Globale Eigenschaften des Hilbert - Symbols

Nach „ A Course of Arithmetric“ von Jean - Pierre Serre

Vortrag zum Seminar

„ Quadratische Formen über den rationalen Zahlen“

Sommersemester 2007,

Prof. Dr. K. Wingberg, Ruprecht-Karls-Universität Heidelberg

Maike Parplies und Anna Paulus

31.05.2007

$\mathbb{Q}$ lässt sich als Teilkörper in jedes $\mathbb{Q}_p$ und in $\mathbb{R}$ einbetten. Seien $a,b\in\mathbb{Q}^*$, dann bezeichne $(a,b)_p$ das Hilbertsymbol bezüglich deren Bilder in $\mathbb{Q}_p$ und $(a,b)_\infty$ bezüglich deren Bilder in $\mathbb{R}$. P bezeichne die Menge aller Primzahlen. Wir definieren die Menge V durch $V:=P\cup\{\infty\}$ und setzen $\mathbb{Q}_\infty:=\mathbb{R}$. Damit gilt, dass $\mathbb{Q}$ dicht in $\mathbb{Q}_v$ für alle $v\in V$ ist.

Produktformel

Theorem 3 (Hilbert):

Seien $a,b\in\mathbb{Q}^*$. Dann ist $(a,b)_v=1$ für fast alle $v\in V$ (alle bis auf endlich viele) und es ist $\prod_{v\in V}(a,b)_v=1$.

Beweis:

Da $a,b\in\mathbb{Q}^*=\mathbb{Q}\setminus\{0\}$, können a und b durch Multiplikation mit rationalen Quadraten in ganze Zahlen übergeführt werden. Aus der Bemerkung zu Theorem 1 ist bekannt, dass sich dadurch das Hilbert Symbol von a und b nicht ändert. Deshalb kann ohne Beschränkung der Allgemeinheit angenommen werden, dass a und b ganze Zahlen sind. Wegen der endlichen Primfaktorzerlegbarkeit der ganzen Zahlen gilt: $a=\prod_{i=1}^{n}p_i$, $b=\prod_{j=1}^{m}q_j$ mit $p_i,q_j\in P\cup\{-1\}$ (nicht notwendig verschieden).

Behauptung:
Aufgrund der Bilinearität des Hilbert – Symbols genügt es, Theorem 3 für den Fall zu beweisen, dass a und b entweder den Wert -1 haben oder Primzahlen sind.

Beweis der Behauptung:
Sei $E(x,y):=\{v\in V \mid (x,y)_v=-1\}$.

Es gilt, dass $E(a,b)\subseteq \bigcup_{i=1}^{n}\bigcup_{j=1}^{m}E(p_i,q_j)$, da $(a,b)_v=\prod_{i=1}^{n}\prod_{j=1}^{m}(p_i,q_j)_v$. Wenn nämlich $(a,b)_v=-1$ ist, muss mindestens eines der $(p_i,q_j)=-1$ sein. Wenn aber $(a,b)_v=1$ ist, können trotzdem eine gerade Anzahl der $(p_i,q_j)=-1$ sein.
Annahme:
$E(p_i,q_j)$ ist eine endliche Menge für alle $1\leq i\leq n$ und $1\leq j\leq m$.

Da E(a,b) damit eine endliche Vereingung endlicher Mengen ist, ist E(a,b) auch endlich.
Somit gilt:

$$\prod_{v\in V}(a,b)_v=\prod_{v\in V}\prod_{i=1}^{n}\prod_{j=1}^{m}(p_i,q_j)_v=\prod_{v\in E(a,b)}\prod_{i=1}^{n}\prod_{j=1}^{m}(p_i,q_j)_v=\prod_{i=1}^{n}\prod_{j=1}^{m}\prod_{v\in E(a,b)}(p_i,q_j)_v$$

$$=\prod_{i=1}^{n}\prod_{j=1}^{m}\prod_{v\in V}(p_i,q_j)_v$$

Das heißt, wenn $\prod_{v\in V}(p_i,q_j)_v=1$ für alle $1\leqslant i\leqslant n$ und $1\leqslant j\leqslant m$ ist, gilt auch $\prod_{v\in V}(a,b)_v=1$.

