Zeitschrift: Elemente der Mathematik
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 41 (1986)
Heft: 6

Artikel: Ein Beweis für die Existenz von Normalbasen in endlichen Körpern
Autor: Blessenohl, D. / Johnsen, K.
DOI: https://doi.org/10.5169/seals-39480

Ein Beweis für die Existenz von Normalbasen in endlichen Körpern

Ein grundlegendes Resultat der Körpertheorie ist der Satz von der Normalbasis [4; S. 283]:

Ist L/K eine endliche galoissche Körpererweiterung mit Galoisgruppe G, so gibt es in L ein Element x mit der Eigenschaft, daß die Menge $\{x^\gamma \mid \gamma \in G\}$ der Konjugierten von x eine Basis des K-Vektorraumes L ist.

Die erste Formulierung dieses Satzes wurde 1850 von G. Eisenstein [2] für den Fall gegeben, daß K ein Körper mit p Elementen für eine Primzahl p ist. Dieser Spezialfall des Satzes wurde von K. Hensel 1888 in [3] bewiesen. Den allgemeinen Fall behandelten E. Noether in [6] und M. Deuring in [1]. In der Folge sind zahlreiche Beweise für diesen Satz angegeben worden. Eine gute Übersicht über die Literatur findet man in [5; S. 76].

Wir wollen den Satz zunächst in einer anderen Form aussprechen. Dazu sei $R := \mathrm{End}_K L$ die K-Algebra der linearen Abbildungen von L in sich. Indem wir $l \in L$ mit der Multiplikation $\varrho_l : x \mapsto xl$ identifizieren, können wir L als Teilring von R auffassen. Setzt man für $\varphi \in R$ und $l \in L$ nun $\varphi l := \varphi\varrho_l$, so ist R ein L-Vektorraum mit $\dim_L R = \dim_K L = |G|$. Nach Dedekinds Unabhängigkeitssatz [4; S. 280] ist G eine L-Basis von R, d. h. es ist

$$R = GL = \left\{ \sum_{\gamma \in G} \gamma l_\gamma \mid l_\gamma \in L \right\}.$$

Mit GK sei die von G erzeugte K-Teilalgebra von R bezeichnet. Ist $\varphi = \sum_{\gamma \in G} \gamma l_\gamma \in GL = R$, so ist $x^\varphi = \sum_{\gamma \in G} x^\gamma l_\gamma$ für alle $x \in L$. Der Satz von der Normalbasis kann nun aufgefaßt werden als eine Aussage über die Struktur von L als GK-Modul:

Satz: *L ist ein zyklischer GK-Modul; d. h. es gibt in L ein Element x mit $L = x^{GK} = \{x^\varphi \mid \varphi \in GK\}$.*

Für den Fall, daß K und L endliche Körper sind, wollen wir diesen Satz mit einer unseres Wissens unbekannten Argumentation beweisen. Dazu seien im folgenden p eine Primzahl, n eine natürliche Zahl und $q := p^n$. Es sei K ein Körper mit q Elementen und L ein Erweiterungskörper von K von endlichem Grad $L : K$. Dann ist L/K galoissch, und die Galoisgruppe G von L/K ist die von dem Automorphismus $\sigma : L \to L$, $x \mapsto x^q$ erzeugte zyklische Gruppe. Da K der Fixkörper von σ ist, ist GK der Zentralisator von G in $R = GL$, d. h. $GK = \{\varphi \mid \varphi \in R, \varphi\sigma = \sigma\varphi\}$. Ist $K[t]$ ein Polynomring über K, so ist die Abbildung $s : K[t] \to GK$, $f(t) \mapsto f(\sigma)$ ein Algebrenepimorphismus, also GK isomorph zu einem Faktorring von $K[t]$. Insbesondere ist jedes Ideal I von GK von einem Element α erzeugt, also $I = \alpha GK$. Für einen GK-Teilmodul M von L sei $\mathrm{An}_{GK} M := \{\alpha \mid \alpha \in GK, m^\alpha = 0 \text{ für alle } m \in M\}$ der Annullator von M in GK, und für ein Ideal I von GK sei $\mathrm{An}_L I := \{l \mid l \in L, l^\alpha = 0 \text{ für alle } \alpha \in I\}$ der Annullator von I in L.

