UNIVERSITÄT DES SAARLANDES

Fachrichtung Mathematik
Prof. Dr. Gabriela Weitze-Schmithüsen
Dr. Tobias Columbus
Christian Steinhart

Algebra

Übungsblatt 8

Aufgabe 1 (4 Punkte)

a) Für ein $n \in \mathbb{N}, n \geq 2$ sei

$$pr_n : \mathbb{Z}[X] \to \mathbb{Z}/n\mathbb{Z}[X] \ , \ \sum_{i=0}^{k} \lambda_i X^i \mapsto \sum_{i=0}^{k} \overline{\lambda}_i X^i$$

die übliche Projektion auf den Polynomringen. Sei $f \in \mathbb{Z}[X]$ ein normiertes Polynom und $pr_n(f) \in \mathbb{Z}/n\mathbb{Z}[X]$ irreduzibel. Zeige, dass dann auch f in $\mathbb{Z}[X]$ irreduzibel ist.

b) Zeige, dass das Polynom $f(X) = X^3 + 2X^2 + 3X + 4 \in \mathbb{Z}[X]$ irreduzibel ist.

c) Zeige, dass das Polynom $f(X) = X^4 + 1 \in \mathbb{Z}[X]$ irreduzibel ist, aber für jede Primzahl p das Bild $pr_p(f) \in \mathbb{Z}/p\mathbb{Z}[X] = \mathbb{F}_p[X]$ reduzibel ist. Für letzteres kannst Du für $p \geq 3$ wie folgt vorgehen:

(i) Zeige, dass ein irreduzibles $f \in \mathbb{F}_p[X]$ von Grad 2 existiert.

(ii) Zeige, dass in $\mathbb{F}_p[X]/(f)$ eine primitive achte Einheitswurzel (s. Aufgabe 4 b)) $u \in \mathbb{F}_p[X]/(f)$ existiert.

(iii) Betrachte $\mathbb{F}_p[X]/(f)$ als $\mathbb{F}_p$-Vektorraum und Multiplikation mit u als Vektorraumhomomorphismus m_u und folgere hieraus, dass $X^4 + 1$ von einem Polynom von Grad ≤ 2 geteilt wird.

Aufgabe 2 (4 Punkte)

Gib jeweils (mit einer kurzen Begründung) an, ob die folgenden Polynome in den jeweiligen Ringen irreduzibel sind:

a) $X^4 + X^3 + X^2 + X + 1 \in \mathbb{F}_2[X]$

b) $X^4 + X^3 + X^2 + X + 1 \in \mathbb{R}[X]$

c) $3X^4 + 4X^3 + 8X + 10 \in \mathbb{Q}[X]$

d) $X^2 + Y^2 + 1 \in \mathbb{C}[X, Y]$

Aufgabe 3 (4 Punkte)

a) Sei R ein faktorieller Ring. Zeige, dass es unendlich viele irreduzible Elemente in $R[X]$ gibt.

b) Sei k ein Körper mit q Elementen. Zeige, dass $X^q - X = \prod_{\lambda \in k}(X - \lambda)$ in dem Ring $k[X]$ gilt.

c) Sei $p \in \mathbb{N}$ eine Primzahl. Folgere aus dem a)-Teil, dass es unendlich viele endliche Körper mit paarweise unterschiedlich vielen Elementen existieren, die $\mathbb{F}_p$ als Teilring enthalten.

Aufgabe 4 (4+4 Bonuspunkte Punkte)

a) Sei R ein kommutativer Ring mit Eins. Auf seinem Polynomring $R[X]$ ist die formale Ableitung wie folgt definiert:

$$\mathrm{der} : R[X] \to R[X] \ , \ \sum_{i=0}^{n} \lambda_i X^i \mapsto \sum_{i=1}^{n} (i \cdot \lambda_i) X^{i-1}$$

Zeige, dass „der“ die Produktregel [1] erfüllt.

b) Es sei $n \geq 1$ eine natürliche Zahl und k ein Körper mit $\mathrm{char}(k) \nmid n$. Zeige, dass das Polynom $X^n - 1 \in k[X]$ keine mehrfachen Faktoren hat.[2]

Für $n \in \mathbb{N}$ definieren wir durch

$$\Phi_1(X) = X - 1,$$
$$\Phi_n(X) = \frac{X^n - 1}{\mathrm{kgV}\big(\Phi_d \mid d \neq n \text{ und } \ \text{teilt } n\big)}.$$

die Kreisteilungspolynome $\Phi_n \in \mathbb{Z}[X]$.

c) Zeige, dass die Polynome $\Phi_n \in \mathbb{Z}[X]$ wohldefiniert, normiert und von Grad $\varphi(n)$ sind.[3]

d) Ein $\zeta \in \mathbb{C}$ heißt *primitive n-te Einheitswurzel*, wenn $\zeta^n = 1$ und $\zeta^k \neq 1$ für $1 \leq k < n$. Zeige, dass die Nullstellen von Φ_n in $\mathbb{C}$ genau die primitiven n-ten Einheitswurzeln sind.

Wir wollen nun zeigen, dass Φ_n irreduzibel über $\mathbb{Q}$ ist. Dazu sei $f \in \mathbb{Q}[X]$ ein irreduzibler Faktor von Φ_n. Wir können ohne Einschränkung annehmen, dass f in $\mathbb{Z}[X]$ liegt und normiert ist.[4]

Wir betrachten eine Primzahl $p \in \mathbb{N}$, die kein Teiler von n ist sowie die Abbildung $\mathbb{Q}[X] \to \mathbb{Q}[X]/(f)$ mit $h \mapsto h(X^p)$. Der Kern dieser Abbildung ist ein Ideal $(g) \subseteq \mathbb{Q}[X]$.

e) Zeige, dass für eine Nullstelle $\zeta \in \mathbb{C}$ von f die Potenz ζ^p eine Nullstelle von g ist. Schlußfolgere, dass g ein Teiler von $X^n - 1$ in $\mathbb{Q}[X]$ ist und wir daher ohne Einschränkung annehmen können, dass $g \in \mathbb{Z}[X]$ und normiert ist.

f) Sei $h \in \mathbb{F}_p[X]$ ein Polynom. Zeige, dass $(h(X))^p = h(X^p)$ gilt.

g) Folgere hieraus, dass $f = g$ gilt indem Du die Annahme, dass f und g zwei verschiedene und somit teilerfremde Teiler von $X^n - 1$ sind, zum Widerspruch führst. Betrachte dazu die Reduktionen von f und g in $\mathbb{F}_p[X]$.

h) Zeige, dass die Nullstellen von f in $\mathbb{C}$ unter der Operation $\zeta \mapsto \zeta^p$ für jede Primzahl $p \in \mathbb{N}$ mit $p \nmid n$ abgeschlossen sind. Schließe daraus $f = \Phi_n$.

Abgabe bis spätestens Montag, den 16.12, um 12:00 Uhr. Werfen Sie Ihre Lösungsvorschläge in die dafür vorgesehenen Einwurfkästen vor dem Zeichensaal in Gebäude E 2 5. Abgabe zu dritt ist möglich. Bitte geben Sie Ihren Namen und Ihre Matrikelnummer an!

[1] D.h. für $f, g \in R[X]$ gilt $\mathrm{der}(fg) = \mathrm{der}(f)g + f\,\mathrm{der}(g)$.

[2] Ein mehrfacher Faktor eines Polynoms $f \in k[X]$ ist ein nichttrivialer Teiler g von f, sodass auch g^2 ein Teiler von f ist.

[3] Hier bezeichne φ die Eulersche φ-Funktion.

[4] Warum?