STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZUIVERE WISKUNDE

Colloquium "P-adische getallen"

o.l.v

Prof.Dr. J.F. Koksma en Dr. C.G. Lekkerkerker

februari-december 1960

The Mathematical Centre at Amsterdam, founded the 11th of February 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications, and is sponsored by the Netherlands Government trough the Netherlands Organization for Pure Research (Z.W.O.) and the Central National Council for Applied Scientific Research in the Netherlands (T.N.O.), by the Municipality of Amsterdam and by several industries.

Deze syllabus is verkrijgbaar tegen de kosten van vermenigvuldiging en verzending, ten bedrage van f.3,25

Colloquium "P-adische getallen"

Eerste bijeenkomst: 12 februari 1960

J.F. Koksma, Algemene Inleiding.

§1. De p-adische getallen zijn ingevoerd door K. Hensel (1).
Ga uit van de schrijfwijze in ons tientallig stelsel. Daar geldt b.v. voor het getal a=432=2 eenh. + 3 tient. + 4 honderdt. Een logische schrijfwijze ware a=2,34, welke notatie echter reeds is gereserveerd voor tiendelige breuken. De getallen 2,3,4 zijn bepaald door de achtereenvolgende congruenties

$$a \equiv 2 \pmod{10}; \quad \frac{a-2}{10} \equiv 3 \pmod{10}; \quad \frac{a-2-30}{100} \equiv 4 \pmod{10}.$$

Dit laatste proces nu gaat ook op voor gebroken getallen $a = \frac{t}{n}$ mits de noemer n geen factoren 2 of 5 bevat en we een dergelijke breuk deelbaar door 10 ($\equiv 0 \pmod{10}$) noemen als de teller t het is. Met de bovengesuggereerde schrijfwijze vinden we dan bijvoorbeeld

(a) $$\frac{3}{7} = 9,\overline{241758} = 9 + 2.10 + 4.100 + 1.1000 + \ldots$$

overeenkomstig de congruenties:

$$\frac{3}{7} \equiv 9 \pmod{10}; \quad \frac{\frac{3}{7} - 9}{10} \equiv 2 \pmod{10}, \text{ enz.}$$

Dit is dus wel te onderscheiden van de decimale breuk

(b) $$\frac{3}{7} = 0,\overline{428571} = 0 + \frac{4}{10} + \frac{2}{100} + \ldots$$

waar het rechterlid in tegenstelling tot dat van (a) een in conventionele zin convergente machtreeks voorstelt.
Voor de breuk $\frac{300}{7}$ zou men gevonden hebben

(c) $$\frac{300}{7} = 0,09\overline{241758},$$

d.w.z. een verschuiving van de komma naar rechts over twee plaatsen.

Hensel gaat nu nog een stap verder en beschouwt de verzameling aller rijen

(1) $$a_{-n}a_{-n+1}\ldots a_0,a_1a_2\ldots = \frac{a_{-n}}{10^n}+\ldots+\frac{a_{-1}}{10}+a_0+a_1\cdot 10 + a_2\cdot 10^2+a_3\cdot 10^3+\ldots$$

met gehele a_i $(0\leq a_i\leq 9)$,

waarin die der afbrekende en die der repeterende slechts een deelverzameling vormen. Natuurlijk kan men de modulus 10 vervangen door iedere andere $m>1$ en uitdr. (1) beschouwen thans met $0\leq a_i\leq m-1$. Hensel definieert een optelling en een vermenigvuldiging en toont aan dat de uitdrukkingen (1) alsdan een ring vormen. Kiest men voor m een priemgetal p, dan krijgt men zelfs een lichaam: het lichaam der p-adische getallen, waarin Hensel uitvoerig de rekenkunde en hoofdstukken uit de analyse ontwikkelt (het laatste na invoering van een limietbegrip).
Het gaat dus niet om een nieuwe schrijfwijze van reeds bekende getallen, maar om een geheel nieuw getalbegrip.

§2. a. We gaan de ontwikkeling volgens Hensel hier niet uitvoeren, omdat door een idee van Kürschak((1),(2)) een andere toegangsweg tot de p-adische getallen wordt gegeven, die de definities en de resultaten van Hensel in een algemeen licht plaatst.
Ga uit van het lichaam Q der rationale getallen, van dat der reële getallen R of van dat der complexe getallen C. In elk dier lichamen heeft men het begrip "absolute waarde": aan een willekeurig element a van het lichaam is een getal $|a|\geq 0$ toegevoegd met de eigenschappen:

$|0| = 0$; $|a| > 0$ als $a\neq 0$, $|ab| = |a|\cdot|b|$ en

(de "driehoeksongelijkheid"): $|a+b|\leq |a| + |b|$.

Dit begrip maakt de invoering van het limietbegrip mogelijk; vele belangrijke bewijzen betreffende limieten berusten op de driehoeksongelijkheid. Gaat men uit van het lichaam Q, dan stoot men via het beginsel van Cauchy op de fundamentaalrijen $\{a_n\}$, d.w.z. op rijen met de eigenschap dat voor iedere positieve ε op den duur geldt $|a_n-a_m|<\varepsilon$.
Een rij met $a_n\to 0$ heet nulrij. Twee fundamentaalrijen $\{a_n\}$ en $\{b_n\}$ heten aequivalent als hun verschilrij $\{a_n-b_n\}$ een nulrij is.
Terwijl iedere in Q convergente rij een fundamentaalrij is, geldt het omgekeerde niet en juist door zulke rijen (althans de aequivalentie-

klassen van zulke rijen) per definitie te beschouwen als "reële getallen", kan men Q "completeren" tot het lichaam R der reële getallen.

b. Ga nu uit van een willekeurige ring K met elementen $\alpha_1\ \beta_1\ \gamma_1 \ldots$ en probeer daar een analogon van het begrip absolute waarde in te voeren door de definitie ener waardering(sfunctie) $v(\alpha)$ met de volgende eigenschappen

$$(\mathrm{I}) \quad \begin{cases} v(0) = 0 \\ v(\alpha) > 0 \text{ als } \alpha \neq 0 \\ v(\alpha\beta) = v(\alpha) \cdot v(\beta) \\ v(\alpha+\beta) \leq v(\alpha) + v(\beta). \end{cases}$$

We kunnen in zo'n gewaardeerde ring dan een limietdefinitie invoeren door voor $\alpha_n \in K$, $\alpha \in K$ te zeggen: $\operatorname{Lim} \alpha_n = \alpha$ dan en slechts dan als bij iedere $\varepsilon > 0$ op den duur geldt

$$v(\alpha - \alpha_n) < \varepsilon.$$

Nodig voor convergentie is weer dat de rij $\{\alpha_n\}$ een "fundamentaalrij" is, d.w.z. dat op den duur bij iedere $\varepsilon > 0$ geldt

$$v(\alpha_n - \alpha_m) < \varepsilon .$$

Uit de driehoeksongelijkheid volgt:

$$v(\alpha_n) = v(\alpha_m + \alpha_n - \alpha_m) \leq v(\alpha_m) + v(\alpha_n - \alpha_m)$$

$$\text{of} \quad v(\alpha_n) - v(\alpha_m) \leq v(\alpha_n - \alpha_m)$$

en dus (verwissel n en m):

$$(2) \qquad |v(\alpha_n) - v(\alpha_m)| \leq v(\alpha_n - \alpha_m).$$

D.w.z. de bij $\{\alpha_n\}$ behorende reële rij $\{v(\alpha_n)\}$ vormt ook een fundamentaalrij en dus heeft $v(\alpha_n)$ een limiet voor $n \to \infty$.

Opm.1. Een dergelijke waardering (I) heeft men kennelijk altijd door te stellen:

$v(0) = 0$; $v(\alpha) = 1$, als $\alpha \neq 0$. We noemen dat de triviale waardering $v_0^*(\alpha)$, doch interesseren ons uiteraard meer voor de niet-triviale waarderingen.

Opm.2. Steeds is $v(1) = v(1.1) = v(1) \cdot v(1)$, d.w.z. $v(1) = 1$.

Opm.3. Meestal beschouwen we het geval dat K een lichaam is. Uit $\frac{\alpha}{\beta}\cdot\beta=\alpha$ volgt dan $v(\frac{\alpha}{\beta})\cdot v(\beta)=v(\alpha)$, dus

$$v(\tfrac{\alpha}{\beta}) = \frac{v(\alpha)}{v(\beta)} .$$

§3. We gaan nu volgens Kürschák de idee uit §2b op het lichaam Q der rationale getallen toepassen. We hebben daar reeds de waardering door middel van de absolute waarde $|\alpha|$, en de triviale waardering $v_0(\alpha)$. Wij definiëren thans de z.g. p-adische waardering, geschreven $v(\alpha) = |\alpha|_p$, waarbij we uitgaan van een willekeurig vast gekozen priemgetal $p \geq 2$. Daartoe schrijven we het te waarderen rationale getal α in de vorm $p^f \cdot \frac{a}{b}$, waar $b>0$ en a gehele getallen zijn die p niet als factor bevatten en waar $f \gtreqless 0$ een gehele exponent is. Dit kan kennelijk steeds als $\alpha \neq 0$ en ook slechts op één manier.
Wij definiëren nu:

$$(3) \qquad \begin{cases} v(\alpha) = |\alpha|_p = 0 \text{ voor } \alpha = 0 \\ v(\alpha) = |\alpha|_p = p^{-f} \text{ voor } \alpha \neq 0, \end{cases}$$

en kunnen dan aantonen, dat de wetten I van §2b vervuld zijn.
Bij het bewijs van (I) zal zelfs blijken, dat de driehoeksongelijkheid geldt zelfs in de verscherpte vorm

$$(4) \qquad v(\alpha+\beta) \leq \mathrm{Max}(v(\alpha),v(\beta)).$$

Hieruit volgt in tegenstelling tot de absolute-waardering waar geldt

$$|n\alpha| = n|\alpha| \to \infty \text{ voor } \alpha \neq 0 \text{ als } n \to \infty$$

de eigenschap

$$v(n\alpha) = v(\alpha+\alpha+\ldots+\alpha) \leq v(\alpha).$$

(„niet-archimedische waardering").

Opm. We kunnen dus (4) schrijven:

$$(5) \qquad |\alpha+\beta|_p \leq \mathrm{Max}(|\alpha|_p, |\beta|_p).$$

Uit het bewijs volgt zelfs nog, dat steeds geldt

$$(6) \qquad |\alpha+\beta|_p = \mathrm{Max}(|\alpha|_p, |\beta|_p), \text{ als } |\alpha|_p \neq |\beta|_p.$$

Het < teken kan dus in (5) alleen optreden als $|\alpha|_p = |\beta|_p$.

§4. Men zal opmerken, dat de gewone waardering $v(\alpha)=|\alpha|$ van Q haar essentiële eigenschappen houdt als men ze vervangt door $\overline{v}(\alpha)=|\alpha|^c$ bij een willekeurige constante exponent c met $0<c\leq 1$. Net zo houdt de p-adische waardering $v(\alpha)=|\alpha|_p=p^{-f}$ haar eigenschappen als men haar vervangt door $\overline{v}(\alpha)=|\alpha|_p^c=p^{-cf}$ met willekeurige constante exponent $c>0$.
Afgezien van die speling geldt de stelling van Ostrowski (3):
<u>Het lichaam Q der rationale getallen laat geen andere waardering toe dan a) de triviale; b) de absolute, c) de p-adische met willekeurig te kiezen p.</u>

§5a. Thans denken wij het lichaam Q der rationale getallen uitgebreid tot het lichaam der aequivalentieklassen van fundamentaalrijen met betrekking tot de p-adische waardering. Zulks wordt in details o.m. beschreven in het eerste hoofdstuk van Turkstra (1). Men verkrijgt dan een uitbreidingslichaam Q_p (ook: K(p)) van Q analoog aan dat der reële getallen R, doch met geheel andere eigenschappen.

b. Een gewichtig feit is dat voor elke fundamentaalrij $\{\alpha_n\}$ die geen <u>nulrij</u> is (dus waar niet geldt $\alpha_n\to 0$), een n_o bestaat zodanig dat $|\alpha_n|_p=|\alpha_{n_o}|_p$ voor alle $n\geq n_o$. Dit verrassende feit (vergelijk de opmerking bij (2)) is een gevolg van het niet-Archimedisch zijn der waardering (zie (5),(6)).

c. We kunnen nu ook K(p) waarderen: Neem een element uit K(p), dan wordt dat gerepresenteerd door een fundamentaalrij $\{\alpha_n\}$ en dan ligt het voor de hand te stellen $v(a)=\text{Lim}\, v(\alpha_n)=\lim\limits_{n\to\infty}|\alpha_n|_p=\begin{cases}|\alpha_{n_o}|_p & \text{als } \alpha\neq 0,\\ 0 & \text{als } \alpha=0.\end{cases}$

We schrijven weer $|a|_p$ in plaats van $v(a)$.

De verzameling der waarden op K(p) is dus dezelfde als die op Q, in sterke tegenstelling met het gedrag van R t.o.v. Q ("discrete" waardering op K(p) tegenover "continue" waardering op R).
Natuurlijk moet even bewezen worden, dat de definitie van $|a|_p$ op K(p) aan alle eisen (I) voldoet. Het blijkt weer dat ook aan (5) en (6) voldaan is. Ook volgt dat K(p) nu <u>volledig</u> is, d.w.z. dat iedere fundamentaalrij $\{a_n\}$ met elementen uit K(p) een limiet heeft in K(p).

d. Zeer belangrijk is dat wegens

$$|u_{n+1}+\ldots+u_{n+k}|_p \leqq \operatorname*{Max}_{i=1,2,\ldots,k} |u_{n+i}|_p$$

het volgende convergentiekriterium voor reeksen geldt:

Stelling. De reeks $\sum_{n=1}^{\infty} u_n$ met elementen $u_n \in K(p)$ convergeert dan en slechts dan als $u_n \to 0$ voor $n \to \infty$.

e. Men bewijst nu, dat bij iedere $a \in K(p)$ ondubbelzinnig omkeerbaar een ontwikkeling

$$(7) \qquad a = a_{-n}p^{-n}+a_{-n+1}p^{-n+1}+\ldots+a_0+a_1p+a_2p^2+\ldots \qquad (a_i=0,1,\ldots \text{ of } p-1)$$

kan worden gevonden. Kennelijk is deze reeks convergent (zie § 5d). Voor a schrijven we nu ook

$$a = a_{-n}a_{-n+1}\ldots a_0,a_1a_2\ldots$$

waardoor de aansluiting aan het door Hensel gedefinieerde lichaam der grootheden (1) met p in plaats van 10 uit § 2 gevonden is.

§ 6. In dit lichaam K(p), of algemener in niet-archimedisch gewaardeerde lichamen, kan men nu rekenkunde (Hensel (1),(2)) en analyse bedrijven: theorie der machtreeksen en analytische functies (Schöbe (1), Loonstra (1), de Groot (1)), theorie der continue functies (Dieudonné (1), Mahler (12)) en der differentiaalvergelijkingen (Dieudonné (1), Loonstra (1)), theorie der algebraische en transcendente getallen (Mahler (1),(2),(4),(5), Turkstra (1), Lock (1)), meetkunde der getallen (Mahler (9),(10),(11), Monna (2)), diophantische approximaties (Chabauty (1), Lock (1), Lutz (1), Mahler (3), Turkstra (1)), theorie der lineaire ruimten (Hilbert-ruimten) (Kalish (1), Dorleyn (1), Monna (3)) en maattheorie in de zin van Lebesgue (Turkstra (1), Popken en Turkstra (1), Monna (1), Lock (1)) en in de zin van Hausdorff (Lock (1)). Natuurlijk hebben speciaal de algebraische aspecten ook zeer sterk de onderzoekers getrokken (Ostrowski (1),(2),(3),(4), Rychlik (1), Krull (1), Mahler (6), (7), (8), Schilling (3) en vele anderen).

§ 7. We noemen enkele eenvoudige losse feiten en stellingen over K(p) ter illustratie van de bovengenoemde probleemgebieden; in volgende colloquia kan daarop wellicht worden teruggekomen.

1) Intervallen $|x-\alpha|_p < r$ met "middelpunt" α en positieve "straal" r zijn zowel open als gesloten. Iedere x uit zo'n interval kan als middelpunt fungeren. Hebben twee intervallen een punt gemeen, dan ligt een er van geheel in de ander.

2) In verband met de grafische voorstelling van K(p) (een "boom") noemt men het interval uit b) ook: takverzameling.

3) De machtreeks $\sum_{n=0}^{\infty} \frac{x^n}{n!}$ is ook in p-adische zin convergent, mits $|x|_p < 1$. $p \neq 2$. Voor $p = 2$ moet $|x|_p \leqslant \frac{1}{4}$ zijn.

4) Voor ieder irrationaal algebraisch getal α uit K(p) geldt als $\frac{u}{v}$ een rationaal getal is

$$\left|\alpha - \frac{u}{v}\right|_p \geq \frac{c(\alpha)}{\{\operatorname{Max}|u|, |v|\}^n}$$

als n de graad van α is. Hierin hangt $c(\alpha)$ alleen van α af.

5) Het getal $\sum_{n=0}^{\infty} p^{n!}$ is transcendent.

6) Bij iedere op $|x|_p \leq 1$ uniform continue functie $\varphi(x)$ met p-adische waarden is een rij functies $\varphi_n(x)$ aan te geven met

$$\varphi_n(x) \Rightarrow \varphi(x)$$
$$\varphi_n'(x) \Rightarrow 0,$$

hetgeen wel sterk afwijkt van de theorie in R of C.

Algemene literatuurlijst:

C. Arf — Untersuchungen über reinverzweigte Erweiterungen diskret bewerteter perfekter Körper. J.für Math.164 (1921).

E. Artin — Uber die Bewertungen algebraischer Zahlkörper. J.f.d. r.u.ang.Math.167 (1932).

E. Artin en G. Whapples — Axiomatic characterization of fields by the product formula for valuations. Bull.A.M.S.51 (1945).

C. Chabauty — Répartition modulo un de suites p-adiques. C.R.Acad. Sci.Paris 231 (1950).

M. Deuring — Verzweigungstheorie bewerteter Körper. Math.Annalen 105 (1931).

J. Dieudonné — Sur les fonctions continues p-adiques. Bull.Sci.Math. (2), 68 (1944).

M. Dorleijn — Beschouwingen over coördinatenruimten, oneindige matrices en determinanten in een niet-archimedisch gewaardeerd lichaam. Diss. V.U. 1951.

A. Fraenkel — Axiomatische Begründungen von Hensels P-adische Zahlen. J.f.d.r.u.ang.Math.141 (1912).

J. de Groot — Bemerkungen über die analytische Fortsetzung in bewertete Körpern. Proc.Ned.Akad.v.Wetensch.45 (1942).

J. de Groot en F. Loonstra — Topologische Eigenschaften bewerteter Körpern. Proc.Ned.Akad.v.Wetensch.45 (1942).

H. Hasse (1) Uber p-adische Schiefkörper und ihre Bedeutung für die Arithmetik hyperkomplexer Zahlsysteme. Math.Ann.104 (1931).

——— (2) Zahlentheorie. Berlijn 1949.

——— en Schmidt — Die Struktur diskret bewerteten Körper. J.f.d.r. u.ang.Math.170 (1934).

K. Hensel (1) Theorie der algebraischen Zahlen I. Leipzig 1908.

——— (2) Zahlentheorie. Berlijn 1913.

V. Jarnik — Uber einen p-adischen Ubertragungssatz. Monatsh.Math. Phys.48 (1939).

G.K. Kalish — On p-adic Hilbert spaces. Ann.of Math.(2)48 (1947).

I. Kaplansky (1) Maximal fields with valuations. Diss.Harvard 1941.

——— (2) Maximal fields with valuations. Duke J. 9 (1942).

M. Krassner — Sur la primitivité des corps P-adiques. Mathematica XIII (1937).

W. Krull — Allgemeine Bewertungstheorie. J.f.d.r.u.ang.Math.167 (1932)

D.J. Lock — Metrisch-diophantische onderzoekingen in $K(P)$ en $K^{(n)}(P)$. Diss. V.U. 1947.

F. Loonstra (1) Analytische Untersuchungen über bewertete Körper. Diss. Amsterdam 1941.

——— (2) Im Kleinen kompakte nichtarchimedische bewertete Körper. Proc.Ned.Akad.v.Wetensch.45 (1942).

——— (3) Pseudokonvergente Folgen in nichtarchimedisch bewerteten Körpern. Proc.Ned.Akad.v.Wetensch.45 (1942).

E. Lutz Sur les approximations diophantiennes P-adiques. Diss. Parijs 1955.

K. Mahler (1) Ein Beweis der Transzendenz der P-adischen Exponentialfunktion. J.f.d.r.u.ang.Math.169 (1933).

———— (2) Zur Approximation P-adischer Irrationalzahlen. Nieuw Arch.v.Wisk.(2) 18 (1934).

———— (3) Uber Diophantische Approximationen im Gebiete der P-adischen Zahlen. Jahresber.d.D.Math.Ver.44 (1934).

———— (4) Uber eine Klasseneinteilung der P-adischen Zahlen. Mathematica III (1934-1935).

