Sommersemester 2007

Seminar: Quadratische Formen über den rationalen Zahlen

Von: Zeng,Yuefei und Andreas Rieth

Am: 10.05.07

Hilfsmittel:

H1: 1. Isomorphiesatz: Sei $\varphi : X \to Y$ ein surjektiver Homomorpismus .

Dann induziert φ einen Isomorphismus $\varphi' : X / Kern(\varphi) \cong Y$.

H2: 2. Isomorphiesatz: Sei X , Y Untergruppen von Z , dann gilt:
$(X+Y)/Y \cong X/(X \cap Y)$

H3: Proposition auf Seite 12

H4: Ist B eine Untergruppe der abelschen Gruppe A mit endlichem Index [A:B], dann gilt für jede B umfassende Untergruppe U von A, also mit $B \subset U \subset A$, die Gleichung $[A:B]=[A:U] \cdot [U:B]$.

§ 3. Die multiplikative Gruppe $\mathbb{Q}_p^*$

3.1: Filtration der Einheitengruppe U

Sei $U= \mathbb{Z}_p^*$ die p-adische Einheitengruppe

Satz 1: $U/ U_n \cong (\mathbb{Z} / p^n \mathbb{Z})^*$,wobei $U_n := 1+ p^n \mathbb{Z}_p$, $n \geq 1$.

Beweis: Der Homomorphismus $\epsilon_n : U \to (\mathbb{Z} / p^n \mathbb{Z})^*, u \mapsto u \bmod (\mathbb{Z} / p^n \mathbb{Z})^*$

ist offenbar surjektiv, und den Kern findet man durch:

$u_n \bmod p^n = (1+ p^n x) \bmod p^n = 1$.

Also ist U_n der Kern von ϵ_n. Und die Behauptung folgt aus H1. □

Korollar 1: $U/ U_1 \cong F_p^*$

Beweis:Da U_1 der Kern von $\epsilon_1 : U \to (\mathbb{Z}/p\mathbb{Z})^* = F_p^*$ ist, folgt die

Behauptung aus H1. Insbesondere hat U/ U_1 die Ordnung p-1. □

Korollar 2: U $\cong \varprojlim$ U/ U_n

Beweis: U= $\mathbb{Z}_p^* \cong (\varprojlim \mathbb{Z}/p^n\mathbb{Z})^* \cong \varprojlim (\mathbb{Z}/p^n\mathbb{Z})^* \cong \varprojlim$ U/ U_n □

Satz 2: φ : $U_n / U_{n+1} \to \mathbb{Z}/p\mathbb{Z}$, $(1+p^n x) \bmod p^{n+1} \mapsto x \bmod p$ ist

ein Isomorphismus. Insbesondere gilt $\#(U_n / U_{n+1}) = p$.

Beweis: Dass φ ein Homomorphismus ist, folgt aus

$(1+p^n x)(1+p^n y) \equiv 1+p^n(x+y) \pmod{p^{n+1}}$

Und nun ist es genug zu zeigen, U_{n+1} =Kern($U_n \to \mathbb{Z}/p\mathbb{Z}$), dann folgt

die Behauptung aus H1 :

Also $u=1+p^n x \mapsto 0 \Leftrightarrow x \equiv 0 \bmod p \Leftrightarrow u=1+p^{n+1} x'$,wobei $x=p x'$

$\Leftrightarrow u \in U_{n+1}$ □

Korollar 3: Ord(U_1 / U_n) = p^{n-1}

Beweis: Es gilt offenbar $U_1 \supset U_2 \supset U_3 \supset \cdots$

Wende H4 an : Ord(U_1 / U_n) =[$U_1 : U_n$]=[$U_1 : U_2$]·[$U_2 : U_n$]= $\cdots$

$= [U_1 : U_2] \cdot [U_2 : U_3] \cdot \ldots \cdot [U_{n-1} : U_n] = p^{n-1}$ □

Lemma 1: Sei $0 \longrightarrow A \xrightarrow{\beta} E \xrightarrow{\alpha} B \longrightarrow 0$ eine exakte Sequenz von kommuti-

ven Gruppen (bzgl. Addtion). Ord(A)=a , Ord(B)=b, a,b<∞ sind

teilerfremd . Sei $B' := \{ x \in E \mid bx=0 \}$. Dann ist $E=A \oplus B'$, und B' ist

die einzige Untergruppe von E, die isomorph zu B ist.

Beweis: a , b teilerfremd $\Rightarrow$ ar+bs=1 . Da die Sequenz exakt ist , ist β injektiv, α surjektiv . Nehme für β Einbettung, α Projektion, dann haben wir $\beta(A) \cong A$; $\alpha(E)=B$. Für ein beliebiges $x \in \beta(A) \cap B'$ gilt ax=0

und bx=0 $\Rightarrow x=1 \cdot x=(ar+bs)x=rax+sbx=0 \Rightarrow \beta(A) \cap B'=0$.

Wegen Exaktheit gilt $\beta(A)=\mathrm{Kern}(\alpha)$. $\forall x\in E$: $\alpha(bsx)=sb\alpha(x)=0$, also $bsx\in\beta(A)$ und $arxb=rabx=0$, also $arx\in B'$. $\Rightarrow E=\beta(A)\oplus B'=A\oplus B'$.

