

ÜBUNGSAUFGABEN ZUR ALGEBRA (BACHELOR)

Blatt 14
ohne Abgabe

54. (a) Zeigen Sie, dass das Polynom $f = x^3 + 6x^2 - 12x + 2$ irreduzibel über \mathbb{Q} ist.
(b) Zeigen Sie, dass f auch über $\mathbb{Q}(\sqrt[5]{2})$ irreduzibel ist.
55. Sei $f = x^3 + x + 1 \in \mathbb{F}_2[x]$.
- (a) Beweisen Sie, dass der Ring $K = \mathbb{F}_2[x]/\langle f \rangle$ ein Körper ist.
(b) Finden Sie einen Erzeuger der Gruppe K^* .
(c) Berechnen Sie das Inverse von $x + \langle f \rangle$ in K .
56. Sei $\zeta = (1\ 2\ \dots\ n) \in S_n$ ein Zykel der Länge n und sei $\sigma \in S_n$. Zeigen Sie, dass $\zeta\sigma = \sigma\zeta$ genau dann gilt, wenn $\sigma = \zeta^k$ für ein $k \in \mathbb{N}_0$ gilt. Stimmt die gleiche Aussage auch für einen Zykel der Länge $n - 1$?
57. Es sei G eine Gruppe und seien H und K zwei Untergruppen von G . Zeigen Sie: Für $x, y \in G$ ist $xH \cap yK$ entweder leer oder eine Linksnebenklasse von $H \cap K$ in G .
58. Es sei $L = \mathbb{Q}(\alpha, \omega)$ mit $\alpha^3 = 2$ und $\omega = \frac{-1 + \sqrt{-3}}{2}$. Zeigen Sie:
- (a) Die Erweiterung $\mathbb{Q} \subset L$ hat Grad 6 und eine \mathbb{Q} -Basis von L ist durch $1, \alpha, \alpha^2, \omega, \omega\alpha, \omega\alpha^2$ gegeben. (*Hinweis:* Berechnen Sie als erstes ω^2 und ω^3 .)
(b) Das Element $\gamma = \alpha + \omega$ ist ein primitives Element von $\mathbb{Q} \subset L$.
(*Vorschlag:* Zeigen Sie, dass $1, \gamma, \gamma^2, \gamma^3$ linear unabhängig über \mathbb{Q} sind.)

Lösungen.

54. (a) Das Polynom f ist ein Eisenstein-Polynom zur Primzahl 2.
(b) Das Polynom $x^5 - 2$ ist irreduzibel über \mathbb{Q} . Deshalb hat $\mathbb{Q}(\sqrt[5]{2})$ den Grad 5 über \mathbb{Q} . Wäre f reduzibel in $\mathbb{Q}(\sqrt[5]{2})$, dann müsste f dort eine Nullstelle α haben (denn ein kubisches Polynom ist genau dann reduzibel, wenn es eine Nullstelle besitzt). In diesem Fall hätte $\mathbb{Q}(\alpha)$ den Grad 3 über \mathbb{Q} . Aus $\alpha \in \mathbb{Q}(\sqrt[5]{2})$ würde dann

$$5 = [\mathbb{Q}(\sqrt[5]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[5]{2}) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[5]{2}) : \mathbb{Q}(\alpha)] \cdot 3$$

folgen, ein Widerspruch.

55. (a) Das Polynom $f = x^3 + x + 1$ ist irreduzibel über \mathbb{F}_2 , denn es hat Grad 3 und keine Nullstelle. Der Faktorring $\mathbb{F}_2[x]/\langle f \rangle$ ist deshalb die Körpererweiterung $K = \mathbb{F}_2(\alpha)$, die durch Adjunktion der Nullstelle $\alpha = x + \langle f \rangle$ entsteht.

(b) Weil f den Grad 3 hat, hat K den Grad 3 über \mathbb{F}_2 und damit $2^3 = 8$ Elemente. Die multiplikative Gruppe K^* ist deshalb zyklisch der Ordnung 7. Sie wird also von jedem Element ungleich 1 in K^* erzeugt, zum Beispiel von $\alpha = x + \langle f \rangle$.

(c) Da f irreduzibel ist, sind x und f teilerfremd. Es gilt also $\text{ggT}(f, x) = 1$ und damit gibt es eine Darstellung $pf + qx = 1$ mit $p, q \in \mathbb{F}_2[x]$. Eine solche können wir durch Division mit Rest oder einfach durch Hinschauen bestimmen, nämlich $1 \cdot f - (x^2 + 1)x = 1$. Damit ist $(x^2 + 1) + \langle f \rangle = \alpha^2 + 1$ ein Inverses von $\alpha = x + \langle f \rangle$ in K .

