Die Stickelberger-Gleichung, Teil 1

Anna Henningsen und Lily Dörflinger

26. Juli 2017

1 Grundvoraussetzungen

Im folgenden sind $m \in \mathbb{N}$ und $P \subset_{\text{prim}} D_m \subset \mathbb{Q}(\zeta_m)$ ein Primideal im Ganzheitsring von $\mathbb{Q}(\zeta_m)$ mit $m \notin P$. Wir wiederholen die folgenden Definitionen:

- Die *Norm* eines Primideals P in D_m ist definiert als $N(p) = |D_m/P| = q = p^f$ mit $p\mathbb{Z} = P \cup Z$, $D_m/P \cong \mathbb{F}_{p^f}$, und es gilt $N(P) \equiv 1\ (m)$.
- Für $\alpha \in D_m$ bezeichnet das Symbol $\left(\frac{\alpha}{P}\right)$ die (eindeutige) m-te Einheitswurzel ζ_m^k mit $\left(\frac{\alpha}{P}\right) \equiv \alpha^{(N(P)-1)/m}\ (P)$.

Nach einem Lemma des vorherigen Vortrags gilt:

- $\left(\frac{\alpha\beta}{P}\right) = \left(\frac{\alpha}{P}\right)\left(\frac{\beta}{P}\right)$ für α, β aus D_m, sowie:
- Aus $\alpha \equiv \beta\ (P)$ folgt $\left(\frac{\alpha}{P}\right) = \left(\frac{\beta}{P}\right)$.

2 Die Spur tr auf $\mathbb{F}_{p^f}$

Im folgenden sei $F = \mathbb{F}_{p^f}$ ein beliebiger endlicher Körper.

Definition 2.1. Für $\alpha \in F$ ist die *Spur* von α definiert als $\operatorname{tr}(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \ldots + \alpha^{p^{f-1}}$.

Bemerkung. Diese Definition von Spur deckt sich sinngemäß mit der vorigen Definition der Spur für galoisschen Körpererweiterungen $F \subset \mathbb{C}$ von $\mathbb{Q}$, in denen $\operatorname{tr}(z) = \sum_{\sigma \in \operatorname{Gal}(F/\mathbb{Q})} \sigma(z)$ definiert war.

In diesem Fall ist $\operatorname{tr}(\alpha) = \sum_{\sigma \in \operatorname{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p)} \sigma(\alpha)$ und $\operatorname{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p)$ die vom Frobeniusautomorphismus $\alpha \mapsto \alpha^p$ erzeugte zyklische Galoisgruppe.

Lemma 2.2. Für α, β in $F = \mathbb{F}_{p^f}$, $\alpha \in \mathbb{F}_p$ gilt:

(a) $\operatorname{tr}(\alpha) \in \mathbb{F}_p$

(b) $\operatorname{tr}(\alpha + \beta) = \operatorname{tr}(\alpha) + \operatorname{tr}(\beta)$

(c) $\operatorname{tr}(a \cdot \alpha) = a \cdot \operatorname{tr}(\alpha)$

(d) $\mathrm{tr}\colon F \to \mathbb{F}_p$ ist surjektiv.

Beweis. (a) In Charakteristik p is Potenzieren mit p ein Homomorphismus, also gilt: $(\alpha + \alpha^p + \alpha^{p^2} + \ldots + \alpha^{p^{f-1}})^p = \alpha^p + \alpha^{p^2} + \alpha^{p^3} + \ldots + \alpha^{p^f}$ Da F^* zyklisch der Ordnung $p^f - 1$ ist, ist $\alpha^{p^f} = \alpha$, und entsprechend steht auf beiden Seiten der Gleichung $\mathrm{tr}(\alpha) = \mathrm{tr}(\alpha)^p$.

Da wie bemerkt die Galoisgruppe $\mathrm{Gal}(F/\mathbb{F}_p)$ von $x \mapsto x^p$ erzeugt wird, muss also $\mathrm{tr}(\alpha)$ bereits im Fixkörper dieses Automorphismus, also $\mathbb{F}_p$, liegen.

