2. *Struktur der Divisionsalgebren über diskret bewerteten perfekten Körpern.*

Von Mikao MORIYA.
Mathematisches Institut der Kaiserlichen Hokkaido Universität, Sapporo.
(Comm. by T. TAKAGI, M.I.A., Jan. 12, 1942.)

1. Es sei k ein perfekter Körper in bezug auf eine (Exponenten-) Bewertung w, und D eine Divisionsalgebra vom Range m mit k als Koeffizientenkörper. Dann kann man stets die Bewertung w von k auf eine einzige und zwar auf folgende Weise in D fortsetzen:

Ist α ein Element aus D und $f(x)=x^\mu+\cdots+a_\mu$ das Minimalpolynom von α über k, so setze man: $w(\alpha)=\frac{1}{\mu}\big(w(a_\mu)\big)$. Wie man leicht bestätigt, genügt w allen Bewertungspostulaten[1], und die Divisionsalgebra D ist perfekt in bezug auf w[2]. Die Wertgruppe $w(D)$ von D nach w enthält die Wertgruppe $w(k)$ als eine Untergruppe; berücksichtigt man dabei, daß der Rang m von D stets durch den Grad des Minimalpolynomes eines Elementes aus D teilbar ist, so überzeugt man sich leicht davon, daß die Faktorgruppe $w(D)/w(k)$ eine additive Gruppe vom Exponenten m ist.

Ein Element α aus D heißt in bezug auf w *ganz*, wenn $w(\alpha)\geqq 0$ ist. Die Gesamtheit $\mathfrak{O}$ aller, in bezug auf w, ganzen Elemente aus D bildet einen Ring, welcher den Bewertungsring von k als einen Teilring enthält. Anderseits stimmt $\mathfrak{O}$ mit der Menge aller, in bezug auf den Bewertungsring von k, ganzen Elemente aus D überein. Wenn man in D den zu w gehörigen Primdivisor mit $\mathfrak{P}$ bezeichnet und den Restklassenring $\mathfrak{D}$ von D nach $\mathfrak{P}$ wie üblich definiert, so ist $\mathfrak{D}$ ein Schiefkörper, welcher den Restklassenkörper $\mathfrak{k}$ von k nach dem zu w gehörigen Primdivisor $\mathfrak{p}$ aus k als einen Teilkörper enthält. Nun wollen wir beweisen:

Satz 1. *Die Ordnung von $w(D)/w(k)$ und der Rang von $\mathfrak{D}$ über $\mathfrak{k}$ sind stets endlich. Ferner gilt:*

$$\big(w(D):w(k)\big)\,(\mathfrak{D}:\mathfrak{k})\leqq m\,.$$

Beweis. $\bar{\omega}_1, \bar{\omega}_2, \ldots, \bar{\omega}_\mu$ seien Elemente aus $\mathfrak{D}$, welche über $\mathfrak{k}$ linear unabhängig sind, und ferner seinen $\bar{\lambda}_1, \bar{\lambda}_2, \ldots, \bar{\lambda}_\nu$ voneinander unabhängige Elemente aus $w(D)/w(k)$. Da $w(D)/w(k)$ vom Exponenten m ist, so ist die Ordnung von jedem $\bar{\lambda}_i$ stets endlich, wir bezeichnen sie durch e_i. Nun bezeichnen wir mit ω_i ein zur Restklasse $\bar{\omega}_i$ gehöriges Element aus D und mit λ_i ein Element aus D mit $w(\lambda_i)=\bar{\lambda}_i$. Die $\mu e_1\cdots e_\nu$ Elemente

1) Vgl. hierzu etwa O. F. G. Schilling und M. Moriya, Divisionsalgebren über unendlichen perfekten Körpern, Journ. of Science, Hokkaidô Imp. Univ., Ser. I. Vol. 6 (1937), S. 103–105.

