

Algebra 1 – Blatt 10

Mona Scheerer und Nils Witt

Wintersemester 2020

Aufgabe 1. Es sei $f = X^4 + 2X^2 + 2 \in \mathbb{F}_3[X]$. Man bestimme einen Zerfällungskörper L von f über \mathbb{F}_3 sowie die Galoisgruppe und alle Zwischenkörper.

Beweis. Wir zeigen zuerst, dass f irreduzibel ist. Dazu beobachten wir zwei Dinge

- (i) f hat keine Nullstelle in \mathbb{F}_3 , denn

$$f(0) = 0^4 + 2 \cdot 0^2 + 2 = 2 \neq 0$$

$$f(1) = 1 + 2 + 2 = 5 = 2 \neq 0$$

$$f(2) = 2^4 + 2^3 + 2 = 16 + 8 + 2 = 26 = 2 \neq 0$$

daher kann f nicht in einen linearen Faktor und ein kubisches Polynom zerfallen.

- (ii) f hat keine Faktorisierung in quadratische Polynome. Angenommen, das wäre so, dann gäbe es $X^2 + a_1X + b_1, X^2 + a_2X + b_2 \in \mathbb{F}_3[X]$ mit

$$\begin{aligned} f &= X^4 + 2X^2 + 2 = (X^2 + aX + b)(X^2 + cX + d) \\ &= X^4 + (a_1 + a_2)X^3 + (b_2 + a_1a_2 + b_1)X^2 + (a_1b_2 + a_2b_1)X + b_1b_2 \end{aligned}$$

Daraus folgt mit Koeffizientenvergleich

$$a_1 + a_2 = 0 \implies a_1 = -a_2 \tag{1}$$

$$b_2 + a_1a_2 + b_1 = 2$$

$$a_1b_2 + a_2b_1 = 0 \xrightarrow{(1)} a_2(b_1 - b_2) = 0 \tag{2}$$

$$b_1b_2 = 2$$

Aus (2) folgt $a_2 = 0$ oder $b_1 - b_2 = 0$. Angenommen $a_2 = 0$. Dann ist $b_1 + b_2 = 2$ und $b_1b_2 = 2$. $b_1, b_2 \neq 0$, weil $b_1b_2 \neq 0$. Ist $b_1 = 1$, dann muss $b_2 = 2 - 1 = 1$, dann ist aber $b_1b_2 = 1 \neq 2$. Analog für $b_2 = 1$. Ist $b_1 = 2$, so ist $b_2 = 0$, also $b_1b_2 = 0 \neq 2$. Analog, falls $b_2 = 2$. Also ist $a_2 \neq 0$ und $b_1 = b_2$. Dann gilt aber $b_1b_2 = b_1^2 = 2$. Aber für $0^2, 1^2, 2^2 \neq 2$ also gibt es kein Element in \mathbb{F}_3 dessen Quadrat 2 ist. Also muss f irreduzibel sein.

Sei nun $\alpha \in \overline{\mathbb{F}_3}$ eine Nullstelle von f . Behauptung: Die Nullstellen von f sind dann gerade $\{\pm\alpha, \pm\sqrt{2}/\alpha\}$, wobei $\sqrt{2}$ wieder eine Nullstelle von $X^2 - 2 \in \mathbb{F}_3[X]$ in $\overline{\mathbb{F}_3}$ meint.

Tasächlich: $f(-\alpha) = 0$, denn in f hat nur gerade Potenzen von X . Und es gilt

$$f\left(\frac{\sqrt{2}}{\alpha}\right) = \frac{4}{\alpha^4} + 2 \cdot \frac{2}{\alpha^2} + 2 = \frac{2 \cdot (\alpha^4 + 2\alpha^2 + 2)}{\alpha^4} = 0$$

und für $-\sqrt{2}/\alpha$ wieder weil nur gerade Potenzen von X in f vorkommen. Behauptung: Es gilt $\sqrt{2} \in \mathbb{F}_3(\alpha)$. Denn es gilt

$$(\alpha^2 + 1)^2 - 2 = \alpha^4 + 2\alpha^2 + 1 - 2 = \alpha^4 + 2\alpha^2 - 1 = \alpha^4 + 2\alpha^2 + 2 = f(\alpha) = 0$$

Also ist $\alpha^2 + 1$ eine Nullstelle von $X^2 - 2 \in \mathbb{F}_3[X]$ nach Definition gilt dann $\alpha^2 + 1 = \sqrt{2}$, da die $\sqrt{2}$ nach Wahl eines algebraischen Abschlusses von \mathbb{F}_3 eindeutig festgelegt ist.

Daher ist $\mathbb{F}_3(\sqrt{2}, \alpha) = \mathbb{F}_3(\alpha)$ ein Zerfällungskörper von f über \mathbb{F}_3 , da alle Nullstellen darin liegen (das haben wir ja gerade gezeigt) und er auch gerade durch Adjunktion der Nullstellen entsteht.