(b) Es gilt

$$\begin{aligned} \mathrm{tr}(\alpha + \beta) &= (\alpha + \beta) + (\alpha + \beta)^p + \ldots + (\alpha + \beta)^{p^{f-1}} \\ &= (\alpha + \beta) + (\alpha^p + \beta^p) + \ldots + (\alpha^{p^{f-1}} + \beta^{p^{f-1}}) \\ &= (\alpha + \alpha^p + \ldots + \alpha^{p^{f-1}}) + (\beta + \beta^p + \ldots + \beta^{p^{f-1}}) \\ &= \mathrm{tr}(\alpha) + \mathrm{tr}(\beta) \end{aligned}$$

(c) Es gilt wieder $a^p = a$ und damit

$$\begin{aligned} \mathrm{tr}(a \cdot \alpha) &= (a \cdot \alpha) + (a \cdot \alpha)^p + \ldots + (a \cdot \alpha)^{p^{f-1}} \\ &= (a \cdot \alpha) + (a^p \cdot \alpha^p) + \ldots + (a^{p^{f-1}} \cdot \alpha^{p^{f-1}}) \\ &= a \cdot (\alpha + \alpha^p + \ldots \alpha^{p^{f-1}}) \\ &= a \cdot \mathrm{tr}(\alpha) \end{aligned}$$

(d) $\mathrm{tr}(X)$ hat als Polynom den Grad p^{f-1}, $\mathbb{F}_{p^f}$ jedoch p^f Elemente, also gibt es ein $\alpha \in F$ dass keine Nullstelle von tr ist: $\mathrm{tr}(\alpha) = c \neq 0$ für ein $c \in \mathbb{F}_p$.

Für ein beliebiges $b \in \mathbb{F}_p$ ergibt sich:

$$\mathrm{tr}\left(\frac{b}{c} \cdot \alpha\right) \overset{\text{(c)}}{=} \frac{b}{c} \cdot \mathrm{tr}(\alpha) = b$$

□

Definition 2.3. Wir definieren einen additiven Charakter $\psi\colon F \to \mathbb{C}$ durch $\psi(\alpha) = \zeta_p^{\mathrm{tr}(\alpha)}$.

Lemma 2.4. Aus den Eigenschaften der Spur folgen die folgenden Eigenschaften von ψ:

(a) $\psi(\alpha + \beta) = \psi(\alpha)\psi(\beta)$

(b) Es gibt ein $\alpha \in F$ mit $\psi(\alpha) \neq 1$.

(c) $\sum_{\alpha \in F} \psi(\alpha) = 0$

Beweis. (a) Es gilt:

$$\psi(\alpha + \beta) = \zeta_p^{\mathrm{tr}(\alpha+\beta)} = \zeta_p^{\mathrm{tr}(\alpha)+\mathrm{tr}(\beta)} = \zeta_p^{\mathrm{tr}(\alpha)} \zeta_p^{\mathrm{tr}(\beta)} = \psi(\alpha)\psi(\beta)$$

(b) Da tr surjektiv ist, existiert ein $\alpha \in F$ mit $\mathrm{tr}(\alpha) = 1$ und damit $\psi(\alpha) = \zeta_p \neq 1$.

(c) Wir bezeichnen die Summe als $S = \sum_{\alpha \in F} \psi(\alpha)$, und wählen nach (b) ein β mit $\psi(\beta) \neq 1$. Dann gilt

$$\psi(\beta)S = \sum_{\alpha \in F} \psi(\beta)\psi(\alpha) = \sum_{\alpha \in F} \psi(\beta + \alpha) = S$$

wobei in der letzten Gleichheit ausgenutzt wurde dass α und $\beta + \alpha$ jeweils alle Werte in F durchlaufen. Es folgt wegen $\psi(\beta) \neq 1$, dass $S = 0$ gelten muss.

□

Lemma 2.5. Seien $\alpha, x, y \in F$. Dann gilt mit $q = p^f = |F|$ und $\delta(x, y) = 1$ für $x = y$, $\delta(x, y) = 0$ sonst:

$$\sum_{\alpha \in F} \psi(\alpha(x - y)) = q\delta(x, y)$$

Beweis. Falls $x = y$, so ist $\sum_{\alpha \in F} \psi(\alpha(x - y)) = \sum_{\alpha \in F} \psi(0) = |F| \cdot 1 = q$.

Falls $x \neq y$, so ist $x - y$ invertierbar, also durchläuft $\alpha(x - y)$ alle Werte in F genau einmal: $\sum_{\alpha \in F} \psi(\alpha(x - y)) = \sum_{\beta \in F} \psi(\beta) = 0$ nach 2.4 (c). □

3 Die Stickelberger-Gleichung

Im Folgenden ist $F = D_m/P$ immer der Quotient des Ganzheitsrings $D_m \subset \mathbb{Q}(\zeta_m)$ nach einem Primideal P.