2) Van der Waerden, Moderne Algebra, I. Teil, 2. Aufl. (1937), S. 263–264.

$$\omega_i \lambda_1^{x_{i1}} \dots \lambda_\nu^{x_{i\nu}} \qquad \begin{array}{l} i=1, \dots, \mu \\ 0 \leqq x_{ij} \leqq e_j - 1, j=1, \dots, \nu \end{array}$$

sind über k linear unabhängig. Gilt nämlich eine lineare Relation

$$L(\omega, \lambda) = \sum_{i=1}^{\mu} \left\{ c(i; x_{i1}, \dots, x_{i\nu}) \lambda_1^{x_{i1}} \dots \lambda_\nu^{x_{i\nu}} + c(i; y_{i1}, \dots, y_{i\nu}) \lambda_1^{y_{i1}} \dots \lambda_\nu^{y_{i\nu}} + \cdots \right\} \omega_i = 0$$

für nicht alle verschwindenden Elemente $c(i; x_{i1}, \dots, x_{i\nu})$, $c(i; y_{i1}, \dots, y_{i\nu})$, $\dots$ aus k, so gibt es nach einem Bewertungspostulat zwei nicht verschwindende Summanden $c(i; s_{i1}, \dots, s_{i\nu})\, \omega_i \lambda_1^{s_{i1}} \dots \lambda_\nu^{s_{i\nu}}$, $c(j; t_{j1}, \dots, t_{j\nu}) \omega_j \lambda_1^{t_{j1}} \dots \lambda_\nu^{t_{j\nu}}$, deren Bewertungen einander gleich sind. Es besteht also:

$$\sum_{r=1}^{\nu} (s_{ir} - t_{jr})\, w(\lambda_r) = -w\big(c(i; s_{i1}, \dots, s_{i\nu})\big) + w\big((j; t_{j1}, \dots, t_{j\nu})\big)$$
$$-w(\omega_i) + w(\omega_j) \in w(k)\,,$$

weil $w(\omega_i) = 0 = w(\omega_j)$ ist. Da $w(\lambda_r) = \bar{\lambda}_r$ ist, so muß für jedes r $s_{ir} = t_{jr}$ sein. Betrachtet man also in $L(\omega, \lambda)$ alle Summanden, deren Bewertungen am kleinsten sind, so besitzen sie für ein passend gewähltes Zahlensystem $a_1, \dots, a_\nu$ das Produkt $\lambda_1^{a_1} \dots \lambda_\nu^{a_\nu}$ als einen gemeinsamen Faktor. Es seien $c(i_1; a_1, \dots, a_\nu)\, \omega_{i_1} \lambda_1^{a_1} \dots \lambda_\nu^{a_\nu}$, $c(i_2, a_1, \dots, a_\nu)\, \omega_{i_2} \lambda_1^{a_1} \dots \lambda_\nu^{a_\nu}$, $\dots$, $c(i_s; a_1, \dots, a_\nu)\, \omega_{i_s} \lambda_1^{a_1} \dots \lambda_\nu^{a_\nu}$ die sämtlichen derartigen Summanden in $L(\omega, \lambda)$. Dann gilt offenbar folgende Ungleichung:

$$w(c_1 \omega_{i_1} + c_2 \omega_{i_2} + \cdots + c_s \omega_{i_s}) > 0\,,$$

worin $c_1, \dots, c_s$ bzw. die Quotienten von $c(i_1; a_1, \dots, a_\nu)$, $c(i_2; a_1, \dots, a_\nu)$ $\dots$, $c(i_s; a_1, \dots, a_\nu)$ durch $c(i_1; a_1, \dots, a_\nu)$ bezeichnen. Beziechnet man nun mit $\bar{c}_1, \dots . \bar{c}_s$ bzw. die $c_1, \dots, c_s$ enthaltenden Restklassen aus $\mathfrak{k}$, so entsteht beim Übergang in die Restklassendivisionsalgebra $\mathfrak{D}$ die Gleichung $\bar{c}_1 \bar{\omega}_{i_1} + \cdots + \bar{c}_s \bar{\omega}_{i_s} = 0$, weil $w(c_1 \omega_{i_1} + \cdots + c_s \omega_{i_s}) > 0$ ist. Wegen $c_1 = 1$ würden $\bar{\omega}_{i_1}, \dots, \bar{\omega}_{i_s}$, entgegen der Annahme, über k linear abhängig sein. Es müssen also die $\mu e_1 \dots e_\nu$ Elemente $\omega_i \lambda_1^{x_{i1}} \dots \lambda_\nu^{x_{i\nu}}$ über k linear unabhängig sein. Da der Rang von D über k gleich m ist, so ist stets $\mu e_1 \dots e_\nu \leqq m$.

