Name: Tuan Pham
ID: 4652218

Math 8201: General Algebra
Homework #5

50/50
10

(1) Let A be a factorial ring and $a \in A \setminus \{0\}$. We will show that $A[X]/(aX-1)$ is also a factorial ring.

To do so, we'll follow the following main steps.

Step 1: Describe the ideal $(aX-1)A[X]$.

Since A is an integral domain, it can be imbedded into a field, for example the field K of fractions ~~of~~ A. Then each $h(X) \in A[X]$ can be viewed as an element in $K[X]$. We'll show that

$$h\left(\tfrac{1}{a}\right) = 0 \iff \exists\, q(X) \in A[X] : h(X) = (aX-1)\,q(X). \qquad (1)$$

In other words, this property characterizes the ideal generated by $(aX-1)$.

$$(aX-1)A[X] = \left\{ h \in A[X] : h\left(\tfrac{1}{a}\right) = 0 \right\}. \qquad (2)$$

For each $g(X) \in A[X]$, we denote by $[g(X)]$ the equivalence class of $g(X)$ in $A[X]/(aX-1)$. Then we have an immediate consequence of (1) as follow.

"If $f, g \in A[X]$ and $f\left(\tfrac{1}{a}\right) = g\left(\tfrac{1}{a}\right)$ then $[f(X)] = [g(X)]$".

Proof of the consequence. Put $h(X) = f(X) - g(X) \in A[X]$. Then

$h\left(\tfrac{1}{a}\right) = f\left(\tfrac{1}{a}\right) - g\left(\tfrac{1}{a}\right) = 0$. By (2), we get $h(X) \in (aX-1)A[X]$. Therefore,

$$[f(X)] - [g(X)] = [h(X)] = 0.$$

Step 2: Show that $A[X]/(aX-1)$ is an integral domain. The idea is to show that the ideal $(aX-1)A[X]$ given by (2) is a prime ideal.

Step 3: Describe the units of $A[X]/(aX-1)$.

To each $g(X) = a_0 + a_1 X + \cdots + a_n X^n \in A[X]$, we associate $\hat{g}(X) = a_0 X^n + a_1 X^{n-1} + \cdots + a_n$, which is obtained by reversing the order of coefficients of $g(X)$. We see that

$$g\left(\frac{1}{a}\right) = a_0 + \frac{a_1}{a} + \cdots + \frac{a_n}{a^n} = \frac{a_0 a^n + a_1 a^{n-1} + \cdots + a_n}{a^n} = \frac{\hat{g}(a)}{a^n}.$$

We will show that

"$[g(X)]$ is a unit of $A[X]/(aX-1) \iff \hat{g}(a) \mid a^N$ for some $N \in \mathbb{N}$". (3)

Step 4: Develop a decomposition into prime factors.

~~For Each $f(X) \in A[X] \setminus \{0\}$,~~ Each nonzero element $[f(X)] \in A[X]/(aX-1)$ has $\hat{f}(a) = a^n f\left(\frac{1}{a}\right) \neq 0$. Since A is factorial, we can write $\hat{f}(a)$ as a product of a unit and prime elements in A:

$$\hat{f}(a) = u\, p_1 \cdots p_e, \text{ where } u \text{ is a unit, } p_1, \ldots, p_e \text{ are primes in } A.$$

By grouping the prime divisors of a which occur in the above product into α, we get $\hat{f}(a) = \alpha\, q_1 \cdots q_k$, where all prime divisors of α are also divisors of a, and $q_i \nmid a$ for all $i = 1, \ldots, k$. Since all prime divisors of α are also divisors of a, there exists $N \in \mathbb{N}$ such that $\alpha \mid a^N$. Of course, we

can choose a such a number N that $N > n$. ~~Then there exists $\alpha' \in A[\frac{1}{a}]$ such that $\alpha\alpha' = a^N$.~~ We put $g(X) = \alpha^* X^{\deg q_i}$,

$$g_i(X) \equiv q_i \text{ for all } i = 1, \dots, k$$

We will show that

(i) $[g(X)]$ is a unit in $A[X]/(aX-1)$,

(ii) $[g_i(X)]$ is a prime in $A[X]/(aX-1)$,

(iii) $[f(X)] = [g(X)]\,[g_1(X)] \cdots [g_k(X)]$.

Then (iii) says that $[f(X)]$ can be written as a finite product of a unit and prime elements in $A[X]/(aX-1)$, whence the proof completes.

Details of proofs

Proof of (1) We take $h(X) \in A[X]$.

($\Leftarrow$) Suppose that there exists $q(X) \in A[X]$ such that $h(X) = (aX-1)q(X)$.

By considering both sides as polynomials over K, the field of fractions over A, we can evaluate them at $X = \frac{1}{a}$. Then

$$h\left(\frac{1}{a}\right) = \left(a\cdot\frac{1}{a} - 1\right) q\left(\frac{1}{a}\right) = 0.$$

($\Rightarrow$) Suppose that $h\left(\frac{1}{a}\right) = 0$. Then there exists $\tilde{q}(X) \in K[X]$ such that

$$h(X) = \left(X - \frac{1}{a}\right)\tilde{q}(X) \qquad (*)$$

Because $X - \frac{1}{a} = \frac{aX-1}{a}$, the content $\mathrm{cont}\left(X - \frac{1}{a}\right) = \frac{1}{a}$.

4

We write $h(X) = \mathrm{cont}(h)\,\tilde{h}(X)$ and $\tilde{q}(X) = \mathrm{cont}(\tilde{q})\,\tilde{\tilde{q}}(X)$, where $\mathrm{cont}(h) \in A$ and $\mathrm{cont}(\tilde{q}) \in K$ and $\tilde{h}(X) \in A[X]$ and $\tilde{\tilde{q}}(X) \in A[X]$.

By (*) and Gauss's lemma, we get $\mathrm{cont}(h) = \frac{1}{a}\,\mathrm{cont}(\tilde{q})$. Then

$$(*) \Leftrightarrow \mathrm{cont}(h)\,\tilde{h}(X) = \frac{1}{a}\,\mathrm{cont}(\tilde{q})\,(aX-1)\,\tilde{\tilde{q}}(X)$$

$$\Leftrightarrow \tilde{h}(X) = (aX-1)\,\tilde{\tilde{q}}(X)$$

$$\Leftrightarrow h(X) = (aX-1)\,\underbrace{\mathrm{cont}(h)}_{\in A}\,\underbrace{\tilde{\tilde{q}}(X)}_{\in A[X]}$$

Thus, $\mathrm{cont}(h)\,\tilde{\tilde{q}}(X) = q(X) \in A[X]$.

Proof of Step 2

To show that $(aX-1)A[X]$ is ~~an integral domain~~ a prime ideal, we take $f(X), g(X)$ in $A[X]$ and assume that $f(X)\,g(X) \in (aX-1)A[X]$. Then there exists $h_1(X) \in A[X]$ such that $f(X)\,g(X) = (aX-1)\,h_1(X)$. Then $f\left(\frac{1}{a}\right) g\left(\frac{1}{a}\right) = 0$.

~~Using The result (2) for $h(X) = f(X)\,g(X)$~~, Then $f\left(\frac{1}{a}\right) = 0$ or $g\left(\frac{1}{a}\right) = 0$.

Assume without loss of generality, $f\left(\frac{1}{a}\right) = 0$. Using the result (1) with $h = f$, we get $f(X) \in (aX-1)A[X]$.

Proof of (3) Take $g(X) \in A[X]$.

($\Rightarrow$) Suppose that $[g(X)]$ is a unit of $A[X]/(aX-1)$. Then there exists $[h_1(X)]$ such that $[g(X)]\,[h_1(X)] = [1]$. Thus, there exists $h_2(X) \in A[X]$

such that $g(X)h_1(X) = 1 + (aX-1)h_2(X)$. Evaluating both sides at $X = \frac{1}{a}$, we get $g(\frac{1}{a})h_1(\frac{1}{a}) = 1$. Thus, $\frac{\hat{g}(a)}{a^n}\frac{\hat{h}_1(a)}{a^m} = 1$,

where n is the degree of $g(X)$ and m is the degree of $h_1(X)$. Then

$$\hat{g}(a)\hat{h}_1(a) = a^{m+n}.$$

Thus, $\hat{g}(a) \mid a^{m+n}$.

($\Leftarrow$) Suppose that there exists $N \in \mathbb{N}$ such that $\hat{g}(a) \mid a^N$. We can assume $N \geq n$, the degree of $g(X)$. Then there exists $\alpha \in A$ such that $\hat{g}(a)\alpha = a^N$. Put $g_1(X) = \alpha X^{N-n}$. We'll show that $[g_1(X)]$ is the inverse of $[g(X)]$. Put $h(X) = g(X)g_1(X) - 1$. we have

$$h(\tfrac{1}{a}) = g(\tfrac{1}{a})g_1(\tfrac{1}{a}) - 1 = \frac{\hat{g}(a)}{a^n}\hat{g}_1(\tfrac{1}{a}) - 1 = \frac{\hat{g}(a)}{a^n}\frac{\alpha}{a^{N-n}} - 1 = 0.$$

By (2), we get $h(X) \in (aX-1)A[X]$. Thus $[g(X)][g_1(X)] - [1] = [h(X)] = 0$.

Proof of (i) in Step 4

With $g(X) = \alpha^* X^n$ and $\alpha^* \mid a^N$, we'll show that $[g(X)]$ is a unit. we have $\hat{g}(a) = a^n g(\frac{1}{a}) = a^n \frac{\alpha^*}{a^n} = \alpha^*$. Thus $\hat{g}(a) \mid a^N$. By property (3) that we have just proved in Step 2, we conclude that $[g(X)]$ is a unit.

