

## 5. Proof of (3)

Objektyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **27 (1981)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **14.09.2024**

### **Nutzungsbedingungen**

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

### **Haftungsausschluss**

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Thus

$$(9) \quad \eta^n = \frac{\chi^{ln}(l) G_{fn}(\chi^\delta)}{G_{fn}(\chi^{\delta l})} \prod_{j=1}^{l-1} \frac{G_{fn}(\chi^\delta \psi^j)}{G_{fn}(\psi^j)}.$$

Since  $n \equiv \delta \pmod{q-1}$ ,  $\chi^{ln}(l) = \chi^{\delta l}(l)$ . Therefore, by (7), the right side of (9) equals 1, so

$$(10) \quad \eta^n = 1.$$

By the definition of  $\eta$  and of Gauss sums,

$$\eta^l \equiv \frac{\chi^{l^2}(l) \bar{\chi}^l(l) G_f(\chi^l)}{G_f^l(\chi^l)} \prod_{j=1}^e \prod_{k=1}^r \prod_{c=1}^{w^{r-k}} \frac{\bar{\chi}^{\delta l}(l) G_{fn}(\chi^{\delta l})}{1} \pmod{w},$$

so

$$\eta^l \equiv \frac{\chi^{l^2-l-l\delta(l-1)/n}(l) G_{fn}^{(l-1)/n}(\chi^{\delta l})}{G_f^{l-1}(\chi^l)} \pmod{w}.$$

By (6),  $G_{fn}(\chi^{\delta l}) = G_f^n(\chi^l)$ ; hence

$$(11) \quad \eta^l \equiv 1 \pmod{w}.$$

Thus  $w$  divides the norm  $N(\eta^l - 1)$ . By (10),  $\eta^l$  is an  $n$ -th root of unity. Thus if  $\eta^l - 1 \neq 0$ , then  $N(\eta^l - 1)$  divides  $n$ , which contradicts the fact that  $w + n$ . Therefore  $\eta^l = 1 = \eta^n$ , so since  $(l, n) = 1$ ,  $\eta = 1$ .

### 5. PROOF OF (3)

Let  $\eta$  denote the right side of (3). We assume that  $0 < \alpha < q - 1$ . To see that this presents no loss of generality, we now show that  $\eta$  is unchanged when  $\alpha$  is replaced by  $\alpha + (q-1)j$ , where  $j$  is an integer. Clearly  $G_f(\chi^\alpha)$  and  $\chi^\alpha(l)$  are unchanged, since the restriction  $\chi|_{GF(q)}$  has order  $q - 1$ . Finally,  $G_{fl}(\chi^{\alpha\beta})$  is also unchanged, as

$$(12) \quad G_{fl}(\chi^{\alpha\beta}) = G_{fl}(\chi^{\alpha\beta q^j}) = G_{fl}(\chi^{\beta(\alpha+j(q-1))}),$$

where  $\alpha_j$  is defined by  $\alpha_j \alpha \equiv j \pmod{l}$ ,  $\alpha_j \geq 0$ .

Let  $\psi = \chi^{\beta(q-1)}$ . Using (6), we have

$$\eta^l = \frac{G_{fl}(\chi^{\alpha\beta l})}{\chi^{\alpha l}(l) G_{fl}^l(\chi^{\alpha\beta})} \prod_{j=1}^{l-1} G_{fl}(\psi^j).$$

For each  $j \in \{0, 1, \dots, l - 1\}$ , we have, by (12),

$$G_{fl}(\chi^{\alpha\beta}) = G_{fl}(\chi^{\alpha\beta}\psi^j).$$

Thus,

$$(13) \quad \eta^l = \frac{G_{fl}(\chi^{\alpha\beta l})}{\chi^{\alpha l}(l)} \prod_{j=0}^{l-1} \frac{G_{fl}(\psi^j)}{G_{fl}(\chi^{\alpha\beta}\psi^j)}.$$

Since  $\chi^{\alpha l}(l) = \chi^{\alpha\beta l}(l)$ , the right side of (13) equals 1 by (7), so

$$(14) \quad \eta^l = 1.$$

Let  $P$  be the prime ideal above  $p$  in  $\mathcal{O} = Z[\omega]$ , where

$$\omega = \exp(2\pi i/p(q^l - 1)),$$

with  $P$  chosen such that  $\chi$  is the character of order  $q^l - 1$  on  $\mathcal{O}/P \approx GF(q^l)$  which maps the coset  $\omega + P$  to  $\bar{\omega}$ . To show that  $\eta = 1$ , it suffices to show that  $\eta \equiv 1 \pmod{P}$ . For, if  $\eta \not\equiv 1 \pmod{P}$ , then by (14), the norm  $N(\eta - 1)$  divides  $l$ ; but if also  $\eta \equiv 1 \pmod{P}$ , then  $p \mid N(\eta - 1)$ , which yields the contradiction  $p \mid l$ .