Wäre nun mindestens eines von $(\mathfrak{D} : \mathfrak{k})$ und $\big(w(D) : w(k)\big)$ unendlich, so könnte man aus D wie oben die $\mu e_1 \dots e_\nu$, über k linear unabhängigen Elemente $\omega_i \lambda_1^{x_{i1}} \dots \lambda_\nu^{x_{i\nu}}$ herausgreifen, deren Anzahl $\mu e_1 \dots e_\nu$ größer ist als m. Hieraus schließt man sofort, daß $w(D)/w(k)$ und $(\mathfrak{D} : \mathfrak{k})$ endlich sind, und ferner $\big(w(D) : w(k)\big)\, (\mathfrak{D} : \mathfrak{k}) \leqq m$ ist.

Im folgenden nennen wir $\big(w(D) : w(k)\big)$ bzw. $(\mathfrak{D} : \mathfrak{k})$ die *Verzweigungsordnung* bzw. den *Restklassengrad* von D über k.

Nun beschränken wir uns auf einen Spezialfall, wo die Bewertung w von k *diskret* ist. Dann wird die Fortsetzung von w in D, wie leicht bestätigt wird, auch diskret; die Faktorgruppe $w(D)/w(k)$ ist also *zyklisch*. Wenn man mit Π ein Primelement des Primdivisors $\mathfrak{P}$ von D bezeichnet, so gilt für ein Primelement π von $\mathfrak{p}$ aus k:

$$\pi = \eta \Pi^e ,$$

wo η eine Einheit aus D bezeichnet. Der Exponent e ist bekanntlich gleich der Ordnung von $w(D)/w(k)$. Wählt man nun in k ein vollständiges Restsystem S mod. $\mathfrak{p}$ fest, und bezeichnet mit $\omega_1, \cdots, \omega_f$ ein Repräsentantensystem einer Basis $\bar{\omega}_1, \cdots, \bar{\omega}_f$ von $\mathfrak{D}$ über $\mathfrak{k}$, so ist ein von Null verschiedenes Element α aus D als eine unendliche Reihe von der Form:

$$\alpha = \sum_{\substack{-\infty < \nu \\ 0 \leq t < e}} \left(a_1(\nu, t)\,\omega_1 + \cdots + a_f(\nu, t)\,\omega_f\right) \pi^\nu \Pi^t ,$$

wobei die Koeffizienten $a_1(\nu, t), \cdots, a_f(\nu, t)$ aus S herausgegriffen sind. Durch eine leichte Umformung erhält man aus der obligen unendlichen Reihe: $\alpha = \sum_{i=1}^{f} \sum_{0 \leq t < e} \omega_i \Pi^t \sum_{-\infty < \nu} a_i(\nu, t)\pi^\nu$. Da $\sum_{-\infty < \nu} a_i(\nu, t)\pi^\nu$ als eine konvergente Reihe ein Elemente aus k ist, so ist der Rang von D über k nicht größer als ef. Mit Hilfe von Satz 1 folgt nun

Satz 2. *Wenn die Bewertung w von k diskret ist, so gilt für den Rang m einer Divisionsalgebra D mit k als Koeffizientenkörper:*

$$m = ef .$$

Dabei bezeichnet e bzw. f die Verzweigungsordnung bzw. den Restklassengrad von D über k.

