D-MATH Algebra I HS17
Prof. Emmanuel Kowalski

Solution 3

Fraction Fields, Polynomial Rings

1. Show that the fraction field of $\mathbb{Z}[i]$ is

$$\mathbb{Q}(i) = \{a + ib : a, b \in \mathbb{Q}\}.$$

Similarly, show that the fraction field of $\mathbb{Z}[\sqrt{2}]$ is $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

Solution: We prove some useful lemmas.

Lemma 1. *Let K be a field, S a* non-trivial *ring (that is, such that $1_S \neq 0_S$) and $\varphi : K \longrightarrow S$ a ring homomorphism. Then φ is injective.*

Proof. Let $x, y \in K$ and suppose that $\varphi(x) = \varphi(y)$. Then, since φ is a ring homomorphism, $\varphi(x - y) = \varphi(x) - \varphi(y) = 0_S$. If $x - y = 0_K$, then we are done. Else, $(x - y)$ has an inverse $(x - y)^{-1} \in K$ and

$$0_S = \varphi(x - y)\varphi((x - y)^{-1}) = \varphi((x - y)(x - y)^{-1}) = \varphi(1_K) = 1_S,$$

a contradiction. □

Lemma 2 (Universal Property of the fraction field)**.** *Let R be an integral domain and $F := \mathrm{Frac}(R)$. Let $\iota : R \hookrightarrow F$ be the inclusion $r \mapsto \frac{r}{1}$. For every field K and injective ring homomorphism $f : R \hookrightarrow K$ there exists a unique ring homomorphism $\overline{f} : F \longrightarrow K$ such that $\overline{f} \circ \iota = f$, i.e., the following diagram commutes:*

$$\begin{tikzcd}
R \arrow[r, "\iota"] \arrow[dr, "f"'] & F = \mathrm{Frac}(R) \arrow[d, "\overline{f}"] \\
 & K.
\end{tikzcd}$$

It is given by $\overline{f}(\frac{r}{s}) := f(r)f(s)^{-1}$.

Proof. Suppose $\overline{f} : F \longrightarrow K$ is such a morphism and let $\frac{r}{s} \in F$. Then, $\overline{f}(\frac{r}{1}) = \overline{f}(\iota(r)) = f(r)$ and $\overline{f}(\frac{s}{1}) = \overline{f}(\iota(s)) = f(s)$. Then, in K, there is an equality

$$f(r) = \overline{f}\left(\frac{r}{1}\right) = \overline{f}\left(\frac{r}{s}\right)\overline{f}\left(\frac{s}{1}\right) = \overline{f}\left(\frac{r}{s}\right)f(s)$$

which implies, by multiplying by $f(s)^{-1}$, that

$$\overline{f}\left(\frac{r}{s}\right) = f(r)f(s)^{-1}. \tag{1}$$

Hence there is at most one way to define $\overline{f}$ so that the diagram above commutes. Let us check that (1) is indeed a well-defined ring homomorphism F $\longrightarrow K$. First, notice that for $\frac{r}{s} \in F$ the elements s is supposed to be $\neq 0$, so that $f(s) \neq 0$ since f is injective and $f(s)^{-1} \in K$, so that the expression (1) makes sense. Now suppose that $\frac{r}{s} = \frac{r'}{s'}$, that is, $rs' = r's$. Then, since f is a ring homomorphism,

$$\begin{aligned}\overline{f}\left(\frac{r}{s}\right) &= f(r)f(s)^{-1} = f(r')f(r)f(s')f(r')^{-1}f(s)^{-1}f(s')^{-1} \\ &= f(r')f(rs')f(r's)^{-1}f(s')^{-1} \overset{rs'=r's}{=} f(r')f(s')^{-1} = \overline{f}\left(\frac{r'}{s'}\right)\end{aligned}$$

so that $\overline{f}$ is well-defined. Clearly,

$$\overline{f}(1_F) = \overline{f}\left(\frac{1}{1}\right) = f(1)f(1)^{-1} = 1 \cdot 1 = 1.$$

The fact that $\overline{f}$ respects the sum and the multiplication is similarly proven, by using its definition. This concludes the proof of our claim. □

