# Regular elements of a ring, monic polynomials and "lcm-coprimality"

Darij Grinberg

August 5, 2019

## Contents

# 1. The statements

## 1.1. The main theorems

**Convention 1.1.** In this paper, the word "ring" will always mean "ring with unity".

Furthermore, the letter $\mathbb{N}$ shall always mean the set $\{0, 1, 2, \ldots\}$.

Consider the following fact:

**Theorem 1.2.** Let $A$ be a commutative ring. Let $n \in \mathbb{N}$. Let $f \in A\left[X_1, X_2, \ldots, X_n\right]$ be a polynomial in the $n$ indeterminates $X_1, X_2, \ldots, X_n$ over $A$. Assume that $f$ is divisible by $X_i - X_j$ for every $(i, j) \in \{1, 2, \ldots, n\}^2$ satisfying $i < j$. Then, $f$ is divisible by $\prod_{1 \leq i < j \leq n} \left(X_i - X_j\right)$.

(Here, the symbol "$\prod_{1 \leq i < j \leq n}$" is an abbreviation for "$\prod_{\substack{(i,j) \in \{1,2,\ldots,n\}^2; \\ i<j}}$". Thus, when $n = 0$ or $n = 1$, the product $\prod_{1 \leq i < j \leq n} \left(X_i - X_j\right)$ is an empty product and therefore

equals 1.)

Theorem 1.2 is rather obvious in the case when $A$ is a unique factorization domain (because then, $A[X_1, X_2, \ldots, X_n]$ is also a unique factorization domain[1]). However, I would not call Theorem 1.2 obvious in the general case. One of the goals of this note is to prove Theorem 1.2 in full generality.

Actually, I shall prove the following more general fact:

**Theorem 1.3.** Let $A$ be a commutative ring with unity. Let $n \in \mathbb{N}$. Let $G$ be a subset of the set $\left\{(i,j) \in \{1,2,\ldots,n\}^2 \mid i < j\right\}$.

Let $f \in A[X_1, X_2, \ldots, X_n]$ be a polynomial in the $n$ indeterminates $X_1, X_2, \ldots, X_n$ over $A$. Assume that $f$ is divisible by $X_i - X_j$ for every $(i,j) \in G$. Then, $f$ is divisible by $\prod_{(i,j)\in G} \left(X_i - X_j\right)$.

Clearly, Theorem 1.2 is the particular case of Theorem 1.3 obtained when $G = \left\{(i,j) \in \{1,2,\ldots,n\}^2 \mid i < j\right\}$. Theorem 1.3 is also evident when $A$ is a unique factorization domain, but not in the general case.

## 1.2. Applications

First of all, why is Theorem 1.2 (and thus, by extension, Theorem 1.3) useful? Here are four applications:

- The *Vandermonde determinant formula* (in one of its many forms) is the statement that if $n \in \mathbb{N}$, and if $x_1, x_2, \ldots, x_n$ are $n$ elements of a commutative ring $A$, then

$$\det \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ x_1 & x_2 & x_3 & \cdots & x_n \\ x_1^2 & x_2^2 & x_3^2 & \cdots & x_n^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_1^{n-1} & x_2^{n-1} & x_3^{n-1} & \cdots & x_n^{n-1} \end{pmatrix} = \prod_{1 \le i < j \le n} \left(x_j - x_i\right). \tag{1}$$

  One of the shortest proofs of this fact (given, e.g., in [Garrett09, §17.1]) proceeds by observing that both the left hand side and the right hand side of (1) are polynomials in the variables $x_1, x_2, \ldots, x_n$, whence we can replace the elements $x_1, x_2, \ldots, x_n$ by the indeterminates $X_1, X_2, \ldots, X_n$ in the polynomial ring $\mathbb{Z}[X_1, X_2, \ldots, X_n]$; but once this has been done, we can observe that the left hand side of (1) is divisible by $X_i - X_j$ for every $(i,j) \in \{1,2,\ldots,n\}^2$ satisfying $i < j$, and therefore (by Theorem 1.2) is also divisible by $\prod_{1 \le i < j \le n} \left(X_i - X_j\right)$.

[1] This follows from one of the many results known as "Gauss's theorem" (e.g., [Knapp2016, Corollary 8.21], applied $n$ times).

This is not the whole proof, but the rest of the proof (degree considerations as well as a comparison of a single coefficient) is not difficult (see [Garrett09, §17.1] for details). What matters for us is that this argument uses Theorem 1.2 (although only in the case when $A = \mathbb{Z}$; as we have said, this is an easy case, since $\mathbb{Z}$ is a unique factorization domain).

- A similar proof that uses Theorem 1.3 (although, again, only in a simple case in which $A$ is a unique factorization domain) is [EGHLSVY11, proof of Lemma 5.15.3][2].

- Theorem 1.2 is used in [LLPT95, proof of Lemma (6.1)][3]. In fact, [LLPT95, proof of Lemma (6.1)] involves an argument saying that "Clearly, $f$ is divisible by all differences $a_q - a_p$ for $p < q$ if and only if $f$ is divisible by the product of all the differences". I believe the word "Clearly" is inappropriate in this argument, and should be replaced by an application of Theorem 1.2.

- Theorem 1.2 is used in [GriRei18, proof of Proposition 2.6.4]. Indeed, [GriRei18, proof of Proposition 2.6.4] involves an argument saying that the polynomial $f(\mathbf{x})$ must "be divisible by $x_i - x_j$, so divisible by the entire product $\prod_{1 \leq i < j \leq n} (x_i - x_j) = a_\rho$". Again, this argument only uses Theorem 1.2 in the particular case when $A$ is a unique factorization domain (because [GriRei18, Proposition 2.6.4] is only stated for $\mathbf{k}$ being $\mathbb{Z}$ or a field of characteristic $\neq 2$; but all such $\mathbf{k}$ are unique factorization domains). However, knowing that Theorem 1.2 holds for arbitrary $A$, we can extend [GriRei18, Proposition 2.6.4] to the case of $\mathbf{k}$ being an arbitrary commutative ring (as long as $\Lambda^{\mathrm{sgn}}$ is defined appropriately).

On our way to the proofs of Theorem 1.2 and Theorem 1.3, we shall develop some basics of commutative algebra from scratch: most importantly, division with remainder by a monic polynomial, and the fact that monic polynomials are non-zero-divisors (or, as we call them, regular elements). This is, of course, perfectly well-known in the case of univariate polynomials over a field; but in the general case, it is rarely discussed in detail in the literature.

We shall then explore the surroundings of these results: alternative proofs, analogues for formal power series, applications to other symmetric polynomials.

## 1.3. Plan of this paper

In Section 2, we shall define the notion of "regular elements" (also known as non-zero-divisors) and show some very basic properties (such as the fact that a product of regular elements is again regular).

[2] This is the proof of Lemma 4.48 in the arXiv draft of [EGHLSVY11].

[3] Notice that the $a_p$ in [LLPT95] are the $X_p$ in Theorem 1.2.

In Section 3, we shall review (with proofs) the basic theory of monic polynomials over a commutative ring, including the fact that division with remainder always works when we are dividing by a monic polynomial (even if the base ring is not a field). We will show that monic polynomials are regular, and prove a first step (Corollary 3.21) towards Theorem 1.3.

In Section 4, we will start studying polynomial rings $A[X_1, X_2, \ldots, X_n]$ in multiple indeterminates, and we will prove some basic properties of the polynomials $X_i$ and $X_i - X_j$ (with $i \neq j$) in these rings. In particular, we will show that these polynomials are regular, and have a "coprimality" property (the particular case of Theorem 1.3 for $|G| = 2$).

In Section 5, we shall prove the crucial Proposition 5.1 about when an intersection of principal ideals of a commutative ring equals the product of these ideals. This will let us derive the full Theorem 1.3 (and thus Theorem 1.2) from this "coprimality" property.

In Section 6, we will start extending our results about polynomials to formal power series. Some things will extend easily, but many will change, either requiring new proofs or ceasing to be valid in the new setting. We will show that analogues of Theorem 1.3 and Theorem 1.2 for power series still hold, but our proofs no longer apply to this case.

In Section 7, we will give a second proof of Proposition 5.1, this time using quotient rings.

In Section 8, we shall rewrite Theorem 1.2 in terms of substitutions of variables.

In Section 9, we shall apply Theorem 1.2 to the construction of symmetric polynomials.

In Section 10 (work in progress), we shall continue our study of univariate power series started in Section 6.

### 1.4. Prerequisites

I have written this paper with the express purpose of being as accessible as it possibly can; only basic notions and facts of abstract algebra (rings, polynomials, formal power series, nilpotence) are assumed. Even the use of quotient rings has been kept to a minimum. The occasional counterexample uses more advanced notions, but counterexamples can be skipped without loss.

## 2. Regular elements (a.k.a. non-zero-divisors)

### 2.1. Definition

We begin with a basic notation:

**Definition 2.1.** Let $A$ be a commutative ring. Let $a \in A$. The element $a$ of $A$ is said to be *regular* if and only if every $x \in A$ satisfying $ax = 0$ satisfies $x = 0$.

Instead of saying that $a$ is regular, one can also say that "$a$ is *cancellable*", or that "$a$ is a *non-zero-divisor*".

This notion of "regular" elements has nothing to do with various other notions of "regularity" in commutative algebra (for example, it is completely unrelated to the notion of a "von Neumann regular element" of a ring). It might sound like a bad idea to employ a word like "regular" that has already seen so much different uses; however, we are not really adding a new conflicting meaning for this word, because the word is already being used in this meaning by various authors (among them, the authors of [LLPT95]), and because our use of "regular" is closely related to the standard notion of a "regular sequence" in a commutative ring[4].

Many authors (for example, Knapp in [Knapp2016]) define a *zero divisor* in a commutative ring $A$ to be a nonzero element of $A$ that is not regular.[5] Thus, at least in classical logic, regular elements are the same as elements that are not zero divisors (with the possible exception of 0). I find the notion of a "zero divisor" less natural than that of a regular element (it is the regular elements, not the zero divisors, that usually exhibit the nicer behavior), and it is much less suitable for constructive logic (as it muddies the waters with an unnecessary negation), but it appears to be more popular for traditional reasons.

## 2.2. Properties of regular elements

Let me state some basic properties of regular elements:

**Proposition 2.2.** Let $A$ be a commutative ring. Let $a \in A$ and $b \in A$ be two regular elements of $A$. Then, the element $ab$ of $A$ is regular.

*Proof of Proposition 2.2.* Every $x \in A$ satisfying $(ab)\,x = 0$ satisfies $a\,(bx) = (ab)\,x = 0$, thus $bx = 0$ (since $a$ is regular), and therefore $x = 0$ (since $b$ is regular). In other words, $ab$ is regular. This proves Proposition 2.2. □

**Proposition 2.3.** Let $A$ be a commutative ring. Let $G$ be a finite set. For every $g \in G$, let $a_g$ be a regular element of $A$. Then, the element $\prod\limits_{g \in G} a_g$ of $A$ is regular.

*Proof of Proposition 2.3.* This follows by induction on $|G|$, using Proposition 2.2 in the induction step[6]. □

The following trivial proposition just says that the regularity of an element is unchanged under ring isomorphisms:

[4]Namely: An element $a$ of a commutative ring $A$ is regular if and only if the one-element sequence $(a)$ is regular.

[5]Some authors drop the "nonzero" requirement in this definition; so they count 0 as a zero divisor, provided $A$ is not a trivial ring.

[6]The induction base involves showing that the element 1 of $A$ is regular; but this is obvious.

**Proposition 2.4.** Let $A$ and $B$ be two commutative rings. Let $f : A \to B$ be a ring isomorphism. Let $a$ be a regular element of $A$. Then, $f(a)$ is a regular element of $B$.

The next proposition is also fairly trivial:

**Proposition 2.5.** Let $B$ be a commutative ring. Let $A$ be a subring of $B$. Let $a$ be an element of $A$ such that $a$ is a regular element of $B$. Then, $a$ is a regular element of $A$.

# 3. Monic polynomials and division with remainder

## 3.1. Monic polynomials, $[X^n]\,p$ and $A[X]_{\leq n}$

Now, let me discuss monic polynomials over a commutative ring $A$. This is not an introduction into the notion of polynomials; we will just introduce the nonstandard notations that we will need, and prove a few basic facts.

**Definition 3.1.** Let $A$ be a commutative ring.

**(a)** If $p \in A[X]$ is a polynomial in some indeterminate $X$ over $A$, and if $n \in \mathbb{N}$, then $[X^n]\,p$ will denote the coefficient of $X^n$ in $p$. For example,

$$\left[X^3\right]\left(2X^4+5X^3+7X+2\right) = 5;$$
$$\left[X^4\right]\left(X^2+1\right) = 0;$$
$$\left[X^0\right](3X+7) = 7.$$

Clearly, every polynomial $p \in A[X]$ satisfies $p = \sum\limits_{n\in\mathbb{N}} ([X^n]\,p)\,X^n$. (The sum $\sum\limits_{n\in\mathbb{N}} ([X^n]\,p)\,X^n$ is well-defined, because all but finitely many among its addends are 0.)

**(b)** If $n \in \mathbb{Z}$, then we define an $A$-submodule $A[X]_{\leq n}$ of $A[X]$ as follows:

$$A[X]_{\leq n} = \{p \in A[X] \mid [X^m]\,p = 0 \text{ for every } m \in \mathbb{N} \text{ satisfying } m > n\}.$$

(In other words, $A[X]_{\leq n}$ is the set of all polynomials $p \in A[X]$ having degree $\leq n$, provided that we understand the degree of the zero polynomial to be a symbol $-\infty$ that is smaller than any integer. However, we want to avoid using the concept of "degree", so we are using the above definition of $A[X]_{\leq n}$ instead.)

**(c)** Let $n \in \mathbb{N}$. A polynomial $p \in A[X]$ is said to be *monic of degree $n$* if and only if it satisfies $[X^n]\,p = 1$ and

$$([X^m]\,p = 0 \text{ for every } m \in \mathbb{N} \text{ satisfying } m > n).$$

Instead of saying that $p$ "is monic of degree $n$", we can also say that $p$ "is a monic polynomial of degree $n$".

**Remark 3.2.** I am going to avoid the notion of the "degree" of a polynomial, since it is (in my opinion) inferior to working with $A[X]_{\leq n}$ (for various reasons: it is not defined when $A$ the trivial ring; it is not preserved by ring homomorphisms; it depends on the vanishing of some coefficients and is therefore not generally meaningful in constructive mathematics; it requires some care in handling deg 0). Nevertheless, I will use the terminology "monic of degree $n$" introduced in Definition 3.1; the way I have defined it above, it is independent of the notion of degree. Please be aware of the following quirk of this terminology: If $A$ is the trivial ring, then there exists only one polynomial $p \in A[X]$, and this polynomial is monic of degree $n$ for every $n \in \mathbb{N}$. Thus, a polynomial $p$ can be monic of degree $n$ for many different $n$. (But this only happens when $A$ is trivial.)

## 3.2. Basic rules for polynomials

Recall how polynomials are added, scaled and multiplied:

**Proposition 3.3.** Let $A$ be a commutative ring. Let $n \in \mathbb{N}$.
**(a)** Every $p \in A[X]$ and $q \in A[X]$ satisfy $[X^n](p+q) = [X^n]p + [X^n]q$.
**(b)** Every $\lambda \in A$ and $p \in A[X]$ satisfy $[X^n](\lambda p) = \lambda [X^n]p$.
**(c)** Every $p \in A[X]$ and $q \in A[X]$ satisfy $[X^n](pq) = \sum_{k=0}^{n} \left([X^k]p\right) \cdot \left([X^{n-k}]q\right)$.

Let us next state a few trivial facts:

**Lemma 3.4.** Let $A$ be a commutative ring. Let $n \in \mathbb{N}$.
**(a)** We have $[X^n](X^n) = 1$.
**(b)** For every $k \in \mathbb{N}$ satisfying $k \neq n$, we have $\left[X^k\right](X^n) = 0$.

**Lemma 3.5.** Let $A$ be a commutative ring. Let $n \in \mathbb{Z}$.
**(a)** For every $q \in A[X]_{\leq n}$ and every $m \in \mathbb{N}$ satisfying $m > n$, we have $[X^m]q = 0$.
**(b)** Let $q \in A[X]$. Assume that $[X^m]q = 0$ for every $m \in \mathbb{N}$ satisfying $m > n$. Then, $q \in A[X]_{\leq n}$.

**Proposition 3.6.** Let $A$ be a commutative ring. Then, $A[X] = \bigcup_{n \in \mathbb{N}} A[X]_{\leq n}$.

**Lemma 3.7.** Let $A$ be a commutative ring. Let $n \in \mathbb{N}$. Let $p \in A[X]$ be a monic polynomial of degree $n$. Then:
**(a)** We have $[X^n]p = 1$.
**(b)** We have $[X^m]p = 0$ for every $m \in \mathbb{N}$ satisfying $m > n$.
**(c)** We have $p \in A[X]_{\leq n}$.

**Lemma 3.8.** Let $A$ be a commutative ring. Let $n \in \mathbb{N}$. Let $p \in A[X]_{\leq n}$ be such that $[X^n]\, p = 1$. Then, $p$ is a monic polynomial of degree $n$.

**Lemma 3.9.** Let $A$ be a commutative ring. Let $n \in \mathbb{N}$. Let $q \in A[X]_{\leq n}$. Assume that $[X^n]\, q = 0$. Then, $q \in A[X]_{\leq n-1}$.

**Lemma 3.10.** Let $A$ be a commutative ring. Then, $A[X]_{\leq -1} = \{0\}$.

**Lemma 3.11.** Let $A$ be a commutative ring. Let $g$ and $h$ be two elements of $\mathbb{Z}$ such that $g \leq h$. Then, $A[X]_{\leq g} \subseteq A[X]_{\leq h}$.

Next, we show an easy fact about the product of a polynomial with a monic polynomial:

**Lemma 3.12.** Let $A$ be a commutative ring. Let $n \in \mathbb{N}$. Let $p \in A[X]$ be a monic polynomial of degree $n$. Let $g \in \mathbb{N}$. Let $q \in A[X]_{\leq g}$. Then:
**(a)** We have $pq \in A[X]_{\leq g+n}$.
**(b)** We have $[X^{g+n}]\,(pq) = [X^g]\, q$.

*Proof of Lemma 3.12.* Let $m \in \mathbb{N}$ be such that $m \geq g+n$. For every $k \in \{0, 1, \ldots, n-1\}$, we have

$$\left[X^{m-k}\right] q = 0 \tag{2}$$

[7]. For every $k \in \{n+1, n+2, \ldots, m\}$, we have

$$\left[X^k\right] p = 0 \tag{3}$$

[8]. Now, $0 \leq n$ (since $n \in \mathbb{N}$); also, from $g \in \mathbb{N}$, we obtain $n \leq g+n \leq m$.

[7] *Proof of (2):* Let $k \in \{0, 1, \ldots, n-1\}$. Then, $\underbrace{m}_{\geq g+n} - \underbrace{k}_{\leq n-1<n} > (g+n) - n = g \geq 0$, so that $m-k \in \mathbb{N}$. Also, $m-k > g$; hence, Lemma 3.5 **(a)** (applied to $g$ and $m-k$ instead of $n$ and $m$) yields $\left[X^{m-k}\right] q = 0$. This proves (2).

[8] *Proof of (2):* Let $k \in \{n+1, n+2, \ldots, m\}$. Thus, $k > n$. Also, $k \in \mathbb{N}$. Hence, Lemma 3.7 **(b)** (applied to $k$ instead of $m$) shows that $\left[X^k\right] p = 0$. This proves (3).