Definition 3.1. Wir definieren den multiplikativen Charakter $\chi_P \colon F^* \to \mathbb{C}$ wie folgt:

Für eine Restklasse $t \in F$ wählen wir einen Repräsentanten $\gamma \in D_m$ mit $\bar{\gamma} = t$. Dann setzen wir:

$$\chi_P(t) = \left(\frac{\gamma}{P}\right)^{-1} \left(= \overline{\left(\frac{\gamma}{P}\right)}\right)$$

Dies ist wohldefiniert, da der Wert von $\left(\frac{\gamma}{P}\right)$ nicht von der konkreten Wahl des Repräsentanten γ abhängt.

Gegebenenfalls wird χ_P durch $\chi_P(0) = 0$ auf F fortgesetzt und bleibt dabei offenbar multiplikativ.

Definition 3.2. Wir definieren $g(P)$ für ein Primideal $P \subset D_m$ als die Gaußsumme $g(\chi_P, \psi) = \sum_{t \in F} \chi_P(t)\psi(t)$, und $\Phi(P) = g(P)^m$.

Das Ziel dieses Abschnitts wird es sein, eine nützliche Darstellung der Primidealzerlegung von $(\Phi(P))$ zu finden.

Lemma 3.3. Es gelten für $g(P)$ und $\Phi(P)$ wie oben definiert:

(a) $g(P) \in \mathbb{Q}(\zeta_m, \zeta_p$

(b) $|g(P)|^2 = q \ (= p^f)$

(c) $\Phi(P) \in \mathbb{Q}(\zeta_m)$

Beweis. (a) Die Behauptung folgt direkt daraus, dass $g(P)$ über Multiplikation und Addition der Werte von χ_P und ψ, also Potenzen von ζ_m und ζ_p, definiert ist.

(b) Wir verwenden hier, dass die Werte von χ_P und ψ Einheitswurzeln sind, d. h. $\overline{\chi_P(t)} = \chi_P(t)^{-1}$ und $\overline{\psi(t)} = \psi(t)^{-1}$ für $t \in F$:

$$
\begin{aligned}
|g(P)|^2 &= \left(\sum_{t\in F}\chi_P(t)\psi(t)\right)\overline{\left(\sum_{t\in F}\chi_P(t)\psi(t)\right)} \\
&= \sum_{t,u\in F^*}\chi_P(t)\psi(t)\overline{\chi_P(u)\psi(u)} \\
&= \sum_{t,u\in F^*}\chi_P(t)\overline{\chi_P(u)}\psi(t)\overline{\psi(u)} \\
&= \sum_{t,u\in F^*}\chi_P(t)\chi_P(u)^{-1}\psi(t)\psi(u)^{-1} \\
&= \sum_{t,u\in F^*}\chi_P(t\cdot u^{-1})\psi(t-u) \\
&\overset{s:=t\cdot u^{-1}}{=} \sum_{s,u\in F^*}\chi_P(s)\psi(su-u) \\
&= \sum_{s,u\in F^*}\chi_P(s)\psi((s-1)u) \\
&= \sum_{s\in F^*}\chi_P(s)\sum_{u\in F^*}\psi((s-1)u) \\
&\overset{\text{Lemma 2.5}}{=} \sum_{s\in F^*}\chi_P(s)(q\delta(s,1)-1) \\
&= \left(\sum_{s\in F^*\setminus\{1\}}\chi_P(s)(-1))\right)+1\cdot(q-1) \\
&= \left(\sum_{s\in F^*}\chi_P(s)(-1))\right)-\chi_P(1)(-1)+1\cdot(q-1) \\
&= 0+1+(q-1)=q
\end{aligned}
$$

(c) Wir betrachten die Körpererweiterung $\mathbb{Q}(\zeta_{mp})=\mathbb{Q}(\zeta_m,\zeta_p)$ von $\mathbb{Q}$, aus der $g(P)$ und damit auch $\Phi(P)$ stammt. Diese ist wie bereits in vorigen Vorträgen gesehen galoisch, und da ein Automorphismus σ durch sein Bild auf ζ_{mp} (das dann selbst wieder eine primitive mp-te Einheitswurzel sein muss) bestimmt ist, ist $\mathrm{Gal}(\mathbb{Q}(\zeta_{mp})/\mathbb{Q})=\{\sigma_c|(c,mp)=1\}$ wobei $\sigma_c\colon \mathbb{Q}(\zeta_{mp})\to\mathbb{Q}(\zeta_{mp})$ durch $\zeta_{mp}\mapsto\zeta_{mp}^c$ gegeben ist.