Now let us consider $R = \mathbb{Z}[i]$. We first prove that $\{a + ib : a, b \in \mathbb{Q}\}$ is a field. It is easily checked that this subset of $\mathbb{C}$ is closed under sum and multiplication and contains 1, so that it is a subring of the field $\mathbb{C}$ and as such it is an integral domain. Given $a, b \in \mathbb{Q}$, such that $(a, b) \neq (0, 0)$, we see that $a + ib \neq 0$ and $N(a + ib) = (a + ib)(a - ib) = a^2 + b^2 \neq 0$. Then

$$1 = \frac{a - ib}{a^2 + b^2}(a + ib) = \left(\frac{a}{a^2 + b^2} - i\frac{b}{a^2 + b^2}\right)(a + ib),$$

so that $(a + ib)$ has inverse

$$\frac{a}{a^2 + b^2} - i\frac{b}{a^2 + b^2} \in \{a + ib : a, b \in \mathbb{Q}\}.$$

This implies that $\mathbb{Q}(i) = \{a + ib : a, b \in \mathbb{Q}\}$ is a field (a better way to define $\mathbb{Q}(i)$ is actually to define it as the smallest subfield of $\mathbb{C}$ containing $\mathbb{Q}$ and i—what we have just shown being that $\mathbb{Q}(i) = \{a + ib : a, b \in \mathbb{Q}\}$). The inclusion $f : \mathbb{Z}[i] \longrightarrow \mathbb{Q}(i)$ sending $a + ib \mapsto a + ib$ is a ring homomorphism, so that there exists a unique ring homomorphism $\overline{f} : \mathrm{Frac}(\mathbb{Z}[i]) \longrightarrow \mathbb{Q}(i)$ such that the following diagram commutes:

$$\begin{tikzcd}
\mathbb{Z}[i] \arrow[r, "\iota"] \arrow[dr, "f"'] & \mathrm{Frac}(\mathbb{Z}[i]) \arrow[d, "\overline{f}"] \\
& \mathbb{Q}(i)
\end{tikzcd}$$

By Lemma 1, $\overline{f}$ is injective. Moreover, for $\alpha + i\beta \in \mathbb{Q}$ we can find integers $a, b, d \in \mathbb{Z}$ such that $\alpha + i\beta = (a + ib)d^{-1}$. Then, as seen in Lemma 2,

$$\overline{f}\left(\frac{a+ib}{d}\right) = (a+ib)d^{-1} = \alpha + i\beta,$$

so that $\overline{f}$ is surjective. Hence $\overline{f}$ is the desired isomorphism $\mathrm{Frac}(\mathbb{Z}[i]) \cong \mathbb{Q}(i)$.

Similarly for $R = \mathbb{Z}[\sqrt{2}]$, we first check that $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is a field by noticing that each non trivial $a + \sqrt{2}b \in \mathbb{Q}$ has inverse

$$(a+\sqrt{2}b)^{-1} = \frac{a-\sqrt{2}b}{(a-\sqrt{2}b)(a+\sqrt{2}b)} = \frac{a-\sqrt{2}b}{a^2-2b^2} = \frac{a}{a^2-2b^2} - \sqrt{2}\frac{b}{a^2-2b^2}.$$

Then, again, we have a unique ring homomorphism $\overline{f} : \mathrm{Frac}(\mathbb{Z}[\sqrt{2}]) \longrightarrow \mathbb{Q}(\sqrt{2})$ making the following diagram commute:

$$\begin{tikzcd}
\mathbb{Z}[\sqrt{2}] \arrow[r, "\iota"] \arrow[dr, "f"'] & \mathrm{Frac}(\mathbb{Z}[\sqrt{2}]) \arrow[d, "\overline{f}"] \\
& \mathbb{Q}(\sqrt{2})
\end{tikzcd}$$

The ring homomorphism $\overline{f}$ is injective by Lemma 1 and surjective because each $\alpha + \sqrt{2}\beta \in \mathbb{Q}(\sqrt{2})$ can be written as $\frac{a+b\sqrt{2}}{d}$ for suitable $a, b, d \in \mathbb{Z}$, so that it lies in the image of $\overline{f}$. Then $\overline{f}$ is an isomorphism $\mathrm{Frac}(\mathbb{Z}[\sqrt{2}]) \cong \mathbb{Q}(\sqrt{2})$.

