *(bzw.* $K_F = Q_\varphi$*), wenn* φ *ein gekoppelter Homomorphismus oder Antihomomorphismus (bzw. ein gekoppelter d-Homomorphismus oder d-Antihomomorphismus) ist.*

b) *Es gilt* $K_F = P_\varphi$ *(bzw.* $K_F = Q_\varphi$*), wenn* $|\Gamma_\varphi| < |F|$ *(bzw.* $|F^*/V_\varphi| < |F|$*).*

c) *Es gilt* $K_F = P_\varphi$ *oder* $K_F = Q_\varphi$, *wenn* Γ_φ *(bzw.* $(F^*/V_\varphi)(\circ)$*) abelsch ist.*

d) *Es gilt* $K_F = P_\varphi$, *wenn* $F(+,\cdot)$ *über* P_φ *links-algebraisch ist und* Γ_φ *nur äußere Automorphismen von* $F(+,\cdot)$ *enthält.*

Beweis: Offenbar sind nur die Punkte c) und d) zu verifizieren.

c) Nach (5.9)b), der Bemerkung vor diesem Satz und dem Hilfssatz 1 aus [60] (§ 1) gilt $K_F = P_\varphi$ oder $K_F = Z_F$. Das beweist die Behauptung, wenn man (8.9) (s. u.) beachtet.

Dem Beweis von d) schicken wir einen weiteren Hilfssatz voraus:

Hs. 4: *Es seien* H *eine Untergruppe von* $F(+)$ *mit* $1 \in H, k \in K_F(H)$ *und* L *ein Teilkörper von* $F(+,\cdot)$ *mit* $k^{a_\varphi} \in L$ *für alle* $a \in H^*$. *Dann gilt* $H \subset L$ *oder* $k \in P_\varphi(H)$.

Insbesondere wird F von $\{k^{x_\varphi} | x \in F^*\}$ als Fastkörper erzeugt, wenn $k \in K_F \setminus P_\varphi$.

Beweis: Für jedes $a \in H^* \setminus \{-1\}$ ist

$$(a+1)k^{(a+1)_\varphi} = (a+1) \circ k = a \circ k + k = ak^{a_\varphi} + k, \quad \text{d. h.}$$

$$a(k^{(a+1)_\varphi} - k^{a_\varphi}) = k - k^{(a+1)_\varphi}.$$

Daher gilt $a \in L$ oder $k = k^{a_\varphi} = k^{(a+1)_\varphi}$.

Die Behauptung „$H \subset L$ oder $k \in P_\varphi(H)$" folgt damit aus der leicht zu bestätigenden Tatsache, daß $\{a \in H^* | k^{a_\varphi} = k\} \cup \{0\}$ eine Untergruppe von $F(+)$ ist. |

Beweis von (8.7)d):

Nach [24] (Prop. 1 (3) auf Seite 166) kann jede endliche Teilmenge von F in einen über P_φ (links-)endlich-dimensionalen Teilkörper L von $F(+,\cdot)$ eingebettet werden, der galoissch über P_φ ist und der Bedingung $L^\gamma \subset L$ für alle $\gamma \in \Gamma_\varphi$ genügt. Wenn die Dimension von $F(+,\cdot)$ über $P_\varphi(+,\cdot)$ unendlich ist, ist K_F also nach dem Hilfssatz 4 – man setze dort $H = F$ – in P_φ enthalten.

Im Fall $[F : P_\varphi]_l < \infty$ ist $|\Gamma_\varphi| < |F|$ nach [24] (Prop. 1(2) auf S. 166); die Behauptung folgt daher aus Teil b). |

Auch die Frage, ob das Zentrum Z_F von $F(+,\circ)$ immer in einem der beiden Körper P_φ oder Q_φ liegt, ist noch offen. Die Antwort ist allerdings dann positiv, wenn Z_F ein Teilkörper von $F(+,\circ)$ ist. Ausgangspunkt ist der

Hs. 5: *Es seien B eine Unterhalbgruppe von $F(\cdot)$ und a ein Element aus $F \setminus \{0, -1\}$. Wenn a und $a+1$ in $Z_F(B)$ enthalten sind, liegen a und $a+1$ in $P_\varphi(B) \cap V_\varphi(B)$ oder in $Q_\varphi(B) \cap U_\varphi(B)$.*

Beweis: Für jedes $x \in B$ gilt $(a+1) \circ x = x \circ (a+1) = a \circ x + x$, so daß a und $a+1$ nach dem Hs. 2 in $U_\varphi(B)$ oder in $V_\varphi(B)$ enthalten sind. Es folgt $x \circ a = a \circ x = ax$ oder $x \circ a = a \circ x = xa$, d. h. $a \in Q_\varphi(B)$ oder $a \in P_\varphi(B)$. Entsprechendes gilt für $a+1$. |

Wegen $P_\varphi(B) \cap V_\varphi(B) = (P_\varphi(B) \cap Z_F(B))^*$ und $Q_\varphi(B) \cap U_\varphi(B) = (Q_\varphi(B) \cap Z_F(B))^*$ besitzt der Hs. 5 das Korollar

(8.8) *B sei eine Unterhalbgruppe von $F(\cdot)$. Dann liegt jede in $Z_F(B)$ enthaltene Unterhalbgruppe A von $F(+)$ mit $1 \in A$ in $P_\varphi(B) \cap Z_F(B)$ oder in $Q_\varphi(B) \cap Z_F(B)$, d. h. $P_\varphi(B) \cap Z_F(B)$ und $Q_\varphi(B) \cap Z_F(B)$ sind die einzig möglichen maximalen, in $Z_F(B)$ liegenden Unterhalbgruppen von $F(+)$, die 1 enthalten.*

Insbesondere folgt

(8.9) *B sei eine Unterhalbgruppe von $F(\cdot)$. Wenn $Z_F(B)$ ein Teilfastkörper von $F(+,\circ)$ ist, gilt $Z_F(B) \subset P_\varphi(B)$ oder $Z_F(B) \subset Q_\varphi(B)$.*

Eine weitere Information über den Zusammenhang zwischen Zentrum und Kern eines D-Fastkörpers enthält

(8.10) *$F(+,\cdot,\circ) = (F, F^\varphi)$ sei ein D-Fastkörperpaar mit $|\Gamma_\varphi| < |K_F|$, und $F(\cdot)$ sei kommutativ. Dann wird $K_F(+,\cdot)$ von Z_F als Körper erzeugt.*

Beweis: Es ist $|K_F^*/(K_F^* \cap U_\varphi)| = |(U_\varphi \circ K_F^*)/U_\varphi| \leqslant |F^*/U_\varphi| = |\Gamma_\varphi| < |K_F|$. Andererseits liegt $K_F^* \cap U_\varphi$ in Z_F; denn es gilt $K_F = P_\varphi$ nach (8.7)b), so daß $a \circ x = ax = xa = x \circ a$ für beliebige $a \in P_\varphi \cap U_\varphi$ und $x \in F$. Es folgt $(*)$: $|K_F^*/Z_F^*| < |K_F|$.

Wir dürfen annehmen, daß K_F unendlich ist, weil andernfalls Γ_φ und damit auch F endlich wären, denn $[F : K_F] = [F : P_\varphi] = |\Gamma_\varphi|$; und dieser Fall ist in (3.3) beantwortet.

Wenn K_F unendlich ist, folgt aus $(*)$ offenbar $|Z_F| = |K_F|$, so daß $(**)$: $|K_F^*/Z_F^*| < |Z_F|$.

Zu jedem $k \in K_F \backslash Z_F$ existieren daher Elemente $z_1, z_2 \in Z_F$ mit $z_1 \neq z_2$ und $(k + z_1)Z_F^* = (k + z_2)Z_F^*$, so daß $k + z_1 = (k + z_2)z_3$ mit $z_3 \in Z_F$. Offenbar ist z_3 von 1 verschieden, und es folgt $k = (1 - z_3)^{-1}(z_2 z_3 - z_1)$. |

Anmerkung: Im allgemeinen wird K_F auch in einem echten D-Fastkörper nicht von Z_F erzeugt. Man vergleiche dazu etwa das Beispiel (Folgerung b)) im Teil C von § 9.

Den Abschluß bilden zwei einfache Bemerkungen über Beziehungen zwischen P_φ und Q_φ einerseits sowie U_φ und V_φ andererseits.

