EINE NOTWENDIGE BEDINGUNG FÜR DIE GÜLTIGKEIT DER KLASSENKÖRPERTHEORIE IM KLEINEN

MIKAO MORIYA

Für den Aufbau der Klassenkörpertheorie im Kleinen über einem diskret bewerteten perfekten Körper k als Grundkörper ist, wie früher gezeigt[1], die folgende Bedingung $(*)$ hinreichend:

i) *Der Restklassenkörper* $\mathfrak{k}$ *von* k *ist vollkommen.*

$(*)$ ii) *Zu jeder natürlichen Zahl* n *existiert über* $\mathfrak{k}$ *genau eine Erweiterung vom Grade* n[2].

Es fragt sich naturgemäß, ob für die Gültigkeit der Klassenkörpertheorie im Kleinen die obige Bedingung auch notwendig ist; d.h. kann man umgekehrt aus der Gültigkeit von einigen Sätzen der Klassenkörpertheorie im Kleinen die obige Bedingung herleiten? Daß dies tatsächlich geschieht, soll in der vorliegenden Note gezeigt werden.

Wir legen nun einen Körper k fest, welcher in bezug auf eine nicht-triviale, nicht-archimedische und diskrete Bewertung w perfekt ist. Dann bezeichnen wir mit $\mathfrak{p}$ den zu w gehörigen Primdivisor aus k und mit $\mathfrak{k}$ den Restklassenkörper von k in bezug auf $\mathfrak{p}$. Eine endliche Erweiterung K über k besitzt genau eine Fortsetzung von w, und K ist perfekt in bezug auf diese Fortsetzung. Im folgenden verstehen wir unter dem Restklassenkörper von $K(\geqq k)$ stets den Restklassenkörper von K in bezug auf denjenigen Primdivisor aus K, der zur Fortsetzung von w in K gehört. Ferner kann man wie üblich annehmen, daß der Restklassenkörper von K den Körper $\mathfrak{k}$ als Teilkörper enthält.

Für eine endliche separable Erweiterung K über k betrachten wir die Gesamtheit $H(K/k)$ aller derjenigen Elemente aus k, die Normen der von Null verschiedenen Elemente aus K nach k sind. Offenbar ist $H(K/k)$ eine Untergruppe der multiplikativen Gruppe k^* aller von

1) M. Moriya, Die Theorie der Klassenkörper im Kleinen über diskret perfekten Körpern. I., II., Proc. Imp. Acad., Tokyo, Vol. **18** (1942).

T. Nakayama und M. Moriya, Die Theorie der Klassenkörper im Kleinen über diskret perfekten Körpern. III., Proc. Imp. Acad., Tokyo, Vol. **19** (1943).

Man vergleiche auch das Buch von Schilling: O. F. G. Schilling, The theory of valuations, Mathematical Surveys, Nr. **6** (1950), Chapt. 6, "Local class field theory".

2) Dies bedeutet, daß in einem algebraisch-abgeschlossenen Körper über $\mathfrak{k}$ genau eine Erweiterung vom Grade n über $\mathfrak{k}$ existiert.

Null verschiedenen Elemente aus k, und man nennt $H(K/k)$ die K zugeordnete *Normgruppe* aus k. Eine endliche separable Erweiterung K über k heißt ein *Klassenkörper* über k, wenn

$$(k^* : H(K/k)) = (K : k)$$

gilt. Wenn man dabei die Bedingung $(*)$ hinzufügt, so gelten folgende Hauptsätze der Klassenkörpertheorie:

I) **Umkehrsatz.** Eine endliche separable abelsche Erweiterung über k ist stets ein Klassenkörper.

II) **Isomorphiesatz.** Ist L ein Klassenkörper über k, so ist die Faktorgruppe $k^*/H(L/k)$ mit der Galoisgruppe von L über k isomorph.

III) **Eindeutigkeitssatz.** Ist H eine Untergruppe von einem endlichen Index aus k^*, so existiert über k höchstens ein Klassenkörper, dessen Normgruppe aus k gleich H ist.