Offenbar ist dann $\mathrm{An}_{GK}M$ ein Ideal von GK und $\mathrm{An}_L I$ ein GK-Teilmodul von L. Wir bezeichnen allgemein für einen Ring S und einen S-Modul X mit $\mathfrak{v}_S(X)$ den Verband der S-Teilmoduln von X und zeigen zunächst:

Lemma: *Die Abbildungen* $An_{GK}: \mathfrak{v}_{GK}(L) \to \mathfrak{v}_{GK}(GK)$ *und* $An_L: \mathfrak{v}_{GK}(GK) \to \mathfrak{v}_{GK}(L)$ *sind Verbandsantiisomorphismen mit* $An_L An_{GK} = id_{\mathfrak{v}_{GK}(L)}$ *und* $An_{GK} An_L = id_{\mathfrak{v}_{GK}(GK)}$.

Beweis:

(1) Sind $M_1, M_2 \in \mathfrak{v}_{GK}(L)$ mit $M_1 \leqq M_2$, so ist offenbar $\mathrm{An}_L M_1 \geqq \mathrm{An}_L M_2$; entsprechendes gilt für An_{GK}.
(2) Sei $M \in \mathfrak{v}_{GK}(L)$. Offenbar ist $\mathrm{An}_L \mathrm{An}_{GK} M \geqq M$. Sei nun $f := \prod_{m \in M} (t-m) \in L[t]$.

Aus der Definition von f folgt unmittelbar:

(i) $f(t+m) = f(t)$ für alle $m \in M$.
Für $0 \neq k \in K$ ist $f(kt) = \prod_{m \in M} (kt-m) = k^{|M|} \prod_{m \in M} (t - m/k) = kf(t)$. Da $f(0) = 0$ ist, haben wir

(ii) $f(kt) = kf(t)$ für alle $k \in K$.
Für $a \in L$ ist $h(t) := f(a+t) \in L[t]$ und $-a+M$ die Menge der Nullstellen von h. Weiterhin ist nach (i) und (ii) für alle $m \in M$

$$f(-a+m) = f(-a) = -f(a),$$

d. h. $-a+M$ ist in der Menge der Nullstellen von $g(t) := f(a)+f(t)$ enthalten. g und h sind normiert mit $\mathrm{Grad}\, g = \mathrm{Grad}\, f = \mathrm{Grad}\, h$. Insgesamt ergibt das $g = h$ und also

(iii) $f(a+t) = f(a) + f(t)$ für alle $a \in L$.
Sei $\varphi: L \to L$ definiert durch $x^\varphi := f(x)$. Nach (ii) und (iii) ist $\varphi \in R$. Wegen $M^\sigma = M$ ist $f \in K[t]$ und deshalb für alle $a \in L$

$$a^{\sigma\varphi} = f(a^\sigma) = f(a)^\sigma = a^{\varphi\sigma},$$

d. h. $\sigma\varphi = \varphi\sigma$ und also $\varphi \in GK$. Wegen $\mathrm{Kern}\, \varphi = M$ ist $\varphi \in \mathrm{An}_{GK} M$ und $\mathrm{An}_L \mathrm{An}_{GK} M \leqq M$.

(3) Sei $I \in \mathfrak{v}_{GK}(GK)$. Offenbar ist $\mathrm{An}_{GK} \mathrm{An}_L I \geqq I$. Sei umgekehrt

$$\beta = \sum_{\gamma \in G} \gamma k'_\gamma \in \mathrm{An}_{GK} \mathrm{An}_L I \quad \text{und} \quad \alpha = \sum_{\delta \in G} \delta k_\delta$$

mit $I = \alpha GK$. Dann ist $\mathrm{Kern}\, \alpha = \mathrm{An}_L I \leqq \mathrm{Kern}\, \beta$. Also gibt es einen K-Epimorphismus μ: $\mathrm{Bild}\, \alpha \to \mathrm{Bild}\, \beta$ mit $\alpha \circ \mu = \beta$. Ist U ein K-Komplement von $\mathrm{Bild}\, \alpha$ in L und $\lambda \in R$ definiert durch $\lambda|_U = 0$ und $\lambda|_{\mathrm{Bild}\, \alpha} = \mu$, so ist $\alpha\lambda = \beta$. Ferner ist $\lambda = \sum_{\eta \in G} \eta l_\eta$ mit geeigneten $l_\eta \in L$. Daher folgt nun $\sum_{\gamma \in G} \gamma k'_\gamma = \sum_{\delta \in G} \delta k_\delta \cdot \sum_{\eta \in G} \eta l_\eta = \sum_{\delta, \eta \in G} \delta\eta k_\delta l_\eta = \sum_{\gamma \in G} \gamma \left(\sum_{\eta \in G} k_{\gamma\eta^{-1}} l_\eta \right)$. Ein Vergleich der Koeffizienten liefert $k'_\gamma = \sum_{\eta \in G} k_{\gamma\eta^{-1}} l_\eta$, $\gamma \in G$. Dieses lineare Gleichungssystem mit Koeffizienten aus K hat eine Lösung in L, folglich auch in K. Daher gilt es $k''_\eta \in K$ mit $k'_\gamma = \sum_{\eta \in G} k_{\gamma\eta^{-1}} k''_\eta$.

