Bemerkung zu einem Satz von Glaubermann

LITERATURVERZEICHNIS

1 C. de Boor: A Practical Guide to Splines. Springer-Verlag, New York, Heidelberg, Berlin 1978.
2 B. Dimsdale: Convex cubic splines. J. Res. Develop. *22*, 168–178 (1978).
3 U. Hornung: Numerische Berechnung monotoner und konvexer Spline-Interpolierender. ZAMM *59*, T64–T65 (1979).
4 H. Mettke, T. Lingner: Ein Verfahren zur konvexen kubischen Splineinterpolation. Wiss. Z. TU Dresden *32*, 77–80 (1983).
5 E. Neuman: Uniform approximation by some Hermite interpolating splines. J. Comput. Appl. Math. *4*, 7–9 (1978).
6 E. Neuman: Convex interpolating splines of odd degree. Utilitas Math. *14*, 129–140 (1978).
7 E. Neuman: Shape preserving interpolation by polynomial splines. Report Nr. N-112, Institut of Computer Science, University of Wroclaw 1982.
8 E. Passow: Monotone quadratic spline interpolation. J. Approximation Theory *19*, 143–147 (1977).
9 E. Passow, J. A. Roulier: Monotone and convex spline interpolation. SIAM J. Numer. Anal. *14*, 904–909 (1977).

 0013-6018/84/040085-11$1.50 + 0.20/0

Bemerkung zu einem Satz von Glauberman

Das Ziel dieser Note ist der Nachweis, dass der unten formulierte Satz von Glauberman ([1], S. 270, Lemma 4.3, und [2], S. 165–171) auch dann gilt, wenn die Charakteristik des Koordinatenkörpers gleich 2 ist. Dieser Satz spielt eine Rolle beim Beweis eines sehr gewichtigen Theorems von Hering und Ostrom ([2], S. 178, Theorem 35.10), das von Kollineationsgruppen endlicher Translationsebenen handelt, die sich durch Scherungen erzeugen lassen.

Satz (Glauberman). *$V \neq 0$ sei ein endlicher Vektorraum und $M \subset GL(V)$ ein System von Vektorraumautomorphismen mit folgenden Eigenschaften:*

I. $\alpha \in M \Rightarrow \alpha^{-1} \in M$.
II. *$M \cup \{0\}$ ist additiv abgeschlossen.*
III. $1 \in M$.

Dann ist $M \cup \{0\}$ ein Körper.

Beweis: Wir beginnen mit einigen Vorbemerkungen. Der Koordinatenschiefkörper K des Vektorraumes V ist natürlich endlich. Ausserdem ist $L := M \cup \{0\}$ bezüglich der Addition eine abelsche Gruppe, deren Exponent mit der Charakteristik von K übereinstimmt. Hinsichtlich der Bezeichnungsweise ist anzumerken, dass mit $\langle X \rangle$ stets das Erzeugnis der Teilmenge $X \subset GL(V)$ in der linearen Gruppe $GL(V)$ gemeint ist. Wir nehmen jetzt unsere Betrachtungen auf mit der Begründung einiger Einzelfeststellungen.

a) $\alpha,\beta \in M \Rightarrow \alpha\beta\alpha \in M$.

Beweis: Im Falle $\alpha \neq \beta^{-1}$ folgt mit I. und der Gruppeneigenschaft von $(L,+)$, dass $\alpha - \beta^{-1}$ und dann auch $-\alpha^{-1} + (\alpha - \beta^{-1})^{-1} = \left(-\alpha^{-1}(\alpha - \beta^{-1}) + 1\right)(\alpha - \beta^{-1})^{-1}$ $= \alpha^{-1}\beta^{-1}(\alpha - \beta^{-1})^{-1} = \left((\alpha - \beta^{-1})\beta\alpha\right)^{-1} = (\alpha\beta\alpha - \alpha)^{-1}$ zu M gehört. Mit I. und II. erhalten wir jetzt die Behauptung.

b) $\alpha \in M \Rightarrow \langle\alpha\rangle \subset M$.

Beweis: Wegen III. kann man in a) $\beta := 1$ setzen. Daher gilt auch $\alpha^2 \in M$. a) zeigt jetzt, dass alle Potenzen von α mit natürlichem Exponenten zu M gehören. Dies genügt, weil $\langle\alpha\rangle$ endlich ist.

c) $\alpha,\beta,\gamma \in M \Rightarrow \alpha\beta + \beta\alpha, \alpha\beta\gamma + \gamma\beta\alpha \in L$.

