Algebra 1 – Blatt 10

Mona Scheerer und Nils Witt

Wintersemester 2020

Aufgabe 3.

Aufgabe 4. Seien p, q zwei verschiedene ungerade Primzahlen. Für zu q teilerfremdes $a \in \mathbb{Z}$ definieren wir das Legendre-Symbol durch

$$\left(\frac{a}{q}\right) := \begin{cases} 1, & \text{falls } a \mod q \in (\mathbb{F}_p^\times)^2 \\ -1, & \text{sonst} \end{cases}$$

(a) Wir zeigen, dass das Legendre multiplikativ ist, d.h. für $a, b \in \mathbb{Z}$ teilerfremd zu q gilt $\left(\frac{ab}{q}\right) = \left(\frac{a}{q}\right)\left(\frac{b}{q}\right)$ und zusätzlich

$$\left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}} = \begin{cases} 1, & \text{falls } q \equiv 1 \mod 4 \\ -1 & \text{falls } q \equiv 3 \mod 4 \end{cases}$$

Beweis. Sei q eine ungerade Primzahl. Nach Blatt 6 Aufgabe 3(c) gilt für $s \in \mathbb{F}_p^\times$, dass

$$s^{\frac{q-1}{2}} = \begin{cases} 1, & \text{falls } s \in (\mathbb{F}_q^\times)^2 \\ -1, & \text{falls } s \notin (\mathbb{F}_q^\times)^2 \end{cases}$$

Seien $a, b \in \mathbb{Z}$ zwei zu q teilerfremde ganze Zahlen und $\overline{a}, \overline{b} \in \mathbb{F}_p^\times$ deren Restklassen (da teilerfremd zu q sind sie $\neq 0$). Dann gilt

$$\begin{aligned} \overline{ab} \in (\mathbb{F}_q^\times)^2 &\iff (\overline{ab})^{\frac{q-1}{2}} \iff \overline{a}^{\frac{q-1}{2}}\overline{b}^{\frac{p-1}{2}} = 1 \\ &\iff (\overline{ab})^{\frac{q-1}{2}} \iff \overline{a}^{\frac{q-1}{2}}, \overline{b}^{\frac{p-1}{2}} = \pm 1 \\ &\iff \overline{a}^{\frac{q-1}{2}}, \overline{b}^{\frac{q-1}{2}} \in (\mathbb{F}_p^\times)^2 \text{ oder } \overline{a}^{\frac{q-1}{2}}, \overline{b}^{\frac{q-1}{2}} \notin (\mathbb{F}_p^\times)^2 \\ &\iff \left(\frac{a}{q}\right), \left(\frac{b}{q}\right) = 1 \text{ oder } \left(\frac{a}{q}\right), \left(\frac{b}{q}\right) = -1 \end{aligned}$$

Analog sieht man, dass

$$\overline{ab} \notin (\mathbb{F}_q^\times)^2 \iff \left(\frac{a}{q}\right) = 1, \left(\frac{b}{q}\right) = -1 \text{ oder } \left(\frac{a}{q}\right) = -1, \left(\frac{b}{q}\right) = 1$$

Das liefert uns die Multiplikativität des Legendresymbols. Ferner gilt wieder nach Blatt 6 Aufgabe 3 (c), dass

$$(-1)^{\frac{q-1}{2}} = \begin{cases} 1, & \text{falls } -1 \in (\mathbb{F}_q^\times)^2 \\ -1, & \text{falls } -1 \notin (\mathbb{F}_q^\times)^2 \end{cases}$$

was nach Definition mit $\left(\frac{-1}{q}\right)$ übereinstimmt. Ist $q \equiv 1 \mod 4$, dann gibt es ein $k \in \mathbb{Z}$ mit $q = 4k+1$ und es gilt

$$(-1)^{\frac{q-1}{2}} = (-1)^{\frac{4k+1-1}{2}} = 1$$

und analog, falls $q \equiv 3 \mod 4$ existiert ein $l \in \mathbb{Z}$ mit $q = 4k+3$ und es folgt

$$(-1)^{\frac{q-1}{2}} = (-1)^{\frac{4l+3-1}{2}} = (-1)^{\frac{2(2l+1)}{2}} = -1$$

was zu zeigen war. □

Sei nun L der Zerfällungskörper von $f = X^p - 1$ über $\mathbb{F}_q$ und $G = \mathrm{Gal}(L/\mathbb{F}_q)$ und wir betten die Galoisgruppe G wie immer (d.h. durch Wirkung auf den Nullstellen von f) via $G \hookrightarrow \mathfrak{S}_p$ ein.