2. Let R be an integral domain. Show that $R[X]^\times = R^\times$. Can $R[X]$ be a field?

   Solution: Of course, $A^\times \subseteq A[X]^\times$ because $A \subseteq A[X]$. To conclude, we just need to prove that any invertible $f \in A[X]$ is indeed in $A^\times$. Suppose that $f \in A[X]^\times$, and that $fg = 1$ for some $g \in A[X]$. Of course f and g cannot be 0, so that we have well-defined $\deg(f), \deg(g) \geqslant 0$. Being A a domain, we have that $\deg(fg) = \deg(f) + \deg(g)$ (because the product of the leading coefficients is the leading coefficient of the product, as it cannot vanish). Hence $0 = \deg(1) = \deg(f) + \deg(g)$, and the only possibility is that $\deg(f) = \deg(g) = 0$. Hence $f, g \in A$, giving $f \in A^\times$.

   The ring $R[X]$ cannot be field because $X \in R[X]$ has no inverse by degree reasons: $Xg(X) = 1$ for $g(X) \in R[X]$ would imply that $\deg(g)+1 = \deg(1) = 0$, impossible. [*This argument works because R is assumed to be a domain. Notice, however, that if R were a commutative ring but not a domain, then $R[X]$ would not be a domain (it would contain the non-trivial zero-divisors of R), so that $R[X]$ would not be a field. Hence $R[X]$ is never a field, whatever commutative ring R we consider.*]

3. (a) Prove that $1 + 2X$ is a unit in $(\mathbb{Z}/4\mathbb{Z})[X]$.

   (*b) Determine $(\mathbb{Z}/4\mathbb{Z})[X]^\times$.

(c) Find $f \in (\mathbb{Z}/4\mathbb{Z})[X]$ of degree 2 such that $f(x) = 0$ for all $x \in \mathbb{Z}/4\mathbb{Z}$.

Solution:

(a) We notice that $(1+2X)^2 = 1 + 4X + 4X^2 = 1$ since $4 = 0$ in $\mathbb{Z}/4\mathbb{Z}$. Hence $1 + 2X$ is an inverse of itself and as such it is a unit of $(\mathbb{Z}/4\mathbb{Z})[X]$.

(b) Taking inspiration from part (a), we notice that for each $f \in (\mathbb{Z}/4\mathbb{Z})[X]$ there is an equality $(1+2f)^2 = 1+4f+4f^2$. We now prove that all units in $(\mathbb{Z}/4\mathbb{Z})[X]$ are of this shape. Notice that the map

$$\begin{aligned} \mathbb{Z}/4\mathbb{Z} &\longrightarrow \mathbb{Z}/2\mathbb{Z} \\ x &\longmapsto x \pmod 2 \end{aligned}$$

is a ring homomorphism. Indeed, it is well defined because if $x, x' \in \mathbb{Z}$ are congruent modulo 4, that is $4|x' - x$, then $2|x' - x$, so that x and x' are congruent modulo 2, and moreover it respects sums and multiplications, and it sends $1 \mapsto 1$.

As seen in class, there exists a unique ring homomorphism

$$\theta : (\mathbb{Z}/4\mathbb{Z})[X] \longrightarrow (\mathbb{Z}/2\mathbb{Z})[X]$$

