15. Charaktere

Der Weil'sche Beweis für $\tau(G) = 2$ benötigt Fouriertransformation auf der additiven Gruppe V_A. Zur Vorbereitung davon dienen die Kapitel 15 und 16.

Definition : Ein Charakter einer abelschen topologischen Gruppe G ist eine stetiger Homomorphismus von G in die Gruppe der komplexen Zahlen vom Betrag 1.

In diesem Kapitel wollen wir die Charaktere von $\mathbb{Q}_p$, A und V_A bestimmen.

$\mathbb{Q}_p$ Sei χ ein stetiger Homomorphismus von $\mathbb{Q}_p$ nach $\{|z| = 1\}$. Zu $\epsilon > 0$ existiert m mit $|\chi(x) - 1| < \epsilon$ für $x \equiv 0 \bmod p^m$. Das Bild $\chi(p^m \mathfrak{o}_p)$ ist eine Untergruppe in $\{|z| = 1\}$. Wählt man ϵ so klein, daß $\{|z - 1| < \epsilon\}$ keine Untergruppe $\neq 1$ von $\{|z| = 1\}$ enthält, so muß $\chi(p^m \mathfrak{o}_p) = 1$ sein.
Wir bestimmen zuerst alle Charaktere mit $\chi(\mathfrak{o}_p) = 1$: Sei χ ein solcher. Dann ist $\chi(\frac{1}{p^n})$ eine p^n-te Einheitswurzel, etwa

$$\chi(\frac{1}{p^n}) = e^{\frac{2\pi i}{p^n} \cdot a_n} \text{ mit } 0 \leq a_n < p^n$$

Aus

$$e^{\frac{2\pi i}{p^{n-1}} a_{n-1}} = \chi(\frac{1}{p^{n-1}}) = \chi(p \cdot \frac{1}{p^n}) = \chi(\frac{1}{p^n})^p = e^{\frac{2\pi i}{p^n} a_n p}$$

folgt

$$a_n \equiv a_{n-1} \bmod p^{n-1}$$

Daraus und aus $0 \leq a_n < p^n$ folgt, daß die Ziffern $\in \{0, 1, ..., p-1\}$ in der p-adischen Entwicklung von a_n und a_{n-1} bis zur Stelle $n-2$ übereinstimmen. Es gibt also eine ganze p-adische Zahl $c = \sum_{i=0}^{\infty} c_i p^i$ mit

$$a_n \equiv c \bmod p^n \text{ für alle } n$$

Ist $x \in \mathbb{Q}_p$ beliebig, etwa

$$x = \frac{x_{-m}}{p^m} + ... + \frac{x_{-1}}{p} + x^0 \text{ mit } x^0 \in \mathfrak{o}_p \text{ und } 0 \leq x_i < p$$

so ist, weil $\chi(\mathfrak{o}_p) = 1$,

$$\chi(x) = \chi(\sum_{j=1}^{m} \frac{x_{-j}}{p^j}) = \prod_{j=1}^{m} \chi(\frac{1}{p^j})^{x_{-j}} = \prod_{j=1}^{m} e^{\frac{2\pi i}{p^j} a_j x_{-j}} =$$

$$e^{2\pi i \sum_{j=1}^{m} \sum_{k=0}^{j-1} c_k p^k x_{-j} p^{-j}}$$

Die Summe im Exponenten läuft über alle Paare (k, j) mit $k - j < 0$. Sie ist der sogenannte p-adische Hauptteil $h_p(cx)$ von cx. Dieser ist für $y \in \mathbb{Q}_p$ nach Definition modulo $\mathbb{Z}$ gekennzeichnet durch

1. $h_p(y)$ ist eine rationale Zahl mit p-Potenznenner
2. $y - h_p(y) \in \mathfrak{o}_p$.

Wir sehen: Zu jedem Charakter χ von $\mathbb{Q}_p$ mit $\chi(\mathfrak{o}_p) = 1$ gibt es eine Zahl $c \in \mathfrak{o}_p$ mit

$$\chi(x) = e^{2\pi i h_p(cx)} \text{ für alle } x \in \mathbb{Q}_p$$

Für einen beliebigen Charakter χ von $\mathbb{Q}_p$ gibt es m mit $\chi(p^m \mathfrak{o}_p) = 1$. Der Charakter $\psi(x) := \chi(p^m x)$ ist gleich 1 auf $\mathfrak{o}_p$, also von der Gestalt $e^{2\pi i h_p(cx)}$, und damit ist $\chi(x) = e^{2\pi i h_p(p^{-m}cx)}$.