2. In diesem Abschnitt bezeichnet $\mathfrak{k}$ einen Körper mit folgenden Beschaffenheiten:

1) $\mathfrak{k}$ *ist vollkommen.*
2) *Zu einer beliebigen natürlichen Zahl n existiert höchstens eine algebraische Erweiterung vom Grade n über $\mathfrak{k}$.*

Zunächst bemerken wir, daß jede endliche algebraische Erweiterung über $\mathfrak{k}$ stets *separabel zyklisch* ist. Ist nämlich $\mathfrak{K}$ eine algebraische Erweiterung vom Grade n über $\mathfrak{k}$, so existieren über $\mathfrak{k}$ genau n zu $\mathfrak{K}$ konjugierte Körper, welche nach Voraussetzung miteinander übereinstimmen müssen; d. h. $\mathfrak{K}$ ist über $\mathfrak{k}$ *separabel galoissch.* Sind nun $p_1, p_2, \cdots, p_r$ die sämtlichen verschiedenen Primteiler von n, so besitzt die Galoisgruppe $\mathfrak{G}$ von $\mathfrak{K}/\mathfrak{k}$ nach Voraussetzung genau eine einzige zu p_i gehörige Sylowgruppe $\mathfrak{G}_i$. Hieraus schließt man leicht, daß $\mathfrak{G}$ als ein direktes Produkt aus $\mathfrak{G}_1, \cdots, \mathfrak{G}_r$ darstellbar ist. Da nach Voraussetzung und nach dem Hauptsatz der galoisschen Theorie die Gruppe $\mathfrak{G}_i$ nur eine einzige Untergruppe vom Index p_1 enthält, so ist sie *zyklisch,* es ist also $\mathfrak{G}$ zyklisch von der Ordnung n[1].

Hilfssatz 1. Jede endliche algebraische Erweiterung $\mathfrak{K}$ über $\mathfrak{k}$ besitzt auch die Beschaffenheiten 1) und 2).

Beweis. Eine beliebige algebraische Erweiterung über $\mathfrak{K}$ ist auch über $\mathfrak{k}$ algebraisch, sie ist also über $\mathfrak{k}$, erst recht über $\mathfrak{K}$, separabel.

Gäbe es nun über $\mathfrak{K}$ zwei verschiedene separable Erweiterungen vom Grade m, so existieren auch über $\mathfrak{k}$ zwei verschiedene Erweiterungen vom Grade $m(\mathfrak{K}:\mathfrak{k})$, was aber ein Widerspruch ist.

Hilfssatz 2. Ist $\mathfrak{K}$ eine endliche algebraische Erweiterung über $\mathfrak{k}$, so ist jedes Element aus $\mathfrak{k}$ stets *Norm* eines Elementes aus $\mathfrak{K}$.

1) A. Speiser, Theorie der Gruppen von endlicher Ordnung, 3. Aufl. (1937), S. 70–71.

Beweis. Zunächst beweisen wir den Satz für den Fall, wo $(\mathfrak{K}:\mathfrak{k})=l$ eine Primzahl ist. Dazu betrachten wir die Gleichung $x^l-a=0$ mit $a\in\mathfrak{k}$ und unterscheiden zwei Fälle:

i) x^l-a ist reduzibel in $\mathfrak{k}[x]$.

Dann existiert in $\mathfrak{k}$ ein Element c mit $c^l=a$, also ist $N_{\mathfrak{K}\mathfrak{k}}(c)=c^l=a$. *Der Fall* i) *tritt immer ein, wenn die Charakteristik von* $\mathfrak{k}$ *gleich* l *ist,* weil sonst über $\mathfrak{k}$ eine inseparable Erweiterung existieren müsste.

ii) x^l-a ist irreduzibel in $\mathfrak{k}[x]$.

