25. *Halblineare Erweiteaung des Satzes der Normal basis und ihre Anwendung auf die Existenz der derivierten (differentialen) Basis, I.*

Von Tadasi NAKAYAMA

Mathematishes Institut, Kaiserliche Universität zu Nagoya.

(Comm. by T. TAKAGI, M.I.A., March 12, 1945.)

In dieser Note soll ein Satz aufgestellt werden, welchen man wohl als eine verschränkte, oder vielmehr halblineare Verallgemeinerung des bekannten Satzes der Normalbasis[1] ansehen kann. Er ergibt sich auf natürlicher Weise, wenn wir den Satz der Normalbasis mit der Theorie der halblinearen Darstellungen, die früher von K. Shoda, M. Osima und dem Verfasser entwickelt wurde,[2] in Verbindung bringen. Aus dem Satz folgt sodann leicht die Existenz der derivierten, oder differentialen Basen, wie sie kürzlich von H. J. Riblet[3] bewiesen wurde. Dieser Weg zur derivierten Basis macht es zugleich klar, dass die Wronskische Determinante der einzige Punkt im Beweis der Existenz solcher Basis ist, wo die Eigenschaften der Derivation eigentlich benutzt werden, wodurch insbesondere die Annahme der Charakteristik 0 bei Riblet durch eine schwächere ersetzt wird.

1. *Halblineare Normalbasis.* Wir beweisen

Satz 1. *Es sei* $\mathfrak{L}$ *eine endliche separable Erweiterung eines Körpers* $\mathfrak{K}$. $\mathfrak{L}^*$ *sei der galoissche Körper von* $\mathfrak{L}/\mathfrak{K}$, *und* L *ein (nicht notwending* $\mathfrak{K}$ *enthaltender) Unterkörper von* $\mathfrak{L}^*$ *derart, dass*

$$(L^*\mathfrak{K} : L^*) \geqq (L^*\mathfrak{K} : \mathfrak{K})$$

ist, wo L^* *den von* L *und seinen Konjugierten bezüglich* $\mathfrak{K}$ *erzeugten Körper bedeutet. Dann gibt es in* $\mathfrak{L}$ *ein Element, dessen* $(\mathfrak{L}:\mathfrak{K})$ *Konjugierte bezüglich* $\mathfrak{K}$ *linear unabhängig über* L *sind.*

Beweis. Es genügt ersichtlich den Fall $L^*=L$ zu erledigen. Zuerst sei

1) E. Noether, Normalbasis bei Körpern ohne höhere Verzweigung, Crelle 167 (1931); M. Deuring, Galoissche Theorie und Darstellungstheorie, Math. Ann. 107 (1932); H. Hasse, Klassenkörpertheorie, Marburg (1932); R. Brauer, Über die Kleinsche Theorie der algebraischen Gleichungen, Math. Ann. 110 (1934); M. Deuring, Anwendungen der Darstellungeu von Gruppen durch linearen Substitutionen auf die Galoissche Theorie, Math. Ann. 113 (1936); R. Stauffer, The construction of a normal basis in a separable normal extension field, Amer. J. Math. 58 (1936); T, Nakayama, On Frobeniusean algebras, II, Ann. Math. 42 (1941). Vgl. anch T. Nakayama, Normal basis of a quasi-field, Proc. Imp. Acad. 16 (1940).

2) T. Nakayama-K. Shoda, Über die Darstellung einer endlichen Gruppe durch halblineare Transformationen, Jap. J. Math. 12 (1936); M. Osima, Über die Darstellung einer Gruppe durch halblineare Transformationen, Proc. Phys.-Math. Soc. Jap. 20 (1938).

3) H. J. Riblet, Algebraic differential fields, Amer. J. Math. 63 (1941).