sending $X \mapsto X$ and $\mathbb{Z}/4\mathbb{Z} \ni a \mapsto a \pmod 2$. It is the one which reduces all coefficients modulo 2. If $g, h \in (\mathbb{Z}/4\mathbb{Z})[X]^\times$, with $gh = 1$, then $1 = \theta(1) = \theta(gh) = \theta(g)\theta(h)$, so that $\theta(g) \in (\mathbb{Z}/2\mathbb{Z})[X]^\times$. But $\mathbb{Z}/2\mathbb{Z}$ is a field and in particular an integral domain, so that $(\mathbb{Z}/2\mathbb{Z})[X]^\times = \{1\}$ by Exercise 2. This means that all non-constant coefficients of g are congruent to 0 or 2 modulo 4, whereas the constant coefficient can be only 1 or 3 modulo 4. In particular, the degree-i coefficient of g for $i > 0$ can be written as $2 \cdot a_i$ for some $a_i \in \mathbb{Z}/4\mathbb{Z}$, whereas the constant coefficient of g can be written as $1 + 2 \cdot a_0$ for some $a_0 \in \mathbb{Z}/4\mathbb{Z}$. Altogether, $g = 1 + 2(a_0 + a_1 X + \cdots + a_n X^n)$ and we can conclude that

$$(\mathbb{Z}/4\mathbb{Z})[X]^\times = \{1 + 2f : f \in (\mathbb{Z}/4\mathbb{Z})[X]\}\,.$$

(c) We first notice that the polynomial $t := X^2 + X$ satisfies the condition $t(\alpha) \in \{0, 2\}$ for all $\alpha \in \mathbb{Z}/4\mathbb{Z}$. Hence, since $2 \cdot 2 = 0$ in $\mathbb{Z}/4\mathbb{Z}$, the polynomial $2t = 2X^2 + 2X$, still of degree-2, vanishes on every $a \in \mathbb{Z}/4\mathbb{Z}$.

4. Let R be an integral domain.

(a) Prove that $R[[X]]$ is an integral domain.

(b) Prove that $1 - X \in R[[X]]^\times$.

(c) Let now $R = K$ be a field. Prove:

$$K[[X]]^\times := \left\{ \sum_{n\in\mathbb{N}} a_n X^n | a_0 \neq 0 \right\}.$$

[*Hint:* Find the coefficients of inverse power series inductively.]

Solution:

(a) Recall that an element of $R[[X]]$ can be written as a formal power series $a = \sum_{i=0}^\infty a_i X^i$. Consider another element $b = \sum_{j=0}^\infty j_j X^j$. Recall how the product ab is defined:

$$ab = \left(\sum_{i=0}^\infty a_i X^i\right) \cdot \left(\sum_{j=0}^\infty b_j X^j\right) = \sum_{k=0}^\infty \Big(\sum_{\substack{i+j=k \\ i,j>0}} a_i b_j \Big) X^k \tag{2}$$

We first prove that X^ℓ is not a zero-divisor for any $k \in \mathbb{N}$. This is because multiplication by X^ℓ translates the coefficients of b up by adding some zero coefficients in the beginning, as can be seen formally by considering the product above for $a = X^\ell$, that is, $a_i = \delta_{i\ell}$. Then

$$\sum_{\substack{i+j=k \\ i,j>0}} a_i b_j = \sum_{\substack{i+j=k \\ i,j>0}} \delta_{i,\ell} b_j = \begin{cases} b_{k-\ell} & k \geqslant \ell \\ 0 & k < \ell, \end{cases}$$

so that $X^\ell b = 0$ implies that $b_{k-\ell} = 0$ for each $k \geqslant \ell$, i.e., $b = 0$.

Suppose that $ab = 0$ and $a \neq 0$.

- We reduce to the case $a_0 \neq 0$. Let $i_0 = \min\{i \in \mathbb{N} : a_i \neq 0\}$. Then a is divisible by X^{i_0}, as can be seen by defining $\alpha = \sum_{u=0}^\infty a_{u+i_0} X^u$ and proving similarly as done above for the product $X^\ell b$ that

$$X^{i_0}\alpha = \sum_{u=0}^{i_0-1} 0 \cdot X^u + \sum_{u=i_0}^\infty a_{u+i_0-i_0} X^u = a.$$

  Then $ab = X^{i_0}\alpha b$ and we notice that α has non-zero constant coefficient. Moreover, since $0 = ab = X^{i_0}\alpha b$ and X^{i_0} is not a zero divisor, we deduce that $\alpha b = 0$. This means that, without loss of generality, we can assume that $a_0 \neq 0$ from the beginning.
- We hence assume that $a_0 \neq 0$. Then, looking at the constant coefficient in (2), the assumption $ab = 0$ implies that $a_0 b_0 = 0$. Since R is a domain and $a_0 \neq 0$, it must be the case that $b_0 = 0$.