(8.11) *Wenn P_φ und Q_φ elementweise bezüglich der Operation $\cdot$ vertauschbar sind, gilt $P_\varphi \subset Q_\varphi$ oder $Q_\varphi \subset P_\varphi$.*

Beweis: Angenommen es existieren Elemente $a \in P_\varphi \backslash Q_\varphi$ und $b \in Q_\varphi \backslash P_\varphi$. Dann entsteht wegen $a, b, ab = ba = b \circ a \in K_F$ nach (8.1) der Widerspruch $a \in Q_\varphi$ oder $b \in P_\varphi$. |

(8.12) a) *Wenn U_φ und V_φ Normalteiler von $F^*(\cdot)$ sind, gilt $U_\varphi \subset V_\varphi$ oder $V_\varphi \subset U_\varphi$.*

b) *Wenn U_φ (bzw. V_φ) ein auflösbarer Normalteiler von $F^*(\cdot)$ ist, liegt U_φ (bzw. V_φ) in C, d. h. $U_\varphi \subset V_\varphi$ (bzw. $V_\varphi \subset U_\varphi$).*

Beweis: a) $U_\varphi \cap V_\varphi$ ist im Zentrum C von $F(+,\cdot)$ enthalten; denn für jedes $a \in U_\varphi \cap V_\varphi$ und alle $x \in F^*$ gilt $ax = a \circ x = xa$. Nach [51] (14.4.5) ist daher U_φ oder V_φ Teilmenge von C; und das zieht offenbar die Behauptung nach sich.

b) folgt aus [51] (14.4.4). |

Anmerkung: Im allgemeinen gilt weder $U_\varphi \subset V_\varphi$ noch $V_\varphi \subset U_\varphi$. Man vergleiche dazu wieder das Beispiel (Folgerung c)) im Teil C von § 9.

§ 9. Fastkörperkonstruktionen

A) Fastkörperpaar-Erweiterungen

F. Pokropp führte in [47] den folgenden Begriff ein:

Definition 1: Das Fastkörperpaar $F(+,\cdot,\circ) = (F,F^\psi)$ wird eine *Erweiterung* des Fastkörperpaars $H(+,\cdot,\circ) = (H,H^\varphi)$ genannt, wenn $H(+,\cdot,\circ)$ eine Unterstruktur von $F(+,\cdot,\circ)$ ist. Diese Erweiterung heißt *Dicksonsch*, wenn $F(+,\cdot)$ ein Körper ist *(D-Erweiterung)*.

Definition 2: Man nennt eine D-Erweiterung $F(+,\cdot,\circ)$ von $H(+,\cdot,\circ)$ *algebraisch, transzendent, galoissch, abelsch,...*, wenn $F(+,\cdot)$ über H algebraisch, transzendent, galoissch, abelsch,... ist.

Wir notieren zwei einfache Eigenschaften:

Wenn (F,F^ψ) eine Erweiterung von (H,H^φ) ist, gilt:

a) Für jedes $x \in H^*$ ist $x_\psi|H = x_\varphi$.

b) $\Gamma_\varphi \cong (H^*)_\psi/N$, wobei $(H^*)_\psi = \{a_\psi | a \in H^*\}$ und $N = \{\gamma \in (H^*)_\psi | \gamma|H = 1_H\}$.

b) folgt aus der Bemerkung, daß $\tau: \begin{cases} (H^*)_\psi \to \Gamma_\varphi \\ x_\psi \to x_\varphi \end{cases}$ ein Homomorphismus von $(H^*)_\psi$ auf Γ_φ mit dem Kern N ist.

In Anbetracht der Aussage a) nennt man ψ eine *Fortsetzung* von φ auf $F(+,\cdot)$ und φ die *Restriktion* von ψ auf $H(+,\cdot)$.

In diesem Abschnitt steht die folgende Problemstellung im Mittelpunkt: Es seien $H(+,\cdot,\circ) = (H,H^\varphi)$ ein Fastkörperpaar und $H(+,\cdot)$ Teilfastkörper eines Fastkörpers $F(+,\cdot)$. Gibt es – unter geeigneten Voraussetzungen – Methoden, φ auf $F(+,\cdot)$ fortzusetzen?

Wir beginnen mit einem – leicht verallgemeinerten – Verfahren, das F. Pokropp in [47] mit Erfolg zur Konstruktion neuer Fastkörper benutzte.

(9.1) *Es seien $H(+,\cdot,\circ) = (H,H^\varphi)$ ein Fastkörperpaar, $H(+,\cdot)$ ein Teilfastkörper von $F(+,\cdot)$ und τ sowie $\varkappa$ Homomorphismen von $F^*(\cdot)$ in $H^*(\cdot)$ bzw. von Γ_φ in $A(F,+,\cdot)$, die der Bedingung*

$$(*)\ \tau\gamma = \gamma^{\varkappa}\tau|F^* \quad \text{für alle} \quad \gamma \in \Gamma_\varphi$$

$$\begin{array}{ccc} F^* & \xrightarrow{\psi} & A(F,+,\cdot) \\ \downarrow{\scriptstyle \tau} & & \uparrow{\scriptstyle \varkappa} \\ H^* & \xrightarrow{\varphi} & \Gamma_\varphi \end{array}$$

genügen.

Dann ist $\psi := \tau\varphi\varkappa$ *eine gekoppelte Abbildung von* $F(+,\cdot)$. *Mit* φ *ist auch* ψ *ein gekoppelter Homomorphismus (bzw. Antihomomorphismus). Wenn außerdem* $(**)\colon \tau|H^* = 1_{H^*}$ *und* $(***)\colon \gamma^{\varkappa}|H = \gamma$ *für alle* $\gamma \in \Gamma_\varphi$ *erfüllt sind, ist* (F,F^{ψ}) *eine Erweiterung von* (H,H^{φ}).

1. Beispiel: Es seien $H(\cdot)$ kommutativ, $F = H$ und $\varkappa$ die Injektion $\gamma \to \gamma$ von Γ_φ in $A(H,+,\cdot)$. Dann erfüllt der Homomorphismus $\tau_n\colon x \to x^n$ von $H^*(\cdot)$ in $H^*(\cdot)$ die Bedingung $(*)$ für jedes $n \in \mathbb{Z}$. Daher ist $\psi_n\colon \begin{cases} H^* \to A(H,+,\cdot) \\ x \to (x^n)_\varphi \end{cases}$ eine gekoppelte Abbildung von $H(+,\cdot)$.

2. Beispiel: (Vgl. [47], § 5). *Einfach-transzendente Erweiterungen.* $H(+,\cdot,\circ) = (H,H^{\varphi})$ sei ein Fastkörperpaar mit kommutativer Verknüpfung $\cdot$, und $F(+,\cdot) = (H(t))(+,\cdot)$ eine transzendente Erweiterung von $H(+,\cdot)$. Jeder Automorphismus γ von $H(+,\cdot)$ kann aufgrund der Vorschrift $\begin{cases} H[t] \to H[t] \\ \sum\limits_{i\in\mathbb{N}} a_i t^i \to \sum\limits_{i\in\mathbb{N}} a_i^{\gamma} t^i \end{cases}$ eindeutig zu einem Automorphismus $\bar{\gamma}$ von $F(+,\cdot)$ fortgesetzt werden.

Jedes Element $f \neq 0$ aus F läßt sich in der Form

$$f = \left(\sum_{i=m}^{r} a_i t^i\right)\left(\sum_{j=n}^{s} b_j t^j\right)^{-1} \quad \text{mit} \quad a_m, a_r, b_n, b_s \neq 0$$

schreiben. Durch

$$\tau\colon f \to a_r b_s^{-1} \quad \text{sowie} \quad \tau'\colon f \to a_m b_n^{-1}$$

werden zwei Homomorphismen τ,τ' von $F^*(\cdot)$ in $H^*(\cdot)$ erklärt, die zusammen mit der Abbildung $\varkappa\colon \gamma \to \bar{\gamma}$ von Γ_φ in $A(F,+,\cdot)$ die Bedingungen $(*)$, $(**)$ und $(***)$ aus (9.1) erfüllen. Daher sind

$$\psi\colon \begin{cases} F^* \to A(F,+,\cdot) \\ f \to \overline{(f^{\tau})_\varphi} \end{cases} \quad \text{und} \quad \psi'\colon \begin{cases} F^* \to A(F,+,\cdot) \\ f \to \overline{(f^{\tau'})_\varphi} \end{cases}$$

gekoppelte Abbildungen von $F(+,\cdot)$, die φ fortsetzen.

