0.1 Proposition 3

Für $p \neq 2$ ist $\mathbb{U}_1$ isomorph zu $\mathbb{Z}_p$. Für $p = 2$ gilt: $\mathbb{U}_1 = \{\pm 1\} \times \mathbb{U}_2$ und $\mathbb{U}_2$ ist isomorph zu $\mathbb{Z}_2$.
Beweis: Betrachte den ersten Fall $p \neq 2$. Wähle ein Element $\alpha \in \mathbb{U}_1 - \mathbb{U}_2$, zum Beispiel $\alpha = 1 + p$. Nach Lemma 2 haben wir $\alpha^{p^i} \in \mathbb{U}_{t+1} - \mathbb{U}_{t+2}$. Sei α_n das Bild von α in $\mathbb{U}_1/\mathbb{U}_n$; es gilt $(\alpha_n)^{p^{n-2}} \neq 1$ und $(\alpha_n)^{p^{n-1}} = 1$. $\mathbb{U}_1/\mathbb{U}_n$ ist aber von der Ordnung p^{n-1}; folglich ist es eine zyklische Gruppe, erzeugt von α_n. Wir bezeichnen nun mit $\theta_{n,\alpha}$ den Isomorphismus $z \mapsto \alpha_n^z$ von $\mathbb{Z}/p^{n-1}\mathbb{Z}$ nach $\mathbb{U}_1/\mathbb{U}_n$. Das Diagramm

$$\begin{array}{ccc} \mathbb{Z}/p^n\mathbb{Z} & \xrightarrow{\theta_{n+1,\alpha}} & \mathbb{U}_1/\mathbb{U}_{n+1} \\ \downarrow & & \downarrow \\ \mathbb{Z}/p^{n-1}\mathbb{Z} & \xrightarrow{\theta_{n,\alpha}} & \mathbb{U}_1/\mathbb{U}_n \end{array}$$

ist kommutativ. Man erkennt daraus, dass die $\theta_{n,\alpha}$ einen Isomorphismus θ von $\mathbb{Z}_p = \lim_{\leftarrow} \mathbb{Z}/p^{n-1}\mathbb{Z}$ nach $\mathbb{U}_1 = \lim_{\leftarrow} \mathbb{U}_1/\mathbb{U}_n$ definieren, daher gilt die Proposition für $p \neq 2$.
Sei nun $p = 2$. Wähle $\alpha \in \mathbb{U}_2 - \mathbb{U}_3$, das bedeutet $\alpha \equiv 5 \pmod 8$. Definiere wie oben Isomorphismen $\theta_{n,\alpha} : \mathbb{Z}/2^{n-2}\mathbb{Z} \to \mathbb{U}_2/\mathbb{U}_n$ und einen Isomorphismus $\theta_\alpha : \mathbb{Z}_2 \to \mathbb{U}_2$. Andererseits induziert der Homomorphismus $\mathbb{U}_1 \to \mathbb{U}_1/\mathbb{U}_2 \simeq \mathbb{Z}/2\mathbb{Z}$ einen Isomorphismus von $\{\pm 1\}$ auf $\mathbb{Z}/2\mathbb{Z}$. Daraus erhalten wir $\mathbb{U}_1 = \{\pm 1\} \times \mathbb{U}_2$. □

0.2 Theorem

Die Gruppe $\mathbb{Q}_p^*$ ist isomorph zu $\mathbb{Z} \times \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$, falls $p \neq 2$, und zu $\mathbb{Z} \times \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$, falls $p = 2$.
Beweis: Jedes Element $x \in \mathbb{Q}_p^*$ kann man eindeutig in der Form $x = p^n u$ schreiben mit $n \in \mathbb{Z}$ und $u \in \mathbb{U}$. Daher gilt: $\mathbb{Q}_p^* \simeq \mathbb{Z} \times \mathbb{U}$. Weiterhin zeigt Proposition 1, dass $\mathbb{U} = \mathbb{V} \times \mathbb{U}_1$, wobei $\mathbb{V}$ zyklisch von der Ordnung $p-1$ ist. Die Struktur von $\mathbb{U}_1$ ist gegeben durch Proposition 3.

