Musterlösung Serie 12

Teilbarkeit, Faktorielle Ringe, Hauptidealringe

1. Sei K ein Körper. Zeige, dass $K[X^2, X^3] \subset K[X]$ ein Integritätsbereich, aber nicht faktoriell ist.

   Lösung: Als Unterring des Integritätsbereichs $K[X]$ ist $R := K[X^2, X^3]$ ebenfalls ein Integritätsbereich.

   Wir behaupten, dass X^n irreduzibel in R ist für $n = 2, 3$. Zunächst ist dieses Element ungleich Null und keine Einheit von R, weil es kein Teiler von 1 ist. Sodann betrachte eine Zerlegung $X^n = g \cdot h$ mit Faktoren $g, h \in R$. Dann ist dies auch eine Zerlegung in $K[X]$, und von dort wissen wir, dass $g = aX^i$ und $h = a^{-1}X^{n-i}$ sein muss für ein $a \in K^\times$ und ein $0 \leqslant i \leqslant n$. Im Fall $i = 1$ ist nun aber $g \notin R$, und im Fall $n - i = 1$ ist $h \notin R$. Wegen $n \leqslant 3$ muss dann $i \in \{0, n\}$ sein und damit eines von g, h schon in $K^\times$ liegen. Dies ist dann aber auch eine Einheit in R. Daher sind X^2 und X^3 irreduzibel in R.

   Die Behauptung impliziert nun, dass $X^2 \cdot X^2 \cdot X^2 = X^6 = X^3 \cdot X^3$ zwei Zerlegungen desselben Elements von R in verschieden viele irreduzible Faktoren sind. Dies ist in einem faktoriellen Ring nicht möglich; deshalb ist R nicht faktoriell.

   Aliter: Wäre X^2 ein Teiler von X^3 in R, so gäbe es ein $f \in R$ mit $X^2 \cdot f = 3$. In $K[X]$ ist diese Gleichung aber nur lösbar mit $f = X$. Da dieses nicht in R liegt, haben wir also einen Widerspruch; somit ist X^2 kein Teiler von X^3. Dafür teilt X^2 das Element $X^6 = X^2 \cdot X^2 \cdot X^2$. Da es keinen der Faktoren von $X^6 = X^3 \cdot X^3$ teilt, ist X^2 also kein Primelement in R. Da in einem faktoriellen Ring jedes irreduzible Element schon ein Primelement ist, ist der Ring R also nicht faktoriell.

2. Sei R ein faktorieller Ring.

   (a) Seien $a, b, c \in R$. Zeige:
   $$c|ab,\ \mathrm{ggT}(a, c) \sim 1 \Longrightarrow c|b.$$

   (b) Sei $u \in R^\times$, und seien $p_1, \ldots, p_n$ Primelemente von R. Zeige, dass die Teiler von $up_1 \cdots p_n$ genau die Elemente der Form $v \cdot \prod_{i \in I} p_i$ sind für alle $v \in R^\times$ und alle Teilmengen $I \subset \{1, \ldots, n\}$.

   Lösung:

(a) Suppose first that $c = 0$. If $b = 0$, then $c|b$ and we are done. Otherwise $c|ab$ implies $ab = 0$, and since $b \neq 0$ and R is an integral domain, it follows that $a = 0$. But then $\mathrm{ggT}(a, c) = \mathrm{ggT}(0, 0) = 0 \neq 1$, contradiction, so the case does not occur.

Now suppose that $c \neq 0$. We write $c = up_1 \cdots p_n$ with $u \in R^\times$ and primes $p_i \in R$ and proceed by induction on n.

If $n = 0$, then $u \cdot (u^{-1}b) = b$ shows that $c = u$ divides b, as desired. Otherwise $p_n|c|ab$ implies that $p_n|ab$ and hence $p_n|a$ or $p_n|b$. In the case $p_n|a$ it follows that $p_n|\,\mathrm{ggT}(a, c) \sim 1$ and hence $p_n|1$, a contradiction. Thus $p_n|b$. Write $b = b'p_n$ and $c' := up_1...p_{n-1}$. The fact that $c|ab$ means that $xc = ab$ for some $x \in R$. Thus we have $xc'p_n = ab'p_n$, and canceling the factor $p_n \neq 0$ implies that $xc' = ab'$. Therefore $c'|ab'$. Also, $\mathrm{ggT}(a, c')$ is a common divisor of a and c' and hence of c; so it is a divisor of $\mathrm{ggT}(a, c)$. Since $\mathrm{ggT}(a, c) \sim 1$, it follows that $\mathrm{ggT}(a, c') \sim 1$. The induction hypothesis for $n - 1$ in place of n thus shows that $c'|b'$. This means that $yc' = b'$ for some $y \in R$; hence $yc = yc'p_n = b'p_n = b$ and thus $c|b$, as desired.