———— (5) Uber transzendente P-adische Zahlen. Comp.Math.2 (1935).

———— (6) Uber Pseudobewertungen I. Acta Math.66 (1935).

———— (7) Uber Pseudobewertungen Ia. Proc.Ned.Akad.v.Wetensch.39 (1936).

———— (8) Uber Pseudobewertungen II. Acta Math.67 (1936).

———— (9) Ein P-adisch Analogon zu einem Satz von Tchebychef. Mathematica B7 (1938).

———— (10) On a geometrical representation of p-adic numbers. Ann. of Math.41 (1940).

———— (11) An analogue to Minkowski's geometry of numbers in a field of series. Ann.of Math.42 (1941).

———— (12) An interpolation series for continuous functions of a p-adic variable. J.f.d.r.u.ang.Math.199 (1958).

A.F. Monna (1) Zur Theorie des Maszes im Körper der P-adischen Zahlen. Proc.Ned.Akad.v.Wetensch.45 (1942).

———— (2) Zur Geometrie der P-adischen Zahlen. Proc.Ned.Akad.v. Wetensch.45 (1942).

———— (3) Over niet-archimedische lineaire ruimten. Proc.Ned.Akad. v. Wetensch.52 (1943).

A. Ostrowski Uber einige Fragen der allgemeine Körpertheorie. J.f.d. r.u.ang.Math.143 (1913).

———— (2) Uber sogenannte perfekte Körper. J.f.d.r.u.ang.Math.147 (1917).

———— (3) Uber einige Lösungen der Funktionalgleichung (x) (y)= (xy). Acta Math.41 (1918).

———— (4) Untersuchungen zur arithmetischen Theorie der Körper I, II,III. Math. Zeitschrift 39 (1934).

J. Popken en H. Turkstra A P-adic analogue of a theorem of Lebesgue in the theory of measure. Proc.Ned.Akad.v.Wetensch.49 (1946).

K. Rychlik Zur Bewertungstheorie der algebraischen Körper. J.f.d.r. u.ang.Math.153 (1924).

O.F.G. Schilling Class fields of infinite degree over p-adic number fields. Ann.of Math.38 (1937).

———— (2) Non-commutative valuations. Bull. A.M.S.51 (1945).

———— (3) The theory of valuations. New York 1950.

L.H. Schnirelman — Über Funktionen in algebraisch abgeschlossenen bewerteten Körpern. Bull.Acad.Sci.U.R.S.S. (1938).

W. Schöbe — Beitrage zur Funktionentheorie in nicht-archimedisch bewerteten Körpern. Diss. Münster 1930.

H. Turkstra — Metrische bijdragen tot de theorie der diophantische approximaties in het lichaam der P-adische getallen. Diss. V.U. 1936.

B.L. van der Waerden — Moderne Algebra I. Berlijn 1937.

D. Zelinsky — Non associative valuations. Bull.A.M.S.54 (1948).

Kürschák (1) — Mengentheoretisches über die Potenzreihen. Nieuw Arch.v.Wisk.(2) X (1913).

——— (2) — Über Limesbildung und die allgemeine Körpertheorie. J.f.d.r.u.ang.Math. 142 (1913).

Colloquium "P-adische getallen"

Voordracht op 26 februari 1960

door

P.C. Baayen

"Continue functies"

§8. Het lichaam Q_p wordt tot een metrische ruimte als wij de afstand van x en y op de gebruikelijke wijze definiëren door $|x-y|_p$. Het feit dat de driehoeksongelijkheid in verscherpte vorm geldt, blijkt dan vele merkwaardige gevolgen te hebben. Verschillende hiervan zijn reeds vermeld in §7.

Zo is ieder gesloten interval $|x-x_o|_p \leq \varepsilon$, dat wij ook zullen aangeven met $V_\varepsilon(x_o)$, ook open, want als bv. $p^{-n-1} \leq \varepsilon < p^{-n}$, dan is $|x-x_o|_p \leq \varepsilon$ aequivalent met $|x-x_o|_p < p^{-n}$; evenzo is ieder open interval ook gesloten. Hieruit volgt, dat Q_p volledig onsamenhangend is; d.w.z. iedere deelverzameling van Q_p die tenminste 2 punten bevat, is niet samenhangend.

Verder kan ieder punt y in $V_\varepsilon(x_o)$ als middelpunt voor dit interval fungeren:

als $x \epsilon V_\varepsilon(x_o)$, dan is $|x-y|_p \leq \max(|x-x_o|_p, |y-x_o|_p) \leq \varepsilon$, en dus $x \epsilon V_\varepsilon(y)$;

als $x \epsilon V_\varepsilon(y)$, dan is $|x-x_o|_p \leq \max(|x-y|_p, |y-x_o|_p) \leq \varepsilon$, en dus $x \epsilon V_\varepsilon(x_o)$.

Een gevolg is, dat van twee intervallen die een punt gemeen hebben, er altijd een geheel binnen de ander is gelegen: stel z ligt in $V_{\varepsilon_1}(x_o)$ zowel als in $V_{\varepsilon_2}(y_o)$, en zij bv. $\varepsilon_1 \leq \varepsilon_2$; dan is

$$V_{\varepsilon_1}(x_o) = V_{\varepsilon_1}(z) \subset V_{\varepsilon_2}(z) = V_{\varepsilon_2}(y_o).$$

Zij N_p het interval $V_1(0)$; N_p heet de verzameling der gehele p-adische getallen. Ieder getal $x \epsilon N_p$ heeft de vorm

(1) $$x = a_o + a_1 p + a_2 p^2 + \ldots + a_n p^n + \ldots,$$

waarbij elke a_i een van de getallen $0,1,\ldots,p-1$ is. Definieer, voor $n=0,1,2,\ldots$, het getal x_n door

(2) $$x_n = a_o + a_1 p + \ldots + a_n p^n;$$

dan is x de limiet van de rij $\{x_n\}$. Als $x \neq 0$, dan is iedere x_n een natuurlijk getal, en dan is dus x de limiet van een rij natuurlijke getallen; terwijl $x=0$ de limiet is van de rij $\{x^n\}$. Aangezien omgekeerd ieder natuurlijk getal tot N_p behoort, volgt, dat N_p de afsluiting is, in Q_p, van de verzameling N der natuurlijke getallen.

§9. Het is zeer belangrijk dat in Q_p de stelling van HEINE-BOREL van kracht is; als we een verzameling A compact noemen, indien iedere overdekking van A met open verzamelingen $\{G_i\}_{i\in I}$ een eindig deelstelsel bevat, dat A ook nog overdekt, dan geldt nl.

Stelling 1. Iedere begrensde gesloten verzameling in Q_p is compact.
Bewijs. Beschouw eerst N_p. Deze verzameling is de vereniging van de p disjuncte intervallen $V_{1/p}(0), V_{1/p}(1), \ldots, V_{1/p}(p-1)$. Elk dezer intervallen is op dezelfde wijze te verdelen in p deelintervallen met straal $1/p^2$, enz. Door volledige inductie volgt dat N_p, bij ieder natuurlijk getal n, overdekt wordt door eindig veel intervallen, elk met straal p^{-n}; m.a.w., N_p is totaal begrensd. Daar N_p ook gesloten is, volgt, dat N_p compact is.

Uitvoeriger:

Zij $\{G_i\}_{i\in I}$ een open overdekking van N_p, en neem aan dat N_p door geen eindig deelstelsel overdekt wordt. Dan geldt hetzelfde voor een van de intervallen $V_{1/p}(0), V_{1/p}(1), \ldots, V_{1/p}(p-1)$; zeg voor $V_{1/p}(x_1)$. Indien nu reeds geconcludeerd is, dat een zeker deelinterval $V_{p^{-n}}(x_n)$ van N_p niet door eindig veel der G_i wordt overdekt, dan zal ook weer een van de p intervallen met straal p^{-n-1}, waarin $V_{p^{-n}}(x_n)$ kan worden verdeeld, diezelfde eigenschap hebben; zeg $V_{p^{-n-1}}(x_{n+1})$.

De op deze wijze geconstrueerde rij $\{x_n\}$ is convergent, omdat $|x_{n+1}-x_n|_p \leq p^{-n}$; omdat N_p gesloten is, behoort de limiet x tot N_p, en dus behoort x ook tot een G_{i_o} . Op den duur geldt dan

$$V_{p^{-n}}(x) = V_{p^{-n}}(x_n) \subset G_{i_o},$$

waarmee een tegenspraak gevonden is. Dus N_p is compact.

Zij nu $V_{p^n}(x_o)$ een willekeurig interval. De afbeelding $x \to p^n(x-x_o)$ beeldt dit 1-1-duidig af op N_p; bovendien gaan bij deze afbeelding, zowel als bij zijn inverse, open verzamelingen over in open verzamelingen. Wij concluderen dat ook $V_{p^n}(x_o)$ compact is.

Zij tenslotte A een willekeurige begrensde gesloten verzameling. Dan is er een interval V met $A \subset V$. Als gesloten deelverzameling van de compacte verzameling V is dan A ook compact: want als $\{G_i\}_{i\in I}$ een willekeurige open overdekking is van A, dan is $\{G_i\}_{i\in I} \cup \{V \setminus A\}$ een open overdekking van V; deze bevat een eindige deeloverdekking van V, waarmee (ev. na weglating van $V\setminus A$) een eindige deeloverdekking van A is gevonden.

Opmerking. Omgekeerd volgt eenvoudig, dat iedere compacte verzameling in Q_p begrensd en gesloten is.

Wij concluderen uit stelling 1, dat Q_p locaal compact is. Bovendien volgt, geheel als in het reële geval, het aequivalent van de stelling van BOLZANO-WEIERSTRASS:

Stelling 2. Iedere oneindige begrensde verzameling in Q_p heeft een verdichtingspunt.

10. De definities van continuiteit of differentieerbaarheid van p-adische functies (met p-adisch argument en waarde) zijn gelijkluidend aan die voor reële of complexe functies. Ook bewijst men geheel als in het reële geval dat de som en het product van twee continue of differentieerbare functies weer continu resp. differentieerbaar is, enz. Daar de functie $f(x)=x$ continu en differentieerbaar is, volgt dan dat dit ook geldt voor alle polynomen.

Als men dan verder tracht in Q_p de differentiaalrekening uit te werken, blijft men al spoedig steken; het blijkt namelijk, dat in Q_p de stelling van het gemiddelde uit de differentiaalrekening niet geldt. Een heel eenvoudig voorbeeld hiervoor levert de karakteristieke functie van een interval $V_{p^{-n}}(x_0)$: deze heeft overal een afgeleide 0, maar is toch niet constant. Wij kunnen dus zelfs onmiddellijk concluderen:

"Er zijn oneindig veel lineair-onafhankelijke niet-constante p-adische functies, die elk differentieerbaar zijn op geheel Q_p en overal afgeleide 0 hebben".

J. Dieudonné (1) heeft zelfs een voorbeeld gegeven van een p-adische functie, gedefinieerd en differentieerbaar voor $x \in N_p$, die een afgeleide 0 heeft, en toch op geen interval, hoe klein ook, constant is: als

(1) $$x = a_0+a_1p+a_2p^2+\ldots+a_np^n+\ldots,$$

definieer dan

$$f(x) = a_0+a_1p^2+a_2p^4+\ldots+a_np^{2n}+\ldots;$$

het is duidelijk dat $f(x)$ in geen interval constant is; maar, als $|x-y|_p = 2p^{-n}$, dan zijn de eerste n termen in de ontwikkelingen van x en y gelijk; dus ook de eerste 2n termen in de ontwikkelingen van $f(x)$ en $f(y)$; m.a.w.

$$|f(x) - f(y)|_p \leqslant p^{-2n} = p^{-n}\cdot|x-y|_p$$

waaruit volgt dat $\frac{f(y)-f(x)}{y-x}$ de limiet 0 heeft als y tot x nadert.

Het is eenvoudig een voorbeeld te geven van een functie die continu is voor $|x|_p \leqslant 1$ maar nergens differentieerbaar: als x de ontwikkeling (1) heeft, definieer dan

$$f(x) = a_0^2+a_1^2p+\ldots+a_n^2p^n+\ldots;$$

het rechterlid is dan wel niet de standaard-ontwikkeling van $f(x)$, maar is toch een convergente reeks. Het is duidelijk dat $f(x)$ continu is voor $|x|_p \leqslant 1$; maar indien $p \geqslant 3$, dan is $f(x)$ nergens differentieerbaar:

voor iedere n zijn er tenminste 2 verschillende gehele getallen b_1,b_2, ongelijk 0, zodanig dat $0 \leqslant a_n+b_i \leqslant p-1$ $(i=1,2)$. Als dan $h_i=b_ip^r$, dan is $|h_i|_p=p^{-n}$ $(i=1,2)$, en

$$\frac{f(x+h_i)-f(x)}{h_i} = 2a_n+b_i \qquad (i=1,2);$$

zodat

$$\left|\frac{f(x+h_1)-f(x)}{h_1} - \frac{f(x+h_2)-f(x)}{h_2}\right|_p = |b_1-b_2|_p = 1 .$$

Dus heeft $\frac{f(x+h)-f(x)}{h}$ geen limiet, voor $h \to 0$.

Een geheel ander voorbeeld, dat ook juist blijft voor p=2, is gegeven door K. Mahler (12), en zal door de volgende spreker worden behandeld.

§11. Als wij trachten een integraalbegrip in te voeren in Q_p, dan wordt de situatie aanzienlijk moeilijker. Doordat nl. Q_p volledig onsamenhangend is, bestaat een weg in Q_p altijd uit slechts 1 punt. Het is dus niet mogelijk een bepaalde integraal in te voeren. Het enige dat we ons kunnen afvragen is, of een gegeven functie $f(x)$ een primitieve functie bezit.

Voor continue $f(x)$ is dit probleem volledig opgelost door J. Dieudonné (1), die bewezen heeft dat iedere differentiaalvergelijking met continu rechterlid een oplossing heeft:

Stelling 3. Zij $F(x,y)$ een functie van 2 p-adische variabelen, met waarden in Q_p, en continu voor $|x-x_0|_p \leq a$, $|y-y_0|_p \leq b$. Zij η een willekeurige positieve constante. Dan bestaat er een functie $f(x)$, continu en differentieerbaar voor $|x-x_0|_p \leq a$, zodanig dat

(a) $f(x_0)=y_0$,

(b) $f'(x)=F(x,f(x))$ voor alle x met $|x-x_0|_p \leq a$,

(c) $|f(x)-y_0|_p \leq \eta$ voor alle x met $|x-x_0|_p \leq a$.

Bewijs. We mogen aannemen dat $x_0=y_0=0$ en $a=1$. Als $|x|_p \leq 1$, dan kunnen we x weer in de vorm (1) schrijven; we definiëren x_n weer door (2).

Zij $M=\max\{|F(x,y)|_p : |x|_p \leq 1, |y|_p \leq b\}$, en zij k een geheel getal, zodanig dat

$$(3) \qquad p^{-(k+1)}M \leq \min(\eta,b).$$

Wij definiëren, voor $|x|_p \leq 1$:

$$\begin{aligned} f_n(x) &= 0 && \text{als } 0 \leq n \leq k; \\ f_k(x) &= (x-x_k)F(x_k,0); \\ f_n(x) &= f_{n-1}(x_n)+(x-x_n)F(x_n,f_{n-1}(x_n)) && \text{als } k < n. \end{aligned}$$

Wij vinden dan, voor $n > k$:

$$(4) \qquad |f_{n+1}(x)-f_n(x)|_p = |x-x_{n+1}|_p \cdot F(x_{n+1},f_n(x_{n+1}))-F(x_n,f_{n-1}(x_n))|_p \leq p^{-(n+2)} \cdot M;$$

daar bovendien

$$|f_k(x)|_p = |x-x_k|_p \cdot |F(x_k,0)|_p \leq p^{-(k+1)} \cdot M,$$

volgt door inductie dat voor alle n

$$(5) \qquad |f_n(x)|_p \leq p^{-(k+1)} \cdot M \leq \min(\eta,b),$$

en dus is bovenstaande definitie zinvol.

Uit (4) volgt bovendien dat $f_{n+1}(x)-f_n(x) \to 0$ voor $n\to\infty$, en dus convergeert $\{f_n(x)\}$ naar een functie $f(x)$; daar steeds $f_n(0)=0$, is $f(0)=0$, en uit (5) volgt dat $|f(x)|_p \leq \eta$ voor $|x|_p \leq 1$. Wij zullen bewijzen dat $f(x)$ differentieerbaar is en aan (b) voldoet.

In de eerste plaats volgt uit (4) door inductie, dat voor $n \geqslant k$ en alle i

$$|f_{n+i}(x) - f_n(x)|_p \leqslant p^{-(n+1)} \cdot M;$$

hieruit volgt, voor $i \to \infty$, dat

$$|f(x) - f_n(x)|_p \leqslant p^{-(n+1)} \cdot M \,, \quad \text{voor } n \geqslant k.$$

De rij $\{f_n(x)\}$ is dus uniform convergent.

Aangezien $F(x,y)$ continu is op de compacte verzameling $|x|_p \leqslant 1$, $|y|_p \leqslant b$, is F daar ook uniform continu; indien dus een willekeurige $\varepsilon > 0$ gegeven is, dan bestaat er een $\delta > 0$ zodanig dat $|F(x,y)-F(x',y')|_p \leqslant \varepsilon$ is zodra $|x-x'|_p \leqslant \delta$ en $|y-y'|_p \leqslant \delta$. Zij m een geheel getal met

$$p^{-(m+1)} \cdot (M+1) \leqslant \delta \;;$$

dan geldt voor $n \geqslant m$:

$$|x-x_n|_p \leqslant \delta \,,$$

en

$$|f(x)-f_{n-1}(x_n)|_p \leqslant \delta \,;$$

en dus

$$|F(x_1,f(x)-F(x_n,f_{n-1}(x_n))|_p \leqslant \varepsilon \,;$$

uit (4) volgt dan

$$|f_{n+1}(x)-f_n(x)|_p \leqslant |x-x_{n+1}|_p \cdot \varepsilon \leqslant p^{-(n+2)} \cdot \varepsilon \,,$$

en vervolgens

(6) $$|f_{n+i}(x)-f_n(x)|_p \leqslant \varepsilon \cdot \max(p^{-(n+i+1)}, \ldots, p^{-(n+2)}) = \\ = p^{-(n+2)} \cdot \varepsilon \,,$$

voor $n \geqslant k$ en $i=1,2,3,\ldots$.

Zij nu x willekeurig in N_p, en zij x' zo gekozen dat $|x-x'|_p \leqslant p^{-(m+1)}$. Als n het gehele getal ($\geqslant m$) is zodat $|x-x'|_p = 2^{-(n+1)}$, dan is $x'_n = x_n$, en $x'_{n+1} \neq x_{n+1}$. Wij vinden dan:

$$f_n(x') - f_n(x) = (x'-x)F(x_n,f_{n-1}(x_n)),$$

en dus

$$\left|\frac{f_n(x')-f_n(x)}{x'-x} - F(x,f(x))\right|_p = \\ = |F(x_n,f_{n-1}(x_n))-F(x,f(x))|_p \leqslant \varepsilon \,.$$

Uit (6) volgt

$$|f_{n+i}(y) - f_n(y)|_p \leq \varepsilon \cdot p^{-(n+2)} = \frac{\varepsilon}{p} \cdot |x-x'|_p$$

voor y=x en voor y=x'; en dus geldt, voor i=1,2,3,...

$$\left| \frac{f_{n+i}(x')-f_{n+i}(x)}{x'-x} - F(x,f(x)) \right|_p \leq \max \left\{ \left| \frac{f_{n+i}(x')-f_n(x')}{x'-x} \right|_p , \left| \frac{f_{n+i}(x)-f_n(x)}{x'-x} \right|_p \left| \frac{f_n(x')-f_n(x)}{x'-x} - F(x,f(x)) \right|_p \right\} \leq \varepsilon .$$

Voor $i \to \infty$ volgt

$$\left| \frac{f(x')-f(x)}{x'-x} - F(x,f(x)) \right|_p \leq \varepsilon$$

voor alle x' met $|x'-x|_p \leq p^{-(m+1)}$; dus is inderdaad f differentieerbaar, en (b) geldt.

Opmerking 1. Er volgt, dat een functie, continu op een gesloten interval, oneindig veel primitieven heeft die door eenzelfde punt gaan.

Opmerking 2. Als x en x' willekeurige punten zijn in N_p, dan geldt voor $n > k$

$$|f_n(x)-f_n(x')|_p = |x-x'|_p \cdot |F(x_n, f_{n-1}(x_n))|_p \leq |x-x'|_p \cdot M;$$

en dus

$$|f(x) - f(x')|_p \leq |x-x'|_p \cdot M.$$

Voor de op deze wijze gedefinieerde functies f(x) geldt dus de st. van het gemiddelde wel. Als bv. $F(x,y)=x^{p-1}$, dan is de op deze wijze verkregen primitieve functie f(x) van x^{p-1} dus zeker niet de functie $\frac{x^p}{p}$.