$\mathfrak{L}/\mathfrak{K}$ galoissch; $\mathfrak{G}=\{G_1, G_2, \cdots, G_g\}$ $(g=(\mathfrak{L} : \mathfrak{K}))$ sei die galoissche Gruppe, und die zum Zwischenkörper $L\mathfrak{K}$ gehörige (invariante) Untergruppe sei mit $\mathfrak{H}$ bezeichnet. Wir betrachten den halblinearen Gruppenring

$$(\mathfrak{G}, L)=G_1L+G_2L+\cdots+G_gL$$

von $\mathfrak{G}$ über L, und seinen Unterring

$$(\mathfrak{H}, L)=H_1L+H_2L+\cdots+H_hL \qquad (h=(\mathfrak{L} : L\mathfrak{K})),$$

welcher nichts anders als die gewohnliche Gruppenalgebra von $\mathfrak{H}$ über L ist. Nun ist der Körper $\mathfrak{L}$ als ein $(\mathfrak{H}, L\mathfrak{K})$-Rechtsmodul mit der Gruppenalgebra $(\mathfrak{H}, L\mathfrak{K})$ selbst isomorph (Satz der Normalbais). Hier ist der $(\mathfrak{H}, L)$-Rechtsmodul $(\mathfrak{H}, L\mathfrak{K})$ die direkte Summe von $(L\mathfrak{K} : L)$ mit $(\mathfrak{H}, L)$ isomorphen Untermoduln. Dasselbe gilt also für den $(\mathfrak{H}, L)$-Rectsmodul $\mathfrak{L}$. Andererseits ist $(\mathfrak{G}, L)$ als $(\mathfrak{H}, L)$-Rechtsmodul die direkte Summe von $(\mathfrak{G} : \mathfrak{H})=(L\mathfrak{K} : \mathfrak{K})$ zu $(\mathfrak{H}, L)$ isomorphen Untermoduln. Da hier nach unserer Annahme $(L\mathfrak{K} : \mathfrak{K})\leqq(L\mathfrak{K} : L)$ ist, ist der $(\mathfrak{H}, L)$-Modul $(\mathfrak{G}, L)$ mit einem direkten Summanden in $\mathfrak{L}$ isomorph. Dann ist $(\mathfrak{G}, L)$, nach der Theorie der halblinearen Darstellungen, auch als $(\mathfrak{G}, L)$-Modul mit einem (direkten Summanden)-Untermodul von $\mathfrak{L}$ isomorph.[4] Der Untermodul ist von der Form

$$\xi^{G_1}L+\xi^{G_2}L+\cdots+\xi^{G_g}L \qquad (\xi\in\mathfrak{L});$$

g Konjugierte von ξ sind linear unabhängig über L.

Es sei nun $\mathfrak{L}/\mathfrak{K}$ nicht notwendig galoissch. Nach dem oben bewiesenen gi

