Solutions 07

1. For any field K, let $K(\!(x)\!)$ be ring of formal Laurent series with coefficients in K:

$$K(\!(x)\!) := \left\{ \sum_{i=m}^{\infty} a_i x^i \;\middle|\; a_i \in K, m \in \mathbb{Z} \right\}$$

where the ring operations are defined as in the ring of formal power series $K[[x]]$. Prove that the commutative ring $K(\!(x)\!)$ is isomorphic to the fields of fractions for the domain $K[[x]]$.

Solution. It suffices to prove that every nonzero element f in the field of fractions $K[[x]]_{\langle 0 \rangle}$ may be written uniquely as $f = x^m\, g$ where m is a integer and g in $K[[x]]$ has order 0.

(*existence*) Let $f = p/q$ where p and q are nonzero elements in $K[[x]]$. It follows that $p = x^j\, u$ and $q = x^k\, v$ for some nonnegative integers j and k and some formal power series u and v having order 0. An element of $K[[x]]$ is unit if and only it it has a nonzero constant term. Since the formal power series u and v are units, we have $f = x^{j-k} u v^{-1}$ where $j - k \in \mathbb{Z}$ and uv^{-1} is a formal power series having a nonzero constant term.

(*uniqueness*) Suppose that $f = x^m\, g$ and $f = x^n\, h$ for some integers m and n and some formal power series g and h having a nonzero constant term. It follows that $x^{m-n} = h\, g^{-1}$ is a formal power series of order 0, so $m = n$ and $g = h$. □

2. Let R be a commutative ring. Consider the ***derivative operator*** $D \colon R[x] \to R[x]$ defined, for any polynomial $f := a_n\, x^n + a_{n-1}\, x^{n-1} + \cdots + a_1\, x + a_0$ in $R[x]$, by

$$D(f) := (n\, a_n)\, x^{n-1} + \big((n-1)\, a_{n-1}\big)\, x^{n-2} + \cdots + a_1\,.$$

i. Prove that the operator D is an R-linear map: for any r and s in the coefficient ring R, and any f and g in the polynomial ring $R[x]$, we have

$$D(r\, f + s\, g) = r\, D(f) + s\, D(g)\,.$$

ii. Prove that the operator D satisfies the Leibniz product rule: for any f and g in the polynomial ring $R[x]$, we have

$$D(f\, g) = D(f)\, g + f\, D(g)\,.$$

iii. Let f be a polynomial in $R[x]$. Assume that z in R is root of f having multiplicity m with $m \geqslant 1$. Prove that z is also a root of the derivative $D(f)$ having multiplicity at least $m - 1$. Moreover, when the product $m\, 1_R$ is invertible in R, prove that z is a root of the derivative $D(f)$ having multiplicity $m - 1$.

Solution.

i. For any r and s in R and any

$$\begin{aligned} f &= a_n\, x^n + a_{n-1}\, x^{n-1} + \cdots + a_1\, x + a_0 \qquad \text{and} \\ g &= b_n\, x^n + b_{n-1}\, x^{n-1} + \cdots + b_1\, x + b_0 \end{aligned}$$

in $R[x]$, we have

$$\begin{aligned}D(f+g) &= D\big((r\,a_n+s\,b_n)x^n+(r\,a_{n-1}+s\,b_{n-1})\,x^{n-1}+ \\ &\qquad \cdots+(r\,a_1+s\,b_1)\,x+(r\,a_0+s\,b_0)\big) \\ &= n\,(r\,a_n+s\,b_n)x^{n-1}+(n-1)\,(r\,a_{n-1}+s\,b_{n-1})\,x^{n-2}+ \\ &\qquad \cdots+(r\,a_1+s\,b_1) \\ &= r\Big((n\,a_n)\,x^{n-1}+\big((n-1)\,a_{n-1}\big)\,x^{n-2}+\cdots+a_1)\Big) \\ &\qquad +s\Big((n\,b_n)\,x^{n-1}+\big((n-1)\,b_{n-1}\big)\,x^{n-1}+\cdots+b_1\Big) \\ &= s\,D(f)+r\,D(g)\,,\end{aligned}$$

which proves that D is an R-linear map.

ii. As part *i* shows that D is R-linear, it suffices to prove that the Leibniz product rule holds for any monomial x^{k+n} where k and n are positive integers. By definition, we have $D(x^{k+n})=(k+n)x^{k+n-1}$. We also have

$$\begin{aligned}D(x^k)\,x^n+x^k\,D(x^n) &= k\,x^{k-1}\,x^n+x^k(n\,x^{n-1}) \\ &= k\,x^{k+n-1}+n\,x^{k+n-1}=(k+n)\,x^{k+n-1}\,,\end{aligned}$$

so the Leibniz product rule holds.