Die Abbildung $c \mapsto \chi_c$ mit $\chi_c(x) = e^{2\pi i h_p(cx)}$ von $\mathbb{Q}_p$ in seine Charaktergruppe $\hat{\mathbb{Q}}_p$ ist also surjektiv. Sie ist offensichtlich ein Homomorphismus, und injektiv ($h_p(cx) \in \mathbb{Z}$ für alle x ist nur möglich für $c = 0$). Sie ist zudem stetig und offen: Die Charaktergruppe wird nach Definition dadurch toplogisiert, daß die Mengen

$$W_{C,\epsilon} := \{\chi \mid \chi(C) \subset U_\epsilon(1)\}$$

wobei C die Kompakta $\ni 0$ und ϵ die positiven reellen Zahlen durchläuft und $U_\epsilon(1) = \{z \mid |z-1| < \epsilon\}$, ein Fundamentalsystem von offenen Einsumgebungen bilden. Nun:

$$\chi_c \; m\text{- nahe } 1 \text{ in } \hat{\mathbb{Q}}_p \Leftrightarrow \chi(cp^{-m}\mathfrak{o}_p) \text{ nahe } 1 \Leftrightarrow h_p(cp^{-m}\mathfrak{o}_p) \subset \mathbb{Z} \Leftrightarrow c \equiv 0 \bmod p^m$$

Ergebnis:

Satz 17. $\hat{\mathbb{Q}}_p \simeq \mathbb{Q}_p$ *als topologische Gruppe.*

$\mathbb{R}$ Dies entnehmen wir aus der Analysis: $c \mapsto \chi_c(x) := e^{-2\pi i c x}$ identifiziert $\mathbb{R}$ (algebraisch und topologisch) mit seiner Charaktergruppe.

A Sei $\chi \in \hat{A}$. Die Kompakta in A sind enthalten in Mengen der Gestalt

$$C = C_\infty \times \prod_p p^{-m_p}\mathfrak{o}_p, \text{ fast alle } m_p = 0$$

Mit demselben Schluß wie oben ($\{|z| = 1\}$ enthält keine kleinen Untergruppen) sehen wir: es gibt eine endliche Menge S und m_p für $p \in S$, so daß

$$\chi(\{0\} \times \prod_{p \in S} p^{-m_p}\mathfrak{o}_p \times \prod_{p \notin S} \mathfrak{o}_p) = 1$$

Für jede Stelle v sei i_v die Einbettung $x \mapsto (0,, ..., 0, x, 0, ...)$ von $\mathbb{Q}_v$ in A . Dann ist $\chi_v := \chi \circ i_v$ ein Charakter von $\mathbb{Q}_v$. Dazu gibt es c_∞ mit $\chi_\infty(x) = e^{-2\pi i c_\infty x}$ und c_p mit $\chi_p(x) = e^{2\pi i h_p(c_p x)}$.
Für $x \in A$ ist $x_p \in \mathfrak{o}_p$ für fast alle p , etwa für $p \notin T$. Wir schreiben

$$x = (x_\infty, ..., x_p, 0, ...) + (0, ..., 0, x_q, ...) = \sum_{v \in S \cup T} i_v(x_v) + (0, ..., 0, x_q, ...)$$

Nach Bestimmung von S ist

$$\chi(x) = \prod_{v \in S \cup T} \chi_v(x_v)$$

Da $\chi_p(x_p) = 1$ für $p \notin S \cup T$, kann man die $\chi_p(x_p)$ formal dem Produkt hinzufügen und schreiben

$$\chi(x) = \prod_v \chi_v(x_v) = e^{-2\pi i c_\infty x_\infty + 2\pi i \sum_p h_p(c_p x_p)} \tag{1}$$

Aus $\chi_p(\mathfrak{o}_p) = 1$ für $p \notin S$ folgt $c_p \in \mathfrak{o}_p$ für $p \notin S$. Also ist $c := (c_\infty, ..., c_p, ...)$ ein Adel. Die Abbildung $c \mapsto \chi_c$ von A nach $\hat{A}$, wo χ_c durch die rechte Seite von (1) definiert ist, ist bijektiv. Sie ist auch stetig und offen:

$$\chi_c \text{ nahe } 1 \text{ in } \hat{A} \Longleftrightarrow$$

mit großem C_0 und großem S und großen m_p ist

$$e^{-2\pi i c_\infty x_\infty + 2\pi i \sum_p c_p x_p} \text{ nahe } 1 \text{ in } \mathbb{C} \text{ für } x \in C_\infty \times \prod_{p \in S} p^{-m_p}\mathfrak{o}_p \times \prod_{p \notin S} \mathfrak{o}_p$$

$$\Longleftrightarrow c_\infty \text{ nahe } 0, c_p \equiv 0 \bmod p^{m_p} \text{ für } p \in S, c_p \in \mathfrak{o}_p \text{ für } p \notin S$$

$$\Longleftrightarrow c \text{ nahe } 0 \text{ in } A$$

Ergebnis:

Satz 18. $\hat{A} \simeq A$ *algebraisch und topologisch* .

Ab jetzt bezeichnen wir $\chi_c(x) =< x, c >$.

Lemma 1. *Für* $\xi \in \mathbb{Q}$ *ist* $\xi \equiv \sum_p h_p(\xi) \bmod \mathbb{Z}$.

Beweis: $\xi - \sum_p h_p(\xi) = [\xi - h_q(\xi)] - \sum_{p \neq q} h_p(\xi)$ ist ganz für q. Dies gilt für jedes q. Also ist $\xi - \sum_p h_p(\xi) \in \mathbb{Z}$.

Für eine Untergruppe $B \subset A$ bezeichne

$$B^\perp = \{x \in A \mid < x, b >= 1 \text{ für alle } b \in B\}$$

Aus Lemma 1 folgt $\mathbb{Q} \subset \mathbb{Q}^\perp$

Mit $C = [0, 1] \times \prod_p \mathfrak{o}_p$ war $A = C + \mathbb{Q}$.

$$W_{C,\epsilon} = \{\chi \in \hat{A} \mid \chi(C) \subset U_\epsilon(1)\}$$

ist offen in $\hat{A}$, und

$$\chi \in W_{C,\epsilon} \cap \mathbb{Q}^\perp \Rightarrow \chi(A) = \chi(C) \subset U_\epsilon(1), \text{ also } = 1 \quad (\epsilon \text{ klein})$$

weil $\chi(A)$ eine Untergruppe von $\{|z| = 1\}$ ist. Das zeigt: $\mathbb{Q}^\perp$ ist diskret in A. Dann ist auch $\mathbb{Q}^\perp/\mathbb{Q}$ diskret in $A/\mathbb{Q}$. Da $A/\mathbb{Q}$ kompakt, ist $\mathbb{Q}^\perp/\mathbb{Q}$ endlich. Anderseits ist $\mathbb{Q}^\perp$ offenbar ein $\mathbb{Q}$-Vektorraum. Dies zusammen ist nur möglich, wenn

$$\mathbb{Q} = \mathbb{Q}^\perp$$

V_A Man nimmt eine über $\mathbb{Q}$ definierte nicht ausgeartete symmetrische Bilinearform $(\ ,\ )$ und identifiziert V_A mit seiner Charaktergruppe vermöge $y \mapsto \chi_y$ mit

$$\chi_y(x) = \chi((x, y))$$

wobei

$$\chi(a) = e^{-2\pi i a_\infty + 2\pi i \sum_p h_p(a_p)}$$

der oben betrachtete Charakter von A ist. Dabei ist wieder

$$V_{\mathbb{Q}}^{\perp} = V_{\mathbb{Q}}$$

denn

$$\chi_y(V_{\mathbb{Q}}) = 1 \Leftrightarrow \chi((y, V_{\mathbb{Q}})) = 1 \Leftrightarrow \chi(\mathbb{Q} \cdot (y, V_{\mathbb{Q}})) = 1 \Leftrightarrow (y, V_{\mathbb{Q}}) \subset \mathbb{Q} \Leftrightarrow y \in V_{\mathbb{Q}}$$

Spezialfall: $V = D$ eine Quaternionenalgebra. Hier nimmt man die symmetrische Bilinearform $(x, y) = sp\,(xy)$, wobei sp die reduzierte Spur von D ist. Wenn $e_0, ..., e_3$ eine Basis von D ist mit $e_0 = 1, e_1^2 = a,\ e_2^2 = b$ und $e_1 e_2 = -e_2 e_1$, $a, b \in \mathbb{Q}^*$, und $x = x_0 + x_1 e_1 + x_2 e_2 + x_3 e_3$, dann ist $sp\,(x) = 2x_0$. Ist D der zweireihige Matrizenring, dann ist sp die Matrizenspur.