2.6 Multiplicity of Roots

2.6.1 Definition. Let m be a positive integer. For any $f \in R[x]$, the ring element $a \in R$ is a root of ***multiplicity*** m if f is divisible by $(x-a)^m$ but not $(x-a)^{m+1}$. A root of multiplicity 1 is a ***simple*** root and a root of multiplicity two is a ***double*** root.

2.6.2 Lemma. *Let m and n be the multiplicities of the root $a \in R$ for the polynomials $f \in R[x]$ and $g \in R[x]$.*

- *The sum $f+g$ has a root of multiplicity at least $\min\{m,n\}$ at a and is equal to $\min\{m,n\}$ if $m \neq n$.*
- *The product fg has a root of multiplicity at least $m+n$ and it is equal to $m+n$ if R is domain.*

Sketch of Proof. Set $f(x) = (x-a)^m\, p(x)$ and $g(x) = (x-a)^n\, q(x)$ where $p, q \in R[x]$ satisfy $p(a) \neq 0 \neq q(a)$. When $m \leqslant n$, it follows that $f(x)+g(x) = (x-a)^m \big(p(x)+(x-a)^{m-n}\, q(x)\big)$ and a is not a root of $p(x)+(x-a)^{m-n}\, q(x)$. We have $f(x)\, g(x) = (x-a)^{m+n}\, p(x)\, q(x)$ and $p(a)\, q(a) \neq 0$ if R is a domain. □

2.6.3 Proposition. *Let R be a domain. Given a nonzero $f \in R[x]$ with distinct roots $a_1, a_2, \ldots, a_\ell$ having multiplicities $m_1, m_2, \ldots, m_\ell$, there is a polynomial $g \in R[x]$ such that $a_1, a_2, \ldots, a_\ell$ are not roots of g and*

$$f(x) = (x-a_1)^{m_1}\, (x-a_2)^{m_2} \cdots (x-a_\ell)^{m_\ell}\, g(x)$$

Proof. We proceed by induction on ℓ. The case $\ell = 1$ is covered by Proposition 2.5.8. Suppose that

$$f(x) = (x-a_1)^{m_1}\, (x-a_2)^{m_2} \cdots (x-a_{\ell-1})^{m_{\ell-1}}\, h(x)$$

Since R is a domain and the root a_ℓ is distinct from $a_1, a_2, \ldots, a_{\ell-1}$, it follows that a_ℓ is not a root of the polynomial

$$(x-a_1)^{m_1}\, (x-a_2)^{m_2} \cdots (x-a_{\ell-1})^{m_{\ell-1}}\,.$$

The element a_ℓ is a root of multiplicity m_ℓ of the polynomial h and Proposition 2.5.8 yields $h(x) = (x-a_\ell)^{m_\ell}\, g(x)$ where $a_1, a_2, \ldots, a_{\ell-1}$ are not roots of g. □

2.6.4 Corollary. *Let R be a domain. Given nonzero polynomial f in $R[x]$ of degree m, the sum of multiplicities of all the roots of f is at most m.* □

2.6.5 Example. Over the ring $R = \mathbb{Z}/\langle 2\rangle \times \mathbb{Z}/\langle 2\rangle$, all four elements are roots of the polynomial $x^2 - x \in R[x]$. ✧

2.6.6 Corollary. *Let R be a domain and consider nonzero polynomials $f, g \in R[x]$ of degree at most m. If there exists $m+1$ pairwise distinct elements $a_0, a_1, \ldots, a_m$ in R such that $f(a_i) = g(a_i)$ for all $0 \leqslant i \leqslant m$, then we have $f = g$.*

Proof. The polynomial $h := f - g$ has degree at most m and has at least $m+1$ roots, so $h = 0$. □

2.6.7 Proposition (Lagrange Interpolation). *Let K be a field and let $a_0, a_1, \dots, a_m$ be $m+1$ distinct elements of K. For any $b_0, b_1, \dots, b_m \in K$, there exists a unique polynomial $f \in K[x]$ of degree at most m such that $f(a_j) = b_j$ for all $0 \leqslant j \leqslant m$.*