Da die Charakteristik von $\mathfrak{k}$ von l verschieden ist, so ist $\mathfrak{K}=\mathfrak{k}(\sqrt[l]{a})$

a) l ist ungerade. In diesem Fall ist sicher $N_{\mathfrak{K}\mathfrak{k}}(\sqrt[l]{a})=a$.

b) l ist gerade. Dann genügt es nur zu zeigen, daß -1 Norm eines Elementes ε aus $\mathfrak{K}$, weil dabei $N_{\mathfrak{K}\mathfrak{k}}(\varepsilon\sqrt{a})=(-1)(-a)=a$ ist. Angenommen, es wäre -1 keine Norm der Elemente aus $\mathfrak{K}$. Dann gehört $i=\sqrt{-1}$ nicht zu $\mathfrak{k}$, weil sonst $N_{\mathfrak{K}\mathfrak{k}}(i)=-1$ wird. Nach Voraussetzung ist $\mathfrak{K}=\mathfrak{k}(i)$. Wir betrachten nun über $\mathfrak{k}$ den biquadratischen Körper $\bar{\mathfrak{K}}$, welcher nach Voraussetzung den Körper $\mathfrak{K}$ enthält und über $\mathfrak{K}$ quadratisch ist. Es sei $x^2-(a+ib)=0$ eine definierende Gleichung von $\bar{\mathfrak{K}}$ über $\mathfrak{K}$, wo a, b Elemente aus $\mathfrak{k}$ bezeichnen.

Betrachtet man dann die Elemente $\sqrt{a^2+b^2}$ und $\sqrt{-(a^2+b^2)}$, so können die beiden Elemente nicht gleichzeitig zu $\mathfrak{k}$ gehören, weil sonst $\sqrt{-1}$ zu $\mathfrak{k}$ gehören müsste. Nimmt man nun an, daß $\sqrt{-(a^2+b^2)}$ zu $\mathfrak{k}$ gehört, so gibt es ein Element c aus $\mathfrak{k}$ mit $c^2=-(a^2+b^2)$, woraus entgegen der Annahme $-1=N_{\mathfrak{K}\mathfrak{k}}\left(\frac{a}{c}+i\frac{b}{c}\right)=\left(\frac{a}{c}\right)^2+\left(\frac{b}{c}\right)^2$ folgt. $\sqrt{a^2+b^2}$ muß daher Element aus $\mathfrak{k}$ sein, weil sonst nach der Theorie der Kummerschen Körper -1 ein Quadrat eines Elementes aus $\mathfrak{k}$ sein müsste. Setzt man nun $r=\sqrt{a^2+b^2}$, so ist das Element $\alpha=\sqrt{r}\left(\sqrt{\frac{r+a}{2r}}+i\sqrt{\frac{r-a}{2r}}\right)$ offenbar eine Nullstelle von $x^2-(a+ib)$, wenn $\sqrt{\frac{r+a}{2r}}$, $\sqrt{\frac{r-a}{2r}}$ von vornherein so normiert sind, daß $\sqrt{\frac{r+a}{2r}}\sqrt{\frac{r-a}{2r}}=\frac{b}{2r}$ wird. Offenbar ist α Element aus $\mathfrak{K}=\mathfrak{k}(i)$, es ist also entgegen der Annahme $x^2-(a+ib)$ in $\mathfrak{K}[x]$ reduzibel; -1 muß daher Norm eines Elementes aus $\mathfrak{K}$ sein.

Es sei $\mathfrak{K}$ eine endliche algebraische Erweiterung vom Grad n über $\mathfrak{k}$. Dann nehmen wir an, daß für alle Erweiterungen $\mathfrak{K}'$, deren Grade nach $\mathfrak{k}$ kleiner sind als n, der Satz schon bewiesen ist. Da nach dem oben Bemerkten $\mathfrak{K}$ über $\mathfrak{k}$ separabel zyklisch ist, so existiert zwischen $\mathfrak{K}$ und $\mathfrak{k}$ ein Zwischenkörper $\mathfrak{K}'$, über dem $\mathfrak{K}$ von Primzahlgrad ist. Ein Element a aus $\mathfrak{k}$ ist nach Induktionsannahme Norm eines Elementes a' aus $\mathfrak{K}'$, welches seinerseits auch Norm eines Elementes α aus $\mathfrak{K}$ ist; es ist wie bekannt $a=N_{\mathfrak{K}\mathfrak{k}}(\alpha)$.

Satz 3. *Über* $\mathfrak{k}$ *existiert keine echte normale Divisionsalgebra*[1].

