Seminar zur Catalanschen Vermutung, Regensburg, Sommersemester 2006

Hinweise zu Vortrag 6, Gabor Wiese, 18. Mai 2006

Ab diesem Vortrag werden wir nicht mehr ohne die p-adischen Zahlen auskommen. Leider werden diese in der Vorlesung erst später behandelt, so dass wir uns hier mit einer ad-hoc-Definition behelfen werden und die wichtigen Sätze glauben werden.

Hier sind einige notwendige Definitionen.

Definition 0.0.1 *Sei K ein Körper und $|\cdot|$ ein Betrag (d.h. $|x| \geq 0$, $|x| = 0 \Leftrightarrow x = 0$, $|xy| = |x||y|$, $|x+y| \leq |x| + |y|$ für alle $x, y \in K$). Der Betrag $|\cdot|$ heißt* archimedisch*, wenn es eine natürliche Zahl n gibt mit $|n| > 1$. Sonst heißt er* ultrametrisch*.*

Betrachten wir Beispiele.

- Der gewöhnliche Betrag auf $\mathbb{Q}$ ist archimedisch. Wir bezeichnen ihn zur Unterscheidung oft mit $|\cdot|_\infty$.
- Sei p eine Primzahl. Wir haben $\mathrm{ord}_p(\frac{r}{s}) = \mathrm{ord}_p(r) - \mathrm{ord}_p(s)$ definiert. Man erhält den *p-Betrag*, indem man
$$|\frac{r}{s}|_p := p^{-\mathrm{ord}_p(\frac{r}{s})}$$
setzt. Dieser Betrag ist klarerweise ultrametrisch.

Lemma 0.0.2 *Sei $|\cdot|$ ein ultrametrischer Betrag auf einem Körper K. Dann gilt die* starke Dreiecksungleichung
$$|x+y| \leq \max\{|x|, |y|\}$$
für alle $x, y \in K$. Ist $|x| \neq |y|$, dann gilt sogar Gleichheit.

Beweis. Zum Beweis können wir ohne Einschränkung $|x| \geq |y|$ annehmen. Dann gilt aber auch für jede natürliche Zahl k, dass
$$|x+y|^k = |\sum_{i=0}^{k} \binom{k}{i} x^i y^{k-i}| \leq (k+1)|x^k|.$$
Also gilt
$$|x+y| \leq |x|(k+1)^{1/k}.$$
Nehmen wir nun den Limes $k \to \infty$, so erhalten wir die erste Aussage, da $(k+1)^{1/k}$ gegen 1 geht.

Um den Nachsatz zu sehen, gelte nun $|x| > |y|$. Wir nehmen an, dass $|x+y| < |x|$. Nun ist aber $|x| = |x+y-y| \leq \max\{|x+y|, |y|\} < |x|$, was ein Widerspruch ist. □

Lemma 0.0.3 *Sei $|\cdot|$ ein ultrametrischer Betrag auf einem Körper K. Sei (a_n) eine Folge von Zahlen aus K.*

Dann ist die Reihe $\sum_{n=0}^{\infty} a_n$ genau dann konvergent, wenn die $(a_n)_n$ eine Nullfolge bilden. Dies ist natürlich in Bezug auf den gegebenen Betrag zu verstehen.

Beweis. Die Reihe konvergiert nach Definition, wenn die Folge der Partialsummen $b_n := \sum_{i=0}^{n} a_i$ eine Cauchy-Folge bildet. Dass die a_n eine Nullfolge bilden müssen, ist klar. Umgekehrt nehmen wir dies nun an. Das heißt, dass es zu vorgegebenem $\epsilon > 0$ ein N gibt, so dass für alle $n > N$ gilt $|a_n| < \epsilon$. Dies bedeutet aber auch für $n > N$ und $m > 0$

$$|b_{n+m} - b_n| = |\sum_{i=n+1}^{n+m} a_n| \leq \max_{i \in \{n+1,\ldots,n+m\}} \{|a_i|\} < \epsilon,$$

was zeigt, dass die Partialsummen eine Cauchy-Folge bilden. □

Aus Analysis 1 ist bekannt, dass $\mathbb{R}$ der kleinste Körper ist, der die Limites aller Cauchy-Folgen bzgl. des gewöhnlichen Betrags enthält.

Der Körper der p-adischen Zahlen $\mathbb{Q}_p$ ist der kleinste Körper, der die Limites aller Cauchy-Folgen bzgl. des p-Betrags enthält. Zu zeigen ist natürlich, dass überhaupt ein solcher Körper existiert!!! Aber wir wollen ja der Vorlesung nicht in allen Einzelheiten vorgreifen. Dennoch geben wir hier eine explizite Beschreibung.

$$\mathbb{Q}_p = \{\sum_{n=r}^{\infty} a_n p^n | r \in \mathbb{Z}, a_n \in \{0, 1, \ldots, p-1\}\}.$$

Es ist übrigens nach dem obigen Lemma ganz klar, dass diese Reihen bzgl. $|\cdot|_p$ konvergieren.