12. Het had voor de hand gelegen, te pogen een primitieve functie van f(x) te vinden, door f(x) uniform te benaderen door polynomen (waarvoor immers dadelijk primitieve functies zijn aan te geven). In het reële geldt toch, dat iedere uniform convergente reeks termsgewijs geïntegreerd worden mag. Inderdaad bewees Dieudonné dat in Q_p het aequivalent van de stelling van WEIERSTRASS geldt:

Stelling 4. Iedere p-adische functie die continu is op een gesloten interval, kan uniform worden benaderd door polynomen.

Onafhankelijk van Dieudonné bewees Mahler (12) deze zelfde stelling. Maar het blijkt dat we er zo niet komen; want de stelling over termsgewijze integratie berust op de st. van het gemiddelde, en we hebben gezien dat deze in Q_p niet van kracht is. En inderdaad is bv. de reeks $\sum_{n=0}^{\infty} p^n x^{p^{2n}-1}$ uniform convergent voor $|x|_p \leq 1$, terwijl in de reeks van primitieve functies $\sum_{n=0}^{\infty} \frac{x^{p^{2n}}}{p^n}$ de algemene term niet naar 0 gaat voor $|x|_p = 1$.

Colloquium "P-adische getallen"
Voordracht op 25 maart 1960
door

P.C. Baayen

"Continue functies" (vervolg)

12. Voor het bewijs van het p-adisch analogon van de approximatiestelling van WEIERSTRASS gebruikt DIEUDONNÉ de volgende hulpstelling:

Lemma 1. Zij X een volledig onsamenhangende compacte Hausdorffruimte, en zij X^* een metrische ruimte, met metriek d. Zij verder A een gesloten verzameling in X, en zij f een continue afbeelding van A in X^*. Dan is er een continue afbeelding g van X in X^* die f voortzet.

Opmerking. Wij hebben alleen nodig het geval waar $X=N_p$ en $X^*=Q_p$; bij de algemenere formulering is het bewijs echter nauwelijks gecompliceerder.

Bewijs. Zij $\omega(f;V)=\sup\{d(fx,fy):x,y\in V\}$, voor $V\subset A$ ($\omega(f;V)$ is de oscillatie van f in V). Omdat f continu is op A, heeft ieder punt $x\in A$ een omgeving U_x zodanig dat $\omega(f;U_x)\leq 1$. Daar X volledig onsamenhangend en compact is, heeft x dan ook een tegelijk open en gesloten omgeving V_x met $V_x\subset U_x$; natuurlijk is ook $\omega(f;V_x)\leq 1$. Daar A gesloten en dus compact is, kan A overdekt worden door eindig veel dergelijke V_x; zeg door $B_1,\dots,B_n$.

Laten $A_1,\dots,A_m$ de niet-lege verzamelingen zijn onder de 2^n verzamelingen $C_1\cap\dots\cap C_n$, waar $C_\nu=B_\nu$ òf $C_\nu=X\setminus B_\nu$, voor $\nu=1,\dots,n$. Dan vormen $A_1,\dots,A_m$ een partitie van X in (disjuncte niet-lege) tegelijk open en gesloten verzamelingen, met $\omega(f;A_\mu\cap A)\leq 1$, voor $\mu=1,\dots,m$.

Definieer f_1 op X als volgt: indien $A_\mu\cap A=0$, dan zij $f_1x=0$, voor alle $x\in A_\mu$; indien $A_\mu\cap A\neq 0$, kies dan $x_\mu\in A_\mu\cap A$, en stel $f_1x=fx_\mu$, voor alle $x\in A_\mu$. Dan is f_1 continu op X, daar alle A_μ tegelijk open en gesloten zijn; en voor alle $x\in A$ geldt:

$$d(fx,f_1x)\leq 1.$$

Neem nu aan dat reeds n continue functies $f_1,\dots,f_n$ op X geconstrueerd zijn, die de volgende eigenschappen hebben:

(I) $d(fx, f_\nu x) \leq \nu^{-2}$, voor $x \in A$ en $\nu = 1, \ldots, n$;

(II) $d(f_{\nu+1}x, f_\nu x) \leq \nu^{-2}$, voor $x \in X$ en $\nu = 1, \ldots, n-1$;

(III) Er is een partitie van X in tegelijk open en gesloten verzamelingen $A_1, \ldots, A_m$, zodanig dat
(a) $f_\nu | A_\mu$ is constant, voor $1 \leq \nu \leq n$ en $1 \leq \mu \leq m$;
(b) Als $A_\mu \cap A \neq 0$, dan is $\omega(f; A \cap A_\mu) \leq n^{-2}$ $(1 \leq \mu \leq m)$;
(c) Als $A_\mu \cap A \neq 0$, dan is er voor iedere ν met $1 \leq \nu \leq n$ een $x_\nu \in A_\mu$ zodanig dat $f_\nu x_\nu = f x_\nu$ $(1 \leq \mu \leq m)$.

Wij zullen een op X continue functie f_{n+1} construeren zodanig dat het stelsel $\{f_1, \ldots, f_{n+1}\}$ weer deze eigenschappen heeft.

Indien $A_\mu \cap A = 0$, zij dan $f_{n+1}x = f_n x$, voor alle $x \in A_\mu$; indien $A_\mu \cap A \neq 0$, overdek dan $A_\mu \cap A$ met eindig veel tegelijk open en gesloten verzamelingen $B_{\mu 1}, \ldots, B_{\mu k}$, zodanig dat $\omega(f; B_{\mu\kappa}) \leq (n+1)^{-2}$ voor $1 \leq \kappa \leq k$, en zij $A_{\mu 1}, \ldots, A_{\mu s_\mu}$ de corresponderende partitie van A_μ (vgl. de constructie van f_1). Indien nu $A_{\mu\sigma} \cap A = 0$, stel $f_{n+1}x = f_n x$, voor alle $x \in A_{\mu\sigma}$; maar indien $A_{\mu\sigma} \cap A \neq 0$, kies dan $x_{\mu\sigma} \in A_{\mu\sigma} \cap A$ en stel $f_{n+1}x = f x_{\mu\sigma}$, voor $x \in A_{\mu\sigma}$.

Op deze wijze is aan (I) voldaan voor $\nu = n+1$, want als $x \in A$, dan is $x \in A_{\mu\sigma} \cap A$, voor zekere μ, σ, en

$$d(f_{n+1}x, fx) \leq \omega(f; A_{\mu\sigma} \cap A) \leq (n+1)^{-2};$$

en aan (II) is ook voldaan, voor $\nu = n$; want als $f_{n+1}x \neq f_n x$, dan is $x \in A_{\mu\sigma} \cap A \subset A_\mu \cap A$, voor zekere μ, σ, en op grond van (III,c) en de definitie van f_{n+1} zijn er punten $x_o, y_o \in A_\mu \cap A$ zodat $f_{n+1}x = f x_o$ en $f_n x = f y_o$; en dus is

$$d(f_{n+1}x, f_n x) = d(f x_o, f y_o) \leq \omega(f; A_\mu \cap A) \leq n^{-2},$$

waarbij de laatste ongelijkheid geldt op grond van (III,b). Tenslotte is het duidelijk dat de nieuwe partitie van X, die we gebruikten om f_{n+1} te definiëren, weer aan de voorwaarden in (III) voldoet.

Zo is dus door inductie een rij continue functies $\{f_n\}$ op X geconstrueerd, zodanig dat (I) en (II) gelden voor $\nu = 1, 2, \ldots$. Op grond van (II) is deze rij uniform convergent; zij g zijn limiet. Dan is g continu op X, en $g|A = f$, op grond van (I).

Aangezien wij essentieel gebruik zullen maken van de eigenschappen van het polynoom $h(x) = 1 - x^{p-1}$ in Q_p, is het nuttig deze in een hulpstelling samen te vatten.

Lemma 2. Zij $h(x)=1-x^{p-1}$. Dan gelden de volgende (on)gelijkheden:

(1) $|h(x)|_p = 1$, als $|x|_p < 1$;

(2) $|h(x)|_p < 1$, als $|x|_p = 1$;

(3) $|h(x)^{p^n}-1|_p \leq p^{-n}$, als $|x|_p < 1$;

(4) $|h(x)^{p^n}|_p \leq p^{-p^n}$ als $|x|_p = 1$;

(5) $|h(x)^{p^n}|_p = |x|_p^{(p-1)\cdot p^n}$, als $|x|_p > 1$.

Bewijs. Als $|x|_p < 1$, dan is $|x|_p \neq |1|_p$ en dus $|1-x^{p-1}|_p =$ $= \max(|1|_p, |x|_p^{p-1}) = |1|_p = 1$. Dit bewijst (1).

Als $|x|_p=1$, schrijf dan x in standaardontwikkeling: $x=a_0+a_1p+a_2p^2+\ldots$; dan is $a_0\neq 0$. De eerste term in de standaardontwikkeling van x^{p-1} is de rest van a_0^{p-1} modulo p; volgens de stelling van Fermat is deze 1; en dus begint de ontwikkeling van $x^{p-1}-1$ met een term die p bevat. Dit bewijst (2); zelfs volgt: $|h(x)|_p \leq \frac{1}{p}$, als $|x|_p=1$. Dan is ook $|h(x)^{p^n}|_p = |h(x)|_p^{p^n} \leq p^{-p^n}$, voor $|x|_p=1$; waarmee (4) is bewezen.

Als $|x|_p > 1$, dan is $|h(x)|_p = |1-x^{p-1}|_p = \max(1, |x|_p^{p-1}) = |x|_p^{p-1}$, en (5) volgt.

Zij tenslotte $|x|_p < 1$, en trachten wij (3) te bewijzen. In dit geval is $|x|_p \leq \frac{1}{p}$; dus heeft de ontwikkeling van $1-x^{p-1}$ de gedaante

$$h(x) = 1-x^{p-1} = 1+cp^r+dp^{r+1},$$

waar c een van de getallen $1,2,\ldots,p-1$ is; r een natuurlijk getal ≥ 1; en $d\in N_p$. Dan volgt:

$$h(x)^p = 1+p\cdot cp^r + \frac{p(p-1)}{2}c^2p^{2r} + d'p^{r+2} =$$

$$= 1+cp^{r+1} + d''p^{r+2};$$

de tweede term in de ontwikkeling van $h(x)^p$ bevat dus tenminste p^{r+1}. Door inductie volgt dat de tweede term in de ontwikkeling van $h(x)p^n$ tenminste p^{r+n} bevat; d.w.z.

$$|h(x)^{p^n}-1|_p \leq p^{-r-n} \leq p^{-n}.$$

§13. Nu kunnen we dan het p-adisch analogon van de stelling van WEIERSTRASS bewijzen:

Stelling 4. Zij K een compacte verzameling in Q_p, en zij f een p-adische functie, gedefinieerd en continu op K. Dan is er bij iedere $\varepsilon > 0$ een polynoom g, zodanig dat

$$|f(x)-g(x)|_p \leq \varepsilon \text{ , voor alle } x \in K.$$

Bewijs.

1. Zij, voor ieder natuurlijk getal n, $U_n = V_{p^{-n}}(0)$. Wij bewijzen eerst een bijzonder geval:
Zij $r < s$ (en dus $U_r \supset U_s$), en zij f op U_r als volgt gedefinieerd: $f(x)=1$ voor $x \in U_s$, en $f(x)=0$ voor $x \in U_r \setminus U_s$. Dan kan f op U_r uniform benaderd worden door polynomen.
Het bewijs is door inductie voor $s-r$.
BASIS: Stel $s=r+1$. Dan is dus $f(x)=1$ als $|x|_p \leq p^{-r-1}$, en $f(x)=0$ als $|x|_p = p^{-r}$; we kunnen f dan benaderen door de polynomen $h(p^{-r}x)^{p^n}$. Want volgens Lemma 2, (3) en (4) geldt:

$$|h(p^{-r}x)^{p^n}-1|_p \leq p^{-n} \quad \text{als } |p^{-r}x|_p < 1, \text{ i.e. als } |x|_p < p^{-r};$$

$$|h(p^{-r}x)^{p^n}-0|_p \leq p^{-p^n} \quad \text{als } |p^{-r}x|_p = 1, \text{ i.e. als } |x|_p = p^{-r}.$$

INDUCTIESTAP: Zij $0 < \varepsilon < 1$. Volgens de inductie-aanname is er een polynoom $h_1(x)$ zodanig dat

$$|h_1(x)-1|_p \leq \varepsilon \quad \text{als } x \in U_s;$$

$$|h_1(x)-0|_p \leq \varepsilon \quad \text{als } x \in U_{s-1} \setminus U_s.$$

Zij $M=\max\{|h_1(x)|_p : x \in U_r \setminus U_s\}$ (dit maximum bestaat, omdat $U_r \setminus U_s$ compact is).
Op grond van de inductiehypothese is er dan ook een polynoom $h_2(x)$ zodanig dat

$$|h_2(x)-1|_p \leq \varepsilon \quad \text{als } x \in U_{s-1};$$

$$|h_2(x)-0|_p \leq \frac{\varepsilon}{M+1} \quad \text{als } x \in U_r \setminus U_{s-1}.$$

Zij tenslotte $g(x)=h_1(x)h_2(x)$; dan is ook g een polynoom, en er geldt, voor alle $x \in U_r$:

$$|g(x)-f(x)|_p \leq \varepsilon .$$

Immers, is $x \in U_s$, schrijf dan $g(x)=1+(h_1(x)-1)+(h_2(x)-1)+$

er volgt dan dat $|g(x)-f(x)|_p = |g(x)-1|_p \leq \varepsilon$. Is $x \in U_{s-1} \setminus U_s$, schrijf dan $g(x)=h_1(x)+h_1(x)(h_2(x)-1)$; we concluderen dat $|g(x)-f(x)|_p = |g(x)|_p \leq \varepsilon$. Is tenslotte $x \in U_r \setminus U_{s-1}$, dan geldt: $|g(x)-f(x)|_p = |g(x)|_p = |h_1(x)|_p |h_2(x)|_p \leq M \cdot \frac{\varepsilon}{M+1} < \varepsilon$.

2. Een onmiddellijke conclusie is de volgende: zijn U en V willekeurige intervallen in Q_p met $U \supset V$, en is f de karakteristieke functie van V, beperkt tot U, dan kan f op U uniform benaderd worden door polynomen.

3. Tenslotte behandelen we het algemene geval. Aangezien K compact is, is K begrensd; dus is $K \subset U_r$, voor zekere r. Op grond van Lemma 1 kunnen we f continu voortzetten over geheel U_r; deze voortgezette functie geven we gemakshalve weer aan met f.

Aangezien U_r compact is, is f uniform continu op U_r. Is $\varepsilon > 0$ gegeven, dan is er dus een $s > r$ zodat $\omega(f; V_{p^{-s}}(x)) \leq \varepsilon$, voor alle $x \in U_r$. Overdek U_r door eindig veel verschillende intervallen $V_{p^{-s}}(x)$ zeg door $V_1, \ldots, V_n$. Dan zijn $V_1, \ldots, V_n$ onderling disjunct; dus, als φ_ν de karakteristieke functie van V_ν is $(1 \leq \nu \leq n)$, dan geldt voor alle $x \in U_r$:

$$|f(x) - \sum_{\nu=1}^{n} \varphi_\nu(x) f(x_\nu)|_p \leq \varepsilon.$$

Zij nu, voor $1 \leq \nu \leq n$, g_ν een polynoom dat voldoet aan

$$|\varphi_\nu(x) - g_\nu(x)|_p \leq \varepsilon \quad , \text{ voor } x \in U_r;$$

het bestaan van g_ν is gegarandeerd door <u>2</u>. Als dan $M=\max\{|f(x)|_p : x \in U_r\}$, dan geldt voor alle $x \in U_r$:

$$|f(x) - \sum_{\nu=1}^{n} f(x_\nu) g_\nu(x)|_p \leq (M+1)\varepsilon \;;$$

en $\sum_{\nu=1}^{n} f(x_\nu) g_\nu(x)$ is een polynoom, waardoor f wordt benaderd.

14. Het is mogelijk stelling 4 te generaliseren, analoog aan de generalisatie van de stelling van WEIERSTRASS door M.H. STONE. Daartoe bewijzen we eerst enige hulpstellingen.

<u>Lemma 3.</u> Stel X en Y zijn volledig onsamenhangende compacte Hausdorffruimten, en zij f een continue afbeelding van de productruimte $X \times Y$ in Q_p. Dan zijn er, voor iedere $\varepsilon > 0$, een natuurlijk getal n, n continue afbeeldingen $f_1, \ldots, f_n$ van X in Q_p, en n continue afbeel-

dingen $g_1,\dots,g_n$ van Y in Q_p, zodanig dat, voor alle $(x,y)\in X\times Y$:

$$|f(x,y) - \sum_{\nu=1}^{n} f_\nu(x)g_\nu(y)|_p \leq \varepsilon .$$

Opmerking. Neemt van van X en Y alleen aan dat zij compacte Hausdorffruimten zijn, en leest men R i.p.v. Q_p (waar R de verzameling der reële getallen is, met gewone metriek), dan heeft men een stelling uit de "gewone" analyse, bewezen door DIEUDONNÉ in 1937 (Sur les fonctions continues numériques définies dans un produit de deux espaces compacts, C.R.Acad.Sc., 205, p.593-595 (1937)).

Bewijs. Zij W_{xy}, voor een willekeurig punt (x,y) van $X\times Y$, een omgeving van dit punt zodanig dat $\omega(f;W_{xy})\leq\varepsilon$. Dan zijn er tegelijk open en gesloten omgevingen U_{xy} van x en V_{xy} van y met $U_{xy}\times V_{xy}\subseteq W_{xy}$; natuurlijk is zeker $\omega(f;U_{xy}\times V_{xy})\leq\varepsilon$.

Bij vastgehouden x kan de compacte ruimte Y overdekt worden door eindig veel der omgevingen V_{xy}; er zijn dus eindig veel punten $y_1(x),\dots,y_{r(x)}^{(x)}$ in Y zodat Y wordt overdekt door de $V_{x,y_\rho}(x)$. Zij

$$U_x = \bigcap_{\rho=1}^{r(x)} U_{x,y_\rho}(x).$$

Daar X compact is, zijn er ook eindig veel punten $x_1,\dots,x_s$ in X zodanig dat $U_{x_1},\dots,U_{x_s}$ de ruimte X overdekken. Zij $A_1,\dots,A_l$ de corresponderende partitie van X (vgl. het bewijs van lemma 1); en zij $B_1,\dots,B_m$ de partitie van Y, verkregen door uit te gaan van de $r(x_1)\cdot\ldots\cdot r(x_s)$ verzamelingen $V_{x_\sigma y_\rho}(x_\sigma)$. Dan zijn alle A_λ en B_μ tegelijk open en gesloten, en er geldt, voor $1\leq\lambda\leq l$ en $1\leq\mu\leq m$,

$$\omega(f;A_\lambda\times B_\mu)\leq\varepsilon .$$

Voor $1\leq\lambda\leq l$ zij nu f_λ de karakteristieke functie van A_λ, en x_λ een vast gekozen punt in A_λ; evenzo zij g_μ, voor $1\leq\mu\leq m$, de karakteristieke functie van B_μ, en y_μ een vastgekozen punt in B_μ. De functies f_λ en g_λ zijn allen continu; en voor willekeurige $(x,y)\in X\times Y$ geldt (als $x\in A_{\lambda_0}$ en $y\in B_{\mu_0}$):

$$|f(x,y)-\sum_{\lambda,\mu} f(x_\lambda,y_\mu)f_\lambda(x)g_\mu(y)|_p = |f(x,y)-f(x_{\lambda_0},y_{\mu_0})|_p$$
$$\leq \omega(f;A_{\lambda_0}\times B_{\mu_0})\leq\varepsilon .$$

Door volledige inductie is lemma 3 uit te breiden tot het geval waar f gedefinieerd is op een eindig product $X_1\times\ldots\times X_n$ van volledig onsamenhangende compacte Hausdorffruimten. Maar wij zullen moeten werken met functies f, gedefinieerd op een willekeurig product $\prod_{\alpha\in A} X_\alpha$.

Het bewijs van onderstaande generalisatie van lemma 3 is zonder meer bruikbaar om de overeenkomstige generalisatie van de reële stelling van DIEUDONNÉ aan te tonen.

Lemma 4. Zij X_α , voor iedere $\alpha\in A$, een volledig onsamenhangende compacte Hausdorffruimte, en zij f een continue afbeelding van de productruimte $X=\prod_{\alpha\in A} X_\alpha$ in Q_p. Dan zijn er, voor iedere voorgegeven $\varepsilon>0$, eindig veel $\alpha_1,\ldots,\alpha_m\in A$, een natuurlijk getal n, en, voor iedere α_μ , continue afbeeldingen $f_{1,\alpha_\mu},\ldots,f_{n,\alpha_\mu}$ van X_{α_μ} in Q_p, zodanig dat, voor alle $x\in X$,

$$\left| f(x) - \sum_{\nu=1}^{n} f_{\nu,\alpha_1}(x_{\alpha_1})\cdot\ldots\cdot f_{\nu,\alpha_m}(x_{\alpha_m})\right|_p \leq \varepsilon \ .$$

Bewijs. Iedere $x\in X$ heeft een omgeving V_x waarvoor $\omega(f;V_x)\leq \frac{\varepsilon}{2}$, en waarbij V_x de eigenschap heeft dat $\pi_\alpha V_x=X_\alpha$, voor bijna alle $\alpha\in A$ (π_α is de projecterende afbeelding van X op X_α). Als product van compacte ruimten is X weer compact (stelling van TYCHONOFF), en dus zijn er eindig veel punten $x_1,\ldots,x_s$ in X zodat $V_{x_1},\ldots,V_{x_s}$ X overdekken.