(b) Das Bild von G in $\mathfrak{S}_p$ ist genau dann in $\mathfrak{A}_p$ enthalten, wenn

$$1 = (-1)^{\frac{p-1}{2}}(-1)^{\frac{q-1}{2}}\left(\frac{p}{q}\right)$$

Beweis. „⇒“: Nach Aufgabe 3(e) ist die Voraussetzung: Das Bild von G in $\mathfrak{S}_p$ ist enthalten in $\mathfrak{A}_p$ äquivalent zu $\Delta_f \in (\mathbb{F}_q^\times)^2$. Nach dem Hinweis gilt mit $n = p, b = 0, c = -1$, dass

$$\Delta_f = (-1)^{\frac{p(p-1)}{2}}((1-p)^{p-1} \cdot 0^p + p^p(-1)^{p-1}) = (-1)^{\frac{p(p-1)}{2}} p^p (-1)^{p-1} \in (\mathbb{F}_q^\times)^2$$

da p ungerade ist, ist $p-1$ gerade und wir haben

$$\Delta_f = (-1)^{\frac{p(p-1)}{2}} p^p = ((-1)^{\frac{p-1}{2}} p)^p \in (\mathbb{F}_q^\times)^2$$

Nach Definition und wegen der Multiplikativität des Legendresymbols gilt

$$\begin{aligned} 1 = \left(\frac{((-1)^{\frac{p-1}{2}}p)^p}{q}\right) = \left(\frac{p \cdot (-1)^{\frac{p-1}{2}}}{q}\right)^p &= \left(\left(\frac{p}{q}\right) \cdot \left(\frac{-1}{q}\right)^{\frac{p-1}{2}}\right)^p \\ &= \left(\left(\frac{p}{q}\right) \cdot (-1)^{\frac{q-1}{2}\cdot\frac{p-1}{2}}\right)^p \end{aligned}$$

Der Ausdruck in der Klammer ist eine ganze Zahl, deren p-te Potenz eins ist. Da p ungerade ist, tritt das dann und nur dann ein, wenn der Ausdruck selbst eins ist. Also ist

$$\left(\frac{p}{q}\right)(-1)^{\frac{q-1}{2}\cdot\frac{p-1}{2}} = 1$$

womit wir die Hinrichtung gezeigt haben.
„⇐“: Wir zeigen, dass $\Delta_f \in (\mathbb{F}_q^\times)^2$, was äquivalent zu dem ist, was wir zeigen wollen nach A3(e). Es berechnet sich Δ_f nach dem Hinweis zu

$$\Delta_f = (-1)^{\frac{p(p-1)}{2}} p^p (-1)^{p-1} = ((-1)^{\frac{p(p-1)}{2}} p)^p$$

und indem wir die Umformungen von oben rückwärtsdurchlaufen erhalten wir, dass $\Delta_f \in (\mathbb{F}_q^\times)^2$, was zu zeigen war. □

Sei $\sigma \in G$ der q-Frobenius, d.h. $\sigma(x) = x^q$ für alle $x \in L$. Nach Wahl einer primitiven p-ten Einheitswurzel ζ_p identifizieren wir die Nullstellen μ_p von f mit $\mathbb{Z}/p\mathbb{Z}$ und die von σ auf $\mathbb{Z}/p\mathbb{Z}$ induzierte Permutation π ist gerade die Multiplikation mit q, d.h. $\pi(a) = qa$ für $a \in \mathbb{Z}/p\mathbb{Z}$. Sei $k \coloneqq \operatorname{ord}_{(\mathbb{Z}/p\mathbb{Z})^\times}(q)$.

(c) Es gilt $\operatorname{sgn}(\pi) = (-1)^{(k-1)\cdot\frac{p-1}{k}}$.

Beweis. Da die Ordnung von q in $(\mathbb{Z}/p\mathbb{Z})^\times$ gerade k ist, enthält π den Zykel $(1\, q\, q^2 \cdots q^{k-1})$, weil $\pi(a) = qa$ für $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ nach der Vorbemerkung. Diesen Zykel schreiben wir als

$$(1\, q\, q^2 \cdots q^{k-1}) = (1\, q) \circ (q\, q^2) \circ (q^2\, q^3) \circ \cdots \circ (q^{k-2}\, q^{k-1})$$

also besteht der Zykel aus genau $k-1$ Transpostionen, daher ergibt sich für das Signum

$$\operatorname{sgn}((1\, q\, q^2 \cdots q^{k-1})) = \prod_{i=0}^{k-2} \operatorname{sgn}((q^i\, q^{i+1})) = (-1)^{k-1}$$

Wegen dem Satz von Lagrange gibt es genau $\frac{\operatorname{ord}(\mathbb{F}_p^\times)}{\operatorname{ord}(q)} = \frac{p-1}{k}$ verschiedene Restklassen in $(\mathbb{Z}/p\mathbb{Z})/\langle q\rangle$. Sei $n \coloneqq (p-1)/k$. Dann gibt es genau n Restklassen $r_1\langle q\rangle, \ldots, r_n\langle q\rangle$ mit $r_1, \ldots, r_n \in \mathbb{Z}/p\mathbb{Z}$ einem Vertretersystem. Die Restklassen entsprechen genau Zykeln der Länge k, denn nach Definition ist $r_i\langle q\rangle = \{r_i q^n \mid n = 0, \ldots, k-1\}$ und das sind genau die Elemente im Zyklus $(r_i\, r_i q \cdots r_i q^{k-1})$ die r_i liegen in verschiedenen Zyklen, weil die Restklassen disjunkt sind. Weil $\mathbb{Z}/p\mathbb{Z}$ disjunkt in die Restklassen modulu q zerfällt liegt auch jedes Element von $\mathbb{Z}/p\mathbb{Z}$ in einer Restklasse, d.h. in einem Zyklus. π ist also die Komposition von $\frac{p-1}{k}$ Zyklen der Länge $k-1$. Da $\operatorname{sgn} : \mathfrak{S}_p \to \{\pm 1\}$ ein Gruppenhomomorphismus ist, folgt die Behauptung. □