In jedem der Fälle (a,b prim oder -1) erhält man den Wert von $(a,b)_v$ mit Hilfe des Theorems 1.

Fall 1: $a=-1,b=-1$

Es ist $(-1,-1)_\infty=-1$ da a,b < 0.

$(-1,-1)_2=-1$ da $\alpha,\beta=0$ und $-1\neq 1\,(\mathrm{mod}\ 4)$ (Kap.3, Beweis zu Theorem 1, Fall p=2, Fall 1).

$(-1,-1)_p=1$ mit $p\neq 2,\infty$ da $\alpha,\beta=0$.

Daraus ergibt sich, dass $\prod_{v\in V}(-1,-1)_v=1$ und $E(-1,-1)=\{\infty,2\}$.

Fall 2: $a=-1,\ b=l,\ l$ *prim*

- $\boxed{l=2}$

  $(-1,2)_\infty=1$, da b>0.

  $(-1,2)_v=1$ für $v\neq 2,\infty, v\in V$ da $\alpha,\beta=0$ gilt.

  Aus Kap. 3, Beweis zu Theorem 1, Fall p=2, Fall 2 $(\alpha=1,\beta=0)$ ist bekannt, dass $(2,-1)_2=1$ äquivalent ist zu $v\equiv\pm 1\ (mod\ 8)$. Da $-1\equiv -1\,(mod\ \ 8)$ ist, gilt $(2,-1)_2=(-1,2)_2=1$.

- $\boxed{l\neq 2}$

  $(-1,l)_\infty=1$ da $l>0$.

  $(-1,l)_v=1$ für $v\neq 2,l$ denn es gilt $\alpha,\beta=0$ da $v\nmid -1$ und $v\nmid l$.

  Für $v=l$ gilt $\alpha=0,\beta=1$ und damit $(-1,l)_l=(\frac{-1}{l})^1$. Nach Theorem 5 in Kapitel 1 gilt dann $(-1,l)_l=(-1)^{\epsilon(l)}$.

  $(-1,l)_2=(-1)^{\epsilon(l)}$ weil $\alpha=0,\beta=0\,und\,\epsilon(-1)=1$ (da $\frac{-1-1}{2}=\frac{-2}{2}=-1\equiv 1\,(mod 2)$).

Damit ergibt sich: $\prod_{v\in V}(-1,l)_v=1$ und $E(-1,l)\subseteq\{l,2\}$ für l prim.

Fall 3: $a=l,b=l'$ mit l,l' prim

- $\boxed{l=l'}$

  Mit Hilfe von Proposition 2 aus Kap. 2 kann $(l,l)_v$ umgeformt werden.

  $(l,l)_v=(l,-l\cdot l)_v=(l,-1)_v\cdot(l,l^2)_v=(l,-1)_v$ Für alle $v\in V$. Damit tritt hier wieder Fall 2 mit $a=-1,b=l,\ l$ prim ein.

- $\boxed{l\neq l' \text{ und } l'=2}$

  Da $l'=2$ ist, gilt $(2,l)_v=1$ für $v\neq 2,l$ weil α und β in diesen Fällen wieder Null sind.

  $(2,l)_\infty=1$ da 2>0.

  Für $v=2$ gilt α =1 und β=0. Nach Kap. 3, Beweis von Theorem 1, Fall p=2, Fall 2 (α =1, β=0) gilt dann $(2,l)_2=(-1)^{\omega(l)}$.