3. Beispiel: (Vgl. [47], § 6). *Körper der formalen Potenzreihen.* Es sei $H(+,\cdot,\circ) = (H,H^{\varphi})$ ein Fastkörperpaar mit kommutativer Verknüpfung $\cdot$,

und $F(+,\cdot) = H^{(t)}(+,\cdot)$ bezeichne den (kommutativen) Körper der in t formalen Potenzreihen:

$$F = H^{(t)} = \left\{ \sum_{i\in\mathbb{Z}} a_i t^i \mid a_i \in H \quad \text{für alle} \quad i\in\mathbb{Z}; a_i = 0 \quad \text{für fast alle} \quad i < 0 \right\}$$

mit

$$\left(\sum_{\mathbb{Z}} a_i t^i\right) + \left(\sum_{\mathbb{Z}} b_i t^i\right) = \sum_{\mathbb{Z}} (a_i + b_i)\, t^i$$

und

$$\left(\sum_{\mathbb{Z}} a_i t^i\right)\cdot\left(\sum_{\mathbb{Z}} b_j t^j\right) = \sum_{\mathbb{Z}} c_k t^k, \quad \text{wobei} \quad c_k = \sum_{i+j=k} a_i b_j .$$

$r\in\mathbb{Z}$ heißt die *Ordnung* des Elements $f = \sum_{\mathbb{Z}} a_i t^i \neq 0$ aus F, wenn $a_r \neq 0$ und $a_i = 0$ für alle $i < r$, i. Z. $r = |f|$.

Durch $\tau: \begin{cases} F^* \to H^* \\ f = \sum_{\mathbb{Z}} a_i t^i \to a_{|f|} \end{cases}$ wird ein Homomorphismus τ von $F^*(\cdot)$ auf $H^*(\cdot)$ eingeführt, der auf H^* die Identität ist. Jeder Automorphismus γ von $H(+,\cdot)$ kann gemäß $\left(\sum_{\mathbb{Z}} a_i t^i\right)^{\bar\gamma} = \sum_{\mathbb{Z}} a_i^{\gamma} t^i$ zu einem Automorphismus $\bar\gamma$ von $F(+,\cdot)$ fortgesetzt werden. τ und $\varkappa: \begin{cases} \Gamma_\varphi \to A(F,+,\cdot) \\ \gamma \to \bar\gamma \end{cases}$ erfüllen die Bedingungen (*), (**) und (***) aus (9.1), d. h. $\psi: \begin{cases} F^* \to A(F,+,\cdot) \\ x \to \overline{(x^\tau)_\varphi} \end{cases}$ ist eine gekoppelte Abbildung von $F(+,\cdot)$, die φ fortsetzt.

4. Beispiel: (Vgl. [47], § 7). *Galoissche Erweiterung.* Es seien $H(+,\cdot,\circ) = (H, H^\varphi)$ ein Fastkörperpaar mit kommutativer Verknüpfung $\cdot$ und $F(+,\cdot)$ eine endliche galoissche, kommutative Körpererweiterung von $H(+,\cdot)$ vom Grad n. $\varkappa: \gamma \to \bar\gamma$ sei ein Homomorphismus von Γ_φ in $A(F,+,\cdot)$ mit den Eigenschaften:

(A) $\bar\gamma | H = \gamma$ für alle $\gamma\in\Gamma_\varphi$

(B) $(\Gamma_\varphi)^\varkappa$ und die Galoisgruppe $\mathfrak{G}(F/H)$ von $F(+,\cdot)$ über H sind elementweise vertauschbar, d. h. $\bar\gamma\sigma = \sigma\bar\gamma$ für alle $\gamma\in\Gamma_\varphi$ und $\sigma\in\mathfrak{G}(F/H)$.

Dann erfüllt der Homomorphismus $\tau = N: x \to \prod_{\sigma\in\mathfrak{G}(F/H)} x^\sigma$ von $F^*(\cdot)$ in $H^*(\cdot)$ zusammen mit $\varkappa$ die Bedingung (*) aus (9.1), so daß $\psi: \begin{cases} F^* \to A(F,+,\cdot) \\ x \to \overline{(x^\tau)_\varphi} \end{cases}$ eine gekoppelte Abbildung von $F(+,\cdot)$ ist. Gilt außerdem

(C) „Jedes Polynom der Form $t^n - a \in H[t]$ besitzt genau eine Nullstelle $\sqrt[n]{a}$ in H“,

so ist $\tau': \begin{cases} F^* \to H^* \\ x \to \sqrt[n]{x^\tau} \end{cases}$ ein Homomorphismus mit den Eigenschaften (*), (**)

und (***). Daher ist $\psi: \begin{cases} F^* \to A(F, +, \cdot) \\ x \to (x^\tau)_\varphi \end{cases}$ eine Fortsetzung von φ auf $F(+, \cdot)$.

In [47] (§ 7) wurde untersucht, wann die Voraussetzungen erfüllt sind.

B) Dickson-Gruppen aus inneren Automorphismen

Wenn ein nicht-kommutativer Körper gegeben ist, liegt der Versuch nahe, gekoppelte Abbildungen mit Hilfe seiner inneren Automorphismen zu konstruieren. In diesem Abschnitt werden zwei Methoden beschrieben.

(9.2) *Es seien $F(+, \cdot)$ ein Körper und τ ein Homomorphismus von $F^*(\cdot)$ in sich derart, daß $(F^*)^{\tau^2}$ im Zentrum von $(F^*)^\tau$ enthalten ist. Dann sind*

$$\varphi: \begin{cases} F^* \to A(F, +, \cdot) \\ x \to i_{(x^\tau)^{-1}} \end{cases} \quad \textit{ein gekoppelter Antihomomorphismus}$$

und

$$\psi: \begin{cases} F^* \to A(F, +, \cdot) \\ x \to i_{x^\tau x} \end{cases} \quad \textit{ein gekoppelter d-Antihomomorphismus}$$

von $F(+, \cdot)$.

Wenn $C_F(A)$ den Zentralisator von $A \subset F$ in $F(\cdot)$ bezeichnet und $C_F(F) = C$ gesetzt wird, folgt:

$$U_\varphi = (C^*)^{\tau^{-1}}, V_\varphi = \{a \in F^* | a^\tau \in C^* \cdot a^{-1}\}, K_F = P_\varphi = C_F(F^{*\tau})$$

sowie

$$Q_\varphi = C_F(\{x x^\tau | x \in F^*\}),$$

wie man sich leicht überzeugt.

Die an τ gestellte Forderung ist sicherlich dann erfüllt, wenn $(F^*)^\tau$ in einem kommutativen Teilkörper von $F(+, \cdot)$ enthalten ist.

Nichttriviale Beispiele für die in (9.2) beschriebene Konstruktionsmethode liefern die *Kalscheuerschen Fastkörper* [25]: Zugrunde gelegt sei der Körper $\mathbb{H}(+, \cdot)$ der Quaternionen über $\mathbb{R}(+, \cdot)$. Für jedes $c \in \mathbb{R}^*$ ist $\tau_c: \begin{cases} \mathbb{H}^* \to \mathbb{H} \\ x \to e^{-ic \log N(x)}, \end{cases}$ (mit $N(x)$ = Norm von x) ein Homomorphismus von $\mathbb{H}^*(\cdot)$ in $\mathbb{C}^*(\cdot)$, der die Voraussetzungen aus (9.2) erfüllt. Daher ist

$$\varphi_c: \begin{cases} \mathbb{H}^* \to A(\mathbb{H}, +, \cdot) \\ x \to i_{(x^{\tau_c})^{-1}} \end{cases}$$

ein gekoppelter Antihomomorphismus (und Homomorphismus) von $\mathbb{H}(+, \cdot)$. Speziell im Fall $c = 1$ – wir schreiben φ statt φ_1 – gilt:

$$K_{\mathbb{H}} = P_\varphi = \mathbb{C}, Q_\varphi = \mathbb{R}, U_\varphi = \{a \in \mathbb{H}^* | N(a) = e^{k\pi} \quad \text{mit} \quad k \in \mathbb{Z}\}$$

sowie

$$Z_{\mathbb{H}}^* = V_\varphi = \{r \cdot e^{-i \log|r|} | r \in \mathbb{R}^*\}.$$

Wir notieren außerdem die folgenden Eigenschaften:

a) Es gilt weder $V_\varphi \subset U_\varphi$ noch $U_\varphi \subset V_\varphi$.

b) Es gilt weder $Z_{\mathbb{H}} \subset C$ noch $C \subset Z_{\mathbb{H}}$ [26]).

c) V_φ ist kein Normalteiler von $\mathbb{H}^*(\cdot)$.

d) $\mathbb{H}(+,\circ)$ besitzt keinen invarianten Teilfastkörper, weil $\mathbb{Q} \not\subset Z_{\mathbb{H}}$. Selbst 2 ist kein Zentrumselement.

