Bemerkungen zur Theorie der Differente.

Von MICHAEL BAUER in Budapest.

1. Es sei in einem algebraischen Zahlkörper K für die Primzahl p

$$p = \mathfrak{p}^g \mathfrak{q}\ , \ (\mathfrak{p}, \mathfrak{q}) = 1,$$

wo $\mathfrak{p}$ ein Primideal r-ten Grades ist und noch die Relationen

$$g = p^s g', (p, g') = 1$$

gelten. Ist die Differente des Körpers genau durch $\mathfrak{p}^{\nu-1}$ teilbar, dann ist im Falle $s = 0$, $\nu = g$; fällt aber $s > 0$ aus, so wird

(1) $$g + 1 \leqq \nu \leqq (s + 1) g.$$

Die obere Schranke kann in der Tat für jeden Wert von s und r bei geignet gewählten Körpern erreicht werden.[1])

2. Wie verhält sich die untere Schranke? Für Galoissche Körper ist nach *Hilbert*.[2])

$$\nu - 1 \geqq g - p^s + 2 (p^s - 1) \geqq g + p^s - 2,$$

also wird

$$\nu > g + 1,$$

ausgenommen den Fall $p^s = 2$. Ich werde jedoch beweisen, dass die untere Schranke für jeden Wert von s und r auftreten kann. Es sei

(2) $$F(x) = f^g(x) + p\, M(x)\ , \ F(w) = 0,$$

wo

$$f(x) = x^r + c_1 x^{r-1} + \ldots + c_r$$

ein ganzzahliges (mod. p) irreduzibles Polynom ist und das ganzzahlige Polynom $M(x)$ relativ prim gegen $f(x)$ (mod. p) ausfällt, der Grad von $M(x)$ soll kleiner als rg sein. In dem durch w

---

[1]) Vgl. meine Arbeit: Verschiedene Bemerkungen über die Differente etc. Math. Zeitschrift Bd. 16 (1923). S. 4.

[2]) *Hilbert:* Die Theorie der alg. Zahlkörper § 47. Jahresbericht der D. M. Vereinigung. Bd. 4 (1897).

erzeugten Körper $K(w)$ sind $p=\mathfrak{p}^g$, $\mathfrak{p}$ ein Primideal r-ten Grades, $\frac{f^g(w)}{p}$ eine ganze Zahl, $\left(\frac{f^g(w)}{p}, p\right)=1$. Die Differente der Zahl w, mithin die Zahl $F'(w)$ enthält genau dieselbe Potenz von $\mathfrak{p}$, wie die Körperdifferente. Wählt man

(2*) $$M(x) \equiv m(x+R) \pmod{p},$$

wo $x+R$ relativ prim gegen $f(x) \pmod{p}$ ist und m eine gegen p relativ prime rationale ganze Zahl bedeutet, so enthält die Zahl

$$F'(w) \equiv g f^{g-1}(w) f'(w) + p\,m \pmod{p^2}$$

genau die Potenz $\mathfrak{p}^g$, es ist daher $v=g+1$.

3. Werden nur Galoissche Körper betrachtet, so hat man (vgl. die Arbeit[1]) im Falle $sg \not\equiv 0 \pmod{(p-1)}$, die Relation

(3) $$g+p^s-1 \leqq v \leqq (s+1)\,g-1.$$

Für den speziellen Fall $g=p>2$, werden beide Schranken einander gleich und man bekommt $v=2p-1$. Diese Formel enthält einen bekannten Satz über Abelsche Körper. Zum Beweise kann man auch die von *H. Speiser*[3]) gegebene obere Schranke der sog. *Hilbert*schen Zahlen verwenden.

