T U ¨ B
Fakultät II – Institut für Mathematik
Prof. Stefan Felsner
Andreas Paffenholz

Diskrete MAFI
Sommersemester 2005

Wiebke Höhn
Raman Sanyal
Xiumei Wang

D M ¨ I
P ¨

Bearbeitung am 22./23. Juni 2005 in den Tutorien

A 1.

Ein *Gruppenhomomorphismus* ist eine Abbildung $\varphi : G \to G$, der die Gruppenoperation respektiert, also für alle $a, b \in G$ gilt, dass $\varphi(ab) = \varphi(a)\varphi(b)$.

- Zeigen Sie, dass die Abbildung $\psi : G \to G$, $x \mapsto x^{-1}$ eine Bijektion ist.
- Zeigen Sie, dass G genau dann kommutativ ist, wenn ψ ein Gruppenhomomorphismus ist.

A 2.

Wir betrachten die Polynome

$$p_1(t) = 3t^4 + t^3 + 4t^2 + t + 1$$
$$p_2(t) = t^3 + 3t^2 + t + 3$$

in einem Polynomring $K[t]$. Bestimmen Sie den größten gemeinsamen Teiler $g(t)$ der beiden Polynome für die beiden Körper $K = \mathbb{R}$ und $K = \mathbb{Z}_5$.

A 3.

(1) Zeigen Sie, dass das Polynom $x^4 - x^2 + 1$ reduzibel über $\mathbb{Z}_5$, jedoch irreduzibel über $\mathbb{Q}$ ist.
(2) Zerlegen Sie das Polynom $f(x) = x^6 + 1 \in \mathbb{Z}_2[x]$ in irreduzible Faktoren.

A 4.

Es sei p eine Primzahl. Wir betrachten den endlichen Körper $\mathbb{Z}_p = \{0, 1, \dots, p-1\}$ mit Addition und Multiplikation modulo p. Zeigen Sie:

(1) Für $x \in \mathbb{Z}_p \setminus \{0\}$ ist die durch $z \mapsto xz$ gegebene Abbildung von $\mathbb{Z}_p$ nach $\mathbb{Z}_p$ bijektiv.
(2) Für $h = \lfloor \frac{p}{2} \rfloor$ sind die Quadrate $0^2, 1^2, 2^2, \dots, h^2$ paarweise verschiedene Elemente von $\mathbb{Z}_p$.

(Tipp zu (b)*:* $x^2 - y^2 = (x-y)(x+y)$)

A 5.

Es sei $f(x) = x^2 - x + 4 \in \mathbb{Z}_5[x]$. Wir betrachten den Ring $\mathbb{Z}_5(f) = \{g \in \mathbb{Z}_5[x] \mid \deg g < 2\}$ mit der Multiplikation modulo f.

(1) Berechnen Sie die folgenden Produkte:

(1) $(x+1)(x-2)$ (2) $(2x-1)(x+2)(x-1)$ (3) $(x+4)(x-4)$

(2) Bestimmen Sie ein Element $g \in \mathbb{Z}_5(f)$, das *kein* inverses Element bzgl. der Multiplikation modulo f besitzt.