(9.3) *Es seien $F(+,\cdot)$ ein Körper und τ ein idempotenter Homomorphismus von $F^*(\cdot)$ in sich. Dann sind*

$$\varphi: \begin{cases} F^* \to A(F,+,\cdot) \\ x \to i_{x^\tau} \end{cases} \quad \textit{ein gekoppelter Homomorphismus}$$

und

$$\psi: \begin{cases} F \to A(F,+,\cdot) \\ x \to i_{(x^\tau)^{-1}x} \end{cases} \quad \textit{ein gekoppelter d-Homomorphismus von } F(+,\cdot).$$

Wir illustrieren dieses Verfahren an dem folgenden

Beispiel: Ausgangspunkt ist wieder der Körper $F(+,\cdot) = H^{(t)}(+,\cdot)$ der in t formalen Potenzreihen über dem kommutativen Körper $H(+,\cdot)$. (Man vgl. das 3. Beispiel im Teil A.)

Wenn π ein Automorphismus von $H(+,\cdot)$ ist, kann F nach D. Hilbert (vgl. etwa [7]) durch die Vorschrift

$$\left(\sum_{\mathbb{Z}} a_i t^i\right) * \left(\sum_{\mathbb{Z}} b_j t^j\right) = \sum_{\mathbb{Z}} c_k t^k \quad \text{mit} \quad c_k = \sum_{i+j=k} a_i b_j^{\pi^i}$$

zu einem Körper $F(+,*)$ gemacht werden. Er ist genau dann kommutativ, wenn $\pi = 1_H$.

Die Abbildung

$$\tau: \begin{cases} F^* \to F^* \\ f = \sum_{i \in \mathbb{Z}} a_i t^i \to a_{|f|} t^{|f|} \end{cases}$$

ist ein idempotenter Homomorphismus von $F^*(*)$ in sich. Daher ist

$$\varphi: \begin{cases} F^* \to A(F,+,*) \\ f \to i_{f^\tau} \end{cases}$$

---

[26]) Dabei bedeuten $C_F(A)$ wieder den Zentralisator von $A \subset F$ in $F(+,\cdot)$ und $C = C_F(F)$ das Zentrum von $F(+,\cdot)$.

ein gekoppelter Homomorphismus von $F(+,*)$. (i_{f^τ} bezeichnet dabei den von f^τ erzeugten inneren Automorphismus von $F(+,*)$.) Wenn $F(+,\circ)$ die φ-Ableitung von $F(+,*)$ bezeichnet, gilt für $f=\sum_{i\in\mathbb{Z}} a_i t^i \in F^*$ und $g=\sum_{j\in\mathbb{Z}} b_j t^j \in F$ wegen $(a_{|f|}t^{|f|})^{-1}=(a_{|f|}^{-1})^{\pi^{-|f|}}t^{-|f|}$:

$$f\circ g=\left(\sum_{i\in\mathbb{Z}} a_i t^i\right)*(a_{|f|}t^{|f|})^{-1}*\left(\sum_{j\in\mathbb{Z}} b_j t^j\right)*(a_{|f|}t^{|f|})=\sum_{k\in\mathbb{Z}} c_k t^k$$

mit

$$c_k=\sum_{i+j=k}\{(a_i b_j^{\pi^{i-|f|}})\cdot(a_{|f|}^{\pi^j}\cdot a_{|f|}^{-1})^{\pi^{i-|f|}}\}.$$

C) Ein weiteres Beispiel und einige Folgerungen

(Vgl. [47], § 6).

Es bedeuten wie im letzten Beispiel des Teils (B) $H(+,\cdot)$ einen kommutativen Körper, $F(+,\cdot)=H^{(t)}(+,\cdot)$ den Körper der formalen Potenzreihen über H und $F(+,*)$ den mit Hilfe eines Automorphismus π von $H(+,\cdot)$ aus $F(+,\cdot)$ gewonnenen Körper.

Schließlich bezeichne τ einen Automorphismus von $F(+,*)$ mit der Eigenschaft

$$(*)\qquad |f^\tau|=|f| \quad \text{für alle} \quad f\in F^*.$$

Dann ist $\varphi:\begin{cases}F^*\to A(F,+,*)\\ f\to\tau^{|f|}\end{cases}$ ein gekoppelter Homomorphismus von $F(+,*)$; φ ist nämlich wegen

$$(**)\qquad |f*g|=|f|+|g| \quad \text{für alle} \quad f,g\in F^*$$

ein (Anti-)Homomorphismus von $F^*(*)$ in $A(F,+,*)$, und es gilt

$$(f^{g_\varphi})_\varphi=(f^{\tau^{|g|}})_\varphi=\tau^{|f^{\tau^{|g|}}|}=\tau^{|f|}=f_\varphi \quad \text{für alle} \quad f,g\in F^*,$$

so daß (2.9)b) anwendbar ist.

Infolge (**) hat offenbar jeder innere Automorphismus von $F(+,*)$ die Eigenschaft (*). Außerdem gewinnt man aus jedem mit π vertauschbaren Automorphismus τ_0 von $H(+,\cdot)$ durch die Erweiterungsvorschrift

$$\tau=\overline{\tau_0}:\begin{cases}F^*\to A(F,+,*)\\ \sum_{i\in\mathbb{Z}} a_i t^i\to\sum_{i\in\mathbb{Z}} a_i^{\tau_0} t^i\end{cases}$$ einen Automorphismus τ von $F(+,*)$ mit der gewünschten Eigenschaft (*) (Man vgl. dazu [47] (§ 6)).

Wir wollen anhand dieser letzten Methode mehrere Folgerungen ziehen und stellen zu dem Zweck einige leicht nachzuprüfende Eigenschaften zusammen. Dabei bezeichnen τ_0 einen mit π vertauschbaren Automorphismus von $H(+,\cdot)$, τ den Automorphismus $\overline{\tau_0}$ von $F(+,*)$, L den [illegible]körper

von τ_0, M den Fixkörper von π, C das Zentrum von $F(+,\cdot)$ und $|\tau_0|, |\pi|, |\tau_0\pi|$ die Ordnungen der Automorphismen $\tau_0, \pi, \tau_0\pi$.

(I) $K_F = P_\varphi = \left\{ \sum_{i\in\mathbb{Z}} a_i t^i \in F | a_i \in L \quad \text{für alle} \quad i \in \mathbb{Z} \right\} = L^{(t)}$

(II) $U_\varphi = \{ f \in F^* | \, |\tau_0| \, | \, |f| \}$

(III) $V_\varphi = \left\{ \sum_{i=0}^{\infty} a_i t^{k\cdot|\tau_0\pi|+i\cdot|\pi|} \in F | k \in \mathbb{Z}; a_i \in M \quad \text{für alle} \quad i \geqslant 0; a_0 \neq 0 \right\}$.

(IV) $C = \left\{ \sum_{i\in\mathbb{Z}} a_i t^{i\cdot|\pi|} \in F | a_i \in M \quad \text{für alle} \quad i \in \mathbb{Z} \right\} = M^{(t^{|\pi|})}$

(V) $Q_\varphi = \left\{ \sum_{i\in\mathbb{Z}} a_i t^{i|\pi|} \in F | a_i \in M \cap L \quad \text{für alle} \quad i \in \mathbb{Z} \right\} = (M \cap L)^{(t^{|\pi|})} =$
$= P_\varphi \cap C$

(VI) $Z_F^* = \left\{ \sum_{i=0}^{\infty} a_i t^{k\cdot|\tau_0\pi|+i\cdot|\pi|} \in F | k \in \mathbb{Z}; a_i \in L \cap M \quad \text{für alle} \right.$
$\left. i \geqslant 0; a_0 \neq 0 \right\} = P_\varphi \cap V_\varphi$

Folgerungen

a) Z_F ist. i. a. nicht in C enthalten.

(Man wähle $H(+,\cdot)$, π und τ_0 so, daß $|\pi| \nmid |\tau_0\pi|$; z. B. $\tau_0 = \pi^{-1} \neq 1_H$.)

b) Z_F kann auch dann ein echter Teilkörper von $K_F(+,\circ)$ sein, wenn $K_F(+,\circ)$ kommutativ ist.

(Wähle $H(+,\cdot)$ und $\pi = \tau_0$ mit $|\pi| = 0$.)

c) I.a. gilt weder $V_\varphi \subset C$ noch $U_\varphi \subset C$, d. h. weder $V_\varphi \subset U_\varphi$ noch $U_\varphi \subset V_\varphi$.