(b) Let $a := up_1...p_n$. If $d := v \cdot \prod_{i \in I} p_i$ is as stated in the problem, then

$$d \cdot uv^{-1} \prod_{j \in I^c} p_j = a$$

for $I^c := \{1, \ldots, n\} \smallsetminus I$ and so $d|a$.

Conversely, let d be a divisor of a. Then there exists an $x \in R$ such that $dx = a$. Since R is factorial, we can write $d = tq_1...q_r$ and $x = wq_{r+1}...q_{r+s}$, where $t, w \in R^\times$, and the q_i are primes. Thus we have

$$a = up_1...p_n = twq_1...q_{r+s}.$$

By the uniqueness of the factorization of a, we have $r + s = n$, and there exists a permutation $\sigma \in S_n$ such that $\forall i : p_{\sigma i} \sim q_i$. For each i, let $u_i \in R^\times$ be such that $u_i p_{\sigma i} = q_i$. Then, with $v := tu_1...u_s$, we have

$$d = v \cdot p_{\sigma 1} ... p_{\sigma s},$$

so d is of the desired form.

3. Betrachte Elemente $a_1, \ldots, a_n$ eines faktoriellen Rings R. Ein Element $b \in R$ mit $\forall i\colon a_i|b$ heisst *gemeinsames Vielfaches von* $a_1, \ldots, a_n$.

   (a) Zeige, dass ein gemeinsames Vielfaches b von $a_1, \ldots, a_n$ existiert, so dass für jedes gemeinsame Vielfache b' von $a_1, \ldots, a_n$ gilt $b|b'$.

   (b) Zeige, dass dieses *kleinste gemeinsame Vielfache von* $a_1, \ldots, a_n$ eindeutig bis auf Assoziiertheit ist. Wir bezeichnen jedes solche mit $\mathrm{kgV}(a_1, \ldots, a_n)$.

(c) Zeige, dass $\mathrm{ggT}(a_1, a_2) \cdot \mathrm{kgV}(a_1, a_2) \sim a_1 \cdot a_2$ gilt.

Lösung: If there exists an i such that $a_i = 0$, then the only common multiple of $a_1, ..., a_n$ is 0, and hence everything holds with $\mathrm{kgV}(a_1, \ldots, a_n) = 0$. Thus we assume that all of the a_i are non-zero.

Choose a system of representatives $\{p_i \mid i \in I\}$ with respect to $\sim$ of the prime elements of R.

(a) Since R is factorial, we can write each a_j uniquely as a product $u_j \prod_i' p_i^{\mu_{ji}}$ with $u_j \in R^\times$ and $\mu_{ji} \geqslant 0$. For each i, set $\mu_i := \max\{\mu_{ji} \mid 1 \leqslant j \leqslant n\}$. Let $b := \prod_i' p_i^{\mu_i}$. By part (b) of the last proposition of §2.2 of the Zusammenfassung b is a multiple of each a_j.
Conversely consider any common multiple b' of the a_i. If $b' = 0$, we already have $b|b'$. Otherwise write $b' = v \prod_i' p_i^{\nu_i}$ with $v \in R^\times$. Then by the same proposition, $a_j|b$ is equivalent to $\mu_{ji} \leqslant \nu_i$ for all i. Thus $\mu_i \leqslant \nu_i$ for all i, and by the same proposition again $b|b'$. Therefore b is a least common multiple of the a_i.

(b) Let $b, b' \in R$ be least common multiples of $a_1, ..., a_n$. The fact that b' satisfies the property in (a) implies that $b'|b$. Similarly $b|b'$, and thus $b \sim b'$.

(c) Write $a_j = u_j \prod_i' p_i^{\mu_{ji}}$ as in (a). In the Vorlesung and in (a) we have seen that

$$\begin{aligned} \mathrm{ggT}(a_1, a_2) &\sim \textstyle\prod_i' p_i^{\min(\mu_{1i}, \mu_{2i})}, \\ \mathrm{kgV}(a_1, a_2) &\sim \textstyle\prod_i' p_i^{\max(\mu_{1i}, \mu_{2i})}. \end{aligned}$$

Thus

$$\mathrm{ggT}(a_1, a_2) \cdot \mathrm{kgV}(a_1, a_2) \sim \textstyle\prod_i' p_i^{\min(\mu_{1i}, \mu_{2i}) + \max(\mu_{1i}, \mu_{2i})} = \prod_i' p_i^{\mu_{1i} + \mu_{2i}} \sim a_1 \cdot a_2,$$

as desired.