56. Sei $\zeta = (1\ 2\ \dots\ n)$. Die eine Richtung ist klar, denn es gilt $\zeta\zeta^k = \zeta^{k+1} = \zeta^k\zeta$ für alle $k \in \mathbb{N}_0$. Sei umgekehrt $\sigma \in S_n$ mit $\sigma\zeta = \zeta\sigma$, also äquivalent mit $\sigma\zeta\sigma^{-1} = \zeta$. Dann ist $\sigma\zeta\sigma^{-1}$ wieder ein n -Zykel, nämlich

$$\sigma\zeta\sigma^{-1} = (\sigma(1)\ \sigma(2)\ \dots\ \sigma(n)).$$

(Denn es gilt $(\sigma\zeta\sigma^{-1})(\sigma(i)) = \sigma(\zeta(i)) = \sigma(i+1)$ für alle $i \in \{1, \dots, n\}$, wobei die Addition modulo n zu lesen ist.) Der Zyklus $(\sigma(1), \dots, \sigma(n))$ stimmt genau dann mit $(1\ 2\ \dots\ n)$ überein, wenn die Einträge zyklisch vertauscht sind, also genau dann, wenn $\sigma = \zeta^k$ für ein k gilt.

Das Gleiche stimmt auch für $\zeta = (1\ 2\ \dots\ n-1)$ mit dem gleichen Argument, denn σ muss dann $(1, \dots, n-1)$ zyklisch vertauschen und es folgt $\sigma(n) = n$.

57. Angenommen $xH \cap yK \neq \emptyset$. Dann gibt es $z \in xH \cap yK$, etwa $z = xh = yk$ mit $h \in H$, $k \in K$. Behaupte, dass

$$xH \cap yK = z(H \cap K)$$

gilt. Denn ist $z' = xh' = yk' \in xH \cap yK$ (mit $h' \in H$, $k' \in K$), dann folgt $z^{-1}z' = h^{-1}x^{-1}xh' = h^{-1}h' \in H$ und $z^{-1}z' = k^{-1}x^{-1}xk' = k^{-1}k' \in K$, also $z^{-1}z' \in H \cap K$ und damit $z' \in z(H \cap K)$. Also gilt $xH \cap yK \subset z(H \cap K)$.

Ist umgekehrt $g \in H \cap K$, dann $zg = xhg = ykg \in xH \cap yK$, also $z(H \cap K) \subset xH \cap yK$.

58. (a) Sei $K = \mathbb{Q}(\alpha)$. Es gilt $\omega + \omega^2 = -1$, also $\omega^2 = -\omega - 1$. Die Erweiterung $K \subset L = K(\omega) = K(\sqrt{-3})$ hat Grad 2 und $1, \omega$ ist eine K -Basis von L . Außerdem ist $1, \alpha, \alpha^2$ eine \mathbb{Q} -Basis von $\mathbb{Q}(\alpha)$. Deshalb bilden die Produkte $1, \alpha, \alpha^2, \omega, \omega\alpha, \omega\alpha^2$ eine Basis von L über \mathbb{Q} .

(b) Wegen $\omega^2 = -\omega - 1$ gilt $\omega^2\alpha = -\omega\alpha - \alpha$. Wir berechnen

$$\gamma^2 = (\alpha + \omega)^2 = \alpha^2 + 2\alpha\omega + \omega^2 = -1 + \alpha^2 - \omega + 2\omega\alpha$$

$$\gamma^3 = (\alpha + \omega)^3 = \alpha^3 + 3\omega\alpha^2 + 3\omega^2\alpha + \omega^3 = 3 - 3\alpha - 3\omega\alpha + 3\omega\alpha^2.$$

In der \mathbb{Q} -Basis $1, \alpha, \alpha^2, \omega, \omega\alpha, \omega\alpha^2$ werden die Elemente $1, \gamma, \gamma^2, \gamma^3$ deshalb dargestellt durch die Zeilenvektoren der Matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ -1 & 0 & 1 & -1 & 2 & 0 \\ 3 & -3 & 0 & 0 & -3 & 3 \end{pmatrix}.$$

Man sieht direkt (aufgrund der Stufenform), dass diese 4 Vektoren linear unabhängig über \mathbb{Q} sind.

Es kann also kein Polynom $g \in \mathbb{Q}[x]$ vom Grad ≤ 3 mit $g(\alpha + \omega) = 0$ geben. Der Grad von $\alpha + \omega$ über \mathbb{Q} muss aber ein Teiler von 6 sein. Also hat das Minimalpolynom von $\alpha + \omega$ über \mathbb{Q} den Grad 6 und es folgt $\mathbb{Q}(\alpha + \omega) = L$.