Proposition 3.3 **(c)** (applied to $m$ instead of $n$) yields

$$\begin{aligned}
\left[X^m\right](pq) &= \sum_{k=0}^{m} \left(\left[X^k\right] p\right) \cdot \left(\left[X^{m-k}\right] q\right) \\
&= \sum_{k=0}^{n-1} \left(\left[X^k\right] p\right) \cdot \underbrace{\left(\left[X^{m-k}\right] q\right)}_{\substack{=0 \\ \text{(by (2))}}} + \sum_{k=n}^{m} \left(\left[X^k\right] p\right) \cdot \left(\left[X^{m-k}\right] q\right) \\
&\qquad \left(\text{since } 0 \leq n \leq m\right) \\
&= \underbrace{\sum_{k=0}^{n-1} \left(\left[X^k\right] p\right) \cdot 0}_{=0} + \sum_{k=n}^{m} \left(\left[X^k\right] p\right) \cdot \left(\left[X^{m-k}\right] q\right) \\
&= \sum_{k=n}^{m} \left(\left[X^k\right] p\right) \cdot \left(\left[X^{m-k}\right] q\right) \\
&= \underbrace{\left(\left[X^n\right] p\right)}_{\substack{=1 \\ \text{(by Lemma 3.7 \textbf{(a)})}}} \cdot \left(\left[X^{m-n}\right] q\right) + \sum_{k=n+1}^{m} \underbrace{\left(\left[X^k\right] p\right)}_{\substack{=0 \\ \text{(by (3))}}} \cdot \left(\left[X^{m-k}\right] q\right) \\
&\qquad \left(\text{since } n \leq m\right) \\
&= \left[X^{m-n}\right] q + \underbrace{\sum_{k=n+1}^{m} 0 \cdot \left(\left[X^{m-k}\right] q\right)}_{=0} = \left[X^{m-n}\right] q. \qquad (4)
\end{aligned}$$

Now, forget that we fixed $m$. We thus have proven (4) for every $m \in \mathbb{N}$ satisfying $m \geq g + n$.

**(a)** For every $m \in \mathbb{N}$ satisfying $m > g + n$, we have

$$\begin{aligned}
\left[X^m\right](pq) &= \left[X^{m-n}\right] q \qquad \text{(by (4))} \\
&= 0 \qquad \left(\begin{array}{c} \text{by Lemma 3.5 \textbf{(a)}, applied to } m-n \text{ and } g \\ \text{instead of } m \text{ and } n \\ \left(\text{since } q \in A\left[X\right]_{\leq g} \text{ and } m - n > g \text{ (since } m > g + n\right)\right)\end{array}\right).
\end{aligned}$$

Hence, Lemma 3.5 **(b)** (applied to $g + n$ and $pq$ instead of $n$ and $q$) shows that $pq \in A\left[X\right]_{\leq g+n}$. This proves Lemma 3.12 **(a)**.

**(b)** Applying (4) to $m = g + n$, we find $\left[X^{g+n}\right](pq) = \left[X^{g+n-n}\right] q = \left[X^g\right] q$. This proves Lemma 3.12 **(b)**. □

## 3.3. Monic polynomials are regular

The next proposition says that if we multiply a monic polynomial $p$ of some degree $n$ with a polynomial $q$ and the result turns out to have degree $< n$ (that is, formally

speaking: $pq \in A[X]_{\leq n-1}$), then $q$ must have been 0 to begin with. This will help us prove that monic polynomials are regular.

**Proposition 3.13.** Let $A$ be a commutative ring. Let $n \in \mathbb{N}$. Let $p \in A[X]$ be a monic polynomial of degree $n$. Let $q \in A[X]$ be such that $pq \in A[X]_{\leq n-1}$. Then, $q = 0$.

*Proof of Proposition 3.13.* Renaming the index $n$ as $d$ in Proposition 3.6, we obtain $A[X] = \bigcup_{d \in \mathbb{N}} A[X]_{\leq d}$.

Now, $q \in A[X] = \bigcup_{d \in \mathbb{N}} A[X]_{\leq d}$. Hence, there exists some $d \in \mathbb{N}$ such that $q \in A[X]_{\leq d}$. Consider this $d$.

We shall now show that

$$q \in A[X]_{\leq d-i} \qquad \text{for every } i \in \{0, 1, \ldots, d+1\}. \tag{5}$$

*Proof of (5):* We shall prove (5) by induction over $i$:

*Induction base:* We have $q \in A[X]_{\leq d}$. In other words, (5) holds for $i = 0$.

*Induction step:* Let $j \in \{0, 1, \ldots, d+1\}$ be positive. Assume that (5) holds for $i = j-1$. We now must prove that (5) holds for $i = j$.

We have assumed that (5) holds for $i = j-1$. In other words, we have $q \in A[X]_{\leq d-(j-1)}$.

Set $g = d-(j-1)$. Then, $g = d-(j-1) = (d+1)-j \geq 0$ (since $j \leq d+1$), so that $g \in \mathbb{N}$.

Lemma 3.12 **(b)** yields $[X^{g+n}](pq) = [X^g]\, q$. But $\underbrace{g}_{\geq 0} + n \geq n > n-1$. Hence, Lemma 3.5 **(a)** (applied to $pq$, $n-1$ and $g+n$ instead of $q$, $n$ and $m$) yields $[X^{g+n}](pq) = 0$ (since $pq \in A[X]_{\leq n-1}$). Comparing this with $[X^{g+n}](pq) = [X^g]\, q$, we obtain $[X^g]\, q = 0$.

But $q \in A[X]_{\leq d-(j-1)} = A[X]_{\leq g}$ (since $d-(j-1) = g$). Lemma 3.9 (applied to $g$ instead of $n$) thus shows that $q \in A[X]_{\leq g-1}$ (since $[X^g]\, q = 0$). Since $\underbrace{g}_{=d-(j-1)} - 1 = d-(j-1)-1 = d-j$, this rewrites as $q \in A[X]_{\leq d-j}$. In other words, (5) holds for $i = j$. This completes the induction step. Thus, the induction proof of (5) is complete.

Now, applying (5) to $i = d+1$, we obtain $q \in A[X]_{\leq d-(d+1)} = A[X]_{\leq -1} = \{0\}$ (by Lemma 3.10). In other words, $q = 0$. This proves Proposition 3.13. □

**Corollary 3.14.** Let $A$ be a commutative ring. Let $n \in \mathbb{N}$. Let $p \in A[X]$ be a monic polynomial of degree $n$. Let $u \in A[X]_{\leq n-1}$ be such that $p \mid u$ (in the ring $A[X]$). Then, $u = 0$.

*Proof of Corollary 3.14.* We have $p \mid u$. In other words, there exists some $q \in A[X]$ such that $u = pq$. Consider this $q$. We have $pq = u \in A[X]_{\leq n-1}$. Thus, Proposition 3.13 shows that $q = 0$. Hence, $u = p\underbrace{q}_{=0} = 0$. This proves Corollary 3.14. □

**Corollary 3.15.** Let $A$ be a commutative ring. Let $n \in \mathbb{N}$. Let $p \in A[X]$ be a monic polynomial of degree $n$. Then, the element $p$ of $A[X]$ is regular.

*Proof of Corollary 3.15.* We must prove that $p$ is regular. In other words, we must prove that every $x \in A[X]$ satisfying $px = 0$ satisfies $x = 0$ (because this is what it means for $p$ to be regular).

So let $x \in A[X]$ satisfy $px = 0$. Then, $px = 0 \in A[X]_{\leq n-1}$. Hence, Proposition 3.13 (applied to $q = x$) yields $x = 0$. This completes our proof of Corollary 3.15. □

## 3.4. Division with remainder

Now, we shall state the most important result in this section: division with remainder by a monic polynomial:

**Theorem 3.16.** Let $A$ be a commutative ring. Let $n \in \mathbb{N}$. Let $p \in A[X]$ be a monic polynomial of degree $n$. Let $f \in A[X]$. Then, there exists a unique pair $(q, r) \in A[X] \times A[X]_{\leq n-1}$ such that $f = qp + r$.

**Remark 3.17.** Let $A$, $n$, $p$ and $f$ be as in Theorem 3.16. Theorem 3.16 claims that there exists a unique pair $(q, r) \in A[X] \times A[X]_{\leq n-1}$ such that $f = qp + r$. The two entries $q$ and $r$ of this pair $(q, r)$ are called the *quotient* and the *remainder* (respectively) *obtained when dividing $f$ by $p$*. Note that the remainder $r$ belongs to $A[X]_{\leq n-1}$ (since $(q, r) \in A[X] \times A[X]_{\leq n-1}$).

We shall prove the existence and the uniqueness parts of Theorem 3.16 separately, beginning with the uniqueness part:

**Lemma 3.18.** Let $A$ be a commutative ring. Let $n \in \mathbb{N}$. Let $p \in A[X]$ be a monic polynomial of degree $n$. Let $f \in A[X]$. Then, there exists **at most one** pair $(q, r) \in A[X] \times A[X]_{\leq n-1}$ such that $f = qp + r$.

*Proof of Lemma 3.18.* Let $(q_1, r_1)$ and $(q_2, r_2)$ be two pairs $(q, r) \in A[X] \times A[X]_{\leq n-1}$ such that $f = qp + r$. We shall prove that $(q_1, r_1) = (q_2, r_2)$.

We know that $(q_1, r_1)$ is a pair $(q, r) \in A[X] \times A[X]_{\leq n-1}$ such that $f = qp + r$. In other words, $(q_1, r_1)$ is a pair in $A[X] \times A[X]_{\leq n-1}$ such that $f = q_1 p + r_1$. Similarly, $(q_2, r_2)$ is a pair in $A[X] \times A[X]_{\leq n-1}$ such that $f = q_2 p + r_2$.

We have $r_1 \in A[X]_{\leq n-1}$ (since $(q_1, r_1) \in A[X] \times A[X]_{\leq n-1}$) and $r_2 \in A[X]_{\leq n-1}$ (similarly). Thus, $r_2 - r_1 \in A[X]_{\leq n-1}$. Now, $q_1 p + r_1 = f = q_2 p + r_2$. Hence, $q_1 p - q_2 p = r_2 - r_1 \in A[X]_{\leq n-1}$. Thus, $p(q_1 - q_2) = (q_1 - q_2) p = q_1 p - q_2 p \in A[X]_{\leq n-1}$. Proposition 3.13 (applied to $q = q_1 - q_2$) thus shows that $q_1 - q_2 = 0$. In other words, $q_1 = q_2$. Hence, $r_2 - r_1 = \underbrace{q_1}_{=q_2} p - q_2 p = q_2 p - q_2 p = 0$, so that $r_1 = r_2$. Now, $\left( \underbrace{q_1}_{=q_2}, \underbrace{r_1}_{=r_2} \right) = (q_2, r_2)$.

We thus have shown that if $(q_1, r_1)$ and $(q_2, r_2)$ are two pairs $(q, r) \in A[X] \times A[X]_{\leq n-1}$ such that $f = qp + r$, then $(q_1, r_1) = (q_2, r_2)$. In other words, there exists **at most one** pair $(q, r) \in A[X] \times A[X]_{\leq n-1}$ such that $f = qp + r$. This proves Lemma 3.18. □

Now, let us state the existence part of Theorem 3.16; actually, let us make a slightly stronger claim:

**Lemma 3.19.** Let $A$ be a commutative ring. Let $n \in \mathbb{N}$. Let $p \in A[X]$ be a monic polynomial of degree $n$. Let $d \in \{-1, 0, 1, \ldots\}$. Let $f \in A[X]_{\leq d}$. Then, there exists **at least one** pair $(q, r) \in A[X]_{\leq d-n} \times A[X]_{\leq n-1}$ such that $f = qp + r$.

*Proof of Lemma 3.19.* We shall prove Lemma 3.19 by induction on $d$:

*Induction base:* Lemma 3.19 holds in the case when $d = -1$ (because in this case, we have $f \in A[X]_{\leq d} = A[X]_{\leq -1} = \{0\}$ and therefore $f = 0$, so that we can take $(q, r) = (0, 0)$).

*Induction step:* Let $D \in \mathbb{N}$. Assume that Lemma 3.19 holds in the case when $d = D - 1$. We must prove that Lemma 3.19 holds in the case when $d = D$.

Let $A$, $n$ and $p$ be as in Lemma 3.19. Let $f \in A[X]_{\leq D}$. We are going to show the following claim:

> *Claim 1:* There exists **at least one** pair $(q, r) \in A[X]_{\leq D-n} \times A[X]_{\leq n-1}$ such that $f = qp + r$.

*Proof of Claim 1:* If $D \leq n - 1$, then $A[X]_{\leq D} \subseteq A[X]_{\leq n-1}$ (by Lemma 3.11). Hence, if $D \leq n - 1$, then Claim 1 holds (because we can just set $(q, r) = (0, f)$, using the fact that $f \in A[X]_{\leq D} \subseteq A[X]_{\leq n-1}$). Hence, we WLOG assume that we don't have $D \leq n - 1$. Thus, $D \geq n$ (since $D$ and $n$ are integers), so that $D - n \in \mathbb{N}$.

Define an element $\alpha \in A$ by $\alpha = \left[X^D\right] f$. Then, the polynomial $\alpha X^{D-n} \in A[X]$ is well-defined (since $D - n \in \mathbb{N}$) and belongs to $A[X]_{\leq D-n}$. Hence, Lemma 3.12 **(a)** (applied to $D - n$ and $\alpha X^{D-n}$ instead of $g$ and $q$) yields $p\alpha X^{D-n} \in A[X]_{\leq (D-n)+n} = A[X]_{\leq D}$. Moreover, Lemma 3.12 **(b)** (applied to $D - n$ and $\alpha X^{D-n}$ instead of $g$ and $q$) yields

$$\left[X^{(D-n)+n}\right]\left(p\alpha X^{D-n}\right) = \left[X^{D-n}\right]\left(\alpha X^{D-n}\right) = \alpha.$$

Since $(D - n) + n = D$, this rewrites as $\left[X^D\right]\left(p\alpha X^{D-n}\right) = \alpha$.

Both $f$ and $p\alpha X^{D-n}$ belong to $A[X]_{\leq D}$. Hence, the difference $f - p\alpha X^{D-n}$ also belongs to $A[X]_{\leq D}$ (since $A[X]_{\leq D}$ is an $A$-submodule of $A[X]$). In other words, $f - p\alpha X^{D-n} \in A[X]_{\leq D}$. Furthermore,

$$\left[X^D\right]\left(f - p\alpha X^{D-n}\right) = \underbrace{\left[X^D\right] f}_{=\alpha} - \underbrace{\left[X^D\right]\left(p\alpha X^{D-n}\right)}_{=\alpha} = \alpha - \alpha = 0.$$

Hence, Lemma 3.9 (applied to $D$ and $f - p\alpha X^{D-n}$ instead of $n$ and $q$) shows that $f - p\alpha X^{D-n} \in A[X]_{\leq D-1}$. Therefore, we can apply Lemma 3.19 to $D - 1$ and

$f - p\alpha X^{D-n}$ instead of $d$ and $f$ (since we have assumed that Lemma 3.19 holds in the case when $d = D-1$). We thus obtain that there exists **at least one** pair $(q,r) \in A[X]_{\leq (D-1)-n} \times A[X]_{\leq n-1}$ such that $f - p\alpha X^{D-n} = qp + r$. Denote this pair $(q,r)$ by $(\widetilde{q},\widetilde{r})$. Thus, $(\widetilde{q},\widetilde{r})$ is a pair in $A[X]_{\leq (D-1)-n} \times A[X]_{\leq n-1}$ satisfying $f - p\alpha X^{D-n} = \widetilde{q}p + \widetilde{r}$.

We have $(\widetilde{q},\widetilde{r}) \in A[X]_{\leq (D-1)-n} \times A[X]_{\leq n-1}$; in other words, $\widetilde{q} \in A[X]_{\leq (D-1)-n}$ and $\widetilde{r} \in A[X]_{\leq n-1}$. Now, $\widetilde{q} \in A[X]_{\leq (D-1)-n} \subseteq A[X]_{\leq D-n}$ (since $(D-1)-n \leq D-n$). Hence, both $\widetilde{q}$ and $\alpha X^{D-n}$ belong to $A[X]_{\leq D-n}$ (since we know that $\alpha X^{D-n} \in A[X]_{\leq D-n}$). Thus, the sum $\widetilde{q} + \alpha X^{D-n}$ also belongs to $A[X]_{\leq D-n}$ (since $A[X]_{\leq D-n}$ is an $A$-submodule of $A[X]$). In other words, $\widetilde{q} + \alpha X^{D-n} \in A[X]_{\leq D-n}$. Combining this with $\widetilde{r} \in A[X]_{\leq n-1}$, we obtain $\left(\widetilde{q} + \alpha X^{D-n}, \widetilde{r}\right) \in A[X]_{\leq D-n} \times A[X]_{\leq n-1}$. Furthermore, from $f - p\alpha X^{D-n} = \widetilde{q}p + \widetilde{r}$, we obtain

$$f = \underbrace{p\alpha X^{D-n} + \widetilde{q}p}_{=(\widetilde{q}+\alpha X^{D-n})p} + \widetilde{r} = \left(\widetilde{q} + \alpha X^{D-n}\right) p + \widetilde{r}.$$

Thus, there exists **at least one** pair $(q,r) \in A[X]_{\leq D-n} \times A[X]_{\leq n-1}$ such that $f = qp + r$ (namely, $(q,r) = \left(\widetilde{q} + \alpha X^{D-n}, \widetilde{r}\right)$). This proves Claim 1.

Now, forget that we have fixed $A$, $n$, $p$ and $f$. We thus have shown that if $A$, $n$ and $p$ are as in Lemma 3.19, and if $f \in A[X]_{\leq D}$, then Claim 1 holds. In other words, Lemma 3.19 holds in the case when $d = D$. This completes the induction step. The induction proof of Lemma 3.19 is thus complete. □

Finally, we can prove Theorem 3.16:

*Proof of Theorem 3.16.* The existence of the pair $(q,r)$ follows from Lemma 3.19[9]; its uniqueness from Lemma 3.18. □

## 3.5. $aR \cap pR = apR$ for monic $p$ and arbitrary $a$

**Convention 3.20.** Here and in the following, we shall observe the following convention: Multiplication (of elements of a ring, or of ideals of a ring, or of an element of a ring with an ideal of a ring) precedes set-theoretical operations such as $\cap$ and $\cup$. Thus, if $A$ is a ring, if $S$ and $T$ are two ideals of $A$, and if $a$ is an element of $A$, then the expression "$aS \cap T$" means "$(aS) \cap T$" (and not "$a(S \cap T)$"). Similarly, if $U$, $V$ and $W$ are three ideals of a ring, then the expression "$U \cap VW$" means "$U \cap (VW)$" (and not "$(U \cap V) W$").

Now, let us prove a consequence of Theorem 3.16 that will reveal its use later:

[9] Here we are using the fact that there exists some $d \in \mathbb{N}$ such that $f \in A[X]_{\leq d}$. (But this follows immediately from Proposition 3.6.)

**Corollary 3.21.** Let $A$ be a commutative ring. Let $n \in \mathbb{N}$. Let $p \in A[X]$ be a monic polynomial of degree $n$. Let $a \in A$. Set $R = A[X]$. Then, $aR \cap pR = apR$.

*Proof of Corollary 3.21.* Combining $a \underbrace{pR}_{\subseteq R} \subseteq aR$ with $\underbrace{ap}_{=pa} R = p \underbrace{aR}_{\subseteq R} \subseteq pR$, we obtain $apR \subseteq aR \cap pR$.

Now, let $u \in aR \cap pR$. Thus, $u \in aR \cap pR \subseteq aR$. In other words, there exists some $f \in R$ such that $u = af$. Consider this $f$.

We have $f \in R = A[X]$. Hence, Theorem 3.16 shows that there exists a unique pair $(q, r) \in A[X] \times A[X]_{\leq n-1}$ such that $f = qp + r$. Consider this $(q, r)$.

We have $(q, r) \in A[X] \times A[X]_{\leq n-1}$; in other words, $q \in A[X]$ and $r \in A[X]_{\leq n-1}$. Now, $u = a \underbrace{f}_{=qp+r} = a(qp + r) = aqp + ar$.

On the other hand, $u \in aR \cap pR \subseteq pR$. In other words, there exists some $v \in R$ such that $u = pv$. Consider this $v$. We have $pv = u = aqp + ar$. Solving this equation for $ar$, we obtain $ar = pv - aqp = pv - paq = p(v - aq)$.

But $r \in A[X]_{\leq n-1}$ and thus $ar \in A[X]_{\leq n-1}$ (since $a \in A$ and since $A[X]_{\leq n-1}$ is an $A$-submodule of $A[X]$). Hence, $p(v - aq) = ar \in A[X]_{\leq n-1}$. Thus, Proposition 3.13 (applied to $v - aq$ instead of $q$) yields $v - aq = 0$. Hence, $v = aq$, so that $u = p \underbrace{v}_{=aq} = paq = ap \underbrace{q}_{\in R} \in apR$.

