.....
Name

....
Matr-Nr. Gruppe

Algebra – Blatt 12

Abgabe am 4.7.2018 bis 10:30 Uhr

1	2	3	Σ

Bitte drucken Sie diese Seite aus und verwenden Sie sie als Deckblatt für Ihre Lösungen.

Wie üblich sind alle Antworten zu begründen/beweisen.

Aufgabe 1 (5 Punkte):

Welche der folgenden Behauptungen gelten für alle Körpererweiterungen L/K und alle Elemente $a, b \in L$?

(a) Das Element a ist algebraisch über K genau dann, wenn a^2 algebraisch über K ist.

(b) Haben sowohl a als auch b Grad kleiner gleich d über K (für ein $d \in \mathbb{N}$), so ist auch der Grad von $a+b$ über K höchstens d.

(c) Ist a algebraisch über K und b transzendent über K, so ist $a+b$ transzendent über K.

(d) Ist a algebraisch, so zerfällt $\mathrm{MiPo}_{a/K}$ in $K(a)[X]$ in Linearfaktoren.

(e) Ist a algebraisch, so ist $\mathrm{MiPo}_{a/K}$ in $K(a)[X]$ nicht irreduzibel.

Aufgabe 2 (4 Punkte):

(a) Sei $f(X) := X^2 + \bar{2} \in \mathbb{F}_5[X]$. Zeigen Sie: f ist (in $\mathbb{F}_5[X]$) irreduzibel.
Hinweis: Probieren Sie einfach alle Elemente von $\mathbb{F}_5$ durch, um mögliche Nullstellen von f zu finden.

(b) Ist $K := \mathbb{F}_5[X]/(f)$ ein Körper? Wie viele Elemente hat K? Ist K als Ring isomorph zu $\mathbb{Z}/n\mathbb{Z}$ für ein n? (Wenn ja, was ist n?)

(c) Sei p jetzt eine beliebige Primzahl ≥ 3. Zeigen Sie, dass es in $\mathbb{F}_p$ ein Element $\bar{a}$ gibt, das kein Quadrat ist (d. h. so dass es kein $\bar{b} \in \mathbb{F}_p$ gibt mit $\bar{b}^2 = \bar{a}$).
Hinweis: Eine Möglichkeit: Zeigen Sie, dass die Abbildung $\mathbb{F}_p \to \mathbb{F}_p, x \mapsto x^2$ nicht injektiv und damit auch nicht surjektiv ist.

(d) Zeigen Sie: Für jede Primzahl ≥ 3 gibt es einen Körper mit p^2 vielen Elementen.

Aufgabe 3 (1+1+2+1+1+1 Punkte):

Im Folgenden sei p eine Primzahl.

Im Folgenden verwenden wir Kongruenz-Notation für Polynome: Sind $g_1, g_2 \in \mathbb{Z}[X]$, so bedeutet „$g_1 \equiv g_2 \mod p$“, dass $g_1 - g_2 = p \cdot h$ ist für ein $h \in \mathbb{Z}[X]$.

(a) Zeigen Sie: Sind $g_1, g_2 \in \mathbb{Z}[X]$, so ist $(g_1+g_2)^p \equiv g_1^p + g_2^p \mod p$.
Hinweis: Ist p prim und $1 \leq k < p$, so ist der Binomialkoeffizient $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ durch p teilbar.

(b) Von nun an sei $f(X) := 1 + X^p + \cdots + X^{p(p-1)}$ und $g(Y) := f(Y+1)$. Wir schreiben $g(Y) = \sum_{i=0}^{p(p-1)} a_i Y^i$.
Bestimmen Sie a_0 und $a_{p(p-1)}$.

(c) Zeigen Sie: $g(Y) \cdot Y^p \equiv Y^{p^2} \mod p$.
Hinweis: Hier sind ein paar nützliche Zwischenschritte, die Sie zeigen und verwenden können:
für $X := Y+1$ ist $Y^p \equiv X^p - 1 \mod p$; $\quad f(X)(X^p-1) = X^{p^2}-1$; $\quad X^{p^2}-1 \equiv (X-1)^{p^2} \mod p$

(d) Zeigen Sie, dass f irreduzibel ist.
Hinweis: Verwenden Sie die vorigen Aufgabenteile, um zu prüfen, dass sich das Eisenstein-Kriterium auf g anwenden lässt.

(e) Zeigen Sie: Ist ζ eine primitive p^2-te Einheitswurzel, so ist f das Minimalpolynom von ζ.

(f) Folgern Sie: Ist $p \geq 3$, so ist das regelmäßige p^2-Eck nicht mit Zirkel und Lineal konstruierbar.