Beweis. Wäre $\mathfrak{D}$ eine normale Divisionsalgebra vom Grade $n(>1)$

1) Hierzu vgl. auch R. Brauer, Konstruktion der Schiefkörper von endlicher Rang, Crelle's Journ., Bd. 168 (1932), S. 60.

über $\mathfrak{k}$, so besäße $\mathfrak{D}$ einen Zerfällungskörper $\mathfrak{Z}$ vom Grade n über $\mathfrak{k}$[1], welcher nach dem oben Bemerkten über $\mathfrak{k}$ zyklisch ist; $\mathfrak{D}$ ist also eine zyklische Algebra über $\mathfrak{k}$ und infolgedessen von der Form: $\mathfrak{D}=(a, \mathfrak{Z}, S)$. Da nach Hilfssatz 2 a Norm eines Elementes aus $\mathfrak{K}$ ist, so ist $\mathfrak{D}$ eine vollständige Matrixalgebra über $\mathfrak{k}$, was aber ein Widerspruch ist[2].

3. In diesem Abschnitt bezeichnet k durchweg einen *diskret perfekten* Körper in bezug auf einen Primdivisor $\mathfrak{p}$. Ferner besitze der Restklassenkörper $\mathfrak{k}$ von k nach $\mathfrak{p}$ die folgenden Beschaffenheiten:

1) $\mathfrak{k}$ *ist vollkommen.*

2) *Zu einer beliebigen natürlichen Zahl n existiert genau eine algebraische Erweiterung vom Grade n über* $\mathfrak{k}$.

Dann gilt nach Satz 2 für eine endliche algebraische Erweiterung K stets:

$$(K:k)=ef,$$

wobei e bzw. f die Verzweigungsordnung bzw. den Restklassengrad von K über k bezeichnet. Wenn insbesondere K über k *separabel* ist, so ist der *Trägheitskörper* W von K über k zyklisch, weil der Restklassenkörper $\mathfrak{K}$ von K stets über k separabel zyklisch ist; ferner ist offenbar $(W:k)=f=(\mathfrak{K}:\mathfrak{k})$[3]. Wir können auch leicht bestätigen, daß eine endliche separable, unverzweigte Erweiterung K über k stets über k zyklisch ist. Nun beweisen wir folgenden

Hilfssatz 3. Ist W der Trägheitskörper einer endlichen separablen Erweiterung über k, so ist jede Einheit aus k Norm einer Einheit aus W.

Beweis. Es sei ε_0 eine Einheit aus k, und $\bar{\varepsilon}_0$ die ε_0 enthaltende Restklassen aus $\mathfrak{k}$. Da nach Hilfssatz 2 jedes Element aus $\mathfrak{k}$ Norm eines Elementes aus dem Restklassenkörper $\mathfrak{K}$ von W ist, so gibt es in W ein Element ε derart, daß für die ε enthaltende Restklasse $\bar{\varepsilon}$ aus $\mathfrak{K}$ $N_{\mathfrak{K}\mathfrak{k}}(\bar{\varepsilon})=\bar{\varepsilon}_0$ gilt.

Betrachtet man jetzt die Norm $N_{Wk}(\varepsilon)$ und berücksichtigt die Tatsache, daß die Galoisgruppe $\mathfrak{K}/\mathfrak{k}$ zu der von W/k isomorph ist, so schließt man sofort, daß $\overline{N_{Wk}(\varepsilon)}=N_{\mathfrak{K}\mathfrak{k}}(\bar{\varepsilon})=\bar{\varepsilon}_0$ ist, wobei $\overline{N_{Wk}(\varepsilon)}$ die $N_{Wk}(\varepsilon)$ enthaltende Restklasse aus k bezeichnet. Hieraus folgt ohne weiteres:

$$\frac{\varepsilon_0}{N_{Wk}(\varepsilon)}\equiv 1 \text{ mod. } p\,;$$

d. h. $\dfrac{\varepsilon_0}{N_{Wk}(\varepsilon)}$ ist eine Einseinheit aus k. Da jede Einseinheit aus k Norm einer Einheit aus W ist[4], so wird ε_0 Norm einer Einheit aus W.