---

4) Es sei $\mathfrak{M}$ ein $(\mathfrak{G}, L)$-(Rechts-) Modul, und sei

$$\mathfrak{M}=\mathfrak{m}_1+\mathfrak{m}_2+\cdots+\mathfrak{m}_m \qquad (*)$$

seine (bis auf $(\mathfrak{H}, L)$-Isomorphismus eindeutige) direkte Zerlegung in direkt-unzerlegbare $(\mathfrak{H}, L)$-Untermoduln. Da $\mathfrak{M}=\mathfrak{m}_1G+\mathfrak{m}_2G+\cdots+\mathfrak{m}_mG$, für jedes $G\in\mathfrak{G}$, ist, sind $\mathfrak{m}_1G$, $\mathfrak{m}_2G, \cdots, \mathfrak{m}_mG$ in einer geeigneten Anordnung mit $\mathfrak{m}_1, \mathfrak{m}_2, \cdots, \mathfrak{m}_m$ $(\mathfrak{H}, L)$-isomorph. Also ist die Anzahl der mit einem Komponenten, etwa $\mathfrak{m}_1$, $(\mathfrak{H}, L)$-isomorphen Summanden in (*) gleich der der mit $\mathfrak{m}_1G$ $(\mathfrak{H}, L)$-isomorphen. Nun konstruieren wir für jeden Summanden $\mathfrak{m}_i$ den von ihm *induzierten* $(\mathfrak{G}, L)$-Modul $\overline{\mathfrak{M}}_i=\mathfrak{m}_iS_2+\cdots+\mathfrak{m}_iS_s$ $(\mathfrak{G}=\Sigma\mathfrak{H}S)$ (wo die Summe direkt ist), und dann die direkte Summe $\overline{\mathfrak{M}}=\Sigma\overline{\mathfrak{M}}_i$. Ferner führen wir einen Modul $\mathfrak{M}^s$ ein, der die direkte Summe von $s=(\mathfrak{G}:\mathfrak{H})$ mit $\mathfrak{M}$ isomorphen Moduln ist. Aus dem oben Bemerkten folgt dann leicht, dass $\overline{\mathfrak{M}}$ und $\mathfrak{M}^s$ als $(\mathfrak{H}, L)$-Moduln zueinander isomorph sind. Also sind sie auch als $(\mathfrak{G}, L)$ Moduln zueinander isomorph (Siehe Nakayama-Shoda, l.c., Satz 8 (für halbeinfachen Fall) und Osima, l.c., Satz 1 (für allgemeinen Fall)). Ist nun $\mathfrak{N}$ ein zweiter $(\mathfrak{G}, L)$-Modul und ist er als $(\mathfrak{H}, L)$-modul einem direkten Summanden von $\mathfrak{M}$ isomorph, so ist der entsprechende Modul $\overline{\mathfrak{N}}$ ersichtlich einem direkten Komponenten in $((\mathfrak{G}, L)$-Modul $\overline{\mathfrak{M}}$ isomorph. Dasselbe gilt dann für $\mathfrak{N}^s$ und $\mathfrak{M}^s$, also auch für $\mathfrak{N}$ und $\mathfrak{M}$ selbst. Somit ist bewiesen: *Ist ein* $(\mathfrak{G}, L)$*-Modul* $\mathfrak{N}$ *als* $(\mathfrak{H}, L)$*-Modul mit einem* $((\mathfrak{H}, L)$*-zulässigen, aber nicht notwendig* $\mathfrak{G}$*-zulässigen) direkten Summanden eines zweiten* $(\mathfrak{G}, L)$*-Moduls* $\mathfrak{M}$ *isomorph, so ist* $\mathfrak{N}$ *auch als* $(\mathfrak{G}, L)$*-Modul mit einem direkten Summanden in* $((\mathfrak{G}, L)$*-Modul)* $\mathfrak{M}$ *isomrph.*

Beim unendlich viele Elemente enthaltenden Grundkörper können wir analoge Sätze für (nicht direkten) Teilmodul und Restklassenmodul beweisen, etwa in analoger Weise wie bei Osima, Satz 1. Im Fall eines endlichen Grundkörpers bietet sich eine gewisse Schwierigkeit. Hierauf möchte ich an einer anderen Gelegenheit zurückkommen.

es ein Element ξ^* in $\mathfrak{L}^*$, dessen $(\mathfrak{L}^* : \mathfrak{K})$ $\mathfrak{K}$-Konjugierte über L linear unabhängig sind. Dann sind die $(\mathfrak{L} : \mathfrak{K})$ $\mathfrak{K}$-Konjugierten von $\xi = \mathrm{Sp}_{\mathfrak{L}^*/\mathfrak{L}}(\xi^*) \in \mathfrak{L}$ über L linear unabhängig, wie man unmittelbar einsieht.

Bemerkung. Im Falle $\mathfrak{L}^* = \mathfrak{L}$, $L = \mathfrak{K}$ reduziert sich der Satz auf den gewöhnlichen Satz der Normalbasis.

