10.12.2008

I. Bouw
L. Brewis und D.Ufer

Übungen zur Algebra I - WS08/09
Blatt 9

Abgabe ist Mittwoch, den 17.12.2008, vor der Vorlesung (**zu zweit!**)

Aufgabe 1: Faktorisierung $(1 + 1 + 1 + 1 + 2 = 6)$
Überprüfen Sie, ob die folgenden Polynome irreduzibel über $\mathbb{Q}$ sind.

(a) $x^4 + 5x^2 + 30x + 20$.
(b) $x^5 + 9x^3 + 12x^2 + 12x + 3$.
(c) $4x^3 - 3x + \frac{1}{2}$.
(d) $x^4 + 7x^3 + 2x + 3$.
(e) $x^5 + x^4 + 4x^3 + 4x^2 + 4x + 1$. Tipp: Faktorisieren Sie das Polynom in $\mathbb{F}_2$.

Aufgabe 2: Endliche Körper $(3 + 2 + 1 + 1 = 7)$
Sei $\mathbb{F}_q$ der endliche Körper mit $q = p^r$ Elementen. Sei $n \in \mathbb{Z}$ mit $p \nmid n$. Ein Element $x \in \mathbb{F}_q$ heisst *primitive n-te Einheitswurzel*, falls $x^n = 1$ und $x^m \neq 1$ für alle $m < n$.

(a) Zeigen Sie, dass $\mathbb{F}_q$ genau dann eine primitive n-te Einheitswurzel enthält wenn $n|(q-1)$. Wie viele primitive n-te Einheitswurzeln gibt es in $\mathbb{F}_q$ im Fall $n|(q-1)$? Tipp: Benutzen Sie Korollar 4.5.7 im Skript.
(b) Für welche q ist $x^2 + x + 1$ irreduzibel über $\mathbb{F}_q$?
(c) Zeigen Sie, dass wenn $\mathbb{F}_{q_2} \supset \mathbb{F}_{q_1}$, dann folgt $q_1|q_2$.
(d) Was ist die kleinste Erweiterung $\mathbb{F}_q$ von $\mathbb{F}_2$, sodass $\mathbb{F}_q$ eine primitive 5-te Einheitswurzel enthält?

Aufgabe 3: Ideale von $\mathbb{Z}[x]$ (3)
Seien f und g Polynome über $\mathbb{Z}$. Zeigen Sie, dass $ggT(f, g) = 1$ in $\mathbb{Q}[x]$ genau dann, wenn das von f und g erzeugte Ideal in $\mathbb{Z}[x]$ ein Element von $\mathbb{Z}$ enthält. Tipp: Benutzen Sie Aufgabe 1 von Blatt 7.