Musterlösung Serie 15

FAKTORIELLE RINGE

---

76. Wir betrachten den Ring

$$R := \left\{ \sum_{n=0}^{\infty} a_{n/q} t^{n/q} : q \in \mathbb{N}, q > 0, a_{n/q} \in \mathbb{C} \right\}.$$

Beweisen Sie, dass R nicht faktoriell ist.

Lösung: Wir bemerken, dass das Argument aus Aufgabe 74 (a), Serie 14 auch hier beweist, dass eine Potenzreihe $f \in R$ eine Einheit ist dann und nur dann falls $f(0) \neq 0$. Wir nehmen an R sei faktoriell. Sei $f \in R$ mit $f \neq 0$ ein Element, so dass $f = g^n$ für ein $g \notin R^*$. Dann besitzt jede Faktorisierung von f in irreduzible Elemente mindestens n Faktoren, weil die Faktorisierung von g hat bereits mindestens einen Faktor. Für jedes $n \geqslant 1$ gilt $t = (t^{1/n})^n$, also hat die irreduzible Faktorisierung von t mindestens n Faktoren. Dies ist jedoch ein Widerspruch, weil eine irreduzible Faktorisierung von t hat nur endlich viele Faktoren.

77. Beweisen Sie, dass in einem faktoriellen Ring jedes irreduzible Element ein Primelement ist.

Lösung: Sei $r \in R$ ein irreduzibles Element. Seien $a, b \in R$, so dass $r | ab$. Dann existiert $s \in R$ mit $sr = ab$. Weil R faktoriell ist, existieren Faktorisierungen $a = u_1 u_2 \cdots u_k$ und $b = v_1 v_2 \cdots v_m$ von a und b in irreduzible Elemente. Die Eindeutigkeit der Faktorisierung besagt nun, dass ein u_i oder ein v_j assoziiert zu r ist. O.B.d.A. nehmen wir an, dass u_1 zu r assoziiert ist. Dann existiert eine Einheit $u \in R$ so dass $u_1 = ur$. Also gilt

$$a = u_1 u_2 \cdots u_k = r(u^{-1} u_2 \cdots u_k).$$

Somit folgt $r | a$.

78. Beweisen Sie, dass das Polynom $x^n - t \in \mathbb{C}[[t]][x]$ für alle $n \geqslant 1$ irreduzibel ist.

Lösung: Das Polynom ist primitiv, denn es ist monisch. Weiter teilt t alle Koeffizienten bis auf den Leitkoeffizienten. Jedoch teilt t^2 den konstanten Koeffizienten nicht. Wir haben bereits in der Lösung zu Aufgabe 74 (b) bewiesen, dass t ein irreduzibles Element in $\mathbb{C}[[t]]$ ist. Also folgt die Irreduzibilität aus dem Schönemann-Eisenstein Kriterium.

79. Sei $\mathbb{C}[x, y] := (\mathbb{C}[x])[y]$ der komplexe Polynomring in zwei Variabeln. Beweisen Sie, dass $x^2 + y^2 - 1$ irreduzibel in $\mathbb{C}[x, y]$ ist.

Lösung: Die Koeffizienten von $x^2 + y^2 - 1 = y^2 + (x^2 - 1)$ als Polynom in y sind 1 und $x^2 - 1$, also ist dies ein primitives Polynom in y. Nach dem Lemma von Gauss reicht es aus die Irreduzibilität des Polynoms in $\mathbb{C}(x)[y]$ zu beweisen. Wir nehmen an, es ist nicht irreduzibel in $\mathbb{C}(x)[y]$. Dann zerfällt es in zwei Linearfaktoren, also existiert ein Polynom $p_0 \in \mathbb{C}(x)$ mit

$$p_0^2 = x^2 - 1.$$

Wir schreiben $p_0 = p/q$ mit $p, q \in \mathbb{C}[x]$, so dass p und q teilerfremd sind und q monisch ist. Wir erhalten

$$p^2 = q^2(x^2 - 1).$$

Nun folgt $q = 1$, weil p und q teilerfremd sind. Wir erhalten nun

$$p^2 = x^2 - 1 = (x - 1)(x + 1).$$

Nach der Eindeutigkeit der Faktorisierung von Polynomen in $\mathbb{C}[x]$ ist dies ein Widerspruch. Also ist $x^2 + y^2 - 1$ irreduzibel.