4. Seien a and b positive ganze Zahlen. Beweise unter Verwendung der Isomorphiesätze die Identität

$$\mathrm{ggT}(a, b) \cdot \mathrm{kgV}(a, b) = ab.$$

Lösung: We have seen that $\mathrm{ggT}(a, b)\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$ (for ideals, but these are the same as subgroups of $\mathbb{Z}$). The definition of the least common multiple means that $\mathrm{kgV}(a, b)\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$. Using the first isomorphism theorem, we obtain

$$a\mathbb{Z}/\,\mathrm{kgV}(a, b)\mathbb{Z} = a\mathbb{Z}/(a\mathbb{Z} \cap b\mathbb{Z}) \cong (a\mathbb{Z} + b\mathbb{Z})/b\mathbb{Z} = \mathrm{ggT}(a, b)\mathbb{Z}/b\mathbb{Z}.$$

On the other hand, for any $m|n$ we have $(\mathbb{Z}/n\mathbb{Z})/(m\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z}$ by the second isomorphism theorem. By Lagrange we therefore have $|\mathbb{Z}/n\mathbb{Z}| = |\mathbb{Z}/m\mathbb{Z}| \cdot |m\mathbb{Z}/n\mathbb{Z}|$ and hence $|m\mathbb{Z}/n\mathbb{Z}| = \frac{n}{m}$. Thus

$$\frac{\mathrm{kgV}(a, b)}{a} = \big|a\mathbb{Z}/\,\mathrm{kgV}(a, b)\mathbb{Z}\big| = \big|\mathrm{ggT}(a, b)\mathbb{Z}/b\mathbb{Z}\big| = \frac{b}{\mathrm{ggT}(a, b)}.$$

5. Sei R ein Hauptidealring. Zeige, dass jedes von Null verschiedene Primideal in R maximal ist.

   Lösing: Let $(\pi) \subset R$ be a non-zero prime ideal, and let $(a) \subset R$ be an ideal containing (π). Then $\pi \in (a)$ implies that $\pi = xa$ for some $x \in R$. From the lecture we know that π is a prime element in R. Since principal ideal domains (Hauptidealringe) are factorial, this means that π is irreducible. Therefore we have $x \in R^\times$ or $a \in R^\times$. In the first case, we have $p \sim a$ and hence $(\pi) = (a)$. Otherwise we have $(a) = (1) = R$. Therefore every ideal containing (π) is equal to (π) or all of R, and we have shown that (π) is maximal.

6. Im Ring $R := \mathbb{Z}[i\sqrt{5}] \subset \mathbb{C}$ gilt die Gleichheit

$$6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5}).$$

   Zeige:

   (a) Die Funktion $N\colon R \to \mathbb{Z}^{\geqslant 0}, z = a + bi\sqrt{5} \mapsto |z|^2 = a^2 + 5b^2$ ist multiplikativ (das heisst, $\forall \alpha, \beta \in R : N(\alpha\beta) = N(\alpha)N(\beta)$).

   (b) $R^\times = \{u \in R \mid N(u) = 1\} = \{\pm 1\}$.

   (c) Die Elemente $2, 3, 1 + i\sqrt{5}, 1 - i\sqrt{5}$ sind unzerlegbar in R.

   (d) Die Elemente $2, 3, 1 + i\sqrt{5}, 1 - i\sqrt{5}$ sind keine Primelemente in R.

   (e) Für das Ideal $I = (2, 1 + i\sqrt{5})$ gilt $I \cdot I = (2)$.

   (f) I ist kein Hauptideal von R.

   (g) I ist ein maximales Ideal von R.

   (h) R ist nicht faktoriell.

