Algebra 1 – Blatt 11

Simon Paege

22. Dezember 2021

(1)
- Für alle $x \in k$ ist $1 \cdot x = x = x \cdot 1$, also $1 \in Z$. Insbesondere $Z \neq \emptyset$.
- Seien $a, b \in Z$. Für $x \in k$ gilt dann $x(a-b) = xa - xb = ax - bx = (a-b)x$. Also ist $a - b \in Z$. Damit ist Z eine additive Untergruppe von k.
- Seien $a, b \in Z$. Für $x \in k$ gilt dann $xab = axb = abx$, also $ab \in Z$. Damit ist Z ein Unterring von k.
- Sei $a \in Z$ mit $a \neq 0$. Dann gilt $xa^{-1} = a^{-1}axa^{-1} = a^{-1}xaa^{-1} = a^{-1}x$, also $a^{-1} \in Z$. Damit ist Z ein Teilschiefkörper von k.

Offensichtlich ist Z kommutativ, also ein Körper. Mit k ist auch Z endlich, also ist Z ein endlicher Körper.

(2) k wird zu einem Z-Vektorraum durch die Addition $k \times k \to k, (x, y) \mapsto x + y$ und die skalare Multiplikation $Z \times k \to k, (a, x) \mapsto ax$, die schon durch die Schiefkörperstruktur von k gegeben sind. Die Vektorraumaxiome folgen direkt aus den Schiefkörperaxiomen.

Da k endlich ist, gibt es ein endliches Erzeugendensystem von k als Z-Vektorraum. Also ist $n = \dim_Z k < \infty$. Nun ist $k \cong Z^n$ als Vektorräume, also $|k| = |Z|^n = q^n$. Es ist $q > 0$, denn sonst wäre $|k| = 1$, aber k enthält mit 0 und 1 zwei verschiedene Elemente.

(3)
- $1 \cdot x = x = x \cdot 1$, also $1 \in k_x$. Insbesondere ist $k_x \neq \emptyset$.
- Seien $a, b \in k_x$. Dann ist $x(a-b) = xa - xb = ax - bx = (a-b)x$, also $a - b \in k_x$. Damit ist k_x eine additive Untergruppe von k.
- Seien $a, b \in k_x$. Dann ist $xab = axb = abx$, also $ab \in k_x$. Damit ist k_x ein Unterring von k.
- Sei $a \in k_x$ mit $a \neq 0$. Dann ist $xa^{-1} = a^{-1}axa^{-1} = a^{-1}xaa^{-1} = a^{-1}x$, also $a^{-1} \in k_x$. Damit ist k_x ein Teilschiefkörper von k.

$$\begin{aligned} k_x &= \{y \in k = k^\times \cup \{0\} : yx = xy\} \\ &= \{0\} \cup \{y \in k^\times : yx = xy\} \\ &= \{0\} \cup \{y \in k^\times : yxy^{-1} = x\} \\ &= \{0\} \cup \operatorname{Stab}(x) \end{aligned}$$

(4) **Mit Vektorräumen über Schiefkörpern** Genau wie in (2) zeigt man, dass k ein Vektorraum (= Linksmodul) über k_x ist. Genau wie im kommutativen Fall kann man zeigen, dass jeder Vektorraum über einem Schiefkörper eine Basis hat. Da k endlich, also endlich-dimensional über k_x ist, hat man also $k \cong k_x^m$ als k_x-Vektorräume für ein $m \in \mathbb{N}_0$. Es folgt

$$q^n = |k| = |k_x|^m = \left(q^d\right)^m = q^{md} \Longrightarrow n = md.$$

Also $d \mid n$.

Mit Lagrange Da k_x ein Teilschiefkörper von k ist, ist $k_x^\times$ eine Untergruppe von $k^\times$. Nach Lagrange ist $|k_x^\times| = q^d - 1$ ein Teiler von $|k^\times| = q^n - 1$. Schreibe $n = md + r$ mit $0 \leq r < d$. Dann ist $q^d - 1$ auch ein Teiler von

$$(q^d - 1) \cdot q^r \sum_{i=0}^{m-1} q^{id} = q^r(q^{md} - 1) = q^n - q^r$$

Also ist $q^d - 1$ auch ein Teiler von $(q^n - 1) - (q^n - q^r) = q^r - 1$. Wegen $0 \leq q^r - 1 < q^d - 1$ ist $q^r - 1 = 0$, als $r = 0$ und $n = md$.