Now, forget that we fixed $u$. We thus have shown that every $u \in aR \cap pR$ satisfies $u \in apR$. In other words, $aR \cap pR = apR$. Combined with $apR \subseteq aR \cap pR$, this yields $aR \cap pR = apR$. This proves Corollary 3.21. □

The claim of Corollary 3.21 can be restated as follows: If $A$, $n$, $p$, $a$ and $R$ as in Corollary 3.21, then every polynomial in $R$ that is divisible by $a$ and by $p$ must be divisible by $ap$. This is a "sort of coprimality statement" (not in the usual sense of the word "coprimality", but more akin to the property of coprime positive integers $m$ and $n$ to satisfy $\operatorname{lcm}(m, n) = mn$). Theorems 1.3 and 1.2 are also statements of this kind, and ultimately we will use Corollary 3.21 as the first stepping stone in deriving these two theorems.

For the sake of (future) convenience, let us state a variant of Corollary 3.21 "translated through a ring isomorphism":

**Corollary 3.22.** Let $A$ and $B$ be two commutative rings. Let $f : A[X] \to B$ be a ring isomorphism. Let $n \in \mathbb{N}$. Let $p \in B$ be such that $f^{-1}(p)$ is a monic polynomial of degree $n$. Let $b \in B$ be such that $f^{-1}(b) \in A$. Then, $bB \cap pB = bpB$.

*Proof of Corollary 3.22.* Set $R = A[X]$. Corollary 3.21 (applied to $f^{-1}(b)$ and $f^{-1}(p)$ instead of $a$ and $p$) yields $f^{-1}(b) R \cap f^{-1}(p) R = f^{-1}(b) f^{-1}(p) R$.

But $f$ is a ring isomorphism from $A[X]$ to $B$, thus from $R$ to $B$ (since $R = A[X]$). Hence, applying $f$ to both sides of the equality $f^{-1}(b) R \cap f^{-1}(p) R = f^{-1}(b) f^{-1}(p) R$, we obtain $bB \cap pB = bpB$. This proves Corollary 3.22.

□

# 4. On multivariate polynomials

## 4.1. Notations and the isomorphisms $\rho_i$

Next, we shall discuss some properties of multivariate polynomial rings of the form $A[X_1, X_2, \ldots, X_n]$. First, we recall that such rings can be obtained recursively by adjoining one variable after the other; indeed, for each $n \in \mathbb{N}$ and each $i \in \{1, 2, \ldots, n\}$, there is a canonical isomorphism

$$A[X_1, X_2, \ldots, X_n] \cong \left(A\left[X_1, X_2, \ldots, \widehat{X}_i, \ldots, X_n\right]\right)[X_i] \tag{6}$$

(where the "$\widehat{X}_i$" means that the element $X_i$ is removed from the list), which is often used to identify $A[X_1, X_2, \ldots, X_n]$ with $\left(A\left[X_1, X_2, \ldots, \widehat{X}_i, \ldots, X_n\right]\right)[X_i]$ (though we shall not make such identification). Let us first explain our notations:

**Convention 4.1.** Let $n \in \mathbb{N}$. Let $(u_1, u_2, \ldots, u_n)$ be a list of $n$ arbitrary objects. Let $i \in \{1, 2, \ldots, n\}$. Then, $(u_1, u_2, \ldots, \widehat{u_i}, \ldots, u_n)$ will denote the list $(u_1, u_2, \ldots, u_{i-1}, u_{i+1}, u_{i+2}, \ldots, u_n)$ (this is a list of $n-1$ objects). Thus, the hat over the symbol $u_i$ signifies that the $i$-th entry of the list is being removed. (It does **not** mean that every object that happens to be equal to $u_i$ is removed from the list; we only remove the $i$-th object. So, for example, the list $\left((-5)^2, (-4)^2, \ldots, \widehat{2^2}, \ldots, 5^2\right)$ contains the entry $(-2)^2$, even though this entry equals the removed entry $2^2$.)

**Definition 4.2.** Let $A$ be a commutative ring. Let $n \in \mathbb{N}$. Let $R$ denote the polynomial ring $A[X_1, X_2, \ldots, X_n]$. For each $i \in \{1, 2, \ldots, n\}$, we let $R_i$ denote the polynomial ring $A\left[X_1, X_2, \ldots, \widehat{X}_i, \ldots, X_n\right]$ (a polynomial ring in $n-1$ indeterminates).

For each $i \in \{1, 2, \ldots, n\}$, we regard $R_i$ as an $A$-subalgebra of $R$. For each $i \in \{1, 2, \ldots, n\}$, we let $\rho_i : R_i[X] \to R$ be the $R_i$-algebra homomorphism which sends every $p \in R_i[X]$ to $p(X_i)$. In other words, $\rho_i : \left(A\left[X_1, X_2, \ldots, \widehat{X}_i, \ldots, X_n\right]\right)[X] \to A[X_1, X_2, \ldots, X_n]$ is the $A$-algebra homomorphism which satisfies

$$\left(\rho_i(X_j) = X_j \qquad \text{for every } j \in \left\{1, 2, \ldots, \widehat{i}, \ldots, n\right\}\right) \tag{7}$$

an

$$\rho_i(X) = X_i. \tag{8}$$

It is well-known that this $\rho_i$ is actually an $R_i$-algebra isomorphism. Indeed, this $\rho_i$ is the isomorphism responsible for (6) (at least if we rename the indeterminate

$X$ in $R_i[X]$ as $X_i$). Since the map $\rho_i$ is a $R_i$-algebra isomorphism, its inverse $\rho_i^{-1}$ is well-defined and also a $R_i$-algebra isomorphism.

These notations $A$, $n$, $R$, $R_i$ and $\rho_i$ shall be in place for the whole Section 4.

## 4.2. Regularity of $X_i - X_j$

**Proposition 4.3.** Let $i$ and $j$ be two distinct elements of $\{1, 2, \ldots, n\}$.
**(a)** The polynomial $\rho_i^{-1}(X_i - X_j) \in R_i[X]$ is monic of degree 1.
**(b)** The element $X_i - X_j$ of $R$ is regular.

*Proof of Proposition 4.3.* The definition of $R_i$ yields $R_i = A\left[X_1, X_2, \ldots, \widehat{X_i}, \ldots, X_n\right]$.

Combining $j \in \{1, 2, \ldots, n\}$ with $j \neq i$ (since $i$ and $j$ are distinct), we obtain $j \in \{1, 2, \ldots, n\} \setminus \{i\} = \left\{1, 2, \ldots, \widehat{i}, \ldots, n\right\}$. Hence, $X_j \in A\left[X_1, X_2, \ldots, \widehat{X_i}, \ldots, X_n\right] = R_i$. Hence, $X - X_j$ is a well-defined polynomial in $R_i[X]$. Clearly, this polynomial $X - X_j \in R_i[X]$ is monic of degree 1.

Now, $\rho_i$ is an $R_i$-algebra homomorphism. Hence,

$$\rho_i(X - X_j) = \underbrace{\rho_i(X)}_{\substack{=X_i \\ \text{(by (8))}}} - \underbrace{\rho_i(X_j)}_{\substack{=X_j \\ \text{(by (7))}}} = X_i - X_j.$$

Hence, $X - X_j = \rho_i^{-1}(X_i - X_j)$.

Now, recall that the polynomial $X - X_j \in R_i[X]$ is monic of degree 1. Since $X - X_j = \rho_i^{-1}(X_i - X_j)$, this rewrites as follows: The polynomial $\rho_i^{-1}(X_i - X_j) \in R_i[X]$ is monic of degree 1. This proves Proposition 4.3 **(a)**.

**(b)** The map $\rho_i : R_i[X] \to R$ is an $R_i$-algebra isomorphism, thus a ring isomorphism.

The polynomial $X - X_j \in R_i[X]$ is monic of degree 1. Thus, Corollary 3.15 (applied to 1, $R_i$ and $X - X_j$ instead of $n$, $A$ and $p$) shows that the element $X - X_j$ of $R_i[X]$ is regular. Hence, Proposition 2.4 (applied to $R_i[X]$, $R$, $\rho_i$ and $X - X_j$ instead of $A$, $B$, $f$ and $a$) shows that $\rho_i(X - X_j)$ is a regular element of $R$ (since $\rho_i : R_i[X] \to R$ is a ring isomorphism). In other words, $X_i - X_j$ is a regular element of $R$ (since $\rho_i(X - X_j) = X_i - X_j$). This proves Proposition 4.3. □

**Corollary 4.4.** The polynomial $\prod_{1 \leq i < j \leq n} (X_i - X_j)$ is a regular element of $R$.

*Proof of Corollary 4.4.* Proposition 4.3 **(b)** shows that $\prod_{1 \leq i < j \leq n} (X_i - X_j)$ is a product of finitely many regular elements. Hence, $\prod_{1 \leq i < j \leq n} (X_i - X_j)$ is itself regular (since Proposition 2.3 shows that a product of finitely many regular elements must itself be regular). □

## 4.3. Simultaneous multiples of $X_p - X_q$ and $X_u - X_v$

**Proposition 4.5.** Let $H$ be the set $\left\{(i,j) \in \{1,2,\ldots,n\}^2 \mid i < j\right\}$. Let $(p,q)$ and $(u,v)$ be two distinct elements of $H$. Then, either $X_u - X_v \in R_p$ or $X_u - X_v \in R_q$ (or both).

*Proof of Proposition 4.5.* We have $(p,q) \in H$; in other words, $(p,q) \in \{1,2,\ldots,n\}^2$ and $p < q$ (by the definition of $H$). Similarly, $(u,v) \in \{1,2,\ldots,n\}^2$ and $u < v$.

We now observe that if $r$ is an element of $\{1,2,\ldots,n\}$ satisfying $r \notin \{u,v\}$, then

$$X_u - X_v \in R_r \tag{9}$$

[10].

But it is impossible that both $p$ and $q$ belong to the set $\{u,v\}$ [11]. Hence, we are in one of the following two cases:

*Case 1:* We have $p \notin \{u,v\}$.

*Case 2:* We have $q \notin \{u,v\}$.

In Case 1, we have $p \notin \{u,v\}$ and therefore $X_u - X_v \in R_p$ (by (9), applied to $r = p$). Hence, Proposition 4.5 holds in Case 1.

In Case 2, we have $q \notin \{u,v\}$ and therefore $X_u - X_v \in R_q$ (by (9), applied to $r = q$). Hence, Proposition 4.5 holds in Case 2.

Thus, Proposition 4.5 holds in both Cases 1 and 2. Hence, Proposition 4.5 holds always. □

We now prove a "coprimality statement" for polynomials of the form $X_i - X_j$:

**Proposition 4.6.** Let $H$ be the set $\left\{(i,j) \in \{1,2,\ldots,n\}^2 \mid i < j\right\}$. For every $(i,j) \in H$, define an element $a_{(i,j)}$ of $R$ by $a_{(i,j)} = X_i - X_j$. Let $g$ and $h$ be two distinct elements of $H$. Then, $a_g R \cap a_h R = a_g a_h R$.

Before we prove this, let us state a lemma (for the sake of convenience):

[10] *Proof of (9):* Let $r$ be an element of $\{1,2,\ldots,n\}$ satisfying $r \notin \{u,v\}$. From $r \notin \{u,v\}$, we obtain $r \neq u$ and $r \neq v$. From $r \neq u$, we obtain $u \neq r$, so that $u \in \{1,2,\ldots,n\} \setminus \{r\} = \{1,2,\ldots,\widehat{r},\ldots,n\}$. Hence, $X_u \in A\left[X_1, X_2, \ldots, \widehat{X_r}, \ldots, X_n\right] = R_r$ (since $R_r$ was defined as $A\left[X_1, X_2, \ldots, \widehat{X_r}, \ldots, X_n\right]$). Similarly, $X_v \in R_r$. Thus, both polynomials $X_u$ and $X_v$ belong to $R_r$; hence, so does their difference $X_u - X_v$. In other words, $X_u - X_v \in R_r$. This proves (9).

[11] *Proof.* Assume the contrary. Hence, both $p$ and $q$ belong to the set $\{u,v\}$. Since $p < q$, this shows that $p$ is the smaller of the two integers $u$ and $v$, whereas $q$ is the larger of the two integers $u$ and $v$. But the smaller of the two integers $u$ and $v$ is $u$ (since $u < v$). Thus, $p = u$ (since $p$ is the smaller of the two integers $u$ and $v$); similarly, $q = v$. Hence, $\left(\underbrace{p}_{=u}, \underbrace{q}_{=v}\right) = (u,v)$. This contradicts the fact that $(p,q)$ and $(u,v)$ are distinct. This contradiction shows that our assumption was wrong, qed.

**Lemma 4.7.** Let $u$, $v$ and $r$ be three elements of $\{1,2,\ldots,n\}$ such that $u \neq v$. Assume that $X_u - X_v \in R_r$.

Set $b = X_u - X_v$. Also, let $p \in R$ be such that $\rho_r^{-1}(p) \in R_r[X]$ is a monic polynomial of degree 1. Then, $bR \cap pR = bpR$.

*Proof of Lemma 4.7.* Recall that $\rho_i : R_i[X] \to R$ is an $R_i$-algebra isomorphism for every $i \in \{1,2,\ldots,n\}$. Applying this to $i = r$, we see that $\rho_r : R_r[X] \to R$ is an $R_r$-algebra isomorphism, thus a ring isomorphism.

We have $b = X_u - X_v \in R_r \subseteq R_r[X]$. Hence, $\rho_r(b)$ is well-defined. Moreover, $b \in R_r$ and thus $\rho_r(b) = b$ (since $\rho_r$ is an $R_r$-algebra homomorphism); thus, $\rho_r^{-1}(b) = b \in R_r$. Thus, Corollary 3.22 (applied to $R_r$, $R$, $\rho_r$ and 1 instead of $A$, $B$, $f$ and $n$) shows that $bR \cap pR = bpR$. This proves Lemma 4.7. □

*Proof of Proposition 4.6.* Write the elements $g$ and $h$ of $H$ in the forms $g = (p,q)$ and $h = (u,v)$. Thus, $p < q$ and $u < v$.

The elements $g$ and $h$ are distinct. In other words, the elements $(p,q)$ and $(u,v)$ are distinct (since $g = (p,q)$ and $h = (u,v)$).

From $g = (p,q)$, we obtain $a_g = a_{(p,q)} = X_p - X_q$ (by the definition of $a_{(p,q)}$). Similarly, $a_h = X_u - X_v$.

Proposition 4.5 shows that we have either $X_u - X_v \in R_p$ or $X_u - X_v \in R_q$ (or both). In other words, we are in one of the following two cases:

*Case 1:* We have $X_u - X_v \in R_p$.

*Case 2:* We have $X_u - X_v \in R_q$.

Let us first consider Case 1. In this case, we have $X_u - X_v \in R_p$. Hence, $a_h = X_u - X_v \in R_p$.

But the elements $p$ and $q$ of $\{1,2,\ldots,n\}$ are distinct (since $p < q$). Proposition 4.3 **(a)** (applied to $i = p$ and $j = q$) thus yields that the polynomial $\rho_p^{-1}(X_p - X_q) \in R_p[X]$ is monic of degree 1. In other words, the polynomial $\rho_p^{-1}(a_g) \in R_p[X]$ is monic of degree 1 (since $a_g = X_p - X_q$). Thus, Lemma 4.7 (applied to $p$, $a_h$ and $a_g$ instead of $r$, $b$ and $p$) yields $a_h R \cap a_g R = a_h a_g R$. Thus,

$$a_g R \cap a_h R = a_h R \cap a_g R = \underbrace{a_h a_g}_{= a_g a_h} R = a_g a_h R.$$

Hence, Proposition 4.6 is proven in Case 1.

Let us now consider Case 2. In this case, we have $X_u - X_v \in R_q$. Hence, $a_h = X_u - X_v \in R_q$.

But the elements $q$ and $p$ of $\{1,2,\ldots,n\}$ are distinct (since $p < q$). Proposition 4.3 **(a)** (applied to $i = q$ and $j = p$) thus yields that the polynomial $\rho_q^{-1}(X_q - X_p) \in R_q[X]$ is monic of degree 1. In other words, the polynomial $\rho_q^{-1}(-a_g) \in R_q[X]$ is monic of degree 1 (since $-\underbrace{a_g}_{= X_p - X_q} = -(X_p - X_q) = X_q - X_p$). Thus, Lemma 4.7 (applied to $q$, $a_h$ and $-a_g$ instead of $r$, $b$ and $p$) yields $a_h R \cap (-a_g) R = a_h (-a_g) R$.

Now,

$$a_g R \cap a_h R = a_h R \cap \underbrace{a_g R}_{=-a_g R=\left(-a_g\right)R} = a_h R \cap \left(-a_g\right) R = a_h \underbrace{\left(-a_g\right) R}_{=-a_g R=a_g R}$$
$$= \underbrace{a_h a_g}_{=a_g a_h} R = a_g a_h R.$$

Hence, Proposition 4.6 is proven in Case 2.

We have now proven Proposition 4.6 in each of the two Cases 1 and 2. Thus, Proposition 4.6 always holds. □

# 5. "lcm-coprimality"

## 5.1. A general fact about intersections of principal ideals

One way to characterize coprime positive integers is the following: Two positive integers $n$ and $m$ are coprime if and only if $\operatorname{lcm}(n,m) = nm$. In slightly more algebraic terms: Two positive integers $n$ and $m$ are coprime if and only if $n\mathbb{Z} \cap m\mathbb{Z} = nm\mathbb{Z}$. (This also holds for arbitrary nonzero integers $n$ and $m$, but fails if $n$ or $m$ is allowed to be zero.) In analogy to this, we might wonder when two elements $b$ and $c$ of a commutative ring $R$ satisfy $bR \cap cR = bcR$. This is one possible way to generalize coprimality of positive integers to ring elements[12].

Our proof of Theorem 1.3 will use a combination of Proposition 4.6 and the following general fact:

**Proposition 5.1.** Let $R$ be a commutative ring. Let $G$ be a finite set. For every $g \in G$, let $a_g$ be a regular element of $R$. Assume that every two distinct elements $g$ and $h$ of $G$ satisfy $a_g R \cap a_h R = a_g a_h R$. Then, $\bigcap\limits_{g\in G} \left(a_g R\right) = \left(\prod\limits_{g\in G} a_g\right) R$.

*Proof of Proposition 5.1.* We have assumed that every two distinct elements $g$ and $h$ of $G$ satisfy

$$a_g R \cap a_h R = a_g a_h R. \tag{10}$$

Now, we shall prove that every subset $S$ of $G$ satisfies

$$\bigcap_{g\in S} \left(a_g R\right) = \left(\prod_{g\in S} a_g\right) R. \tag{11}$$

*Proof of (11):* We will prove (11) by induction on $|S|$:

[12] though not the only possible way – for example, another, non-equivalent generalization is to study elements $b$ and $c$ of $R$ satisfying $bR + cR = R$

*Induction base:* The equality (11) holds in the case when $|S| = 0$ [13].

*Induction step:* Let $N$ be a positive integer. Assume (as our induction hypothesis) that (11) holds in the case when $|S| = N - 1$. We must prove that (11) holds in the case when $|S| = N$.

Let $S$ be a subset of $G$ satisfying $|S| = N$.

We have $|S| = N > 0$. Hence, there exists a $k \in S$. Pick such a $k$.

Define an element $b \in R$ by $b = \prod_{g \in S \setminus \{k\}} a_g$.

From $k \in S$, we obtain $|S \setminus \{k\}| = \underbrace{|S|}_{=N} - 1 = N - 1$. Hence, we can apply (11) to $S \setminus \{k\}$ instead of $S$ (because of the induction hypothesis). We thus obtain

$$\bigcap_{g \in S \setminus \{k\}} \left(a_g R\right) = \underbrace{\left(\prod_{g \in S \setminus \{k\}} a_g\right)}_{=b} R = bR. \tag{12}$$

But $k \in S$. Hence,

$$\bigcap_{g \in S} \left(a_g R\right) = a_k R \cap \underbrace{\bigcap_{g \in S \setminus \{k\}} \left(a_g R\right)}_{\substack{=bR \\ \text{(by (12))}}} = a_k R \cap bR. \tag{13}$$

On the other hand, $k \in S$, so that

$$\prod_{g \in S} a_g = a_k \underbrace{\prod_{g \in S \setminus \{k\}} a_g}_{=b} = a_k b. \tag{14}$$

Combining $a_k \underbrace{bR}_{\subseteq R} \subseteq a_k R$ with $\underbrace{a_k b}_{=ba_k} R = b \underbrace{a_k R}_{\subseteq R} \subseteq bR$, we obtain $a_k bR \subseteq a_k R \cap bR$.