Stel $\alpha_1,\ldots,\alpha_m$ zijn de (eindig vele) $\alpha\in A$ waarvoor $\pi_\alpha V_{x_\sigma}\neq X_\alpha$, voor tenminste één σ . Indien $\alpha\neq\alpha_1,\ldots,\alpha_m$, zij dan a_α een vastgekozen punt in X_α . Als $x\in X$, definieer dan $\overline{x}$ als volgt: $\overline{x}_{\alpha_\mu}=x_{\alpha_\mu}$ $(1\leq\mu\leq m)$; $\overline{x}_\alpha=a_\alpha$ $(\alpha\neq\alpha_1,\ldots,\alpha_\mu)$. Ook $\overline{x}$ is een punt in X.

Zij nu x een willekeurig punt in X. Dan is $x\in V_{x_\sigma}$, voor zekere σ ; maar dan is ook $\overline{x}\in V_{x_\sigma}$, en dus $|f(x)-f(\overline{x})|_p\leq \omega(f;V_{x_\sigma})$. Er volgt dat voor alle $x\in X$:

$$|f(x)-f(\overline{x})|_p \leq \frac{\varepsilon}{2} \ .$$

Nu is $f(\overline{x})$ een continue functie van de m veranderlijken $x_{\alpha_1},\ldots,x_{\alpha_m}$; het gestelde volgt dus door gebruik te maken van (de generalisatie tot eindige productruimten van) lemma 3.

§15. Wij kunnen nu DIEUDONNÉ's analogon van de stelling van STONE-WEIERSTRASS bewijzen:

Stelling 5. Zij X een volledig onsamenhangende compacte Hausdorffruimte, en zij $\{f_\alpha\}_{\alpha\in A}$ een stelsel op X continue functies met p-adische waarden, met de volgende eigenschap: als x,y verschillende punten in X zijn, dan is er een $\alpha \in A$ zodat $f_\alpha(x) \neq f_\alpha(y)$.

Dan is bij iedere op X continue functie f met waarden in Q_p, en voor willekeurige $\varepsilon > 0$, een polynoom g in eindig vele der f_α te vinden, zodanig dat, voor alle $x \in X$,

$$|f(x)-g(x)|_p \leqslant \varepsilon.$$

Bewijs. De beeldruimten $f_\alpha X$ zijn allen compacte deelruimten van Q_p. Dus is ook hun product $Y = \prod_{\alpha \in A} f_\alpha X$ een volledig onsamenhangende compacte Hausdorff-ruimte. De afbeelding φ van X in Y, gedefinieerd door: $\varphi(x)=(f_\alpha(x))$, is continu en 1-1-duidig; daar X compact is, is φ dus een topologische afbeelding. Zij ψ de inverse afbeelding van φX op X.

Ook de afbeelding $h=f \circ \psi$ van φX in Q_p is continu; op grond van lemma 1 kan h dus worden voortgezet tot een continue afbeelding $\bar{h}$ van geheel Y in Q_p. Volgens lemma 4 zijn er, bij voorgegeven $\varepsilon > 0$, eindig veel $\alpha_1, \ldots, \alpha_m \in A$, een natuurlijk getal n, en, voor iedere α_μ, n continue afbeeldingen φ_{ν,α_μ} van $f_{\alpha_\mu} X$ in Q_p, zodanig dat, voor alle $y \in Y$,

$$\left|\bar{h}(y)-\sum_{\nu=1}^{n} \varphi_{\nu,\alpha_1}(y_{\alpha_1})\, \varphi_{\nu,\alpha_2}(y_{\alpha_2}) \cdot \ldots \cdot \varphi_{\nu,\alpha_m}(y_{\alpha_m})\right|_p \leqslant \frac{\varepsilon}{2}.$$

De ruimten $f_\alpha X$ zijn allen compact; op grond van stelling 4 kan dus iedere φ_{ν,α_μ} in $f_{\alpha_\mu} X$ uniform benaderd worden door polynomen. Er is dus een polynoom $p(y_{\alpha_1}, \ldots, y_{\alpha_m})$ zodanig dat, voor alle $y \in Y$,

$$|\bar{h}(y) - p(y_{\alpha_1}, \ldots, y_{\alpha_m})|_p \leqslant \varepsilon.$$

Nemen we i.h.b. $y = \varphi(x)$, dan is $\bar{h}(y)=h(y)=f(\psi(\varphi(x))) = f(x)$, en $y_{\alpha_\mu} = (\varphi(x))_{\alpha_\mu} = f_{\alpha_\mu}(x)$; dus geldt, voor alle $x \in X$,

$$|f(x)-p(f_{\alpha_1}(x), \ldots, f_{\alpha_m}(x))|_p \leqslant \varepsilon.$$

Definieer nu: $g(x)=p(f_{\alpha_1}(x), \ldots, f_{\alpha_m}(x))$, en het bewijs is voltooid.

Tenslotte zij opgemerkt dat de analogie met de stelling van STONE-WEIERSTRASS nog vergroot kan worden. Het is nl. geoorloofd in stelling 5 de hypothese dat X volledig onsamenhangend is weg te laten. Om dit aan te tonen hebben we nog één resultaat uit de algemene topologie nodig:

Lemma 5. Zij X een compacte Hausdorff-ruimte, en zij $R(x,y)$ de aequivalentierelatie: "x en y behoren tot dezelfde maximale samenhangende component van X". Dan is X/R (de ruimte, verkregen uit X door aequivalente punten te identificeren) een volledig onsamenhangende compacte Hausdorff-ruimte.

Voor het bewijs zij verwezen naar N. BOURBAKI, Topologie Générale II, 2[e] druk, § 4, Proposition 4.

Met behulp van lemma 5 kunnen we nu gemakkelijk aantonen:

Stelling 6. Zij X een compacte Hausdorff-ruimte, en zij $\{f_\alpha\}_{\alpha\in A}$ een stelsel op X continue functies, met p-adische waarden, zodanig dat er, voor ieder puntenpaar $x,y \in X$ met $x\neq y$, een $\alpha \in A$ is met $f_\alpha(x)\neq f_\alpha(y)$. Voor iedere op X continue p-adische functie f, en voor iedere $\varepsilon > 0$, is er dan een polynoom g in eindig vele der f_α, zodanig dat, voor alle $x \in X$, $|f(x)-g(x)|_p \leq \varepsilon$.

Bewijs. Zij C een samenhangende component van X, en f een op X continue p-adische functie. Dan is $f(C)$ een samenhangende verzameling in Q_p; omdat Q_p volledig onsamenhangend is, bestaat $f(C)$ uit slechts 1 punt. M.a.w. f is op iedere component van X constant, en dus is er een op X/R continue p-adische functie φ zodat $f=\varphi\circ\pi$, waar π de natuurlijke afbeelding $X \to X/R$ is.

Evenzo is er, voor iedere $\alpha \in A$, een op X/R continue p-adische functie φ_α zodanig dat $f_\alpha = \varphi_\alpha \circ \pi$. Aangezien de ruimte X/R en het stelsel functies $\{\varphi_\alpha\}_{\alpha\in A}$ voldoen aan de hypotheses van stelling 5, zijn er eindig veel $\alpha_1,\ldots,\alpha_m \in A$, en een polynoom $p(z_1,\ldots,z_m)$ in m variabelen, zodanig dat

$$|\varphi(y)-p(\varphi_{\alpha_1}(y),\ldots,\varphi_{\alpha_m}(y))|_p \leq \varepsilon,$$

voor alle $y \in X/R$. Dan geldt ook, voor alle $x \in X$,

$$|f(x)-p(f_{\alpha_1}(x),\ldots,f_{\alpha_m}(x))|_p \leq \varepsilon,$$

waarmee de stelling volledig is bewezen.

Colloquium "P-adische getallen"

Voordracht op 6 mei 1960

door

M.A. Maurice

§16. "Continue en differentiëerbare functies"

Literatuur: K. Mahler, An interpolation series for continuous functions of a P-adic variable, Journal für die reine und angewandte Mathematik 1958 (199), 23 t/m 34).

16.1 Q_p: lichaam van alle p-adische getallen.

N_p: $\{x \,/\, x \in Q_p,\ |x|_p \leqslant 1\}$.

We beschouwen functies $f(x) \in Q_p$ voor $x \in N_p$.

N : verzameling van alle niet-negatieve geheel-rationale getallen ($N \subset N_p$).

Stelling: N ligt overal dicht in N_p.

Bewijs: zie §8.

16.2 Zij
$$a_n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} f(n-k) \qquad (n = 0,1,2,\ldots)$$
$$f^*(x) = \sum_{n=0}^{\infty} a_n \binom{x}{n} .$$

Stelling: $f^*(m) = f(m)$, indien $m \in N$.

Bewijs: volgt, na een korte herleiding, uit de definities.

16.3 Stelling: $f^*(x) = \sum_{n=0}^{\infty} a_n \binom{x}{n}$ convergeert voor alle $x \in N_p$, dan en slechts dan als $\lim_{n\to\infty} a_n = 0$.

Bewijs:

a. $f^*(-1) = \sum_{n=0}^{\infty} (-1)^n a_n$ convergeert dan en slechts dan als $\lim_{n\to\infty} a_n = 0$.

b. Zij $\lim_{n\to\infty} a_n = 0$.

Bij $x \in N_p$ is een $y \in N$ te vinden, zodanig dat
$$\left|\frac{x-y}{n!}\right|_p \leqslant 1;$$

ook is dan $\left|\binom{y}{n-k}\right|_p \leqslant 1 \qquad (k = 0,1,2,\ldots,n)$

Hieruit leidt men gemakkelijk af, dat dan

$$\left|\binom{x-y}{k}\right|_p \leqslant 1 \qquad (k = 0,1,2,\ldots,n).$$

Op grond van de relatie

$$\binom{x}{n} = \sum_{k=0}^{n} \binom{x-y}{k}\binom{y}{n-k}$$

is dan bovendien

$$\left|\binom{x}{n}\right|_p \leqslant 1 \qquad (x \in N_p,\ y \in N) \qquad\qquad (I)$$

Dus: $\left|a_n\binom{x}{n}\right|_p \leqslant \left|a_n\right|_p \to 0$, als $n \to \infty$.

Dat betekent, dat $f^*(x)$ convergeert (zelfs uniform).

Gevolg: $f^*(x)$ is continu.

Stelling: Zij $f(x)$ continu op N_p. Indien $\lim_{n\to\infty} a_n = 0$, dan is $f^*(x) = f(x)$ voor $x \in N_p$.

Bewijs: volgt uit de stellingen van 16.1 en 16.2.

16.4 Stelling: Zij $f(x)$ continu op N_p, dan is

$$\lim_{n\to\infty} a_n = 0,$$

en dus

$$f(x) = \sum_{n=0}^{\infty} a_n\binom{x}{n}, \text{ als } x \in N_p.$$

Bewijs:

a. N_p is compact, $f(x)$ is dus begrensd en uniform continu op N_p. Zonder beperking der algemeenheid kunnen we dus aannemen, dat

$$\left|f(x)\right|_p \leqslant 1 \quad \text{voor} \quad x \in N_p .$$

Voorts bestaat bij elk geheel rationaal getal $s > 0$ een geheel rationaal $t = t(s) > 0$, zodanig, dat

$$\left|f(x) - f(y)\right|_p \leqslant p^{-s}, \text{ indien } x,y \in N_p,\ \left|x-y\right|_p \leqslant p^{-t}.$$

b. Neem aan, dat $x,y \in N$.
Bij elke $x \in N$ bestaat precies één $g(x) \in N$, met
$|f(x) - g(x)|_p \leq p^{-s}$, $0 \leq g(x) \leq p^s - 1$.
$g(x)$ is periodiek op N:
$g(x) = g(y)$, indien $x,y \in N$, $x \equiv y \pmod{p^t}$.

c. Zij:
$$b_n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} g(n-k) \qquad (n = 0,1,2,\ldots) .$$

Kennelijk is:
$$|a_n - b_n|_p \leq p^{-s} \qquad (n = 0,1,2,\ldots) .$$

d. Zij nu ω één of andere primitieve p^t-eenheidswortel.
Dan is:
$$\sum_{n=0}^{p^t-1} \omega^{mn} = \begin{cases} p^t, & \text{indien } m \equiv 0 \pmod{p^t} \\ 0, & \text{indien } m \not\equiv 0 \pmod{p^t} \end{cases} .$$

e. Stel nu
$$\lambda_m = p^{-t} \sum_{n=0}^{p^t-1} \omega^{-mn} g(n) \qquad (m = 0,1,2,\ldots,p^t-1),$$
dan is
$$g(n) = \sum_{m=0}^{p^t-1} \lambda_m \omega^{mn} \qquad (n = 0,1,2,\ldots,p^t-1);$$
maar zowel $g(n)$ als $\sum_{m=0}^{p^t-1} \lambda_m \omega^{mn}$ zijn periodieke functies met met periode p^t; dus geldt de laatstgenoemde relatie voor alle $n \in N$.
Voorts is dan:
$$b_n = \sum_{m=0}^{p^t-1} \lambda_m (\omega^m - 1)^n \qquad \text{voor } n \in N .$$

f. Zij P het lichaam der rationale getallen en zij $K = P(\omega)$.
Laat verder R de ring van alle gehele algebraïsche getallen in K zijn.
Dan is
$$p^t (\omega - 1)^{-n} b_n \in R \qquad \text{voor } n \in N . \tag{1}$$
En bovendien geldt
$$|p| = (\omega - 1)^{p^{t-1}(p-1)} ,$$
waarin $(\omega-1)$ priemideaal is.

Zij nu

$$N_0 = \left[np^{-(t-1)}(p-1)^{-1}\right] .$$

Dan volgt uit (1)

$$p^{t-N_0}\, b_n \in R;$$

maar dan zijn de rationale getallen $p^{t-N_0} b_n$ geheel-algebraïsche getallen; het zijn dus gehele rationale getallen.

Dus: $$|b_n|_p \leqslant p^{t-N_0} .$$

Hieruit leidt men gemakkelijk af, dat

$$|b_n|_p \leqslant p^{-s} , \text{ indien } n \geqslant \text{ zekere } n_0(s) .$$

g. Tenslotte is dus

$$|a_n|_p \leqslant \max(|a_n-b_n|_p, |b_n|_p) \leqslant p^{-s}, \text{ indien } n \geqslant n_0(s),$$

d.w.z.

$$\lim_{n\to\infty} a_n = 0.$$

16.5 Stelling: Zij $f(x)$ continu op N_p. Indien nu $x,y \in N_p$, dan convergeren alle reeksen

$$a_n(y) = \sum_{k=0}^{\infty} a_{n+k}\binom{y}{k} \qquad (n = 0,1,2,\ldots)$$

en bovendien is

$$\lim_{n\to\infty} a_n(y) = 0, \; f(x+y) = \sum_{n=0}^{\infty} a_n(y)\binom{x}{n} .$$

Bewijs: Dat $a_n(y)$ convergeert, volgt uit $\lim\limits_{n\to\infty} a_{n+k} = 0$, daar $\left|\binom{y}{k}\right|_p \leqslant 1$. Bovendien is $\{a_n(y)\}$ een nulrij, want $|a_n(y)|_p \leqslant \max\limits_{k=0,1,2,\ldots} |a_{n+k}|_p \to 0$ als $n\to\infty$.

De relatie $f(x+y) = \sum\limits_{n=0}^{\infty} a_n(y)\binom{x}{n}$, tenslotte, volgt, na enige herleiding uit de definitie van $a_n(y)$.

16.6 Het, in het artikel van Prof. Mahler, weergegeven bewijs van de volgende Tauberstelling is niet correct. Of de stelling zelf juist is, is (nog) niet bekend.

<u>Stelling</u>: Zij $\{a_n\}$ een nulrij. Indien nu de p-adische limiet

$$\lambda = \lim_{|x|_p \to 0} \sum_{n=1}^{x} \frac{a_n}{n} \binom{x-1}{n-1}$$

over alle elementen $x \neq 0$ van N bestaat, dan is

$$\lim_{n \to \infty} \frac{a_n}{n} = 0$$

Het <u>bewijs</u> zou als volgt verlopen:

1) Neem aan, dat λ bestaat, maar dat

$$\limsup_{n \to \infty} \left| \frac{a_n}{n} \right|_p = \infty .$$

Dan is er een deelrij $\left\{\frac{a_{n_r}}{n_r}\right\}$ van de rij $\left\{\frac{a_n}{n}\right\}$, zodanig dat

$$\lim_{r \to \infty} \left| \frac{a_{n_r}}{n_r} \right|_p = \infty .$$

Zonder beperking van de algemeenheid kunnen we aannemen, dat

$$\left|\frac{a_n}{n}\right|_p < \left|\frac{a_{n_r}}{n_r}\right|_p \quad \text{voor } n = 1,2,\dots,n_r-1 \quad (r = 1,2,3,\dots)$$

Uit

$$\lambda = \lim_{r \to \infty} \left\{ \frac{a_{n_r}}{n_r} + \sum_{n=1}^{n_r-1} \frac{a_n}{n} \binom{n_r-1}{n-1} \right\}$$

volgt dan

$$|\lambda|_p = \lim_{r \to \infty} \left| \frac{a_{n_r}}{n_r} \right|_p = \infty ,$$

in tegenspraak met het gegeven.

2) Neem aan, dat λ bestaat, en dat $\left\{\frac{a_n}{n}\right\}$ een begrensde rij, maar geen nulrij is. Zonder beperking van de algemeenheid kunnen we dan aannemen, dat

$$|a_n|_p \leq 1, \quad \left|\frac{a_n}{n}\right|_p \leq 1 \qquad (n = 1,2,\dots)$$
$$\limsup_{n \to \infty} \left|\frac{a_n}{n}\right|_p = 1 . \tag{1}$$

Voorts bestaat er een positief getal s, zodanig dat

$$\left| \sum_{n=1}^{x} \frac{a_n}{n} \binom{x-1}{n-1} - \lambda \right|_p \leq \frac{1}{p} \quad \text{voor } x \in N,\ 0 < |x|_p \leq p^{-s}, \tag{2}$$

en deze ongelijkheid blijft gelden, als s wordt vergroot.

Stel: $x = p^s(\xi+1)$, $\xi \in N$

Verder zou nu uit

$$\lim_{\substack{n\to\infty \\ p^s \nmid n}} \frac{a_n}{n} = 0$$

volgen (door eventueel s te vergroten), dat men zonder beperking der algemeenheid kan aannemen, dat

$$\left|\frac{a_n}{n}\right|_p \leqslant \frac{1}{p} \quad \text{voor} \quad p^s \nmid n,\ n \geqslant p^s \tag{3}$$

Dit is echter onjuist, zoals men gemakkelijk inziet. (Andere mogelijkheden, om aan (3) te voldoen - zoals het veranderen van een eindig aantal termen van de rij $\{a_n\}$ - schijnen voorshands ook niet tot het beoogde doel te leiden.)

Indien aan (3) wel voldaan kon worden, verliep het bewijs verder als volgt:

Uit (2) en (3) volgt:

$$\left|\sum_{n=1}^{p^s-1}\frac{a_n}{n}\binom{x-1}{n-1} + \sum_{\substack{n=p^s \\ p^s/n}}^{x}\frac{a_n}{n}\binom{x-1}{n-1} - \lambda\right|_p \leqslant \frac{1}{p} \quad \text{voor } x = p^s(\xi+1), \xi \in N \tag{4}$$

Zij nu:

$$G = g_0 + g_1p + g_2p^2 + \ldots + g_rp^r, \quad H = h_0 + h_1p + h_2p^2 + \ldots + h_rp^r.$$

$$(0 \leqslant g_i, h_i \leqslant p-1;\ i = 0,1,2,\ldots,r)$$

Dan is:

$$\binom{G}{H} \equiv \binom{g_0}{h_0}\binom{g_1}{h_1}\cdots\binom{g_r}{h_r} \pmod p .$$

Toepassing van deze congruentie leidt tot het resultaat

<u>voor $n \leqslant p^s-1$</u>:

$$\binom{x-1}{n-1} \equiv (-1)^{h(n)} \pmod p ;$$

<u>voor $n \geqslant p^s, p^s/n$</u> (zodat dan $n = p^s(\nu+1)$, $\nu \in N$):

$$\binom{x-1}{n-1} \equiv \binom{\xi}{\nu} \pmod p .$$

Derhalve is:

$$\sum_{n=1}^{p^s-1}\frac{a_n}{n}\binom{x-1}{n-1} = \sum_{n=1}^{p^s-1}\chi(n)\frac{a_n}{n} + \rho(x)$$

en: $$\sum_{\substack{n=p^s \\ p^s/n}}^{x} \frac{a_n}{n}\binom{x-1}{n-1} = \sum_{\nu=0}^{\xi} \alpha_\nu \binom{\xi}{\nu} + \sigma(x),$$

waarin: 1) $\chi(n) = (-1)^{h(n)}$ alleen van n afhangt, en niet van

2) $\alpha_\nu = \frac{a_n}{n}$ voor $n = p^s(\nu+1)$

3) $|\rho(x)|_p \leqslant \frac{1}{p}$, $|\sigma(x)|_p \leqslant \frac{1}{p}$.