Da W über k (eigentlich-) unverzweigt ist, so ist $\mathfrak{p}$ auch der Primdivisor aus W. Eine Potenz π^ν eines Primelementes π von $\mathfrak{p}$ aus k ist

---

1) Vgl. etwa M. Deuring, Algebren, Ergebnisse d. Math. u. ihrer Grenzgebiete, VI. Bd. (1935), S. 47.

2) Vgl. etwa M. Deuring, loc. cit., S. 65.

3) Hierzu vgl. etwa M. Moriya, Einige Eigenschaften der endlichen separablen algebraischen Erweiterungen über perfekten Körpern, Proc. **17** (1941), 406.

4) M. Moriya, loc. cit., S. 408–409.

also dann und nur dann Norm eines Elementes aus W, wenn ν durch $(W:k)$ teilbar ist. Hieraus folgt mit Hilfe von Hilfssatz 3:

Zusatz zu Hilfssatz 3. Bezeichnet A die Gesamtheit aller von Null verschiedenen Elemente aus k, so ist die Faktorgruppe A nach der W zugeordneten Normgruppe[1] zyklisch von der Ordnung $(W:k)$.

Ist nun über k ein algebraisch-abgeschlossener Körper Ω festgelegt, so existiert zu einer gegebenen natürlichen Zahl n eine eigentlich-unverzweigte, separable zyklische Erweiterung W_n über k aus Ω. Nämlich nach Voraussetzung über k existiert stets eine separable zyklische Erweiterung $\mathfrak{Z}$ vom Grade n über $\mathfrak{k}$. Es bezeichne $\bar{f}(x)=\bar{a}_0x^n+\cdots+\bar{a}_n=0$ eine definierende Gleichung von $\mathfrak{Z}$ über $\mathfrak{k}$. Sind dann $a_0, \ldots, a_n$ bzw. die zu den Restklassen $\bar{a}_0, \ldots, \bar{a}_n$ gehörigen Elemente aus k, so ist $f(x)=a_0x^n+\cdots+a_n$ offenbar ein separables Polynom aus $k[x]$. Bezeichnet nun θ eine Nullstelle von $f(x)$ aus Ω, so ist $\big(k(\theta):k\big)=n$. Die θ enthaltende Restklasse $\bar{\theta}$ aus $k(\theta)=W_n$ genügt im Restklassenkörper von W_n der Gleichung $\bar{f}(x)=0$; d. h. $\mathfrak{k}(\bar{\theta})$ ist äquivalent zu $\mathfrak{Z}$ über $\mathfrak{k}$. Da der Restklassenkörper von W_n den Körper $\mathfrak{k}(\bar{\theta})$ enthält und $\big(\mathfrak{k}(\bar{\theta}):\mathfrak{k}\big)=n=(W_n:k)$ ist, so ist W_n eigentlich-unverzweigt vom Grade n über k, und infolgedessen über k zyklisch.

Wir beweisen weiter, daß in Ω eine einzige separable zyklische, eigentlich-unverzweigte Erweiterung W_n vom Grade n über k existiert. Angenommen, es wäre W'_n ein anderer Teilkörper von Ω/k als W_n, welcher über k separabel zyklisch, und eigentlich-unverzweigt vom Grade n ist. Dann überzeugt man sich leicht davon, daß das Kompositum $W_nW'_n$ von W_n und W'_n auch über k unverzweigt ist, und folglich über k separabel zyklisch ist. Dies ist aber ein Widerspruch, weil sonst $W_nW'_n$ zwei verschiedene Erweiterungen vom Grade n über k als Teilkörper enthielte. Wir haben somit folgenden Hilfssatz bewiesen:

Hilfssatz 4. In einem festgelegten algebraisch-abgeschlossenen Körper über k existiert zu einer beliebigen natürlichen Zahl n genau eine separable, unverzweigte Erweiterung W_n vom Grade n über k, und zwar ist W_n stets über k zyklisch.