On the other hand, let $x \in a_k R \cap bR$. Then, $x \in a_k R \cap bR = \bigcap_{g \in S} \left(a_g R\right)$ (by (13)). In other words,

$$x \in a_g R \qquad \text{for every } g \in S. \tag{15}$$

But $x \in a_k R \cap bR \subseteq a_k R$. In other words, there exists some $z \in R$ such that $x = a_k z$. Consider this $z$. We have

$$z \in a_g R \qquad \text{for every } g \in S \setminus \{k\}. \tag{16}$$

[13] Indeed, in the case when $|S| = 0$, the set $S$ is empty; thus, the left hand side of (11) is the empty intersection of subsets of $R$ (and thus equal to $R$), whereas the right hand side of (11) is $1R$ (because the product $\prod_{g \in S} a_g$ is the empty product and thus equals 1). So (11) becomes $R = 1R$ in this case; but this holds obviously.

[*Proof of (16):* Let $g \in S \setminus \{k\}$. We want to show that $z \in a_g R$.

We have $g \in S \setminus \{k\}$. In other words, $g \in S$ and $g \neq k$. From $g \in S \subseteq G$ and $k \in S \subseteq G$, we conclude that $g$ and $k$ are two elements of $G$. Furthermore, these two elements are distinct (since $g \neq k$). Hence, (10) (applied to $h = k$) yields $a_g R \cap a_k R = a_g a_k R$.

But (15) yields $x \in a_g R$. Combining this with $x \in a_k R$, we obtain $x \in a_g R \cap a_k R = a_g a_k R$. In other words, there exists some $w \in R$ such that $x = a_g a_k w$. Consider this $w$.

We have $a_k \left(z - a_g w\right) = \underbrace{a_k z}_{=x} - \underbrace{a_k a_g}_{=a_g a_k} w = x - \underbrace{a_g a_k w}_{=x} = x - x = 0$. But the element $a_k$ of $R$ is regular (indeed, $a_h$ is a regular element of $R$ for each $h \in G$). Hence, from $a_k \left(z - a_g w\right) = 0$, we obtain $z - a_g w = 0$. Hence, $z = a_g \underbrace{w}_{\in R} \in a_g R$. This proves (16).]

From (16), we obtain $z \in \bigcap_{g \in S \setminus \{k\}} \left(a_g R\right) = bR$ (by (12)). Hence, $x = a_k \underbrace{z}_{\in bR} \in a_k bR$.

Now, forget that we fixed $x$. We thus have shown that every $x \in a_k R \cap bR$ satisfies $x \in a_k bR$. In other words, $a_k R \cap bR \subseteq a_k bR$. Combining this with $a_k bR \subseteq a_k R \cap bR$, we obtain $a_k R \cap bR = a_k bR$.

Now, (13) becomes

$$\bigcap_{g \in S} \left(a_g R\right) = a_k R \cap bR = \underbrace{a_k b}_{\substack{= \prod_{g \in S} a_g \\ \text{(by (14))}}} R = \left(\prod_{g \in S} a_g\right) R.$$

Now, forget that we fixed $S$. We thus have shown that every subset $S$ of $G$ satisfying $|S| = N$ satisfies $\bigcap_{g \in S} \left(a_g R\right) = \left(\prod_{g \in S} a_g\right) R$. In other words, (11) holds in the case when $|S| = N$. This completes the induction proof of (11).

Now, Proposition 5.1 follows by applying (11) to $S = G$. □

## 5.2. Application to the polynomials $X_i - X_j$

**Corollary 5.2.** Let $A$ be a commutative ring with unity. Let $n \in \mathbb{N}$. Let $G$ be a subset of the set $\left\{(i,j) \in \{1,2,\ldots,n\}^2 \mid i < j\right\}$. Let $R$ be the polynomial ring $A\left[X_1, X_2, \ldots, X_n\right]$. Then,

$$\bigcap_{(i,j) \in G} \left(\left(X_i - X_j\right) R\right) = \left(\prod_{(i,j) \in G} \left(X_i - X_j\right)\right) R.$$

*Proof of Corollary 5.2.* Let $H$ be the set $\left\{(i,j) \in \{1,2,\ldots,n\}^2 \mid i < j\right\}$. Thus, $G \subseteq H \subseteq \{1,2,\ldots,n\}^2$.

For every $(i,j) \in H$, define an element $a_{(i,j)}$ of $R$ by $a_{(i,j)} = X_i - X_j$. Hence, an element $a_g$ of $R$ is defined for each $g \in G$ (since $G \subseteq H$).

For every $g \in G$, the element $a_g$ is a regular element of $R$ [14]. Every two distinct elements $g$ and $h$ of $G$ satisfy $a_g R \cap a_h R = a_g a_h R$ [15]. Hence, Proposition 5.1 shows that

$$\bigcap_{g \in G} \left(a_g R\right) = \left(\prod_{g \in G} a_g\right) R.$$

Renaming the index $g$ as $(i,j)$ on both sides of this equality, we obtain

$$\bigcap_{(i,j) \in G} \left(a_{(i,j)} R\right) = \left(\prod_{(i,j) \in G} a_{(i,j)}\right) R.$$

Since $a_{(i,j)} = X_i - X_j$ for every $(i,j) \in G$, this rewrites as

$$\bigcap_{(i,j) \in G} \left(\left(X_i - X_j\right) R\right) = \left(\prod_{(i,j) \in G} \left(X_i - X_j\right)\right) R.$$

This proves Corollary 5.2. □

## 5.3. Proving Theorems 1.3 and 1.2

We can now prove Theorems 1.3 and 1.2:

*Proof of Theorem 1.3.* Let $R$ be the polynomial ring $A\left[X_1, X_2, \ldots, X_n\right]$.

We know that $f$ is divisible by $X_i - X_j$ for every $(i,j) \in G$. In other words, $f \in \left(X_i - X_j\right) R$ for every $(i,j) \in G$. In other words, $f \in \bigcap_{(i,j) \in G} \left(\left(X_i - X_j\right) R\right)$.

Now,

$$f \in \bigcap_{(i,j) \in G} \left(\left(X_i - X_j\right) R\right) = \left(\prod_{(i,j) \in G} \left(X_i - X_j\right)\right) R \qquad \text{(by Corollary 5.2)}.$$

[14] *Proof.* Let $g \in G$. Then, $g \in G \subseteq \left\{(i,j) \in \{1,2,\ldots,n\}^2 \mid i < j\right\}$. In other words, $g = (i,j)$ for some $(i,j) \in \{1,2,\ldots,n\}^2$ satisfying $i < j$. Consider this $(i,j)$. From $g = (i,j)$, we obtain $a_g = a_{(i,j)} = X_i - X_j$ (by the definition of $a_{(i,j)}$).

Clearly, $i$ and $j$ are elements of $\{1,2,\ldots,n\}$ (since $(i,j) \in \{1,2,\ldots,n\}^2$) and are distinct (since $i < j$). Therefore, Proposition 4.3 **(b)** shows that the element $X_i - X_j$ of $R$ is regular. In other words, the element $a_g$ of $R$ is regular (since $a_g = X_i - X_j$). Qed.

[15] *Proof.* Let $g$ and $h$ be two distinct elements of $G$. Then, $g \in G \subseteq H$ and $h \in G \subseteq H$. Hence, $g$ and $h$ are two elements of $H$. Thus, Proposition 4.6 shows that $a_g R \cap a_h R = a_g a_h R$. Qed.

In other words, $f$ is divisible by $\prod_{(i,j)\in G}\left(X_i - X_j\right)$ in the ring $R$. This proves Theorem 1.3.

□

*Proof of Theorem 1.2.* Theorem 1.2 follows from Theorem 1.3 if we set $G = \left\{(i,j) \in \{1,2,\ldots,n\}^2 \mid i < j\right\}$. □

# 6. Analogues for power series

## 6.1. When is $X - a \in A\left[\left[X\right]\right]$ regular?

Let us now try to extend some of the above results from polynomials to power series.

Recall that if $A$ is a commutative ring, then $A\left[\left[X\right]\right]$ denotes the ring of formal power series in one indeterminate $X$ over $A$. This ring contains $A\left[X\right]$ as a subring. First, I shall show two facts that can be viewed as partial analogues of Corollary 3.15:

**Proposition 6.1.** Let $A$ be a commutative ring. Let $a$ be a nilpotent element of $A$. Then, the element $X - a$ of $A\left[\left[X\right]\right]$ is regular.

**Proposition 6.2.** Let $A$ be a commutative ring. Let $a$ be a regular element of $A$. Then, the element $X - a$ of $A\left[\left[X\right]\right]$ is regular.

*Proof of Proposition 6.1.* Let $x \in A\left[\left[X\right]\right]$ be such that $\left(X - a\right)x = 0$. We shall prove that $x = 0$.

Write the power series $x$ in the form $x = \sum_{i\in\mathbb{N}} c_i X^i$ for some sequence $(c_0, c_1, c_2, \ldots) \in A^{\mathbb{N}}$.

Extend the sequence $(c_0, c_1, c_2, \ldots) \in A^{\mathbb{N}}$ to a sequence $(c_{-1}, c_0, c_1, c_2, \ldots) \in A^{\{-1,0,1,\ldots\}}$ by setting $c_{-1} = 0$. Then,

$$\begin{aligned}\sum_{i\in\mathbb{N}} c_{i-1}X^i &= \underbrace{c_{-1}}_{=0}X^0 + \sum_{\substack{i\in\mathbb{N};\\ i>0}} c_{i-1}X^i = \underbrace{0X^0}_{=0} + \sum_{\substack{i\in\mathbb{N};\\ i>0}} c_{i-1}X^i = \sum_{\substack{i\in\mathbb{N};\\ i>0}} c_{i-1}X^i \\ &= \sum_{i\in\mathbb{N}} c_i \underbrace{X^{i+1}}_{=XX^i} \qquad \text{(here, we have substituted } i \text{ for } i-1 \text{ in the sum)} \\ &= \sum_{i\in\mathbb{N}} c_i XX^i = X\underbrace{\sum_{i\in\mathbb{N}} c_i X^i}_{=x} = Xx. \end{aligned} \tag{17}$$

On the other hand, $(X-a)\,x = 0$. Thus,

$$0 = (X-a)\,x = \underbrace{Xx}_{\substack{=\sum_{i\in\mathbb{N}} c_{i-1}X^i \\ \text{(by (17))}}} - a \underbrace{x}_{=\sum_{i\in\mathbb{N}} c_i X^i} = \sum_{i\in\mathbb{N}} c_{i-1}X^i - a \underbrace{\sum_{i\in\mathbb{N}} c_i X^i}_{=\sum_{i\in\mathbb{N}} ac_i X^i}$$
$$= \sum_{i\in\mathbb{N}} c_{i-1}X^i - \sum_{i\in\mathbb{N}} ac_i X^i.$$

In other words,

$$\sum_{i\in\mathbb{N}} c_{i-1}X^i = \sum_{i\in\mathbb{N}} ac_i X^i.$$

Comparing coefficients on both sides of this equality, we obtain

$$c_{i-1} = ac_i \qquad \text{for every } i \in \mathbb{N}. \tag{18}$$

Now, we can easily see that every $i \in \{-1, 0, 1, \ldots\}$ and $j \in \mathbb{N}$ satisfy

$$c_i = a^j c_{i+j} \tag{19}$$

[16].

But the element $a$ of $A$ is nilpotent. In other words, there exists some $k \in \mathbb{N}$ such that $a^k = 0$ (by the definition of "nilpotent"). Consider this $k$. Every $i \in \mathbb{N}$ satisfies

$$c_i = \underbrace{a^k}_{=0} c_{i+k} \qquad \text{(by (19) (applied to } j = k\text{))}$$
$$= 0. \tag{20}$$

Now, $x = \sum_{i\in\mathbb{N}} \underbrace{c_i}_{\substack{=0 \\ \text{(by (20))}}} X^i = \sum_{i\in\mathbb{N}} 0X^i = 0$.

Now, forget that we fixed $x$. We thus have shown that every $x \in A\,[[X]]$ satisfying $(X-a)\,x = 0$ satisfies $x = 0$.

[16] *Proof of (19):* Fix $i \in \{-1, 0, 1, \ldots\}$. We shall prove (19) by induction over $j$:

*Induction base:* We have $\underbrace{a^0}_{=1}\underbrace{c_{i+0}}_{=c_i} = c_i$. Thus, $c_i = a^0 c_{i+0}$. In other words, (19) holds for $j = 0$. This completes the induction base.

*Induction step:* Let $J \in \mathbb{N}$ be positive. Assume that (19) holds for $j = J-1$. We must now show that (19) holds for $j = J$.

We have assumed that (19) holds for $j = J-1$. In other words, we have $c_i = a^{J-1}c_{i+J-1}$. Now,

$$c_i = a^{J-1} \underbrace{c_{i+J-1}}_{\substack{=ac_{i+J} \\ \text{(by (18) (applied to } i+J \\ \text{instead of } i\text{))}}} = \underbrace{a^{J-1}a}_{=a^J} c_{i+J} = a^J c_{i+J}.$$

In other words, (19) holds for $j = J$. Thus, the induction step is complete. Hence, (19) is proven by induction.

But the element $X - a$ of $A[[X]]$ is regular if and only if every $x \in A[[X]]$ satisfying $(X - a)\, x = 0$ satisfies $x = 0$ (by the definition of "regular"). Hence, the element $X - a$ of $A[[X]]$ is regular (since every $x \in A[[X]]$ satisfying $(X - a)\, x = 0$ satisfies $x = 0$). This proves Proposition 6.1. □

We shall generalize Proposition 6.1 in Subsection 10.2 (and show a second proof for it).

*Proof of Proposition 6.2.* The element $a$ of $A$ is regular if and only if every $x \in A$ satisfying $ax = 0$ satisfies $x = 0$ (by the definition of "regular"). Hence,

$$\text{every } x \in A \text{ satisfying } ax = 0 \text{ satisfies } x = 0 \tag{21}$$

(since the element $a$ of $A$ is regular).

Let $x \in A[[X]]$ be such that $(X - a)\, x = 0$. We shall prove that $x = 0$.

Write the power series $x$ in the form $x = \sum_{i \in \mathbb{N}} c_i X^i$ for some sequence $(c_0, c_1, c_2, \ldots) \in A^{\mathbb{N}}$.

Extend the sequence $(c_0, c_1, c_2, \ldots) \in A^{\mathbb{N}}$ to a sequence $(c_{-1}, c_0, c_1, c_2, \ldots) \in A^{\{-1,0,1,\ldots\}}$ by setting $c_{-1} = 0$. Then, the equality (18) holds (for the same reasons that we explained in the proof of Proposition 6.1). Using this equality and the regularity of $a$, we can easily find that

$$c_i = 0 \qquad \text{for every } i \in \{-1, 0, 1, \ldots\} \tag{22}$$

[17].

Now, $x = \sum_{i \in \mathbb{N}} \underbrace{c_i}_{\substack{=0 \\ \text{(by (22))}}} X^i = \sum_{i \in \mathbb{N}} 0 X^i = 0$.

Now, forget that we fixed $x$. We thus have shown that every $x \in A[[X]]$ satisfying $(X - a)\, x = 0$ satisfies $x = 0$.

But the element $X - a$ of $A[[X]]$ is regular if and only if every $x \in A[[X]]$ satisfying $(X - a)\, x = 0$ satisfies $x = 0$ (by the definition of "regular"). Hence, the element $X - a$ of $A[[X]]$ is regular (since every $x \in A[[X]]$ satisfying $(X - a)\, x = 0$ satisfies $x = 0$). This proves Proposition 6.2. □

Proposition 6.1 and Proposition 6.2 give two sufficient criteria for a power series of the form $X - a$ to be a regular element of $A[[X]]$. These criteria are not necessary

[17] *Proof of (22):* We shall prove (22) by induction over $i$:

*Induction base:* We have $c_{-1} = 0$. In other words, (22) holds for $i = -1$. This completes the induction base.

*Induction step:* Let $j \in \mathbb{N}$. Assume that (22) holds for $i = j - 1$. We must prove that (22) holds for $i = j$.

We have assumed that (22) holds for $i = j - 1$. In other words, we have $c_{j-1} = 0$. Now, (18) (applied to $i = j$) yields $c_{j-1} = ac_j$. Hence, $ac_j = c_{j-1} = 0$. Thus, $c_j = 0$ (by (21) (applied to $c_j$ instead of $x$)). In other words, (22) holds for $i = j$. This completes the induction step. Hence, the induction proof of (22) is complete.

(not even in combination); for example, the power series $X - \overline{2} \in (\mathbb{Z}/6\mathbb{Z})[[X]]$ (where $\overline{2}$ denotes the residue class of $2 \in \mathbb{Z}$ modulo 6) is regular, even though the element $\overline{2}$ of $\mathbb{Z}/6\mathbb{Z}$ is neither nilpotent nor regular. More generally, the element $X - a$ of $A[[X]]$ is regular whenever the ring $A$ is Noetherian[18]; it is also regular whenever there exists a $k \in \mathbb{N}$ satisfying $a^k A = a^{k+1} A$. We leave the proofs of these facts to the reader. Let me observe that **some** condition on $A$ and $a$ is needed to guarantee the regularity of $X - a$; in full generality the claim would not be true, as the following example shows:

**Example 6.3.** Let $K$ be a field. Let $A$ be the commutative $K$-algebra with generators $a, x_{-1}, x_0, x_1, \ldots$ and relations

$$x_{-1} = 0 \qquad \text{and} \qquad x_i = a x_{i+1} \text{ for all } i \geq -1.$$

Then, the power series $X - a \in A[[X]]$ is **not** regular.

*Proof of Example 6.3 (sketched).* Define a power series $x \in A[[X]]$ by $x = \sum_{i \in \mathbb{N}} x_i X^i$. Then, it is easy to see that $(X - a)\, x = 0$.

Let us now prove that $x_0 \neq 0$. Indeed, let us assume the contrary. Thus, $x_0 = 0$.

Let $\mathbf{A}$ be the polynomial algebra over $K$ in the indeterminates $\mathbf{a}, \mathbf{x}_{-1}, \mathbf{x}_0, \mathbf{x}_1, \mathbf{x}_2, \ldots$. Then, there is a unique ring homomorphism $\pi : \mathbf{A} \to A$ sending $\mathbf{a}$ to $a$ and sending each $\mathbf{x}_i$ to the corresponding $x_i$. This ring homomorphism $\pi$ is surjective, and its kernel is the ideal $\mathbf{I}$ of $\mathbf{A}$ generated by $\mathbf{x}_{-1}$ and $\mathbf{x}_i - \mathbf{a}\mathbf{x}_{i+1}$ for all $i \geq -1$. Since $\pi(\mathbf{x}_0) = x_0 = 0$, we see that the polynomial $\mathbf{x}_0 \in \mathbf{A}$ lies in this ideal $\mathbf{I}$. In other words, $\mathbf{x}_0$ is an $\mathbf{A}$-linear combination of $\mathbf{x}_{-1}$ and $\mathbf{x}_i - \mathbf{a}\mathbf{x}_{i+1}$ for all $i \geq -1$. In other words, there exists some $s \in \{-1, 0, 1, \ldots\}$, some $\mathbf{u} \in \mathbf{A}$ and some $\mathbf{v}_{-1}, \mathbf{v}_0, \ldots, \mathbf{v}_{s-1} \in \mathbf{A}$ such that

$$\mathbf{x}_0 = \mathbf{u} \cdot \mathbf{x}_{-1} + \sum_{i=-1}^{s-1} \mathbf{v}_i \cdot (\mathbf{x}_i - \mathbf{a}\mathbf{x}_{i+1}). \tag{23}$$

Consider these $s$, $\mathbf{u}$ and $\mathbf{v}_{-1}, \mathbf{v}_0, \ldots, \mathbf{v}_{s-1}$.

Now, consider the polynomial ring $K[T]$. The substitution

$$\mathbf{a} \mapsto T, \qquad \mathbf{x}_i \mapsto \begin{cases} T^{s-i}, & \text{if } i \leq s; \\ 0, & \text{if } i > s \end{cases}$$

defines a $K$-algebra homomorphism $\mathbf{A} \to K[T]$. Let $\widetilde{\mathbf{u}}$ and $\widetilde{\mathbf{v}}_i$ denote the images of $\mathbf{u}$ and $\mathbf{v}_i$ under this substitution. If we apply this substitution to both sides of the equality (23), then we obtain

$$T^s = \widetilde{\mathbf{u}} \cdot T^{s+1} + \sum_{i=-1}^{s-1} \widetilde{\mathbf{v}}_i \cdot \underbrace{\left(T^{s-i} - T T^{s-(i+1)}\right)}_{=0} = \widetilde{\mathbf{u}} \cdot T^{s+1}.$$

[18] Actually, a much stronger statement holds: If $A$ is Noetherian, then a power series $f \in A[[X]]$ is regular in $A[[X]]$ if and only if every $b \in A$ satisfying $bf = 0$ must satisfy $b = 0$. See [Fields71, Theorem 5].