80. Sei $q = p^e$ eine Potenz einer Primzahl $p \in \mathbb{N}$ mit $e \geqslant 1$ und sei $r = p^{e-1}$. Wir definieren das *q-te zyklotomische Polynom* oder das *q-te Kreisteilungspolynom* als

$$\Phi_q(x) := \frac{x^q - 1}{x^r - 1} \in \mathbb{Z}[x].$$

Beweisen Sie, dass das p-te Kreisteilungspolynom Φ_p irreduzibel ist.

Hinweis: Verwenden Sie die Substitution $y = x - 1$.

Lösung: Sei $y + 1 := x$. Dann gilt

$$(x^p - 1)/(x - 1) = ((y + 1)^p - 1)/y = \sum_{i=1}^{p} \binom{p}{i} y^{i-1}.$$

Für $p \geqslant i > 0$ ist der Binomialkoeffizient ist gegeben durch

$$\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{1 \cdot 2 \cdots i}.$$

Falls $i < p$, dann hat es im Zähler einen Faktor von p und im Nenner sind alle Zahlen koprim zu p. Also teilt p den Binomialkoeffizienten. Der konstante Koeffizient ist gegeben durch

$$\binom{p}{1} = p.$$

Also erfüllt $\Phi_p(y)$ die Bedingungen des Schönemann-Eisenstein Kriterion.

81. Sei R ein faktorieller Ring mit Quotientenkörper K.

(a) Sei $f \in R[x]$ ein Polynom vom Grad $n > 0$, so dass

$$f = (x - a)^n + tF(x)$$

für ein irreduzibles Element $t \in R$, ein Element $a \in R$, und ein Polynom $F \in R[x]$ mit

$$F(a) \not\equiv 0 \pmod{t}.$$

Beweisen Sie, dass das Polynom f irreduzibel in $K[x]$ ist.

(b) Sei $p \in \mathbb{N}$ eine Primzahl. Beweisen Sie die Kongruenz

$$x^p - 1 \equiv (x-1)^p \pmod p$$

von Polynomen in $\mathbb{Z}[x]$ und leiten Sie mit Aufgabe (a) nochmals die Irreduzibilität des p-ten Kreisteilungspolynom Φ_p her.

Lösung:

(a) Wir verwenden die Substitution $y := x - a$. Dann gilt

$$f(y) = y^n + tF(y+a).$$

Es gilt $f(0) = tF(a)$. Also teilt der konstante Koeffizient von $f(y)$ das irreduzible Element t, jedoch nicht t^2. Der Leitkoeffizient ist kongruent zu 1 modulo t, also teilt dieser t nicht. Insbesondere ist ein ggT b der Koeffizienten nicht teilbar durch t. Das Schönemann-Eisnstein Kriterium besagt nun, dass $f(y)/b$ irreduzibel in $R[y]$ ist. Also folgt aus Gauss' Lemma, dass $f(x)$ irreduzibel in $K[x]$ ist.

(b) Wir haben

$$(x-1)^p = \sum_{i=0}^{p} (-1)^i \binom{p}{i} x^i.$$

Wir haben bereits in Aufgabe 79 (b) die Teilbarkeit $p | \binom{p}{i}$ für alle $1 \leqslant i < p$ festgestellt, also erhalten wir die gewünsche Kongruenz

$$(x-1)^p \equiv x^p - 1 \pmod p.$$

Somit gilt

$$\Phi_p(x) \equiv (x-1)^{p-1} \pmod p.$$

Weiters haben wir $\Phi_p(1) = p$, also erfüllt Φ_p die Bedingungen aus Aufgabe (a). Somit ist Φ_p irreduzibel in $\mathbb{Q}[x]$. Da es primitiv ist, ist es auch irreduzibel in $\mathbb{Z}[x]$.