Proof of (ii) in Step 4

What we need to show is as follow: "let β be a prime of A and $\beta \nmid a$. Then $g(X) \equiv \beta$ is a prime of $A[X]/(aX-1)$".

Suppose that $[\beta] = [u(X)][v(X)]$. we'll show that $[u(X)]$ or $[v(X)]$ must be a unit. There exists $w(X) \in A[X]$ such that

$$u(X)v(X) - \beta = (aX-1)w(X).$$

Evaluating both sides at $X = \frac{1}{a}$, we have $u\left(\frac{1}{a}\right)v\left(\frac{1}{a}\right) - \beta = 0$. Thus,

$$\frac{\hat{u}(a)\,\hat{v}(a)}{a^n a^m} - \beta = 0, \text{ where } n \text{ and } m \text{ are degrees of } u(X) \text{ and } v(X).$$

Thus, $\hat{u}(a)\hat{v}(a) = \beta a^{m+n}$. Thus $\beta \mid \hat{u}(a)\hat{v}(a)$. Since β is a prime of A, we have $\beta \mid \hat{u}(a)$ or $\beta \mid \hat{v}(a)$. Without loss of generality, we can assume $\beta \mid \hat{u}(a)$. Then there exists $\beta' \in A$ such that $\beta\beta' = \hat{u}(a)$. Then

$$(\beta\beta')\,\hat{v}(a) = \beta a^{m+n}$$

Thus $\beta' \hat{v}(a) = a^{m+n}$. Thus $\hat{v}(a) \mid a^{m+n}$. By property (8), $[v(X)]$ is a unit.

Proof of (iii) in Step 4

Because $\hat{f}(a) = \alpha q_1 \cdots q_k$ and $\hat{g}(a) = \alpha$, $\hat{g}_i(a) = q_i$, we have $\hat{f}(a) = \hat{g}(a)\hat{g}_1(a) \cdots \hat{g}_k(a)$. Thus $a^n f\left(\frac{1}{a}\right) = a^n g\left(\frac{1}{a}\right) g_1\left(\frac{1}{a}\right) \cdots g_k\left(\frac{1}{a}\right)$. Thus, $f\left(\frac{1}{a}\right) = g\left(\frac{1}{a}\right) g_1\left(\frac{1}{a}\right) \cdots g_k\left(\frac{1}{a}\right)$. Thus $[f(X)] = [g(X)\, g_1(X) \cdots g_k(X)]$

$$= [g(X)]\,[g_1(X)] \cdots [g_k(X)].$$

(2) Let k be a field. The problem has two parts. We'll solve part (b) first because the properties to be proved in (a) and (b) are the same, and Y^2-X^3 looks simpler than $Y^2-X^2-X^3$.

(b) Consider the quotient ring $k[X,Y]/(Y^2-X^3)$. We will

1) show that this ring is an integral domain,

2) show that $k[X,Y]/(Y^2-X^3) \simeq (k[X]\times k[X], +, *)$, where

$$(f_1,f_2)+(g_1,g_2) := (f_1+g_1, f_2+g_2),$$

$$(f_1,f_2)*(g_1,g_2) := (f_1g_1+X^3f_2g_2, f_1g_2+f_2g_1),$$

for all $f_1, f_2, g_1, g_2 \in k[X]$,

3) show that the ring $k[X]\times k[X]$ with the addition and multiplication above is not factorial,

4) show that $K(k[X]\times k[X]) \simeq K(k[X])$, where $K(A)$ denotes the field of fractions of an integral domain A.

Proof of Step 1

To show that the quotient ring $k[X,Y]/(Y^2-X^3)$ is an integral domain, we will show that Y^2-X^3 is a prime element. Since k is a field, it's also a factorial ring. Thus $k[X,Y]$ is factorial. Thus prime elements are the same as irreducible elements. Thus, we need to show that Y^2-X^3 is

irreducible in $k[X,Y]$. Suppose that there are $g, h \in k[X,Y]$ such that

$$Y^2 - X^3 = g(X,Y)\,h(X,Y). \qquad (1)$$

We'll show that either g or h is a unit. That is, to show that $\deg g = 0$ or $\deg h = 0$. Suppose by contradiction that $\deg g, \deg h \geq 1$. Equating the degree of both sides of (1), we get $3 = \deg g + \deg h$. Thus, one degree equals 1 and one degree equals 2. We can assume $\deg g = 1$. There there exist $a, b, c \in k$ with a and b not simultaneously equal to 0, such that $g(X,Y) = aX + bY + c$. Then (1) becomes

$$Y^2 - X^3 = (aX + bY + c)\,h(X,Y). \qquad (2)$$

Evaluating both sides of (2) at $X = 0$, we get $Y^2 = (bY + c)\,h(0,Y)$.

If $b \neq 0$ then we evaluate both sides at $Y = -cb^{-1}$ and get $c^2 b^{-2} = 0$.

Thus $c = 0$. Thus we always have $c = 0$ or $b = 0$.

Similarly, we evaluate both sides of (2) at $Y = 0$ and get $-X^3 = (aX + c)h(X,0)$.

If $a \neq 0$ then we evaluate both sides at $X = -a^{-1}c$ and get $a^{-3}c^3 = 0$.

Thus $c = 0$. Thus we always have $c = 0$ or $a = 0$.

Since a and b cannot be zero at once, c must be zero. Then (2) becomes

$$Y^2 - X^3 = (aX + bY)\,h(X,Y). \qquad (3)$$

If $a \neq 0$, by considering $k[X,Y] = k[Y][X]$, we can evaluate both sides of (3) at $X = -a^{-1}bY$ and get $Y^2 + a^{-3}b^3 Y^3 = 0$. This is a contradiction.

If $b \neq 0$, by considering $k[X,Y] = k[X][Y]$, we can evaluate both sides of (3) at $Y = -b^{-1}aX$ and get $b^{-2}a^2X^2 - X^3 = 0$. This is a contradiction.

Proof of Step 2

For each $f(X,Y) \in k[X,Y]$, we denote $[f(X,Y)]$ by the equivalence class of $f(X,Y)$ in $k[X,Y]/(Y^2-X^3)$. We can write

$$f(X,Y) = \sum_{i=1}^{l} c_i X^{n_i} Y^{m_i}, \text{ where } c_i \in k,\ m_i, n_i \geq 0,\ l \geq 0.$$

For any integer $m \geq 2$, $n \geq 0$, we have $Y^m X^n = (Y^2 - X^3) Y^{m-2} X^n + Y^{m-2} X^{n+3}$.

Thus $[Y^m X^n] = [Y^{m-2} X^{n+3}]$. Thus, if m is even, i.e. $m = 2k$, we have $[Y^{2k}, X^n] = [Y^0 X^{n+3k}] = [X^{n+3k}]$. If m is odd, i.e $m = 2k+1$, we have $[Y^{2k+1} X^n] = [Y X^{n+3k}]$. Thus,

$$[f(X,Y)] = \sum_{i=1}^{l} c_i [X^{n_i} Y^{m_i}] = [f_1(X)] + [f_2(X) Y] = [f_1(X) + f_2(X) Y],$$

where f_1 and f_2 are some polynomials in $k[X]$. We will show that $f_1(X)$ and $f_2(X)$ are uniquely determined by $f(X,Y)$. Suppose that we have

$$[f(X,Y)] = [f_1(X) + f_2(X) Y] = [\tilde{f}_1(X) + \tilde{f}_2(X) Y]$$

Then $f_1(X) - \tilde{f}_1(X) + (f_2(X) - \tilde{f}_2(X)) Y$ is divisible by $(Y^2 - X^3)$. Put $\tilde{\tilde{f}}_1(X) = f_1(X) - \tilde{f}_1(X)$ and $\tilde{\tilde{f}}_2(X) = f_2(X) - \tilde{f}_2(X)$. Then there exists $g(X,Y)$ such that $\tilde{\tilde{f}}_1(X) + \tilde{\tilde{f}}_2(X) Y = (Y^2 - X^3) g(X,Y)$.

Unless both sides are zeros, the degree of Y on the left hand side is at most one, while its degree on the right hand side is at least two, which is impossible. Since $\tilde{f}_1(X) + \tilde{f}_2(X)\,Y = 0$, we get $\tilde{f}_1(X) = \tilde{f}_2(X) = 0$. Thus $f_1(X) = \tilde{f}_1(X)$ and $f_2(X) = \tilde{f}_2(X)$. Therefore, each $f(X,Y) \in k[X,Y]$ will determine uniquely a pair $(f_1(X), f_2(X))$ in $k[X] \times k[X]$ such that $[f(X,Y)] = [f_1(X) + f_2(X)\,Y]$. This property determines a map as follow.

$$k[X,Y] \longrightarrow k[X] \times k[X]$$
$$f(X,Y) \longmapsto (f_1(X), f_2(X)).$$

Moreover, if $[f(X,Y)] = [\tilde{f}(X,Y)]$ then $[f(X,Y) - \tilde{f}(X,Y)] = 0$. Then $[(f_1(X) + f_2(X)\,Y) - (\tilde{f}_1(X) + \tilde{f}_2(X)\,Y)] = 0$. Then $[f_1(X) - \tilde{f}_1(X) + (f_2(X) - \tilde{f}_2(X))\,Y] = 0$.