Uit (4) leidt men dan gemakkelijk af:

$$\sum_{\nu=0}^{\xi} \alpha_\nu \binom{\xi}{\nu} = \mu + \tau(\xi), \tag{5}$$

waarin:

1) $\mu = \lambda - \sum_{n=1}^{p^s-1} \chi(n)\frac{a_n}{n}$

2) $|\tau(\xi)|_p \leqslant \frac{1}{p}$. (6)

Substitueert men in (5) achtereenvolgens $\xi = 0,1,2,3,\ldots$, dan verkrijgt men een stelsel van oneindig veel vergelijkinge in $\alpha_0, \alpha_1, \alpha_2, \ldots$.

Op grond van (6) kan men daaruit concluderen

$$|\alpha_\nu|_p \leqslant \frac{1}{p} \quad \text{als} \quad \nu = 1,2,3,4 . \tag{7}$$

Echter: Uit (1) en (3) volgt, dat er oneindig vele indices n zijn, waarvoor

$$p^s/n \quad \text{en} \quad \left|\frac{a_n}{n}\right|_p = 1 ,$$

en dus zijn er oneindig vele indices ν, waarvoor

$$|\alpha_\nu|_p = 1 ,$$

in strijd met (7).

In ieder geval is dus wel juist de volgende, veel zwakkere, bewering (i.p.v. stelling 16.6).

"Stelling": Zij $\{a_n\}$ een nulrij. Indien nu de p-adische limie

$$\lambda = \lim_{|x|_p \to 0} \sum_{n=1}^{x} \frac{a_n}{n}\binom{x-1}{n-1}$$

over alle elementen $x \neq 0$ van N bestaat, dan is

$$\lim_{n\to\infty} \frac{a_n}{n} = 0 ,$$

mits bovendien aan de volgende conditie is voldaan:

$$(\Phi) \ \ldots \quad \begin{cases} \text{Bij iedere keuze van het getal } A \text{ bestaat een } s > A, \\ \text{zodanig dat } \left|\frac{a_n}{n}\right|_p \leqslant \frac{1}{p} \text{ voor } p^s \nmid n,\ n \geqslant p^s . \end{cases}$$

16.7 Stelling: Zij $\left\{\frac{a_n}{n}\right\}$ een p-adische nulrij. Dan bestaat de limie

$$\lambda = \lim_{x\to 0} \sum_{n=0}^{\infty} \frac{a_n}{n}\binom{x-1}{n-1}$$

over alle $x \in N$, en bovendien is

$$\lambda = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{a_n}{n} .$$

Bewijs: Bij elke $s > 0$ bestaat een $M = M(s)$, zodanig dat

$$\left|\frac{a_n}{n}\right|_p \leqslant p^{-s} \quad \text{als } n > M,$$

en dus

$$\left|\sum_{n=M+1}^{\infty} (-1)^{n-1} \frac{a_n}{n}\right|_p \leqslant p^{-s} \text{ en } \left|\sum_{n=M+1}^{\infty} \frac{a_n}{n}\binom{x-1}{n-1}\right|_p \leqslant p^{-s} \qquad (1)$$

Voorts volgt uit de continuïteit van een eindige som van polynomen het bestaan van een $t = t(s) > 0$, zodanig dat

$$\left|\sum_{n=1}^{M} \frac{a_n}{n}\binom{x-1}{n-1} - \sum_{n=1}^{M}(-1)^{n-1} \frac{a_n}{n}\right|_p \leqslant p^{-s} \text{ als } |x|_p \leqslant p^{-t} \qquad (2)$$

Uit (1) en (2) volgt hetgeen te bewijzen was.

16.8 Stelling: Zij $f(x) = \sum_{n=0}^{\infty} a_n\binom{x}{n}$ continu op N_p, en zij

$$a_n(y) = \sum_{k=0}^{\infty} a_{n+k}\binom{y}{k}.$$

1. Indien nu

$$\lim_{n\to\infty} \frac{a_n(y)}{n} = 0,$$

dan bestaat $f'(y)$ en bovendien is

$$f'(y) = \sum_{n=1}^{\infty}(-1)^{n-1} \frac{a_n(y)}{n} .$$

2. Indien $f'(y)$ bestaat en de rij $\{a_n(y)\}$ voldoet aan de voorwaarde (Φ), dan is $\lim \frac{a_n(y)}{n} = 0$.

Bewijs: Dit volgt onmiddellijk uit de voorgaande stellingen, op grond van de relatie

$$\frac{f(x+y)-f(x)}{x} = \sum_{n=1}^{\infty} \frac{a_n(y)}{n}\binom{x-1}{n-1} .$$

Opmerking: Indien aan de voorwaarde (Φ) reeds op grond van de overige gegevens zou zijn voldaan, gold de veel fraaiere stelling

"bestaan $f'(y) \Longleftrightarrow \lim\limits_{n\to\infty} \frac{a_n(y)}{n} = 0$".

16.9 Stelling: Zij $f(x) = \sum_{n=0}^{\infty} a_n\binom{x}{n}$ continu op N_p. Indien nu de afgeleide $f'(x)$ bestaat en continu is voor alle $x \in N_p$, en bovendien voldoet de rij $\{a_n(y)\}$ aan de voorwaarde (Φ) (voor alle $y \in N$), dan geldt

1) de reeksen $a'_n = \sum_{k=1}^{\infty} (-1)^{k-1} \frac{a_{k+n}}{k}$ zijn convergent $(n = 0,1,2,\ldots)$

2) $\{a'_n\}$ is een nulrij

3) $$f'(x) = \sum_{n=0}^{\infty} a'_n\binom{x}{n} \quad \text{voor } x \in N_p .$$

Bewijs: Zij $y \in N$. Dan is op grond van de vorige stelling

$$\left\{\frac{a_k(y)}{k}\right\} \quad (\text{voor alle } y \in N)$$

een nulrij. Hieruit volgt, dat ook de rijen

$$\left\{\frac{a_{k+n}}{k}\right\}_{k=1}^{\infty} \quad (n = 0,1,2,\ldots)$$

nulrijen zijn.

Derhalve zijn de reeksen a'_n convergent, en bovendien

$$f'(y) = \sum_{n=0}^{y} a'_n\binom{y}{n}$$

$$= \sum_{n=0}^{\infty} a'_n\binom{y}{n} \quad \text{voor } y \in N \qquad (1)$$

Voorts is $f'(x)$ continu voor alle $x \in N_p$, zodat volgens stelling 16.4 $f'(x)$ in een convergente reeks

$$f'(x) = \sum_{n=0}^{\infty} b_n \binom{x}{n} \qquad (x \in N_p) \tag{2}$$

is te ontwikkelen.
Uit (1) en (2) volgt:

$$b_n = a'_n ,$$

zodat

$$f'(x) = \sum_{n=0}^{\infty} a'_n \binom{x}{n} \quad \text{voor } x \in N_p .$$

Op grond van stelling 16.4 is tenslotte $\{a'_n\}$ een nulrij.

Colloquium "P-adische getallen"

Voordrachten op 20 mei en 3 juni 1960

door

H. de Vries en H. Jager

$\mathfrak{p}$-adische waardering van algebraïsche getallenlichamen

Litteratuur: E. Hecke, Vorlesungen über die Theorie der algebraïschen Zahlen.

B.L. van der Waerden, Moderne Algebra.

§ 17. Factorontbinding van idealen

Notaties: G: de ring der gehele getallen

Q: het lichaam der rationale getallen

K: een eindige lichaamsuitbreiding van Q

S: de ring der gehele algebraïsche getallen in K.

Hulpstelling 1. Als $a \in K$ dan is $a = \frac{a'}{g}$ met $a' \in S$, $g \in G$.

Gevolg: K is een quotiëntenlichaam van S.

Gebruik zal worden gemaakt van:

Stelling A. K kan worden verkregen door adjunctie van één enkel element ϑ aan Q: $K = Q(\vartheta)$.

Zij n de graad van ϑ t.o.v. Q.

Stelling 1. De additieve groep van S heeft een eindig lineair onafhankelijk stelsel voortbrengenden (een basis).

Bewijs: Zij $K=Q(\vartheta)$; dan kunnen we veronderstellen dat $\vartheta \in S$ (hulpstelling 1).

Stel $s \in S$, dan kan men s schrijven als

$$s = \sum_{\nu=0}^{n-1} r_\nu \vartheta^\nu \qquad (r_\nu \in Q).$$

Laat $\vartheta = \vartheta_1, \vartheta_2, \ldots \vartheta_n$ de geconjugeerden van ϑ zijn in een uitbreiding van K; dan definiëren we

$$(1) \qquad s_\rho = \sum_{\nu=0}^{n-1} r_\nu \vartheta_\rho^\nu , \qquad \rho = 1,2,\ldots n.$$

De s_ρ zijn geheel algebraïsch, maar niet noodzakelijk in K.

Als nu $\Delta = \det(\vartheta_\rho^\nu)_{\substack{\nu=0,1,\ldots n-1 \\ \rho=1,\ldots n}}$, dan is

$$\Delta = \prod_{1 \leq \lambda < \mu \leq n} (\vartheta_\lambda - \vartheta_\mu) \neq 0 \quad \text{(Vandermonde).}$$

Uit dit laatste zien we onmiddellijk dat Δ^2 een geheel rationale, symmetrische functie met coëfficiënten uit G in de ϑ_ρ is. Daar de elementair symmetrische functies in de ϑ_ρ geheel rationale getallen zijn volgt met de hoofdstelling van de symmetrische functies dat Δ^2 een geheel rationaal getal is.

Uit (1) verkrijgen we:

$$\Delta\, r_\nu = \sum_{\rho=1}^{n} t_{\nu\rho}\, s_\rho \quad , \quad \nu=0,\ldots n-1, \quad t_{\nu\rho} \text{ geheel algebr.}$$

$$\text{of } \Delta^2 r_\nu = \sum_{\rho=1}^{n} \Delta\, t_{\nu\rho}\, s_\rho \, .$$

We zien nu onmiddellijk dat het rechterlid geheel algebraïsch en het linkerlid rationaal is. Dus: $\Delta^2 r_\nu \in G$.

We schrijven nu (1) als

$$s_\rho = \sum_{\nu=0}^{n-1} \Delta^2 r_\nu \frac{\vartheta_\rho^\nu}{\Delta^2}, \quad \rho=1,2,\ldots n;$$

i.h.b. $$s = \sum_{\nu=0}^{n-1} \Delta^2 r_\nu \frac{\vartheta^\nu}{\Delta^2}.$$

Dus is S een ondergroep van de vrije abelse groep, voortgebracht door de basis $\left\{ \frac{\vartheta^\nu}{\Delta^2} \right\}_{\nu=0}^{n-1}$; dan is ook S een vrije abelse groep met eindige basis. Uit hulpstelling 1 volgt dat zo'n basis uit n elementen moet bestaan. Hierbij is gebruik gemaakt van de volgende:

Stelling B. Een ondergroep van een vrije abelse groep met eindige basis, is een vrije abelse groep met een eindige basis.

Met behulp van deze stelling bewijzen we nu gemakkelijk:

Stelling 2. Zij V een vrije abelse groep.
Dan geldt:
In V breekt iedere opstijgende rij van ondergroepen af $\Longleftrightarrow$ V heeft een eindige basis.

Bewijs $\Longrightarrow$: Stel V heeft geen eindige basis. Zij dan $\{a_1, a_2, \ldots\}$ een oneindig stelsel lin.onafh. elementen van V en V_n de groep, voortgebracht door $\{a_1, a_2, \ldots a_n\}$. Dan breekt de rij $\{V_1, V_2, \ldots\ldots\}$ niet af.

$\Longleftarrow$ Stel $\{H_1, H_2, \ldots\}$ een opstijgende rij ondergroepen van V en $H = \bigcup_{\mu=1}^{\infty} H_\mu$. Dan heeft H een eindige basis, $\{b_1, \ldots b_n\}$ (stelling B).

Elke b_ν ligt in een H_μ. Er is dus een m met $b_\nu \in H_m$, $\nu = 1, \ldots n$. Dan moet echter $H = H_m = H_\mu$, $\mu \geq m$.

Uit stelling 1 en stelling 2 volgt onmiddellijk:

<u>Stelling 3.</u> Elke opstijgende rij van idealen in S breekt af.

<u>Definitie.</u> Een ideaal $\mathfrak{p}$ van een commutatieve ring R heet een <u>priemideaal</u> indien: $ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p}$ of $b \in \mathfrak{p}$ $(a, b \in R)$, ofwel als $R/_{\mathfrak{p}}$ een integriteitsgebied is.

Een ideaal $\mathfrak{m}$ van een commutatieve ring R heet <u>maximaal</u>, als $\mathfrak{m} \neq R$ en: $\mathfrak{m} \subset \mathfrak{n} \subset R \Rightarrow \mathfrak{m} = \mathfrak{n}$ of $\mathfrak{n} = R$, waarbij ook $\mathfrak{n}$ een ideaal van R is, ofwel als $R/_{\mathfrak{m}}$ een lichaam is, als R ook een eenheidselement bevat.

<u>Stelling 4.</u> In S is ieder echt priemideaal dat niet het nulideaal is, maximaal.

Bewijs. Stel $\mathfrak{p}$ een echt priemideaal van S, $\mathfrak{p} \neq (0)$. Neem $0 \neq t \in \mathfrak{p}$; dan voldoet t aan een betrekking

$$t^h + a_1 t^{h-1} + a_2 t^{h-2} + \ldots + a_h = 0, \quad a_i \in G,$$

met $a_h \neq 0$. Dan $a_h \in (t) \subset \mathfrak{p}$ dus

$$a_h \in \mathfrak{p} \cap G.$$

Nu is $\mathfrak{p} \cap G \neq (0)$ een echt priemideaal van G dus een maximaal ideaal van G.

Stel $\mathfrak{a}$ een ideaal van S met $\mathfrak{p} \subset \mathfrak{a} \subset S$, $\mathfrak{p} \neq \mathfrak{a}$. Neem $u \in \mathfrak{a} \setminus \mathfrak{p}$. Omdat u een geheel algebraïsch getal is, is er i.h.b. een congruentie van laagste graad

$$u^k + b_1 u^{k-1} + \ldots + b_k \equiv 0 \pmod{\mathfrak{p}}, \quad b_i \in G.$$

Uit het feit dat $\mathfrak{p}$ een priemideaal is volgt dat $b_k \equiv 0 \pmod{\mathfrak{p}}$. Nu is $b_k \in (u, \mathfrak{p}) \subset \mathfrak{a}$, dus $b_k \in \mathfrak{a} \cap G$, $b_k \in \mathfrak{p} \cap G$, dus $\mathfrak{a} \cap G = G$.

I.h.b. $1 \in \mathfrak{a}$ dus $\mathfrak{a} = S$. q.e.d.

Definitie. Het product van twee idealen $\mathfrak{a}$ en $\mathfrak{b}$ van een commutatieve ring R is gedefinieerd als

$$\left\{ \sum_{\nu} a_\nu b_\nu \mid a_\nu \in \mathfrak{a},\ b_\nu \in \mathfrak{b} \right\}.$$

Het product $\mathfrak{a}\mathfrak{b}$ van $\mathfrak{a}$ en $\mathfrak{b}$ is weer een ideaal; productvorming is associatief.

Stelling 5. Bij ieder ideaal $\mathfrak{a} \neq (0)$ van S zijn er priemidealen, $\mathfrak{p}_1, \mathfrak{p}_2, \dots \mathfrak{p}_r$, $\mathfrak{p}_\rho \neq (0)$, die $\mathfrak{a}$ omvatten, met

$$\mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_r \subset \mathfrak{a}.$$

Bewijs: Stel $\mathfrak{a}$ niet priem (anders triviaal). Er zijn dus elementen $b, c \in S$ met $bc \in \mathfrak{a}$, $b \notin \mathfrak{a}$, $c \notin \mathfrak{a}$. Is de stelling nu waar voor $\mathfrak{b} = (\mathfrak{a}, b)$ en $\mathfrak{c} = (\mathfrak{a}, c)$, dan is de stelling ook waar voor $\mathfrak{a}$. Geldt de stelling dus niet voor $\mathfrak{a}$, dan is er een groter ideaal waarvoor hij ook niet geldt (n.l. $\mathfrak{b}$ of $\mathfrak{c}$). In dat geval is er een niet afbrekende, opstijgende rij van idealen (waarvoor de stelling niet geldt), in tegenspraak met stelling 3.

Hulpstelling 2. Als $\mathfrak{a}$ en $\mathfrak{b}$ idealen zijn van een commutatieve ring R en $\mathfrak{p}$ een priemideaal van R dan:

$$\mathfrak{a}\mathfrak{b} \subset \mathfrak{p} \Rightarrow \mathfrak{a} \subset \mathfrak{p} \text{ of } \mathfrak{b} \subset \mathfrak{p}.$$

Bewijs: Stel noch $\mathfrak{a} \subset \mathfrak{p}$ noch $\mathfrak{b} \subset \mathfrak{p}$. Neem dan $a \in \mathfrak{a} \setminus \mathfrak{p}$ en $b \in \mathfrak{b} \setminus \mathfrak{p}$; nu is $ab \in \mathfrak{a}\mathfrak{b} \subset \mathfrak{p}$ dus $a \in \mathfrak{p}$ of $b \in \mathfrak{p}$. Tegenspraak.

Definitie. Als A en B twee deelverzamelingen van K zijn dan definiëren we het product AB van A en B als volgt:

$$AB = \left\{ \sum a_\nu b_\nu \mid a_\nu \in A,\ b_\nu \in B \right\}.$$

Deze vermenigvuldiging is associatief.
Als A uit slechts één enkel element a bestaat dan schrijven we ook aB i.p.v. AB.

Definitie. Zij $\mathfrak{p}$ een priemideaal ($\neq (0)$) van S. Dan definiëren we:

$$\mathfrak{p}^{-1} = \left\{ a \in K \mid a\mathfrak{p} \subset S \right\}.$$

Hulpstelling 3. Als $\mathfrak{p}$ een priemideaal van S is ($\mathfrak{p} \neq (0)$) dan is $\mathfrak{p}\mathfrak{p}^{-1} = S$.

Bewijs: Als $\mathfrak{p}=S$ dan $\mathfrak{p}^{-1}=S$ en $\mathfrak{p}\mathfrak{p}^{-1}=S$.

Stel nu $\mathfrak{p}\neq S$. Neem $c\in\mathfrak{p}$, $c\neq 0$. Volgens stelling 5 zijn er nu priemidealen $\mathfrak{p}_\rho$ $(\rho=1,\ldots,r)$ met $\mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_r\subset(c)$. Stel r minimaal. Daar ook $\mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_r\subset\mathfrak{p}$ is er een $\mathfrak{p}_\rho$ met $\mathfrak{p}_\rho\subset\mathfrak{p}$ volgens hulpstelling 2 waarbij we mogen veronderstellen dat $\rho=1$. Nu is $\mathfrak{p}_1=\mathfrak{p}$ daar $\mathfrak{p}_1$ maximaal is (stelling 4). Daar r minimaal was, is $\mathfrak{p}_2\mathfrak{p}_3\ldots\mathfrak{p}_r\not\subset(c)$; neem $b\in\mathfrak{p}_2\mathfrak{p}_3\ldots\mathfrak{p}_r\setminus(c)$. Dan $\mathfrak{p}b\subset(c)$, en $\frac{b}{c}\in\mathfrak{p}^{-1}$, $\frac{b}{c}\notin S$ (daar $b\notin(c)$).

Nu is $\mathfrak{p}\mathfrak{p}^{-1}$ een ideaal van S, en daar $1\in\mathfrak{p}^{-1}$, $\mathfrak{p}\subset\mathfrak{p}\mathfrak{p}^{-1}\subset S$. I.h.b. $c\cdot\frac{b}{c}=b\in\mathfrak{p}\mathfrak{p}^{-1}$; maar $b\notin\mathfrak{p}$ dus $\mathfrak{p}\mathfrak{p}^{-1}=S$, daar $\mathfrak{p}$ maximaal.

Stelling 6. Elk ideaal $\mathfrak{a}\neq(0)$ van S is een product van priemidealen van S.

Bewijs: Stel $\mathfrak{p}_1\cdot\mathfrak{p}_2\ldots\mathfrak{p}_r\subset\mathfrak{a}$, $\mathfrak{p}_\rho$ priem, $\mathfrak{p}_\rho\supset\mathfrak{a}$, r minimaal (stelling 5).

We gebruiken nu inductie naar r.

Als r=1 dan $\mathfrak{a}=\mathfrak{p}_1$ of $\mathfrak{a}=S$.

Stel nu $r>1$.