2. *Derivierte Basis.* Es sei in einem Körper $\mathfrak{K}$ eine (nicht triviale, d.h. nicht identisch verschwindende) abstrakte Derivation $a \longrightarrow a' = D(a)$ definiert, und $\mathfrak{L}$ sei ein endlicher separabler Oberkörper von $\mathfrak{K}$. D lässt sich in eindeutiger Weise auf L erweitern; wir bezeichnen die Erweiterungsderivation wieder mit D. L sei der Körper der D-Konstanten in $\mathfrak{L}$: $L = [a \mid D(a) = 0]$. Ist hier die Charakteristik von $\mathfrak{K}$ gleich 0, so haben wir $(\mathfrak{L} : L) = \infty$, $(\mathfrak{L}^* : L^*) = \infty$, also

$$(L^*\mathfrak{K} : L^*) = \infty,$$

wo $\mathfrak{L}^*$ der galoissche Körper von $\mathfrak{L}/\mathfrak{K}$ ist und L^* den Körper der D-Konstanten in $\mathfrak{L}^*$ bedeutet. Im Fall einer Primzahlcharakteristik p nehmen wir aber an, dass

$$(L^*\mathfrak{K} : L^*) \geqq (L^*\mathfrak{K} : \mathfrak{K})$$

ist;[5] dies ist sicher der Fall, sobald etwa $p \geqq (\mathfrak{L}^* : \mathfrak{K})$ (oder nur $\geqq (L^*\mathfrak{K} : \mathfrak{K})$) gilt. Als Anwendung unseres Satzes der halblinearen Normalbasis beweisen wir nun

Satz 2. *$\mathfrak{L}$ besitzt eine (D-)derivierte (oder differentiale)* Basis über $\mathfrak{K}$, *d.h. es gibt in $\mathfrak{L}$ ein ξ mit*

$$\mathfrak{L} = \xi\mathfrak{K} + \xi'\mathfrak{K} + \xi''\mathfrak{K} + \ldots + \xi^{(n-1)}\mathfrak{K}, \quad n = (\mathfrak{L} : \mathfrak{K})$$

(Strich bedeutet Derivation).

Beweis. Nach Satz 1 existiert in $\mathfrak{L}$ ein Element ξ, so dass seine n $\mathfrak{K}$-Konjugierten $\xi_1, \xi_2, \ldots, \xi_n$ linear unabhängig über L^* sind.[6] Dann ist die Wronskische Determinante $|\xi_i, \xi_i', \ldots, \xi_i^{(n-1)}| \neq 0$. Also sind $\xi, \xi', \ldots, \xi^{(n-1)}$ über $\mathfrak{K}$ linear unabhängig, den eine lineare Relation unter $\xi, \xi', \ldots, \xi^{(n-1)}$ würde dieselbe unter $\xi_i, \xi_i', \ldots, \xi_i^{(n-1)}$ $(i = 1, 2, \ldots, n)$ induzieren.

3. *Halblinearer Galoismodul.*[7] Nun kommen wir auf den Fall vom Nummer 1 des allgemeinen Körpers $\mathfrak{K}$ zurück, nehmen wir aber an, dass $\mathfrak{L}/\mathfrak{K}$

---

5) Dass diese Annahme für das Bestehen des folgenden Satzes 2 nicht überflüssig ist, sieht man etwa bei einem einfachen Beispiel der gewöhnlichen Derivation in einem rationalen Funktionenkörper mit einem Koeffizientenkörper der Charakteristik p ein. Vgl. auch die II. Mitteilung.

6) Theorem 1 bei Riblet, l.c.

7) Für Galoismoduln im gewöhnlichen Sinne siehe die zwe te der oben zitierten Arbeiten von M. Deuring (für halbeinfachen Fall) und die erste des Verfassers (für allgemeinen Fall).