As shown above, $f_1(X) = \tilde{f}_1(X)$, and $f_2(X) = \tilde{f}_2(X)$. Thus we, in fact, have a map

$$\phi : k[X,Y]/(Y^2 - X^3) \longrightarrow k[X] \times k[X]$$
$$[f(X,Y)] \longmapsto (f_1(X), f_2(X)),$$

such that $[f(X,Y)] = [f_1(X) + f_2(X)\,Y]$. What we have shown results immediately in that ϕ is injective. Moreover, for each pair $(f_1(X), f_2(X))$, we have $\phi([f_1(X) + f_2(X)\,Y]) = (f_1(X), f_2(X))$. Thus ϕ is surjective. Therefore, ϕ is a bijection. We can equip a ring structure on $k[X] \times k[X]$ by the structure on $k[X,Y]/(Y^2 - X^3)$. In particular, if $[g(X,Y)] = [g_1(X) + g_2(X)\,Y]$ then

$$(f_1, f_2) + (g_1, g_2) := \phi([f] + [g]) = \phi([f+g]) = (f_1 + g_1, f_2 + g_2),$$

$$(f_1, f_2) * (g_1, g_2) := \phi([f]) * \phi([g]) := \phi([fg])$$

$$= \phi([(f_1 + f_2 Y)(g_1 + g_2 Y)])$$

$$= \phi([f_1 g_1 + f_2 g_2 Y^2 + (f_1 g_2 + f_2 g_1) Y])$$

$$= \phi([f_1 g_1 + f_2 g_2 X^3 + \underbrace{f_2 g_2 (Y^2 - X^3)}_{=0} + (f_1 g_2 + f_2 g_1) Y])$$

$$= (f_1 g_1 + f_2 g_2 X^3,\ f_1 g_2 + f_2 g_1).$$

With this addition and multiplication, $(k[X] \times k[X], +, *)$ is isomorphic to $k[X,Y]/(Y^2 - X^3)$. Thus, we can work on $k[X] \times k[X]$ instead of $k[X,Y]/(Y^2 - X^3)$ hereafter.

Proof of Step 3

We'll show that $k[X] \times k[X]$ is not factorial. To do so, we'll point out an irreducible element that is not a prime. Such an element is $(X, 0)$. Suppose that $(X, 0) = (f_1, f_2) * (g_1, g_2)$. Then $(X, 0) = (f_1 g_1 + f_2 g_2 X^3,\ f_1 g_2 + f_2 g_1)$. Then

$$\begin{cases} X = f_1 g_1 + f_2 g_2 X^3 & (1) \\ 0 = f_1 g_2 + f_2 g_1 & (2) \end{cases}$$

Since $X \neq f_2 g_2 X^3$, we get $f_1 g_1 \neq 0$. Thus $f_1 \neq 0$ and $g_1 \neq 0$. If $g_2 = 0$ or $f_2 = 0$, (2) implies both of them are zeros. Then (1) gives $X = f_1 g_1$. Thus since X is a prime in $k[X]$, either f_1 or g_1 must be a unit. Thus $(f_1, 0)$ or $(g_1, 0)$

is a unit of $k[X] \times k[X]$. In case $g_2 \neq 0$ and $f_2 \neq 0$, the coefficient of X^3 in the right hand side of (1) must be vanished. Thus $\deg(f_1 f_2) = \deg(f_2 g_2 X^3)$.

Thus $\deg f_1 + \deg g_2 = 3 + \deg f_2 + \deg g_2$. (3)

The ~~coeff~~ leading coefficients of the right hand side of (2) must be vanished.

Thus $\deg(f_1 g_2) = \deg(f_2 g_1)$. Thus

$$\deg f_1 + \deg g_2 = \deg f_2 + \deg g_1. \qquad (4)$$

Summing up (3) and (4) gives us $2\deg f_1 = 3 + 2\deg f_2$. This is a contradiction.

Therefore, $(X, 0)$ is irreducible in $k[X] \times k[X]$. We'll show that it is not a prime.

Indeed, $(X,1)(X,1) = (X^2 + X^3, 2X) = (X,0)(X + X^2, 2)$. If $(X,0)$ divides $(X,1)$ then $(X,1) = (X,0)(f_1, f_2)$; then $1 = X f_1$, which is a contradiction.

Thus, $(X,0)$ is not a prime.

Proof of Step 4

We'll show that $K(k[X] \times k[X]) \simeq K(k[X])$. Consider the natural set-injection $\lambda : R[X] \longrightarrow k[X] \times k[X]$;

$$f \longmapsto (f, 0).$$

We have $\lambda(fg) = (fg, 0) = (f,0) * (g,0) = \lambda(f) * \lambda(g)$ and

$\lambda(f+g) = (f+g, 0) = (f,0) + (g,0)$ and

$\lambda(1) = (1,0)$.

Thus λ is a ring-monomorphism.

We have proved that from the ring's point of view, $k[X]$ is "smaller" than $k[X]\times k[X]$. Thus, $K(k[X])$ is intuitively smaller than $K(k[X]\times k[X])$. To see the converse, we need to make an injection from $k[X]\times k[X]$ to $k[X]$. This is harder but possible. We define the following map

$$\lambda' : k[X]\times k[X] \longrightarrow k[X],$$
$$(f_1(X), f_2(X)) \longmapsto f_1(X^2) + X^3 f_2(X^2).$$

We see that
$$\begin{aligned}\lambda'\big((f_1(X), f_2(X)) + (g_1(X), g_2(X))\big) &= \lambda'\big(f_1(X)+g_1(X), f_2(X)+g_2(X)\big)\\ &= \big(f_1(X^2)+g_1(X^2)\big) + X^3\big(f_2(X^2)+g_2(X^2)\big)\\ &= \big(f_1(X^2)+X^3 f_2(X^2)\big) + \big(g_1(X^2)+X^3 g_2(X^2)\big)\\ &= \lambda'(f_1(X), f_2(X)) + \lambda'(g_1(X), g_2(X)).\end{aligned}$$

$$\begin{aligned}\lambda'\big((f_1, f_2)*(g_1, g_2)\big) &= \lambda'\big(f_1 g_1 + X^3 f_2 g_2,\ f_1 g_2 + f_2 g_1\big)\\ &= \big[f_1(X^2) g_1(X^2) + X^6 f_2(X^2) g_2(X^2)\big] + X^3\big[f_1(X^2) g_2(X^2) + f_2(X^2) g_1(X^2)\big]\\ &= \big(f_1(X^2) + X^3 f_2(X^2)\big)\big(g_1(X^2) + X^3 g_2(X^2)\big)\\ &= \lambda'(f_1, f_2)\,\lambda'(g_1, g_2).\end{aligned}$$

$$\lambda'(1, 0) = 1 + X^3 \cdot 0 = 1.$$

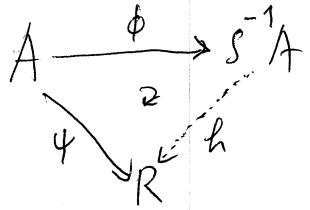
Thus, λ' is a ring-morphism. For $(f_1, f_2) \in \ker \lambda'$, we have

$$f_1(X^2) + X^3 f_2(X^2) = 0 \qquad (1)$$

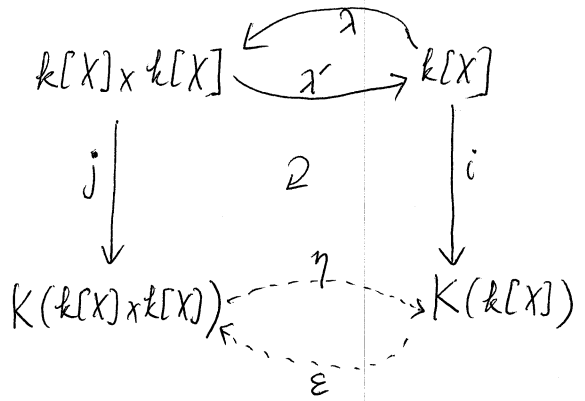
Thus all coefficients of LHS(1) are zeros. Since f_1 contains all coefficients

of even degrees, and f_2 contains all coefficients of odd degrees, we must have $f_1(X) = f_2(X) = 0$. Thus λ' is injective. We have proved that $k[X] \times k[X]$ is intuitively smaller than $k[X]$ from the viewpoint of rings. Let $i: k[X] \longrightarrow K(k[X])$ and $j: k[X] \times k[X] \longrightarrow K(k[X] \times k[X])$ be the canonical inclusions. We'll use the universal property of the rings of fractions to show that $K(k[X]) \simeq K(k[X] \times k[X])$. That universal property is as follow.

Let A be a commutative ring and S be a multiplicative subset. Denote by $\phi: A \longrightarrow S^{-1}A$, $\phi(a) = \frac{a}{1}$. Then for any ring morphism $\psi: A \to R$ such that $\psi(s)$ is invertible in R for all $s \in S$, there exists a unique ring morphism $h: S^{-1}A \to R$ that make the following diagram commute.