(Man wähle $H(+,\cdot)$, π und τ_0 derart, daß $|\pi| \nmid |\tau_0\pi|$.)

d) Auch ein in $(U_\varphi \cap V_\varphi) \cup \{0\} \subset C$ enthaltener Teilkörper von $F(+,\circ)$ ist i. a. nicht invariant.

(Wähle $H(+,\cdot)$, π und τ_0 derart, daß $M^{\tau_0} \not\subset M$. Dann ist M^* in $U_\varphi \cap V_\varphi$ enthalten, aber kein Normalteiler von $F^*(\circ)$.)

e) Ein in $(U_\varphi \cap K_F) \cup \{0\}$ liegender (kommutativer) Teilkörper von $F(+,\circ)$ ist i.a. nicht invariant.

(Man wähle $H(+,\cdot)$, π und τ_0 so, daß $L^\pi \not\subset L$ (oder $L \not\subset M$). Dann ist L^* in $U_\varphi \cap K_F$ enthalten, aber kein Normalteiler von $F^*(\circ)$.)

f) V_φ (bzw. U_φ) ist i. a. kein Normalteiler von $F^*(*)$.

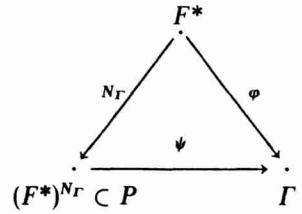
(Wähle $H(+,\cdot)$, $\tau_0 = \pi^{-1} \neq 1_H$. Dann ist t Element von V_φ; $b * t * b^{-1} = b(b^{-1})^\pi t$ ist für $b \in H^*$ aber genau dann in V_φ enthalten, wenn $b(b^{-1})^\pi \in M$, d. h. $(b(b^{-1})^\pi)^\pi = b(b^{-1})^\pi$, d. h. wenn $(b^\pi)^2 = b^{\pi^2} \cdot b$. Aus $V_\varphi \lhd F^*(*)$ folgte also $(b^\pi)^2 = b^{\pi^2} \cdot b$ und $\{(b+1)^\pi\}^2 = (b^\pi)^2 + 2b^\pi + 1 = (b+1)^{\pi^2} \cdot (b+1) = bb^{\pi^2} + b^{\pi^2} + b + 1 = (b^\pi)^2 + (b^\pi)^2 b^{-1} + b + 1$, d. h. $2bb^\pi = (b^\pi)^2 + b^2$, so daß $b^\pi = b$ für alle $b \neq 0,1$ aus H im Widerspruch zu $\pi \neq 1_H$.)

g) Ein Teilkörper von $F(+,*)$ ist i. a. kein Teilfastkörper von $F(+,\circ)$. (Man wähle $H(+,\cdot), \pi, \tau_0$ und einen Teilkörper E_0 von $H(+,\cdot)$ derart, daß $E_0^{\pi} = E_0$, aber $E_0^{\tau_0} \not\subset E_0$. Dann ist $E := E_0^{\langle t \rangle}$ ein Teilkörper von $F(+,*)$, aber kein Teilfastkörper von $F(+,\circ)$.)

D) Gekoppelte Homomorphismen mit zyklischen D-Gruppen

Jedem Dicksonschen Fastkörperpaar $F(+,\cdot,\circ) = (F, F^{\varphi})$ entspricht die galoissche Körpererweiterung $F(+,\cdot)/P_{\varphi}(+,\cdot)$. Naturgemäß erhebt sich die folgende Frage: Unter welchen Voraussetzungen gibt es zu einer galoisschen Körpererweiterung $F(+,\cdot)/P(+,\cdot)$ eine gekoppelte Abbildung φ von $F(+,\cdot)$, deren Fixkörper P_{φ} mit P übereinstimmt? H. Karzel hat sie in [31] (4) für den Fall beantwortet, daß $F(+,\cdot)$ kommutativ und $F(+,\cdot)/P(+,\cdot)$ von Primzahlrang ist. Wir fassen seine Ergebnisse in abgewandelter und verallgemeinerter Form zusammen.

(9.4) a) *Es seien $F(+,\cdot)$ ein kommutativer Körper, Γ eine endliche Automorphismengruppe von $F(+,\cdot)$ mit dem Fixkörper P, $N_{\Gamma}: \begin{cases} F^* \to P^* \\ x \to \prod\limits_{\gamma \in \Gamma} x^{\gamma} \end{cases}$ die Norm von $F(+,\cdot)/P(+,\cdot)$ und ψ ein Homomorphismus von $(F^*)^{N_{\Gamma}}$ in Γ.*
Dann ist $\varphi := N_{\Gamma}\psi$ ein gekoppelter Homomorphismus von $F(+,\cdot)$ mit $P \subset P_{\varphi}, \Gamma_{\varphi} \subset \Gamma$ und Kern $N_{\Gamma} \subset U_{\varphi}$.



b) *Es sei φ eine gekoppelte Abbildung des kommutativen Körpers $F(+,\cdot)$ mit endlicher D-Gruppe Γ_{φ}, und es gelte Kern $N_{\Gamma_{\varphi}} \subset U_{\varphi}$.*
Dann existiert ein Homomorphismus ψ von $(F^*)^{N_{\Gamma_{\varphi}}}$ auf Γ_{φ} derart, daß $\varphi = N_{\Gamma_{\varphi}}\psi$, und φ ist ein gekoppelter Homomorphismus und Antihomomorphismus von $F(+,\cdot)$.

Es sei φ insbesondere ein gekoppelter Homomorphismus des kommutativen Körpers $F(+,\cdot)$ mit endlicher zyklischer D-Gruppe Γ_{φ}. Dann ist die Bedingung Kern $N_{\Gamma_{\varphi}} \subset U_{\varphi}$ erfüllt; der Kern von $N_{\Gamma_{\varphi}}$ hat nämlich unter diesen Voraussetzungen die Form $\{x^{\gamma}x^{-1} | x \in F^*\}$ für jedes Erzeugende γ von Γ_{φ} („Hilberts Satz 90"), und die Elemente $x^{\gamma}x^{-1}$ sind nach (2.9) in U_{φ} enthalten. Daher besitzt (9.4) das Korollar

(9.5) *Es sei Γ eine endliche zyklische Automorphismengruppe des kommutativen Körpers $F(+,\cdot)$ mit dem Fixkörper P. Dann gibt es zu jedem gekoppelten Homomorphismus φ von $F(+,\cdot)$ mit $\Gamma_\varphi = \Gamma$ (d. h. $P_\varphi = P$) einen Homomorphismus ψ von $(F^*)^{N_\Gamma}$ auf Γ derart, daß $\varphi = N_\Gamma\psi$; und jeder Epimorphismus $\psi : (F^*)^{N_\Gamma} \to \Gamma$ führt auf diese Weise zu einem gekoppelten Homomorphismus φ von $F(+,\cdot)$ mit $\Gamma_\varphi = \Gamma$.*

Zusatz: Besonders günstig ist die Situation, wenn Γ außerdem die Voraussetzung von (2.10)b) erfüllt (z. B. wenn Γ Primzahlordnung hat), weil dann jede gekoppelte Abbildung mit der D-Gruppe Γ ein Homomorphismus ist ([31], Satz 11).

Als Anwendung bestimmte H. Karzel sämtliche gekoppelten Abbildungen von $\mathbb{Q}(i)$.

F. Pokropp hat in [47] (§ 8) gekoppelte Homomorphismen mit endlich erzeugten abelschen D-Gruppen untersucht.

E) Einfach-transzendente Erweiterungen

In diesem Abschnitt bezeichnet $F(+,\cdot) = (H(t))(+,\cdot)$ eine einfach-transzendente Erweiterung eines kommutativen Körpers $H(+,\cdot)$. Unser Ziel ist es, eine gewisse Übersicht über sämtliche gekoppelten Homomorphismen (und damit auch Antihomomorphismen) φ von $F(+,\cdot)$ zu gewinnen, deren Fixkörper P_φ den zugrunde liegenden Körper H enthalten. Das Ergebnis besteht in einer Reduktion auf das Problem, Homomorphismen von $F^*(\cdot)$ in $H(+), H^*(\cdot)$ bzw. in weiter unten definierte Gruppen $\bar{H}(\overset{*}{\lambda})$ zu finden, die gewissen Zusatzbedingungen genügen.

Es bedeuten im folgenden $\mathfrak{M}$ die Menge der zweireihigen quadratischen, regulären Matrizen über H, E die Einheitsmatrix in $\mathfrak{M}$, und $\mathfrak{P}(H)$ die Menge aller normierten, irreduziblen Polynome aus $H[t]$ [27]. Offenbar ist $\mathfrak{P}(H) \cup H^*$ ein Erzeugendensystem von $F^*(\cdot)$.