$B\cong B'$ folgt aus $B\cong E/\mathrm{Kern}(\alpha)=\beta(A)\oplus B'/\beta(A)\cong B'/0=B'$.

Eindeutigkeit von B': Sei B'' eine weitere Untergruppe mit $B''\cong B$

Da B von der Ordnung b ist , ist B''auch. Daraus folgt $\forall$ $x\in B''$,

$bx=0 \Rightarrow B''\subset B'$. Da B' auch von der Ordnung b ist, gilt $B'=B''$ □

Propositon 1: Es gilt $U = V \times U_1$, wobei $V = \{x\in U \mid x^{p-1}=1\}$ die eindeutige Untergruppe von U , die ismorph zu F_p^* ist. (Man nennt V die Gruppe der multiplikative Repräsentaten der Elmente aus F_p^*)

Beweis: Da Ord(U) und Ord(U_1) unendlich sind , können wir Lemma 1 nicht direkt anwenden. Aber man kann Lemma 1 auf Sequenz

$1 \longrightarrow U_1 / U_n \xrightarrow{\beta} U / U_n \xrightarrow{\alpha} F_p^* \longrightarrow 1$ anwenden , da Ord(U_1 / U_n)= p^{n-1} ,

Ord(F_p^*)=p-1 sind. Und p^{n-1}, p-1 sind offenbar teilerfremd.

Wir müssen nun nur die Exaktheit untersuchen: Wegen Proposition 2 auf Seite 12 erhalten wir: $\sum_{i=0}^{\infty} a_i\, p^i = x\in U \Leftrightarrow$ x ist nicht durch p teilbar

$\Leftrightarrow$ $a_0 \neq 0$. Denn $U_1=\{ 1+px \mid x\in \mathbb{Z}_p\}$, also gilt: $\forall$ $u\in U_1$, $a_0 \neq 0$.

$\Rightarrow U_1 \subset U \Rightarrow$ $U_1 \xrightarrow{Einbettung}$ U ist wohldefiniert

$\Rightarrow U_1 / U_n \xrightarrow{Einbettung}$ U/ U_n ist wohldefiniert , also $U_1 / U_n \cong$ Bild(β)

Andererseits: $U= \{ x= \sum_{i=0}^{\infty} a_i\, p^i \mid a_0 \neq 0 \}$

Definiere $\Gamma : U \longrightarrow F_p^*=\{ \bar{1}, \bar{2}, \ldots, \overline{p-1} \}$, $x\mapsto a_0 \bmod p$

Offenbar gilt : Kern(Γ)=$\{ x= \sum_{i=0}^{\infty} a_i p^i \mid a_0 = 1 \} = \{ x= 1+ \sum_{i=0}^{\infty} a_{i+1} p^i \}$

Also Kern(Γ) = U_1 $\Rightarrow$ Kern($\alpha: U/U_n \longrightarrow F_p^*$) = U_1 / U_n $\Rightarrow$

Bild(β)$\cong$Kern(α) . Damit ist die Exaktheit bewiesen.

Nach Lemma 1 enthält U/U_n eine eindeutige Untergruppe V_n, die isomorph zu F_p^* ist, wobei $V_n := \{x \in U/U_n \mid x^{p-1}=1\}$. Und die Projektion $U/U_n \longrightarrow U/U_{n-1}$ bildet V_n ismorph nach V_{n-1} ab, wobei man

$V_{n-1} := \{x \in U/U_{n-1} \mid x^{p-1}=1\}$ definiert.

$U = \varprojlim U/U_n$ $\Rightarrow$ $V = \varprojlim V_n$; $V_n \cong F_p^*$ $\Rightarrow$ $V \cong F_p^*$. Mit $U_1 = \varprojlim U_1/U_n$ folgt $U = V \times U_1$. Und die Eindeutigkeit von V folgt aus der von V_n.

□

Korollar 4: $\mathbb{Q}_p$ enthält die (p-1)te Einheitswurzeln.

Beweis: Die Behauptung folgt mit Proposition 1 aus $U = \mathbb{Z}_p^* \subset \mathbb{Q}_p^* \subset \mathbb{Q}_p$

□

3.2 Struktur von U_1

Lemma 2: Sei $x \in U_n - U_{n+1}$ mit $n \geq 1$, falls $p \neq 2$; und $n \geq 2$, falls $p=2$.

Dann gilt $x^p \in U_{n+1} - U_{n+2}$.

Beweis: OEdA :$x \in U_n - U_{n+1}$, $x = 1 + k p^n$, wobei k nicht durch p teilbar ist.

$\Rightarrow$ $x^p = (1+k p^n)^p = \sum_{i=0}^{p} \binom{p}{i} (k p^n)^i = 1 + k p^{n+1} + \ldots + k^p p^{np}$

Weiter gilt $np \geq n+2$ (da $n \geq 2$, falls $p=2$) $\Rightarrow$ $x^p \equiv 1 + k p^{n+1} \pmod{p^{n+2}}$

$\Rightarrow$ $x^p \in U_{n+1} - U_{n+2}$.

□