(5)

$$|\omega(x)| = (k^\times : \mathrm{Stab}(x)) = (k^\times : k_x^\times) = \frac{q^n - 1}{q^d - 1}$$

Keine Ahnung, wofür (4) hier gut sein soll.

(6) Sei hier $x \notin Z$, sonst klappt es nicht.

Nach (4) ist $d \mid n$, also ist $X^d - 1 \mid X^n - 1$ in $Z[X]$ (Quotient ist $\sum_{i=0}^{\frac{n}{d}} X^{id}$). Wegen $X^n - 1 = \prod_{m|n} \Phi_m$ ist Φ_n ein Teiler von $X^n - 1$. Zeige noch, dass Φ_n nicht $X^d - 1$ teilt. Dann folgt $\Phi_n \mid \frac{X^n-1}{X^d-1}$. Jetzt q einsetzen, fertig.

Angenommen, es ist $\Phi_n \mid X^d - 1 = \prod_{m|d} \Phi_m$. Die Φ_j sind alle normiert und irreduzibel, also folgt $\Phi_n = \Phi_m$ für ein $m \mid d$. Das geht nur für $n = m$, also $n \mid d$. Nach (4) ist $d \mid n$, also $d = n$. Dann ist $k_x = k$, also $x \in Z$. Widerspruch!

(7) Ein Element aus $k^\times$ bildet genau dann eine Bahn der Länge 1, wenn es mit allen $x \in k^\times$ kommutiert. Das bedeutet gerade, dass es in Z liegt. Die Bahnen der Länge 1 entsprechen also den Elementen aus $k^\times \cap Z = Z^\times$.

Sei V ein Vertretersystem der Bahnen der Länge > 1. Da $k^\times$ in eine disjunkte Vereiningung der Bahnen zerfällt, gilt dann

$$k^\times = \biguplus_{x \in V \cup Z^\times} \omega(x)$$

$$|k^\times| = \sum_{x \in V \cup Z^\times} |\omega(x)| = \sum_{x \in Z^\times} 1 + \sum_{x \in V} |\omega(x)|$$

(8) Sei $V = \{x_i : 1 \leq i \leq r\}$. Nach (5) ist $|\omega(x_i)| = \frac{q^n-1}{q^{d_i}-1}$ für einen Teiler d_i von n. Wegen $|\omega(x_i)| > 1$ ist $d_i \neq n$, also ist d_i ein echter Teiler. Dann folgt aus (7):

$$q^n - 1 = q - 1 + \sum_{i=1}^{r} \frac{q^n - 1}{q^{d_i} - 1}$$

(9) Hier braucht man zusätzlich $\zeta \neq 1$.

Wegen $|\zeta| = 1$ und $\zeta \neq 1$ ist $\Re\zeta < 1$.

$$|q - \zeta|^2 = (q - \zeta)(q - \bar{\zeta}) = q^2 - 2q\Re\zeta + |\zeta|^2 > q^2 - 2q + 1 = (q - 1)^2$$

Damit folgt $|q - \zeta| > q - 1$ (brauchen wir gleich noch). Wegen $q \geq 2$ folgt $|q - \zeta| > 1$.

(10) Nach (9) gibt es ein $a \in \mathbb{Z}$ mit $a\Phi_n(q) = q - 1$. Sei ζ eine primitive n-te Einheitswurzel über $\mathbb{Q}$. Dann ist $\Phi_n(q) = \prod_{i \in (\mathbb{Z}/n\mathbb{Z})^\times} (X - \zeta^i)$.

$$q - 1 = |a| \cdot |\Phi_n(q)| = |a| \cdot |q - \zeta| \prod_{i \neq 1} |q - \zeta^i| > |a| \cdot (q - 1) \cdot 1$$

Also ist $a = 0$ und damit $q - 1 = 0 \cdot \Phi_n(q) = 0$. Widerspruch!