1 Quadrate in $\mathbb{Q}_p^*$

1.1 Theorem

Sei $p \neq 2$ und sei $x = p^n u$ ein Element von $\mathbb{Q}_p^*$ mit $n \in \mathbb{Z}$ und $u \in \mathbb{U}$. Damit x ein Quadrat ist, ist es hinreichend und notwendig, dass n gerade ist und das Bild $\overline{u}$ von u in $\mathbb{F}_p^* = \mathbb{U}/\mathbb{U}_1$ ein Quadrat ist. Die letzte Bedingung bedeutet,

dass das *Legendresymbol* $\left(\frac{\overline{u}}{p}\right)$ von $\overline{u}$ gleich 1 ist.
Beweis: Zerlege u in der Form $u = v.u_1$ mit $v \in \mathbb{V}$ und $u_1 \in \mathbb{U}_1$. Die Zerlegung $\mathbb{Q}_p^* \simeq \mathbb{Z} \times \mathbb{V} \times \mathbb{U}_1$ in 0.2 (Theorem) zeigt, dass x genau dann ein Quadrat ist, wenn n gerade ist und v und u_1 Quadrate sind. Aber die multiplikative Gruppe $\mathbb{U}_1$ ist isomorph zur additiven Gruppe $\mathbb{Z}_p$ und 2 ist multiplikativ invertierbar in $\mathbb{Z}_p$. Alle Elemente von $\mathbb{U}_1$ sind damit Quadrate. Weil $\mathbb{V}$ isomorph zu $\mathbb{F}_p^*$ ist, folgt die Behauptung.

1.2 Korollar

Für $p \neq 2$ ist die Gruppe $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ eine Gruppe vom Typ $(2,2)$, also isomorph zu $(\mathbb{Z}/2\mathbb{Z})^2$. Sie hat $\{1, p, u, up\}$ als Repräsentanten, wobei $u \in \mathbb{U}$ so gewählt ist, dass $\left(\frac{u}{p}\right) = -1$.
Beweis ist klar.

1.3 Theorem

Ein Element $x = 2^n u$ von $\mathbb{Q}_2^*$ ist genau dann ein Quadrat, wenn n gerade ist und $u \equiv 1(\mod 8)$.
Beweis: Die Zerlegung $\mathbb{U} = \{\pm 1\} \times \mathbb{U}_2$ zeigt, dass u dann und nur dann ein Quadrat ist, wenn u zu $\mathbb{U}_2$ gehört und in $\mathbb{U}_2$ ein Quadrat ist. Der Isomorphismus $\theta : \mathbb{Z}_2 \to \mathbb{U}_2$, den wir schon im Beweis zu 0.1 (Theorem) konstruiert haben, bildet $2^n\mathbb{Z}_2$ auf $\mathbb{U}_{n+2}$ ab. Wenn wir $n = 1$ wählen, sehen wir, dass die Menge der Quadrate in $\mathbb{U}_2$ gleich $\mathbb{U}_3$ ist. Ein Element $u \in \mathbb{U}$ ist genau dann ein Quadrat, wenn es kongruent zu 1 modulo 8 ist, daraus folgt das Theorem.

1.4 Korollar

Die Gruppe $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$ ist vom Typ $(2,2,2)$, also isomorph zu $(\mathbb{Z}/2\mathbb{Z})^3$. Sie hat $\{\pm 1, \pm 5, \pm 2, \pm 10\}$ als Repräsentanten.
Beweis: Das folgt aus der Tatsache, dass $\{\pm 1, \pm 5\}$ ein Repräsentantensystem für $\mathbb{U}/\mathbb{U}_3$ ist.

Bemerkungen:

1. Für $p = 2$ definiere Homomorphismen $\varepsilon, \omega : \mathbb{U}/\mathbb{U}_3 \to \mathbb{Z}/2\mathbb{Z}$ mit Hilfe

der Formeln von Kapitel I, Nummer 3.2:

$$\varepsilon(z) \equiv \frac{z-1}{2} (\mod 2) = \begin{cases} 0, \text{ falls } z \equiv +1 (\mod 4) \\ 1, \text{ falls } z \equiv -1 (\mod 4) \end{cases}.$$

$$\omega(z) \equiv \frac{z^2-1}{8} (\mod 2) = \begin{cases} 0, \text{ falls } z \equiv \pm 1 (\mod 8) \\ 1, \text{ falls } z \equiv \pm 5 (\mod 8) \end{cases}.$$

ε definiert einen Isomorphismus von $\mathbb{U}/\mathbb{U}_2$ auf $\mathbb{Z}/2\mathbb{Z}$ und ω einen Isomorphismus von $\mathbb{U}_2/\mathbb{U}_3$ auf $\mathbb{Z}/2\mathbb{Z}$. Das Paar (ε, ω) definiert damit einen Isomorphismus von $\mathbb{U}/\mathbb{U}_3$ auf $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Im Besonderen ist eine 2-adische Einheit z genau dann ein Quadrat, wenn $\varepsilon(z) = \omega(z) = 0$.

2. Die Theoreme 1.1 und 1.3 zeigen, dass $\mathbb{Q}_p^{*2}$ eine offene Untergruppe von $\mathbb{Q}_p^*$ ist.