Hence, $T^s$ is divisible by $T^{s+1}$ in $K[T]$. But this is clearly absurd. Hence, we have obtained a contradiction.

Thus, $x_0 \neq 0$ is proven. Since $x_0$ is the constant term of the power series $x$, this entails that $x \neq 0$. Hence, $X - a$ is not regular (because if $X - a$ were regular, then $(X - a)\, x = 0$ would yield $x = 0$, which would contradict $x \neq 0$). This completes the proof of Example 6.3.

(Notice that this proof mostly begs the question how the $K$-algebra $A$ looks like – e.g., whether it has an explicit combinatorial basis. It only shows that the element $x_0$ of $A$ is nonzero; as we saw, this was enough for our purposes.[19]) □

More general criteria for regularity of power series in $A[[X]]$ will be discussed in Section 10.

## 6.2. Notations and the isomorphisms $\rho_i$

We can now prove an analogue of Corollary 4.4 for power series, whose proof will be more or less the same as the proof of Corollary 4.4 itself. Let us first build up some notations.

Rings of formal power series (of the form $A[[X_1, X_2, \ldots, X_n]]$) can be obtained recursively by adjoining one variable after the other (similarly to polynomial rings $A[X_1, X_2, \ldots, X_n]$); indeed, for each $n \in \mathbb{N}$ and each $i \in \{1, 2, \ldots, n\}$, there is a canonical ring isomorphism

$$A[[X_1, X_2, \ldots, X_n]] \cong \left(A\left[\left[X_1, X_2, \ldots, \widehat{X_i}, \ldots, X_n\right]\right]\right)[[X_i]] \tag{24}$$

(where the "$\widehat{X_i}$" again means that the element $X_i$ is removed from the list).[20] This isomorphism is rather useful; let me introduce a notation for it:

[19] An explicit combinatorial basis can nevertheless be found. Namely,

$$\left(1, a, a^2, a^3, \ldots, x_0, x_1, x_2, \ldots\right)$$

is a basis of the $K$-vector space $A$. Indeed, to prove its linear independence, argue using substitutions such as the one above (for varying $s$). In order to prove that it spans $A$, argue that any product of two (or more) $x_i$'s is 0 (because $x_i \underbrace{x_j}_{=a^{i+1}x_{j+i+1}} = \underbrace{a^{i+1}x_i}_{=x_{-1}=0}\, x_{j+i+1} = 0$), and that any product of the form $a^i x_j$ can be rewritten as $\begin{cases} x_{j-i}, & \text{if } j \geq i; \\ 0, & \text{if } j < i \end{cases}$.

[20] Let me make some comments about this isomorphism:

Rings of formal power series are topological rings; the topology ensures that "reasonable" infinite sums such as $\sum_{i \in \mathbb{N}} X^i$ or $\sum_{(i,j) \in \mathbb{N}^2} X^i Y^j$ converge. This topology is defined as follows:

Let $B$ be a topological ring. Then, for any $m \in \mathbb{N}$ and any $m$ indeterminates $Y_1, Y_2, \ldots, Y_m$, we endow the ring $B[[Y_1, Y_2, \ldots, Y_m]]$ with the following topology: The $B$-module $B^{\mathbb{N}^m}$ is canonically equipped with a product topology (since $B$ itself has a topology). Use the $B$-module

**Definition 6.4.** Let $A$ be a commutative ring. Let $n \in \mathbb{N}$. Let $R$ denote the ring $A\left[\left[X_1, X_2, \ldots, X_n\right]\right]$ (a ring of formal power series in $n$ indeterminates). For each $i \in \{1, 2, \ldots, n\}$, we let $R_i$ denote the ring $A\left[\left[X_1, X_2, \ldots, \widehat{X_i}, \ldots, X_n\right]\right]$ (a ring of formal power series in $n-1$ indeterminates).

For each $i \in \{1, 2, \ldots, n\}$, we regard $R_i$ as an $A$-subalgebra of $R$. For each $i \in \{1, 2, \ldots, n\}$, we let $\rho_i : R_i\left[\left[X\right]\right] \to R$ be the continuous $R_i$-algebra homomorphism which sends every $p \in R_i\left[\left[X\right]\right]$ to $p\left(X_i\right)$. In other words, $\rho_i : \left(A\left[\left[X_1, X_2, \ldots, \widehat{X_i}, \ldots, X_n\right]\right]\right)\left[\left[X\right]\right] \to A\left[\left[X_1, X_2, \ldots, X_n\right]\right]$ is the continuous $A$-algebra homomorphism which satisfies

$$\left(\rho_i\left(X_j\right) = X_j \qquad \text{for every } j \in \left\{1, 2, \ldots, \widehat{i}, \ldots, n\right\}\right) \tag{25}$$

an

$$\rho_i\left(X\right) = X_i. \tag{26}$$

It is well-known that this $\rho_i$ is actually an $R_i$-algebra isomorphism. Indeed, this $\rho_i$ is the isomorphism responsible for (24) (at least if we rename the indeterminate $X$ in $R_i\left[\left[X\right]\right]$ as $X_i$). Since the map $\rho_i$ is a $R_i$-algebra isomorphism, its inverse $\rho_i^{-1}$ is well-defined and also a $R_i$-algebra isomorphism.

These notations $A$, $n$, $R$, $R_i$ and $\rho_i$ shall be in place for the rest of Section 6.

---

isomorphism

$$B\left[\left[Y_1, Y_2, \ldots, Y_m\right]\right] \to B^{\mathbb{N}^m},$$
$$f \mapsto \left(\text{the coefficient of } Y_1^{k_1} Y_2^{k_2} \cdots Y_m^{k_m} \text{ in } f\right)_{(k_1, k_2, \ldots, k_m) \in \mathbb{N}^m}$$

to transport the product topology from $B^{\mathbb{N}^m}$ to $B\left[\left[Y_1, Y_2, \ldots, Y_m\right]\right]$. The resulting topology on $B\left[\left[Y_1, Y_2, \ldots, Y_m\right]\right]$ makes the $B$-algebra $B\left[\left[Y_1, Y_2, \ldots, Y_m\right]\right]$ into a topological $B$-algebra; this is the topology we want. Notice that it depends on the topology on $B$. Explicitly, it is characterized by the following property: A net $\left(f_s\right)_{s \in S} \in \left(B\left[\left[Y_1, Y_2, \ldots, Y_m\right]\right]\right)^S$ of power series in $B\left[\left[Y_1, Y_2, \ldots, Y_m\right]\right]$ converges to a power series $f \in B\left[\left[Y_1, Y_2, \ldots, Y_m\right]\right]$ if and only if for each $(k_1, k_2, \ldots, k_m) \in \mathbb{N}^m$, the net $\left(\text{the coefficient of } Y_1^{k_1} Y_2^{k_2} \cdots Y_m^{k_m} \text{ in } f_s\right)_{s \in S} \in B^S$ converges to $\left(\text{the coefficient of } Y_1^{k_1} Y_2^{k_2} \cdots Y_m^{k_m} \text{ in } f\right)$ in $B$.

If $B$ is just a ring (not a topological ring), then the preceding definition still applies, provided that we regard $B$ as a topological ring by equipping it with the discrete topology.

Thus, the commutative ring $A$ becomes a topological ring (using the discrete topology), and therefore both sides of the isomorphism (24) become topological rings. The isomorphism (24) becomes an isomorphism of topological rings.

Let me once again reiterate that the topology on $B\left[\left[Y_1, Y_2, \ldots, Y_m\right]\right]$ is constructed using the topology on $B$. In particular, the topology on $\left(A\left[\left[X_1, X_2, \ldots, \widehat{X_i}, \ldots, X_n\right]\right]\right)\left[\left[X_i\right]\right]$ is constructed using the topology on $A\left[\left[X_1, X_2, \ldots, \widehat{X_i}, \ldots, X_n\right]\right]$, which is not (in general) the discrete topology!

## 6.3. Regularity of $X_i$ and $X_i - X_j$

**Proposition 6.5.** Let $i \in \{1, 2, \ldots, n\}$. Then, the element $X_i$ of $R$ is regular.

*Proof of Proposition 6.5.* The map $\rho_i : R_i[[X]] \to R$ is an $R_i$-algebra isomorphism, thus a ring isomorphism.

The element 0 of $R_i$ is nilpotent (since $0^1 = 0$). Hence, Proposition 6.1 (applied to $R_i$ and 0 instead of $A$ and $a$) yields that the element $X - 0$ of $R_i[[X]]$ is regular. In other words, the element $X$ of $R_i[[X]]$ is regular (since $X - 0 = X$). Hence, Proposition 2.4 (applied to $R_i[[X]]$, $R$, $\rho_i$ and $X$ instead of $A$, $B$, $f$ and $a$) shows that $\rho_i(X)$ is a regular element of $R$ (since $\rho_i : R_i[[X]] \to R$ is a ring isomorphism). In other words, $X_i$ is a regular element of $R$ (since $\rho_i(X) = X_i$). This proves Proposition 6.5. □

**Proposition 6.6.** Let $i$ and $j$ be two distinct elements of $\{1, 2, \ldots, n\}$. The element $X_i - X_j$ of $R$ is regular.

*Proof of Proposition 6.6.* The definition of $R_i$ yields $R_i = A\left[\left[X_1, X_2, \ldots, \widehat{X_i}, \ldots, X_n\right]\right]$. Recall that $R_i$ is an $A$-subalgebra of $R$, thus a subring of $R$.

Combining $j \in \{1, 2, \ldots, n\}$ with $j \neq i$ (since $i$ and $j$ are distinct), we obtain $j \in \{1, 2, \ldots, n\} \setminus \{i\} = \left\{1, 2, \ldots, \widehat{i}, \ldots, n\right\}$. Hence, $X_j \in A\left[\left[X_1, X_2, \ldots, \widehat{X_i}, \ldots, X_n\right]\right] = R_i$. So we have proven that $X_j$ is an element of $R_i$.

Now, $\rho_i$ is an $R_i$-algebra homomorphism. Hence,

$$\rho_i\left(X - X_j\right) = \underbrace{\rho_i(X)}_{\substack{=X_i \\ \text{(by (26))}}} - \underbrace{\rho_i\left(X_j\right)}_{\substack{=X_j \\ \text{(by (25))}}} = X_i - X_j.$$

Proposition 6.5 (applied to $j$ instead of $i$) shows that the element $X_j$ of $R$ is regular. Hence, Proposition 2.5 (applied to $R_i$, $R$ and $X_j$ instead of $A$, $B$ and $a$) shows that $X_j$ is a regular element of $R_i$ (since $R_i$ is a subring of $R$, and since $X_j$ is an element of $R_i$). Hence, Proposition 6.2 (applied to $R_i$ and $X_j$ instead of $A$ and $a$) yields that the element $X - X_j$ of $R_i[[X]]$ is regular. Hence, Proposition 2.4 (applied to $R_i[[X]]$, $R$, $\rho_i$ and $X - X_j$ instead of $A$, $B$, $f$ and $a$) shows that $\rho_i\left(X - X_j\right)$ is a regular element of $R$ (since $\rho_i : R_i[[X]] \to R$ is a ring isomorphism). In other words, $X_i - X_j$ is a regular element of $R$ (since $\rho_i\left(X - X_j\right) = X_i - X_j$). This proves Proposition 6.6. □

We can now state an analogue of Corollary 4.4 (actually, a generalization):

**Corollary 6.7.** The polynomial $\prod_{1 \leq i < j \leq n} \left(X_i - X_j\right)$ is a regular element of $R$.

*Proof of Corollary 6.7.* Analogous to the proof of Corollary 4.4 (but using Proposition 6.6 instead of Proposition 4.3 **(b)**). □

## 6.4. Analogues of other properties of polynomials

Analogues of Theorem 1.3, Theorem 1.2 and Corollary 5.2 for power series can also be stated:

**Theorem 6.8.** Let $G$ be a subset of the set $\left\{(i,j) \in \{1,2,\ldots,n\}^2 \mid i < j\right\}$.

Let $f \in R$ be a formal power series in the $n$ indeterminates $X_1, X_2, \ldots, X_n$ over $A$. Assume that $f$ is divisible by $X_i - X_j$ for every $(i,j) \in G$. Then, $f$ is divisible by $\prod\limits_{(i,j)\in G} \left(X_i - X_j\right)$.

**Theorem 6.9.** Let $f \in R$ be a formal power series in the $n$ indeterminates $X_1, X_2, \ldots, X_n$ over $A$. Assume that $f$ is divisible by $X_i - X_j$ for every $(i,j) \in \{1,2,\ldots,n\}^2$ satisfying $i < j$. Then, $f$ is divisible by $\prod\limits_{1\le i<j\le n} \left(X_i - X_j\right)$.

(Here, the symbol "$\prod\limits_{1\le i<j\le n}$" is to be understood as in Theorem 1.2.)

**Corollary 6.10.** Let $G$ be a subset of the set $\left\{(i,j) \in \{1,2,\ldots,n\}^2 \mid i < j\right\}$. Then,

$$\bigcap_{(i,j)\in G} \left(\left(X_i - X_j\right) R\right) = \left(\prod_{(i,j)\in G} \left(X_i - X_j\right)\right) R.$$

Theorem 6.8, Theorem 6.9 and Corollary 6.10 are analogues of Theorem 1.3, Theorem 1.2 and Corollary 5.2, respectively. I am not sure whether they can be proven in a similar manner to the proofs given above. However, they can be derived from their polynomial counterparts using a fairly straightforward homogeneity argument (indeed, the power series $X_i - X_j$ are actually homogeneous polynomials, and therefore so are their products; hence, the divisibility of a power series $f$ by a product of such power series can be decided by separately studying each homogeneous component of $f$). We shall give these proofs in Subsection 6.5.

Let us next discuss some properties of the polynomial ring $A[X_1, X_2, \ldots, X_n]$ that do **not** directly carry over to the ring $R = A[[X_1, X_2, \ldots, X_n]]$ of formal power series.

**Question 6.11.** What conditions would make an analogue of Corollary 3.21 for power series true? If $A$ is a ring, and $a$ and $b$ are two elements of $A$, then what should be required on $A$, $a$ and $b$ in order to guarantee that

$$bA[[X]] \cap (X - a) A[[X]] = b(X - a) A[[X]] \tag{27}$$

? It can be shown that requiring $a$ to be nilpotent suffices. However, requiring that $a$ be regular does **not** suffice, as Example 6.12 below shows.

**Example 6.12.** Let $K$ be a field. Let $A$ be the commutative $K$-algebra with generators

$$a,\ \underbrace{x_{-1}, x_0, x_1, \ldots}_{\text{countably many}},\ b,\ \underbrace{z_{-1}, z_0, z_1, \ldots}_{\text{countably many}} \tag{28}$$

and relations

$$x_{-1} = 0 \qquad \text{and} \qquad x_i - a x_{i+1} = b z_i \text{ for all } i \geq -1.$$

Then, the element $a \in A$ is regular, but we have

$$bA\left[[X]\right] \cap (X - a)\, A\left[[X]\right] \neq b\,(X - a)\, A\left[[X]\right]. \tag{29}$$

*Proof of Example 6.12 (sketched). 1st step:* Let $\mathbf{A}$ be the polynomial algebra over $K$ in the indeterminates

$$\mathbf{a},\ \underbrace{\mathbf{x}_{-1}, \mathbf{x}_0, \mathbf{x}_1, \ldots}_{\text{countably many}},\ \mathbf{b},\ \underbrace{\mathbf{z}_{-1}, \mathbf{z}_0, \mathbf{z}_1, \ldots}_{\text{countably many}}. \tag{30}$$

Then, there is a unique ring homomorphism $\pi : \mathbf{A} \to A$ sending each of the indeterminates listed in (30) to the corresponding generator in (28). This ring homomorphism $\pi$ is surjective, and its kernel is the ideal $\mathbf{I}$ of $\mathbf{A}$ generated by $\mathbf{x}_{-1}$ and $\mathbf{x}_i - \mathbf{a}\mathbf{x}_{i+1} - \mathbf{b}\mathbf{z}_i$ for all $i \geq -1$.

*2nd step:* We shall now prove that the element $a \in A$ is regular.

Indeed, let $p \in A$ be such that $ap = 0$. We must prove that $p = 0$.

Since $\pi$ is surjective, we can write $p$ in the form $p = \pi(\mathbf{p})$ for some $\mathbf{p} \in \mathbf{A}$. Consider this $\mathbf{p}$.

From $a = \pi(\mathbf{a})$ and $p = \pi(\mathbf{p})$, we obtain $ap = \pi(\mathbf{a})\,\pi(\mathbf{p}) = \pi(\mathbf{ap})$, so that $\pi(\mathbf{ap}) = ap = 0$ and therefore $\mathbf{ap} \in \mathbf{I}$. In other words, $\mathbf{ap}$ is an $\mathbf{A}$-linear combination of $\mathbf{x}_{-1}$ and $\mathbf{x}_i - \mathbf{a}\mathbf{x}_{i+1} - \mathbf{b}\mathbf{z}_i$ for all $i \geq -1$. In other words, there exists some $s \in \mathbb{N}$, some $\mathbf{u} \in \mathbf{A}$ and some $\mathbf{v}_{-1}, \mathbf{v}_0, \ldots, \mathbf{v}_{s-1} \in \mathbf{A}$ such that

$$\mathbf{ap} = \mathbf{u} \cdot \mathbf{x}_{-1} + \sum_{i=-1}^{s-1} \mathbf{v}_i \cdot \left(\mathbf{x}_i - \mathbf{a}\mathbf{x}_{i+1} - \mathbf{b}\mathbf{z}_i\right). \tag{31}$$

Consider these $s$, $\mathbf{u}$ and $\mathbf{v}_{-1}, \mathbf{v}_0, \ldots, \mathbf{v}_{s-1}$. We WLOG assume that $s$ is large enough that only the indeterminates

$$\mathbf{a},\ \mathbf{x}_{-1}, \mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_s,\ \mathbf{b},\ \mathbf{z}_{-1}, \mathbf{z}_0, \mathbf{z}_1, \ldots, \mathbf{z}_s \tag{32}$$

appear in the polynomials $\mathbf{p}, \mathbf{u}, \mathbf{v}_{-1}, \mathbf{v}_0, \ldots, \mathbf{v}_{s-1}$ (since we can always increase $s$).

Let $\mathbf{A}_s$ be the polynomial algebra over $K$ in the indeterminates listed in (32). Clearly, $\mathbf{A}_s$ is a subalgebra of $\mathbf{A}$. Furthermore, all of the polynomials $\mathbf{p}, \mathbf{u}, \mathbf{v}_{-1}, \mathbf{v}_0, \ldots, \mathbf{v}_{s-1}$ as well as $\mathbf{a}$, $\mathbf{x}_{-1}$ and the differences $\mathbf{x}_i - \mathbf{a}\mathbf{x}_{i+1} - \mathbf{b}\mathbf{z}_i$ for all $i \in \{-1, 0, 1, \ldots, s-1\}$ belong to $\mathbf{A}_s$. Hence, we can regard (31) as an equality inside $\mathbf{A}_s$.

Let $\mathbf{B}_s$ be the polynomial algebra over $K$ in the indeterminates

$$\mathbf{a},\ \widetilde{\mathbf{x}}_s,\ \mathbf{b},\ \mathbf{z}_{-1}, \mathbf{z}_0, \mathbf{z}_1, \ldots, \mathbf{z}_s. \tag{33}$$

(You are reading right: The indeterminate $\widetilde{\mathbf{x}}_s$ is not $\mathbf{x}_s$, although it is closely related.) Inside $\mathbf{B}_s$, define new elements $\widetilde{\mathbf{x}}_{s-1}, \widetilde{\mathbf{x}}_{s-2}, \ldots, \widetilde{\mathbf{x}}_{-1}$ recursively by setting

$$\widetilde{\mathbf{x}}_{s-i} = \mathbf{a}\widetilde{\mathbf{x}}_{s-(i-1)} + \mathbf{b}\mathbf{z}_{s-i} \qquad \text{for each } i \in \{1, 2, \ldots, s+1\}. \tag{34}$$

Then, it is easy to prove (by induction over $i$) that

$$\widetilde{\mathbf{x}}_{s-i} = \mathbf{a}^i \widetilde{\mathbf{x}}_s + \sum_{k=1}^{i} \mathbf{a}^{i-k} \mathbf{b}\mathbf{z}_{s-k} \qquad \text{for each } i \in \{0, 1, \ldots, s+1\}.$$

Applying this to $i = s+1$, we obtain

$$\widetilde{\mathbf{x}}_{-1} = \mathbf{a}^{s+1} \widetilde{\mathbf{x}}_s + \sum_{k=1}^{s+1} \mathbf{a}^{s+1-k} \mathbf{b}\mathbf{z}_{s-k}. \tag{35}$$

For each $i \in \{-1, 0, \ldots, s-1\}$, we have

$$\widetilde{\mathbf{x}}_i = \mathbf{a}\widetilde{\mathbf{x}}_{i+1} + \mathbf{b}\mathbf{z}_i \tag{36}$$

(by (34), applied to $s-i$ instead of $i$).