- Suppose that $b_0, \ldots, b_{k-1} = 0$. Then, looking at the degree-k coefficient in (2), the assumption $ab = 0$ implies that

$$0 = \sum_{\substack{i+j=k \\ i,j>0}} a_i b_j = \sum_{\substack{0 \leqslant j < k \\ i=k-j}} a_i b_j + a_0 b_k = \sum_{\substack{0 \leqslant j < k \\ i=k-j}} a_i \cdot 0 + a_0 b_k = a_0 b_k,$$

which tells us that $b_k = 0$ since $a_0 \neq 0$ and R is a domain.

Hence, by induction, we proved that $b = 0$, so that $R[[X]]$ is an integral domain.

Alternative, faster solution: Let $a, b \in R[[X]]$ and assume that $a, b \neq 0$. Let $s, t \in \mathbb{N}$ be the smallest integers such that $a_s \neq 0$ and $b_t \neq 0$. Then the $(s+t)$-th coefficient of ab is $a_s b_t \neq 0$, which implies that $ab \neq 0$. Hence $R[[X]]$ is an integral domain.

(b) Basic calculus suggests that

$$\frac{1}{1-X} = \sum_{j=0}^{\infty} X^j.$$

Let us check that this is the case by computing $(1-X)\sum_{j=0}^{\infty} X^j$ with the definition (2) above, $1 - X$ having coefficients $1, -1, 0, 0, \ldots$:

$$(1-X)\sum_{j=0}^{\infty} X^j = 1 \cdot 1X^0 + \sum_{k=1}^{\infty}(1 + 1 \cdot (-1))X^k = 1 + \sum_{k=1}^{\infty} 0X^k = 1.$$

This proves that $1 - X \in R[[X]]$.

(c) The equality $ab = 1$ for $a, b \in K[[X]]$ (with coefficients a_i and b_j respectively) is equivalent to the equalities

$$\begin{cases} a_0 b_0 = 1 \\ a_0 b_k = -\sum_{j=0}^{k-1} a_{k-j} b_j, \quad k > 0. \end{cases}$$

The first equation tells us that if $a \in K[[X]]^\times$ then $a_0 \neq 0$. Conversely, if $a_0 \neq 0$, there exists $a_0^{-1} \in K$ and the equations above are equivalent to

$$\begin{cases} b_0 = a_0^{-1} \\ b_k = -a_0^{-1} \sum_{j=0}^{k-1} a_{k-j} b_j, \quad k > 0. \end{cases}$$

which inductively define the coefficients b_k of the inverse b of a. We can hence conclude that

$$K[[X]]^\times = \left\{ \sum_{n \in \mathbb{N}} a_n X^n : a_0 \neq 0 \right\}.$$

5. Let R be a commutative ring.

   (a) Show that there exists a unique map $D : R[X] \longrightarrow R[X]$ such that
   $$\begin{aligned} D(X^i) &= iX^{i-1}, \quad i \geqslant 1 \\ D(1) &= 0 \end{aligned}$$
   which is R-*linear*, i.e., such that
   $$\forall r \in R, \forall f, g \in R[X],\ D(rf+g) = rD(f) + D(g).$$

   (b) Is D a ring homomorphism?

   (c) Prove that for all $f, g \in R[X]$ one has
   $$D(fg) = fD(g) + gD(f)$$

   (*d) We say that $\alpha \in R$ is a *multiple root* of $f \in R[X]$ if there exists $g \in R[X]$ such that $f = (X-\alpha)^2 g$. Prove: α is a multiple root of f if and only if $f(\alpha) = D(f)(\alpha) = 0$. [*Hint:* Notice that $X^k = (X-\alpha+\alpha)^k = (X-\alpha)g_k + \alpha^k$ for some $g_k \in R[X]$ and deduce that for each $h \in R[X]$ we can write $h = (X-\alpha)\ell + h(\alpha)$ for some $\ell \in R[X]$. You'll need to use part (b) as well.]