Proof. Uniqueness follows from Corollary 2.6.6. For all $0 \leqslant j \leqslant m$, consider

$$g_j(x) := \prod_{k \neq j} \frac{(x - a_k)}{(a_j - a_k)}\,.$$

It follows that $\deg(g_j) = m$ and $g_j(a_k) = \delta_{j,k}$. Thus, we may take $f(x) := \sum_{j=0}^{m} b_j\, g_j(x)$. □

2.6.8 Proposition. *Let m be a positive integer. If $a \in R$ is a root of the polynomial $f \in R[x]$ having multiplicity m, then a is a root of the derivative $Df \in R[x]$ having multiplicity at least $m-1$. When $m\,1_R \neq 0$ in R, then a is a root of Df having multiplicity $m-1$.*

Let m be a positive integer such that $m\,1_R = 0$ in R. For the polynomial $f := x^m$, we have $Df = m\,x^{m-1} = 0$, so the derivative has 0 as a root of arbitrarily high multiplicity.

Proof. Proposition 2.5.8 establishes that there exists $g \in R[x]$ such that $f = (x-a)^m\, g$ and $g(a) \neq 0$. It follows that

$$Df = m(x-a)^{m-1}\, g + (x-a)^m\, Dg = (x-a)^{m-1}\big(m\, g + (x-a)\, Dg\big)$$

giving the first part. Since the evaluation map sends the polynomial $m\, g + (x-a)\, Dg$ to the ring element $m\, g(a)$, this ring element is nonzero when $m\,1_R \neq 0$. □

2.6.9 Corollary. *Let m be an integer such that $m!\,1_R \neq 0$ in the ring R. An element $a \in R$ is a root of the polynomial $f \in R[x]$ having multiplicity m if and only if a is a root of $f, Df, \dots, D^{m-1}f$ and not a root of $D^m f$.*

Proof. Follows immediately from Proposition 2.6.8. □

2.7 Euclidean Domains

Last updated: 2020–10–15

2.7.1 Definition. A ***Euclidean domain*** is a domain R equipped with a function $\partial : R \setminus \{0\} \to \mathbb{N}$ such that
- for all $f, g \in R \setminus \{0\}$, we have $\partial(f) \leqslant \partial(fg)$;
- for all $f \in R$ and all $g \in R \setminus \{0\}$, there exists $q, r \in R$ such that $f = q\,g + r$ and either $r = 0$ or $\partial(r) < \partial(g)$.

2.7.2 Example. The integers $\mathbb{Z}$ form a Euclidean domain where the function $\partial : \mathbb{Z} \setminus \{0\} \to \mathbb{N}$ is defined by $\partial(m) := |m|$. ✧

2.7.3 Example. For any field K, the polynomial ring $K[x]$ forms a Euclidean domain where the function $\partial : K[x] \setminus \{0\} \to \mathbb{N}$ is defined by $\partial(f) := \deg(f)$. ✧

2.7.4 Example. For any field K, the formal power series ring $K[[x]]$ is a Euclidean domain where the function $\partial : K[[x]] \setminus \{0\} \to \mathbb{N}$ is defined by $\partial(f) = \operatorname{ord}(f)$ and

$$\operatorname{ord}(f) := \min\left(k \;\middle|\; a_k \neq 0 \text{ where } f = \textstyle\sum_{k \geqslant 0} a_k\, x^k\right). \qquad \diamond$$

When $m = \operatorname{ord}(f) \leqslant \operatorname{ord}(g) = n$, we have $f = 0\,g + f$. Otherwise $m > n$, we have $f = x^m\,p$ and $g = x^n\,q$ where $p, q \in K[[x]]$ are units, so $f = x^{m-n}\,p\,q^{-1}g + 0$.

2.7.5 Problem. Show that the ring $\mathbb{Z}[\mathrm{i}]$ is a Euclidean domain where $\partial : K[[x]] \setminus \{0\} \to \mathbb{N}$ is defined by $\partial(a + b\mathrm{i}) := a^2 + b^2$.