IV) **Abgrenzugssatz.** Ist K eine endliche separable Erweiterung über k und L der größte abelsche Teilkörper von K über k, so gilt:

$$H(K/k) = H(L/k);$$

d.h. L ist der Klassenkörper über k, dessen Normgruppe aus k gleich $H(K/k)$ ist.

Zusatz. Ein Klassenkörper K über k ist stets über k abelsch.

V) **Verschiebungssatz.** Es sei k' eine endliche separable Erweiterung über k, und L ein Klassenkörper über k. Dann ist das Kompositum Lk' von L und k' ein Klassenkörper über k', dessen Normgruppe aus allen denjenigen Elementen aus k' besteht, deren Norm nach k in $H(L/k)$ hineinfällt.

Wir führen nun in k^* eine Topologie ein und definieren in bezug auf diese Topologie abgeschlossene Untergruppen aus k^*. Dann gilt:

VI) **Existenzsatz.** Ist H eine abgeschlossene Untergruppe von einem endlichen Index aus k^*, so existiert über k ein Klassenkörper, dessen Normgruppe aus k gleich H ist.

Von jetzt an lassen wir die Bedingung $(*)$ fort und *setzen voraus, daß über einer beliebigen endlichen separablen Erweiterung von k (einschließlich k selbst) als Grundkörper der Abgrenzungssatz, Isomorphiesatz und Umkehrsatz aus der Klassenkörpertheorie im Kleinen gelten.* Dann wollen wir zeigen, daß die Bedingung $(*)$ erfüllt ist. Dazu beweisen wir zunächst folgenden

Satz 1. *Ist W eine endliche separable, unverzweigte Erweiterung über k, so ist W ein zyklischer Klassenkörper über k.*

Beweis. Wir bezeichnen mit n den Grad von W über k. Da W über k unverzweigt ist, so ist ein von Null verschiedenes Element aus W von der Form $\pi^p E$, wo π ein Primelement aus k und E eine Einheit aus W ist. Bezeichnet man nun mit $N(\ )$ die Norm eines Elementes aus W nach k, so ist

$$N(\pi^p E) = \pi^{np} N(E).$$

Dabei ist $N(E)$ offenbar eine Einheit aus k. Der Einfachheit halber wollen wir ohne Mißverständnis auch mit $N(E)$ die multiplikative Gruppe bezeichnen, welche die Norm aller Einheiten E aus W nach k bildet. Ersichtlich ist die W zugeordnete Normgruppe $H(W/k)$ aus k das direkte Produkt $\{\pi^n\} \times N(E)$, wo $\{\pi^n\}$ die von π^n erzeugte zyklische Gruppe bezeichnet. Nun gilt nach dem Abgrenzungssatz:

$$n \geqq (k^* : H(W/k)) = (k^* : \{\pi^n\} \times \varepsilon)(\{\pi^n\} \times \varepsilon : \{\pi^n\} \times N(E)).$$

Dabei bezeichnet k^* die Gesamtheit aller von Null verschiedenen Elemente aus k und ε die Gruppe aller Einheiten aus k. Da offenbar $k^* = \{\pi\} \times \varepsilon$ ist, so ist

$$(k^* : \{\pi^n\} \times \varepsilon) = (\{\pi\} : \{\pi^n\}) = n$$

und

$$(\{\pi^n\} \times \varepsilon : \{\pi^n\} \times N(E)) = (\varepsilon : N(E)).$$

Daraus schließt man ohne weiteres, daß

$$(k^* : H(W/k)) = n \qquad \text{und} \qquad (\varepsilon : N(E)) = 1$$

sind. Also ist W nach Definition ein Klassenkörper über k. Weil $(\varepsilon : N(E)) = 1$ ist, so ist $\varepsilon = N(E)$, und es gilt die Isomorphierelation:

$$k^*/H(W/k) = k^*/\{\pi^n\} \times \varepsilon \cong \{\pi\}/\{\pi^n\}.$$

Daher ist $k^*/H(W/k)$ zyklisch von der Ordnung n; wegen des Isomorphiesatzes ist W über k zyklisch.