iii. As z is a root of f having multiplicity m, there is a polynomial g in $R[x]$ such that $f(x)=(x-z)^m\,g(x)$ and $\mathrm{ev}_z(g)=g(z)\neq 0$. The Leibniz rule implies that

$$\begin{aligned}D\big(f(x)\big) &= m(x-z)^{m-1}\,g(x)+(x-z)^m\,D\big(g(x)\big) \\ &= (x-z)^{m-1}\Big(m\,g(x)+(x-z)\,D(g)\Big)\end{aligned}$$

Hence, z is a root of the derivative $D(f)$ having multiplicity at least $m-1$. When $m\,1_R$ is invertible in R, we also have

$$\begin{aligned}\mathrm{ev}_z\Big(m\,g(x)+(x-z)\,D\big(g(x)\big)\Big) &= m\ \mathrm{ev}_z(g)+0\ \mathrm{ev}_z\big(D(g)\big) \\ &= m\ \mathrm{ev}_z(g)\neq 0\,.\end{aligned}$$

In this case, z is a root of $D(f)$ having multiplicity $m-1$. □

3. Let $\omega := \frac{1}{2}(-1+\sqrt{3}\,\mathrm{i})$ in $\mathbb{C}$ be one of the complex roots of the polynomial x^2+x+1 in $\mathbb{C}[x]$. Prove that the commutative domain $\mathbb{Z}[\omega] := \big\{a+b\,\omega \mid a,b\in\mathbb{Z}\big\}\subset\mathbb{C}$ is a Euclidean domain with the function $\nu\colon\mathbb{Z}[\omega]\to\mathbb{N}$ defined, for any $a+b\,\omega$ in $\mathbb{Z}[\omega]$, by $\nu(a+b\,\omega)=a^2-a\,b+b^2$.

Solution. First, observe that $\omega+\overline{\omega}=-1$, $|\omega|^2=\omega\,\overline{\omega}=1$, and

$$\begin{aligned}|a+b\,\omega|^2 &= (a+b\,\omega)(a+b\,\overline{\omega}) \\ &= a^2+a\,b\,(\omega+\overline{\omega})+b^2\ |\omega|^2=a^2-a\,b+b^2=\nu(a+b\,\omega)\,.\end{aligned}$$

The elements in the ring $\mathbb{Z}[\omega]$ lie on a lattice of unit-side triangles in the complex plane because $\omega^3=1$. For any z in $\mathbb{Z}[\omega]$, the ideal $\langle z\rangle$ forms a similar lattice. Writing $z=r\,e^{\mathrm{i}\theta}$ where r and θ are real numbers satisfying $0\leqslant r$ and $0\leqslant\theta<2\pi$, the lattice corresponding to the ideal $\langle z\rangle$ is obtained by rotating through the angle θ followed by stretching by the factor $r=|z|$. For any complex number w in

$\mathbb{Z}[\omega]$, there is at least one point of the lattice corresponding to the ideal $\langle z \rangle$ whose squared distance from w is at most $\frac{1}{3}\,|z|^2 = \frac{1}{3} r^2$; see Figure 1. Let $q\,z$ be that a closed

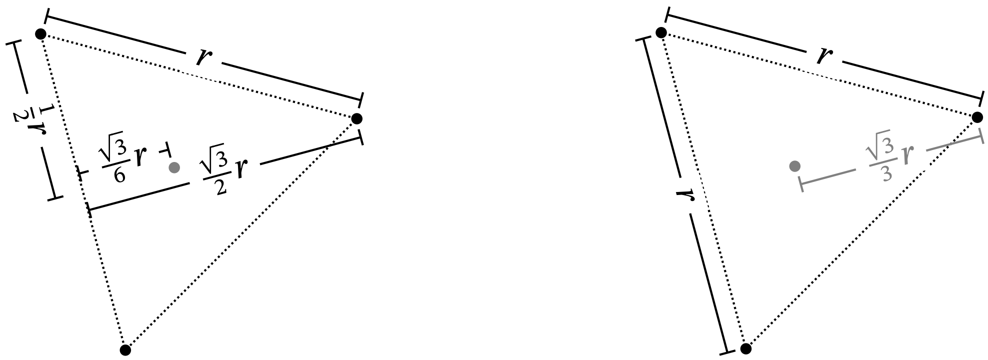

Figure 1. Nearest element in triangular lattice

point and set $p := w - q\,z$. Therefore, we obtain $|p|^2 \leqslant \frac{1}{3}\,|z|^2 < |z|^2$ as required. $\square$