Die Multiplikation und die Addition funktionieren so, wie man sie sich denkt, z.B. wie die schriftliche Multiplikation im Zehnersystem, die man in der Grundschule gelernt hat, nur dass es jetzt unendlich viele Stellen gibt und 10 natürlich durch p ersetzt wird. Man kann sich aus dieser expliziten Beschreibung auch überlegen, dass $\mathbb{Q}_p$ ein Körper ist. Dies folgt daraus, dass Potenzreihen der Form $1 + \sum_{n=1}^{\infty} a_n X^n$ mit a_n in einem Ring invertierbar sind. Man schreibt dazu ein potentielles Inverses der Form $1 + \sum_{n=1}^{\infty} b_n X^n$ hin und sieht dann induktiv, dass sich b_n einfach aus den b_m mit $m < n$ berechnet.

Wir definieren die p-Bewertung einer Zahl $x = \sum_{n=r}^{\infty} a_n p^n \in \mathbb{Q}_p^*$ als

$$\mathrm{ord}_p(x) := \min\{n \in \mathbb{Z} | a_n \neq 0\}.$$

Es ist einfach zu sehen, dass für $x \in \mathbb{Q}$ die neue Definition der p-Bewertung mit der alten identisch ist. Dies sollte man sich auf jeden Fall überlegen!

Wir definieren jetzt die ganzen p-adischen Zahlen $\mathbb{Z}_p$ als diejenigen $x \in \mathbb{Q}_p$, die $\mathrm{ord}_p(x) \geq 0$ erfüllen. Mit anderen Worten besteht $\mathbb{Z}_p$ aus den $x = \sum_{n=r}^{\infty} a_n p^n \in \mathbb{Q}_p$ mit $r \geq 0$.

Insbesondere bedeutet dies, dass alle rationalen Zahlen $\frac{r}{s}$ mit $p \nmid s$ in $\mathbb{Z}_p$ liegen. Anders ausgedrückt sind in $\mathbb{Z}_p$ alle Primzahlen $q \neq p$ invertierbar! Daraus kann man leicht schließen, dass $\mathbb{Z}_p$ ein Ring ist, der nur zwei Primideale enthält, nämlich (0) und (p). Denn für jeden Ringhomomorphismus

$$\phi : \mathbb{Z}_p \to R$$

mit einem Integritätsbereich R folgt für die Einschränkung

$$\psi := \phi|_{\mathbb{Z}} : \mathbb{Z} \to R,$$

dass ψ entweder injektiv ist (woraus folgt, dass auch ϕ injektiv ist) oder $\ker(\psi) = (q)$ für eine Primzahl q. Ist $q \neq p$, dann ist aber $\ker(\phi) = \mathbb{Z}_p$, da q in $\mathbb{Z}_p$ invertierbar ist. Wegen $\phi(1) = 1$ haben wir aber einen Widerspruch. Somit enthält $\ker(\phi)$ das Ideal (p). Wegen $\mathbb{Z}_p/(p) \cong \mathbb{F}_p$ (das sieht man sofort an der expliziten Beschreibung von $\mathbb{Z}_p$!) ist aber (p) bereits ein maximales Ideal und es gilt $\ker(\phi) = (p)$. Also enthält $\mathbb{Z}_p$ nur die beiden Primideale (0) und (p). Letzteres heißt auch das *Bewertungsideal von* $\mathbb{Z}_p$.

Nun kommen wir zu dem Körper $\mathbb{Q}_p(\zeta_p)$, der im Beweis benutzt wird. Hierbei ist ζ_p eine Nullstelle des p-ten Kreisteilungspolynoms

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

Fassen wir dieses Polynom in $\mathbb{Z}_p[X]$ auf, so zeigt uns das Eisensteinkriterium, dass der Grad von $\mathbb{Q}_p(\zeta_p)$ über $\mathbb{Q}_p$ gleich $p-1$ ist. Denn

$$\Phi_p(X+1) = \frac{(X+1)^p - 1}{X} = X^{p-1} + \binom{p}{1} X^{p-2} \cdots + \binom{p}{p-1}$$

ist Eisenstein für das einzige Nicht-Null-Primideal (p) von $\mathbb{Z}_p$.

Damit ist auch die Galoisgruppe $\mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)$ gleich $\{\sigma_a | a = 1, \ldots, p-1\}$, wobei auch hier σ_a durch $\zeta_p \mapsto \zeta_p^a$ eindeutig festgelegt ist. Insbesondere berechnet sich die Norm von $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$ ganz genauso wie die Norm von $\mathbb{Q}(\zeta_p)/\mathbb{Q}$, nämlich als das Produkt über die σ_a für $a = 1, \ldots, p-1$.