Zusatz. Wenn W eine endliche separable, unverzweigte Erweiterung über k ist, so ist jede Einheit aus k Norm einer Einheit aus W nach k.

Satz 2. *Der Restklassenkörper* $\mathfrak{k}$ *von* k *ist vollkommen.*

Beweis. Wir nehmen an, daß $\mathfrak{k}$ *unvollkommen* ist. Dann ist die Charakteristik von $\mathfrak{k}$ eine Primzahl p, und es gibt ein Element $\mathfrak{c}$ aus $\mathfrak{k}$, dessen p-te Wurzel nicht zu $\mathfrak{k}$ gehört; d.h. das Polynom $x^p - \mathfrak{c}$ ist in $\mathfrak{k}[x]$ irreduzibel. Nun betrachten wir für ein zu $\mathfrak{c}$ gehöriges Element c aus k das Polynom

$$x^p - c \qquad \text{oder} \qquad x^p - \pi x - c,$$

je nachdem $p \neq \chi(k)$ (Charakteristik von k) oder $p = \chi(k)$ ist. Dabei bezeichnet π ein Primelement von w aus k. Ist nun $K = k(\theta)$ ein Körper, welcher aus k durch Adjunktion einer Nullstelle θ der beiden obigen Polynome entsteht, so ist θ, wie leicht bestätigt, eine Einheit aus K. Ferner ist die θ enthaltende Restklasse aus dem Restklassenkörper $\mathfrak{K}$ von K eine Nullstelle des Polynomes $x^p - \mathfrak{c}$; d.h. $\mathfrak{K}$ ist mindestens vom Grade p über $\mathfrak{k}$. Weil $(K : k) \leqq p$ ist und infolgedessen $(\mathfrak{K} : \mathfrak{k}) \leqq (K : k) \leqq p$ ist, so muß $(\mathfrak{K} : \mathfrak{k}) = p = (K : k)$ sein; d.h. der Körper K ist unverzweigt vom Grade p über k, und folglich ist nach Satz 1 über k zyklisch. Da $\mathfrak{K}$ aus $\mathfrak{k}$ durch Adjunktion einer Nullstelle des rein-inseparablen Polynomes $x^p - \mathfrak{c}$ aus $\mathfrak{k}[x]$ entsteht, so ist $\mathfrak{K}$ offenbar rein-inseparabel über $\mathfrak{k}$. Wir bezeichnen nun mit $\mathfrak{P}$ den Primdivisor aus K. Dann gibt es zu jeder Einheit E aus K stets eine Einheit ε aus k derart, daß die Kongruenz

$$E^p \equiv \varepsilon \qquad \mod \mathfrak{P}$$

gilt, weil $\mathfrak{K}$ über $\mathfrak{k}$ rein-inseparabel vom Grade p ist. Ferner gilt für einen erzeugenden Automorphismus σ von K/k:

$$(\sigma^i E)^p \equiv \varepsilon \qquad \mod \mathfrak{P} \ (i = 0, 1, \cdots\cdots, p-1).$$

Da die Charakteristik von $\mathfrak{k}$ gleich p ist, so schließen wir aus den obigen Kongruenzen:

$$(E - \sigma^i E)^p \equiv 0 \qquad \mod \mathfrak{P} \ (i = 0, 1, \cdots\cdots, p-1),$$

woraus sofort die Kongruenzen

$$\sigma^i E \equiv E \qquad \mod \mathfrak{P} \ (i = 0, 1, \cdots\cdots, p-1)$$

folgen. Daher gelten:

$$N(E) = \prod_{i=0}^{p-1} \sigma^i E \equiv E^p \qquad \mod \mathfrak{P}$$

und

$$S(E) = \sum_{i=0}^{p-1}\sigma^i E \equiv pE \equiv 0 \qquad \text{mod } \mathfrak{P}.$$