Nu geldt:

$$\mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_r\subset\mathfrak{a}\subset\mathfrak{p}_1$$

dus
$$\mathfrak{p}_1^{-1}\mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_r\subset\mathfrak{p}_1^{-1}\mathfrak{a}\subset\mathfrak{p}_1^{-1}\mathfrak{p},$$

en
$$\mathfrak{p}_2\mathfrak{p}_3\ldots\mathfrak{p}_r\subset\mathfrak{p}_1^{-1}\mathfrak{a}\subset S.$$

M.b.v. de inductie-onderstelling kunnen we nu het ideaal $\mathfrak{p}_1^{-1}\mathfrak{a}$ schrijven als: $\mathfrak{p}_1^{-1}\mathfrak{a}=\mathfrak{p}'_1\mathfrak{p}'_2\ldots\mathfrak{p}'_s$, $\mathfrak{p}'_\sigma$ priem.

Hieruit volgt $\mathfrak{a}=\mathfrak{p}_1\mathfrak{p}'_1\mathfrak{p}'_2\ldots\mathfrak{p}'_s$. q.e.d.

Stelling 7. Als $\mathfrak{a}$ en $\mathfrak{b}$ idealen van S zijn en $\mathfrak{a}\subset\mathfrak{b}$, $\mathfrak{a}=\mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_r$, $\mathfrak{b}=\mathfrak{p}'_1\mathfrak{p}'_2\ldots\mathfrak{p}'_s$, $\mathfrak{p}_\rho$, $\mathfrak{p}'_\sigma$ priem, dan komt iedere $\mathfrak{p}'_\sigma\neq S$ minstens even vaak voor in de productvoorstelling van $\mathfrak{a}$ als in die van $\mathfrak{b}$.

Bewijs: Stel $S\neq\mathfrak{p}'_1$; daar $\mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_r=\mathfrak{a}\subset\mathfrak{b}\subset\mathfrak{p}'_1$, is er een $\mathfrak{p}_\rho=\mathfrak{p}'_1$ (hulpstelling 2, stelling 4); stel $\rho=1$. We gebruiken inductie naar s. Voor s=1 is hier de stelling bewezen. Stel $s>1$.

Dan $\mathfrak{p}_1^{-1}\mathfrak{a}=\mathfrak{p}_2\ldots\mathfrak{p}_r$ (=S als r=1),

$\mathfrak{p}_1^{-1}\mathfrak{b}=\mathfrak{p}'_2\ldots\mathfrak{p}'_s$;

gebruik nu de inductie-veronderstelling.

Hieruit volgt nu onmiddellijk:

Stelling 8 (Fundamentaalstelling).
De voorstelling van een ideaal $\mathfrak{a} \neq (0)$ van S als product van priemidealen, is éénduidig, afgezien van de volgorde en factoren S.

Stelling 9. Zijn $\mathfrak{a}$ en $\mathfrak{b}$ idealen van S, beide $\neq (0)$, $\mathfrak{a} \subset \mathfrak{b}$, dan is er een ideaal $\mathfrak{c}$ van S, met $\mathfrak{a} = \mathfrak{b} \cdot \mathfrak{c}$.

Stelling 10. Zijn $\mathfrak{a}$ en $\mathfrak{b}$ twee idealen van S, beide $\neq (0)$, met productvoorstellingen

$$\mathfrak{a} = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_k \cdot \mathfrak{q}_1 \mathfrak{q}_2 \cdots \mathfrak{q}_l$$

$$\mathfrak{b} = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_k \cdot \mathfrak{w}_1 \mathfrak{w}_2 \cdots \mathfrak{w}_m ,$$

met $\mathfrak{q}_i \neq \mathfrak{w}_j$ dan geldt:

$$(\mathfrak{a}, \mathfrak{b}) = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_k .$$

§18. Invoering van $\mathfrak{p}$-adische getallen.

Stelling 1. Is $\mathfrak{p}$ een priemideaal van S, $\mathfrak{p} \neq S$, dan is

$$\bigcap_{n=1}^{\infty} \mathfrak{p}^n = (0).$$

Bewijs: Neem $a \in S$, $a \neq 0$,

$$(a) = \prod_{\nu=1}^{n} \mathfrak{p}_\nu^{k(\nu)} , \quad \mathfrak{p}_1 = \mathfrak{p} , \quad \mathfrak{p}_i \neq \mathfrak{p}_j \text{ voor } i \neq j.$$

(evt. is $k(1)=0$ terwijl we $\mathfrak{p}^0 = S$ stellen).

Dan is $(a) \not\subset \mathfrak{p}^{k(1)+1}$ en dus $a \notin \mathfrak{p}^{k(1)+1}$.

Stelling 2. Zij $\mathfrak{a} \neq (0)$ een ideaal van S. Dan is de restklassenring $S/\mathfrak{a}$ eindig.

Bewijs. Neem $a \in \mathfrak{a}$, $a \neq 0$. Zij $a=a_1, a_2, \ldots a_k$ de algebraïsch geconjugeerden van a (in een uitbreiding van K). Dan is $c=a_1 a_2 \ldots a_k \in G$ en $s=a_2 . a_3 \ldots a_k \in K$; ook $s \in S$ daar s geheel algebraïsch is. Dus $c=as \in \mathfrak{a}$.
Nu geldt: $b \in S \Rightarrow bc \in \mathfrak{a}$.
In de eindig voortgebrachte additieve groep $S/\mathfrak{a}$ heeft dus elk element een eindige orde, n.l. een deler van c; $S/\mathfrak{a}$ is dan eindig.

Stelling 3. Ieder priemideaal $\mathfrak{p} \neq 0$, $\neq S$ van S bevat juist één priemgetal p.

Bewijs. Volgens stelling 2 bevat $\mathfrak{p}$ een natuurlijk getal; dan bevat $\mathfrak{p}$ ook minstens een priemfactor ervan. Aan de andere kant kan $\mathfrak{p}$ niet twee priemgetallen bevatten, daar anders ook $1 \in \mathfrak{p}$ dus $\mathfrak{p} = S$.

Definitie. Stel $\mathfrak{p}$ een priemideaal $\neq (0)$, $\neq S$ van S, p het priemgetal $\in \mathfrak{p}$, $p \in \mathfrak{p}^e$, e maximaal.
Nu definiëren we de $\mathfrak{p}$-adische waardering van een element $a \in S$, $a \neq 0$ als volgt:

als $a \in \mathfrak{p}^s$, s maximaal, dan

$$|a|_{\mathfrak{p}} = p^{-\frac{s}{e}} \quad \text{en}$$

$$|0|_{\mathfrak{p}} = 0.$$

Nu geldt:
1) $|a|_{\mathfrak{p}} = 0 \Leftrightarrow a = 0$,
2) $|ab|_{\mathfrak{p}} = |a|_{\mathfrak{p}} |b|_{\mathfrak{p}}$,
3) $|a+b|_{\mathfrak{p}} \leqq \max(|a|_{\mathfrak{p}}, |b|_{\mathfrak{p}})$.

We breiden nu deze waardering van S op de volgende wijze uit tot het quotiëntenlichaam K van S:
Als $a \in S$, $b \in S$, $b \neq 0$ dan definiëren we

$$\left|\frac{a}{b}\right|_{\mathfrak{p}} = \frac{|a|_{\mathfrak{p}}}{|b|_{\mathfrak{p}}} .$$

De eigenschappen 1) t/m 3) gelden nu ook in K.

Definitie. Door op de bekende manier aequivalentieklassen van fundamentaalrijen van K te beschouwen verkrijgen we het volledig omhulsel $K_{\mathfrak{p}}$ van K, de $\mathfrak{p}$-adische getallen.

$K_{\mathfrak{p}}$ is een lichaam waarvan de elementen met $\mathfrak{p}$-adische waardering $\leqq 1$ een deelring $I_{\mathfrak{p}}$ vormen, de ring der gehele $\mathfrak{p}$-adische getallen van $K_{\mathfrak{p}}$.

Stelling 4. $I_{\mathfrak{p}}$ is compact.

Bewijs. $I_{\mathfrak{p}}$ is de afsluiting van $I = K \cap I_{\mathfrak{p}}$.

We gaan nu aantonen dat I totaal begrensd is d.w.z. voor iedere $\varepsilon > 0$ zijn er elementen $a_1, a_2, \ldots a_n \in I$ met de eigenschap: Voor alle $b \in I$ is er een i met $|b-a_i|_{\mathfrak{p}} < \varepsilon$.

Neem een nat.get. h zó, dat $p^{-\frac{h}{e}} < \varepsilon$.

Zij $a_1, a_2, \ldots a_n$ een volledig stelsel representanten van de eindige restklassenring $S/\mathfrak{p}^h$ $(a_i \in S \subset I)$.

Stel $b_1 \in S$, $b_2 \in S$, $\frac{b_1}{b_2} \in I$ dus $\left|\frac{b_1}{b_2}\right|_{\mathfrak{p}} \leq 1$.

Zij $|b_1|_{\mathfrak{p}} = p^{-\frac{s'}{e}}$, $|b_2|_{\mathfrak{p}} = p^{-\frac{s}{e}}$, $s' \geq s$.

Nu is $(b_2, \mathfrak{p}^{s+h}) = \mathfrak{p}^s$; dus is er een $c \in S$ met $b_1 - b_2 c \in \mathfrak{p}^{s+h}$, daar $b_1 \in \mathfrak{p}^{s'} \subset \mathfrak{p}^s$.

Nu hebben we
$$\left|\frac{b_1}{b_2} - c\right|_{\mathfrak{p}} = \frac{1}{|b_2|_{\mathfrak{p}}} \left|b_1 - b_2 c\right|_{\mathfrak{p}} \leq$$
$$\leq p^{\frac{s}{e}} \cdot p^{-\frac{s+h}{e}} = p^{-\frac{h}{e}}.$$

Nu is er een a_i met $c - a_i \in \mathfrak{p}^h$ dus
$$|c - a_i|_{\mathfrak{p}} \leq \mathfrak{p}^{-\frac{h}{e}}.$$

Tenslotte:
$$\left|\frac{b_1}{b_2} - a_i\right|_{\mathfrak{p}} \leq \max\left(\left|\frac{b_1}{b_2} - c\right|_{\mathfrak{p}}, \left|c - a_i\right|_{\mathfrak{p}}\right) \leq p^{-\frac{h}{e}} < \varepsilon.$$

Colloquium "P-adische getallen"

Voordracht op 21 oktober 1960

door

H. de Vries

Machtreeksen in het lichaam der $\mathfrak{p}$-adische getallen

Literatuur: J. de Groot, Bemerkung über die analytische Fortsetzung in bewerteten Körper, Indag. Math. 4 (1942), 120-122.

F. Loonstra, Analytische Untersuchungen über bewertete Körper.

K. Mahler, Eine arithmetische Eigenschaft der Taylor-koeffizienten rationaler Funktionen, Proc. Kon. Ak. van Wet. 38 (1935), 50-60.

Erratum blz. 42. Het bewijs van § 17, hulpstelling 3 is incorrect. We bewijzen eerst nog het volgende:

Lemma. Als $b \in K$, $0 \neq a \in S$ en ab^n geheel algebraïsch voor alle natuurlijke n, dan is ook b geheel algebraïsch.

Bewijs. Zij H_n de additieve ondergroep van S voortgebracht door de elementen $a, ab, \ldots, ab^n$ $(n=1,2,\ldots)$. Dan geldt: $H_n \subset H_{n+1}$ (n=1,2, Volgens § 17 stelling 1 en stelling 2 is er een natuurlijk getal n met: $H_{n+1} = H_n$. Dan $ab^{n+1} \in H_n$; er zijn dus gehele rationale getallen k_i met:

$$ab^{n+1} = \sum_{i=0}^{n} k_i ab^i \ , \text{ ofwel } \ b^{n+1} = \sum_{i=0}^{n} k_i b^i.$$

Hieruit volgt, dat b geheel algebraïsch is.

De laatste drie regels van het bewijs van hulpstelling 3 dienen nu vervangen te worden door:

Uit het eerste deel van het bewijs blijkt, dat $\mathfrak{p}^{-1}$ een niet geheel algebraïsch element bevat, nl. $\frac{b}{c}$. Nu is $\mathfrak{p}\mathfrak{p}^{-1}$ ee ideaal van S, en daar $1 \in \mathfrak{p}^{-1}$, $\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}^{-1} \subset S$. Ware nu $\mathfrak{p} = \mathfrak{p}\mathfrak{p}^{-}$ dan zou ook $\mathfrak{p}\mathfrak{p}^{-n} = \mathfrak{p}$ voor alle natuurlijke n, en dus i.h.b. ab^n geheel algebraïsch zijn voor alle $a \in \mathfrak{p}$, $b \in \mathfrak{p}^{-1}$ en alle natuurlijke getallen n. Volgens het lemma zouden dan ook alle elementen van $\mathfrak{p}^{-1}$ geheel algebraïsch zijn, wat nie het geval is. Uit de maximaliteit van $\mathfrak{p}$ volgt nu: $\mathfrak{p}\mathfrak{p}^{-1} = S$ q.e.d.

§ 19. Ontwikkeling in machtreeksen.

In deze paragraaf zal $|a|$, voor $a \in K_{\mathfrak{p}}$, steeds de $\mathfrak{p}$-adische waardering $|a|_{\mathfrak{p}}$ van a aanduiden.

Uit het niet-archimedisch zijn van de waardering in $K_{\mathfrak{p}}$ volgt op precies dezelfde wijze als in § 5a d):

Stelling 1. De reeks $\sum_{n=0}^{\infty} u_n$, met $u_n \in K_{\mathfrak{p}}$ $(n=0,1,2,\dots)$ convergeert dan en slechts dan als $u_n \longrightarrow 0$, d.w.z. $|u_n| \longrightarrow 0$.

Uit stelling 1 volgt nu gemakkelijk, dat iedere machtreeks $\sum_{n=0}^{\infty} a_n(x-x_o)^n$ in $K_{\mathfrak{p}}$ een eenduidig bepaalde convergentiestraal ρ heeft met de eigenschappen:

1^o. de reeks convergeert voor alle $x \in K_{\mathfrak{p}}$ met $|x-x_o| \leq \rho$, en divergeert voor alle $x \in K$ met $|x-x_o| > \rho$;

2^o. ρ is een gehele macht van $p^{\frac{1}{e}}$, 0 of ∞.

Stelling 2. In $K_{\mathfrak{p}}$ geldt: als $\sum_{n=0}^{\infty} u_n$ convergeert, dan:

$$\left|\sum_{n=0}^{\infty} u_n\right| \leq \max_{n=0,1,2,\dots} |u_n| .$$

Bewijs: In ieder geval bestaat $\max_{n=0,1,2,\dots} |u_n|$, daar $|u_n| \longrightarrow 0$.

Nu geldt:

$$\left|\sum_{n=0}^{N} u_n\right| \leq \max_{n=0,1,2,\dots,N} |u_n| \leq \max_{n=0,1,2,\dots} |u_n| ,$$

en daar $\lim_{N\to\infty} \left|\sum_{n=0}^{N} u_n\right| = \left|\sum_{n=0}^{\infty} u_n\right|$ ook:

$$\left|\sum_{n=0}^{\infty} u_n\right| \leq \max_{n=0,1,2,\dots} |u_n| \quad , \text{ q.e.d.}$$

Stelling 3. Als in $K_{\mathfrak{p}}$ $f(x) = \sum_{n=0}^{\infty} a_n(x-x_o)^n$, met convergentiestraal $\rho > 0$, dan is f differentieerbaar op $|x-x_o| \leq \rho$, terwijl $f'(x) = \sum_{n=1}^{\infty} na_n(x-x_o)^{n-1}$ voor $|x-x_o| \leq \rho$.

Bewijs: Stel $|x-x_o| \leq \rho$. In de eerste plaats convergeert $\sum_{n=1}^{\infty} na_n(x-x_o)^{n-1}$: $|na_n(x-x_o)^{n-1}| \leq |a_n(x-x_o)^{n-1}| \longrightarrow 0$.

Stel nu c een positief reëel getal met: $|x-x_o| \leq c \leq \rho$.

Als nu $\varepsilon > 0$, $h \in K_{\mathfrak{p}}$, $0 < |h| \leq c$, $|h| \leq \dfrac{\varepsilon}{\max\limits_{n=2,3,\dots} |a_n| c^{n-2}}$,

dan geldt:

$$\left|\frac{f(x+h)-f(x)}{h} - \sum_{n=1}^{\infty} na_n(x-x_o)^{n-1}\right|$$

$$= \left|\sum_{n=1}^{\infty} \left(\frac{a_n}{h}\left((x-x_o+h)^n-(x-x_o)^n\right)-na_n(x-x_o)^{n-1}\right)\right|$$

$$\leq \left|\frac{a_n}{h}\left(\sum_{k=0}^{n}\binom{n}{k}(x-x_o)^{n-k}h^k-(x-x_o)^n\right)-na_n(x-x_o)^{n-1}\right|$$

$$= \left| a_n h \sum_{k=2}^{n} \binom{n}{k} (x-x_0)^{n-k} h^{k-2} \right|$$

$$\leqslant |h| \, |a_n| c^{n-2} \leqslant \varepsilon \, .$$

Hieruit volgt het gestelde.

<u>Gevolg.</u> f is oneindig vaak differentieerbaar op $|x-x_0| \leqslant \rho$, en $a_n = \frac{f^{(n)}(x_0)}{n!}$ $(n=0,1,2,\ldots)$.

<u>Opmerking.</u> Het kan voorkomen, dat de convergentiestraal van de reeks van de afgeleide groter is dan ρ .
Bijv.: neem $a_n=1$ als $n=p^r$ $(r=0,1,2,\ldots)$, en $a_n=0$ anders. Dan convergeert $\sum_{n=0}^{\infty} a_n x^n$ niet als $|x| = 1$, maar wel als $|x| < 1$. Daar nu ρ een gehele macht van $p^{\frac{1}{e}}$ moet zijn, is $\rho = p^{-\frac{1}{e}}$. De reeks van de afgeleide heeft echter $p^{\frac{e-1}{e}}$ tot convergentiestraal.

<u>Stelling 4.</u> Als in $K_{\mathfrak{p}}$ $f(x) = \sum_{n=0}^{\infty} a_n (x-x_0)^n$, met convergentiestraal $\rho > 0$, en $|x_1-x_0| \leqslant \rho$, dan is:

$$(*) \quad f(x) = \sum_{n=0}^{\infty} \frac{f^{(n)}(x_1)}{n!} (x-x_1)^n \text{ voor } |x-x_1| \leqslant \rho \, .$$

<u>Gevolg.</u> Daar de gebieden $|x-x_0| \leqslant \rho$ en $|x-x_1| \leqslant \rho$ samenvallen, hebben we ook: de convergentiegebieden van beide machtreeksen vallen samen, en analytische voortzetting is in $K_{\mathfrak{p}}$ niet mogelijk.

<u>Bewijs:</u> Stel $|x-x_0| \leqslant \rho$, en c een positief reëel getal met $\rho \geqslant c \geqslant \max\{|x_1-x_0|, |x-x_1|\}$. Stel $\varepsilon > 0$, en N zó, dat $|a_n| c^n < \varepsilon$ voor $n \geqslant N$.
Nu is $f^{(n)}(x_1) = \sum_{k=0}^{\infty} \frac{(n+k)!}{k!} a_{n+k} (x_1-x_0)^k$, en de waardering van de algemene term van de reeks $(*)$:

$$\left| \sum_{k=0}^{\infty} \frac{(n+k)!}{n!k!} a_{n+k} (x_1-x_0)^k (x-x_1)^n \right|$$

$$\leqslant \left| \binom{n+k}{k} a_{n+k} (x_1-x_0)^k (x-x_1)^n \right| \quad \text{(voor zekere k)}$$

$$\leqslant |a_{n+k}| c^{n+k} < \varepsilon \quad \text{voor } n \geqslant N.$$

Hiermede is de convergentie van de reeks $(*)$ bewezen.

We bewijzen nu, dat $(*)-f(x)=0$.
Nu is:

$$\left|\sum_{n=N+1}^{\infty}\left(\sum_{k=0}^{\infty}\binom{n+k}{k} a_{n+k}(x_1-x_0)^k(x-x_1)^n - a_n(x-x_0)^n\right)\right|$$

$$\leq \left|\sum_{k=0}^{\infty}\binom{n+k}{k} a_{n+k}(x_1-x_0)^k(x-x_1)^n - a_n(x-x_0)^n\right| \quad \text{(voor zekere } n > N)$$

$$\leq \max\left\{\left|\binom{n+k}{k} a_{n+k}(x_1-x_0)^k(x-x_1)^n\right| , \left| a_n(x-x_0)^n \right|\right\}$$

(voor zekere

$$\leq \max\left\{|a_{n+k}|c^{n+k} , |a_n|c^n\right\} < \varepsilon .$$

Hieruit volgt:

$$|(*)-f(x)| \leq \max\Big\{\Big|\sum_{n=0}^{N}\Big(\sum_{k=0}^{N}\binom{n+k}{k}a_{n+k}(x_1-x_0)^k(x-x_1)^n - a_n(x-x_0)^{n}$$

$$\Big|\sum_{n=0}^{N}\ \sum_{k=N+1}^{\infty}\binom{n+k}{k}a_{n+k}(x_1-x_0)^k(x-x_1)^n\Big|, \varepsilon\Big\} \leq$$

$$\leq \max\Big\{\Big|\sum_{\substack{n,k=0\\ n+k>N}}^{N}\binom{n+k}{k}a_{n+k}(x_1-x_0)^k(x-x_1)^n\Big| ,$$

$$\Big|\sum_{k=N+1}^{\infty}\binom{m+k}{k} a_{m+k}(x-x_0)^k(x-x_1)^m\Big| ,$$

(voor zekere m)

$$\leq \max\left\{|a_n|c^n , |a_{m+l}|c^{m+l}, \varepsilon\right\} \quad \text{(voor zekere } n,l > N)$$

$$= \varepsilon .$$

Hieruit volgt het gestelde.