  Wenn $v=l$, ist α =1 und β=0 für $a=l,b=2$ und damit gilt $(l,2)_l=(\frac{2}{l})$. Theorem 5

aus Kap. 1 besagt, dass $(\frac{2}{l})=(-1)^{\omega(p)}$, damit gilt: $(l,2)_l=(-1)^{\omega(l)}$

- $\boxed{l\neq l',\ l\neq 2,\ l'\neq 2}$
  $(l,l')_v=1$ für $v\neq 2,l,l',\infty$ da α und β in diesen Fällen wieder Null sind.
  $(l,l')_\infty=1$ da l,l' Primzahlen sind und somit größer als Null.
  $(l,l')_2=(-1)^{\epsilon(l)\cdot\epsilon(l')}$ da $\alpha,\beta=0$.
  $(l,l')_l=(\frac{l'}{l})$ da $\alpha=1$ und $\beta=0$.
  $(l,l')_{l'}=(\frac{l}{l'})$ da $\alpha=0$ und $\beta=1$.

Damit ergibt sich für l,l' prim: $\prod_{v\in V}(l,l')_v=(-1)^{\omega(l)}\cdot(-1)^{\omega(l)}\cdot(-1)^{\epsilon(l)\cdot\epsilon(l')}\cdot(\frac{l'}{l})\cdot(\frac{l}{l'})$

$=(-1)^{\epsilon(l)\cdot\epsilon(l')}\cdot(\frac{l'}{l})\cdot(\frac{l}{l'})$

Nach dem Quadratischen Reziprozitätsgesetzt (Kap. 1, Theorem 6) gilt:

$(\frac{l'}{l})\cdot(\frac{l}{l'})=(-1)^{\epsilon(l)\cdot\epsilon(l')}$ da $l\nmid l'$ und $l'\nmid l$

Somit erhalten wir $\prod_{v\in V}(l,l')_v=1$ und $E(l,l')\subseteq\{l,l',2\}$ für l,l' prim.

Wir haben also bewießen, dass sowohl alle $E(p_i,q_j)$ endliche Mengen sind als auch das $\prod_{v\in V}(p_i,q_j)_v=1$ für alle $1\leqslant i\leqslant n$ und $1\leqslant j\leqslant m$ gilt. Damit ist das Theorem 3 bewießen.

Lemma 1 (Chinesischer Restsatz) Seien $a_1,\dots,a_n$, $m_1,\dots,m_n\in\mathbb{Z}$, mit m_i paarweise Teilerfremd. Dann existiert eine ganze Zahl a, so dass $a\equiv a_i \bmod m_i$ für alle i gilt.

Lemma 2 (Approximations Satz) Sei S eine Teilmenge von V. Dann ist das Bild von $\mathbb{Q}$ dicht in $\prod_{v\in S}\mathbb{Q}_v$.

Beweis von Lemma 2 :
Wir erweitern S mit ∞ , falls es nicht in S enthalten ist. Dies ist erlaubt, da dadurch mehr bewießen wird als nötig ist. S ist nun von der Form $S=\{\infty,p_1,\dots,p_n\}$ wobei die p_i verschiedene Primzahlen sind. Zu beweißen ist nun, dass das Bild von $\mathbb{Q}$ dicht in $\mathbb{R}\times\mathbb{Q}_{p_1}\times\dots\times\mathbb{Q}_{p_n}$ ist.

Das heißt, es ist zu zeigen, dass zu jedem beliebigen $(x_v)_{v\in S}=(x_\infty,x_1,\dots,x_n)\in\prod_{v\in S}\mathbb{Q}_v$ und zu jedem ε > 0 ein $x\in\mathbb{Q}$ gibt, so dass $d_v(x,x_v)\leq\epsilon$ für alle $v\in S$. Das ist gleichbedeutend damit, dass es zu jedem ε und zu jedem $N\in\mathbb{N}$ ein $x\in\mathbb{Q}$ existiert, so dass $v_{p_i}(x-x_{p_i})\geq N$ für alle $p_i\in S,\ 1\leq i\leq n$ und $|(x-x_\infty)|\leq\epsilon$.

Durch Multiplikation des Tupels mit einer geeigneten ganzen Zahl h können wir annehmen, dass die $\hat{x}_i:=h\cdot x_i\in\mathbb{Z}_{p_i}$ für $i=1,\dots,n$ sind und $\hat{x_\infty}:=h\cdot x_\infty$. Ein geeignetes h wäre zum Beispiel

$h=\prod_{i=1}^{n}p^{-\inf\{v_{p_i}(x_i),0\}}$.