Setzen wir $\vartheta := \sum_{\eta \in G} \eta k''_\eta$, so ist $\alpha\vartheta = \beta$ und also $\beta \in \alpha GK = I$; d. h. es ist

$$\mathrm{An}_{GK}\mathrm{An}_L I \leqq I .$$

(4) Wegen (2) und (3) sind An_{GK} und An_L bijektiv. Nach (1) sind beide Abbildungen Verbandsantiisomorphismen.
Das Lemma gilt für jede endliche galoissche Erweiterung mit abelscher Galoisgruppe. Im Falle nicht endlicher Körper ist uns aber kein Beweis bekannt, der nicht schon die Isomorphie von L und GK als GK-Moduln, also die Existenz einer Normalbasis, benutzte.
Wir können den Satz für endliche Körper nun beweisen. Sei $s: K[t] \to GK$ wie oben und $\mathrm{Kern}\, s = fK[t]$. Ferner sei $f = f_1^{a_1} \ldots f_r^{a_r}$ die Primfaktorzerlegung von f in $K[t]$. Für $a, b \in \mathbb{Z}$ bezeichne $[a, b]$ den Verband $(\{z \mid z \in \mathbb{Z},\ a \leqq z \leqq b\}, \max, \min)$. Dann ist $\mathfrak{v}_{K[t]}(K[t]/fK[t])$ antiisomorph zu dem direkten Produkt $\prod_{i=1}^{r} [0, a_i]$ der Verbände $[0, a_i]$.
Nach dem Homomorphiesatz für Ringe ist $\mathfrak{v}_{GK}(GK) \cong \mathfrak{v}_{K[t]}(K[t]/fK[t])$, woraus mit dem Lemma folgt:

$$(*) \quad \mathfrak{v}_{GK}(L) \cong \prod_{i=1}^{r} [0, a_i] .$$

Seien nun M, N verschiedene maximale GK-Teilmoduln von L. Wir setzen $D := M \cap N$, $\bar{M} := M/D$, $\bar{N} := N/D$ und $\bar{L} := L/D$. Wegen (*) sind dann $\bar{M}$ und $\bar{N}$ die einzigen maximalen Teilmoduln von $\bar{L}$. Insbesondere sind $\bar{M}$ und $\bar{N}$ nicht GK-isomorph. Wäre nämlich $\varphi: \bar{M} \to \bar{N}$ ein GK-Isomorphismus, so wäre $\{\bar{m} + \bar{m}^\varphi \mid \bar{m} \in \bar{M}\}$ ein von $\bar{M}$ und $\bar{N}$ verschiedener maximaler Teilmodul von $\bar{L}$.
Bezeichnet $\mathrm{Rad}_{GK} L$ den Durchschnitt aller maximalen GK-Teilmoduln von L, so folgt nun $L/\mathrm{Rad}_{GK} L = M_1 \oplus \ldots \oplus M_l$, wobei M_i paarweise nichtisomorphe, irreduzible GK-Teilmoduln sind. Ist $y = x + \mathrm{Rad}_{GK} L$ so gewählt, dass die M_i-Komponente von y für alle $i \in \{1, \ldots, l\}$ von 0 verschieden ist, so ist $y^{GK} = L/\mathrm{Rad}_{GK} L$ und daher $x^{GK} + \mathrm{Rad}_{GK} L = L$, woraus bekanntlich $x^{GK} = L$ folgt.

D. Blessenohl und K. Johnsen, Math. Seminar, Universität Kiel

LITERATURVERZEICHNIS

1 M. Deuring: Galoissche Theorie und Darstellungstheorie. Mathematische Annalen *107*, 140–144 (1933).
2 G. Eisenstein: Lehrsätze. J.f.d. reine und angewandte Mathematik *39*, 180–182 (1850).
3 K. Hensel: Über die Darstellung der Zahlen eines Gattungsbereichs für einen beliebigen Primdivisor. J.f.d. reine und angewandte Mathematik *103*, 230–237 (1888).
4 N. Jacobsen: Basic Algebra I, San Francisco (1974).
5 R. Lidl, H. Niederreiter: Finite Fields. Encyclopedia of Mathematics and its Applications, London-Amsterdam 1983.
6 E. Noether: Normalbasis bei Körpern ohne höhere Verzweigung. J.f.d. reine und angewandte Mathematik *167*, 147–152 (1932).