

# Die Theorie der $p$ -adischen bzw. $\mathfrak{P}$ -adischen Zahlen und die gewöhnlichen algebraischen Zahlkörper.

Von

Michael Bauer in Budapest.

Die Methoden zur Untersuchung der algebraischen Körper hat H. Hensel durch die Theorie der sogenannten  $p$ -adischen bzw.  $\mathfrak{P}$ -adischen Zahlen bereichert. Seine erste diesbezügliche Publikation<sup>1)</sup> verwendet noch die klassische Idealtheorie; die späteren Publikationen betrachten die neue Theorie selbst dann als Prius, wenn mittels derselben gewöhnliche algebraische Zahlkörper untersucht werden sollen<sup>2)</sup>.

In den folgenden Zeilen möchte ich von der klassischen Idealtheorie ausgehend, ein sehr naheliegendes Verfahren auseinandersetzen, welches der Gleichung

$$(1) \quad f(x) = x^n + c_1 x^{n-1} + \dots + c_n = 0,$$

deren Koeffizienten gewöhnliche rationale ganze Zahlen sind und die im gewöhnlichen Sinne irreduzibel ist,  $n$  solche  $\mathfrak{P}$ -adische Wurzeln zuordnet, welche mit den gewöhnlichen Wurzeln als *identisch* betrachtet werden können. Durch weitere idealththeoretische und algebraische Betrachtungen wird unvermittelt der Zusammenhang aufgedeckt, welcher zwischen den  $p$ -adischen irreduziblen Faktoren von (1) und den Primidealfaktoren von  $p$  im Körper, der durch eine Wurzel von (1) gegeben wird, besteht.

Der § 1 enthält idealththeoretische und algebraische Tatsachen, § 2 gibt die Konstruktion des  $\mathfrak{P}$ -adischen Körpers und die Zerfällung von (1) im

---

<sup>1)</sup> Über die Entwicklung der algebraischen Zahlen in Potenzreihen, *Mathematische Annalen* 55 (1902), S. 301–336.

<sup>2)</sup> Hier kommen in erster Linie in Betracht: Theorie der algebraischen Zahlen 1 (1908). Über die zu einer algebraischen Gleichung gehörigen Auflösungskörper, *Journal für Mathematik* 136 (1909), S. 183–209. Eine neue Theorie der algebraischen Zahlen, *Mathematische Zeitschrift* 2 (1918), S. 433–452.

$p$ -adischen Körper<sup>3)</sup>, § 3 beweist die Henselsche Tatsache, daß jede  $p$ -adische algebraische Gleichung „algebraisch“ auflösbar ist, eine Tatsache, die — wie es sich hier ergibt — im engsten Zusammenhange mit der Hilbertschen Theorie der Zerlegungsgruppe ist<sup>4)</sup>. (Die Untersuchungen sind auf Relativkörper ausdehnbar.)

# § 1.

## Sätze aus der Idealtheorie und der Algebra.

1. Es sei  $w$  eine Wurzel von (1), welche den Körper  $K$  bestimmt. Der Galoissche Körper von  $K$  soll durch  $G$  bezeichnet werden, seine Gruppe sei  $\mathfrak{G}$  und  $K$  gehöre zur Untergruppe  $\mathfrak{R}$ . Eine grundlegende Regel von Dedekind<sup>5)</sup> gibt die Zerfällung von  $p$  folgendermaßen an. Es sei  $\mathfrak{P}$  ein beliebiges Primideal von  $p$  im Körper  $G$ , die Zerlegungsgruppe von  $\mathfrak{P}$  soll durch  $\mathfrak{S}$  bezeichnet werden. Zunächst muß die Gruppe  $\mathfrak{G}$  (mod  $\mathfrak{S}$ ,  $\mathfrak{R}$ ) zerlegt werden, es sei<sup>6)</sup>

$$(2) \quad \mathfrak{G} = \mathfrak{S} R_1 \mathfrak{R} + \mathfrak{S} R_2 \mathfrak{R} + \dots + \mathfrak{S} R_k \mathfrak{R},$$

hier bedeuten  $R_1 = E, R_2, \dots, R_k$  die (mod  $\mathfrak{S}$ ,  $\mathfrak{R}$ ) inkongruenten Elemente. Wenn (2) statthat, so ist im Körper  $K$

$$(2^*) \quad p = \mathfrak{p}_1^{g_1} \mathfrak{p}_2^{g_2} \dots \mathfrak{p}_k^{g_k},$$

wo die Primideale  $\mathfrak{p}_i$  den Grad  $f_i$  besitzen und das Produkt  $f_i g_i$  gleich der Anzahl der verschiedenen Elemente des Komplexes  $\mathfrak{S} R_i \mathfrak{R}$  dividiert durch die Anzahl der verschiedenen Elemente von  $\mathfrak{R}$  ausfällt.