Beweis: Da $(L,+)$ eine Gruppe ist, folgt aus a) $\alpha\beta\gamma + \gamma\beta\alpha = (\alpha + \gamma)\beta(\alpha + \gamma)$ $- \alpha\beta\alpha - \gamma\beta\gamma \in L$. Weil man $\gamma := 1$ setzen darf, gilt auch $\alpha\beta + \beta\alpha \in L$.

d) *Für* $\alpha,\beta \in M$, $\varepsilon_0,\ldots,\varepsilon_r,\eta_0,\ldots,\eta_r \in \mathbf{Z}$ *gilt*

$$\prod_{i=0}^{r} (\alpha^{\varepsilon_i}\beta^{\eta_i}) + \prod_{i=0}^{r} (\beta^{\eta_{r-i}}\alpha^{\varepsilon_{r-i}}) \in L.$$

Beweis (durch Induktion nach r): b) und c) erledigen den Fall $r = 0$. c), die Gruppeneigenschaft von $(L,+)$ und die folgende Gleichung zusammen ermöglichen den Induktionsschluss.

$$\begin{aligned}
&\alpha^{\varepsilon_0}(\alpha^{\varepsilon_{r+1}}\beta^{\eta_r}\alpha^{\varepsilon_r}\beta^{\eta_{r-1}}\ldots\alpha^{\varepsilon_1}\beta^{\eta_0} + \beta^{\eta_0}\alpha^{\varepsilon_1}\ldots\beta^{\eta_{r-1}}\alpha^{\varepsilon_r}\beta^{\eta_r}\alpha^{\varepsilon_{r+1}})\beta^{\eta_{r+1}} \\
&+ \beta^{\eta_{r+1}}(\alpha^{\varepsilon_{r+1}}\beta^{\eta_r}\alpha^{\varepsilon_r}\beta^{\eta_{r-1}}\ldots\alpha^{\varepsilon_1}\beta^{\eta_0} + \beta^{\eta_0}\alpha^{\varepsilon_1}\ldots\beta^{\eta_{r-1}}\alpha^{\varepsilon_r}\beta^{\eta_r}\alpha^{\varepsilon_{r+1}})\alpha^{\varepsilon_0} \\
&= (\alpha^{\varepsilon_0+\varepsilon_{r+1}}\beta^{\eta_r}\alpha^{\varepsilon_r}\beta^{\eta_{r-1}}\ldots\alpha^{\varepsilon_1}\beta^{\eta_0+\eta_{r+1}} + \beta^{\eta_0+\eta_{r+1}}\alpha^{\varepsilon_1}\ldots\beta^{\eta_{r-1}}\alpha^{\varepsilon_r}\beta^{\eta_r}\alpha^{\varepsilon_0+\varepsilon_{r+1}}) \\
&+ (\alpha^{\varepsilon_0}\beta^{\eta_0}\alpha^{\varepsilon_1}\beta^{\eta_1}\ldots\alpha^{\varepsilon_{r+1}}\beta^{\eta_{r+1}} + \beta^{\eta_{r+1}}\alpha^{\varepsilon_{r+1}}\ldots\beta^{\eta_1}\alpha^{\varepsilon_1}\beta^{\eta_0}\alpha^{\varepsilon_0}).
\end{aligned}$$

e) *Sind die Elemente von M (bezüglich der Multiplikation) paarweise vertauschbar, so ist L ein Körper.*

Beweis: Wir haben nur zu zeigen, dass M multiplikativ abgeschlossen ist. Dazu seien $\alpha,\beta \in M$ beliebig vorgegeben.

1. Fall: $\mathit{char}\,K \neq 2$. Mit c) folgt $2\alpha\beta = \alpha\beta + \beta\alpha \in L$ und daraus $\alpha\beta \in L$, weil $\mathit{char}\,K \neq 2$ ist. Wegen $\alpha\beta \neq 0$ gilt $\alpha\beta \in M$.

2. Fall: $\mathit{char}\,K = 2$. Der von α in $\mathit{End}\,V$ erzeugte Teilring ist wegen b) und der Gruppeneigenschaft von $(L,+)$ in L enthalten und daraufhin ein Körper. Weil dieser die Charakteristik 2 hat, ist die Ordnung von α bezüglich der Multiplikation ungerade. Daher gibt es ein $\gamma \in \langle\alpha\rangle \subset M$ mit $\gamma^2 = \alpha$. a) zeigt nun $\alpha\beta = \gamma^2\beta = \gamma\beta\gamma \in M$.