Sei nun $L = \mathbb{F}_3(\alpha)$. Es ist L/\mathbb{F}_3 einfach und algebraisch und da f irreduzibel und normiert ist, ist f das Mipo von α . Daher gilt $[L : \mathbb{F}_3] = 4$. Als endliche Erweiterung endlicher Körper ist L/\mathbb{F}_3 endlich galoissch. Ferner ist wird die Galoisgruppe vom Frobenius $\sigma : L \rightarrow L, a \mapsto a^3$ erzeugt, ist also zyklisch, von der Ordnung vier. Insgesamt haben wir also $G := \text{Gal}(L/\mathbb{F}_3) = \langle \sigma \rangle \simeq \mathbb{Z}/4\mathbb{Z}$. Wir wissen, dass $\mathbb{Z}/4\mathbb{Z}$ nur eine nicht-triviale Untergruppe hat, nämlich $H := \langle \sigma^2 \rangle \subset \mathbb{Z}/4\mathbb{Z}$.

Wir haben die folgenden Elemente der Galoisgruppe, denn da f irreduzibel wirkt die Galoisgruppe transitiv auf den Nullstellen von f

- (1) $\sigma_1 : L \rightarrow L$ mit $\alpha \mapsto \alpha$
- (2) $\sigma_2 : L \rightarrow L$ mit $\alpha \mapsto -\alpha$
- (3) $\sigma_3 : L \rightarrow L$ mit $\alpha \mapsto \sqrt{2}/\alpha$.
- (4) $\sigma_4 : L \rightarrow L$ mit $\alpha \mapsto -\sqrt{2}/\alpha$.

Das Element σ_2 hat die Ordnung zwei, sein Fixkörper ist also gerade quadratisch über \mathbb{F}_3 und ist also isomorph zu \mathbb{F}_9 , weil es bis auf Isomorphie genau einen Körper gibt, der quadratisch über \mathbb{F}_3 ist. Sei E ein echter Zwischenkörper von L/\mathbb{F}_3 , dann gilt $[E : \mathbb{F}_3] \mid [L : \mathbb{F}_3] = 4$ und da $[E : \mathbb{F}_3] \neq 1, 4$, folgt $[E : \mathbb{F}_3] = 2$. Da es aber bis auf Isomorphie nur einen Zwischenkörper gibt, der über \mathbb{F}_3 quadratisch ist, folgt, dass L/\mathbb{F}_3 die Zwischenkörper: $L, \mathbb{F}_3, \mathbb{F}_9$ hat. Wir können L konkreter angeben, nämlich ist $[L : \mathbb{F}_3] = 4$, also ist $L \simeq \mathbb{F}_{81}$ und wir haben somit auch einen konkreten Zerfällungskörper von f angegeben. \square

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

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

- (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

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

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 $\bar{a}, \bar{b} \in \mathbb{F}_p^\times$ deren Restklassen (da teilerfremd zu q sind sie $\neq 0$). Dann gilt

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

Analog sieht man, dass

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

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 $q \equiv 1 \pmod{4}$, 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 $q \equiv 3 \pmod{4}$ 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 $G = \text{Gal}(L/\mathbb{F}_q)$ 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. „ \Rightarrow “: 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.

„ \Leftarrow “: 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

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

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

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 $k := \text{ord}_{(\mathbb{Z}/p\mathbb{Z})^\times}(q)$.

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

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

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

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

$$\text{sgn}((1 \ q \ q^2 \ \dots \ q^{k-1})) = \prod_{i=0}^{k-2} \text{sgn}((q^i \ q^{i+1})) = (-1)^{k-1}$$

Wegen dem Satz von Lagrange gibt es genau $\frac{\text{ord}(\mathbb{F}_p^\times)}{\text{ord}(q)} = \frac{p-1}{k}$ verschiedene Restklassen in $(\mathbb{Z}/p\mathbb{Z})/\langle q \rangle$. Sei $n := (p-1)/k$. Dann gibt es genau n Restklassen $r_1 \langle q \rangle, \dots, r_n \langle q \rangle$ mit $r_1, \dots, r_n \in \mathbb{Z}/p\mathbb{Z}$ einem Vertretersystem. Die Restklassen entsprechen genau Zykeln der Länge k , denn nach Definition ist $r_i \langle q \rangle = \{r_i q^n \mid n = 0, \dots, k-1\}$ und das sind genau die Elemente im Zyklus $(r_i \ r_i q \ \dots \ r_i q^{k-1})$ die r_i liegen in verschiedenen Zyklen, weil die Restklassen disjunkt sind. Weil $\mathbb{Z}/p\mathbb{Z}$ disjunkt in die Restklassen modulo 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 $\text{sgn} : \mathfrak{S}_p \rightarrow \{\pm 1\}$ ein Gruppenhomomorphismus ist, folgt die Behauptung. \square

(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 $\text{sgn}(\pi) = 1$.

Nach (c) gilt dann

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

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 $k = \text{ord}_{(\mathbb{Z}/p\mathbb{Z})^\times}(q) \mid \frac{p-1}{2}$, 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

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

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

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

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

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

was gerade die Aussage des quadratischen Reziprozitätsgesetzes ist. \square