We can regard $\widetilde{\mathbf{x}}_{-1} \in \mathbf{B}_s$ as a polynomial in the indeterminate $\mathbf{a}$ over the unique factorization domain $K\left[\widetilde{\mathbf{x}}_s,\ \mathbf{b},\ \mathbf{z}_{-1}, \mathbf{z}_0, \mathbf{z}_1, \ldots, \mathbf{z}_s\right]$. Then, (35) shows that this polynomial $\widetilde{\mathbf{x}}_{-1}$ has leading coefficient $\widetilde{\mathbf{x}}_s$, and that the prime $\mathbf{b}$ of the unique factorization domain $K\left[\widetilde{\mathbf{x}}_s,\ \mathbf{b},\ \mathbf{z}_{-1}, \mathbf{z}_0, \mathbf{z}_1, \ldots, \mathbf{z}_s\right]$ divides all coefficients of $\widetilde{\mathbf{x}}_{-1}$ except for its leading coefficient (which is $\widetilde{\mathbf{x}}_s$), and that $\mathbf{b}^2$ does not divide the constant term of $\widetilde{\mathbf{x}}_{-1}$ (because the constant term of $\widetilde{\mathbf{x}}_{-1}$ is $\mathbf{b}\mathbf{z}_{-1}$). Therefore, Eisenstein's Irreducibility Criterion (see, e.g., [Knapp2016, Corollary 8.22]) shows that this polynomial $\widetilde{\mathbf{x}}_{-1}$ is irreducible over the fraction field of $K\left[\widetilde{\mathbf{x}}_s,\ \mathbf{b},\ \mathbf{z}_{-1}, \mathbf{z}_0, \mathbf{z}_1, \ldots, \mathbf{z}_s\right]$. Moreover, the coefficients of this polynomial $\widetilde{\mathbf{x}}_{-1}$ have no common divisor except for units[21]; therefore, $\widetilde{\mathbf{x}}_{-1}$ is irreducible over the ring $K\left[\widetilde{\mathbf{x}}_s,\ \mathbf{b},\ \mathbf{z}_{-1}, \mathbf{z}_0, \mathbf{z}_1, \ldots, \mathbf{z}_s\right]$ as well. In other words, $\widetilde{\mathbf{x}}_{-1}$ is a prime element of the unique factorization domain $\mathbf{B}_s$.

The substitution

$$\mathbf{a} \mapsto \mathbf{a}, \qquad \mathbf{x}_i \mapsto \widetilde{\mathbf{x}}_i, \qquad \mathbf{b} \mapsto \mathbf{b}, \qquad \mathbf{z}_i \mapsto \mathbf{z}_i$$

defines a $K$-algebra homomorphism $\alpha : \mathbf{A}_s \to \mathbf{B}_s$. Let $\widetilde{\mathbf{p}}$, $\widetilde{\mathbf{u}}$ and $\widetilde{\mathbf{v}}_i$ denote the images of $\mathbf{p}$, $\mathbf{u}$ and $\mathbf{v}_i$ under this substitution. If we apply this substitution to both sides of the equality (31), then we obtain

$$\mathbf{a}\widetilde{\mathbf{p}} = \widetilde{\mathbf{u}} \cdot \widetilde{\mathbf{x}}_{-1} + \sum_{i=-1}^{s-1} \widetilde{\mathbf{v}}_i \cdot \underbrace{\left(\widetilde{\mathbf{x}}_i - \mathbf{a}\widetilde{\mathbf{x}}_{i+1} - \mathbf{b}\mathbf{z}_i\right)}_{\substack{=0 \\ \text{(by (36))}}} = \widetilde{\mathbf{u}} \cdot \widetilde{\mathbf{x}}_{-1}.$$

[21] Indeed, this is clear from observing that the leading coefficient is $\widetilde{\mathbf{x}}_s$, whereas the constant term is $\mathbf{b}\mathbf{z}_{-1}$.

Hence, $\mathbf{a}\widetilde{\mathbf{p}}$ is divisible by $\widetilde{\mathbf{x}}_{-1}$ in $\mathbf{B}_s$. Since $\widetilde{\mathbf{x}}_{-1}$ is a prime element of the unique factorization domain $\mathbf{B}_s$, we thus conclude that either $\mathbf{a}$ or $\widetilde{\mathbf{p}}$ is divisible by $\widetilde{\mathbf{x}}_{-1}$ in $\mathbf{B}_s$. But since $\mathbf{a}$ is not divisible by $\widetilde{\mathbf{x}}_{-1}$ in $\mathbf{B}_s$ (indeed, the constant term of $\widetilde{\mathbf{x}}_{-1}$, when regarded as a polynomial in $\mathbf{a}$, is $\mathbf{b}\mathbf{z}_{-1}$, which has no common divisors with $\mathbf{a}$ except for units), this shows that $\widetilde{\mathbf{p}}$ is divisible by $\widetilde{\mathbf{x}}_{-1}$ in $\mathbf{B}_s$. In other words, $\widetilde{\mathbf{p}} = \widetilde{\mathbf{x}}_{-1}\widetilde{\mathbf{q}}$ for some $\widetilde{\mathbf{q}} \in \mathbf{B}_s$. Consider this $\widetilde{\mathbf{q}}$.

Let $\mathbf{J}_s$ be the ideal of $\mathbf{A}_s$ generated by the polynomials $\mathbf{x}_i - \mathbf{a}\mathbf{x}_{i+1} - \mathbf{b}\mathbf{z}_i$ with $i \in \{-1, 0, 1, \ldots, s-1\}$. The homomorphism $\alpha : \mathbf{A}_s \to \mathbf{B}_s$ sends the generators of $\mathbf{J}_s$ to 0; therefore, it factors through $\mathbf{A}_s/\mathbf{J}_s$, yielding a $K$-algebra homomorphism $\alpha' : \mathbf{A}_s/\mathbf{J}_s \to \mathbf{B}_s$. This homomorphism $\alpha'$ is invertible[22], and therefore injective. In other words, $\operatorname{Ker}\alpha = \mathbf{J}_s$. Also, $\alpha$ is surjective (since $\alpha'$ is invertible), and thus there exists some $\mathbf{q} \in \mathbf{A}_s$ such that $\widetilde{\mathbf{q}} = \alpha(\mathbf{q})$. Consider this $\mathbf{q}$.

Now, $\alpha(\mathbf{p}) = \widetilde{\mathbf{p}} = \underbrace{\widetilde{\mathbf{x}}_{-1}}_{=\alpha(\mathbf{x}_{-1})}\underbrace{\widetilde{\mathbf{q}}}_{=\alpha(\mathbf{q})} = \alpha(\mathbf{x}_{-1})\alpha(\mathbf{q}) = \alpha(\mathbf{x}_{-1}\mathbf{q})$, so that $\mathbf{p} - \mathbf{x}_{-1}\mathbf{q} \in \operatorname{Ker}\alpha = \mathbf{J}_s$.

But the homomorphism $\pi$ sends $\mathbf{J}_s$ to 0. Thus, from $\mathbf{p} - \mathbf{x}_{-1}\mathbf{q} \in \mathbf{J}_s$, we obtain $\pi(\mathbf{p} - \mathbf{x}_{-1}\mathbf{q}) = 0$. In other words, $\pi(\mathbf{p}) = \pi(\mathbf{x}_{-1}\mathbf{q}) = \underbrace{\pi(\mathbf{x}_{-1})}_{=0}\pi(\mathbf{q}) = 0$. Thus, $p = \pi(\mathbf{p}) = 0$. This completes our 2nd step.

*3rd step:* It remains to prove (29).

Define a power series $x \in A[[X]]$ by $x = \sum_{i\in\mathbb{N}} x_i X^i$. Then, it is easy to see that

$$(X-a)\,x = \sum_{i\in\mathbb{N}} \underbrace{(x_{i-1} - ax_i)}_{\substack{=bz_{i-1} \\ \text{(by one of the} \\ \text{defining relations of } A)}} X^i = \sum_{i\in\mathbb{N}} bz_{i-1}X^i = b\sum_{i\in\mathbb{N}} z_{i-1}X^i \in bA[[X]].$$

Combining this with $(X-a)\,x \in (X-a)\,A[[X]]$ (which is obvious), we obtain

$$(X-a)\,x \in bA[[X]] \cap (X-a)\,A[[X]].$$

If we now can prove that

$$(X-a)\,x \notin b\,(X-a)\,A[[X]], \tag{37}$$

[22] *Proof.* The substitution

$$\mathbf{a} \mapsto \mathbf{a}, \qquad \widetilde{\mathbf{x}}_s \mapsto \mathbf{x}_s, \qquad \mathbf{b} \mapsto \mathbf{b}, \qquad \mathbf{z}_i \mapsto \mathbf{z}_i$$

defines a $K$-algebra homomorphism $\beta : \mathbf{B}_s \to \mathbf{A}_s$. Composing this $K$-algebra homomorphism $\beta : \mathbf{B}_s \to \mathbf{A}_s$ with the canonical projection $\mathbf{A}_s \to \mathbf{A}_s/\mathbf{J}_s$ produces a $K$-algebra homomorphism $\beta' : \mathbf{B}_s \to \mathbf{A}_s/\mathbf{J}_s$. Using (34), we can show (by induction over $i$) that this homomorphism $\beta'$ sends $\widetilde{\mathbf{x}}_{s-i}$ to (the remainder class of) $\mathbf{x}_{s-i}$ for each $i \in \{0, 1, \ldots, s+1\}$. In other words, $\beta$ sends $\widetilde{\mathbf{x}}_i$ to (the remainder class of) $\mathbf{x}_i$ for each $i \in \{-1, 0, 1, \ldots, s-1\}$. Now, the two $K$-algebra homomorphisms $\alpha' \circ \beta'$ and $\beta' \circ \alpha'$ both preserve the generators listed in (33) and (32), respectively (or, rather, their remainder classes), and therefore are the identity maps. In other words, the homomorphisms $\alpha'$ and $\beta'$ are mutually inverse. Hence, $\alpha'$ is invertible. Qed.

then (29) will follow, and thus we will be done. Hence, it remains to prove (37).

*4rd step:* Let us prove (37). Indeed, assume the contrary. Thus,

$$(X-a)\,x \in b\,(X-a)\,A\,[[X]]\,.$$

In other words,

$$(X-a)\,x = b\,(X-a)\,y \tag{38}$$

for some $y \in A\,[[X]]$. Consider this $y$.

Let $y_0$ be the constant term of the power series $y$. Recall that $x_0$ is the constant term of the power series $x$. Comparing the constant terms on both sides of (38), we thus obtain $-ax_0 = -bay_0$. Thus, $ax_0 = bay_0$. Since the element $a$ of $A$ is regular, we can cancel $a$ from this equality, and therefore obtain $x_0 = by_0$.

Now, let $A'$, $a'$ and $x_i'$ be what was denoted by $A$, $a$ and $x_i$ in Example 6.3. Then, $x_0' \neq 0$. (Indeed, this is exactly the statement "$x_0 \neq 0$" that we proved in our proof of Example 6.3.)

Let $J$ be the ideal of $A$ generated by $b$, $\underbrace{z_{-1}, z_0, z_1, \ldots}_{\text{countably many}}$. Then, there is a canonical isomorphism $A/J \to A'$ sending the projections of $a$, $\underbrace{x_{-1}, x_0, x_1, \ldots}_{\text{countably many}}$ onto $A/J$ to the generators $a'$, $\underbrace{x'_{-1}, x'_0, x'_1, \ldots}_{\text{countably many}}$ of $A'$ (indeed, just compare the definitions of $A$ and $A'$, and observe that the former becomes the latter if $b$, $\underbrace{z_{-1}, z_0, z_1, \ldots}_{\text{countably many}}$ are set to 0).

The canonical projection $A \to A/J$ sends $x_0$ to $x_0'$ and sends $b$ to 0. Hence, projecting both sides of the equality $x_0 = by_0$ onto $A/J$, we obtain $x_0' = 0y_0'$, where $y_0'$ is the image of $y_0$. Therefore, $x_0' = 0y_0' = 0$, contradicting $x_0' \neq 0$. This contradiction completes our proof of (37), and this in turn finishes our proof of Example 6.12. □

In Section 10, we shall see some sufficient criteria for analogues of Corollary 3.21 to hold in $A\,[[X]]$.

## 6.5. Appendix: The graded component trick

In this subsection, we shall prove Theorem 6.8, Theorem 6.9 and Corollary 6.10. Their proofs will all rely on the notion of homogeneous components. Let us recall how this notion is defined and introduce a notation for it:

**Definition 6.13.** Let $f \in R$ be a formal power series. Let $d \in \mathbb{Z}$. Then, $f_{\deg=d}$ shall mean the $d$-th homogeneous component of $f$; this is defined as follows: Write the formal power series $f$ in the form $f = \sum_{(i_1,i_2,\ldots,i_n)\in\mathbb{N}^n} a_{(i_1,i_2,\ldots,i_n)} X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}$, where

$a_{(i_1,i_2,\ldots,i_n)} \in A$ are its coefficients. Then, the $d$-th homogeneous component of $f$ is defined to be the finite sum

$$\sum_{\substack{(i_1,i_2,\ldots,i_n)\in\mathbb{N}^n; \\ i_1+i_2+\cdots+i_n=d}} a_{(i_1,i_2,\ldots,i_n)} X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}.$$

Thus,

$$f_{\deg=d} = \sum_{\substack{(i_1,i_2,\ldots,i_n)\in\mathbb{N}^n; \\ i_1+i_2+\cdots+i_n=d}} a_{(i_1,i_2,\ldots,i_n)} X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}. \tag{39}$$

Hence,

$$f_{\deg=d} \in A\left[X_1, X_2, \ldots, X_n\right] \tag{40}$$

(since the right hand side of (39) is a **finite** sum of monomials), and

$$f_{\deg=d} \text{ is a homogeneous polynomial of degree } d \tag{41}$$

(because all the monomials $X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}$ appearing on the right hand side of (39) are of degree $d$).

If $f \in R$ and if $d$ is a negative integer, then $f_{\deg=d} = 0$ (because the sum on the right hand side of (39) is empty in this case). Furthermore, it is clear that every formal power series $f \in R$ satisfies

$$f = \sum_{d\in\mathbb{N}} f_{\deg=d} = \sum_{d\in\mathbb{Z}} f_{\deg=d}. \tag{42}$$

Note that the sums $\sum_{d\in\mathbb{Z}} f_{\deg=d}$ and $\sum_{d\in\mathbb{N}} f_{\deg=d}$ in this equality differ only in the presence (or absence) of the addends $f_{\deg=d}$ for negative integers $d$; but all these addends are 0. Thus, the difference is insubstantial.

The polynomial ring $A\left[X_1, X_2, \ldots, X_n\right]$ is a graded ring (since every polynomial $f \in A\left[X_1, X_2, \ldots, X_n\right]$ is a **finite** sum of homogeneous polynomials), unlike the ring $R = A\left[\left[X_1, X_2, \ldots, X_n\right]\right]$ of formal power series. However, $R$, too, has the following property:

**Lemma 6.14.** Let $(p_d)_{d\in\mathbb{Z}} \in R^{\mathbb{Z}}$ be a family of formal power series. Assume that for each $d \in \mathbb{Z}$,

$$\text{the power series } p_d \text{ is a homogeneous polynomial of degree } d. \tag{43}$$

Then:

**(a)** The infinite sum $\sum_{d\in\mathbb{Z}} p_d$ is well-defined (i.e., it converges with respect to the topology on $R$).

**(b)** We have

$$\left(\sum_{d\in\mathbb{Z}} p_d\right)_{\deg=e} = p_e \qquad \text{for all } e \in \mathbb{Z}.$$

Using Lemma 6.14, we can show another basic property of homogeneous components:

**Lemma 6.15.** Let $c \in \mathbb{Z}$. Let $p \in A[X_1, X_2, \ldots, X_n]$ be a homogeneous polynomial of degree $c$. Let $g \in R$ be any formal power series. Then,

$$(pg)_{\deg=e} = p \cdot g_{\deg=e-c} \qquad \text{for all } e \in \mathbb{Z}.$$

*Proof of Lemma 6.15.* Applying (42) to $f = g$, we obtain

$$g = \sum_{d \in \mathbb{Z}} g_{\deg=d} = \sum_{d \in \mathbb{Z}} g_{\deg=d-c}$$

(here, we have substituted $d - c$ for $d$ in the sum). Hence,

$$p \underbrace{g}_{= \sum_{d \in \mathbb{Z}} g_{\deg=d-c}} = p \cdot \sum_{d \in \mathbb{Z}} g_{\deg=d-c} = \sum_{d \in \mathbb{Z}} p \cdot g_{\deg=d-c}. \tag{44}$$

Now, if $d \in \mathbb{Z}$ is arbitrary, then $p \cdot g_{\deg=d-c}$ is a homogeneous polynomial of degree $d$ [23].

Hence, Lemma 6.14 **(a)** (applied to $(p_d)_{d \in \mathbb{Z}} = \left(p \cdot g_{\deg=d-c}\right)_{d \in \mathbb{Z}}$) yields that the infinite sum $\sum_{d \in \mathbb{Z}} p \cdot g_{\deg=d-c}$ is well-defined. Moreover, Lemma 6.14 **(b)** (applied to $(p_d)_{d \in \mathbb{Z}} = \left(p \cdot g_{\deg=d-c}\right)_{d \in \mathbb{Z}}$) yields that

$$\left( \sum_{d \in \mathbb{Z}} p \cdot g_{\deg=d-c} \right)_{\deg=e} = p \cdot g_{\deg=e-c} \qquad \text{for all } e \in \mathbb{Z}.$$

But (44) yields $pg = \sum_{d \in \mathbb{Z}} p \cdot g_{\deg=d-c}$. Hence,

$$(pg)_{\deg=e} = \left( \sum_{d \in \mathbb{Z}} p \cdot g_{\deg=d-c} \right)_{\deg=e} = p \cdot g_{\deg=e-c} \qquad \text{for all } e \in \mathbb{Z}.$$

This proves Lemma 6.15. □

[23] *Proof.* Let $d \in \mathbb{Z}$ be arbitrary. Then, (40) (applied to $g$ and $d - c$ instead of $f$ and $d$) shows that $g_{\deg=d-c} \in A[X_1, X_2, \ldots, X_n]$. Also, (41) (applied to $g$ and $d - c$ instead of $f$ and $d$) shows that $g_{\deg=d-c}$ is a homogeneous polynomial of degree $d - c$. On the other hand, $p$ is a homogeneous polynomial in $A[X_1, X_2, \ldots, X_n]$ of degree $c$ (since $p \in A[X_1, X_2, \ldots, X_n]$).

But $A[X_1, X_2, \ldots, X_n]$ is a graded ring. Hence, the product of two homogeneous elements of $A[X_1, X_2, \ldots, X_n]$ is again homogeneous, and its degree is the sum of the degrees of the two factors. Applying this to $p$ and $g_{\deg=d-c}$, we conclude that the product $p \cdot g_{\deg=d-c}$ is a homogeneous polynomial of degree $c + (d - c)$ (since $p$ is a homogeneous polynomial in $A[X_1, X_2, \ldots, X_n]$ of degree $c$, and since $g_{\deg=d-c}$ is a homogeneous polynomial in $A[X_1, X_2, \ldots, X_n]$ of degree $d - c$). In other words, $p \cdot g_{\deg=d-c}$ is a homogeneous polynomial of degree $d$ (since $c + (d - c) = d$). Qed.