(d) Folgern Sie aus (c), dass das Bild von G in $\mathfrak{S}_p$ genau dann in $\mathfrak{A}_p$ enthalten ist, wenn

$$1 = \left(\frac{q}{p}\right)$$

und folgern sie dann das quadratische Reziprozitätsgesetz.

Beweis. Wir wissen, dass $G = \langle\sigma\rangle$, wobei $\sigma \in G$ der q-Frobenius ist. Dann ist das Bild von G in $\mathfrak{S}_p$ in $\mathfrak{A}_p$ enthalten genau dann, wenn das Bild von σ, also π in $\mathfrak{S}_n$ in $\mathfrak{A}_n$ enthalten ist, d.h. genau dann, wenn $\operatorname{sgn}(\pi) = 1$.
Nach (c) gilt dann

$$\begin{aligned}\pi \in \mathfrak{A}_p &\iff \operatorname{sgn}(\pi) = 1 \iff (-1)^{(k-1)\cdot\frac{p-1}{k}} = 1\\ &\iff (k-1)\cdot\frac{p-1}{k} \text{ gerade} \iff k\cdot\frac{p-1}{k} - \frac{p-1}{k} \text{ gerade}\\ &\iff \frac{p-1}{k} \text{ gerade}\end{aligned}$$

die letzte Äquivalenz gilt, weil $p-1$ gerade ist. Dann existiert ein $s \in \mathbb{Z}$ mit

$$\frac{p-1}{k} = 2s \iff ks = \frac{p-1}{2} \implies q^{\frac{p-1}{2}} - 1 = (q^k)^s - 1 = 0$$

also ist q eine Nullstelle von $X^{\frac{p-1}{2}} - 1 \in \mathbb{F}_p[X]$, was äquivalent dazu ist, dass $q \in (\mathbb{F}_p^\times)^2$.
Ist andererseits q eine Nullstelle von $X^{\frac{p-1}{2}} - 1$, dann $k = \operatorname{ord}_{(\mathbb{Z}/p\mathbb{Z})^\times}(q) \mid \frac{p-1}{2}$, denn: angenommen das wäre nicht der Fall, dann gäbe es $s, r \in \mathbb{Z}$ mit $0 < r < k$ und

$$\frac{p-1}{2} = s\cdot k + r \implies 1 = q^{\frac{p-1}{2}} = (q^k)^s \cdot q^r = q^r$$

da $r < k$ und k die Ordnung von q ist, ist das ein Widerspruch. Also teilt k doch $\frac{p-1}{2}$.
Also ist q ein Quadrat in $(\mathbb{F}_p)^\times$ genau dann, wenn $k \mid (p-1)/2$. Dann können wir aber die obigen Äquivalenzen auch rückwärtsdurchlaufen und erhalten, dass $q \in (\mathbb{F}_p^\times)^2$ genau dann, wenn $\pi \in \mathfrak{A}_p$ genau dann, wenn das Bild von G in $\mathfrak{S}_p$ in $\mathfrak{A}_p$ enthalten ist.
Zusammen mit Teil (b) haben wir die folgenden Äquivalenzen

$$\begin{aligned}&\text{Bild von } G \text{ in } \mathfrak{S}_p \text{ in } \mathfrak{A}_p \text{ enthalten} \iff\\ &1 = \left(\frac{p}{q}\right)\cdot(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \iff \left(\frac{q}{p}\right) = 1\end{aligned}$$

Nach Teil (a) erhalten wir

$$(-1)^{\frac{q-1}{2}\frac{p-1}{2}} = \left((-1)^{\frac{q-1}{2}}\right)^{\frac{p-1}{2}} = \begin{cases}-1, & \text{falls } \frac{p-1}{2}, \frac{q-1}{2} \notin 2\mathbb{Z} \Leftrightarrow q, p \equiv 3 \mod 4\\ 1 & \text{sonst}\end{cases}$$

Und es gilt weil das Produkt von $\left(\frac{p}{q}\right)$ und $(-1)^{\frac{q-1}{2}\frac{p-1}{2}}$ gerade eins sein muss, dass

$$\left(\frac{p}{q}\right) = \begin{cases} -1, & p, q \equiv 3 \mod 4 \\ 1, & \text{sonst} \end{cases}$$

und das ist genau dann der Fall, wenn $\left(\frac{q}{p}\right) = 1$. Insgesamt erhalten damit, dass

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = \begin{cases} -1, & p, q \equiv 3 \mod 4 \\ 1, & \text{sonst} \end{cases}$$

was gerade die Aussage des quadratischen Reziprozitätsgesetzes ist. □