Ist also E eine solche Einheit aus K, daß $N(E)$ eine Einseinheit aus k ist, so folgt aus der Kongruenz $N(E) \equiv E^p$ mod $\mathfrak{P}$:

$$E^p \equiv 1 \qquad \text{mod } \mathfrak{P};$$

es muß also $E \equiv 1$ mod $\mathfrak{P}$ sein. Weil nach Zusatz zu Satz 1 jede Einheit aus k Norm einer Einheit aus K nach k ist, so schließt man aus dem oben Bewiesenen sofort, daß jede Einseinheit aus k Norm einer Einseinheit aus K nach k ist.

Eine von 1 verschiedene Einseinheit E aus K ist von der Form

$$E = 1 + E_\nu \pi^\nu + E_{\nu+1}\pi^{\nu+1} + \cdots\cdots \qquad E_\nu \neq 0,$$

wo die $E_\nu, E_{\nu+1}, \cdots\cdots$ entweder Einheiten aus K oder 0 sind. Setzt man nun $\varphi(\pi) = \sum_{i=\nu}^{\infty} E_i \pi^{i-\nu}$, so ist

$$\begin{aligned} N(E) &= N(1 + \pi^\nu \varphi(\pi)) \\ &= 1 + \pi^\nu S(\varphi(\pi)) + \pi^{2\nu} A_2 + \cdots\cdots + \pi^{n\nu} A_n, \end{aligned}$$

wo die $A_2, A_3, \cdots\cdots, A_n$ ganze Elemente aus k bezeichnen. Weil nach dem oben Bewiesenen $S(\varphi(\pi)) \equiv 0$ mod $\mathfrak{P}$ und $S(\varphi(\pi))$ ein Element aus k ist, so gilt:

$$S(\varphi(\pi)) \equiv 0 \qquad \text{mod } \mathfrak{p},$$

daher ist

$$N(E) \equiv 1 \qquad \text{mod } \mathfrak{p}^{\nu+1}.$$

Hieraus folgt ohne weiteres, daß eine Einseinheit $1 + \varepsilon_1 \pi$ (ε_1 ist eine Einheit aus k) sicher keine Norm der Einheiten aus K ist. Dies ist aber ein Widerspruch, daher muß $\mathfrak{K}$ vollkommen sein.

Satz 3. *Jede endliche Erweiterung über $\mathfrak{k}$ ist stets zyklisch.*

Beweis. Es sei $\mathfrak{K}$ eine Erweiterung vom Grade n über $\mathfrak{k}$. Dann besitzt $\mathfrak{K}$ ein primitives Element $\bar{\theta}$ über $\mathfrak{k}$, weil $\mathfrak{k}$ nach Satz 2 vollkommen ist. Also genügt $\bar{\theta}$ einer irreduziblen Gleichung

$$\bar{f}(x) = x^n + \bar{a}_1 x^{n-1} + \cdots\cdots + \bar{a}_n = 0$$

aus $\mathfrak{k}$, wo die $\bar{a}_1, \cdots\cdots, \bar{a}_n$ Elemente aus $\mathfrak{k}$ bezeichnen. Offenbar ist dabei $\bar{f}(x)$ ein separables Polynom aus $\mathfrak{k}[x]$. Nun greifen wir aus den $\bar{a}_1, \cdots\cdots, \bar{a}_n$ bzw. die Elemente $a_1, \cdots\cdots, a_n$ aus k heraus. Dann ist, wie man leicht bestätigt, das Polynom $f(x) = x^n + a_1 x^{n-1} + \cdots\cdots + a_n$ in $k[x]$ separabel. Wir betrachten jetzt den Körper K, welcher aus k durch Adjunktion einer Wurzel θ von $f(x) = 0$ entsteht, wo θ ersichtlich eine Einheit aus K ist. Bezeichnet man nun mit $\mathfrak{P}$ den Primdivisor aus K, so ist die θ enthaltende Restklasse mod $\mathfrak{P}$ sicher eine Wurzel der Gleichung $\bar{f}(x) = 0$; d.h. der Restklassenkörper von K enthält einen mit $\mathfrak{K}$ isomorphen Körper als einen Teilkörper. Weil aber $(\mathfrak{K} : \mathfrak{k}) = n = (K : k)$ ist, so muß der Restklassenkörper von K mit $\mathfrak{K}$ isomorph sein, also ist K über k unverzweigt und infolgedessen nach Satz 1 über k zyklisch.