Die Bedingung $v_{p_i}(x-x_{p_i})\geq N$ ändert sich durch die Multiplikation mit h in

$v_{p_i}(\hat{x}-\hat{x_{p_i}})\geq\{N+\max\{v_{p_i}(h)\}\}:=\hat{N}$ und $|(x-x_{p_i})|\leq\epsilon$ wird zu $|(\hat{x}-\hat{x_{p_i}})|\leq\frac{\epsilon}{h}$.

Definiert man $m_i := p_i^{\hat{N}}$ und $a_i := \hat{x}_i$ so existiert nach Lemma 1 ein $x_0 \in \mathbb{Z}$ mit der Eigenschaft $v_{p_i}(\hat{x}_0 - \hat{x}) \geq \hat{N}$ für $1 \leq i \leq n$.
Nun wähle man eine natürliche Zahl $q \geq 2$, welche zu allen anderen p_i teilerfremd ist. Dies könnte zum Beispiel eine Primzahl sein, die nicht in S enthalten ist.

Behauptung:
Die rationalen Zahlen $\{\frac{a}{q^k} | a \in \mathbb{Z}, k \in \mathbb{N}\}$ liegen dicht in $\mathbb{R}$.
Beweis der Behauptung:
Zu jedem beliebigen $x \in \mathbb{R}, \epsilon > 0, q \in \mathbb{N}$ existiert ein $k \in \mathbb{N}$, so dass $q^{-k} < \epsilon$ gilt. Außerdem gibt es ein $a \in \mathbb{Z}$ mit der Eigenschaft $|x \cdot q^k - a| < 1$, somit gilt $|x - \frac{a}{q^k}| < \epsilon$ und die Behauptung ist bewießen.

Jetzt wähle man k = m so, dass für die Zahl $u = \frac{a}{q^m}$ $\left|\hat{x}_0 - \hat{x}_\infty + u \cdot p_1^{\hat{N}} \cdot \ldots \cdot p_n^{\hat{N}}\right| \leq \epsilon$ gilt und definieren $\hat{x} = \hat{x}_0 + u \cdot p_1^{\hat{N}} \cdot \ldots \cdot p_n^{\hat{N}}$. Somit gilt:
$v_{p_i}(\hat{x} - \hat{x}_i) = v_{p_i}(\hat{x}_0 + u \cdot p_1^{\hat{N}} \cdot \ldots \cdot p_n^{\hat{N}} - x_i) \geq \inf \{ \underbrace{v_{p_i}(\hat{x}_0 - \hat{x}_i)}_{\geq \hat{N}}, v_{p_i}(u) + \underbrace{v_{p_i}(p_1^{\hat{N}} \cdot \ldots \cdot p_n^{\hat{N}})}_{= \hat{N}} \}$.
Jetzt muss nur noch $v_{p_i}(u)$ bestimmt werden. $u = a \cdot p^{-m}$,daher gilt $v_{p_i}(u) = v_{p_i}(a) - v_{p_i}(p^m)$. q wurde so gewählt, dass $q \nmid p_i$ für i = 1,...,n, damit gilt für diese i`s auch $q^m \nmid p_i$ und so auch $v_{p_i}(q^m) = 0$. Da a aus $\mathbb{Z}$ gewählt wurde liegt es automatisch auch in allen $\mathbb{Z}_{p_i}$ denn $\mathbb{Z} \subset \mathbb{Z}_p \forall$ p prim. Eine zu den anderen äquivalenten Definitionen von $\mathbb{Z}_p$ ist $\mathbb{Z}_p = \{ x \in \mathbb{Q}_p \mid v_p(x) \geq 0 \}$. Somit ist klar, dass $v_{p_i}(a) \geq 0$ und damit ist auch $v_{p_i}(u) \geq 0$.