Es gelten:

- σ_c fixiert $\mathbb{Q}(\zeta_m)$ genau dann, wenn $c\equiv 1\ (m)$, denn: $\sigma_c(\zeta_m)=\sigma_c(\zeta_{mp}^p)=\sigma_c(\zeta_{mp})^p=(\zeta_{mp}^c)^p=\zeta_{mp}^{cp}=\zeta_m^c$, und analog:

- σ_c fixiert $\mathbb{Q}(\zeta_p)$ genau dann, wenn $c \equiv 1\ (p)$.

Also ist zu zeigen, dass $\Phi(P)^{\sigma_c}$ $(= \sigma_c(\Phi(P))) = \Phi(P)$ für $c \equiv 1\ (m)$ erfüllt ist.

Sei also $c \equiv 1\ (m)$. Wir bestimmen zunächst $g(P)^{\sigma_c}$ und nutzen aus, dass nach Definition $\chi_P(t) \in \mathbb{Q}(\zeta_m)$ und damit $\chi_P(t)^{\sigma_c} = \chi_P(t)$:

$$\begin{aligned}
g(P) &= \sum_{t\in F} \chi_P(t)\psi(t) \\
\Rightarrow g(P)^{\sigma_c} &= \sum_{t\in F} \chi_P(t)^{\sigma_c}\psi(t)^{\sigma_c} \\
&= \sum_{t\in F} \chi_P(t)(\zeta_p^{\mathrm{tr}(t)})^{\sigma_c} \\
&= \sum_{t\in F} \chi_P(t)(\zeta_p^{c\cdot\mathrm{tr}(t)}) \\
&\overset{(*)}{=} \sum_{t\in F} \chi_P(t)(\zeta_p^{\mathrm{tr}(c\cdot t)}) \\
&= \sum_{t\in F} \chi_P(t)\psi(ct) \\
&= \chi_P(c)^{-1} \sum_{t\in F} \chi_P(c)\chi_P(t)\psi(ct) \\
&= \chi_P(c)^{-1} \sum_{t\in F} \chi_P(ct)\psi(ct) \\
&= \chi_P(c)^{-1} g(P)
\end{aligned}$$

Dabei ist $(*)$ erlaubt, da c als Potenz auf ζ_p wirkt, welches die multiplikative Ordnung p hat, und daher c als Element von $\mathbb{F}_p$ aufgefasst werden kann, vgl. Lemma 2.2 (c).

Damit ergibt sich für $\Phi(P)$: $\Phi(P)^{\sigma_c} = (g(P)^m)^{\sigma_c} = (\chi_P(c)^{-m} g(P)^m) = \Phi(P)$, da $\chi_P(c)$ nach Definition eine m-te Einheitswurzel ist.

□

Um mit der *Stickelberger-Gleichung* eine geeignete Darstellung für $(\Phi(P))$ zu erhalten, werden zunächst drei Spezialfälle betrachtet.

Beispiel 3.4. 1. $m = 2$. In diesem Fall ist $\mathbb{Q}(\zeta_2) = \mathbb{Q}$, also der Ganzheitsring $D_2 = \mathbb{Z}$. Primideale in $\mathbb{Z}$ haben die Form $P = (p) = p\mathbb{Z}$ für eine Primzahl p. Für den Körper F ergibt sich $F = D_2/P = \mathbb{Z}/p\mathbb{Z}$ mit $|F| = p$ Elementen, also $q = p^f$ für $f = 1$. Das Symbol $(\frac{\gamma}{P})_2 = (\frac{\gamma}{P})$ ist hier einfach das Legendre-Symbol (vgl. den dritten Vortrag). Insgesamt ergibt sich

$$g(P) = g(\chi_P, \psi) = \sum_{\bar{t} \in \mathbb{Z}/p\mathbb{Z}} \chi_P(\bar{t})\psi(\bar{t}) = \sum_{\bar{t} \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{t}{P}\right)^{-1} \zeta_p^{\bar{t}} = g_1,$$

wobei g_1 die quadratische Gaußsumme bezeichnet. Ebenfalls aus dem dritten Vortrag folgt $g(P)^2 = g_a^2 = (-1)^{\frac{p-1}{2}} p$.