Wir setzen genauso wie im Text $\pi := \zeta_p - 1$, welches wir nun in $\mathbb{Z}[\zeta_p]$ und in $\mathbb{Z}_p[\zeta_p]$ auffassen können. Mit einem ähnlichen Trick wie für $\mathbb{Z}_p$ kann man zeigen, dass $\mathbb{Z}_p[\zeta_p]$ nur genau zwei Primideale hat, nämlich die Hauptideale (0) und (π).

Wir definieren nun die π-Bewertung für $x \in \mathbb{Q}_p(\zeta_p)$ durch

$$\mathrm{ord}_\pi(x) := \max\{i | \pi^{-i} x \in \mathbb{Z}_p[\zeta_p]\}.$$

Mit dieser Definition ist ganz analog zur Situation oben $\mathbb{Z}_p[\zeta_p]$ die Menge der Elemente von $\mathbb{Q}_p(\zeta_p)$ von nicht-negativer π-Bewertung. Wir erklären nun den π-Betrag für $x \in \mathbb{Q}_p(\zeta_p)$ durch

$$|x|_\pi := p^{-\mathrm{ord}_\pi(x)}.$$

Ganz offenbar ist $|\cdot|_\pi$ ein ultrametrischer Betrag.

Lemma 0.0.4 *Der Körper $\mathbb{Q}_p(\zeta_p)$ ist vollständig, d.h. jede Cauchy-Folge $(a_n)_n$ mit $a_n \in \mathbb{Q}_p(\zeta_p)$ nimmt einen Limes in $\mathbb{Q}_p(\zeta_p)$ an.*

Beweis. Zunächst ist klar $\mathbb{Q}_p(\zeta_p) = \mathbb{Q}_p(\pi)$. Wir schreiben $a_n = \sum_{i=1}^{p-1} b_n^{(i)} \pi^i$ mit $b_n^{(i)} \in \mathbb{Q}_p$ für alle n, i. Wir zeigen nun, dass für festes i die Folgen $(b_n^{(i)})_n$ Cauchy-Folgen in $\mathbb{Q}_p$ bilden und damit ihre Limites in $\mathbb{Q}_p$ annehmen, denn von $\mathbb{Q}_p$ wissen wir ja bereits, dass er vollständig ist. Also sei $\epsilon > 0$ vorgegeben. Es gibt nach Annahme ein N derart, dass für alle $n, m > N$

$$|a_n - a_m|_\pi = |\sum_i (b_n^{(i)} - b_m^{(i)})\pi^i|_\pi < \epsilon.$$

Die π-Bewertung einer Zahl in $\mathbb{Q}_p$ ist ein Vielfaches von $p-1$. Dies zeigt, dass die π-Bewertungen von $(b_n^{(i)} - b_m^{(i)})\pi^i$ für feste n, m für alle $i = 1, \ldots, p-1$ verschieden sein müssen. Daher liefert die strikte Dreiecksungleichung

$$|\sum_i (b_n^{(i)} - b_m^{(i)})\pi^i|_\pi = \max_{i=1,\ldots,p-1} \{p^{-i} |b_n^{(i)} - b_m^{(i)}|_\pi\} < \epsilon.$$

Daher sind die Koordinatenfolgen $(b_n^{(i)})_n$ Cauchy-Folgen, woraus die Behauptung sofort folgt. □

Im Vortrag kann dies alles natürlich nicht vorgeführt werden. Es soll zu einem vorläufigen Verständnis der Vortragenden beitragen. Im Vortrag sollte sich auf das Wesentliche beschränkt werden.

Zu Anfang könnte kurz ein ultrametrischer Betrag eingeführt und die strikte Dreiecksungleichung aufgeschrieben werden. Die Reihenkonvergenz sollte daraus gefolgert werden. $\mathbb{Z}_p$ und $\mathbb{Q}_p$ können z.B. durch die explizite Beschreibung eingeführt werden. Wir können dann glauben, dass $\mathbb{Z}_p$ ein Hauptidealring mit zwei Primidealen ist, dessen Quotientenkörper $\mathbb{Q}_p$ ist. Wegen des Eisensteinkriteriums ist $\mathbb{Q}_p(\zeta_p)$ von Grad $p-1$ über $\mathbb{Q}_p$ mit angegebener Galoisgruppe. Ferner ist $\mathbb{Z}_p[\zeta_p]$ ein Hauptidealring mit zwei Primidealen. Daher kann man den π-Betrag definieren, der ultrametrisch ist. Dann kann man glauben, dass $\mathbb{Q}_p(\zeta_p)$ vollständig für diesen Betrag ist.