Für $x = \frac{\hat{x}}{h}$ gilt dann $|x - x_\infty| = \left|\frac{\hat{x} - \hat{x}_\infty}{h}\right| \leq \frac{\epsilon}{h} \leq \epsilon$ und
$v_{p_i}(x - x_i) = v_{p_i}(\frac{\hat{x} - \hat{x}_i}{h}) = v_{p_i}(\hat{x} - \hat{x}_i) - v_{p_i}(h) \geq \hat{N} - \max_{1 \leq i \leq n} \{ v_{p_i}(h) \} = N$. Die letzte Abschätzung ist erlaubt, da $h \in \mathbb{N}$ und damit wie bei a gilt: $v_{p_i}(h) \geq 0$.

Also haben wir nun das gesuchte $x \in \mathbb{Q}$ mit $x = \frac{\hat{x}}{h} = \frac{x_0 + u \cdot p_1^{\hat{N}} \cdot \ldots \cdot p_n^{\hat{N}}}{h}$ gefunden. Lemma 2 ist somit bewießen.

Existenz rationaler zahlen mit gegebenem Hilbertsymbol

Theorem 4 Sei $(a_i)_{(i \in I)}$ mit $(a_i) \in \mathbb{Q}^*$, I eine endliche Menge, und sei $(\epsilon_{i,v})_{(i \in I, v \in V)}$ mit $\epsilon_{i,v} \in \{\pm 1\}$. Es gibt genau dann ein $x \in \mathbb{Q}^*$ mit
$$(a_i, x)_v = \epsilon_i, v \text{ für alle } v \in V \text{ , } i \in I \text{ ,}$$
wenn folgende Bedingungen (1)-(3) erfüllt sind
(1) Fast alle $\epsilon_{(i,v)}$ sind gleich 1
(2) Es gilt $\prod_{(v \in V)} \epsilon_{(i,v)} = 1$ für i=1,...n
(3) Für jedes $v \in V$ existiert ein $x_v \in \mathbb{Q}_v{}^*$ mit $(a_i, x_v)_v = \epsilon_{(i,v)}$ für alle $i \in I$
(Satz 9.7.4 Seite 177)

Lemma 3 (Dirichletscher Primzahlensatz) Sei $n \in \mathbb{N}$ und $a \in \mathbb{Z}$ und a,n teilerfremd. Dann

gibt es unendlich viele Primzahlen p mit
$p \equiv a \bmod n$
(Theorem 8.6.1 Seite 149)
der Beweis hierfür wird in Kapitel 4 gegeben.

Beweis von Theorem 4

→ Die Gültigkeit der Bedingungen (1) und (2) folgt aus Theorem 3 und mit $x_v := x$ ist die Bedingung (3) erfüllt.

← Seien die Bedingungen (1)-(3) erfüllt. Nach Multplikation mit einer geeigneten Quadratzahl können wir annehmen, dass die a_i ganze Zahlen sind (dabei werden die Hilbertsymbole nicht verändert)
Sei S die Menge aller Primteiler der a_i vereinigt mit $\{2,\infty\}$.
Sei T die Menge der $v \in P$ mit $\epsilon_{(i,v)} = -1$ für ein i.
$S, T \subseteq P$ Beide Teilmengen sind endlich. (S klar, T nach Bedingung (1))

1.Fall

$S \cap T = \emptyset$ dann ist $\infty \notin T$
Setze $a = \prod_{l \in T,\, l \neq \infty} l$ und $m = 8 \prod_{l \in S,\, l \neq 2,\infty} l$
weil $S \cap T = \emptyset$ sind a und m teilerfremd und nach dem Dirichletscher Primzahlensatz existiert eine Primzahl $p \equiv a \bmod m$ mit $p \notin S \cup T$ (p kann so gewählt werden, da es unendlich viele solcher Primzahlen gibt, die Mengen S,T aber endlich sind) .
Wir zeigen, dass $x = pa$ die gewünschte Eigenschaft hat, d.h. $(a_i, x)_v = \epsilon_{i,v}$ für alle $v \in V$, i=1,...,n,