   Lösung:

   (a) Für alle $\alpha \in R$ gilt $N(\alpha) = |\alpha|^2$, wobei $|\ |$ den gewöhnlichen komplexen Absolutbetrag bezeichnet. Für alle $\alpha, \beta \in R$ folgt daraus $N(\alpha\beta) = |\alpha\beta|^2 = |\alpha|^2|\beta|^2 = N(\alpha)N(\beta)$, wie gewünscht.
   Aliter: Seien $\alpha = a_1 + a_2 i\sqrt{5}$ und $\beta = b_1 + b_2 i\sqrt{5} \in R$. Dann ist

$$\begin{aligned} N(\alpha\beta) &= N(a_1b_1 - 5a_2b_2 + (a_1b_2 + a_2b_1)i\sqrt{5}) \\ &= (a_1b_1 - 5a_2b_2)^2 + 5(a_1b_2 + a_2b_1)^2 \\ &= a_1^2b_1^2 + 25a_2^2b_2^2 + 5a_1^2b_2^2 + 5a_2^2b_1^2 \\ &= (a_1^2 + 5b_1^2)(b_1^2 + 5b_2^2) \\ &= N(a_1 + a_2 i\sqrt{5}) \cdot N(b_1 + b_2 i\sqrt{5}) = N(\alpha)N(\beta). \end{aligned}$$

(b) Betrachte eine Einheit $u = a + bi\sqrt{5} \in R^\times$. Dann ist auch $u^{-1} \in R$, und da N multiplikativ ist, gilt $N(u^{-1}) \cdot N(u) = N(u^{-1}u) = N(1) = 1$. Wegen $N(u^{-1}), N(u) \in \mathbb{Z}^{\geqslant 0}$ muss daher $a^2 + 5b^2 = N(u) = 1$ sein. Daraus folgt sofort $b = 0$ und $a^2 = 1$, also $u = a = \pm 1$. Umgekehrt gilt für jedes Element $u = a + bi\sqrt{5} \in R$ mit $a^2 + 5b^2 = 1$ auch $(a + bi\sqrt{5})(a - bi\sqrt{5}) = 1$, also ist u eine Einheit in R.

(c) Falls $2 = \alpha\beta$ mit $\alpha, \beta \in R$ ist, folgt $4 = N(2) = N(\alpha)N(\beta)$. Wenn α und β keine Einheiten sind, ist $N(\alpha), N(\beta) > 1$ nach (b). Es gibt dann nur die Möglichkeit $N(\alpha) = N(\beta) = 2$. Diese kann aber nicht auftreten, da 2 wegen $a^2 + 5b^2 \neq 2$ für alle $a, b \in \mathbb{Z}$ nicht im Bild von N liegt. Somit ist 2 unzerlegbar in R.

Wegen $a^2 + 5b^2 \neq 3$ für alle $a, b \in \mathbb{Z}$ liegt auch 3 nicht im Bild von N. Wegen $N(3) = 9 = 3 \cdot 3$ folgt darum analog, dass 3 unzerlegbar in R ist.

Falls $1 + i\sqrt{5} = \alpha\beta$ mit $\alpha, \beta \in R$ ist, folgt $6 = N(1 + i\sqrt{5}) = N(\alpha)N(\beta)$. Wenn α und β keine Einheiten sind, dann müssen $N(\alpha), N(\beta) \in \{2, 3\}$ sein. Dies ist wiederum nicht möglich, da 2 und 3 nicht im Bild von N liegen. Daher ist $1 + i\sqrt{5}$ unzerlegbar. Mit der gleichen Argumentation folgt auch die Unzerlegbarkeit von $1 - i\sqrt{5}$.

(d) Wegen der Gleichheit $6 = 2 \cdot 3 = (1 + i\sqrt{5}) \cdot (1 - i\sqrt{5})$ sind 2 und 3 Teiler von $(1 + i\sqrt{5}) \cdot (1 - i\sqrt{5})$ und $1 + i\sqrt{5}$ und $1 - i\sqrt{5}$ Teiler von $2 \cdot 3$. Keines der vier Elemente ist aber ein Teiler eines anderen, weil sie nach (c) unzerlegbar sind, sich aber nach (b) nicht um Einheiten unterscheiden, da sie verschiedene Bilder unter N haben.

(e) Durch Multiplikation der Erzeuger erhalten wir

$$I \cdot I = (2, 1 + i\sqrt{5})(2, 1 + i\sqrt{5}) = (4, 2 + 2i\sqrt{5}, -4 + 2i\sqrt{5}).$$

Offenbar sind diese drei Elemente Vielfache von 2; daher gilt $I \cdot I \subset (2)$. Umgekehrt ist $2 = (2 + 2i\sqrt{5}) - (-4 + 2i\sqrt{5}) - 4 \in I \cdot I$ und daher $(2) \subset I \cdot I$. Somit gilt $(2) = I \cdot I$.