Wenn $A \in \mathfrak{M}$ keinen Eigenwert in H besitzt, Q_A das charakteristische Polynom von A und (Q_A) das von Q_A erzeugte maximale Ideal in $H[t]$ bezeichnen, ist der Ring $L_A(+,\cdot) := (H \cdot E + H \cdot A)(+,\cdot)$ von Matrizen ein zu $(H[t]/(Q_A))(+,\cdot)$ isomorpher kommutativer Körper. Wir beschreiben jetzt eine für das folgende zweckmäßige Darstellung der Faktorgruppe $(L_A^*/H^*)(\cdot)$:

Es sei ω ein nicht in H enthaltenes Symbol, und es werde in $\bar{H} := H \cup \{\omega\}$ durch die Vorschrift

---

[27]) Ein Polynom $a_n t^n + \ldots + a_0 \in H[t]$ heiße *normiert*, wenn $a_n = 1$.

$$\alpha *_A \beta = \left\{ \begin{array}{r} \dfrac{\alpha\beta - D(A)}{\alpha + \beta + S(A)}, \text{ wenn } \alpha + \beta + S(A) \neq 0 \\ \omega, \text{ wenn } \alpha + \beta + S(A) = 0 \end{array} \right\}^{28)} \text{ für alle } \alpha, \beta \in H,$$

sowie

$$\omega *_A \alpha = \alpha *_A \omega = \alpha \quad \text{für alle} \quad \alpha \in \bar{H}$$

eine Verknüpfung $*_A$ erklärt.

Dann ist

$$\varepsilon: \begin{cases} L^*_A/H^* & \to \bar{H} \\ (\alpha \cdot E + \beta \cdot A)H^* & \to \begin{cases} \alpha\beta^{-1}, & \text{falls} \quad \beta \neq 0 \\ \omega, & \text{falls} \quad \beta = 0 \end{cases} \end{cases}$$

ein Isomorphismus von $(L^*_A/H^*)(\cdot)$ auf $\bar{H}(*_A)$, wie man sich leicht überzeugt.

Mit diesen Bezeichnungen läßt sich der folgende Satz aussprechen ([57], (9.6)):

(9.6) a) *Es seien* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathfrak{M} \setminus H^* E$ *eine Matrix, die in* H *keine Eigenwerte besitzt,* τ_0 *ein Homomorphismus von* $H^*(\cdot)$ *in* $\bar{H}(*_A)$ *und* τ_1 *eine Abbildung von* $\mathfrak{P}(H)$ *in* $\bar{H}$ *mit der folgenden Eigenschaft:*

(*) *Für jedes* $P(t) \in \mathfrak{P}(H)$ *und alle* $x \in F^*$ *gilt*

$$\left\{ P\left(\frac{(x^\tau + a)t + b}{ct + (x^\tau + d)} \right) \right\}^\tau = \{P(t)\}^{\tau_1}, \quad \textit{falls} \quad x^\tau \neq \omega;$$

wobei τ *den eindeutig bestimmten Homomorphismus von* $F^*(\cdot)$ *in* $\bar{H}(*_A)$ *bezeichnet, der* τ_0 *und* τ_1 *fortsetzt.*

Dann ist die durch $x_\varphi | H = 1_H$ *sowie*

$$x_\varphi: t \to \begin{cases} \dfrac{(x^\tau + a)t + b}{ct + (x^\tau + d)}, & \textit{falls} \quad x^\tau \neq \omega \\ t, & \textit{falls} \quad x^\tau = \omega \end{cases}$$

erklärte Abbildung φ *von* F^* *in* $A(F, +, \cdot)$ *ein gekoppelter Homomorphismus von* $F(+, \cdot)$, *dessen Fixkörper* H *enthält.*

b) *Es seien* M *ein Element aus* $\mathfrak{M}$, σ_0 *ein Homomorphismus von* $H^*(\cdot)$ *in* $H(+)$ *(bzw. in* $H^*(\cdot)$*) und* σ_1 *eine Abbildung von* $\mathfrak{P}(H)$ *in* H *(bzw. in* H^**) mit der folgenden Eigenschaft:*

(**) *Für jedes* $P(t) \in \mathfrak{P}(H)$ *und alle* $x \in F^*$ *gilt*

$$\left\{ P\left(\frac{a_x t + b_x}{c_x t + d_x} \right) \right\}^\sigma = \{P(t)\}^{\sigma_1};$$

---

[28]) $S(A)$ bezeichnet die Spur, $N(A)$ die Norm von A.

wobei σ den eindeutig bestimmten Homomorphismus von $F^*(\cdot)$ in $H(+)$ (bzw. in $H^*(\cdot)$) bedeutet, der σ_0 und σ_1 fortsetzt, und wobei $\begin{pmatrix} a_x & b_x \\ c_x & d_x \end{pmatrix} = M \cdot \begin{pmatrix} 1 & x^\sigma \\ 0 & 1 \end{pmatrix} \cdot M^{-1} \left(\text{bzw. } = M \cdot \begin{pmatrix} 1 & 0 \\ 0 & x^\sigma \end{pmatrix} \cdot M^{-1} \right)$. *Dann wird durch* $x_\varphi | H = 1_H$ *sowie* $t^{x_\varphi} = \dfrac{a_x t + b_x}{c_x t + d_x}$ *ein gekoppelter Homomorphismus von $F(+,\cdot)$ definiert, dessen Fixkörper H umfaßt.*

c) *Jeder gekoppelte Homomorphismus von $F(+,\cdot)$, dessen Fixkörper den Körper H enthält und dessen D-Gruppe in keiner Kleinschen Vierergruppe liegt, kann auf eine dieser Weisen konstruiert werden.*

Bevor wir (9.6) zur Konstruktion von Fastkörpern heranziehen, wollen wir an einem Beispiel zeigen, daß die D-Gruppe eines gekoppelten Homomorphismus φ von $F(+,\cdot)$ sehr wohl eine Kleinsche Vierergruppe sein kann: Es seien $H(+,\cdot)$ und $a,b,c \in H^*$ so gewählt, daß die Teilmengen $A = \{t-a, t+a, t-a^{-1}, t+a^{-1}\}$, $B = \{t-b, t+b, t-b^{-1}, t+b^{-1}\}$ und $C = \{t-c, t+c, t-c^{-1}, t+c^{-1}\}$ von F paarweise disjunkt sind. Schließlich seien ρ,σ,τ die durch $\rho|H = \sigma|H = \tau|H = 1_H$ sowie $t^\rho = -t, t^\sigma = \frac{1}{t}, t^\tau = -\frac{1}{t}$ erklärten Automorphismen von $F(+,\cdot) = H(t)(+,\cdot)$. Dann ist der durch

$$x_\varphi = \begin{cases} \rho & \text{für alle } x \in A \\ \sigma & \text{für alle } x \in B \\ \tau & \text{für alle } x \in C \\ 1_F & \text{für alle } x \in H^* \quad \text{und alle } x \in \mathfrak{P}(H) \setminus (A \cup B \cup C) \end{cases}$$

eindeutig bestimmte Homomorphismus φ von $F^*(\cdot)$ in $A(F,+,\cdot)$ ein gekoppelter Homomorphismus von $F(+,\cdot)$ mit der Kleinschen Vierergruppe $\{1_F, \rho, \sigma, \tau\}$ als D-Gruppe, wie man mit Hilfe von (2.9) leicht bestätigt.

Insbesondere der Punkt b) aus (9.6) gibt uns die Möglichkeit, zahlreiche gekoppelte Homomorphismen von $F(+,\cdot) = H(t)(+,\cdot)$ aufzufinden. Der Einfachheit halber sei $M = E$ angenommen. Dann sind die folgenden Bedingungen zu erfüllen:

1. Fall: Man bestimme

α) einen Homomorphismus σ_0 von $H^*(\cdot)$ in sich,

β) eine Abbildung σ_1 von $\mathfrak{P}(H)$ in H^* mit der Eigenschaft

$$(P(x^\sigma t))^\sigma = (P(t))^{\sigma_1} \quad \text{für alle} \quad P(t) \in \mathfrak{P}(H) \quad \text{und} \quad x \in F^*.$$

2. Fall: Man bestimme

α) einen Homomorphismus ρ_0 von $H^*(\cdot)$ in $H(+)$,

β) eine Abbildung ρ_1 von $\mathfrak{P}(H)$ in H mit der Eigenschaft

$$(P(t + x^{\rho}))^{\rho_1} = (P(t))^{\rho_1} \quad \text{für alle} \quad P(t) \in \mathfrak{P}(H) \quad \text{und} \quad x \in F^*.$$

ρ und σ sind dabei die ρ_0 und ρ_1 bzw. σ_0 und σ_1 fortsetzenden Homomorphismen von $F^*(\cdot)$ in $H(+)$ (bzw. in $H^*(\cdot)$).