2. *$m = 3$.* $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3}), P = (\pi), \pi$ primär.
   Mit zusätzlichem Wissen über kubische Reziprozität (nachzulesen in [1], Kapitel 9, §4) kann gezeigt werden, dass $g(P)^3 = p\bar{\pi} = \pi\bar{\pi}^2$ gilt.

3. *$m = 4$.* $\mathbb{Q}(\zeta_4) = \mathbb{Q}(\sqrt{-1}), P = (\pi), \pi$ primär.
   Mit zusätzlichem Wissen über biquadratische Reziprozität (nachzulesen in [1], Kapitel 9, §7) kann gezeigt werden, dass $g(P)^4 = p\bar{\pi}^2 = \pi\bar{\pi}^3$ gilt.

Sei nun $K/\mathbb{Q}$ ein über $\mathbb{Q}$ galois'scher Zahlkörper mit Galoisgruppe $\mathrm{Gal}(K/\mathbb{Q}) = G$. Definiere $\mathbb{Z}[G] = \{\sum_{\sigma \in G} a(\sigma)\sigma \mid a(\sigma) \in \mathbb{Z}\}$ und für $\alpha \in K$

$$\alpha^{\sum a(\sigma)\sigma} = \prod_{\sigma} \sigma(\alpha)^{a(\sigma)}.$$

Für ein Ideal A läuft die Definition analog. Die Spezialfälle aus Beispiel 3.4 können dann in der Form $\Phi(P) = \pi^{1+2\sigma}$ für $\sigma \in \mathrm{Aut}(\mathbb{Q}(\sqrt{-3})/\mathbb{Q})$, bzw. $\Phi(P) = \pi^{1+3\tau}$ für $\tau \in \mathrm{Aut}(\mathbb{Q}(\sqrt{-1})/\mathbb{Q})$ dargestellt werden. Insgesamt ergibt sich folgendes wichtiges Theorem, das endgültig erst im nächsten Vortrag bewiesen wird:

Theorem 3.5. (*Stickelberger-Gleichung*) Sei P ein Primideal in D_m mit $m \notin P$. Dann gilt

$$(\Phi(P)) = P^{\sum t\sigma_t^{-1}},$$

wobei über alle $1 \leq t < m$ mit $\mathrm{ggT}(t, m) = 1$ summiert wird.

4 Beweis der Stickelberger-Gleichung

Für den Beweis der Stickelberger-Gleichung werden zunächst drei Lemmata gezeigt.

Lemma 4.1. Sei $p \in \mathbb{N}$. Dann gibt es für jede Zahl $a \in \mathbb{N}$ eine eindeutige Darstellung $a = \sum_{i=0}^{n} a_i p^i$ mit $0 \leq a_i < p$.

Beweis. (a) *Existenz:* Sei $a \in \mathbb{N}$. Dann gilt $p^n \leq a < p^{n+1}$ für ein eindeutiges $n \in \mathbb{N}$. Wiederholte Division mit Rest ergibt

1. $a = a_n p^n + r_n$ für ein $a_n < p,\ 0 \leq r_n < p^n$
2. $r_n = a_{n-1} p^{n-1} + r_{n-1}$ für $a_{n-1} < p,\ 0 \leq r_{n-1} < p^{n-1}$
   $\dots$

n+1. $r_1 = a_0 p^0$ für $a_0 < p$

in endlich vielen Schritten. Setzt man diese Ergebnisse ein, so erhält man die gewünschte Darstellung $a = a_n p^n + a_{n-1} p^{n-1} + \cdots + a_0$.

(b) *Eindeutigkeit:* Sei $\sum_{i=0}^{n} a_i p^i = \sum_{i=0}^{m} b_i p^i$ mit $0 \leq a_i, b_i < p$. O.B.d.A. sei $m = n$. Es gilt dann $a_0 - b_0 = \sum_{i=0}^{n} (b_i - a_i) p^i = p \sum_{i=0}^{n} (b_i - a_i) p^{i-1}$, also $p \mid a_0 - b_0$. Außerdem gilt $\mid a_0 - b_0 \mid < p$, womit dann $a_0 = b_0$ folgt. Es ergibt sich $\sum_{i=1}^{n} a_i p^i = \sum_{i=1}^{n} b_i p^i$ und nach mehrfacher Wiederholung des Arguments folgt die Behauptung.