Return to the problem. Because $i\lambda'$ maps every nonzero element of $k[X] \times k[X]$ to a nonzero element of $K(k[X])$ (because i and λ' are injective), it maps nonzero elements to invertible elements. Thus, there exists a unique (ring) morphism $\eta: K(k[X] \times k[X]) \longrightarrow K(k[X])$

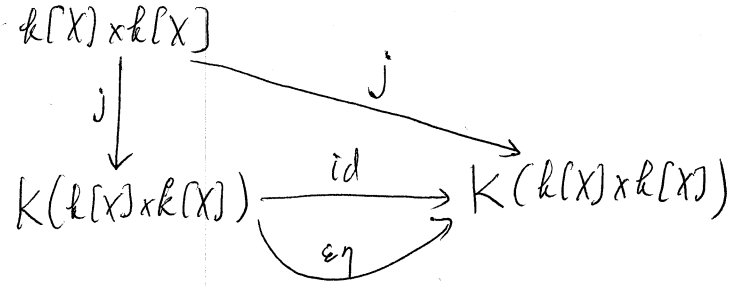


such that the diagram with λ', i, η, j commutes.

Similarly, since λ and j are injective, $j\lambda$ map nonzero elements in $k[X]$ to nonzero (thus invertible) elements of $K(k[X]\times k[X])$. By the universal property, there exists a unique morphism $\varepsilon: K(k[X]) \to K(k[X]\times k[X])$ such that the diagram with $\lambda, j, \varepsilon, i$ commutes. Then we have

$$j = \varepsilon i \lambda' = \varepsilon \eta j$$

Thus there are two morphism from $K(k[X]\times k[X])$ to itself that make the following diagram commute. They are id and $\varepsilon\eta$.



By the universal property, $\varepsilon\eta = id$. Thus ε and η are ring isomorphisms. Therefore, $K(k[X]\times k[X]) \simeq K(k[X])$.

(a) Consider the quotient ring $k[X,Y]/(Y^2 - X^2 - X^3)$.

We'll mimick the approach in part (b). We'll follow the same four steps, with modification in each step if needed.

Step 1 We'll show that $k[X,Y]/(Y^2-X^2-X^3)$ is an integral domain. To do so, we'll show that $Y^2-X^2-X^3$ is irreducible. We see that

16

$$y^2 - x^2 - x^3 = y^2 - x^2(x+1).$$

If we can show that $x+1$ is a prime in $k[x]$ and $(x+1) \nmid x^2$ then we would conclude that $y^2 - x^2(x+1)$ is irreducible in $k[x,y]$ according to Eisenstein's criterion. Since $k[x]$ is factorial, it suffices to show that $x+1$ is irreducible. Any decomposition $x+1 = g(x)h(x)$ will result in that either $\deg g = 0$ or $\deg h = 0$. Thus $g(x)$ or $h(x)$ is invertible. Thus $x+1$ is irreducible. Moreover, $x^2 = (x+1)(x-1)+1$ and $(x+1) \nmid 1$. Then $(x+1) \nmid x^2$.

Step 2 we will try to associate an element $[f(x,y)] \in k[x,y]/(y^2-x^2-x^3)$ with a pair $(f_1(x), f_2(x)) \in k[x] \times k[x]$. We see that

$$y^m x^n = (y^2 - x^2 - x^3) y^{m-2} x^n + y^{m-2}(x^{n+2} + x^{n+3}) \quad \forall m \geq 2, n \geq 0$$

Thus, $[y^m x^n] = [y^{m-2}(x^{n+2} + x^{n+3})]$. By continuing applying this rule, we can lower the exponent of y from m to 0 or 1. Thus each monomial $y^m x^n$ satisfies $[y^m x^n] = [y f(x)]$ or $[y^m x^n] = [f(x)]$. Therefore, each $f(x,y) \in k[x,y]$ associates with a pair $(f_1(x), f_2(x)) \in k[x] \times k[x]$ such that

$$[f(x,y)] = [f_1(x) + f_2(x) y].$$

To show that this association is a map from $k[x,y]$ to $k[x] \times k[x]$, we need to show that if $f_1(x) + f_2(x) y = (y^2 - x^2 - x^3) g(x,y)$ then $f_1(x) = f_2(x) = 0$.

This is true because the highest degree of Y on the left hand side is at most Y, while on the right is at least Y^2, unless $f_1(X) = f_2(X) = 0$.

Because of this property, this map from $k[X,Y]$ to $k[X] \times k[X]$ also factors through a map from $k[X,Y]/(Y^2 - X^2 - X^3)$ to $k[X] \times k[X]$. We still call it ϕ as in part (a).

$$\phi : k[X,Y]/(Y^2 - X^2 - X^3) \longrightarrow k[X] \times k[X],$$

$$[f(X,Y)] \longmapsto (f_1(X), f_2(X)).$$

The argument above also implies that ϕ is injective. Since $\phi([f_1(X) + Y f_2(X)]) = (f_1(X), f_2(X))$, ϕ is surjective. Thus ϕ is a set-theoretic bijection. Then we impose the ring structure on $k[X] \times k[X]$ by the one on $k[X,Y]/(Y^2 - X^2 - X^3)$ to make ϕ an isomorphism. Then

$$(f_1, f_2) + (g_1, g_2) := (f_1 + g_1, f_2 + g_2).$$

$$(f_1, f_2) \cdot (g_1, g_2) := \phi([f(X,Y)\, g(X,Y)]), \text{ where } \phi([f(X,Y)]) = (f_1, f_2), \quad \phi([g(X,Y)]) = (g_1, g_2).$$

$$= \phi([(f_1 + f_2 Y)(g_1 + g_2 Y)])$$

$$= \phi([f_1 f_2 + f_2 g_2 Y^2 + (f_1 g_2 + f_2 g_1) Y])$$

$$= \phi([f_1 f_2 + (X^2 + X^3) f_2 g_2 + \underbrace{(Y^2 - X^2 - X^3) f_2 g_2}_{=0} + (f_1 g_2 + f_2 g_1) Y])$$

$$= \phi\left([f_1g_1 + (X^2+X^3)f_2g_2 + (f_1g_2 + f_2g_1)Y]\right)$$

$$= \left(f_1g_1 + (X^2+X^3)f_2g_2,\ f_1g_2 + f_2g_1\right).$$

In short, the operations on $k[X]\times k[X]$ are

$$(f_1, f_2) + (g_1, g_2) = (f_1+g_1, f_2+g_2),$$

$$(f_1, f_2)\circ(g_1, g_2) = \left(f_1g_1 + (X^2+X^3)f_2g_2,\ f_1g_2 + f_2g_1\right).$$

Thus, we can work on $(k[X]\times k[X], +, \circ)$ instead of $k[X,Y]/(Y^2-X^2-X^3)$.

Step 3

We'll show that $k[X]\times k[X]$ is not factorial. Again, we'll look for an irreducible element which is not prime. We'll show that it is $(X, 0)$.

Suppose that $(X, 0) = (f_1, f_2)\circ(g_1, g_2)$. Then

$$\begin{cases} X = f_1(X)g_1(X) + (X^2+X^3)f_2(X)g_2(X), & (1) \\ 0 = f_1(X)g_2(X) + f_2(X)g_1(X). & (2) \end{cases}$$

We'll treat this exactly the same as in Part (a). If $f_2 = 0$ or $g_2 = 0$, (2) implies both of them are zero. Then (1) implies f_1 or g_2 must be unit because X is a prime in $k[X,Y]$. If $f_2 \neq 0$ and $g_2 \neq 0$ then $f_1 \neq 0$ and $g_1 \neq 0$. Comparing the leading exponents of two sides in (1) and (2), we have

$$\begin{cases} \deg f_1 + \deg g_1 = 3 + \deg f_2 + \deg g_2 \\ \deg f_1 + \deg g_2 = \deg f_2 + \deg g_1 \end{cases}$$

Adding them up, we get $2\cdot\deg f_1 = 3 + 2\cdot\deg f_2$. This is a contradiction.

We have $(X,0)$ is ~~ir~~reducible. We see that

$$(X,1):(X,1) = (X^2+X^2+X^3, 2X) = (X,0)\circ(2X+X^2, 2).$$

If $(X,1)$ is divisible by $(X,0)$ then $(X,1)=(X,0)(f_1,f_2)$. Then $1=Xf_2$. This is a contradiction. Thus, $(X,0)$ is not a prime.

Step 4

We'll show that $K(k[X]\times k[X]) \simeq K(k[X])$. If we can find a monomorphism from $k[X]$ ~~to~~ $k[X]\times k[X]$, and a monomorphism from $k[X]\times k[X]$ to $k[X]$ then we can conclude $K(k[X]\times k[X]) \simeq K(k[X])$ by chasing the diagram as in Part (a).

The inclusion $\lambda : k[X] \longrightarrow k[X]\times k[X]$, satisfies

$$f \longmapsto (f,0)$$

$$\lambda(fg) = (fg,0) = (f,0)\circ(g,0) = \lambda(f)\circ\lambda(g),$$

$$\lambda(f)+\lambda(g) = (f,0)+(g,0) = (f+g,0) = \lambda(f+g),$$

$$\lambda(1) = (1,0).$$

Thus λ is a ring morphism, and hence a monomorphism.