Beispiel

Es bezeichne $|P(t)|$ den Grad von $P(t) \in H[t]$. Offenbar gilt

$$|P(x^{\sigma} t)| = |P(t)| = |P(t + x^{\rho})| \quad \text{für alle} \quad P(t) \in \mathfrak{P}(H) \quad \text{und alle} \quad x \in F^*.$$

Für jede Funktion f von $\mathbb{N}$ in H^* (bzw. H) genügt daher die durch $(P(t))^{\sigma_1} = f(|P(t)|)$ (bzw. $(P(t))^{\rho_1} = f(|P(t)|)$) definierte Abbildung $\sigma_1 : \mathfrak{P}(H) \to H^*$ (bzw. $\rho_1 : \mathfrak{P}(H) \to H$) den geforderten Bedingungen.

In [47] wurden beispielsweise $f : n \to d^n$ (bzw. $f : n \to dn$) mit $d \in H^*$ benutzt.

Zum Abschluß betrachten wir eine gekoppelte Abbildung von $F(+,\cdot)$, deren D-Gruppe die Ordnung 2 hat:

Für jedes $x = \gamma t^r \dfrac{t^m + \alpha_{m-1} t^{m-1} + \cdots + \alpha_0}{t^n + \beta_{n-1} t^{n-1} + \cdots + \beta_0} \in H(t)^*$ mit $\gamma, \alpha_0, \beta_0 \neq 0$ sei $e_x = (-1)^{m-n}$ gesetzt.

Die Abbildung $e : x \to e_x$ ist ein Homomorphismus von $F^*(\cdot)$ in $\{-1, +1\}$; sein Kern U ist ein Normalteiler vom Index 2 in $F^*(\cdot)$. Für jedes $x \in F^*$ werde $x_{\varphi} \in A(F, +, \cdot)$ durch

$$x_{\varphi}|H = 1_H \quad \text{und} \quad t^{x_{\varphi}} = \begin{cases} t, & \text{wenn} \quad x \in U \\ \dfrac{1}{ct}, & \text{wenn} \quad x \notin U \end{cases}$$

definiert, wobei c beliebig aus H^* gewählt ist.

Da $e_{x^y\varphi} = e_x$ für alle $x, y \in F^*$ gilt, ist φ nach (2.9) ein gekoppelter Homomorphismus von $F(+,\cdot)$ und $|\Gamma_{\varphi}| = 2$.

Dieses Beispiel kann leicht dadurch abgeändert werden, daß man $t + a$ mit $a \in H^*$ an die Stelle des Primpolynoms t treten läßt.

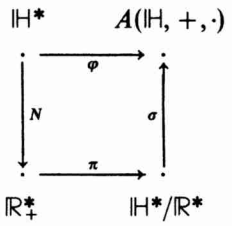
F) Quaternionen über R

Es bezeichne $\mathbb{H}(+,\cdot)$ den Quaternionenkörper über dem Körper $\mathbb{R}(+,\cdot)$ der reellen Zahlen: $\mathbb{H} = \{\alpha + \beta i + \gamma j + \delta ij | \alpha, \beta, \gamma, \delta \in \mathbb{R}\}$, $i^2 = j^2 = -1$, $ij = -ji$. Der nächste Satz gibt Auskunft über die gekoppelten Homomorphismen und Antihomomorphismen von $\mathbb{H}(+,\cdot)$, ([57], (9.9)–(9.11)):

(9.7) a) $\varphi : \begin{cases} \mathbb{H}^* \to A(\mathbb{H}, +, \cdot) \\ x \to i_x \end{cases}$ *ist der einzige gekoppelte Homomorphismus von* $\mathbb{H}(+,\cdot)$ *mit nicht-kommutativer D-Gruppe.* $\mathbb{H}^{\varphi}(+,\cdot)$ *ist der zu* $\mathbb{H}(+,\cdot)$ *duale Körper.*

b) *Es gibt keinen gekoppelten Antihomomorphismus von* $\mathbb{H}(+,\cdot)$ *mit nicht-kommutativer D-Gruppe.*

c) *Zu jedem gekoppelten Homomorphismus* φ *von* $\mathbb{H}(+,\cdot)$ *mit kommutativer D-Gruppe existiert ein Homomorphismus* π *von* $\mathbb{R}^*_+(\cdot)$ *in* $(\mathbb{H}^*/\mathbb{R}^*)(\cdot)$ *derart, daß* $\varphi = N\pi\sigma$; *und jeder derartige Homomorphismus* π *führt zu einem gekoppelten Homomorphismus* $\varphi = N\pi\sigma$ *von* $\mathbb{H}(+,\cdot)$ *mit kommutativer D-Gruppe. Dabei bezeichnen* $N : \alpha + \beta i + \gamma j + \delta ij \to \alpha^2 + \beta^2 + \gamma^2 + \delta^2$ *die Norm und* $\sigma : x \cdot \mathbb{R}^* \to i_x$ *den kanonischen Isomorphismus von* $(\mathbb{H}^*/\mathbb{R}^*)(\cdot)$ *auf* $A(\mathbb{H}, +, \cdot)$.



Bemerkungen:

1. Weitere gekoppelte Abbildungen von $\mathbb{H}(+,\cdot)$ erhält man durch Übergang zu der zu $\mathbb{H}(+,\cdot)$ dualen Quaternionenalgebra.

2. Die Homomorphismen $\pi_c: \begin{cases} \mathbb{R}^*_+ = \mathbb{H}^*/\mathbb{R}^* \\ x \to (e^{ic\log x})\,\mathbb{R}^* \end{cases}$, (mit $c \in \mathbb{R}^*$), liefern nach (9.7)c) die Kalscheuerschen Fastkörper (Beispiel im Abschnitt B).

3. Für jedes $t \neq 1$ aus $\mathbb{R}^*_+$ bezeichne W_t die Untergruppe $W_t = \{t^r | r \in \mathbb{Q}\}$ von $\mathbb{R}^*_+(\cdot)$. Wenn G_t eine maximale Untergruppe von $\mathbb{R}^*_+(\cdot)$ mit $G_t \cap W_t = \{1\}$ ist, gilt $\mathbb{R}^*_+ = G_t \times W_t$. Der Homomorphismus $\pi_t = \pi(t, G_t)$ von $\mathbb{R}^*_+(\cdot)$ in $\mathbb{H}^*/\mathbb{R}^*$, der jedes $x \in G_t \cdot t^r$ in $e^{ir} \cdot \mathbb{R}^*$ überführt, liefert nach (9.7)c) einen gekoppelten Homomorphismus $\varphi_t: \begin{cases} \mathbb{H}^* \to A(\mathbb{H}, +, \cdot) \\ x \to x^{N\pi_t\sigma} \end{cases}$.

Literaturverzeichnis

[1] Amitsur, S. A.: Finite subgroups of division rings. Trans. Amer. Math. Soc. **80** (1955) 361–386.

[2] André, J.: Über nicht-Desarguessche Ebenen mit transitiver Translationsgruppe. Math. Z. **60** (1954) 156–186.

[3] André, J.: Projektive Ebenen über Fastkörpern. Math. Z. **62** (1955) 137–160.

[4] André, J.: Eine Beziehung zwischen Zentrum und Kern endlicher Fastkörper. Arch. d. Math. **14** (1963) 145–146.

[5] André, J.: Über unvollständige Fastkörper und verallgemeinerte affine Räume. Math. Z. **119** (1971) 254–266.