galoissch ist, und betrachten ein Linksideal $\mathfrak{l}$ im halblinearen Gruppenring $(\mathfrak{G}, L)$ und sein Bild $\mathfrak{m}(\mathfrak{l}, \xi)$ bei dem ($(\mathfrak{G}, L)$-Operator-)Isomorphismus zwischen $(\mathfrak{G}, L)$ und $\xi^{G_1}L+\xi^{G_2}L+\cdots+\xi^{G_g}L$; Wir nennen diesen Modul $\mathfrak{m}(\mathfrak{l}, \xi)$ den zu $\mathfrak{l}$ gehörigen halblinearen Galoismodul (über L) bezüglich ξ. Ist

$$\xi^{G_1}L+\xi^{G_2}L+\cdots+\xi^{G_g}L=\eta^{G_1}L+\eta^{G_2}L+\cdots+\eta^{G_g}L$$

mit einem zweiten Element η in $\mathfrak{L}$, so fällt $\mathfrak{m}(\mathfrak{l}, \xi)$ mit $\mathfrak{m}(\mathfrak{l}, \eta)$ zusammen; denn bei jedem Automorphismus von $(\mathfrak{G}, L)$ als Rechtsideal wird jedes Linksideal auf sich selbst abgebildet. *Ferner wird das Linksideal $\mathfrak{l}$ von dem zugehörigen Modul $\mathfrak{m}=\mathfrak{m}(\mathfrak{l}, \xi)$ eindeutig bestimmt*, d.h. aus $\mathfrak{m}(\mathfrak{l}, \xi)=\mathfrak{m}(\mathfrak{l}_1, \zeta)$ folgt $\mathfrak{l}=\mathfrak{l}_1$. $\mathfrak{l}$ ist ja das Links-Annulatorideal der Elemente a in $(\mathfrak{G}, L)$ mit $\mathfrak{m}^a=0$, man ersieht dies leicht daraus, dass der halblineare Gruppenring $(\mathfrak{G}, L)$ vom Frobeniusschen Typ ist.[8]

Es sei nun $\mathfrak{R}_1$ ein Zwischenkörper von $\mathfrak{L}/\mathfrak{R}$, und $\mathfrak{G}_1$ die zugehörige Untergruppe von $\mathfrak{G}$. Ist L_1^* der von L und seinen $\mathfrak{R}_1$-Konjugierten erzeugte Körper, so gilt

$$\begin{aligned}(L_1^*\mathfrak{R}_1 : L_1^*)&=(L^*\mathfrak{R}_1 : L^*)(L^* : L_1^*)/(L^*\mathfrak{R}_1 : L_1^*\mathfrak{R}_1)\\ &\geqq(L^*\mathfrak{R}_1 : \mathfrak{R})(L^* : L_1^*)/(L^*\mathfrak{R}_1 : L_1^*\mathfrak{R}_1)\\ &=(L_1^*\mathfrak{R}_1 : \mathfrak{R})(L^* : L_1^*)\geqq(L_1^*\mathfrak{R}_1 : \mathfrak{R})\geqq(L_1^*\mathfrak{R}_1 : \mathfrak{R}_1).\end{aligned}$$

Ausserdem sind die $\mathfrak{R}_1$-Konjugierten von ξ linear unabhängig über L. Wir haben nun

Satz 3. *Es sei $\mathfrak{m}$ ein zum Linksideal $\mathfrak{l}$ gehöriger (halblinearer) Galoismodul über L bei $\mathfrak{L}/\mathfrak{R}$ derart, dass für jedes $\lambda(\neq 0)$ aus $\mathfrak{R}_1$ das Produkt $\lambda\mathfrak{m}$ wieder ein demselben Linksideal $\mathfrak{l}$ zugehöriger Galoismodul (bezüglich eines vielleicht von dem ursprünglichen verschiedenen Bezugselement) ist. So ist*

$$\mathfrak{l}=(\mathfrak{G}, L)\mathfrak{l}_1 \qquad (\mathfrak{l}_1=\mathfrak{l}\frown(\mathfrak{G}_1, L)),$$

und $\mathfrak{m}$ ist die direkte Summe von $(\mathfrak{R}_1 : \mathfrak{R})$ zu $\mathfrak{l}_1$ gehörigen Galoismoduln in $\mathfrak{L}/\mathfrak{R}_1$.[9]