Solution:

(a) Suppose such a map D exists. Notice that R-linearity implies additivity because in the definition one can take $r = 1$. Then,
$$D(0) = D(0+0) = D(0) + D(0),$$
so that $0 = D(0)$. Now, the condition of linearity for $g = 0$ gives
$$\forall r \in R, \forall f \in R[X],\ D(rf) = D(rf+0) = rD(f) + D(0) = rD(f). \tag{3}$$
The additivity of D can be inductively proven to generalize to finite sums, so that if $f = \sum_{i=0}^n a_i X^i$ the given conditions on D give
$$D(f) = D\left(\sum_{i=0}^n a_i X^i\right) = \sum_{i=0}^n D\left(a_i X^i\right) \overset{(3)}{=} \sum_{i=0}^n a_i D(X^i) = \sum_{i=1}^n a_i i X^{i-1}. \tag{4}$$
so that D is uniquely defined. Let us now check that (4) indeed defines an R-linear map satisfying the given properties. Those properties are trivially satisfied by construction. As concerns linearity, let $f = \sum_{i=0}^n a_i X^i,\ g = \sum_{j=0}^n b_j X^j \in R[X]$ and $r \in R$ (the sums describing f and g range up to

$n = \max \deg(f), \deg(g)$, by eventually adding zero higher coefficients to one of the two polynomials). Then $rf + g = r\sum_{j=0}^{n}(a_j r + b_j)X^j$ and

$$\begin{aligned} D(rf+g) &= \sum_{j=1}^{n}(a_j r + b_j)jX^{j-1} \\ &= r\sum_{j=1}^{n} a_j jX^{j-1} + \sum_{j=1}^{n} b_j jX^{j-1} = rD(f) + D(g), \end{aligned}$$

so that D is R-linear and we are done.

(b) The map D cannot be a ring homomorphism, since it sends $1 \mapsto 0 \neq 1$. Unless R is the trivial ring, in which case $R[X] = 0$ and $D : 0 \longrightarrow 0$ is a ring homomorphism as well.

(c) The identity can be directly checked by writing $f = \sum_{i=0}^{m} a_i X^i$ and $g = \sum_{j=0}^{n} b_j X^j$ and computing both sides. An equivalent (but faster) way to do this is to observe that both sides of the identity $D(fg) = fD(g) + gD(f)$ are linear in f and in g. Then it is enough to check the equality for an arbitrary f and $g = X^k$, $k \geqslant 0$, and this is then equivalent to check the equality for $f = X^j$ and $g = X^k$, with $j, k \geqslant 0$, which is immediate:

$$D(X^jX^k) = D(X^{j+k}) = (j+k)D^{j+k-1} = X^j \cdot kX^{k-1} + X^k \cdot jX^{j-1}.$$

(d) We follow the hint. The equalities

$$\begin{aligned} X^k = (X - \alpha + \alpha)^k &= \alpha^k + \sum_{i=1}^{k}\binom{k}{i}(X-\alpha)^i\alpha^{k-i} \\ &= \alpha^k + (X-\alpha)\sum_{i=1}^{k}\binom{k}{i}(X-\alpha)^{i-1}\alpha^{k-i} = \alpha^k + (X-\alpha)g_k, \end{aligned}$$

holding for $g_k = \sum_{i=1}^{k}\binom{k}{i}(X-\alpha)^{i-1}\alpha^{k-i}$, imply for $h = \sum_{k=0}^{n} u_k X^k$ that

$$\begin{aligned} h &= \sum_{k=0}^{n} u_k X^k = \sum_{k=0}^{n}(u_k\alpha^k + u_k(X-\alpha)g_k) \\ &= \sum_{k=0}^{n} u_k\alpha^k + (X-\alpha)\sum_{k=0}^{n} u_k g_k = h(\alpha) + (X-\alpha)\ell_h \end{aligned}$$

for $\ell_h = \sum_{k=0}^{n} u_k g_k \in R[X]$.