Nun betrachten wir eine *normale* Divisionsalgebra D vom Grade n über k, und bezeichnen mit $\mathfrak{P}$ den Primdivisor von D, welcher der Primteiler des Primdivisors $\mathfrak{p}$ von k ist. Da der Rang von D über k gleich n^2 ist, so gilt nach Satz 2: $n^2=ef$, wo e, f bzw. die Verzweigungsordnung und den Restklassengrad von D über k bezeichnen. Die Restklassenring von D nach $\mathfrak{P}$ wird nach Satz 3 stets ein *kommutativer* Körper; wir bezeichnen ihn mit $\mathfrak{K}$.

Da nach Voraussetzung $\mathfrak{K}$ über $\mathfrak{k}$ endlich separabel ist, so existiert ein primitives Element $\bar{\xi}$ von $\mathfrak{K}$ über $\mathfrak{k}$. Es sei $\bar{f}(x)=\bar{a}_0x^f+\cdots+\bar{a}_f$ ein separables Polynom aus $\mathfrak{k}[x]$, dessen eine Nullstelle aus $\mathfrak{K}$ $\bar{\xi}$ ist. Ist dann ξ ein zu $\bar{\xi}$ gehöriges Element aus D, und sind $a_0, \ldots, a_f$ bzw. die zu $\bar{a}_0, \ldots, \bar{a}_f$ gehörigen Elemente aus k, so gilt im Körper $k(\xi)$ die Kongruenz:

1) Die W zugeordnete Normgruppe besteht aus den Normen der von Null verschiedenen Elemente aus W nach k.

$$f(x)=a_0x^f+\cdots+a_f\equiv(x-\xi)h(x) \text{ mod. } \mathfrak{P}_0,$$

wo $\mathfrak{P}_0$ den Primteiler von $\mathfrak{p}$ aus $k(\xi)$ und $h(x)$ ein Polynom von x mit den für $\mathfrak{P}_0$ ganzen Koeffizienten aus $k(\xi)$ bezeichnet. Es ist dabei nicht schwer zu zeigen, daß $f(x)$ in $k(\xi)$ eine Nullstelle besitzt, weil $x-\xi$ und $h(x)$ mod. $\mathfrak{P}_0$ einander teilerfremd sind[1]. Der Einfachheit halber wollen wir annehmen, daß ξ von vornherein als eine Nullstelle von $f(x)$ gewählt ist. Dann ist $k(\xi)$ offenbar über k separabel, weil $\bar{f}(x)$ in $\mathfrak{k}[x]$ und folglich $f(x)$ in $k[x]$ separabel ist. $k(\xi)$ ist daher eigentlich-unverzweigt vom Grade f über k. Da $k(\xi)$ ein Teilkörper von D über k ist, so ist: $n\geqq \big(k(\xi):k\big)=f$. Wir bezeichnen im folgenden den Körper $k(\xi)$ mit W. Bildet man nun für ein Primelement Π von $\mathfrak{P}$ den Körper $k(\Pi)$, so gilt offenbar: $n\geqq \big(k(\Pi):k\big)\geqq e$. Da $e\leqq n$, $f\leqq n$, und $ef=n^2$ sind, so folgt ohne weiteres:

$$e=n \quad \text{und} \quad f=n.$$

Die normale Divisionsalgebra vom Grade n über k enthält also einen separablen zyklischen, unverzweigten Teilkörper W vom Grade n über k als einen maximal-kommutativen Teilkörper. Nach der allgemeinen Theorie der zyklischen Algebren ist D eine zyklische Algebra vom Grade n über k. Bezeichnet nun π ein fest gewähltes Primelement von $\mathfrak{p}$ aus k, so ist D stets von der Form:

$$D=(\pi^\nu,\ W,\ S),$$

weil nach Hilfssatz 3 jede Einheit aus k Norm einer Einheit aus W ist. Dabei bezeichnet S einen erzeugenden Automorphismus von W/k, und ν eine natürliche Zahl, welche, wie in einer anderen Gelegenheit bewiesen wird, zu n prim ist.

---

1) Vgl. M. Moriya, loc. cit., S. 406.