Beweis. Es sei $\mathfrak{r}=r(\mathfrak{l})$ der Rechts-Annulator von $\mathfrak{l}$ in $(\mathfrak{G}, L)$. Für $a\in\mathfrak{m}$, $\Sigma_G G\rho_G\in\mathfrak{r}$ haben wir $\Sigma a^G\rho_G=0$. Wegen unserer Annahme über $\mathfrak{m}$ gilt weiter

$$\Sigma\lambda^G a^G\rho_G=\Sigma_T\lambda^T\Sigma_{A\in G_1}a^{AT}\rho_{AT}=0$$

für jedes λ aus $\mathfrak{R}_1$, wo $\mathfrak{G}=\Sigma_T\mathfrak{G}_1 T$ die rechtsseitige Zerlegung von $\mathfrak{G}$ bezüglich $\mathfrak{G}_1$ ist. Da die Diskriminante $|\lambda_i^T|^2$ von $\mathfrak{R}_1/\mathfrak{R}$ nicht verschwindet, bekommen wir daraus $\Sigma_A a^{AT}\rho_{AT}=0$, oder

$$\Sigma_A a^A\rho_{AT}^{T^{-1}}=0.$$

---

8) Siehe Nakayama, l.c.

9) Die vom Linksideal $\mathfrak{l}$ definierte (halblineare) Darstellung von $\mathfrak{G}$ ist die sogenannte von der zu $\mathfrak{l}_1$ gehörigen Darstellung von $\mathfrak{G}_1$ *induzierte*.

Weil aber diese Berechnung umgekehrt werden kann, so überzeugen wir uns davon, dass $\mathfrak{m}$ aus allen diese letzten Relationen erfüllenden Elementen aus $\Sigma\xi^G L$ besteht, wo ξ das Bezugselement von $\mathfrak{m}$ ist. Also muss $\mathfrak{l}$ mit dem Links-Annulator $l(\Sigma_A \rho_{AT}^{T^{-1}})$ der Elemente $\Sigma A\rho_{AT}^{T^{-1}}$ in $(\mathfrak{G}, L)$ zusammenfallen. Da hier $\Sigma A\rho_{AT}^{T^{-1}} \in (\mathfrak{G}_1, L)$ sind, gilt $\mathfrak{l}=(\mathfrak{G}, L)\mathfrak{l}_1$, wo $\mathfrak{l}_1=\mathfrak{l}\frown(\mathfrak{G}_1, L)$ der Links-Annulator von $\Sigma A \rho_{AT}^{T^{-1}}$ in $(\mathfrak{G}_1, L)$ ist. Ferner ist $\Sigma\xi^G L=\Sigma_U\Sigma_A\xi^{UA}(\mathfrak{G}=\Sigma_U U\mathfrak{G}_1)$, wobei jeder Summand $\Sigma_A\xi^{UA}L$ als $(\mathfrak{G}_1, L)$-Modul mit $(\mathfrak{G}_1, L)$ isomorph ist. Bezeichnet man also mit $\mathfrak{m}_U$ den zum Linksideal $\mathfrak{l}_1$ in $(\mathfrak{G}_1, L)$, Links-Annulator von $\Sigma A \rho_{AT}^{T^{-1}}$, gehörigen $\mathfrak{L}/\mathfrak{H}_1$-Galoismodul bezüglich ξ^U, so ist es nach der obigen Betrachtung klar, dass $\mathfrak{m}$ die direkte Summe $\Sigma_U\mathfrak{m}_U=\Sigma_U\mathfrak{m}(\mathfrak{l}_1, \xi^U)$ ist, was den Satz nachweist.

Zusatz bei der Korrektur (Apr. 8, 1948): Für ein supplementäres Argument, welches im Fall vom unendlichen $(\mathfrak{L}: L)$ bezüglich der Fussnote 4) notwendig ist, vgl. eine demnächst in Amer. J. Math. erscheinende Note des Verfassers: Semilinear normal basis for quasifields. Siehe auch T. Nakayama, Galois theory for general rings with minimum condition, erscheint demnächst in Jour Math. Soc. Japan, wo eine direktere Einführung des Satzes des halblinearen Normalbasis gegeben ist.