Geometric Solution. The elements of $\mathbb{Z}[\mathrm{i}]$ form a square lattice in $\mathbb{C}$. The ideal $\langle z \rangle$, all multiples of z, forms a similar lattice: if we write $z = re^{\mathrm{i}\theta}$, then the lattice corresponding to $\langle z \rangle$ is obtained by rotating through the angle θ followed by stretching by the factor $r = |z|$. It is clear that for every $w \in \mathbb{C}$, there is at least one point of the lattice corresponding to $\langle z \rangle$ whose square distance from w is at most $(1/2)\,|z|^2$. Let that point be qz and set $p := w - qz$. It follows that $|p|^2 \leqslant (1/2)\,|z|^2 < |z|^2$ as required. Since there may be more than one choice for qz, this division with remainder is not unique. □

Algebraic Solution. Divide $w \in \mathbb{C}$ by z: $w = cz$ where $c = x + y\mathrm{i} \in \mathbb{C}$. Choose a nearest Gaussian integer: $x := a + x_0$, $y := b + y_0$ where $a, b \in \mathbb{Z}$ and $-1/2 \leqslant x_0, y_0 < 1/2$. It follows that the product $(a + b\mathrm{i})z$ is the required point in $\langle z \rangle$ because we have $|x_0 + y_0\mathrm{i}|^2 < 1/2$ and $|w - (a + b\mathrm{i})z|^2 = |z(x_0 + y_0\mathrm{i})|^2 < (1/2)\,|z|^2$. □

2.7.6 Definition. A ***principal ideal domain*** is a domain in which every ideal is principal.

2.7.7 Theorem. *Every Euclidean domain is a principal ideal domain.*

Proof. Let I be an ideal in a Euclidean domain R. When $I = \langle 0 \rangle$, the ideal I is principal, so we may assume $I \neq \langle 0 \rangle$. By the well-ordering property of the integers, the set of all degrees of nonzero elements

in I has a minimum, say n. Choose $f \in I$ with $\partial(f) = n$. Since $f \in I$, we have $\langle f \rangle \subseteq I$. For any $g \in I$, there exists $q, r \in R$ with $g = qf + r$ and either $r = 0$ or $\partial(r) < \partial(f)$. However, we have $r = f - qg \in I$ so our choice of f implies that $r = 0$. Therefore, we deduce that $g = qf$ and $I \subseteq \langle f \rangle$. □

2.7.8 Problem. Show that the ideal $\langle 2, x \rangle$ in $\mathbb{Z}[x]$ is not principal.

Solution. Suppose that $\langle f \rangle = \langle 2, x \rangle$. It follows that $gf = 2$ for some $g \in \mathbb{Z}[x]$. Since $\deg(g) + \deg(f) = \deg(2) = 0$, we see that $f, g \in \mathbb{Z}$. Hence, we have $f = \{\pm 1, \pm 2\}$. Since $\langle 2, x \rangle$ is a maximal ideal, the element f cannot be a unit, so $f = \pm 2$. However, we would also have $x \in \langle f \rangle$, so $x = 2h$ for some $h \in \mathbb{Z}[x]$ which is absurd. □

2.7.9 Problem. Show that the ideal $\langle 2, 1 - \sqrt{-3} \rangle$ in $\mathbb{Z}[\sqrt{-3}] \subseteq \mathbb{C}$ is not principal.

Solution. Suppose that $\langle a + b\sqrt{-3} \rangle = \langle 2, 1 - \sqrt{-3} \rangle$. It follows that $g(a + b\sqrt{-3}) = 2$ for some $g \in \mathbb{Z}[\sqrt{-3}]$. Taking absolute values in $\mathbb{C}$ gives $|g|\ (a^2 + 3b^2) = 2$, so $a^2 + 3b^2 \in \{\pm 1, \pm 2\}$. Because $a, b \in \mathbb{Z}$ we must have $a = \pm 1$, $b = 0$ which contradicts the fact that $\langle 2, 1 - \sqrt{-3} \rangle$ is a maximal ideal. □

2.7.10 Example. The rings

- $\mathbb{Z}[\alpha] = \{a + b\alpha \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$ where $\alpha := (1 + \sqrt{-19})/2$,
- $\mathbb{R}[x, y]/\langle x^2 + y^2 + 1 \rangle$,
- $\mathbb{Q}[x, y]/\langle y^2 - 2x^2 - 5 \rangle$,

are principal ideal domains but not Euclidean domains. For more details, see

- Jack C. Wilson, A principal ideal ring that is not a Euclidean ring, *Mathematics Magazine* **46** (1973) 34–38;
- Anthony J. Bevelacqua, A family of non-Euclidean PIDs, *American Mathematical Monthly* 123 (2016), no. 9, 936–939. ✧