<u>Stelling 5.</u> Als $f(x) = \sum_{n=0}^{\infty} a_n(x-x_0)^n$, met convergentiestraal $\rho > 0$, en $f(\xi_i)=0$, waarbij $|\xi_i-x_0| \leq \rho$ $(i=1,2,\dots)$ en $\xi_i \longrightarrow x_0$, dan is $a_n=0$ $(n=0,1,2,\dots)$, dus f identiek nul op $|x-x_0| \leq \rho$.

<u>Bewijs:</u> Daar $f(\xi_i)-a_0=(\xi_i-x_0)\sum_{n=1}^{\infty} a_n(\xi_i-x_0)^{n-1}$, en $\sum_{n=1}^{\infty} a_n(x-x_0)^{n-1}$ continu is in $x=x_0$ (zelfs differentieerbaar), krijgen we bij de limietovergang $\xi_i \rightarrow x_0$:

$$0 - a_0 = 0; \quad \text{dus} \quad a_0 = 0.$$

Als bewezen is, dat $a_m=0$ (voor $m \leq n$, zekere $n \geq 0$), dan heeft $\dfrac{f(\xi_i)}{(\xi_i-x_0)^{n+1}}$ een limiet als $i \longrightarrow \infty$, en

$$\frac{f(\xi_i)}{(\xi_i-x_0)^{n+1}} - a_{n+1} = (\xi_i-x_0)\sum_{k=n+2}^{\infty}(\xi_i-x_0)^{k-n-2} ,$$

zodat we na de limietovergang $\xi_i \longrightarrow x_0$ weer krijgen:

$$a_{n+1} = 0, \quad \text{q.e.d.}$$

Gebruik makende van stelling 4, stelling 5 en § 18, stelling 4, krijgen we een bewijs voor:

Stelling 6. Als in $K_{\mathfrak{p}}$ de convergentiestraal van $f(x) = \sum_{n=0}^{\infty} a_n x^n$ niet kleiner dan 1 is, en f oneindig veel nulpunten in $I_{\mathfrak{p}}$ heeft, dan is f identiek nul op zijn convergentiegebied (dus ook op $I_{\mathfrak{p}}$).

Colloquium "P-adische getallen"

Voordracht op 4 november 1960

door

H. de Vries en H. Jager

Een rekenkundige eigenschap der Taylorcoëfficiënten van rationale functies

§ 20. Het binomium van Newton.

Stelling 1. Als $f_i(z) = \sum_{\nu=0}^{\infty} a_{i\nu} z^{\nu}$ $(z \in I_{\mathfrak{p}}$, $i=1,2,\ldots)$, en $a_{i\nu} \to a_{\nu}$ ($i \to \infty$, gelijkmatig in ν), dan is $f(z) = \sum_{\nu=0}^{\infty} a_{\nu} z^{\nu}$ convergent voor $z \in I_{\mathfrak{p}}$, en $\lim_{i \to \infty} f_i(z) = f(z)$ $(z \in I_{\mathfrak{p}})$.

Bewijs. Stel $\varepsilon > 0$, en N zó, dat $|a_{i\nu}-a_{\nu}|_{\mathfrak{p}} < \varepsilon$ $(i \geq N$, $\nu=1,2,\ldots)$; verder M zó, dat $|a_{N\nu}|_{\mathfrak{p}} < \varepsilon$ $(\nu \geq M)$; dan:

$$|a_{\nu}|_{\mathfrak{p}} = |a_{N\nu} - (a_{N\nu}-a_{\nu})|_{\mathfrak{p}} < \varepsilon \qquad (\nu \geq M), \text{ dus } a_{\nu} \to 0$$

en $\sum_{\nu=0}^{\infty} a_{\nu} z^{\nu}$ convergent op $I_{\mathfrak{p}}$.

Ook:
$$|f(z)-f_i(z)|_{\mathfrak{p}} = \Big|\sum_{\nu=0}^{\infty} (a_{i\nu}-a_{\nu}) z^{\nu}\Big|_{\mathfrak{p}} \leq$$
$$\leq |a_{i\nu}-a_{\nu}|_{\mathfrak{p}} \; |z|_{\mathfrak{p}}^{\nu} \qquad (\text{zekere } \nu)$$
$$< \varepsilon \quad (\text{voor } i \geq N,\ z \in I_{\mathfrak{p}}), \text{ q.e.d.}$$

Stelling 2. Zij $x, z \in K_{\mathfrak{p}}$, $|x|_{\mathfrak{p}} < p^{-\frac{1}{p-1}}$, $|z|_{\mathfrak{p}} \leq 1$, dan is $\sum_{\nu=0}^{\infty} \binom{z}{\nu} x^{\nu}$ convergent, en ook te schrijven als een machtreeks in z.

Bewijs. De priemfactorontbinding van $\nu!$ bevat hoogstens $\left[\frac{\nu}{p}\right] + \left[\frac{\nu}{p^2}\right] + \ldots \leq \frac{\nu}{p-1}$ factoren p, dus $|\nu!|_{\mathfrak{p}}^{-1} \leq p^{\frac{\nu}{p-1}}$.

Schrijven we nu $\binom{z}{\nu} x^{\nu}$ als een polynoom in z:
$\frac{x^{\nu}}{\nu!} \sum_{j=0}^{\nu} c_{j\nu} z^j$, dan zijn de $c_{j\nu}$ geheel rationaal, en vinden we:

$$\left|\binom{z}{\nu} x^{\nu}\right|_{\mathfrak{p}} \leq \frac{|x^{\nu}|_{\mathfrak{p}}}{|\nu!|_{\mathfrak{p}}} \leq |x|_{\mathfrak{p}}^{\nu} \; p^{\frac{\nu}{p-1}} \leq p^{-\frac{\nu}{e}} .$$

($p^{-\frac{1}{e}}$ is de grootste waardering < 1).

Hieruit volgt de convergentie van $\sum_{\nu=0}^{\infty} \binom{z}{\nu} x^{\nu}$.

We kunnen nu schrijven: $f_i(z) = \sum_{\nu=0}^{i} \binom{z}{\nu} x^{\nu} = \sum_{j=0}^{i} \Big(\sum_{\nu=0}^{i} d_{j\nu}\Big)$:
met
$$d_{j\nu} = \frac{x^{\nu}}{\nu!} c_{j\nu}, \text{ dus } |d_{j\nu}|_{\mathfrak{p}} \leq p^{-\frac{\nu}{e}} .$$

Hieruit volgt, dat aan de voorwaarden van stelling 1 is voldaan, en $\lim_{i \to \infty} f_i(z) = \sum_{\nu=0}^{\infty} \binom{z}{\nu} x^{\nu}$ op $I_{\mathfrak{p}}$ in een machtreeks naar z is te ontwikkelen, q.e.d.

Stelling 3. Als $A = \sum_{\nu=0}^{\infty} a_\nu$ en $B = \sum_{\nu=0}^{\infty} b_\nu$ twee convergente reeksen zijn in $K_{\mathfrak{p}}$, en $c_n = \sum_{\nu=0}^{n} a_\nu b_{n-\nu}$ $(n=0,1,2,\dots)$, dan convergeert ook $C = \sum_{\nu=0}^{\infty} c_\nu$, en $AB=C$.

Bewijs. Zij $\varepsilon > 0$, en N zó, dat $|a_\nu|_{\mathfrak{p}} < \varepsilon$, $|b_\nu|_{\mathfrak{p}} < \varepsilon$ $(\nu > N)$. Dan geldt ook: $|A-A_n|_{\mathfrak{p}} < \varepsilon$, $|B-B_n|_{\mathfrak{p}} < \varepsilon$ $(n > N)$, waarbij $A_n = \sum_{\nu=0}^{n} a_\nu$, $B_n = \sum_{\nu=0}^{n} b_\nu$.

Nu geldt: $C_n = \sum_{\nu=0}^{n} c_\nu = \sum_{\nu=0}^{n} a_\nu B_{n-\nu} = A_n B + \sum_{\nu=0}^{n} a_\nu \beta_{n-\nu}$ met $\beta_\nu = B_\nu - B$. Hieruit:

$$|AB-C_n|_{\mathfrak{p}} \leq \max_{\nu=0,1,\dots,n} \left\{ |(A-A_n)B_n|_{\mathfrak{p}}, |a_\nu \beta_{n-\nu}|_{\mathfrak{p}} \right\}.$$

Is nu $M = \max_{\nu=0,1,2,\dots} \left\{ |B|_{\mathfrak{p}}, |\beta_\nu|_{\mathfrak{p}}, |a_\nu|_{\mathfrak{p}} \right\}$, dan geldt voor $n > 2N$:

$$|AB-C_n|_{\mathfrak{p}} \leq \varepsilon M;$$ hieruit volgt het gestelde.

Stelling 4. Als $\sum_{\nu=0}^{\infty} \binom{\alpha}{\nu} x^\nu$ en $\sum_{\nu=0}^{\infty} \binom{\beta}{\nu} x^\nu$ in $K_{\mathfrak{p}}$ convergeren, dan convergeert ook $\sum_{\nu=0}^{\infty} \binom{\alpha+\beta}{\nu} x^\nu$, en

$$\sum_{\nu=0}^{\infty} \binom{\alpha+\beta}{\nu} x^\nu = \left(\sum_{\nu=0}^{\infty} \binom{\alpha}{\nu} x^\nu\right) \cdot \left(\sum_{\nu=0}^{\infty} \binom{\beta}{\nu} x^\nu\right).$$

Bewijs. Volgt uit stelling 3, en het feit, dat

$$\sum_{\nu=0}^{n} \binom{\alpha}{\nu} \binom{\beta}{n-\nu} = \binom{\alpha+\beta}{n}.$$

Het feit, dat $(1+x)^\alpha = \sum_{\nu=0}^{\infty} \binom{\alpha}{\nu} x^\nu$ als α geheel rationaal is, en stelling 4 geven de rechtvaardiging van de schrijfwijze:

$$(1+x)^\alpha = \sum_{\nu=0}^{\infty} \binom{\alpha}{\nu} x^\nu$$ (voor het geval de reeks convergeert).

§ 21. Een arithmetische eigenschap van de Taylorcoëfficiënten van rationale functies

Hoofdstelling. Zij f(z) een, in een omgeving van 0 reguliere, rationale functie met een machtreeksontwikkeling $\sum_{n=0}^{\infty} a_n z^n$, waarin alle a_n, (n=0,1,...) algebraïsch zijn.
Wanneer nu oneindig vele van deze Taylorcoëfficiënten nul zijn bestaat er een natuurlijk getal r en een aantal niet negatieve, geheel rationale getallen $r_1, r_2, \ldots r_\rho$ met

$$r_i \not\equiv r_j \pmod r,\ i \neq j,\ i,j=1,2,\ldots\rho \qquad (\text{dus } \rho \leq r)$$

en zó, dat alle Taylorcoëfficiënten a_n met

$$n \equiv r_i \pmod r,\ n \geqslant r_i,\ (i=1,2,\ldots\rho) \text{ nul zijn.}$$

Buiten deze zijn er nog hoogstens eindig veel andere nul.
Voor het bewijs van deze stelling leiden we een aantal hulpstellingen af.
Hulpstelling 1. Zij $f(z) = \sum_{n=0}^{\infty} a_n z^n$ een in een omgeving van 0 reguliere, rationale functie met algebraïsche Taylorcoëfficiënten. Dan bestaat er een aantal algebraïsche getallen $A_1, A_2, \ldots A_m$ en een aantal polynomen $P_1(x), P_2(x), \ldots P_m(x)$, alle met algebraïsche coëfficiënten, zó, dat voor voldoend grote n $a_n = \sum_{\mu=1}^{m} A_\mu^n P_\mu(n)$.
Bewijs 1°. We trachten f(z) te schrijven als $\frac{B(z)}{C(z)}$, met:

$$B(z) = \sum_{\lambda=0}^{l} b_\lambda z^\lambda,\quad C(z) = \sum_{\nu=0}^{n} c_\nu z^\nu,\quad b_\lambda, c_\nu \text{ algebraïsch}$$

Hiervoor is het voldoende van het volgende stelsel van lineaire vergelijking een algebraïsche oplossing te vinden:

$$\sum_{\mu=0}^{n} c_\mu a_{k-\mu} - b_k = 0 \qquad (k=0,1,\ldots),$$

waarbij de c_μ, b_k de onbekenden zijn; letters met niet-optredende indices nul gesteld. Nu is dit stelsel voor zekere l en n oplosbaar in het lichaam der complexe getallen. De oplosbaarheid kan uitgedrukt worden als volgt: alle (n+l+2) x (n+l+2) deelmatrices van de coëfficiëntenmatrix (die n+l+2 kolommen heeft) zijn singulier.
Deze voorwaarde is volledig uitgedrukt in het lichaam ontstaan door de a_ν aan het lichaam der rationale getallen te adjungeren; ook hierin is dus het stelsel oplosbaar voor zekere l en n, en een oplossing is dan algebraïsch omdat de a_ν algebraïsch zijn.

2°. Schrijf $\frac{B(z)}{C(z)}$ als: $Q(z) + \frac{B^*(z)}{C(z)}$, waarbij Q een polynoom, en gr $B^* <$ gr C. Als $\alpha_1,\ldots,\alpha_m$ de verschillende nulpunten zijn van C(z), dan kunnen we $\frac{B^*(z)}{C(z)}$ schrijven als:

$$\frac{B^*(z)}{C(z)} = \sum_{\mu=1}^{m} \sum_{i=1}^{k_\mu} \frac{d_{\mu i}}{(1-\frac{z}{\alpha_\mu})^i}\;, \alpha_\mu\;, d_{\mu i} \text{ algebraïsch.}$$

$$= \sum_{\nu=0}^{\infty} \sum_{\mu=1}^{m} \sum_{i=1}^{k_\mu} \binom{-i}{\nu}\, d_{\mu i}\, \frac{(-z)^\nu}{\alpha_\mu^\nu}\;,$$

dus $a_\nu = \sum_{\mu=1}^{m} \left(\frac{1}{\alpha_\mu}\right)^\nu P_\mu(\nu)$, voor $\nu >$ graad van Q(z), waarbij de P_μ polynomen met algebraïsche coëfficiënten zijn.

Hulpstelling 2. Gegeven een aantal algebraïsche getallen $A_1, A_2, \ldots A$ en een aantal polynomen $P_1(x), P_2(x), \ldots P_m(x)$ met algebraïsche coëfficiënten. Zij ν een natuurlijk getal, zó, dat $B_\mu = \nu A_\mu$ geheel algebraïsch is en de coëfficiënten in $Q_\mu(x) = \nu P_\mu(x)$ geheel algebraïsch zijn ($\mu = 1,2,\ldots m$). Zij $F(n) = \sum_{\mu=1}^{m} A_\mu^n P_\mu(n)$ en $G(n) = \sum_{\mu=1}^{m} B_\mu^n Q_\mu(n)$. Nu geldt: uit $F(n_0)=0$ volgt $G(n_0)=0$ en omgekeerd.

Bewijs: triviaal.

Zij $\mathfrak{a}$ een ideaal van S, $\mathfrak{a} \neq (0)$, $(\neq (1))$. Onder $\varphi(\mathfrak{a})$ verstaan we nu de orde van de (eindige) groep van eenheden uit de restklassering $S/\mathfrak{a}$.

Hulpstelling 3. (Fermat) Zij $\mathfrak{a}$ een ideaal van S, $\mathfrak{a} \neq (0)$ en zij $b \in S$ zó, dat $((b), \mathfrak{a}) = (1)$. Dan is $b^{\varphi(\mathfrak{a})} \equiv 1 \pmod{\mathfrak{a}}$.

Bewijs. Een element $b+\mathfrak{a}$ uit $S/\mathfrak{a}$ is dan en slechts dan een eenheid, als $((b), \mathfrak{a}) = (1)$. Daar de groep der eenheden van $S/\mathfrak{a}$ de orde $\varphi(\mathfrak{a})$ heeft, geldt: $b^{\varphi(\mathfrak{a})} \equiv 1 \pmod{\mathfrak{a}}$, als $b+\mathfrak{a}$ een eenheid van $S/\mathfrak{a}$.

Lemma. Gegeven: m algebraïsche getallen $A_1, A_2, \ldots A_m$ en m polynomen met algebraïsche coëfficiënten $P_1(x), P_2(x) \ldots P_m(x)$. Zij $F(n) = \sum_{\mu=1}^{m} A_\mu^n P_\mu(n)$, $n=0,1,2,\ldots$.

Wanneer nu F(n) voor oneindig vele n nul wordt, is er een natuurlijk getal r en een eindig aantal getallen $r^{(1)}, r^{(2)}, \ldots r^{(\rho)}$, uit de verzameling $0,1,2,\ldots r-1$, zó, dat $F(r^{(\tau)} + r\nu) = 0$ voor $\tau = 1,2,\ldots \rho$, $\nu = 0,1,2,\ldots$, terwijl er buiten deze punten nog hoogstens een eindig aantal is, waar F(n) ook nul wordt.

Bewijs. Zonder beperking der algemeenheid mag men aannemen, dat zowel de A_μ, $\mu=1,2,\ldots m$, als de coëfficiënten van de polynomen $P_\mu(x)$, $\mu = 1,2,\ldots m$, geheel algebraïsch zijn (hulpstelling 2).

Zij K een eindige algebraïsche uitbreiding van het lichaam der rationale getallen, zó, dat zowel de A_μ als de coëfficiënten van de $P_\mu(x)$, $\mu=1,2,\ldots m$, in K bevat zijn.

In K kan men nu een priemideaal $\mathfrak{p}$ vinden, dat niet voorkomt in de ontbindingen van de hoofdidealen (A_μ), $\mu=1,2,\ldots m$ uit de ring S van de gehele getallen van K.
We nemen nu zo'n $\mathfrak{p}$ en vormen het lichaam $K_\mathfrak{p}$ van de $\mathfrak{p}$-adische getallen.
Is p het rationale priemgetal uit $\mathfrak{p}$, dan kiezen we e zó, dat $p \in \mathfrak{p}^e$ $p \notin \mathfrak{p}^{e+1}$. Daarna kiezen we een natuurlijk getal $k > \frac{e}{p-1}$ en schrijve ter afkorting $r = \varphi(\mathfrak{p}^k)$.
Nu geldt, daar uit $((A_\mu), \mathfrak{p}) = (1)$ volgt dat ook $((A_\mu), \mathfrak{p}^k) = (1)$:

$$A_\mu^r \equiv 1 \pmod{\mathfrak{p}^k},\ \mu=1,2,\ldots m \qquad \text{(hulpstelling 3).}$$

We kiezen nu nog een $\pi \in \mathfrak{p}$, zodat $\pi^2 \notin \mathfrak{p}$ (dit is mogelijk op grond van § 18, stelling 1); dus $|\pi|_\mathfrak{p} = p^{-\frac{1}{e}}$.
In $K_\mathfrak{p}$ kan men nu getallen a_μ vinden met

$$A_\mu^r = 1 + \pi^k a_\mu \quad , \quad \mu=1,2,\ldots m$$

Uit $\pi^k a_\mu \in \mathfrak{p}^k$ volgt: $|\pi^k a_\mu|_\mathfrak{p} \leq p^{-\frac{k}{e}}$ en dus, omdat $k > \frac{e}{p-1}$:

$$|\pi^k a_\mu|_\mathfrak{p} < p^{-\frac{1}{p-1}} .$$

Hieruit volgt (§ 20, stelling 2):

$$\sum_{\nu=0}^{\infty} a_\mu^\nu \pi^{k\nu} \binom{z}{\nu} \quad \text{convergeert voor alle } z \in I_\mathfrak{p}$$

dus $(A_\mu^r)^z$ is nu gedefinieerd voor elke $z \in I_\mathfrak{p}$
Zij $\{n_i\}_{i=1}^{\infty}$ de rij van niet negatieve gehele getallen waarvoor F(n nul wordt. We schrijven $n_i=r_i+rz_i$, waarbij elke r_i een van de getallen 0,1,2,...r-1 is. De rij $\{z_i\}_{i=1}^{\infty}$ is weer een onbegrensde rij van niet negatieve gehele getallen. De rij $\{r_i\}_{i=1}^{\infty}$ is gevormd uit de getallen 0,1,2,...r-1. Minstens één van deze getallen moet dus in $\{r_i\}_{i=1}^{\infty}$ oneindig vaak voorkomen. Stel dat

$$r^{(1)},\ r^{(2)},\ldots r^{(\rho)} \qquad 1 \leq \rho \leq r \quad \text{die getallen onder}$$

de getallen 0,1,2,...,r-1 zijn die in $\{r_i\}_{i=1}^{\infty}$ werkelijk oneindig vaa voorkomen.
Bij elke $r^{(h)}$ hoort dan een rij indices

$$i_1^{(h)}, i_2^{(h)}, i_3^{(h)}, \ldots \qquad h=1,2,\ldots \rho ,$$

zó, dat $r_{i_\tau^{(h)}} = r^{(h)}$ en dus

$$n_{i_\tau^{(h)}} = r^{(h)} + r\, z_{i_\tau^{(h)}} \qquad \begin{array}{l} \tau=1,2,3,\ldots \\ h=1,2,\ldots \rho , \end{array}$$

met $\qquad z_{i_\tau^{(h)}} \rightarrow \infty$ voor $\tau \rightarrow \infty$.