Let $f \in R[X]$ and assume that $f = (X-\alpha)\ell$ for some $\ell \in R[X]$. Then $f(\alpha) = 0 \cdot g(0) = 0$. Conversely, writing $f = f(\alpha) + (X-\alpha)\ell_f$ as above, we see that $f(\alpha) = 0$ implies that $f = (X-\alpha)\ell$ for some $\ell = \ell_f$. This proves the following statement:

$$f(\alpha) = 0 \iff \exists \ell \in R[X] : f = (X-\alpha)\ell$$

Let's now move one degree further using D.

Suppose that α is a multiple root of f, that is, $f = (X-\alpha)^2 g$ for some $g \in R[X]$. In particular we can write $f = (X-\alpha)\ell$ for $\ell = (X-\alpha)g$ so that $f(\alpha) = 0$ by the statement we just proved. Moreover, by part (c),

$$D(f) = D((X-\alpha)^2)g + (X-\alpha)^2 D(g) = 2(X-\alpha)g + (X-\alpha)^2 D(g)$$

so that $D(f)(\alpha) = 0 \cdot g(\alpha) + 0 \cdot D(g)(0) = 0$.

Conversely, assume that $f(\alpha) = D(f)(\alpha) = 0$. We write $f = (X-\alpha)h$ and

$$h = h(\alpha) + (X-\alpha)\ell_h \tag{5}$$

and compute the equality

$$\begin{aligned} D(f) &\overset{\text{(c)}}{=} h + (X-\alpha)D(h) \\ &= h(\alpha) + (X-\alpha)\ell_h + (X-\alpha)D(h) \end{aligned}$$

which evaluated at α gives

$$0 = h(\alpha) + 0 + 0.$$

Then (5) reads $h = (X-\alpha)\ell_h$ and we can conclude that $f = (X-\alpha)h = (X-\alpha)^2\ell_h$, so that α is a multiple root of f.

6. Let R be a domain and $F = \mathrm{Frac}(R)$. Prove that $\mathrm{Frac}(R[X]) \cong F(X)$.

Solution: The canonical inclusion $j : R \longrightarrow F = \mathrm{Frac}(R)$ induces a canonical homomorphism of rings $j' : R[X] \longrightarrow F[X]$. Consider the canonical inclusions $\iota_R : R[X] \longrightarrow \mathrm{Frac}(R[X])$ and $\iota_F : F[X] \longrightarrow \mathrm{Frac}(F[X]) = F(X)$. By Lemma 2 there exists a unique ring homomorphism $\overline{j'} : \mathrm{Frac}(R[X]) \longrightarrow \mathrm{Frac}(F[X]) = F(X)$ such that the following diagram commutes (the maps without label are the usual inclusions of constant polynomials):

$$\begin{tikzcd} R \arrow[r] \arrow[d, "j"'] & R[X] \arrow[r, "\iota_R"] \arrow[d, "j'"'] & \mathrm{Frac}(R[X]) \arrow[d, "\overline{j'}"'] \\ F \arrow[r] & F[X] \arrow[r, "\iota_F"] & \mathrm{Frac}(F[X]) = F(X) \end{tikzcd}$$

The ring homomorphism $\overline{j'}$ is injective by Lemma 1.

Now let $q = f/g \in F(X)$ be a fraction of polynomials $f, g \in F(X)$. Write $f = \sum_{k=0}^{n} \frac{a_k}{b_k} X^k$ for $a_k, b_k \in R$. Then

$$f = \sum_{k=0}^{n} \frac{a_k}{b_k} X^k = \frac{1}{\prod_k b_k} \sum_{k=0}^{n} a'_k X^k$$

for suitable coefficients $a'_k \in R$. Similarly with g. This means that there exist $r, s \in R$ and $f_0, g_0 \in R[X]$ such that

$$f = \frac{1}{r} f_0, \; g = \frac{1}{s} g_0.$$

Then

$$q = \frac{f}{g} = \frac{\frac{1}{r} f_0}{\frac{1}{s} g_0} = \frac{s f_0}{r g_0} = \overline{j'} \left(\frac{s f_0}{r g_0} \right),$$

the last equality holding by Lemma 2—the fraction in the brackets on the right hand side is an element of $\mathrm{Frac}(R[X])$ as $s f_0, r g_0 \in R[X]$.