(f) Nehmen wir an, es sei $I = (\alpha)$ für ein $\alpha \in R$. Wegen (e) ist dann $(\alpha^2) = (\alpha)^2 = I^2 = (2)$ und nach (b) somit $\alpha^2 = \pm 1$. Mit (a) folgt daraus $N(\alpha)^2 = N(\alpha^2) = N(2) = 4$ und somit $N(\alpha) = \pm 2$. In der Lösung von (c) haben wir aber gesehen, dass ± 2 nicht im Bild von N liegt. Daher ist I kein Hauptideal.

(g) Aus (f) folgt bereits, dass $I \neq (1)$, also ein echtes Ideal ist. Betrachte ein echt grösseres Ideal $I \subsetneqq I' \subset R$ und wähle ein Element $a + bi\sqrt{5} \in I' \smallsetminus I$. Die Rechnung $a + bi\sqrt{5} = (a - b) + b \cdot (1 + i\sqrt{5})$ zeigt dann, dass $a - b \notin I$ ist. Wegen $\mathbb{Z} \cap I = 2\mathbb{Z}$ bedeutet dies, dass $a - b$ ungerade ist. Also ist

$$1 \;=\; (a + bi\sqrt{5}) - \tfrac{a-b-1}{2} \cdot 2 - b \cdot (1 + i\sqrt{5}) \;\in\; (a + bi\sqrt{5}) + I \;\subset\; I'.$$

Somit ist $I' = (1)$; und deshalb ist I maximal.

(h) Aus (c) und (d) folgt, dass in R unzerlegbare Elemente existieren, die nicht prim sind. Daher ist R nicht faktoriell.

Aliter: Die Gleichung $6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ ergibt nach (c) zwei Zerlegungen von 6 in unzerlegbare Elemente. Bei (d) haben wir festgestellt, dass $2, 3 \nmid 1 \pm i\sqrt{5}$ und $1 \pm i\sqrt{5} \nmid 2, 3$ gilt. Daher sind $2, 3$ nicht zu $1 \pm i\sqrt{5}$ assoziiert und die beiden obigen Zerlegungen sind nicht zueinander assoziiert. Deshalb kann R nicht faktoriell sein.

*7. Für $p \in \mathbb{C}$ sei $\mathcal{S}_p$ die Menge aller Paare (U, f) bestehend aus einer offenen Umgebung $U \subset \mathbb{C}$ von p und einer holomorphen Funktion $f \colon U \to \mathbb{C}$. Zwei solche Paare (U_1, f_1) und (U_2, f_2) nennen wir äquivalent, falls eine Umgebung $V \subset U_1 \cap U_2$ von p existiert mit $f_1|_V = f_2|_V$. Dies ist eine Äquivalenzrelation auf $\mathcal{S}_p$, und wir bezeichnen die Menge der Äquivalenzklassen mit $\mathcal{O}_p$. Die Elemente von $\mathcal{O}_p$ heissen *Keime holomorpher Funktionen in p.*

(a) Zeige, dass die Addition und Multiplikation von holomorphen Funktionen eine Ringstruktur auf $\mathcal{O}_p$ induzieren.

(b) Entscheide, ob $\mathcal{O}_p$ ein Hauptidealring ist.

Lösung: (a) (Skizze) Zu zwei Paaren (U_1, f_1), $(U_2, f_2) \in \mathcal{S}_p$ assoziieren wir die Summe $(U, f_1|U + f_2|U)$ und das Produkt $(U, (f_1|U) \cdot (f_2|U))$ mit $U := U_1 \cap U_2$. Wir rechnen nach, dass deren Äquivalenzklassen nur von den Äquivalenzklassen $[(U_1, f_1)]$ und $[(U_2, f_2)]$ abhängen. Somit erhalten wir wohldefinierte Abbildungen $+, \cdot \colon \mathcal{O}_p \times \mathcal{O}_p \to \mathcal{O}_p$. Wir behaupten, dass diese eine Ringstruktur mit dem Nullelement $[(\mathbb{C}, 0)]$ und dem Einselement $[(\mathbb{C}, 1)]$ definieren. Jedes der acht Ringaxiome folgt aus dem entsprechenden Axiom für $\mathbb{C}$, indem man Repräsentanten der beteiligten Keime wählt und die Rechnung auf dem Durchschnitt der betreffenden offenen Umgebungen durchführt.