Die Primideale  $\mathfrak{p}_i$  des Körpers  $K$  weisen in  $G$  die Zerfällung

$$(2^{**}) \quad \mathfrak{p}_i = (\mathfrak{P}_{i1} \dots)^{a_i}$$

auf, wo die eingeklammerten Primideale die verschiedenen Ideale des Komplexes  $\mathfrak{S} R_i \mathfrak{R} \mathfrak{P}$  sind. (Der Zusammenhang der Zahlen  $f_i, g_i, a_i$  mit der Zerlegungsgruppe  $\mathfrak{S}$  und der Trägheitsgruppe, sowie der Gruppe  $\mathfrak{R}$  kommt hier nicht in Betracht.)

<sup>3)</sup> Für den Fall, daß die Koeffizienten von (1) rationale  $p$ -adische Zahlen sind und (1) im Körper der rationalen  $p$ -adischen Zahlen irreduzibel ist, kann nach H. Hensel das Problem der  $\mathfrak{p}$ -adischen Wurzeln auf das analoge Problem einer Gleichung  $g(x) = 0$  zurückgeführt werden, welche gewöhnliche rationale Koeffizienten besitzt und im Körper der rationalen  $p$ -adischen Zahlen irreduzibel ausfällt. Das Polynom  $g(x)$  ist ein geeignetes Näherungs-Polynom von  $f(x)$ .

<sup>4)</sup> Grundzüge einer Theorie des Galoisschen Zahlkörpers, Göttinger Nachrichten 1894, S. 224–236. Die Theorie der algebraischen Zahlkörper, Jahresbericht der Deutschen Mathematiker-Vereinigung 4 (1897), § 49.

<sup>5)</sup> Zur Theorie der Ideale, Göttinger Nachrichten 1894, S. 272–277.

<sup>6)</sup> Die Operationen müssen von links nach rechts ausgeübt werden.

2. Zwei Konsequenzen der vorstehenden Regel sind für uns wichtig. Wenn  $p$  bzw.  $\mathfrak{P}$  beliebige Primfaktoren von  $p$  in  $K$  bzw.  $G$  bedeuten, so ist immer ein Element  $R$  der Gruppe  $\mathfrak{G}$  vorhanden, daß  $p$  durch  $R\mathfrak{P}$  teilbar ist, infolgedessen besitzt  $p$  nach den Vorigen nur die verschiedenen Primideale des Komplexes  $\mathfrak{R}R^{-1}\mathfrak{P}$  als Teiler. Also besteht die folgende Tatsache:

I. Ist  $p$  durch  $R\mathfrak{P}$  teilbar, dann sind unter den Konjugierten von  $p$  diejenigen und nur diejenigen durch  $\mathfrak{P}$  teilbar, welche in einem der Körper  $\mathfrak{R}R^{-1}\mathfrak{P}w$  vorkommen.

Hieraus folgt noch, daß die Ordnung einer Zahl von  $K$  in bezug auf  $p$  auch durch die Ordnung einer gewissen konjugierten Zahl in bezug auf  $\mathfrak{P}$  angegeben werden kann. Es gilt nämlich der folgende Satz:

II. Die Ordnung einer Zahl  $\Omega$  des Körpers  $K$  in bezug auf  $p$  ist gleich der Ordnung, welche die Konjugierten von  $\Omega$  in irgendwelchem der Körper  $\mathfrak{R}R^{-1}\mathfrak{P}w$  in bezug auf  $\mathfrak{P}$  besitzen. Letztere Ordnungen bekommt man, wenn der Exponent der Potenz von  $\mathfrak{P}$ , welche in der betreffenden Zahl genau vorkommt, durch den kleinsten positiven Exponenten, welcher im Körper auftritt, dividiert wird.

Um den Beweis zu leisten, muß nur bemerkt werden, daß wenn  $\Omega$  genau  $p^h$  enthält, dann enthält nach den Vorigen eine jede der Zahlen  $\mathfrak{R}R^{-1}\mathfrak{P}\Omega$  genau  $\mathfrak{P}^{ah}$ , wo  $a$  eine konstante Zahl ist, und zwar enthält laut (2\*\*) ein jedes der Ideale  $\mathfrak{R}R^{-1}\mathfrak{P}p$  genau  $\mathfrak{P}^a$ .