De functies

$$f_h(z) = \sum_{\mu=1}^{m} A_\mu^{r^{(h)}} A^{rz} P_\mu (r^{(h)}+rz)$$ zijn in het bijzonder

gedefinieerd voor elke $z \in I_{\mathfrak{p}}$, $h=1,2,\ldots\rho$; zij bezitten steeds in I een oneindige rij nulpunten, n.l.

$$z_{i_1}^{(h)}, z_{i_2}^{(h)}, z_{i_3}^{(h)}, \ldots.,$$ daar voor $n=1,2,\ldots$ $f_h(n)=F(r^{(h)}+rn)$.

Nu is $f_h(z)$ op $I_{\mathfrak{p}}$ voor te stellen als een machtreeks in z, immers

$$f_h(z) = \sum_{\mu=1}^{m} A_\mu^{r^{(h)}} \cdot A_\mu^{rz} P_\mu (r^{(h)}+rz) =$$

$$\sum_{\mu=1}^{m} \sum_{\nu=1}^{\infty} A_\mu^{r^{(h)}} a_\mu^\nu \pi^{k\nu} \binom{z}{\nu} P_\mu (r^{(h)}+rz) = \sum_{n=0}^{\infty} b_n z^n$$

(§ 20, stelling 2).

Uit § 19, stelling 6 volgt nu:

$$f_h(z) \equiv 0 \text{ op } I_{\mathfrak{p}} , \; h=1,2,\ldots \rho ,$$

i.h.b. $\qquad F(r^{(h)}+rn) = 0 \quad$ voor $n=0,1,2,\ldots$.

Dat we hiermee alle nulpunten van $F(n)$ op hoogstens een eindig aantal uitzonderingen na gevonden hebben volgt uit de definitie van de verzameling getallen $r^{(1)}, r^{(2)} \ldots r^{(\rho)}$. Zouden we n.l. nog een oneindig aantal nulpunten overhouden dan zou dit een nieuwe $r^{(\kappa)}$ in deze verzameling opleveren.

Het bewijs van de hoofdstelling volgt nu onmiddellijk uit voorgaand lemma en hulpstelling 1.

Colloquium "P-adische getallen"

Voordracht op 18 november
door
Dr. C.G. Lekkerkerker

Opmerkingen bij de invoering van $K_{\mathfrak{p}}$ (p.43-45)

Literatuur: H. Weyl, Algebraic Theory of Numbers, Princeton, Third printing, 1954.

We gebruiken de volgende notaties:

k : lichaam der rationale getallen

K : algebraïsch getallenlichaam van graad n over k

$\mathfrak{p}$: priemideaal in K.

Getallen in K zullen we met griekse letters aangeven. We zullen $\mathfrak{p}$ een deler noemen van elk geheel getal β in het ideaal $\mathfrak{p}$, en schrijven $\mathfrak{p} | \beta$, of ook $\beta \equiv 0 \pmod{\mathfrak{p}}$. Algemener noemen we $\mathfrak{p}^t$ een deler van $\alpha \in K$, als $\alpha = \frac{\beta}{\gamma}$ (β, γ geheel) en het aantal factoren $\mathfrak{p}$ in de teller β tenminste t meer is dan het aantal in de noemer γ.

We gaan eerst even in op de definitie van p-adische getallen en beschouwen daartoe willekeurige sommen

(1) $$\sum_{t=h}^{\infty} a_t p^t \qquad \text{(h geheel)},$$

waarbij de a_t rationaal en (lokaal) geheel in p zijn, d.w.z. van de volgende vorm zijn:

$$a_t = \frac{b_t}{c_t} \text{ met } b_t, c_t \text{ geheel rationaal en } p \nmid c_t.$$

Zijn alle a_t gehele getallen uit een gegeven volledig restsysteem $\sum$ bijv. het restsysteem $\{0,1,\ldots,p-1\}$, dan noemen we (1) gemakshalve een standaardreeks. Twee uitdrukkingen $\sum a_t p^t$, $\sum a_t' p^t$ heten gelijk, als

(2) $$\sum_{s<t} a_s p^s \equiv \sum_{s<t} a_s' p^s \pmod{p^t} \text{ voor elke t.}$$

Elk getal $a_t = b_t/c_t$ is congruent met één en slechts één getal a_t' in $\sum$, want er is precies één oplossing van

(3) $$c_t x \equiv b_t \pmod{p},\ x \in \sum .$$

Dan is het duidelijk dat elke uitdrukking (1) gelijk is aan één standaardreeks. De uitdrukkingen (1) geven dus, met bovenstaande definiti van gelijkheid, juist het lichaam k_p van de p-adische getallen.

Het voordeel van deze invoering is dat optelling en vermenigvuldiging van p-adische getallen zich op bijzonder eenvoudige en voor de hand liggende wijze laten uitdrukken.

We gaan nu hetzelfde doen voor K en $\mathfrak{p}$. De idealen $\mathfrak{p}$ en $\mathfrak{p}^2$ zijn niet hetzelfde. Er is dus een geheel getal ρ in K met

$$\rho \in \mathfrak{p}\ ,\quad \rho \notin \mathfrak{p}^2 .$$

We beschouwen uitdrukkingen

(4) $$\sum_{t=h}^{\infty} \alpha_t \rho^t \qquad \text{(h geheel rationaal; } \alpha_t \in K \text{ en geheel in } \mathfrak{p}\text{)}$$

Gelijkheid van twee uitdrukkingen (4) definiëren we door

(5) $$\sum_{s<t} \alpha_s \rho^s \equiv \sum_{s<t} \alpha'_s \rho^s \pmod{\mathfrak{p}^t} \quad \text{voor elke t.}$$

Desgewenst kan men in K een volledig restsysteem modulo $\mathfrak{p}$, stel Σ beschouwen (het bestaat uit p^f elementen, waarbij f de <u>graad</u> van $\mathfrak{p}$ heet). Dan is elke uitdrukking (4) gelijk aan één standaardreeks $\sum \alpha'_t \rho^t$, $\alpha'_t \in \Sigma$;dit komt neer op de eenduidige oplosbaarheid van congruenties

$$\alpha_t \rho^t = \frac{\beta_t}{\gamma_t} \rho^t \equiv A \rho^t + \alpha'_t \rho^t \pmod{\mathfrak{p}^{t+1}},$$

ofwel $\beta_t \equiv \gamma_t (A+\alpha'_t) \pmod{\mathfrak{p}}$, zó dat $\alpha'_t \in \Sigma$.

Optelling en vermenigvuldiging worden op de gebruikelijke wijze gedefiniëerd. Dan ontstaat een lichaam. Dit lichaam is volledig; voor een fundamentaalrij van standaardreeksen $\sum \alpha_t^{(i)} \rho^t$ geldt dat bij toenemende i op den duur steeds meer coëfficiënten $\alpha_t^{(i)}$ constant blijven:

$$\alpha_s^{(i_o)} = \alpha_s^{(i_o+1)} = \alpha_s^{(i_o+2)} = \ldots \quad \text{voor } s \leq t \text{ en zekere } i_o = i_o(t).$$

Verder is elke uitdrukking (4) in $\mathfrak{p}$ -adische zin te benaderen door getallen uit K. We hebben dus het lichaam $K_{\mathfrak{p}}$ van de $\mathfrak{p}$ -adische getallen gekregen.

De ring $I_{\mathfrak{p}}$ van de gehele $\mathfrak{p}$ -adische getallen wordt gegeven door de uitdrukkingen (4) met $h \geq 0$. Daar het restsysteem Σ eindig is is het duidelijk dat $I_{\mathfrak{p}}$ compact is.

We willen nog ingaan op de vraag of $K_{\mathfrak{p}}$ te beschouwen is als een uitbreiding van k_p. Zij p het priemgetal in $\mathfrak{p}$. Laat de kanonieke ontbinding van p gegeven worden door

(6) $$p = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g} \qquad (\mathfrak{p}_1 = \mathfrak{p}),$$

en zij $_i$ een geheel getal met $_i$ $_i$, $_i$ $_i^2$ (i=1,...,g). Dan is p= $_i^{e_i}$ $_i$, waarbij $_i$ geheel is in $_i$ (i=1,...,g). Dan is een uitdrukking (1) in de vorm (4) te schrijven; zijn twee uitdrukkingen (1) gelijk, dan ook de corresponderende uitdrukkingen. Dus is k_p bevat in K . Bijzonder eenvoudig is natuurlijk het geval $e_1=1$; dan kunnen we nemen =p.

Om in het algemene geval een beter inzicht te krijgen beschouwen we naast de lichamen k_p, $K_{\mathfrak{p}}$ nog een verzameling K_p. Die bestaat uit uitdrukkingen

$$(7) \qquad \sum_{t \geq h} \alpha_t p^t \qquad\qquad (\alpha_t \in K \text{ en geheel in } \mathfrak{p});$$

gelijkheid wordt gedefinieerd door congruentie van partiële sommen modulo machten $\mathfrak{p}^{et}$. Het is duidelijk hoe k_p ingebed is in K_p immers K_p is onder meer een vectorruimte over k_p van dimensie n. Verde is K_p een ring. We bewijzen nu (Weyl, p.101)

<u>Stelling</u>. K_p is isomorf met de directe som van de g lichamen $K_{\mathfrak{p}_1},\ldots,K_{\mathfrak{p}_g}$.

<u>Bewijs</u>. Een getal $A = \sum \alpha_t p^t$ uit K_p is ook een getal uit $K_{\mathfrak{p}_i}$, voor i=1,...,g, als we schrijven $p=\rho_i^{e_i}\beta_i$; gelijke uitdrukkingen geven weer gelijke uitdrukkingen. Maar nu kunnen verschillende getallen uit K_p corresponderen met hetzelfde getal uit een vaste $K_{\mathfrak{p}_i}$. In elk geval hebben we een zekere afbeeldingen Ω_i van K_p in $K_{\mathfrak{p}_i}$ (i=1,...,g). We beschouwen nu een willekeurig stel getallen

$$A_i = \sum_{t=h_i}^{\infty} \alpha_t^{(i)} \rho_i^t \in K_{\mathfrak{p}_i}$$

en zullen laten zien dat er één en slechts één getal $A=\sum \alpha_t p^t$ in K_p is, zó dat $\Omega_i A = A_i$ (i=1,...,g).

We beschouwen de volgende partiële sommen

$$A_{t,i} = \sum_{s < e_i t} \alpha_s^{(i)} \rho_i^s \quad (i=1,\ldots,g), \qquad A_t = \sum_{s<t} \alpha_s p^s .$$

Verder stellen we

$$\sum_{e_i t \leq s < e_i(t+1)} \alpha_s^{(i)} \rho_i^s = \beta_t^{(i)} p^t .$$

Dan is $\beta_t^{(i)}$ geheel in $\mathfrak{p}_i$. Stel eens dat de α_s met $s < t$ zó bepaald zijn dat $A_t \equiv A_{t,i} \pmod{\mathfrak{p}_i^{e_i t}}$, voor i=1,...,g. We bepalen nu α_t z dat dit ook geldt met t vervangen door t+1. We moeten daartoe voldoe aan de volgende congruenties

$$A_t + \alpha_t p^t \equiv A_{t,i} + \beta_t^{(i)} p^t \pmod{\mathfrak{p}_i^{e_i(t+1)}},$$

ofwel
$$\alpha_t \equiv \beta_t^{(i)} + (A_{t,i}-A_t)p^{-t} \pmod{\mathfrak{p}_i^{e_i}}.$$

De tweede term rechts is geheel in $\mathfrak{p}_i$, voor alle i, wegens de inductieonderstelling. Nu geldt in K de chinese reststelling, ook voor congruenties modulo priemidealen. Dan is er een α_t die aan bovenstaande congruenties voldoet, en deze α_t is eenduidig bepaald modulo $\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g} = p$. Dus is er één getal A met $\Omega_i A=A_i$. En $(\Omega_1,\ldots,\Omega_g)$ is de gezochte isomorfie.

Over de exponenten e_i valt nog het volgende op te merken. Met behulp van Galoistheorie kan men bewijzen dat ze gelijk zijn. Verder zijn ze >1 dan en slechts dan als p een deler is van de discriminant van K.

Er is een vergaande analogie met lichamen van algebraïsche functies. Dan is k het lichaam van de rationale functies en K een algebraische uitbreiding. Priemgetallen zijn de lineaire vormen z-a (a een willekeurig complex getal). De punten a waar de exponenten $e_i > 1$ zijn de vertakkingspunten van het bij K behorende Riemanns oppervlak. De priemidealen $\mathfrak{p}_i$ corresponderen met de verschillende bladen daarvan, en $K_{\mathfrak{p}_i}$ is een lichaam van Laurentreeksen.

Colloquium "P-adische getallen"

Voordracht op 2 december 1960

door

M.A. Maurice

Opmerkingen: 1. Deze syllabus bevat het bewijs van de op blz. 32 uitgesproken stelling van Mahler. Dit bewijs is afkomstig van Prof. Mahler; het zal worden gepubliceerd in "Journal für die reine und angewandte Mathematik".

2. De bladzijden 61 t/m 64 "vervangen" de blz.32 t/m 37 van de syllabus.

§ 16,6'. Lemma 1: Indien $g(x)$ een continue p-adische functie is van x voor $x \in N_p$, zodanig, dat $\lim\limits_{\substack{x \in N \\ |x|_p \to 0}} \left|\frac{g(x)}{x}\right|_p = 0$, dan is ook $\lim\limits_{\substack{x \in N_p \\ |x|_p \to 0}} \left|\frac{g(x)}{x}\right|_p = 0$.

Bewijs: Bij elke $s > 0$ is een $t > 0$ te vinden, zodanig, dat

$$\left|\frac{g(x)}{x}\right|_p \leq p^{-s} \quad \text{voor} \quad x \in N, \quad 0 < |x|_p \leq p^{-t} .$$

Zij ξ een p-adisch getal met $g(\xi) \neq 0$, $0 < |\xi|_p \leq p^{-t}$.

Op grond van de continuiteit van $g(x)$ bestaat er een $u > 0$, zodanig, dat

$$|g(\eta)-g(\xi)|_p < |g(\xi)|_p \quad \text{voor} \quad \eta \in N_p, \quad |\eta-\xi|_p \leq p^{-u},$$

dus

$$|g(\eta)|_p = |g(\xi)|_p \quad \text{voor} \quad \eta \in N_p, \quad |\eta-\xi|_p \leq p^{-u}.$$

Kies $\eta = x \in N$, zodanig, dat

$$|x-\xi|_p \leq \min(p^{-u}, \tfrac{1}{p}|\xi|_p).$$

Dan geldt zowel $|g(x)|_p = |g(\xi)|_p$

als $|x|_p = |\xi|_p \neq 0$.

Dan is echter

$$\left|\frac{g(\xi)}{\xi}\right|_p = \left|\frac{g(x)}{x}\right|_p \leq p^{-s} .$$

Lemma 2: Zij $f(x)$ een continue p-adische functie voor $x \in N_p$. $f(x)$ is dan en slechts dan differentieerbaar in $x=0$ (met afgeleide $f'(0)=\lambda$), indien

$$\lim_{\substack{x \in N \\ |x|_p \to 0}} \left| \frac{f(x)-f(0)}{x} - \lambda \right|_p = 0.$$

Bewijs: a. Uiteraard is de voorwaarde nodig.

b. Stel de voorwaarde vervuld en zij $g(x) = f(x)-f(0) - \lambda x$.

Dan is $\displaystyle \lim_{\substack{x \in N \\ |x|_p \to 0}} \left| \frac{g(x)}{x} \right|_p = 0$

en dus $\displaystyle \lim_{\substack{x \in N_p \\ |x|_p \to 0}} \left| \frac{g(x)}{x} \right|_p = 0,$

m.a.w. $\displaystyle \lim_{\substack{x \in N_p \\ |x|_p \to 0}} \left| \frac{f(x)-f(0)}{x} - \lambda \right|_p = 0.$

Zij nu $f(x)$ een continue p-adische functie, die aan de voorwaarde van lemma 2 voldoet.

Op grond van stelling 16,4 geldt ($x \in N_p$)

$$f(x) = \sum_{n=0}^{\infty} a_n \binom{x}{n}, \quad \lim_{n \to \infty} |a_n|_p = 0.$$

Stelling: Indien $f'(0) = \lambda$ bestaat, dan is $\displaystyle \lim_{n \to \infty} \left| \frac{a_n}{n} \right|_p = 0.$

Bewijs:

Definieer: $h(0) = 0$

$$h(x) = \frac{f(x)-f(0)-\lambda x}{x} = \frac{g(x)}{x} \quad \text{voor } x \neq 0.$$

Dan is $h(x)$ continu voor $x \neq 0$.

$h(x)$ is ook continu in $x=0$, daar $\displaystyle \lim_{\substack{x \in N_p \\ |x|_p \to 0}} |h(x)|_p = 0.$

Zij $\displaystyle h(x) = \sum_{n=0}^{\infty} c_n \binom{x}{n}, \quad \lim_{n \to \infty} |c_n|_p = 0.$

Dan is enerzijds

$$f(x) = f(0) + \lambda x + \sum_{n=0}^{\infty} c_n \left\{ (n+1)\binom{x}{n+1} + n\binom{x}{n} \right\}$$

en anderzijds

$$f(x) = \sum_{n=0}^{\infty} a_n \binom{x}{n}.$$

Hieruit volgt $\quad a_n = n(c_{n-1}+c_n) \quad$ voor $n \geqq 2$, zodat $$\lim_{n\to\infty} \left|\frac{a_n}{n}\right|_p = \lim_{n\to\infty} |c_{n-1}+c_n|_p = 0.$$

<u>Stelling</u>: Zij $\{a_n\}$ een p-adische nulrij. Indien nu

$$\lambda = \lim_{\substack{|x|_p\to 0\\ x\in N_p}} \sum_{n=1}^{\infty} \frac{a_n}{n}\binom{x-1}{n-1}$$

bestaat, dan is

$$\lim_{n\to\infty}\left|\frac{a_n}{n}\right|_p = 0$$

(dit is de stelling van 16,6; blz.32).

<u>Bewijs</u>: volgt onmiddellijk uit de voorgaande stelling.

<u>16,7'</u>: <u>Stelling</u>: Zij $\left\{\frac{a_n}{n}\right\}$ een p-adische nulrij. Dan bestaat de limiet

$$\lambda = \lim_{\substack{x\to 0\\ x\in N}} \sum_{n=0}^{\infty} \frac{a_n}{n}\binom{x-1}{n-1},$$

en bovendien is

$$\lambda = \sum_{n=1}^{\infty} (-1)^{n-1}\frac{a_n}{n} .$$

<u>Bewijs</u>: zie 16,7; blz.35.

<u>16,8'</u>: <u>Stelling</u>: Zij $f(x) = \sum_{n=0}^{\infty} a_n\binom{x}{n}$ continu op N_p, en zij

$$a_n(y) = \sum_{k=0}^{\infty} a_{n+k}\binom{y}{k} .$$

1. Indien $$\lim_{n\to\infty}\frac{a_n(y)}{n} = 0,$$

   dan bestaat $f'(y)$ en bovendien is

$$f'(y) = \sum_{n=1}^{\infty}(-1)^{n-1}\frac{a_n(y)}{n} .$$

2. Indien $f'(y)$ bestaat, dan is

$$\lim_{n\to\infty}\frac{a_n(y)}{n} = 0.$$

<u>Bewijs</u>: dit volgt uit de voorgaande stellingen op grond van de relatie

$$\frac{f(x+y)-f(y)}{x} = \sum_{n=1}^{\infty}\frac{a_n(y)}{n}\binom{x-1}{n-1}.$$

<u>16,9'</u>: <u>Stelling</u>: Zij $f(x) = \sum_{n=0}^{\infty} a_n\binom{x}{n}$ continu op N_p. Indien nu de afgeleide $f'(x)$ bestaat en continu is voor alle $x\in N_p$, dan geldt

1) de reeksen $a'_n = \sum_{k=1}^{\infty} (-1)^{k-1} \frac{a_{k+n}}{k}$ zijn convergent ($n=0,1,2,3,\ldots$).

2) $\{a'_n\}$ is een nulrij

3) $f'(x) = \sum_{n=0}^{\infty} a'_n \binom{x}{n}$ voor $x \in N_p$.

<u>Bewijs</u>: zie 16,9 (blz.36).