4. Der Zusammenhang zwischen der Differente $\vartheta=(\Theta^{(1)}-\Theta^{(2)})\ldots(\Theta^{(1)}-\Theta^{(n)})$ einer primitiven ganzen Zahl Θ des Körpers $K(w)$ und der Körperdifferente wird durch den folgenden *Dedekind*schen Satz geliefert:

(4) $$\vartheta=\mathfrak{f}\,\mathfrak{f},$$

---

[3]) *Speiser:* Die Zerlegungsgruppe. Journal für Math. Bd. 149 (1919), S. 183. Will man bei den Beweisen der Sätze des § 3. (a. a. O. S. 180—184) die Anwendung der Theorie der Matrizen vermeiden, so kann man die folgenden Identitäten benützen. Ist π eine genau durch $\mathfrak{p}$ teilbare ganze Zahl und bedeuten S, $\bar{S}$ beliebige Substitutionen der Körpergruppe, dann ist $S\,\bar{\varphi}-\bar{\varphi}-(\bar{S}\,\varphi-\varphi)=\bar{S}\,S\,\pi-S\,\bar{S}\,\pi$, wo $\varphi=\bar{S}\,\pi-\pi$, $\bar{\varphi}=S\,\pi-\pi$ ausfallen. Für die m-te Iteration von S, gilt die Relation:

$$S^m\,\pi=\pi+\sum_{h=1}^{m}\binom{m}{h}(S\,\pi-\pi)^{(h)}.$$

Diese Identitäten werden noch durch die Formeln ergänzt: Aus

$$S\,\pi \equiv \pi+\alpha\,\pi^{i+1}+\ldots \pmod{\mathfrak{p}^l},\quad \bar{S}\,\pi \equiv \pi+\beta\,\pi^{k+1}+\ldots \pmod{\mathfrak{p}^l}$$

folgen

$$(S\,\pi-\pi)^{(h)} \equiv (i+1)(2i+1)\ldots(\overline{h-1}\,i+1)\,\alpha^h\,\pi^{hi+1} \pmod{\mathfrak{p}^l},$$

$$S\,\varphi-\varphi \equiv (k+1)\,\beta\,\alpha\,\pi^{i+k+1}+\ldots \pmod{\mathfrak{p}^l},$$

$$\bar{S}\,\bar{\varphi}-\bar{\varphi} \equiv (i+1)\,\alpha\,\beta\,\pi^{i+k+1}+\ldots \pmod{\mathfrak{p}^l}.$$

Hier bedeuten S, $\bar{S}$ Substitutionen der Verzweigungsgruppe von $\mathfrak{p}$ und α, β, ... ganze Zahlen des Trägheitskörpers.

wo $\mathfrak{f}$ den Führer des Systems $[1, \Theta, \Theta^2, \ldots, \Theta^{n-1}]$, also ein von Θ abhängiges Ideal und $\mathfrak{j}$ ein nur vom Körper abhängiges Ideal bezeichnet, welches gleich der Körperdifferente ausfällt.[4])

Wir wollen im Folgenden eine möglichst einfache und direkte Anordnung des *Dedekind*schen Beweises geben.

5. Bilden $w_1, w_2, \ldots, w_n$ ein Fundamentalsystem der ganzen Zahlen des Körpers $K(w)$, so wird der Führer $\mathfrak{f}$ als die Gesamtheit der Zahlen γ definiert, welche die Relationen

$$(5) \qquad \gamma\, w_i = \sum_{h=1}^{n} r_{ih}\, \Theta^{h-1}, \quad (i = 1, 2, \ldots, n), \quad r_{ih} \text{ rat.-ganz,}$$

erfüllen. (Die Zahl γ ist also ganz und $\mathfrak{f}$ bildet ein Ideal.) Das komplementäre System von $[1, \Theta, \Theta^2, \ldots, \Theta^{n-1}]$ wird durch die Zahlen

$$\frac{\eta_0}{\vartheta}, \frac{\eta_1}{\vartheta}, \ldots, \frac{\eta_{n-1}}{\vartheta}$$

gegeben, wo

$$(x - \Theta^{(2)}) \ldots (x - \Theta^{(n)}) = \eta_{n-1}\, x^{n-1} + \eta_{n-2}\, x^{n-2} + \ldots + \eta_0$$

ausfällt.[5]) Aus (5) folgt nach einem bekannten Satze über komplementäre Systeme[6])

$$(5^*) \qquad \frac{\eta_{i-1}}{\vartheta} = \sum_{h=1}^{n} r_{hi} \frac{\overline{w}_h}{\gamma}, \quad \gamma\, \eta_{i-1} = \sum_{h=1}^{n} r_{hi}\, \overline{w}_h\, \vartheta$$
$$(i = 1, 2, \ldots, n),$$

wo $[\overline{w}_1, \overline{w}_2, \ldots, \overline{w}_n]$ das komplementäre System des Fundamentalsystems bezeichnet. Da $\eta_{n-1} = 1$ ist, so erfüllen die Zahlen γ notwendig eine Relation

$$(5^{**}) \qquad \gamma = \sum_{h=1}^{n} c_h\, \vartheta\, \overline{w}_h\,, \quad c_h \text{ rat.-ganz.}$$