Nun ist die die Diskriminante von $f(x)$ enthaltende Restklasse mod $\mathfrak{p}$ gleich der Diskriminante von $\bar{f}(x)$ und folglich ist von der Nullklasse mod $\mathfrak{p}$ verschieden. Daher sind die n Wurzeln von $f(x) = 0$ aus K mod $\mathfrak{P}$ voneinander inkongruent. Bezeichnet nun σ einen erzeugenden Automorphismus von K/k, so gilt für $0 \leqq i \leqq n-1$:

$$(\sigma^i \theta)^n + a_1(\sigma^i \theta)^{n-1} + \cdots\cdots + a_n \equiv 0 \qquad \text{mod } \mathfrak{P};$$

weil die $\theta, \sigma\theta, \cdots\cdots, \sigma^{n-1}\theta$ die sämtlichen Wurzeln von $f(x) = 0$ aus K sind, so bestätigt man leicht, daß der Restklassenkörper von K über $\mathfrak{k}$ zyklisch ist. Also muß $\mathfrak{K}$ über $\mathfrak{k}$ zyklisch sein.

Aus dem Beweis von Satz 3 erhält man folgenden

Zusatz. Zu einer endlichen Erweiterung $\mathfrak{K}$ vom Grade n über $\mathfrak{k}$ existiert über k eine separable, unverzweigte Erweiterung vom Grade n, deren Restklassenkörper mit $\mathfrak{K}$ isomorph ist.

Satz 4. *Zu einer natürlichen Zahl n existiert über $\mathfrak{k}$ höchstens eine Erweiterung vom Grade n.*

Beweis. Es seien $\mathfrak{K}_1$ und $\mathfrak{K}_2$ Erweiterungen vom Grade n über $\mathfrak{k}$, welche in einem algebraisch-abgeschlossenen Körper über $\mathfrak{k}$ enthalten sind. Dann kann man offenbar das Kompositum $\mathfrak{K}$ von $\mathfrak{K}_1$ nnd $\mathfrak{K}_2$ bilden. Weil nach Satz 3 $\mathfrak{K}$ über $\mathfrak{k}$ zyklisch ist, so kann $\mathfrak{K}$ einen einzigen Teilkörper vom Grade n über $\mathfrak{k}$ enthalten, also muß $\mathfrak{K}_1 = \mathfrak{K}_2$ sein, w.z.b.w.

Es sei K eine endliche separable Erweiterung über k. Dann bezeichnen wir mit Π ein Primelement des Primdivisors $\mathfrak{P}$ aus K, welcher in $\mathfrak{p}$ aufgeht. Ist nun eine Primzahl l zu $\chi(k)$ (Charakteristik von k) gleich, so ist

$$x^l - x + \frac{1}{\Pi}$$

ein separables Polynom aus $K[x]$, und der Körper Z, welcher aus K durch Adjunktion einer Nullstelle des obigen Polynomes entsteht, ist bekanntlich über K verzweigt und zyklisch. Weil nach dem Umkehrsatz Z ein Klassenkörper über K ist, so existiert ein Element α aus K, welches keine Norm der Elemente aus Z nach K ist. Bildet man dann die zyklische Algebra $D = (\alpha, Z, S)$, so ist D offenbar eine normale Divisionsalgebra vom Grade l über K, wo S einen erzeugenden Automorphismus von Z/K bezeichnet. Weil K in bezug auf $\mathfrak{P}$ perfekt ist, so besitzt D genau einen Primteiler $\mathfrak{P}_D$ von $\mathfrak{P}$, und der Restklassenring von D in bezug auf $\mathfrak{P}_D$ ist ein (kommutativer) Körper $\mathfrak{Z}$ vom Grade l über dem Restklassenkörper $\mathfrak{K}$ von K[1].