3. Zur Gruppe  $\mathfrak{G}$  gehöre der Zerlegungskörper  $H$ . Nach Adjunktion einer primitiven Zahl  $\alpha$  von  $H$  wird nach Landsberg<sup>7)</sup>

$$(3) \quad f(x) = f_1(x, \alpha) f_2(x, \alpha) \dots f_k(x, \alpha),$$

wo die Koeffizienten der irreduziblen Polynome  $f_i(x, \alpha)$  Zahlen des Körpers  $H$  bilden und die Wurzeln von  $f_i(x, \alpha) = 0$  die verschiedenen Zahlen des Komplexes  $\mathfrak{R}R_i^{-1}\mathfrak{P}w$  sind. Da der Körper  $K$  zur Untergruppe  $\mathfrak{R}$  gehört, so ist die Anzahl der Wurzeln nach den Vorigen gleich  $f_i g_i$ .

## § 2.

### Der Körper der rationalen $p$ -adischen Zahlen und seine Erweiterung.

1. Die Konstruktion des  $p$ -adischen bzw.  $\mathfrak{P}$ -adischen Körpers kann leicht durch ein Verfahren geschehen, welchem der von H. Kürschák<sup>8)</sup> eingeführte Begriff der Bewertung zugrunde liegt. Es sei  $\mathfrak{P}$  ein beliebiges

<sup>7)</sup> Über Reduktion von Gleichungen durch Adjunktion, Journal für Mathematik 132 (1907), S. 1–20.

<sup>8)</sup> Über Limesbildung und allgemeine Körpertheorie, Journal für Mathematik 142 (1913), S. 211–253.

Primideal von  $p$  in  $G$ . Jede Zahl  $\Phi$  von  $G$ , welche nicht Null ist, besitzt in bezug auf  $\mathfrak{P}$  einen höchsten Exponenten, es sei dieser durch  $h$  bezeichnet. Als Bewertung von  $\Phi$  definieren wir  $\|\Phi\| = e^{-h}$ , wo  $e > 1$  eine sonst beliebige reelle Zahl ist. Die Bewertung von Null soll gleich Null sein. Es ist ersichtlich, daß die Bewertung eines Produkts gleich dem Produkte der Bewertungen der Faktoren ist. Die Bewertung einer Summe ist nicht größer als die Bewertungen der Glieder und gleich der Bewertung des Gliedes, dessen Bewertung die größte ist, falls ein solches Glied existiert. So entstehen die Begriffe der Fundamentalreihe und des Grenzwertes. Erweitert man die Zahlen des Körpers  $G^0$  durch diese Henselschen Grenzwerte, so bekommt man einen perfekten Körper, welcher die rationalen  $p$ -adischen Zahlen als Unterkörper enthält und in welchem  $f(x) = 0$   $n$  solche  $\mathfrak{P}$ -adische Wurzeln besitzt, die mit den gewöhnlichen Wurzeln als identisch angesehen werden können. Die Gleichung (1) bleibt im Körper der rationalen  $p$ -adischen Zahlen nicht irreduzibel; die in der Formel (3) auftretenden Faktoren  $f_i(x, \alpha)$  werden  $p$ -adisch je einem irreduziblen Polynome  $P_i(x)(p)$  gleich.

2. Zunächst ist nach H. Hilbert eine jede ganze Zahl des Zerlegungskörpers nach dem Modul  $\mathfrak{P}^t$  einer ganzen rationalen Zahl kongruent, welche natürlich von  $t$  abhängt; es ist also jede Zahl des Zerlegungskörpers gleich einer rationalen  $p$ -adischen Zahl und so wird

$$(3^*) \quad f_i(x, \alpha) = P_i(x)(p),$$

wo die Koeffizienten von  $P_i(x)$  rationale  $p$ -adische Zahlen sind. Die Wurzeln von  $P_i(x) = 0(p)$  werden durch die verschiedenen Zahlen<sup>10)</sup> des Komplexes  $\mathfrak{K} R_i^{-1} \mathfrak{H} w$  geliefert, wir werden die Irreduzibilität von  $P_i(x)(p)$  nachweisen. Es sei  $G(x) = 0(p)$  eine Gleichung mit rationalen ganzen  $p$ -adischen Koeffizienten, welche durch eine der Zahlen des Komplexes  $\mathfrak{K} R_i^{-1} \mathfrak{H} w$  erfüllt wird, z. B. bilde die Zahl

$$(3^{**}) \quad \bar{Q} = \bar{K} R_i^{-1} \bar{H} w,$$

<sup>9)</sup> Die Zahl  $\Phi$  wird als Grenzwert der Fundamentalreihe  $\Phi, \Phi, \dots, \Phi, \dots$  betrachtet.