To find a monomorphism from $k[X]\times k[X]$ to $k[X]$, we will start from a rough manipulation

$$(f_1g_1 + (X^2+X^3)f_2g_2,\ f_1g_2+f_2g_1) \Longrightarrow f_1g_1+(X^2+X^3)f_2g_2+\sqrt{X^2+X^3}(f_1g_2+f_2g_1)$$

$$= (f_1+\sqrt{X^2+X^3}f_2)(g_1+\sqrt{X^2+X^3}g_2)$$

This hints us to define $\lambda'(f_1, f_2) = f_1 + \sqrt{X^2+X^3}\, f_2$. But this is nonsense. We should change the variable to eliminate the square root. Since $\sqrt{X^2+X^3}$ "$=$" $X\sqrt{1+X}$, an excellence change of variable is $X \mapsto X^2 - 1$. Therefore, we officially define $\lambda' : k[X] \times k[X] \longrightarrow k[X]$ such that

$$\lambda'(f_1, f_2) = f_1(X^2-1) + X(X^2-1) f_2(X^2-1).$$

We have
$$\begin{aligned}\lambda'(f_1,f_2) + \lambda'(g_1,g_2) &= f_1(X^2-1) + X(X^2-1)f_2(X^2-1) \\ &\quad + g_1(X^2-1) + X(X^2-1)g_2(X^2-1) \\ &= (f_1+g_1)(X^2-1) + X(X^2-1)(f_2+g_2)(X^2-1) \\ &= \lambda'(f_1+g_1, f_2+g_2).\end{aligned}$$

$$\begin{aligned}\lambda'(f_1,f_2)\cdot\lambda'(g_1,g_2) &= \left[f_1(X^2-1) + X(X^2-1)f_2(X^2-1)\right]\left[g_1(X^2-1) + X(X^2-1)g_2(X^2-1)\right] \\ &= f_1(X^2-1)\,g_1(X^2-1) + X^2(X^2-1)^2 f_2(X^2-1)\,g_2(X^2-1) \\ &\quad + X(X^2-1)\left[f_1(X^2-1)\,g_2(X^2-1) + f_2(X^2-1)\,g_1(X^2-1)\right] \\ &= \cancel{f_1 g_1 + X(X^2-1)} \\ &= \left\{f_1(X^2-1)\,g_1(X^2-1) + \left[(X^2-1)^2 + (X^2-1)^3\right] f_2(X^2-1)\,g_2(X^2-1)\right\} \\ &\quad + X(X^2-1)\left[f_1(X^2-1)\,g_2(X^2-1) + f_2(X^2-1)\,g_1(X^2-1)\right] \\ &= \lambda'\left(f_1 g_1 + (X^2+X^3) f_2 g_2,\ f_1 g_2 + f_2 g_1\right) \\ &= \lambda'\left((f_1,f_2)\circ(g_1,g_2)\right).\end{aligned}$$

Moreover, $\lambda'(1,0) = 1$. Thus λ' is a ring morphism.

For each $(f_1, f_2) \in \ker \lambda'$, we have $f_1(X^2-1) + X(X^2-1) f_2(X^2-1) = 0$.

Since f_1 gives rise to monomials of even degrees, and f_2 gives rise to monomials of odd degrees, both of them must be zero. Thus $\ker \lambda' = 0$. Thus λ' is a monomorphism.

(5) Problem 5, Lang, page 213 10

(a) We'll show that the polynomials X^4+1 and X^6+X^3+1 are irreducible over the rational numbers. Consider the following map

$$\phi: \mathbb{Z}[X] \longrightarrow \mathbb{Z}[X],$$
$$f(X) \longmapsto \phi(f)(X) = f(X+1).$$

With this definition, ϕ naturally becomes a ring morphism. Each $g \in \mathbb{Z}[X]$ corresponds uniquely to $f(X) = g(X-1)$ such that $\phi(f) = g$. Thus ϕ is a bijection. Thus ϕ is a ring automorphism. Thus, the irreducibility of $f(X)$ is the same as the irreducibility of $f(X+1)$. We see that

$$(X+1)^4 + 1 = X^4 + 4X^3 + 6X^2 + 4X + 2, \qquad (1)$$

$$(X+1)^6 + (X+1)^3 + 1 = X^6 + 6X^5 + 15X^4 + 21X^3 + 18X^2 + 9X + 3. \qquad (2)$$

Note that 2 and 3 are prime element of $\mathbb{Z}$, which is a factorial ring. Applying the Eisenstein's criterion for $p=2$ in the first case, and $p=3$ in the second case, we conclude that $(X+1)^4+1$ and $(X+1)^6+(X+1)^3+1$ are irreducible over

$\mathbb{Q}[X]$. Therefore X^4+1 and X^6+X^3+1 are irreducible over $\mathbb{Z}[X]$.

(b) Let k be a field and $f \in k[X]$ having degree 3. Suppose that $f(X)$ is reducible. We'll show that $f(X)$ has a root in k.

There exist $g, h \in k[X]$ such that $f(X) = g(X)\,h(X)$ and neither $g(X)$ nor $h(X)$ is a unit. Since k is a field, this happens only if $\deg g, \deg h \geq 1$. We have $\deg g + \deg h = \deg f = 3$. Thus either $\deg g = 1$, $\deg h = 2$ or $\deg g = 2$, $\deg h = 1$. We can assume, by symmetry, that $\deg g = 1$. Then $g(X) = aX + b$ with $a \neq 0$. Then $g(-a^{-1}b) = a(-a^{-1}b) + b = 0$. Thus $f(-a^{-1}b) = 0$. Thus $f(X)$ has a root.

Next, we'll show that the polynomial $f(X) = X^3 - 5X^2 + 1$ is irreducible over the rational numbers. Suppose by contradiction that $f(X)$ is reducible, then $f(X)$ has a root $X = \frac{p}{q}$ with $p, q \in \mathbb{Z}$, $(p,q) = 1$ and $q \neq 0$. Then p divides the constant term and q divides the leading coefficient. Thus $p \mid 1$ and $q \mid 1$. Thus $p, q \in \{-1, 1\}$. Thus $\frac{p}{q} \in \{-1, 1\}$. Since $f(-1) = (-1)^3 - 5(-1)^2 + 1 = -5 \neq 0$ and $f(1) = 1^3 - 5 \cdot 1^2 + 1 = -3 \neq 0$, we get a contradiction.

(c) Put $f(X, Y) = X^2 + Y^2 - 1$. We'll show that f is irreducible over $\mathbb{C}$, and hence irreducible over $\mathbb{Q}$. Suppose by contradiction that f is

reducible. Then there exist $g, h \in \mathbb{C}[X,Y]$ with $\deg g, \deg h \geq 1$ such that $f(X,Y) = g(X,Y)\,h(X,Y)$. Since $\deg g + \deg h = \deg f = 2$, we have $\deg g = \deg h = 1$. Thus g and h are of the forms

$$g(X,Y) = aX + bY + c,$$
$$h(X,Y) = a'X + b'Y + c',$$

where $a, b, c, a', b', c' \in \mathbb{C}$. Thus we have the identity in $\mathbb{C}[X,Y]$:

$$X^2 + Y^2 - 1 = (aX + bY + c)(a'X + b'Y + c') \qquad (1)$$

Equating the constant terms at (1), we get $cc' = -1$.

~~Evaluating both sides at $Y = -1$, we get $X^2 = (aX - b + c)$~~

Equating the coefficients of X^2, we get $aa' = 1$. Thus $a, a' \neq 0$.

Equating the coefficients of Y^2, we get $bb' = 1$. Thus $b, b' \neq 0$.

Evaluating both sides of (1) at $Y = -1$, we get $X^2 = (aX - b + c)(a'X - b' + c')$.

Two roots on the right hand side are $X = a^{-1}(b-c)$ and $X = a'^{-1}(b'-c')$, which are supposed to be zeros. Thus $b = c$, $b' = c'$.

Similarly, evaluating both sides of (1) at $X = -1$, we get $Y^2 = (bY - a + c)(b'Y - a' + c')$. Two roots on the right hand side are $Y = b^{-1}(a-c)$ and $Y = b'^{-1}(a'-c')$, which should be zeros. Thus $a = c$ and $a' = c'$. Thus (1) is now rewritten as

$$X^2 + Y^2 - 1 = (cX + cY + c)(c'X + c'Y + c')$$

which is $X^2+Y^2-1 = cc'(X+Y+1)^2 = -(X+Y+1)^2$

$= -X^2-Y^2-2XY-2X-2Y-1.$

This is a contradiction.

10

④ Let A be a commutative entire ring. Let $a, b \in A$ and assume a is a unit in A. We'll show that the map $X \mapsto aX+b$ extends to a unique automorphism of $A[X]$ inducing an identity on A.

Suppose that $\phi : A[X] \longrightarrow A[X]$ is a ring endomorphism such that $\phi(X) = aX+b$ and $\phi(c) = c$ for all $c \in A$. Then for each $f(X) = a_0 + a_1X + \cdots + a_nX^n$, we have

$$\begin{aligned}\phi(f) &= \phi(a_0 + a_1X + \cdots + a_nX^n) \\ &= \phi(a_0) + \phi(a_1)\phi(X) + \phi(a_2)\phi(X)^2 + \cdots + \phi(a_n)\phi(X)^n \\ &= a_0 + a_1(aX+b) + a_2(aX+b)^2 + \cdots + a_n(aX+b)^n.\end{aligned}$$

Thus such a map ϕ, if exists, is unique and given by the above formula. We'll show that the map $\phi : A[X] \longrightarrow A[X]$

$$\phi\Big(\sum_{k=0}^{n} a_kX^k\Big) = \sum_{k=0}^{n} a_k(aX+b)^k,$$

is indeed a ring morphism. We have $\phi(f) = f(aX+b)$. Thus

$$\phi(f+g)(X) = (f+g)(aX+b) = f(aX+b) + g(aX+b) = \phi(f)(X) + \phi(g)(X),$$

$$\phi(fg)(X) = (fg)(aX+b) = f(aX+b)\,g(aX+b) = \phi(f)(X)\,\phi(g)(X),$$

$$\phi(1) = 1.$$

Thus ϕ is a ring morphism. Moreover, $\phi(c) = c$ for all $c \in A$. We'll

show that ϕ is a ring isomorphism. It suffices to show that ϕ is a set-theoretic bijection. For each $g(X) \in A[X]$, we have

$$\phi(f) = g(X) \iff f(aX+b) = g(X) \qquad (*)$$

Assume that we proved $Y = aX+b$ is a variable over A. Then

$$(*) \iff f(Y) = g(a^{-1}(Y-b)) \qquad (**)$$

Then f exists and unique. Thus ϕ is bijective.