For any integer  $x$ , let  $L(x)$  denote the least nonnegative residue of  $x \pmod{l}$ . For integers  $i \geq 0$ , define

$$\varepsilon_i = \begin{cases} 1, & \text{if } 1 \leq L(i\alpha) \leq L(\alpha) \\ 0, & \text{otherwise,} \end{cases}$$

and

$$c_i = \varepsilon_i + l^{-1}(\alpha - L(\alpha) + (q - 1)L(-i\alpha)).$$

Note that each  $c_i$  is an integer with  $0 \leq c_i \leq q - 1$ . We have

$$\begin{aligned} l\alpha\beta - l \sum_{i=1}^l c_i q^{i-1} &= \sum_{i=1}^l q^{i-1} (\alpha - lc_i) \\ &= \sum_{i=1}^l q^{i-1} \{-l\varepsilon_i + L(\alpha) - L((1-i)\alpha) + L(-i\alpha)\}. \end{aligned}$$

The expressions in braces are easily seen to vanish. Thus we have the following explicit expansion of  $\alpha\beta$  in base  $q$ :

$$(15) \quad \alpha\beta = \sum_{i=1}^l c_i q^{i-1}.$$

By (8), (14), and the definition of  $\eta$ ,

$$(16) \quad \eta \equiv (u\gamma(\alpha))^{-1} l^{\alpha\gamma}(\alpha\beta) \pmod{P},$$

where

$$u = \prod_{j=1}^{l-1} \gamma(j(q-1)/l).$$

By (15) and (16),

$$\eta \equiv (u\gamma(\alpha))^{-1} l^\alpha \prod_{i=1}^l \gamma(c_i) \pmod{P}.$$

Thus by the second congruence in (8), there is an integer  $M$  such that

$$(17) \quad u\eta \equiv \frac{1}{\alpha!} l^\alpha (\zeta-1)^M \prod_{i=1}^l c_i! \pmod{P}.$$

First suppose that  $0 < \alpha < l$ . Then by (17) and the definition of  $c_i$ ,

$$\begin{aligned} u\eta &\equiv \frac{1}{\alpha!} l^\alpha (\zeta-1)^M \prod_{i=1}^l \left( \frac{q-1}{l} L(-i\alpha) \right)! \prod_{j=1}^\alpha \left( 1 + \frac{q-1}{l} (l-j) \right) \\ &\equiv (\zeta-1)^M \prod_{i=1}^l \left( \frac{q-1}{l} L(-i\alpha) \right)! \pmod{P}. \end{aligned}$$

By (14),  $\eta$  is a unit, so again applying the second congruence in (8), we find that

$$u\eta \equiv \prod_{i=1}^l \gamma\left(\frac{q-1}{l} L(-i\alpha)\right) \pmod{P}.$$

Since  $\alpha$  is prime to  $l$ , the numbers  $L(-i\alpha)$  run through a complete residue system  $\pmod{l}$  as  $i$  runs from 1 to  $l$ . Thus, by the definition of  $u$  following (16), we obtain the desired result  $\eta \equiv 1 \pmod{P}$  in the case  $0 < \alpha < l$ .

Finally, suppose that  $l < \alpha < q-1$ . We suppose as induction hypothesis that  $\eta' \equiv 1 \pmod{P}$ , where  $\eta'$  is obtained from  $\eta$  by replacing  $\alpha$  by  $\alpha-l$ . Then by (17) and the definition of  $c_i$ , there is an integer  $N$  such that

$$\begin{aligned} \eta &\equiv \eta/\eta' \equiv \frac{1}{\alpha!} (\zeta-1)^N (\alpha-l)! l^l \prod_{i=1}^l c_i \\ &= \frac{1}{\alpha!} (\zeta-1)^N (\alpha-l)! \prod_{i=1}^l \{l\varepsilon_i + \alpha - L(\alpha) + (q-1)L(-i\alpha)\} \pmod{P}. \end{aligned}$$

Since the numbers  $\{l\varepsilon_i - L(-i\alpha) + \alpha - L(\alpha)\}$  run through the  $l$  numbers  $\alpha, \dots, \alpha-l+1$  as  $i$  runs from 1 to  $l$ , we see that  $N = 0$  and  $\eta \equiv 1 \pmod{P}$ .