<sup>10)</sup> Die sind auch im  $\mathfrak{P}$ -adischen Sinne verschieden. Die Elemente einer Fundamentalreihe, welche keine Nullreihe ist, enthalten von einem genügend großen Index dieselbe Potenz von  $\mathfrak{P}$ . Der Exponent  $h$  sei der zum Grenzwerte gehörige Exponent. Von den Zahlen des Körpers, welche durch eine Wurzel der Gleichung  $P_i(x) = 0(p)$  gegeben wird, sollen die Zahlen mit nicht negativen Exponenten als ganze Zahlen bezeichnet werden. Aus dem Texte ersieht man, daß eine Zahl dann und nur dann ganz wird, wenn sie eine Gleichung mit rationalen ganzen  $p$ -adischen Koeffizienten erfüllt, deren höchster Koeffizient gleich Eins ist. Es ist sogar evident, daß eine Zahl dann und nur dann ganz ist, wenn ihre Norm eine ganze rationale  $p$ -adische Zahl bildet.

wo  $\bar{K}$  bzw.  $\bar{H}$  Elemente der Gruppen  $\mathfrak{K}$  bzw.  $\mathfrak{H}$  sind, eine  $\mathfrak{P}$ -adische Wurzel. Dies bedeutet soviel, daß zu jedem Werte von  $t$  ein geeignetes Näherungs-Polynom  $g(x)$  von  $G(x) \pmod{p}$  existiert, dessen Koeffizienten gewöhnliche rationale ganze Zahlen sind, für welches

$$(4) \quad g(\bar{\Omega}) \equiv 0 \pmod{\mathfrak{P}^t}$$

ausfällt. Übt man auf diese Kongruenz irgendeine Operation der Gruppe  $\mathfrak{H}$  aus, so geht  $\mathfrak{P}$  in sich selbst über, folglich wird die Kongruenz

$$(4^*) \quad g(x) \equiv 0 \pmod{\mathfrak{P}^t}$$

durch jede Zahl des Komplexes  $\bar{K} R_i^{-1} \mathfrak{H} w = \mathfrak{K} R_i^{-1} \mathfrak{H} w$  erfüllt. Dieselben sind somit Wurzeln der Gleichung

$$(5) \quad G(x) = 0 \pmod{p}.$$

Infolgedessen ist  $P_i(x) = 0 \pmod{p}$  im Körper der rationalen  $p$ -adischen Zahlen irreduzibel<sup>11)</sup>. Aus dem Beweise ist ersichtlich, daß die Zerfällung von (1) in irreduzible Faktoren eine eindeutige ist.

3. Der Satz II § 1 ergibt, daß die Ordnung einer Zahl des gewöhnlichen Zahlkörpers  $K$  in bezug auf die  $\mathfrak{p}_i$  gleich ist der Ordnung, welche ihr „Bild“ im „Abbildungskörper“ der durch eine Wurzel der Gleichung  $P_i(x) = 0 \pmod{p}$  gegeben wird, in bezug auf einen Henselschen Primteiler des Körpers besitzt. Der Primteiler hat den Grad  $f_i$ , seine Norm ist äquivalent der Zahl  $p^{f_i}$ <sup>12)</sup>. Werden die Zahlen des Körpers nur in bezug

<sup>11)</sup> Diese Resultate genügen, um die folgende Frage zu lösen. Was ist die notwendige und genügende Bedingung dafür, daß die linke Seite der irreduziblen Gleichung (1) für jede Primzahlpotenz als Modul reduzibel wird. [Vgl. meine Arbeit: Zur Theorie der Fundamentalgleichung, Journal für Mathematik 149 (1919), S. 90.] Die vollständige Lösung dieses Problems ist bisher nicht ohne Anwendung der  $p$ -adischen Zahlen bekannt. Analog verhält sich der viel einfachere Satz. Zu jedem Polynom  $f(x) = x^n + a_1 x^{n-1} + \dots + a_n$  mit rationalen ganzen Koeffizienten ist ein vom Polynom abhängiger Exponent  $t$  vorhanden, daß  $f(x) \pmod{p^v}$ ,  $v \geq t$  eindeutig als Produkt von  $(\text{mod } p^v)$  irreduziblen Faktoren darstellbar ist.