[6] Artin, E.: The orders of the linear groups. Commun. Pure a. Applied Math. **8** (1955) 355–366.
[7] Artin, E.: Geometric Algebra. New York 1957.
[8] Birkhoff, G. D. a. Vandiver, H. S.: On the integral divisors of $a^n - b^n$. Ann. Math. **5** (1904) 173–180.
[9] Brauer, R.: On a theorem of H. Cartan. Bull. Amer. Math. Soc. **55** (1949) 619–620.
[10] Cohn, P. M.: On the embedding of rings in skew fields. Proc. London Math. Soc. **11** (1961) 511–530.
[11] Dancs, S.: Bull. Austral. Math. Soc. **5** (1971) 275–280.
[12] Dancs, S.: On finite Dickson near-fields. Abh. Math. Sem. Univ. Hamburg **37** (1972) 254–257.
[13] Dembowski, P.: Finite geometries. Berlin-Heidelberg-New York 1968.
[14] Dickson, L. E.: On finite algebras. Nachr. Kgl. Ges. Wiss. Göttingen, Math.-Phys. Klasse (1905) 358–393.
[15] Ellers, E.; Karzel, H.: Involutorische Geometrien. Abh. Math. Sem. Univ. Hamburg **25** (1961) 93–104.
[16] Ellers, E.; Karzel, H.: Kennzeichnung elliptischer Geometrien. Abh. Math. Sem. Univ. Hamburg **26** (1963) 55–77.
[17] Ellers, E.; Karzel, H.: Endliche Inzidenzgruppen. Abh. Math. Sem. Univ. Hamburg **27** (1964) 250–264.
[18] Faith, C. C.: On conjugates in division rings. Can. J. Math. **10** (1958) 374–380.
[19] Foulser, D. A.: On finite affine planes and their collineation groups. Thesis, University of Michigan.
[20] Hall, M.: Projective planes. Trans. Amer. Math. Soc. **54** (1943) 229–277.
[21] Hall, M.: The theory of groups. New York 1959.
[22] Herstein, J. N.; Scott, W. R.: Subnormal subgroups of division rings. Can. J. Math. **15** (1963) 80–83.
[23] Huppert, B.: Endliche Gruppen I. Berlin-Heidelberg-New York 1967.
[24] Jacobson, N.: Structure of rings. 1956.
[25] Kalscheuer, F.: Bestimmung aller stetigen Fastkörper über dem Körper der reellen Zahlen als Grundkörper. Abh. Math. Sem. Univ. Hamburg **13** (1940) 413–435.
[26] Karzel, H.: Kommutative Inzidenzgruppen. Arch. Math. **13** (1962) 535–538.
[27] Karzel, H.: Ebene Inzidenzgruppen. Arch. Math. **15** (1964) 10–17.
[28] Karzel, H.: Beziehungen zwischen topologischen Inzidenzgruppen und topologischen Fastkörpern. Gublio 1964.
[29] Karzel, H.: Normale Fastkörper mit kommutativer Inzidenzgruppe. Abh. Math. Sem. Univ. Hamburg **28** (1965) 124–132.
[30] Karzel, H.: Zweiseitige Inzidenzgruppen. Abh. Math. Sem. Univ. Hamburg **29** (1965) 118–136.
[31] Karzel, H.: Unendliche Dicksonsche Fastkörper. Arch. Math. **16** (1965) 247–256.
[32] Karzel, H.: Bericht über projektive Inzidenzgruppen. Jahresber. Deutsch. Math. Ver. **67** (1964) 58–92.
[33] Karzel, H.: Inzidenzgruppen I. Vorlesungsausarbeitung von I. Pieper u. K. Sörensen, Univ. Hamburg 1965.
[34] Karzel, H.: Inzidenzgruppen II. Vorlesungsausarbeitung von I. Pieper u. K. Sörensen, Univ. Hamburg 1966.
[35] Karzel, H.: Zusammenhänge zwischen Fastbereichen, scharf zweifach transitiven Permutationsgruppen und 2-Strukturen mit Rechtecksaxiom. Abh. Math. Sem. Univ. Hamburg **31** (1967) 191–206.

[36] Kerby, W.: Anordnungsfragen in Fastkörpern. Dissertation Univ. Hamburg 1966.
[37] Kerby, W.: Projektive und nicht-projektive Fastkörper. Abh. Math. Sem. Univ. Hamburg **32** (1968) 20–24.
[38] Kerby, W.: Angeordnete Fastkörper. Abh. Math. Sem. Univ. Hamburg **32** (1968) 135–146.
[39] Kerby, W.: Angeordnete Fastkörperebenen. Abh. Math. Sem. Univ. Hamburg **33** (1969) 4–16.
[40] Kerby, W.; Wefelscheid, H.: Bemerkungen über Fastbereiche und scharf 2-fach transitive Gruppen. Abh. Math. Sem. Univ. Hamburg **37** (1972) 20–29.
[41] Kerby, W.; Wefelscheid, H.: Über eine scharf 3-fach transitiven Gruppen zugeordnete algebraische Struktur. Abh. Math. Sem. Univ. Hamburg **37** (1972) 225–235.
[42] Lüneburg, H.: Über die Anzahl der Dicksonschen Fastkörper gegebener Ordnung. Atti del convegno di geometria combinatoria a sue applicazioni. Perugia 1971.
[43] Misfeld, J.; Timm, J.: Topologische Dicksonsche Fastkörper. Abh. Math. Sem. Univ. Hamburg **37** (1972) 60–67.
[44] Neumann, B. H.: On the commutativity of addition. J. London Math. Soc. **15** (1940) 203–208.
[45] Passmann, D. S.: Permutation groups. New York 1968.
[46] Pickert, G.: Projektive Ebenen. Berlin-Göttingen-Heidelberg 1955.
[47] Pokropp, F.: Dicksonsche Fastkörper. Abh. Math. Sem. Univ. Hamburg **30** (1967) 188–219.
[48] Pokropp, F.: Isomorphe Gruppen- und Fastkörperpaare. Arch. Math. **18** (1967) 235–240.
[49] Pokropp, F.: Gekoppelte Abbildungen auf Gruppen. Abh. Math. Sem. Univ. Hamburg **32** (1968) 147–159.
[50] Rao, N.: A question of finite Moufang-Veblen-Wedderburn systems. Journal of algebra **13** (1969) 486–495.
[51] Scott, W. R.: Group theory. New Jersey 1964.
[52] Timm, J.: Zur Theorie der (nicht notwendig assoziativen) Fastringe. Abh. Math. Sem. Univ. Hamburg **35** (1970) 14–31.
[53] Timm, J.: Zur Konstruktion von Fastringen I. Abh. Math. Sem. Univ. Hamburg **35** (1970) 57–75.
[54] Timm, J.: Zur Theorie der Fastringkonstruktionen II. Abh. Math. Sem. Univ. Hamburg **36** (1971) 16–32.
[55] Wähling, H.: Darstellung zweiseitiger Inzidenzgruppen durch Divisionsalgebren. Abh. Math. Sem. Univ. Hamburg **30** (1967) 220–240.
[56] Wähling, H.: Invariante und vertauschbare Teilfastkörper. Abh. Math. Sem. Univ. Hamburg **33** (1969) 197–202.
[57] Wähling, H.: Zur Theorie der Fastkörper. Habilitationsschrift, Hamburg 1972.
[58] Wähling, H.: Ein Zassenhauskriterium für unendliche Fastkörper.
[59] Wähling, H.: Automorphismen Dicksonscher Fastkörperpaare mit kleiner Dicksongruppe.
[60] Wähling, H.: Normale Fastkörper mit kommutativer bzw. zweiseitiger Inzidenzgruppe.
[61] Wefelscheid, H.: Vervollständigung topologischer Fastkörper. Math. Z. **99** (1967) 279–298.
[62] Wefelscheid, H.: Untersuchungen über Fastkörper und Fastbereiche. Habilitationsschrift, Hamburg 1971.
[63] Wefelscheid, H.: Zur Konstruktion bewerteter Fastkörper. Abh. Math. Sem. Univ. Hamburg **38** (1972) 106–117.

[64] Wode, D.: Einbettung von Gruppenräumen in dreidimensionale projektive Räume. Staatsexamensarbeit, Hamburg 1964.
[65] Wolf, J. A.: Spaces of constant curvature. New York 1967.
[66] Zassenhaus, H.: Kennzeichnung endlicher linearer Gruppen als Permutationsgruppen. Abh. Math. Sem. Univ. Hamburg **11** (1936) 17–40.
[67] Zassenhaus, H.: Über endliche Fastkörper. Abh. Math. Sem. Univ. Hamburg **11** (1936) 187–220.
[68] Zemmer, J.: Near-fields, planar and non planar. The Math. Student **31** (1964) 145–150.
[69] Zemmer, J.: The additive group of an infinite near-field is Abelian. J. London Math. Soc. **44** (1969) 65–67.

Nachtrag

[70] Pazderski, G.: Die Ordnungen, zu denen nur Gruppen mit gegebenen Eigenschaften gehören. Arch. Math. **10** (1959) 331–343.

(Eingegangen: 1. 3. 1973)

Mathematisches Seminar
der Universität Hamburg
2 Hamburg 13, Rothenbaumchaussee 67/69