Zahlentheorie und Kryptologie, SS2014
M. Hortmann

Blatt 6

Aufgabe 1
Nachträge zu den *p*-adischen Zahlen, also den Ringen $\mathbb{Z}_{(p)}$.
Die Metrik auf ihnen hat ja die Eigenschaft, daß die Dreiecksungleichung verschärft ist zu $d(x,z)\leq\max\{d(x,y),d(y,z)\}$ (ultrametrische Ungleichung).
(*M*,*d*) sei ein ultrametrischer Raum, also ein metrischer Raum, in dem die ultrametrische Ungleichung gilt.

a) Man zeige: Haben zwei offene Kugeln in *M* nicht leeren Schnitt, so ist eine Teilmenge der anderen.

b) Man zeige: *M* ist „total unzusammenhängend“, d.h. besitzt eine Teilmenge $L\subset M$ mindestens zwei Elemente, so gibt es nicht-leere disjunkte offene Teilmengen $U,V\subset M$ mit $L\subset U\cup V$ [1].

Lösung:
Seien $x,y\in L$ gegeben. Sei $r=d(x,y)$. Dann haben nach die offenen Kugeln $U_r(x)$ und $U_r(y)$ leeren Schnitt: Gäbe es nämlich $z\in U_r(x)\cap U_r(y)$, so wäre $d(x,y)\leq\max\{d(x,z),d(z,y)\}<r$
Man überdecke jetzt *L* mit offenen Kugeln des Radius *r*. Man vereinige alle die Kugeln, die weder mit $U_r(x)$ noch mit $U_r(y)$ nicht-leeren Schnitt haben, mit $U_r(x)$ und erhalte so die offene Menge U_1 . Außerdem gibt es in der Überdeckung von *L* noch diejenigen Kugeln, mit $U_r(x)$ nicht leeren Schnitt haben und mit $U_r(y)$ leeren Schnitt. Diese vereinige man mit U_1 und erhält U . Außerdem vereinige man die Kugeln der Überdeckung, die mit $U_r(y)$ nicht-leeren Schnitt haben und mit $U_r(x)$ leeren Schnitt mit $U_r(y)$ und erhält V .

Kugeln in der Überdeckung, die mit $U_r(x)$ und mit $U_r(y)$ nicht leeren Schnitt haben, gibt es nicht: Wären z.B. $U_r(z)\cap U_r(x)\neq\emptyset$ und $U_r(z)\cap U_r(y)\neq\emptyset$, so gäbe es ein $a\in U_r(z)\cap U_r(x)$ und ein $b\in U_r(z)\cap U_r(y)$. Wegen $d(a,z)<r$ und $d(b,z)<r$ ist $d(a,b)\leq\max\{d(a,z),d(b,z)\}<r$.
Dann hätte man aber auch $d(x,y)\leq\max\{d(x,a),d(a,b),d(b,y)\}<r$

Nach Konstruktion sind sind *U*,*V* nicht leer, besitzen leeren Schnitt und überdecken zusammen *L*.

c) Man zeige: Die Menge der Abstände von einem Punkt *a* zu von *a* verschiedenen Punkten in einem kompakten ultrametrischen Raum ist eine diskrete Teilmenge[2] reeller Zahlen.d.h. jede Folge hat einen Häufungspunkt bzw. jede Folge hat eine konvergente Teilfolge.

Lösung:
Mit Überdeckungen will man hier und in Aufgabe d) nicht arbeiten. Man benutzt, daß in einem kompakten metrischen Raum jede Folge einen Häufungspunkt, bzw. jede Folge eine konvergente Teilfolge besitzt.

Sei nun also $d(x_n,a)$ eine Folge reeller Zahlen mit einem Häufungspunkt *r*>0 und keine der Zahlen

---

1 d.h. nur höchstens einelementige Teilmengen sind zusammenhängend. Die rationalen Zahlen und die irrationalen Zahlen sind als metrischer Raum total unzusammenhängend, ebenfalls die Cantormenge, die sogar im Gegensatz zu im Gegensatz zu den vorigen Beispielen kompakt ist.
2 d.h. jeder Punkt besitzt eine offene Umgebung, die keinen weiteren Punkt der Menge enthält