Now we show that Y is a variable over A. Suppose that g is a polynomial over $A[X]$ with $g(Y) = 0$. We'll show that $g = 0$. Suppose by contradiction that $g \neq 0$. Then we can write $g(X) = a_0 + a_1X + \cdots + a_nX^n$ with $a_n \neq 0$. We have $0 = g(aX+b) = a_0 + a_1(aX+b) + \cdots + a_n(aX+b)^n$. Comparing the leading coefficients of both sides, we get $a_n a^n = 0$. Since a is invertible, this implies $a_n = 0$. This is a contradiction.

Therefore, ϕ is an automorphism, and its inverse is given by $(**)$, namely

$$\phi^{-1}(g) = g(a^{-1}(X-b)) \quad \text{for all } g(X) \in A[X].$$

(5) Let $\phi : A[X] \longrightarrow A[X]$ be an automorphism, where A is a commutative ring, such that $\phi(c) = c$ for all $c \in A$. We will show that $\phi(X) = aX+b$ where a is a unit of A. Put $\phi(X) = f(X) \in A[X]$. First we'll show

that $f(X)$ is of degree 1. Since ϕ induced an identity map on A, and $X \notin A$, we have $f(X) \notin A$. Thus $f(X)$ has the degree of at least one. Put $f(X) = a_0 + a_1 X + \cdots + a_n X^n$ with $a_n \neq 0$. ~~Suppose by contradiction that $n \geq 2$.~~ Since ϕ is surjective, there exists $g \in A[X]$ such that $\phi(g) = X$. We write $g(X) = b_0 + b_1 X + \cdots + b_m X^m$, $m \geq 1$. Then

$$\phi(g) = \phi(b_0 + b_1 X + \cdots + b_m X^m) = \phi(b_0) + \phi(b_1)\phi(X) + \cdots + \phi(b_m)\phi(X)^m$$
$$= b_0 + b_1 \phi(X) + \cdots + b_m \phi(X)^m$$

Thus, $X = b_0 + b_1 f(X) + b_2 f(X)^2 + \cdots + b_m f(X)^m$.

The term with highest degree on the right hand side is $b_m a_n^m X^{mn}$. Therefore,

$$X = b_m a_n^m X^{mn}.$$

Thus $b_m a_n^m = 1$ and $mn = 1$. Thus $m = n = 1$ and $b_m a_n = 1$.

Thus $n = 1$ and a_n is invertible. Thus $f(X)$ is of degree 1 and

$$f(X) = aX + b$$

with a invertible.

(6) Let K be a field, and $K(X)$ the quotient field of $K[X]$. Let $\phi : K(X) \to K(X)$ be an automorphism such that $\phi(\alpha) = \alpha$ for all $\alpha \in K$. We will show that $\phi(X) = \dfrac{aX + b}{cX + d}$ for $a, b, c, d \in K$.

Since ϕ is a isomorphism, it maps nonzero elements to nonzero elements. Assume that $u, v \in K[X]$ and $v \neq 0$. Then $u = \frac{u}{v} \cdot v$. Thus $\phi(u) = \phi\left(\frac{u}{v}\right)\phi(v)$. Since $\phi(v) \neq 0$, we have $\phi\left(\frac{u}{v}\right) = \frac{\phi(u)}{\phi(v)}$. This formula appears to be very handy in our manipulation. Put

$$\phi(X) = \frac{f(X)}{g(X)},$$

where $f(X), g(X) \in K[X]$, $g(X) \neq 0$. We can assume that this fraction was in the reduced form, i.e. $f(X)$ and $g(X)$ are relatively prime and $g(X)$ has the leading coefficient 1. Since $X \neq 0$, $\phi(X) \neq 0$ and $f(X) \neq 0$. Thus we can write

$$f(X) = a_0 + a_1 X + \cdots + a_n X^n, \text{ with } a_n \neq 0,\ n \geq 0,$$

$$g(X) = b_0 + b_1 X + \cdots + b_m X^m, \text{ with } b_m = 1,\ m \geq 0.$$

We'll show that $m, n \leq 1$.

Since ϕ is surjective, there exist $p(X), q(X) \in K[X]$, $q(X) \neq 0$ such that

$$X = \phi\left(\frac{p(X)}{q(X)}\right).$$

We can assume that this fraction was in the reduced form, i.e. $p(X)$ and $q(X)$ are relatively prime and $q(X)$ has the leading coefficient 1. Since $X \neq 0$, $\phi^{-1}(X) \neq 0$ and thus $p(X) \neq 0$. We can write

$$p(X) = c_0 + c_1 X + \cdots + c_r X^r, \text{ with } c_r \neq 0,\ r \geq 0,$$

$$q(X) = d_0 + d_1 X + \cdots + d_s X^s, \text{ with } d_s = 1,\ s \geq 0.$$

28

Since ϕ is a ring homomorphism, we have

$$\begin{aligned}\phi(p(X)) &= \phi(c_0 + c_1 X + \cdots + c_r X^r) \\ &= \phi(c_0) + \phi(c_1)\,\phi(X) + \cdots + \phi(c_r)\,\phi(X)^r \\ &= c_0 + c_1 \phi(X) + \cdots + c_r \phi(X)^r \\ &= c_0 + c_1 \frac{f(X)}{g(X)} + \cdots + c_r \frac{f(X)^r}{g(X)^r} \\ &= \frac{c_0 g(X)^r + c_1 g(X)^{r-1} f(X) + \cdots + c_r f(X)^r}{g(X)^r}.\end{aligned}$$

Similarly, $$\phi(q(X)) = \frac{d_0 g(X)^s + d_1 g(X)^{s-1} f(X) + \cdots + d_s f(X)^s}{g(X)^s}$$

Since $X = \phi\left(\frac{p(X)}{q(X)}\right) = \frac{\phi(p(X))}{\phi(q(X))}$, we get

$$X = \frac{c_0 g(X)^r + c_1 g(X)^{r-1} f(X) + \cdots + c_r f(X)^r}{d_0 g(X)^s + d_1 g(X)^{s-1} f(X) + \cdots + d_s f(X)^s} \cdot \frac{g(X)^s}{g(X)^r} \qquad (*)$$

Using (*), we'll show that $m_{in} \leq 1$. By comparing r, s with 0, we have four cases:

Case ① $\underline{r = s = 0}$:

Then $\frac{p(X)}{q(X)} = \frac{c_0}{1} = c_0$. Thus $X = \phi(c_0) = c_0$. This is impossible.

② $\underline{r = 0,\ s \geq 1}$: Then (*) becomes

$$X = \frac{c_0}{d_0 g(X)^s + \cdots + d_{s-1} g(X) f(X)^{s-1} + f(X)^s} g(X)^s \qquad (1)$$

Thus, $X(d_0 g(X)^s + \cdots + d_{s-1} g(X) f(X)^{s-1} + f(X)^s) = c_0 g(X)^s$. Thus the left hand side is divisible by $g(X)$. Thus $g(X) \mid X f(X)^s$. Since $(f(X), g(X)) = 1$, we

[illegible]

If $g(X) = 1$, (1) becomes $X(d_0 + \cdots + d_{s-1} f(X)^{s-1} + f(X)^s) = c_0$. The left hand side is of degree $1 + ns \geq 1$ while the right hand side is of degree zero. This is impossible.

If $g(X) = X$, (1) becomes $X(d_0 X^s + \cdots + d_{s-1} X f(X)^{s-1} + f(X)^s) = c_0 X^s$. (2)

Since $(g(X), f(X)) = 1$, X doesn't divide $f(X)$. Thus X^2 doesn't divide the left hand side. Thus X^2 doesn't divide the right hand side. Thus $s \leq 1$. Since $s \geq 1$, we get $s = 1$. Then (2) becomes $X(d_0 X + f(X)) = c_0 X$. Thus $d_0 X + f(X) = c_0$. Thus $f(X) = -d_0 X + c_0$, which is of degree ≤ 1.

* $r \geq 1$, $s = 0$

Then $q(X) = 1$. Now (*) becomes $X = \dfrac{c_0 g(X)^r + c_1 g(X)^{r-1} f(X) + \cdots + c_r f(X)^r}{g(X)^r}$

Thus $X g(X)^r = c_0 g(X)^r + \cdots + c_{r-1} g(X) f(X)^{r-1} + c_r f(X)^r$. (3)

Since the left hand side ~~divides~~ is divisible by $g(X)$, so is the right hand side.

Then $g(X) \mid c_r f(X)^r$. Since $(f(X), g(X)) = 1$, that implies $g(X) \mid f(X)$, and thus $g(X) = 1$. Then (3) becomes $X = c_0 + c_1 f(X) + \cdots + c_r f(X)^r$.

Comparing the degree on both sides gives us $1 = nr$. Thus $n = r = 1$.