I. $v \in S$:
Dann ist $v \notin T$ und deshalb $\epsilon_{(i,v)} = 1$
Ist $v = \infty$, dann ist $(a_i, x)_\infty = 1$ wegen $x > 0$ (Kapitel 3, Theorem1)
Ist $v = l$ eine Primzahl, dann ist $x = pa \equiv a^2 (\bmod m)$, also ist $x \equiv a^2 \bmod 8$ für $l = 2$ und $x \equiv a^2 \bmod l$ für $l \neq 2$. das zeigt, dass x ein Quadrat in $\mathbb{Q}_l^*$ ist, also ist $(a_i, x)_v = 1$.
($l = 2$: $x \equiv a^2 \bmod 8$ → $a^2 = 1,4$, aber a ist nicht 4 weil a und m teilerfremd, → $x \equiv 1 \bmod 8$ → x ist ein Quadrat in $\mathbb{Q}_l^*$ (nach Theorem 4, Kapitel 2, 3.3); $l \neq 2$: Hilfssatz[1]: Es sei $x = p^n * u$, $u \in \mathbb{Z}_p^*$. Es existiert genau dann eine Quadratwurzel aus x in $\mathbb{Q}_p$, wenn $2 | n$ und $(\frac{u}{p}) = 1$. Da $x = ap$ und $l \in S$ folgt $l \nmid a, p$ → $n = 0$ und $2 | 0$ weiterhin ist $x = ap$ quadratischer Rest mod l und damit $(\frac{x}{l}) = 1$ → x ist ein Quadrat in $\mathbb{Q}_l^*$)

II. $v \notin S$
$v = l$ prim: Dann gilt $\forall k \in I : a_k \in \mathbb{Z}_l^*$ d.h. die a_k sind Einheiten (denn $l \nmid a_k$). Da $l \neq 2$ folgt aus Theorem 1 Kapitel 3:

$$\forall k \in I, b \in \mathbb{Q}_l^{(*)} : (a_k, b)_l = (\frac{a_k}{l})^{(v_l(b))}$$

(Die a_k werden wie folgt Dargestellt: $a_k = u * l^0$ (weil $l \nmid a_k$) → $\alpha = 0$ $\beta = v_l(b)$)

- $l \notin T \cup p$: Dann gilt $x = pa \in \mathbb{Z}_l^*$ (denn $l \nmid p, l \nmid a = \prod T$), also $v_l(x) = 0$ und wir erhalten aus der oberen Formel $(a_i, x)_l = (\frac{a_i}{l})^0 = 1$. Wegen $l \notin T$ ist $\epsilon_{(i,l)} = 1$ → $(a_i, x)_l = \epsilon_{(i,l)}$

1 Alexander Schmidt: Einführung in die algebraische Zahlentheorie; Satz 9.9.5 Seite 168

- $l \in T$: Dann ist $v_l(x)=1$ (denn $x=ap$ ist ein Produkt verschiedener Primzahlen, $l|a$). wegen Bedingung (3) exitiert ein ein $x_l \in \mathbb{Q}^*_l$ mit $(a_i, x_l)_l = \epsilon_{(i,l)}$ für alle $i \in I$. wegen $l \in T$ gibt es ein $j \in I$ für das $\epsilon_{(j,l)} = -1$ und wir haben $(a_j, x_l)_l = -1 = (\frac{a_j}{l})^{(v_l(x_l))}$, deshalb muss $v_l(x_l) \equiv 1 (mod\, 2)$ sein ($v_l(x_l)$ muss ungerade sein!), also gilt $(a_i, x)_l = (\frac{a_i}{l})^{(v_l(x))} = (\frac{a_i}{l}) = (\frac{a_i}{l})^{(v_l(x_l))} = (a_i, x_l)_l = \epsilon_{(i,l)}$