Using Lemma 6.15, we can now prove the following fact, which helps reduce divisibilities in $R$ to divisibilities of polynomials:

**Lemma 6.16.** Let $p \in A[X_1, X_2, \ldots, X_n]$ be a homogeneous polynomial. Let $f \in R$ be any formal power series. Assume that

$$p \mid f_{\deg=e} \text{ (in the ring } R) \qquad \text{for each } e \in \mathbb{Z}. \tag{45}$$

Then, $p \mid f$ in the ring $R$.

*Proof of Lemma 6.16.* The polynomial $p$ is homogeneous. In other words, there exists a $c \in \mathbb{Z}$ such that $p$ is homogeneous of degree $c$. Consider this $c$.

Let $e \in \mathbb{Z}$. Then, (45) shows that $p \mid f_{\deg=e}$ (in the ring $R$). In other words, there exists an element $g_e \in R$ such that $f_{\deg=e} = pg_e$. Consider this $g_e$.

At this point it would be tempting to finish the proof by saying that

$$f = \sum_{e\in\mathbb{Z}} \underbrace{f_{\deg=e}}_{=pg_e} = \sum_{e\in\mathbb{Z}} pg_e = p \sum_{e\in\mathbb{Z}} g_e.$$

However, this is not entirely correct, since the sum $\sum_{e\in\mathbb{Z}} g_e$ might not be well-defined (it is an infinite sum, and nothing guarantees that it converges with respect to the topology on $R$). Thus, we need to be somewhat more careful.

We first observe an obvious fact: If $u \in A[X_1, X_2, \ldots, X_n]$ is a homogeneous polynomial of degree $e$, then

$$u_{\deg=e} = u \tag{46}$$

(since $u_{\deg=e}$ is the $e$-th homogeneous component of $u$, but $u$ is already homogeneous of degree $e$).

Applying (40) to $d = e$, we see that $f_{\deg=e} \in A[X_1, X_2, \ldots, X_n]$. Applying (41) to $d = e$, we see that $f_{\deg=e}$ is a homogeneous polynomial of degree $e$. Hence, (46) (applied to $u = f_{\deg=e}$) yields $\left(f_{\deg=e}\right)_{\deg=e} = f_{\deg=e}$. Hence,

$$f_{\deg=e} = \left(\underbrace{f_{\deg=e}}_{=pg_e}\right)_{\deg=e} = (pg_e)_{\deg=e} = p \cdot (g_e)_{\deg=e-c} \tag{47}$$

(by Lemma 6.15, applied to $g_e$ instead of $g$). Note that $(g_e)_{\deg=e-c}$ is a homogeneous polynomial of degree $e - c$ (by (41), applied to $g_e$ and $e - c$ instead of $f$ and $d$).

Now, forget that we fixed $e$. Thus, for each $e \in \mathbb{Z}$, we have constructed a $g_e \in R$ such that (47) holds, and such that

$$(g_e)_{\deg=e-c} \text{ is a homogeneous polynomial of degree } e - c. \tag{48}$$

Now, for each $d \in \mathbb{Z}$, the power series $(g_{d+c})_{\deg=d}$ is a homogeneous polynomial of degree $d$ [24]. Hence, Lemma 6.14 **(a)** (applied to $(p_d)_{d\in\mathbb{Z}} = \left((g_{d+c})_{\deg=d}\right)_{d\in\mathbb{Z}}$) shows that the infinite sum $\sum_{d\in\mathbb{Z}} (g_{d+c})_{\deg=d}$ is well-defined. Hence,

$$\begin{aligned} p \cdot \sum_{d\in\mathbb{Z}} (g_{d+c})_{\deg=d} &= \sum_{d\in\mathbb{Z}} p \cdot (g_{d+c})_{\deg=d} = \sum_{e\in\mathbb{Z}} p \cdot \underbrace{\left(g_{(e-c)+c}\right)_{\deg=e-c}}_{\substack{=(g_e)_{\deg=e-c} \\ \text{(since } (e-c)+c=e\text{)}}} \\ &\qquad \left(\text{here, we have substituted } e-c \text{ for } d \text{ in the sum}\right) \\ &= \sum_{e\in\mathbb{Z}} \underbrace{p \cdot (g_e)_{\deg=e-c}}_{\substack{=f_{\deg=e} \\ \text{(by (47))}}} = \sum_{e\in\mathbb{Z}} f_{\deg=e} = \sum_{d\in\mathbb{Z}} f_{\deg=d} \\ &\qquad \left(\text{here, we have renamed the summation index } e \text{ as } d\right) \\ &= f \qquad \left(\text{by (42)}\right). \end{aligned}$$

Hence, $f = p \cdot \sum_{d\in\mathbb{Z}} (g_{d+c})_{\deg=d}$. Thus, $p \mid f$ in the ring $R$. This proves Lemma 6.16. □

We can now prove Theorem 6.8:

*Proof of Theorem 6.8.* We have assumed that

$$f \text{ is divisible by } X_i - X_j \text{ for every } (i,j) \in G. \tag{49}$$

The product $\prod_{(i,j)\in G} \left(X_i - X_j\right)$ is clearly a homogeneous polynomial of degree $|G|$.

Now, let $e \in \mathbb{Z}$. Then, (40) (applied to $d = e$) shows that $f_{\deg=e} \in A\left[X_1, X_2, \ldots, X_n\right]$.

Let $(i,j) \in G$. Then, $f$ is divisible by $X_i - X_j$ (by (49)). In other words, there exists a formal power series $g \in R$ such that $f = \left(X_i - X_j\right) \cdot g$. Consider this $g$. Note that (40) (applied to $g$ and $e-1$ instead of $f$ and $d$) shows that $g_{\deg=e-1} \in A\left[X_1, X_2, \ldots, X_n\right]$.

Clearly, $X_i - X_j$ is a homogeneous polynomial of degree 1, and thus belongs to $A\left[X_1, X_2, \ldots, X_n\right]$. Hence, Lemma 6.15 (applied to $c = 1$ and $p = X_i - X_j$) yields

$$\left(\left(X_i - X_j\right) \cdot g\right)_{\deg=e} = \left(X_i - X_j\right) \cdot g_{\deg=e-1}.$$

In view of $f = \left(X_i - X_j\right) \cdot g$, this rewrites as

$$f_{\deg=e} = \left(X_i - X_j\right) \cdot g_{\deg=e-1}.$$

[24] *Proof.* Let $d \in \mathbb{Z}$. Then, (48) (applied to $e = d + c$) shows that $(g_{d+c})_{\deg=(d+c)-c}$ is a homogeneous polynomial of degree $(d+c)-c$. In other words, $(g_{d+c})_{\deg=d}$ is a homogeneous polynomial of degree $d$ (since $(d+c)-c = d$). Qed.

Hence, $f_{\deg=e}$ is divisible by $X_i - X_j$ in the ring $A[X_1, X_2, \ldots, X_n]$ (since $g_{\deg=e-1} \in A[X_1, X_2, \ldots, X_n]$).

Now, forget that we fixed $(i, j)$. Thus, we have shown that $f_{\deg=e}$ is divisible by $X_i - X_j$ in the ring $A[X_1, X_2, \ldots, X_n]$ for every $(i, j) \in G$. Hence, Theorem 1.3 (applied to $f_{\deg=e}$ instead of $f$) yields that $f_{\deg=e}$ is divisible by $\prod_{(i,j)\in G} (X_i - X_j)$ in the ring $A[X_1, X_2, \ldots, X_n]$. In other words, $\prod_{(i,j)\in G} (X_i - X_j) \mid f_{\deg=e}$ in the ring $A[X_1, X_2, \ldots, X_n]$. Therefore, $\prod_{(i,j)\in G} (X_i - X_j) \mid f_{\deg=e}$ in the ring $R$ (since $A[X_1, X_2, \ldots, X_n]$ is a subring of $R$).

Now, forget that we fixed $e$. We thus have shown that $\prod_{(i,j)\in G} (X_i - X_j) \mid f_{\deg=e}$ (in the ring $R$) for each $e \in \mathbb{Z}$. Hence, Lemma 6.16 (applied to $p = \prod_{(i,j)\in G} (X_i - X_j)$) shows that $\prod_{(i,j)\in G} (X_i - X_j) \mid f$ in the ring $R$ (since $\prod_{(i,j)\in G} (X_i - X_j)$ is a homogeneous polynomial). In other words, $f$ is divisible by $\prod_{(i,j)\in G} (X_i - X_j)$. This proves Theorem 6.8. □

*Proof of Theorem 6.9.* Theorem 6.9 follows from Theorem 6.8 if we set $G = \left\{(i, j) \in \{1, 2, \ldots, n\}^2 \mid i < j\right\}$. □

*Proof of Corollary 6.10.* It is easy to see that

$$\left(\prod_{(i,j)\in G} (X_i - X_j)\right) R \subseteq \bigcap_{(i,j)\in G} \left((X_i - X_j) R\right)$$

(since every element of $\left(\prod_{(i,j)\in G} (X_i - X_j)\right) R$ is a multiple of the product $\prod_{(i,j)\in G} (X_i - X_j)$, and therefore a multiple of each factor $X_i - X_j$ of this product). But Theorem 6.8 says that

$$\bigcap_{(i,j)\in G} \left((X_i - X_j) R\right) \subseteq \left(\prod_{(i,j)\in G} (X_i - X_j)\right) R$$

(since $\bigcap_{(i,j)\in G} \left((X_i - X_j) R\right)$ is the set of all $f \in R$ that are divisible by all $X_i - X_j$ with $(i, j) \in G$, whereas $\left(\prod_{(i,j)\in G} (X_i - X_j)\right) R$ is the set of all $f \in R$ that are divisible by $\prod_{(i,j)\in G} (X_i - X_j)$). Combining these two relations, we obtain

$$\bigcap_{(i,j)\in G} \left((X_i - X_j) R\right) = \left(\prod_{(i,j)\in G} (X_i - X_j)\right) R.$$

This proves Corollary 6.10. □

# 7. lcm-coprimality meets regularity

## 7.1. Connecting lcm-coprimality to regularity in $A/pA$

Let us take one more look at "lcm-coprimality" – i.e., relations of the form $bR \cap cR = bcR$ for two elements $b$ and $c$ of a commutative ring $R$ (as they appear, for example, in Proposition 4.6). Let us first connect such relations with regular elements:

**Proposition 7.1.** Let $A$ be a commutative ring. Let $p$ and $d$ be two elements of $A$. For each $a \in A$, let $\overline{a}$ denote the residue class of $a$ modulo the ideal $pA$; this is an element of the quotient ring $A/pA$.

**(a)** If the element $\overline{d}$ of $A/pA$ is regular, then $dA \cap pA = dpA$.

**(b)** Assume that the element $d$ of $A$ is regular. If $dA \cap pA = dpA$, then the element $\overline{d}$ of $A/pA$ is regular.

*Proof of Proposition 7.1.* **(a)** Assume that the element $\overline{d}$ of $A/pA$ is regular. We must show that $dA \cap pA = dpA$. We have

$$dpA = dpA \cap \underbrace{dp}_{=pd} A = d \underbrace{pA}_{\subseteq A} \cap p \underbrace{dA}_{\subseteq A} \subseteq dA \cap pA. \tag{50}$$

The element $\overline{d}$ of $A/pA$ is regular if and only if every $x \in A/pA$ satisfying $\overline{d}x = 0$ satisfies $x = 0$ (by the definition of "regular"). Hence,

$$\text{every } x \in A/pA \text{ satisfying } \overline{d}x = 0 \text{ satisfies } x = 0 \tag{51}$$

(since the element $\overline{d}$ of $A/pA$ is regular).

Let $y \in dA \cap pA$. Then, $y \in dA \cap pA \subseteq pA$. Thus, $\overline{y} = 0$ (since $\overline{y}$ is the residue class of $y$ modulo the ideal $pA$).

We have $y \in dA \cap pA \subseteq dA$. In other words, there exists some $z \in A$ such that $y = dz$. Consider this $z$. We have $y = dz$ and thus $\overline{y} = \overline{dz} = \overline{d} \cdot \overline{z}$. Comparing this with $\overline{y} = 0$, we obtain $\overline{d} \cdot \overline{z} = 0$. Thus, (51) (applied to $x = \overline{z}$) yields $\overline{z} = 0$. In other words, $z \in pA$ (since $\overline{z}$ is the residue class of $z$ modulo the ideal $pA$). Now, $y = d \underbrace{z}_{\in pA} \in dpA$.

Now, forget that we fixed $y$. We thus have shown that $y \in dpA$ for every $y \in dA \cap pA$. In other words, $dA \cap pA \subseteq dpA$. Combining this with (50), we obtain $dA \cap pA = dpA$. This proves Proposition 7.1 **(a)**.

**(b)** The element $d$ of $A$ is regular if and only if every $x \in A$ satisfying $dx = 0$ satisfies $x = 0$ (by the definition of "regular"). Hence,

$$\text{every } x \in A \text{ satisfying } dx = 0 \text{ satisfies } x = 0 \tag{52}$$

(since the element $d$ of $A$ is regular).

Assume that $dA \cap pA = dpA$. Let $x \in A/pA$ be such that $\overline{d}x = 0$. We shall show that $x = 0$.

We have $x \in A/pA$. In other words, $x = \overline{y}$ for some $y \in A$. Consider this $y$. We have $x = \overline{y}$ and thus $\overline{d}\underbrace{x}_{=\overline{y}} = \overline{d} \cdot \overline{y} = \overline{dy}$. Thus, $\overline{dy} = \overline{d}x = 0$. In other words, $dy \in pA$ (since $\overline{dy}$ is the residue class of $dy$ modulo the ideal $pA$). Combining $d\underbrace{y}_{\in A} \in dA$ with $dy \in pA$, we obtain $dy \in dA \cap pA = dpA$. In other words, there exists some $z \in A$ such that $dy = dpz$. Consider this $z$. We have $d(y - pz) = dy - dpz = 0$ (since $dy = dpz$). Hence, (52) (applied to $y - pz$ instead of $x$) yields $y - pz = 0$. Thus, $y = p\underbrace{z}_{\in A} \in pA$, so that $\overline{y} = 0$ (since $\overline{y}$ is the residue class of $y$ modulo the ideal $pA$). Hence, $x = \overline{y} = 0$.

Now, forget that we fixed $x$. We thus have shown that

$$\text{every } x \in A/pA \text{ satisfying } \overline{d}x = 0 \text{ satisfies } x = 0. \tag{53}$$

But the element $\overline{d}$ of $A/pA$ is regular if and only if every $x \in A/pA$ satisfying $\overline{d}x = 0$ satisfies $x = 0$ (by the definition of "regular"). Hence, the element $\overline{d}$ of $A/pA$ is regular (since every $x \in A/pA$ satisfying $\overline{d}x = 0$ satisfies $x = 0$). This proves Proposition 7.1 **(b)**. □

Using Proposition 7.1, we can show the following counterpart to Proposition 4.6:

**Proposition 7.2.** Let $R$ be a commutative ring. Let $G$ be a finite set. For every $g \in G$, let $a_g$ be a regular element of $R$. Let $p \in R$. Assume that every $g \in G$ satisfies $pR \cap a_g R = pa_g R$. Let $b = \prod_{g \in G} a_g$. Then, $pR \cap bR = pbR$.

*Proof of Proposition 7.2.* For each $a \in R$, let $\overline{a}$ denote the residue class of $a$ modulo the ideal $pR$; this is an element of the quotient ring $R/pR$. Notice that

$$\prod_{g \in G} \overline{a_g} = \overline{\prod_{g \in G} a_g} = \overline{b}$$

(since $\prod_{g \in G} a_g = b$).

We have assumed that every $g \in G$ satisfies

$$pR \cap a_g R = pa_g R. \tag{54}$$

Now, let $g \in G$. Then, $a_g$ is a regular element of $R$. Also,

$$\begin{aligned} a_g R \cap pR = pR \cap a_g R &= \underbrace{pa_g}_{=a_g p} R \qquad \text{(by (54))} \\ &= a_g pR. \end{aligned}$$

Hence, Proposition 7.1 **(b)** (applied to $A = R$ and $d = a_g$) yields that the element $\overline{a_g}$ of $R/pR$ is regular.

Now, forget that we fixed $g$. We thus have proven that the element $\overline{a_g}$ of $R/pR$ is regular for each $g \in G$. Thus, Proposition 2.3 (applied to $R/pR$ and $\overline{a_g}$ instead of $A$ and $a_g$) yields that the element $\prod\limits_{g \in G} \overline{a_g}$ of $R/pR$ is regular. In other words, the element $\overline{b}$ of $R/pR$ is regular (since $\prod\limits_{g \in G} \overline{a_g} = \overline{b}$). Hence, Proposition 7.1 **(a)** (applied to $A = R$ and $d = b$) yields that $bR \cap pR = \underbrace{bp}_{=pb} R = pbR$. Thus, $pR \cap bR = bR \cap pR = pbR$. This proves Proposition 7.2. □

## 7.2. A second proof of Proposition 5.1

Proposition 7.2 leads to an alternative proof of Proposition 5.1 (or, more precisely, allows us to simplify our proof above):

*Second proof of Proposition 5.1.* We proceed precisely as in the above proof of Proposition 5.1, until we prove (14) (in the induction step). From there, Proposition 7.2 allows us to take the following shortcut:

The element $a_g$ is a regular element of $R$ for every $g \in S \setminus \{k\}$. Moreover, every $g \in S \setminus \{k\}$ satisfies $a_k R \cap a_g R = a_k a_g R$ (by (10), applied to $k$ and $g$ instead of $g$ and $h$). Hence, Proposition 7.2 (applied to $S \setminus \{k\}$ and $a_k$ instead of $G$ and $p$) yields $a_k R \cap bR = a_k bR$. Hence, (13) becomes

$$\bigcap_{g \in S} \left(a_g R\right) = a_k R \cap bR = \underbrace{a_k b}_{\substack{= \prod\limits_{g \in S} a_g \\ \text{(by (14))}}} R = \left(\prod_{g \in S} a_g\right) R.$$

Once again, this completes the induction step, and thus Proposition 5.1 is proven again. □

**Remark 7.3.** Proposition 5.1 **cannot** be generalized by lifting the condition that the $a_g$ be regular. Here is a counterexample:

Let $K$ be a field. Let $R$ be the commutative $K$-algebra given by generators $x, y, z$ and relations $yz = zx = xy$. Notice that $R$ is a quotient of the polynomial ring $K[\mathbf{x}, \mathbf{y}, \mathbf{z}]$ by the homogeneous ideal generated by $\mathbf{yz} - \mathbf{zx}$ and $\mathbf{zx} - \mathbf{xy}$; thus, computations inside $R$ can easily be done on a computer. (A Gröbner basis of said ideal with respect to the lexicographic order is $\left(\mathbf{xy} - \mathbf{yz}, \mathbf{xz} - \mathbf{yz}, \mathbf{y}^2\mathbf{z} - \mathbf{yz}^2\right)$. A basis of the $K$-vector space $R$ is the family $\left(x^i\right)_{i \geq 0} \cup \left(yz^i\right)_{i \geq 0} \cup \left(z^i\right)_{i \geq 1}$.)

Let $G = \{1, 2, 3\}$, and set $a_1 = x$, $a_2 = y$ and $a_3 = z$. (Of course, none of the three elements $a_1, a_2, a_3$ of $R$ is regular.) It is easy to see that every two distinct elements $g$ and $h$ of $G$ satisfy $a_g R \cap a_h R = a_g a_h R$. However, it is not true

that $\bigcap\limits_{g\in G}\left(a_gR\right) = \left(\prod\limits_{g\in G} a_g\right) R$ (since the element $yz = zx = xy$ of $R$ belongs to $\bigcap\limits_{g\in G}\left(a_gR\right)$ but not to $\left(\prod\limits_{g\in G} a_g\right) R$).

Proposition 7.2 also fails if we lift the condition that the $a_g$ be regular. A counterexample can be obtained from the same setting, using $G = \{1,2\}$ and $p = a_3$ this time.

# 8. Some words on substitutions

We are next going to restate Theorem 1.2 in a different way (one which is often easier to apply in practical use cases):

**Corollary 8.1.** Let $A$ be a commutative ring. Let $n \in \mathbb{N}$. Let $f \in A\left[X_1, X_2, \ldots, X_n\right]$ be a polynomial in the $n$ indeterminates $X_1, X_2, \ldots, X_n$ over $A$. Assume that $f$ satisfies the following property:

*Property 1:* For every $(i,j) \in \{1,2,\ldots,n\}^2$ satisfying $i < j$, the result of substituting $X_j$ for $X_i$ in $f$ is 0.