Wenn aber $l \neq \chi(k)$ ist, so adjungieren wir zu K eine primitive l-te Einheitswurzel ζ. Wir bezeichnen dann mit Π_1 ein Primelement des Primdivisors aus dem Körper $K_1 = K(\zeta)$. Offenbar ist das Polynom $x^l - \Pi_1$ in $K_1[x]$ separabel, und der Körper Z_1, welcher aus K_1 durch Adjunktion einer Nullstelle des obigen Polynomes entsteht, ist über K_1 verzweigt und zyklisch. Da nach Voraussetzung Z_1 ein Klassenkörper über K_1 ist, so kann man wie oben über K_1 eine normale Divisionsalgebra D_1 vom Grade l bilden. Dabei ist der Restklassenring $\mathfrak{Z}_1$ von D_1 ein kommutativer Körper vom Grade l über dem Restklassenkörper $\mathfrak{K}_1$ von K_1. Weil aber nach Satz 3 $\mathfrak{Z}_1$ über $\mathfrak{k}$ zyklisch ist, so ist $\mathfrak{Z}_1$ auch über $\mathfrak{K}$ zyklisch. Hieraus schließt man sofort, daß $\mathfrak{Z}_1$ einen Teilkörper vom Grade l über $\mathfrak{K}$ besitzt.

Satz 5. *Ist $l^e (e \geqq 1)$ eine Potenz einer Primzahl l, so existiert über $\mathfrak{k}$ eine Erweiterung vom Grade l^e.*

Beweis. Wir nehmen an, daß für l^{e-1} der Satz richtig ist, und bezeichnen mit $\mathfrak{K}$ eine Erweiterung vom Grade l^{e-1} über $\mathfrak{k}$. Dann existiert nach Zusatz zu Satz 3 eine endliche separable Erweiterung K vom Grade l^{e-1} über k, deren Restklassenkörper $\mathfrak{K}'$ mit $\mathfrak{K}$ isomorph ist. Nach dem oben Bewiesenen existiert über $\mathfrak{K}'$ eine Erweiterung vom Grade l; die letzte Erweiterung ist aber vom Grade l^e über $\mathfrak{k}$.

Satz 6. *Ist $n (>1)$ eine natürliche Zahl, so existiert über $\mathfrak{k}$ genau eine Erweiterung vom Grade n.*

Beweis. Es sei $n = l_1^{e_1} \cdots\cdots l_s^{e_s}$ die Primzahlpotenzzerlegung von n.

1) Vgl. etwa O. F. G. Schilling, a.a.O., S. 52-55.

Dann existiert nach Satz 4 zu jeder Primzahl $l_i (1 \leqq i \leqq s)$ über $\mathfrak{k}$ eine Erweiterung $\mathfrak{K}_i$ vom Grade $l_i^{\nu_i}$. Weil nach Satz 3 die $\mathfrak{K}_1, \cdots\cdots, \mathfrak{K}_s$ über $\mathfrak{k}$ zyklisch sind, so ist das Kompositum von den $\mathfrak{K}_1, \cdots\cdots, \mathfrak{K}_s$ über $\mathfrak{k}$ zyklisch vom Grade n. Gemäß Satz 4 existiert über $\mathfrak{k}$ genau eine Erweiterung vom Grade n.

Somit ist gezeigt, daß die Bedingung (*) erfüllt ist.

DEPARTMENT OF MATHEMATICS,
OKAYAMA UNIVERSITY

(*Received May 14, 1952*)