(b) Der Ring $\mathcal{O}_p$ ist ein Hauptidealring. Dies zeigen wir wie folgt:

(i) Für $(U, f) \in \mathcal{S}_p$ hängt der Wert $f(p)$ nur von der Äquivalenzklasse $[(U, f)]$ ab. Damit haben wir eine natürliche Abbildung $\mathcal{O}_p \to \mathbb{C}$, $[(U, f)] \mapsto f(p)$. Aus der Konstruktion der Ringstruktur auf $\mathcal{O}_p$ folgt, dass dies ein Ringhomomorphismus ist. Ausserdem sehen wir anhand konstanter Funktionen, dass er surjektiv ist. Insbesondere ist $\mathcal{O}_p$ nicht der Nullring.

(ii) *Behauptung:* $[(U, f)] \in \mathcal{O}_p$ ist invertierbar genau dann, wenn $f(p) \neq 0$ ist.

Beweis: Ist $[(V, g)]$ ein Inverses von $[(U, f)]$, so folgt $f(p) \cdot g(p) = 1$ und damit $f(p) \neq 0$. Sei umgekehrt $f(p) \neq 0$. Da f stetig ist, existiert dann eine offene Umgebung $V \subset U$ von p, auf der f keine Nullstelle hat. Auf dieser ist die Funktion $(f|V)^{-1}$ holomorph, und $[(V, (f|V)^{-1})]$ ist ein Inverses von $[(U, f)]$. $\square$

(iii) Betrachte den Keim $q := [(\mathbb{C}, z-p)]$. *Behauptung:* Jedes von Null verschiedene Element $[(U, f)] \in \mathcal{O}_p$ ist eine Einheit mal q^n für ein eindeutiges $n \in \mathbb{Z}^{\geqslant 0}$.

Beweis: Ist $[(U, f)]$ ungleich Null, so existiert keine Umgebung $V \subset U$ von p, auf der die Funktion f identisch verschwindet. Aus der Funktionentheorie wissen wir dann, dass eine natürliche Zahl n und eine holomorphe Funktion $g \colon U \to \mathbb{C}$ mit $g(p) \neq 0$ existieren, so dass $f(z) = g(z)(z-p)^n$ ist für alle $z \in U$. Nach (ii) ist dann $[(U, g)]$ eine Einheit und somit $[(U, f)]$ eine Einheit mal q^n.

Sei $[(U, f)] = [(V, h)] \cdot q^m$ für eine weitere natürliche Zahl m und eine weitere Einheit $[(V, h)]$. Dann gilt $g(z)(z-p)^n = f(z) = h(z)(z-p)^m$ auf einer geeigneten Umgebung $W \subset U \cap V$ mit $g(p), h(p) \neq 0$. Aus der Funktionentheorie wissen wir, dass daraus $n = m$ folgt. Somit ist n eindeutig bestimmt. $\square$

(iv) *Behauptung:* Der Ring $\mathcal{O}_p$ ist ein Integritätsbereich.

Beweis: Wir haben bereits gesehen, dass $\mathcal{O}_p$ nicht der Nullring ist. Betrachte also zwei von Null verschiedene Keime. Nach (ii) sind diese jeweils eine Einheit mal q^n, beziehungsweise eine Einheit mal q^m. Ihr Produkt ist daher eine Einheit mal q^{n+m}. Nun ist aber die Funktion $(z-p)^{n+m}$ auf keiner Umgebung von p identisch Null. Daher ist q^{n+m} nicht Null, und das Produkt der beiden gegebenen Keime ebenso. Somit hat $\mathcal{O}_p$ keine Nullteiler. $\square$

(v) *Behauptung:* Jedes Ideal von $\mathcal{O}_p$ ist ein Hauptideal.

Beweis: Dies ist klar für das Nullideal. Betrachte also ein von Null verschiedenes Ideal $\mathfrak{a} \subset \mathcal{O}_p$. Unter allen von Null verschiedenen Elementen von $\mathfrak{a}$ gibt es dann eines, für das die in (iii) definierte natürliche Zahl n minimal ist. Da dieser Keim eine Einheit mal q^n ist, ist dann auch schon $q^n \in \mathfrak{a}$. Nach (iii) ist nun jedes von Null verschiedene Element von $\mathfrak{a}$ eine Einheit mal q^m für ein $m \geqslant n$. Somit ist es ein Vielfaches von q^n und damit in dem Ideal (q^n) enthalten. Insgesamt folgt daraus $\mathfrak{a} = (q^n)$. $\square$