Nach diesen Vorüberlegungen beweisen wir jetzt den Satz durch Induktion nach $n := \dim V$. Im Falle $n = 1$ gilt $GL(V) \cong K^{\times}$. Weil K als endlicher Schiefkörper nach dem Satz von Wedderburn kommutativ ist, sind die Elemente von M paarweise vertauschbar. Daraufhin ist L nach e) ein Körper. Nun sei $n > 1$ und die Behauptung zutreffend für Dimensionen $< n$. Wegen e) genügt es zu zeigen, dass zwei beliebig vorgegebene Elemente $\alpha, \beta \in M$ vertauschbar sind. Zur Begründung dieser Behauptung nehmen wir eine Fallunterscheidung vor.

1. Fall: $\langle\alpha,\beta\rangle$ lässt einen nichttrivialen Unterraum $U \subset V$ im ganzen fest. Wir ziehen $M_U := \{\gamma \in M \mid U^\gamma = U\}$ in Betracht. Für $\gamma \in M_U$ ist die Einschränkung $\bar{\gamma} := \gamma|_U$ von γ auf U ein Automorphismus von U. Das System $\bar{M} := \{\bar{\gamma} \mid \gamma \in M_U\}$ hat offenbar die Eigenschaften I.–III. Wegen $0 < \dim U < \dim V = n$ ist $\bar{M} \cup \{0\}$ nach Induktionsannahme ein Körper. Weil $\bar{M}$ als Multiplikationsgruppe eines endlichen Körpers zyklisch ist, gibt es ein $\gamma \in M_U$ mit $\bar{M} = \langle\bar{\gamma}\rangle$. Zu beliebig vorgegebenem $\delta \in M_U$ findet man ein $k \in \mathbf{Z}$ mit $\bar{\delta} = \bar{\gamma}^k$. Aus b) und der Gruppeneigenschaft von $(L,+)$ folgt $\delta - \gamma^k \in L$ und dann $\delta - \gamma^k = 0$, weil $\delta - \gamma^k$ nicht injektiv ist. Also gilt $\delta = \gamma^k \in \langle\gamma\rangle$. Nun haben wir $\alpha, \beta \in M_U \subset \langle\gamma\rangle$ und damit die Vertauschbarkeit von α und β.

2. Fall: $\langle\alpha,\beta\rangle$ operiert irreduzibel auf V. Wir fassen den von $\langle\alpha,\beta\rangle$ erzeugten Teilring $R \subset \mathit{End}\, V$ ins Auge. Klar ist, dass die Nullteilerfreiheit des Ringes R die Vertauschbarkeit von α und β mit sich bringt, weil ein endlicher nullteilerfreier Ring $\neq \{0\}$ als endlicher Schiefkörper nach dem Satz von Wedderburn kommutativ ist. Zum Beweis der Nullteilerfreiheit fixieren wir einen Nullteiler $u \in R$. u lässt sich als Summe passender Elemente $u_i \in \langle\alpha,\beta\rangle$ darstellen: $u = \sum_{i=1}^{s} u_i$. Jeder der Summanden u_i besitzt eine Darstellung der Gestalt

$$u_i = \prod_{j=0}^{r_i} \alpha^{\varepsilon_{ij}} \beta^{\eta_{ij}} \quad (r_i \in \mathbf{N}_0, \varepsilon_{ij}, \eta_{ij} \in \mathbf{Z}).$$

Wir setzen

$$u_i' := \prod_{j=0}^{r_i} \beta^{\eta_{i,r_i-j}} \alpha^{\varepsilon_{i,r_i-j}} \quad (1 \le i \le s), \qquad u' := \sum_{i=1}^{s} u_i'$$

und behaupten

$$u + u' \in L, \tag{1}$$

$$u \gamma u' = 0 \quad \text{für jedes} \quad \gamma \in \langle\alpha\rangle \cup \langle\beta\rangle. \tag{2}$$

Die Gültigkeit von (1) folgt unmittelbar aus d). Zur Begründung von (2) notieren wir zunächst

$$u \gamma u' = \left(\sum_{i=1}^{s} u_i\right) \gamma \left(\sum_{i=1}^{s} u_i'\right) = \sum_{i=1}^{s} u_i \gamma u_i' + \sum_{i<j} (u_i \gamma u_j' + u_j \gamma u_i').$$

Die Summanden $u_i \gamma u_i'$ bzw. $u_i \gamma u_j' + u_j \gamma u_i'$ gehören nach a) bzw. d) zu L. Weil $(L,+)$ eine Gruppe ist, erhält man $u \gamma u' \in L$. Da u als Nullteiler von R kein Automorphismus von V ist, folgt $u \gamma u' = 0$.

