Diekert/Weiß — Sommersemester 2019

Konkrete Mathematik
Aufgabenblatt 1

Besprechung: 6. und 7. Mai 2019

1. Sei G eine abelsche Gruppe. Zeigen Sie: sind $g, h \in G$ Elemente mit teilerfremden Ordnungen $m, n \in \mathbb{N}$, dann hat gh Ordnung mn.

2. Sei R ein Integritätsbereich (d.h. nullteilerfreier, kommutativer Ring). Zeigen Sie: die Anzahl an Nullstellen eines Polynoms $f \in R[X]$ mit $f \neq 0$ ist maximal $\deg(f)$.

3. Sei $\mathbb{F}$ ein Körper. Zeigen Sie: jede endliche Untergruppe der multiplikativen Gruppe $\mathbb{F}^*$ ist zyklisch.

Hinweis: Benutzen Sie Aufgaben 1 und 2.

4. Compute $\gcd(X^6 + X^5 + X^3 + X, X^8 + X^7 + X^6 + X^4 + X^3 + X + 1)$ in the polynomial ring $\mathbb{F}_2[X]$ over the two-element field $\mathbb{F}_2$.

5. Let $f(X) = X^5 + X^2 + 1 \in \mathbb{F}_2[X]$. Show that $f(X)$ is irreducible over the two-element field $\mathbb{F}_2$.

6. *Körper einfach selber Bauen*

a) Bestimmen Sie ein Polynom vom Grad 2, das über $\mathbb{Z}/2\mathbb{Z}$ irreduzibel ist.

b) Geben Sie die Additions- und die Multiplikationstabelle eines Körpers mit 4 Elementen an.

c) Bestimmen Sie den Zerfällungskörper von $X^4 - 1$ über $\mathbb{Q}$.

d) Bestimmen Sie den Zerfällungskörper L von $x^3 - 2$ über $\mathbb{Q}$. Was ist der Grad $[L : \mathbb{Q}]$ der Körpererweiterung?

7. Let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$. Show that if $r \in \mathbb{Q}$ is a root of $f(X)$, then $r \in \mathbb{Z}$ and r divides a_0.

8. *Eisenstein Kriterium (nach F. Gotthold M. Eisenstein, 1823–1852)*

Let $f(X) = a_nX^n + \cdots + a_0X^0 \in \mathbb{Z}[X]$ with $n \geq 1$ and $a_n \neq 0$. Suppose there exists a prime number p such that $p \nmid a_n,\ p \mid a_{n-1},\ p \mid a_{n-2},\ \ldots,\ p \mid a_0$, but $p^2 \nmid a_0$. Show that $f(X)$ is irreducible over $\mathbb{Q}$.

Hinweis: Zeigen Sie zunächst, dass $f(X)$ irreduzibel über $\mathbb{Z}$ ist.

9. Prove the following statements using Eisenstein's criterion from the previous exercise:

a) Let p be a prime number and $f(X) = X^n - p$ for $n \geq 1$. Then $f(X)$ is irreducible over $\mathbb{Q}$ and thus in particular $\sqrt[n]{p} \notin \mathbb{Q}$.

b) Let p be a prime number and $f(X) = X^{p-1} + X^{p-2} + \cdots + 1$. Then $f(X)$ is irreducible over $\mathbb{Q}$.
Hint: $f(X)$ can be written as $f(X) = \frac{X^p - 1}{X-1} \in \mathbb{Z}[X]$, and $f(X)$ is irreducible over $\mathbb{Q}$ if and only if $f(X+1)$ is.