<sup>12)</sup> Es sollen hier folgende Tatsachen bemerkt werden. Es sei im Körper  $K$

$$p = \mathfrak{p}_1^{g_1} \mathfrak{p}_2^{g_2} \dots \mathfrak{p}_k^{g_k}, \quad w = \mathfrak{p}_1^{a_1} \mathfrak{p}_2^{a_2} \dots \mathfrak{p}_k^{a_k} q, \quad (p, q) = 1.$$

Bezeichnen wir eine beliebige Wurzel der Gleichung

$$P_i(x) = x^{n_i} + d_1^{(i)} x^{n_i-1} + \dots + d_{n_i}^{(i)} = 0, \quad n_i = f_i g_i$$

durch  $\Omega_i$ , einen Henselschen Primteiler, des durch  $\Omega_i$  gegebenen Körpers  $\pi_i$ . Wie wir gesehen haben, sind  $p \sim \pi_i^{g_i}$ ,  $\Omega_i \sim \pi_i^{a_i}$ . Daher ist

$$\frac{\alpha_i}{g_i} = \frac{\alpha_i f_i}{g_i f_i} = \frac{r_{n_i}^{(i)}}{n_i},$$

wo  $r_{n_i}^{(i)}$  die Ordnung der Zahl  $d_{n_i}^{(i)}$  in bezug auf  $p$  bedeutet. Nun besitzt nach

auf  $p$  untersucht, wie dies in den grundlegenden Untersuchungen von Hensel<sup>13)</sup> über die multiplikative Darstellung der algebraischen Zahlen geschieht (vgl. auch eine Abhandlung von H. Tonio Rella<sup>14)</sup>), dann genügt die Zahlen des Körpers durch solche Henselsche Grenzwerte zu ergänzen, welche mittels des Primideals  $\mathfrak{p}$  gebildet werden. In diesem Falle benützen wir nur jenen  $p$ -adischen irreduziblen Faktor von (1), welchem  $w$  genügt.

### § 3.

#### Die „algebraische“ Lösbarkeit der $p$ -adischen Gleichungen.

4. Wir können voraussetzen, daß die Gleichung

$$(6) \quad G(x) = x^n + a_1 x^{n-1} + \dots + a_n = 0, \quad G(w) = 0,$$

rationale ganze Koeffizienten besitzt und im gewöhnlichen Sinne eine irreduzible Galoissche Gleichung ist. Die Gruppe der Gleichung sei  $\mathfrak{G}$  und es soll

$$p = (\mathfrak{P} \dots)^g$$

ausfallen, wo die sämtlichen eingeklammerten Primideale vom Grade  $f$  sind. Das Primideal  $\mathfrak{P}$  besitze die Zerlegungsgruppe  $\mathfrak{S}$ , deren Ordnung gleich  $fg$  ist. Wir bekommen den  $\mathfrak{P}$ -adischen Körper, wenn wir die Zahlen des Körpers  $G$  durch die Henselschen Grenzwerte ergänzen. Im Körper der rationalen  $p$ -adischen Zahlen zerfällt  $G(x)$  in irreduzible Faktoren vom Grade  $fg$ ; der Faktor, dem  $w$  genügt, besitzt die Zahlen  $\mathfrak{S}w$  als Wurzeln. (Hier wenden wir nicht die allgemeinen Resultate von § 1 an.) Die  $p$ -adische irreduzible Gleichung für  $w$  ist auch im  $p$ -adischen Sinne eine Galoissche Gleichung, ihre Gruppe ist isomorph der Gruppe  $\mathfrak{S}$ . Dieselbe ist nach Hilberts Untersuchungen „auflösbar“, durch diese Tatsache tritt unsere Behauptung in Evidenz.

H. Dumas [Sur quelques cas d'irréductibilité des polynômes à coefficients rationnels, Journal de Mathématiques (6) 2 (1906), S. 191–258] das irreduzible Polynom  $P_i(x)(p)$  eine einzige Priseuxsche Zahl in bezug  $p$ , die infolgedessen gleich dem Quotienten  $\frac{r_i^{(t)}}{n_i}$  ausfällt. [Vgl. meine Arbeit, Zur allgemeinen Theorie der algebraischen Größen, Journal für Mathematik 132 (1907) S. 21–32.]

<sup>13)</sup> Die multiplikative Darstellung usw., Journal für Mathematik 146 (1916), S. 189–215. — Untersuchung der Zahlen eines algebraischen Körpers usw., Journal für Mathematik 146 (1916), S. 216–228. — Allgemeine Theorie der Kongruenzklassengruppen usw., Journal für Mathematik 147 (1917), S. 1–15.

<sup>14)</sup> Über die multiplikative Darstellung usw., Journal für Mathematik 150 (1919), S. 157–174.

(Eingegangen am 14. Oktober 1921.)