- $r \geq 1, s \geq 1$

By comparing r and s, we have three subcases

\ $s = r$: Then (*) becomes $X = \dfrac{c_0 g(X)^r + c_1 g(X)^{r-1} f(X) + \cdots + c_r f(X)^r}{d_0 g(X)^r + d_1 g(X)^{r-1} f(X) + \cdots + d_r f(X)^r}$

Thus $\underbrace{X(d_0 g(X)^r + \cdots + d_r f(X)^r)}_{\equiv d_r X f(X)^r \bmod g(X)} = \underbrace{c_0 g(X)^r + \cdots + c_r f(X)^r}_{\equiv c_r f(X)^r \bmod g(X)}$. (4)

Thus $g(X) \mid (d_r X f(X)^r - c_r f(X)^r)$. Thus $g(X) \mid (d_r X - c_r) f(X)^r$. Since $(g(X), f(X)) = 1$, we get $g(X) \mid (d_r X - c_r)$. Thus $\deg g = m \leq 1$.

Using the same treatment for $f(X)$ at (4), we also get $\deg f = n \leq 1$.

\ $s < r$: Then (*) becomes $X = \dfrac{c_0 g(X)^r + \cdots + c_{r-1} g(X) f(X)^{r-1} + c_r f(X)^r}{d_0 g(X)^s + \cdots + d_{s-1} g(X) f(X)^{s-1} + d_s f(X)^s} \cdot \dfrac{1}{g(X)^{r-s}}$

Thus, $\underbrace{X(d_0 g(X)^s + \cdots + d_s f(X)^s) g(X)^{r-s}}_{\equiv 0 \bmod g(X)} = \underbrace{c_0 g(X)^r + \cdots + c_{r-1} g(X) f(X)^{r-1} + c_r f(X)^r}_{\equiv c_r f(X)^r \bmod g(X)}$

Thus, $g(X) \mid c_r f(X)^r$. Thus $g(X) \mid f(X)^r$ and hence $g(X) = 1$. Then the above identity becomes $X(d_0 + d_1 f(X) + \cdots + d_s f(X)^s) = c_0 + c_1 f(X) + \cdots + c_r f(X)^r$. Thus $f(X) \mid (d_0 X - c_0)$. Thus $\deg f \leq 1$ unless $c_0 = d_0 = 0$. This case couldn't

happen because if so, $X \mid p(X)$ and $X \mid q(X)$, which contradicts our ~~choice~~ assumption that $p(X)$ and $q(X)$ are relatively prime.

\ $r<s$: Then (*) becomes $$X = \frac{c_0 g(X)^r + \cdots + c_r f(X)^r}{d_0 g(X)^s + \cdots + d_s f(X)^s} g(X)^{s-r}$$

Thus $X(d_0 g(X)^s + \cdots + d_{s-1} g(X) f(X)^{s-1} + f(X)^s) = (c_0 g(X)^r + \cdots + c_r f(X)^r) g(X)^{s-r}$. (5)

Thus the left hand side should be divisible by $g(X)$. Thus $g(X) \mid (X f(X)^s)$.

Since $(f(X), g(X)) = 1$, $g(X) \nmid X$. Thus $g(X) = 1$ or $g(X) = X$.

If $g(X) = 1$, then (5) becomes $X(d_0 + d_1 f(X) + \cdots + d_{s-1} f(X)^{s-1} + f(X)^s)$

$$= c_0 + c_1 f(X) + \cdots + c_r f(X)^r.$$

The left hand side has degree $1+ns$, and the right hand side has degree nr. This case couldn't happen because $1+ns > nr$.

If $g(X) = X$, then (5) becomes $X(d_0 X^s + \cdots + d_{s-1} X f(X)^{s-1} + f(X)^s)$

$$= (c_0 X^r + \cdots + c_r f(X)^r) X^{s-r}.$$

The left hand side has degree $1+ns$, while the right-hand side has degree $nr+(s-r)$. This case couldn't happen ~~either~~ when $n>0$ because

$$1+ns \geq 1+(n-1)r+s = nr+s-r.$$

Thus $n = 0$.

Now we have shown that $f(X)$ and $g(X)$ are of degree at most 1. We can write $f(X) = aX+b$, $g(X) = cX+d$. Then

$$\phi(X) = \frac{aX+b}{cX+d}.$$

Since ϕ induces the identity map on K and ϕ is injective, $\phi(X) \notin K$.

The condition for $\phi(X) \in K$ is that $\exists x \in K$ such that $\frac{aX+b}{cX+d} = x$, which is equivalent to say the vectors (a,b) and (c,d) are parallel. This is equivalent to $ad - bc = 0$. Thus,

$$\phi(X) \notin K \iff ad - bc \neq 0.$$

We will show that this property characterizes any automorphism on $K(X)$, which is identity on K.

Let $\phi(X) = \frac{aX+b}{cX+d}$ with $a,b,c,d \in K$ and $ad-bc \neq 0$,

we'll show that ϕ extends to a unique automorphism of $K(X)$ inducing identity on K. By these hypotheses, there is only one way to extend ϕ in such a manner, namely

$$\phi\left(\frac{a_0 + a_1 X + \cdots + a_n X^n}{b_0 + b_1 X + \cdots + b_m X^m}\right) := \frac{a_0 + a_1 \phi(X) + \cdots + a_n \phi(X)^n}{b_0 + b_1 \phi(X) + \cdots + b_m \phi(X)^m}$$

In other words, if $f, g \in K[X]$ and $g \neq 0$, we have to define

$$\phi\left(\frac{f(X)}{g(X)}\right) := \frac{f(\phi(X))}{g(\phi(X))}.$$

Assume that $Y = \phi(X)$ is a variable over K. Then

$$\phi\left(\frac{f(X)}{g(X)}\right) = \frac{f(Y)}{g(Y)} \qquad (**)$$

this means ϕ is just a change of variable, in the fashion of linear fraction.

With the definition (**), it is not hard to show that ϕ is an automorphism.

Indeed,

- ϕ is well-defined since we can ~~choose~~ replace X by any variable we like.

- $$\phi\left(\frac{f_1(X)}{g_1(X)}+\frac{f_2(X)}{g_2(X)}\right)=\phi\left(\frac{f_1(X)g_2(X)+f_2(X)g_1(X)}{g_1(X)g_2(X)}\right)=\frac{f_1(Y)g_2(Y)+f_2(Y)g_1(Y)}{g_1(Y)g_2(Y)}$$
$$=\frac{f_1(Y)}{g_1(Y)}+\frac{f_2(Y)}{g_2(Y)}$$
$$=\phi\left(\frac{f_1(X)}{g_1(X)}\right)+\phi\left(\frac{f_2(X)}{g_2(X)}\right).$$

- $$\phi\left(\frac{f_1(X)}{g_1(X)}\cdot\frac{f_2(X)}{g_2(X)}\right)=\phi\left(\frac{f_1(X)f_2(X)}{g_1(X)g_2(X)}\right)=\frac{f_1(Y)f_2(Y)}{g_1(Y)g_2(Y)}=\frac{f_1(Y)}{g_1(Y)}\cdot\frac{f_2(Y)}{g_2(Y)}$$
$$=\phi\left(\frac{f_1(X)}{g_1(X)}\right)\cdot\phi\left(\frac{f_2(X)}{g_2(X)}\right)$$

- $\phi(1)=1$

- $\phi\left(\frac{f(X)}{g(X)}\right)=0 \Rightarrow \frac{f(Y)}{g(X)}=0 \Rightarrow f(Y)=0 \Rightarrow f(X)=0 \Rightarrow \frac{f(X)}{g(X)}=0.$

- ϕ is ~~obviously surjective~~. For each $\frac{u(X)}{v(X)}\in K(X)$, we ~~define~~ put the fraction
$$\frac{f(X)}{g(X)}=\frac{u\left(\frac{-dX+b}{cX-a}\right)}{v\left(\frac{-dX+b}{cX-a}\right)}$$
for some $f(X), g(X)\in K[X]$, $g(X)\neq 0$.

Then $$\phi\left(\frac{f(X)}{g(X)}\right)=\frac{f(Y)}{g(Y)}=\frac{f(\phi(X))}{g(\phi(X))}=\frac{u\left(\frac{-d\phi(X)+b}{c\phi(X)-a}\right)}{v\left(\frac{-d\phi(X)+b}{c\phi(X)-a}\right)}=\frac{u(X)}{v(X)}$$

Therefore ϕ is an isomorphism.

Thus, all what we need to show is that $Y = \phi(X) = \frac{aX+b}{cX+d}$ is a variable over K. Suppose that there exists $f \in K[T] \setminus \{0\}$ such that $f(Y) = 0$. We write $f(T) = a_0 + a_1 T + \cdots + a_n T^n$ with $a_n \neq 0$. Since $f(Y) = 0$ and $f \neq 0$, $n \geq 1$. We have

$$0 = f(Y) = f(\phi(X)) = a_0 + a_1 \phi(X) + \cdots + a_n \phi(X)^n$$

$$= a_0 + a_1 \frac{aX+b}{cX+d} + \cdots + a_n \frac{(aX+b)^n}{(cX+d)^n} \qquad (***)$$

$$= \frac{a_0 (cX+d)^n + a_1 (aX+b)(cX+d)^{n-1} + \cdots + a_n (aX+b)^n}{(cX+d)^n}.$$

Thus $a_0 (cX+d)^n + a_1 (aX+b)(cX+d)^{n-1} + \cdots + a_n (aX+b)^n = 0$. Thus, $(cX+d) \mid [a_n (aX+b)^n]$. Since $a_n \in K \setminus \{0\}$, it is just a unit in $K[X]$. Thus, $(cX+d) \mid (aX+b)^n$ in $K[X]$. Since ~~$K[X]$~~ Thus there exists $g(X) \in K[X]$ such that $(aX+b)^n = (cX+d)\, g(X)$. If $c \neq 0$ then we can ~~evaluate~~ evaluate both sides at $X = -c^{-1}d$ to get $(-ac^{-1}d + b)^n = 0$. Thus $ad = bc$, which is a contradiction. Therefore $c = 0$. Then $(***)$ becomes

$$0 = a_0 + \frac{a_1}{d}(aX+b) + \cdots + \frac{a_n}{d^n}(aX+b)^n$$

If $a \neq 0$ then by problem ③ above, $aX+b$ is avariable over K. Then

$a_0 = \frac{a_1}{d} = \frac{a_2}{d^2} = \cdots = \frac{a_n}{d^n} = 0$. Then $a_i = 0$ for all i. Thus $f(T) = 0$.