$d(x_n, a)$ sei gleich *r*. Dann gibt es eine Teilfolge, die *r* als Grenzwert besitzt. Die x_n , die in dieser Teilfolge vorkommen, besitzen einen Häufungspunkt in M, also kann man eine weitere Teilfolge auswählen, so daß die x_n konvergieren. Ab jetzt betrachten wir ausschließlich diese letztere Folge, für die gilt:
Die Abstände $d(x_n, a)$ besitzen den Grenzwert *r*, keine der Zahlen $d(x_n, a)$ ist gleich r, und die x_n konvergieren in M mit Grenzwert *x*.
Jetzt folgt wegen der Stetigkeit der Metrik, daß $d(x, a) = d(\lim x_n, a) = \lim d(x_n, a) = r$.
Auch folgt, daß es einen Folgenindex *n* gibt, für den $d(x_n, x) < r$ gilt.

Jetzt kommen die Ultrametrik-Argumente:
Es ist $d(a, x_n) \leq \max\{d(a, x), d(x_n, x)\} = \max\{r, d(x_n, x)\}$
Wegen $d(x_n, x) < r$ und $d(a, x_n) \neq r$ muß also $d(a, x_n) < r$ sein.

Andererseits haben wir dann auch $d(a, x) \leq \max\{d(a, x_n), d(x_n, x)\} < r$: Widerspruch! Also gab es keine Folge (x_n) , so daß $d(x_n, a)$ einen Häufungspunkt besitzt!

d) Man beweise oder widerlege: $\mathbb{Z}_{(p)}$ ist kompakt.

Gezeigt wird die Folgenkompaktheit. Dies ist in einem metrischen Raum mit abzählbarer Umgebungsbasis äquivalent zur Kompaktheit. $\mathbb{Z}_{(p)}$ ist ein solcher Raum.
Im Gegensatz zu c) ist die Metrik durch den Betrag in $\mathbb{Z}_{(p)}$ gegeben, für den ebenfalls eine „Ultra"-Ungleichung gilt: $|x + y| \leq \max\{|x|, |y|\}$.
Man erinnere sich, daß $|0| := 0$ und für ein von 0 verschiedenes Element $\left|\sum_{i=0}^{\infty} a_i p^i\right| = p^{-n}$ definiert wird, wobei $n = \max\left\{m \in \mathbb{N}_0 \middle| \forall i \leq m : a_i = 0\right\}$.
Bei einem normalen Betrag beweist man über die Dreiecksungleichung $||x| - |y|| \leq |x - y|$. Für einen „Ultra"-Betrag zeigt man entsprechend $\min\{|x|, |y|\} \leq |x - y|$. Das brauchen wir aber im Folgenden nicht.

Sei (x_n) eine Folge in $\mathbb{Z}_{(p)}$.

Wir konstruieren rekursiv eine konvergente Teilfolge.
Induktionsanfang
Wähle $a_0 \in \mathbb{Z}_p$, so daß unendlich viele Folgenglieder ihre p-adische Entwicklung mit a_0 beginnen und setze $M_0 := \left\{n \in \mathbb{N} \middle| \text{die p-adische Entwicklung von } x_n \text{ beginnt mit } a_0\right\}$; die Menge M_0 ist also unendlich.

Seien $a_0 \ldots a_i \in \mathbb{Z}_p$ und die Mengen $M_0 \ldots M_k$ bereits gewählt, wobei die $M_i := \left\{n \in \mathbb{N} \middle| \text{die p-adische Entwicklung von } x_n \text{ beginnt mit } a_0 \ldots a_i\right\}$ unendliche Mengen sind mit $M_{i+1} \subset M_i$.
Wieder können wir $a_{k+1} \in \mathbb{Z}_p$ wählen, so daß für unendlich viele Folgenglieder mit Indizes in M_k die Menge derjenigen, deren p-adische Entwicklung mit $a_0 \ldots a_{k+1}$ beginnt, unendlich ist, so daß auch $M_{k+1} := \left\{n \in \mathbb{N} \middle| \text{die p-adische Entwicklung von } x_n \text{ beginnt mit } a_0 \ldots a_{k+1}\right\}$ eine unendliche Menge ist.

Man wähle jetzt für jedes $m \in \mathbb{N}$ ein $n_m \in M_m$ so, daß die Folge (n_m) monoton steigt.

Nach Konstruktion ist die Folge (x_{n_m}) konvergent! Wir haben also eine konvergente Teilfolge der Ausgangsfolge erhalten.