$\square$

Damit kann folgendes definiert werden:

Definition 4.2. Sei $q = p^f$.

1. Falls $0 \leq a < q - 1$, schreibe $a = \sum_{i=0}^{f-1} a_i p^i$ mit $0 \leq a_i < p$ und setze $S(a) = \sum_{i=0}^{f-1} a_i$.
2. Für $a \in \mathbb{N}$ beliebig setze $S(a) = S(r)$, wobei $a \equiv r\ (q-1),\ 0 \leq r < q-1$.

Definition 4.3. Sei $u \in \mathbb{R}$.
$\langle u \rangle = u - \lfloor u \rfloor \in [0, 1)$ heißt *Bruchanteil* von u.

Lemma 4.4. $S(a) = (p-1) \sum_{i=0}^{f-1} \langle \frac{p^i a}{q-1} \rangle$.

Beweis. Zunächst gilt $S(a + x(q-1)) = S(a)$, sowie $(p-1) \sum \langle \frac{p^i(a + x(q-1))}{q-1} \rangle = (p-1) \sum \langle \frac{p^i a}{q-1} + p^i x \rangle = (p-1) \sum \langle \frac{p^i a}{q-1} \rangle$ für jedes $x \in \mathbb{Z}$. Auf beiden Seiten der Gleichung ändert sich also nichts, wenn Vielfache von $q-1$ zu a addiert werden. O.B.d.A. kann deshalb $1 \leq a < q - 1$ angenommen werden.

Schreibe also $a = a_0 + a_1 p + \cdots + a_{f-1}p^{f-1}$ wie in der Definition. (Mehrfache) Multiplikation mit p ergibt

$$\begin{aligned} pa &= a_0 p + \cdots + a_{f-2}p^{f-1} + a_{f-1}p^f \\ &\equiv a_{f-1} + a_0 p + \cdots + a_{f-2}p^{f-1} \ (q-1) \\ p^2 a &\equiv a_{f-2} + a_{f-1}p + \cdots + a_{f-3}p^{f-1} \ (q-1) \\ \text{usw.} \end{aligned}$$

Da die rechten Seiten alle kleiner sind als $q-1$, folgt

$$\begin{aligned} \langle \frac{p^i a}{q-1} \rangle &= \frac{1}{q-1} \cdot (\text{rechte Seite der } i\text{-ten Kongruenz}), \text{bzw.} \\ \sum_{i=0}^{f-1} \langle \frac{p^i a}{q-1} \rangle &= \frac{1}{q-1}(a_0 + \cdots + a_{f-1}p^{f-1} + a_{f-1} + \cdots + a_{f-2}p^{f-1} + \cdots) \\ &= \frac{1}{q-1} S(a)(1 + p + \cdots + p^{f-1}). \end{aligned}$$

Umstellen dieser Gleichung liefert

$$S(a) = \frac{q-1}{1 + p + \cdots + p^{f-1}} \sum_{i=0}^{f-1} \langle \frac{p^i a}{q-1} \rangle = (p-1) \sum_{i=0}^{f-1} \langle \frac{p^i a}{q-1} \rangle.$$

□

Lemma 4.5. $\sum_{a=1}^{q-2} S(a) = \frac{f(p-1)(q-2)}{2}$.

Beweis. Schreibe $a = a_0 + \cdots + a_{f-1}p^{f-1}$ mit $0 \le a_i < p$ wie in Definition 4.2. Dann gilt $q - 1 = (p-1) + (p-1)p + \cdots + (p-1)p^{f-1}$
$\Rightarrow q - 1 - a = p - 1 - a_0 + (p - 1 - a_1)p + \cdots + (p - 1 - a_{f-1})p^{f-1}$
$\Rightarrow S(a) + S(q-1-a) = a_0 + \cdots + a_{f-1} + (p - 1 - a_0) + \cdots + (p - 1 - a_{f-1})$
$= fp - f = f(p-1)$
$\Rightarrow 2\sum_{a=1}^{q-2} S(a) = \sum_{a=1}^{q-2} S(a) + S(q-1-a) = (q-2)f(p-1)$ □

Literatur

[1] K. Ireland, M. Rosen: A Classical Introduction to Modern Number Theory. 2. Auflage, Springer 1990.