If $a = 0$, then $ad - bc = 0 \cdot d - b \cdot 0 = 0$. This is impossible.

(7) A polynomial $P(X) \in \mathbb{Q}[X]$ may satisfy $P(n) \in \mathbb{Z}$ for all sufficiently large $n \in \mathbb{Z}$ without necessarily P having integer coefficients. 10

(a) An example of such a polynomial is $P(X) = \frac{1}{2}X^2 + \frac{1}{2}X$.

For each $n \in \mathbb{Z}$, $P(n) = \frac{1}{2}n^2 + \frac{1}{2}n = \frac{n(n+1)}{2}$.

Since the numerator is always even, the fraction is actually an integer.

Thus $P(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$.

(b) A polynomial $P(X)$ satisfying the property above is called integral valued.

We'll show that $P(X)$ is of the form

$$P(X) = c_0\binom{X}{r} + c_1\binom{X}{r-1} + \cdots + c_r$$

for some $c_0, \ldots, c_r \in \mathbb{Z}$. Before showing that, we'll prove the following lemma.

Lemma Let $P(X) \in \mathbb{Q}[X]$ and $P(X) = a_m X^m + \cdots + a_1 X + a_0$ with $a_m \neq 0$. If $P(X)$ is integral valued then $m! a_m \in \mathbb{Z}$.

Proof For $m = 0$, $P(X) \equiv a_0$. $P(X)$ is integral valued if and only if $a_0 \in \mathbb{Z}$.

For $m = 1$, $P(X) = a_1 X + a_0$. For all $n > N$, where N is some positive integer, we have $P(n) \in \mathbb{Z}$. Thus $P(n+1) - P(n) \in \mathbb{Z}$. Thus

$$\underbrace{\left(a_1(n+1)+a_0\right)-\left(a_1 n+a_0\right)}_{a_1} \in \mathbb{Z}$$

Thus $a_1 \in \mathbb{Z}$. Then $a_0 = P(n) - a_1 n \in \mathbb{Z}$.

Now assume that the lemma is true for m. We'll show that it is true for $m+1$. Let $Q(X) = b_{m+1}X^{m+1} + \cdots + b_1 X + b_0$ be an integral valued polynomial of degree $m+1$. Then $P(X) = Q(X+1) - Q(X)$ is also integral valued. We have

$$P(X) = b_{m+1}\left((X+1)^{m+1} - X^{m+1}\right) + b_m\left((X+1)^m - X^m\right) + \cdots + b_1\left((X+1) - X\right)$$

$$= b_{m+1}(m+1)X^m + \text{terms of lower degree}.$$

Thus $P(X)$ is of degree m. By the induction hypothesis, $m!\,(b_{m+1}(m+1)) \in \mathbb{Z}$.

Thus $b_{m+1}(m+1)! \in \mathbb{Z}$. ∎

Return to the problem. We will prove the following claim:

[Let $P(X) \in \mathbb{Q}[X]$ and $P(X) = a_m X^m + \cdots + a_1 X + a_0$ with $a_m \neq 0$. ~~Then that~~ If $P(X)$ is integral valued then there exist $c_0, c_1, \ldots, c_m \in \mathbb{Z}$ such that

$$P(X) = c_0\binom{X}{m} + c_1\binom{X}{m-1} + \cdots + c_{m-1}\binom{X}{1} + c_m. \ ]$$

For $m=0$ or $m=1$, we have shown in the proof of the above lemma that all coefficients of $P(X)$ are integers. Thus the claim holds for $m=0, m=1$.

Now assume that the claim holds ~~for~~ up to m. We'll show that it's also

true for $m+1$. Let $Q(X)$ be an integral valued polynomial of degree $m+1$.

$$Q(X) = b_{m+1}X^{m+1} + \cdots + b_1 X + b_0 .$$

By the lemma, $(m+1)!\, b_{m+1} \in \mathbb{Z}$. Granted for a moment that $\binom{X}{r}$ is integral valued, we have $\phi(X) = \binom{X}{m+1}$ is integral valued. The leading coefficient of $\phi(X)$ is $\frac{1}{(m+1)!}$. Put

$$P(X) = Q(X) - b_{m+1}(m+1)!\,\phi(X).$$

Then $P(X)$ is integral valued having degree of at most m. By the induction hypothesis, there exist $c_0', c_1', \ldots, c_r' \in \mathbb{Z}$ with $r \le m$ such that

$$P(X) = c_0'\binom{X}{r} + c_1'\binom{X}{r-1} + \cdots + c_{r-1}'\binom{X}{1} + c_r'.$$

Thus,

$$\begin{aligned} Q(X) &= b_{m+1}(m+1)!\,\phi(X) + P(X) \\ &= b_{m+1}(m+1)!\binom{X}{m+1} + c_0'\binom{X}{r} + \cdots + c_{r-1}'\binom{X}{1} + c_r'. \end{aligned}$$

Thus the claim holds for $m+1$.

The proof would finish if we could show that $\binom{X}{r}$ is integral valued for all $r \ge 1$. That is to show that $\binom{n}{r} \in \mathbb{Z}$ for all $r \ge 1$ and n sufficiently large. We see that $\binom{n}{1} = n \in \mathbb{Z}$. For $r \ge 2$, we have

$$\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}.$$

Thus if $\binom{n-1}{r} \in \mathbb{Z}$ for all $r \geq 1$ then $\binom{n}{r} \in \mathbb{Z}$ for all $r \geq 1$.

Thus, it suffices to show that $\binom{0}{r} \in \mathbb{Z}$ for all $r \geq 1$. But this is trivial because $\binom{0}{r} = \frac{0(0-1)\cdots(0-r+1)}{r!} = 0$ for all $r \geq 1$.

Therefore $\binom{n}{r} \in \mathbb{Z}$ for all $n \geq 0$ and $r \geq 1$. We see that $\binom{-n}{r} = (-1)^r \binom{n+r-1}{r}$. Thus $\binom{-n}{r} \in \mathbb{Z}$ for all $n \geq 0$. Thus $\binom{n}{r} \in \mathbb{Z}$ for all $n \in \mathbb{Z}$, $r \geq 1$. Consequently, any integral valued polynomial

$$P(X) = c_0 \binom{X}{m} + c_1 \binom{X}{m-1} + \cdots + c_{m-1} \binom{X}{1} + c_m$$

has $P(n) = c_0 \binom{n}{m} + c_1 \binom{n}{m-1} + \cdots + c_{m-1} \binom{n}{1} + c_m \in \mathbb{Z}$ for all $n \in \mathbb{Z}$.

(c) Let $f : \mathbb{Z} \to \mathbb{Z}$. ~~We define~~ Assume that there exists an integral valued polynomial $Q(X)$ and $N \in \mathbb{N}$ such that $f(n) - f(n-1) = Q(n)$ for all $n > N$. We will find an integral valued polynomial $P(X)$ such that $f(n) = P(n)$ for all $n > N$.

For $n > N$, we have $f(n) - f(N) = \sum_{k=N+1}^{n} \big(f(k) - f(k-1)\big) = \sum_{k=N+1}^{n} Q(k)$. (*)

Since Q is an integral valued polynomial, there exist $c_0, c_1, \ldots, c_r \in \mathbb{Z}$ such that

$$Q(X) = c_0 \binom{X}{r} + c_1 \binom{X}{r-1} + \cdots + c_{r-1} \binom{X}{1} + c_r.$$

By the identity $\binom{X}{s} = \binom{X+1}{s+1} - \binom{X}{s+1}$, we have

$$Q(X) = c_0\left(\binom{X+1}{r+1} - \binom{X}{r+1}\right) + c_1\left(\binom{X+1}{r} - \binom{X}{r}\right) + \cdots + c_{r-1}\left(\binom{X+1}{2} - \binom{X}{2}\right)$$

$$+ c_r\left(\binom{X+1}{1} - \binom{X}{1}\right)$$

$$= \tilde{Q}(X+1) - \tilde{Q}(X), \text{ where } \tilde{Q}(X) = c_0\binom{X}{r+1} + c_1\binom{X}{r} + \cdots + c_r\binom{X}{1}.$$

Then $\tilde{Q}$ is also an integral valued polynomial. From (*), we have

$$f(n) - f(N) = \sum_{k=N+1}^{n} Q(k) = \sum_{k=N+1}^{n} \left(\tilde{Q}(k+1) - \tilde{Q}(k)\right) = \tilde{Q}(n+1) - \tilde{Q}(N+1).$$

Thus, $f(n) = \tilde{Q}(n+1) + f(N) - \tilde{Q}(N+1)$ for all $n > N$.

Put $P(X) = \tilde{Q}(X+1) + f(N) - \tilde{Q}(N+1)$. Then $P(X)$ is integral valued and $f(n) = P(n)$ for all $n > N$.