Um die beiden jetzt gesicherten Aussagen (1) und (2) auszuwerten, nehmen wir eine Fallunterscheidung vor. Bei $u + u' = 0$ erhalten wir mit d) $\gamma u - u\gamma = \gamma u + u'\gamma \in L$. Aus (2) folgt ausserdem $(\gamma u - u\gamma)^2 = 0$. $\gamma u - u\gamma$ ist also kein Automorphismus von V und dann als Mitglied von L der Nullendomorphismus. Die jetzt begründete Vertauschbarkeit $\gamma u = u\gamma$ zeigt, dass $Bild\, u$ γ-invariant ist für jedes $\gamma \in \langle\alpha\rangle \cup \langle\beta\rangle$. $Bild\, u \neq V$ ist also ein bezüglich $\langle\alpha,\beta\rangle$ invarianter Unterraum. Nun folgt $Bild\, u = 0$, d.h. $u = 0$. Im Falle $u + u' \neq 0$ ist $u + u'$ als Mitglied von L ein Automorphismus von V. Daraufhin haben die Endomorphismen u, u' fremde Kerne, wir gewinnen die Ungleichung $def\, u' \leq rg\, u$. Andererseits gilt nach (2) $uu' = 0$ und deshalb $Bild\, u \subset Kern\, u'$. Zusammen mit der zuvor begründeten Ungleichung folgt jetzt $Bild\, u = Kern\, u'$, dann mit (2), dass $Bild\, u$ γ-invariant ist für jedes $\gamma \in \langle\alpha\rangle \cup \langle\beta\rangle$ und daraus wie oben $u = 0$.

Zum Abschluss möchte ich noch zwei Bemerkungen anfügen. Erstens erscheint mir erwähnenswert, dass der vorstehende Beweis mit sehr bescheidenen Hilfsmitteln auskommt. Die einzige nennenswerte Zutat ist die Kenntnis, dass die multiplikative Gruppe eines endlichen Schiefkörpers zyklisch ist. Die zweite Bemerkung betrifft III. Ersetzt man III. durch die schwächere Forderung $M \neq \emptyset$, so braucht $M \cup \{0\}$ kein Körper zu sein. Im Falle $char\, K = 2$ bereitet die Herstellung eines Gegenbeispiels keinerlei Mühe.

$$M := \left\{ \begin{pmatrix} \alpha & \alpha \\ 0 & \alpha \end{pmatrix} \middle| \alpha \in K^{\times} \right\}$$

hat die Eigenschaften I. und II., $M \cup \{0\}$ aber ist kein Körper. Auch bei ungerader Charakteristik p findet man Gegenbeispiele. Dazu betrachten wir $V := GF(p^{2s})$ $(s \in \mathbf{N})$ als Vektorraum über $K := GF(p)$. Wegen $p \neq 2$ gibt es ein Element $\lambda \in GF(p^{2s})^{\times}$ mit $o(\lambda) = 2(p^s - 1)$. $\alpha: V \to V$ sei die Abbildung mit $x^{\alpha} := x\lambda$. Dann ist

$$M := \{\alpha^k | k \in \mathbf{Z} \text{ ungerade}\}$$

ein System von Automorphismen des endlichen Vektorraumes $V \neq 0$ mit den Eigenschaften I. und II. $M \cup \{0\}$ ist nicht multiplikativ abgeschlossen, also kein Körper.

Günter Heimbeck, Math. Institut der Universität Würzburg, Würzburg

LITERATURVERZEICHNIS

1 G. Glauberman: A sufficient condition of p-stability. Proc. London Math. Soc. (3), *25*, 253–287 (1972).

2 H. Lüneburg: Translation Planes. Springer-Verlag, New York 1980.

 0013-6018/84/040095-04$1.50 + 0.20/0