

Übungen zur Algebra I

Blatt 4

Aufgabe 13 (2+2+2)

Beweisen Sie die folgenden Ableitungsregeln für Polynome φ, ψ über einem Körper K :

- (i) $(\varphi + \psi)' = \varphi' + \psi'$;
- (ii) $(\varphi\psi)' = \varphi'\psi + \varphi\psi'$;
- (iii) $(\varphi \circ \psi)' = (\varphi' \circ \psi)\psi'$.

Aufgabe 14 (2+2)

Sei K ein endlicher Körper und $q := |K|$ ungerade. Zeigen Sie:

- (i) Für $a \in K \setminus \{0\}$ ist $a^{(q-1)/2} = \pm 1$.
- (ii) Dabei gilt $a^{(q-1)/2} = 1$ genau dann, wenn ein $b \in K$ mit $b^2 = a$ existiert.

Aufgabe 15 (2)

Zeigen Sie, dass für jeden Körper K und alle $m, n \in \mathbb{N}$ im Polynomring $K[X]$ gilt:

$$\text{ggT}(X^m - 1, X^n - 1) = X^{\text{ggT}(m,n)} - 1 .$$

Aufgabe 16 (2)

Stellen Sie die Additions- und Multiplikationstabelle für einen Körper mit 9 Elementen auf.

Aufgabe 17 (4)

Geben Sie die irreduziblen Polynome der Grade 1,2,3,4 in $\mathbb{F}_2[X]$ an.