---

[4]) *Dedekind:* Über die Discriminanten endlicher Körper § 10. Abh. der Kgl. Gesellschaft der Wiss. zu Göttingen Bd. 29 (1882). Reproduziert bei *Bachmann:* Zahlentheorie V. Teil (1905). S. 314 Andere Beweise: *Hilbert* a. a. O. § 32., *Landsberg,* Über Modulsysteme zweiter Stufe und Zahlenringe. Göttinger Nachrichten (1897), S. 277—303. Vgl. Abschnitt III. S. 292—298. — Es sei noch die schöne Darstellung im § 36. des während der Drucklegung erschienenen Buches, *E. Hecke:* Vorlesungen über die Theorie der alg. Zahlen, erwähnt. Der *Hecke*sche Beweis lässt sich leicht auf Relativkörper ausdehnen. (§ 38. a. a. O.) [Zusatz bei der Korrektur.]

[5]) *Dedekind* a. a. O. § 8. Punkt 11. Hier ist nur die Tatsache wichtig, dass die η_{i-1} ganze Zahlen des Körpers $K(w)$ sind und $\eta_{n-1} = 1$ ausfällt. Einen direkten Beweis bekommt man durch die bekannte Darstellung der Elemente des komplementären Systems mittels Determinantenbrüche.

[6]) *Dedekind* a. a. O § 8. Punkt 10.

Man kann beweisen, dass diese Relation für die Gestalt der eine genügende ist. Sei nämlich ζ eine beliebige ganze Zahl des Körpers $K(w)$, dann ist nach dem angeführten Satze über komplementäre Systeme:

$$\beta_i = w_i \zeta = \sum_{h=1}^{n} \varrho_{ih} w_h \qquad w_i \zeta = \sum_{h=1}^{n} \varrho_{hi} w_h$$

$$(i = 1, 2, \ldots, n) \;, \; \varrho_{ih} \text{ rat.-ganz,}$$

also sind die Produkte $w_i \overline{w}_k$ homogene lineare Funktionen der Grössen w_i mit rational-ganzen Koeffizienten. Infolgedessen erhält man aus (5**) wieder die Relationen (5*) und (5). Ist D die Körperdiskriminante, dann sind die Zahlen $w_i \sqrt{D}$ ganze Zahlen und nach den Vorigen bilden die Zahlen $\overline{w}_i D$, $(i = 1, 2, \ldots, n)$ das Fundamentalsystem eines Ideals, welches durch $\mathfrak{z}$ bezeichnet werde. Aus (5**) erhält man:

$$D = \mathfrak{z}\, \vartheta,$$

da das Ideal D durch $\mathfrak{z}$ teilbar ist (weil $D = \sum_{i=1}^{n} w_i \overline{w}_i D$ ausfällt), wird[7])

$$D = \mathfrak{z}\, \mathfrak{j} \;, \; \vartheta = \mathfrak{f}\, \mathfrak{j},$$

womit der Beweis geleistet ist. Da bei einer geigneten Wahl von Θ, $\mathfrak{f}$ nach *Dedekind* relativ prim gegen ein beliebig gegebenes Primideal ist,[8]) bildet das Ideal den grössten gemeinsamen Teiler der Differenten ϑ, folglich ist $\mathfrak{j}$ mit der Körperdifferente $\mathfrak{d}$ aequivalent.[9])

---

[7]) Hier wird erst der Hauptsatz der Idealtheorie angewendet.

[8]) Vgl. den vereinfachten Beweis bei *Hilbert* a. a. O. § 32.

[9]) Vgl. den direkten Beweis dieser Behauptung in meiner Arbeit I.) Ein indirekter Beweis, welcher den Norm-Begriff ausnützt, steht bei *Hilbert* a. a. O. gegen Ende des § 32.