- $l = p$: Dann gilt: $(a_i, x)_p = \prod_{v \neq p} (a_i, x)_v = \prod_{v \neq p} \epsilon_{(i,v)} = \epsilon_{(i,p)}$ (Nach Theorem 3, sowie den Fällen I und II und Bedingung (2) $\prod_{v \in V} (a_i, x)_v = 1 \Leftrightarrow \prod_{v \neq p} (a_i, x)_v = \frac{1}{(a_i, x)_p} = (a_i, x)_p = \prod_{v \neq p} (a_i, x)_v = \prod_{v \neq p} \epsilon_{(i,v)} = 1 = \epsilon_{(i,p)}$)

Wir wollen nun den Spezialfall auf den allgemeinen Fall zurückführen

2. Fall

$S \cap T \neq \emptyset$ Die Quadrate $\mathbb{Q}_v{}^{*2}$ bilden eine offene Untergruppe in $\mathbb{Q}_v{}^*$ (Kapitel 2, 3.3) . wähle $x_v \in \mathbb{Q}_v^*$ dann ist x_v auch Element der offenen Umgebung $x_v(\mathbb{Q}_v^*)^2$, d.h $x_v \in x_v(\mathbb{Q}_v^*)^2$, weil nach Lemma 2 $\mathbb{Q}$ dicht in $\mathbb{Q}_v$ liegt, existiert ein $x' \in \mathbb{Q}$ sodass $x' \in x_v(\mathbb{Q}_v^*)^2 \Leftrightarrow \frac{(x')}{x_v} \in (\mathbb{Q}_v^*)^2$, $\frac{x'}{x_v}$ ist also ein Quadrat in $\mathbb{Q}_v^*$

Setzen wir für alle $i \in I, v \in V$: $\eta_{(i,v)} := \epsilon_{(i,v)}(a_i, x')_v$ dann erfüllt die Familie $(\eta_{(i,v)})$ die Bedingungen (1)-(3) und es ist $\eta_{(i,v)} = 1 \; \forall i \in I, v \in S$ .Denn nach den Bedingungen für $\epsilon_{(i,v)}$ und Theorem 3 gilt:

(1) Fast alle $\eta_{(i,v)} = \epsilon_{(i,v)}(a_i, x')_v$ sind gleich 1 (Bedingung (1), Theorem 3)

(2) Für alle $i \in I$ ist $\prod_{v \in V} \eta_{(i,v)} = \prod_{v \in V} (\epsilon_{(i,v)}(a_i, x')_v) = \prod_{v \in V} \epsilon_{(i,v)} \prod_{v \in V} (a_i, x')_v = 1$

(3) $\forall v \in V : \exists x'_v \in \mathbb{Q}_v^* : \forall i \in I : (a_i, x'_v)_v = \eta_{(i,v)}$. Setze $x'_v := \frac{x'}{x_v}$, dann ist

$$(a_i, \frac{x'}{x_v})_v = (a_i, x')_v (a_i, \frac{1}{x_v})_v = (a_i, x')_v (a_i, \frac{1}{x_v} * (x_v)^2)_v = (a_i, x')_v (a_i, x_v)_v = \epsilon_{(i,v)}(a_i, x')_v = \eta_{(i,v)}$$

Falls $v \in S$, dann ist $\frac{x'}{x_v} \in \mathbb{Q}_v^{(*2)}$, also $\forall i \in I : \eta_{(i,v)} = (a_i, \frac{x'}{x_v})_v = 1$

Wir können jetzt auf die Familie $\eta_{(i,v)}$ Fall 1 anwenden, denn $\tilde{T} := \{ v \in V : \exists i \in I : \eta_{(i,v)} = -1 \}$ ist disjunkt zu S. Es existiert also ein $y \in \mathbb{Q}^*$ mit $\forall i \in I, v \in V : (a_i, y)_v = \eta_{(i,v)}$. Setzen wir $x := yx'$, dann ist $\forall i \in I, v \in V : (a_i, x)_v = (a_i, y)_v (a_i, x')_v = \eta_{(i,v)}(a_i, x')_v = \epsilon_{(i,v)}$.