Then, $f$ is divisible by $\prod\limits_{1\leq i<j\leq n}\left(X_i - X_j\right)$.

In order to derive this corollary from Theorem 1.2, we shall need the following lemma:

**Lemma 8.2.** Let $A$ be a commutative ring. Let $n \in \mathbb{N}$. Let $f \in A\left[X_1, X_2, \ldots, X_n\right]$ be a polynomial in the $n$ indeterminates $X_1, X_2, \ldots, X_n$ over $A$. Let $(i,j) \in \{1,2,\ldots,n\}^2$ be such that $i < j$.

Assume that the result of substituting $X_j$ for $X_i$ in $f$ is 0. Then, $f$ is divisible by $X_i - X_j$.

*Proof of Lemma 8.2.* Let us use the notations $R$, $R_i$ and $\rho_i$ introduced in Definition 4.2. Thus, $f \in A\left[X_1, X_2, \ldots, X_n\right] = R$.

Let $\kappa$ be the map from $A\left[X_1, X_2, \ldots, X_n\right]$ to $A\left[X_1, X_2, \ldots, X_n\right]$ which sends each $p \in A\left[X_1, X_2, \ldots, X_n\right]$ to the result of substituting $X_j$ for $X_i$ in $p$. This map $\kappa$ is an $A$-algebra homomorphism (in fact, it is an evaluation homomorphism); it satisfies

$$\kappa\left(X_u\right) = \begin{cases} X_u, & \text{if } u \neq i; \\ X_j, & \text{if } u = i \end{cases} \qquad \text{for each } u \in \{1,2,\ldots,n\}. \tag{55}$$

The map $\kappa$ is an $A$-algebra homomorphism from $A\left[X_1, X_2, \ldots, X_n\right]$ to $A\left[X_1, X_2, \ldots, X_n\right]$. Since $R = A\left[X_1, X_2, \ldots, X_n\right]$, this rewrites as follows: The map $\kappa$ is an $A$-algebra homomorphism from $R$ to $R$.

Let $u$ be the element $X_i - X_j$ of $R$. Clearly, $uR$ is an ideal of $R$; thus, $R/uR$ is a quotient ring of $R$. Let $\pi$ be the canonical projection $R \to R/uR$. Then, $\pi$ is an $A$-algebra homomorphism satisfying $\operatorname{Ker}\pi = uR$. Thus, $\pi \circ \kappa : R \to R/uR$ is an $A$-algebra homomorphism (since it is the composition of the two $A$-algebra homomorphisms $\pi : R \to R/uR$ and $\kappa : R \to R$).

We have $(\pi \circ \kappa)(X_u) = \pi(X_u)$ for each $u \in \{1, 2, \ldots, n\}$ [25]. In other words, the two $A$-algebra homomorphisms $\pi \circ \kappa$ and $\pi$ are equal to each other on each of the elements $X_1, X_2, \ldots, X_n$.

But $R = A[X_1, X_2, \ldots, X_n]$. Hence, the elements $X_1, X_2, \ldots, X_n$ generate the $A$-algebra $R$. Therefore, if two $A$-algebra homomorphisms $\phi : R \to S$ and $\psi : R \to S$ (where $S$ is any $A$-algebra) are equal to each other on each of the elements $X_1, X_2, \ldots, X_n$, then these two $A$-algebra homomorphisms $\phi$ and $\psi$ must be identical. Applying this to $S = R/uR$, $\phi = \pi \circ \kappa$ and $\psi = \pi$, we conclude that the

[25] *Proof.* Let $u \in \{1, 2, \ldots, n\}$. We must prove that $(\pi \circ \kappa)(X_u) = \pi(X_u)$.

We are in one of the following two cases:

*Case 1:* We have $u = i$.

*Case 2:* We have $u \neq i$.

Let us first consider Case 1. In this case, we have $u = i$. Now, (55) yields $\kappa(X_u) = \begin{cases} X_u, & \text{if } u \neq i; \\ X_j, & \text{if } u = i \end{cases} = X_j$ (since $u = i$). Now,

$$(\pi \circ \kappa)(X_u) = \pi\left(\underbrace{\kappa(X_u)}_{=X_j}\right) = \pi(X_j).$$

Hence,

$$\pi\left(\underbrace{X_u}_{\substack{=X_i \\ (\text{since } u=i)}}\right) - \underbrace{(\pi \circ \kappa)(X_u)}_{=\pi(X_j)} = \pi(X_i) - \pi(X_j)$$
$$= \pi(X_i - X_j) \qquad (\text{since } \pi \text{ is an } A\text{-algebra homomorphism})$$
$$= 0$$

(since $X_i - X_j = u \in uR = \operatorname{Ker}\pi$). Thus, $(\pi \circ \kappa)(X_u) = \pi(X_u)$. Hence, $(\pi \circ \kappa)(X_u) = \pi(X_u)$ is proven in Case 1.

Let us now consider Case 2. In this case, we have $u \neq i$. The equality (55) yields $\kappa(X_u) = \begin{cases} X_u, & \text{if } u \neq i; \\ X_j, & \text{if } u = i \end{cases} = X_u$ (since $u \neq i$). Now,

$$(\pi \circ \kappa)(X_u) = \pi\left(\underbrace{\kappa(X_u)}_{=X_u}\right) = \pi(X_u).$$

Hence, $(\pi \circ \kappa)(X_u) = \pi(X_u)$ is proven in Case 2.

We thus have proven $(\pi \circ \kappa)(X_u) = \pi(X_u)$ in both Cases 1 and 2. Since these two Cases cover all possibilities, this shows that $(\pi \circ \kappa)(X_u) = \pi(X_u)$ always holds.

two $A$-algebra homomorphisms $\pi \circ \kappa$ and $\pi$ must be identical (since $\pi \circ \kappa$ and $\pi$ are equal to each other on each of the elements $X_1, X_2, \ldots, X_n$). In other words, $\pi \circ \kappa = \pi$.

Now, the definition of $\kappa$ shows that $\kappa(f)$ is the result of substituting $X_j$ for $X_i$ in $f$. In other words, $\kappa(f)$ is 0 (since the result of substituting $X_j$ for $X_i$ in $f$ is 0). Thus, $\kappa(f) = 0$. Hence, $(\pi \circ \kappa)(f) = \pi\left(\underbrace{\kappa(f)}_{=0}\right) = \pi(0) = 0$ (since $\pi$ is an $A$-algebra homomorphism). Since $\pi \circ \kappa = \pi$, this rewrites as $\pi(f) = 0$. In other words, $f \in \operatorname{Ker} \pi = uR$. In other words, $f$ is divisible by $u$. In other words, $f$ is divisible by $X_i - X_j$ (since $u = X_i - X_j$). This proves Lemma 8.2. □

*Proof of Corollary 8.1.* The polynomial $f$ is divisible by $X_i - X_j$ for every $(i,j) \in \{1,2,\ldots,n\}^2$ satisfying $i < j$ [26]. Hence, Theorem 1.2 shows that $f$ is divisible by $\prod_{1 \leq i < j \leq n} (X_i - X_j)$. This proves Corollary 8.1. □

# 9. A consequence on symmetric polynomials

## 9.1. Dividing by regular elements

From Corollary 8.1, we can furthermore derive a fact about symmetric polynomials. Let us first prepare by showing two trivial facts and making some definitions:

**Lemma 9.1.** Let $A$ be a commutative ring. Let $b$ be a regular element of $A$. Let $z_1$ and $z_2$ be two elements of $A$ such that $bz_1 = bz_2$. Then, $z_1 = z_2$.

*Proof of Lemma 9.1.* We have $b(z_1 - z_2) = bz_1 - bz_2 = 0$ (since $bz_1 = bz_2$). Since $b$ is regular, this results in $z_1 - z_2 = 0$. In other words, $z_1 = z_2$. This proves Lemma 9.1. □

**Proposition 9.2.** Let $A$ be a commutative ring. Let $b$ be a regular element of $A$. Let $c \in A$. If $c \in bA$, then there exists a **unique** element $x \in A$ satisfying $c = bx$.

*Proof of Proposition 9.2.* Assume that $c \in bA$.

If $z_1$ and $z_2$ are two elements $x \in A$ satisfying $c = bx$, then $z_1 = z_2$ [27]. In other words, there exists **at most one** element $x \in A$ satisfying $c = bx$. On the other hand, there exists some element $x \in A$ satisfying $c = bx$ (because $c \in bA$). Combining the preceding two sentences, we conclude that there exists a **unique** element $x \in A$ satisfying $c = bx$. This proves Proposition 9.2. □

[26] *Proof.* Fix any $(i,j) \in \{1,2,\ldots,n\}^2$ satisfying $i < j$. We must prove that $f$ is divisible by $X_i - X_j$.

Property 1 (in the statement of Corollary 8.1) shows that the result of substituting $X_j$ for $X_i$ in $f$ is 0. Thus, Lemma 8.2 shows that $f$ is divisible by $X_i - X_j$. Qed.

[27] *Proof.* Let $z_1$ and $z_2$ be two elements $x \in A$ satisfying $c = bx$. Thus, $z_1$ and $z_2$ are two elements of $A$ satisfying $c = bz_1$ and $c = bz_2$. Now, $bz_1 = c = bz_2$. Hence, Lemma 9.1 shows that $z_1 = z_2$. Qed.

**Definition 9.3.** Let $A$ be a commutative ring. Let $b$ be a regular element of $A$. Let $c \in A$. If $c \in bA$, then there exists a **unique** element $x \in A$ satisfying $c = bx$ (according to Proposition 9.2). This element $x$ is denoted by $\frac{c}{b}$ or by $c/b$. This notation generalizes the standard notation for quotients of (e.g.) rational numbers; it also satisfies analogous rules (for example, if $b \in A$ and $b' \in A$ are any two regular elements, and if $c \in bA$ and $c' \in b'A$, then $\frac{c}{b} + \frac{c'}{b'} = \frac{cb' + bc'}{bb'}$ and $\frac{c}{b} \cdot \frac{c'}{b'} = \frac{cc'}{bb'}$).

## 9.2. Symmetric polynomials

**Definition 9.4.** Let $n \in \mathbb{N}$. Then, $S_n$ denotes the group of permutations of the set $\{1, 2, \ldots, n\}$. This group is called the *$n$-th symmetric group*.

The sign of a permutation $\sigma \in S_n$ shall be denoted by $(-1)^\sigma$.

**Definition 9.5.** Let $A$ be a commutative ring. Let $n \in \mathbb{N}$. Let $g \in A[X_1, X_2, \ldots, X_n]$ be a polynomial in the $n$ indeterminates $X_1, X_2, \ldots, X_n$ over $A$. The polynomial $g$ is said to be *symmetric* if and only if each $\sigma \in S_n$ satisfies

$$g\left(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)}\right) = g\left(X_1, X_2, \ldots, X_n\right).$$

(Of course, we have $g\left(X_1, X_2, \ldots, X_n\right) = g$.)

For example, if $n = 3$, then the polynomials $X_1 + X_2 + X_3 - 7$ and $(X_1 + 5)(X_2 + 5) + (X_1 + 5)(X_3 + 5) + (X_2 + 5)(X_3 + 5)$ are symmetric, but the polynomial $X_1 + X_3$ is not (unless the ring $A$ is trivial).

## 9.3. Symmetric polynomials from dividing by $\prod_{1 \le i < j \le n} \left(X_i - X_j\right)$

Now, we claim the following:

**Proposition 9.6.** Let $A$ be a commutative ring. Let $n \in \mathbb{N}$. Let $f \in A[X_1, X_2, \ldots, X_n]$ be a polynomial in the $n$ indeterminates $X_1, X_2, \ldots, X_n$ over $A$. Assume that $f$ satisfies the following two properties:

*Property 1:* For every $(i, j) \in \{1, 2, \ldots, n\}^2$ satisfying $i < j$, the result of substituting $X_j$ for $X_i$ in $f$ is 0.

*Property 2:* Each $\sigma \in S_n$ satisfies

$$f\left(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)}\right) = (-1)^\sigma f\left(X_1, X_2, \ldots, X_n\right). \tag{56}$$

Then, $f$ is divisible by $\prod\limits_{1\leq i<j\leq n}\left(X_i - X_j\right)$, and the quotient $\dfrac{f}{\prod\limits_{1\leq i<j\leq n}\left(X_i - X_j\right)} \in A\left[X_1, X_2, \ldots, X_n\right]$ is a symmetric polynomial.

Note that Proposition 9.6 is essentially the "(iii) $\Longrightarrow$ (ii)" part of [LLPT95, Chapter SYM, Lemma (6.1)].[28]

For the proof of Proposition 9.6, we shall use the following well-known fact:

**Proposition 9.7.** Let $n \in \mathbb{N}$. Let $\sigma \in S_n$. Let $R$ be a commutative ring. If $x_1, x_2, \ldots, x_n$ are $n$ elements of $R$, then

$$\prod_{1\leq i<j\leq n}\left(x_{\sigma(i)} - x_{\sigma(j)}\right) = (-1)^{\sigma} \cdot \prod_{1\leq i<j\leq n}\left(x_i - x_j\right).$$

*Proof of Proposition 9.7.* In the case when $R = \mathbb{C}$ (so that $x_1, x_2, \ldots, x_n$ are $n$ complex numbers), the statement of Proposition 9.7 is precisely the claim of [Grinbe15, Exercise 5.13 **(a)**]. The proof given in [Grinbe15, solution to Exercise 5.13 **(a)**] works just as well in the general case. □

*Proof of Proposition 9.6.* Let $R$ be the commutative ring $A\left[X_1, X_2, \ldots, X_n\right]$. Thus, $X_1, X_2, \ldots, X_n$ are $n$ elements of $R$. Hence, for each $\sigma \in S_n$, we have

$$\prod_{1\leq i<j\leq n}\left(X_{\sigma(i)} - X_{\sigma(j)}\right) = (-1)^{\sigma} \cdot \prod_{1\leq i<j\leq n}\left(X_i - X_j\right) \tag{57}$$

(by Proposition 9.7 (applied to $x_i = X_i$)).

Corollary 8.1 shows that $f$ is divisible by $\prod\limits_{1\leq i<j\leq n}\left(X_i - X_j\right)$. In other words, $f \in \left(\prod\limits_{1\leq i<j\leq n}\left(X_i - X_j\right)\right) R$. Furthermore, the polynomial $\prod\limits_{1\leq i<j\leq n}\left(X_i - X_j\right)$ is a regular element of $R$ (by Corollary 4.4). Hence, the quotient $\dfrac{f}{\prod\limits_{1\leq i<j\leq n}\left(X_i - X_j\right)} \in A\left[X_1, X_2, \ldots, X_n\right]$ is well-defined.

Denote this quotient $\dfrac{f}{\prod\limits_{1\leq i<j\leq n}\left(X_i - X_j\right)} \in A\left[X_1, X_2, \ldots, X_n\right]$ by $g$. Thus,

$$g \cdot \prod_{1\leq i<j\leq n}\left(X_i - X_j\right) = f. \tag{58}$$

[28] "Essentially" because in [LLPT95, Chapter SYM, Lemma (6.1)], the result of substituting $X_j$ for $X_i$ in $f$ is considered not for $i < j$ but for $i > j$. But this makes little difference (it merely boils down to renaming the indeterminates).

Now, fix any permutation $\sigma \in S_n$. The element $(-1)^\sigma$ satisfies $(-1)^\sigma \cdot (-1)^\sigma = \left((-1)^\sigma\right)^2 = 1$ (since $(-1)^\sigma \in \{1, -1\}$). In particular, $(-1)^\sigma$ is invertible (as an element of $R$).

Substituting $X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)}$ for $X_1, X_2, \ldots, X_n$ on both sides of the equality (58), we obtain

$$g\left(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)}\right) \cdot \prod_{1 \leq i < j \leq n} \left(X_{\sigma(i)} - X_{\sigma(j)}\right) = f\left(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)}\right).$$

Hence,

$$\begin{aligned} f\left(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)}\right) &= g\left(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)}\right) \cdot \underbrace{\prod_{1 \leq i < j \leq n} \left(X_{\sigma(i)} - X_{\sigma(j)}\right)}_{\substack{= (-1)^\sigma \cdot \prod_{1 \leq i < j \leq n} \left(X_i - X_j\right) \\ \text{(by (57))}}} \\ &= g\left(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)}\right) \cdot (-1)^\sigma \cdot \prod_{1 \leq i < j \leq n} \left(X_i - X_j\right) \\ &= (-1)^\sigma \cdot \left(\prod_{1 \leq i < j \leq n} \left(X_i - X_j\right)\right) \cdot g\left(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)}\right). \end{aligned}$$

Comparing this with (56), we obtain

$$(-1)^\sigma \cdot \left(\prod_{1 \leq i < j \leq n} \left(X_i - X_j\right)\right) \cdot g\left(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)}\right) = (-1)^\sigma f\left(X_1, X_2, \ldots, X_n\right).$$

We can cancel the factor $(-1)^\sigma$ from both sides of this equality (since $(-1)^\sigma$ is invertible as an element of $R$). As a result, we obtain

$$\begin{aligned} &\left(\prod_{1 \leq i < j \leq n} \left(X_i - X_j\right)\right) \cdot g\left(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)}\right) \\ &= f\left(X_1, X_2, \ldots, X_n\right) = f = g \cdot \prod_{1 \leq i < j \leq n} \left(X_i - X_j\right) = \left(\prod_{1 \leq i < j \leq n} \left(X_i - X_j\right)\right) \cdot g. \end{aligned}$$

Hence, Lemma 9.1 (applied to $R$, $\prod_{1 \leq i < j \leq n} \left(X_i - X_j\right)$, $g\left(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)}\right)$ and $g$ instead of $A$, $b$, $z_1$ and $z_2$) shows that $g\left(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)}\right) = g$ (since $\prod_{1 \leq i < j \leq n} \left(X_i - X_j\right)$ is a regular element of $R$). Hence, $g\left(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)}\right) = g = g\left(X_1, X_2, \ldots, X_n\right)$.

Now, forget that we fixed $\sigma$. We thus have shown that each $\sigma \in S_n$ satisfies $g\left(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)}\right) = g\left(X_1, X_2, \ldots, X_n\right)$. In other words, the polynomial

$g$ is symmetric. In other words, the polynomial $\dfrac{f}{\prod\limits_{1\leq i<j\leq n}\left(X_i - X_j\right)}$ is symmetric (since $g = \dfrac{f}{\prod\limits_{1\leq i<j\leq n}\left(X_i - X_j\right)}$). In other words, the quotient $\dfrac{f}{\prod\limits_{1\leq i<j\leq n}\left(X_i - X_j\right)} \in A\left[X_1, X_2, \ldots, X_n\right]$ is a symmetric polynomial. This completes the proof of Proposition 9.6. □

## 9.4. Schur and factorial Schur polynomials

As an application of Proposition 9.6, let us construct the Schur polynomials (as quotients of determinants) and the factorial Schur polynomials. We begin with a standard piece of notation:

**Definition 9.8.** Let $A$ be a commutative ring. Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$. Let $a_{i,j}$ be an element of $A$ for each $i \in \{1, 2, \ldots, n\}$ and $j \in \{1, 2, \ldots, m\}$. Then, $\left(a_{i,j}\right)_{1\leq i\leq n,\ 1\leq j\leq m}$ shall denote the $n \times m$-matrix over $A$ whose $(i, j)$-th entry is $a_{i,j}$ for all $i \in \{1, 2, \ldots, n\}$ and $j \in \{1, 2, \ldots, m\}$.

For example, the matrix $\begin{pmatrix} 2 & 3 & 4 \\ 3 & 4 & 5 \end{pmatrix}$ can be rewritten as $(i+j)_{1\leq i\leq 2,\ 1\leq j\leq 3}$ using this notation.

Now, we can define the Schur polynomials:

**Corollary 9.9.** Let $A$ be a commutative ring. Let $n \in \mathbb{N}$. Consider the polynomial ring $A\left[X_1, X_2, \ldots, X_n\right]$ in the $n$ indeterminates $X_1, X_2, \ldots, X_n$ over $A$. Let $a_1, a_2, \ldots, a_n$ be $n$ nonnegative integers.

Let $F$ be the $n \times n$-matrix $\left(\left(X_i\right)^{a_j}\right)_{1\leq i\leq n,\ 1\leq j\leq n}$ over $A\left[X_1, X_2, \ldots, X_n\right]$. Then, the polynomial $\det F$ is divisible by $\prod\limits_{1\leq i<j\leq n}\left(X_i - X_j\right)$, and the quotient $\dfrac{\det F}{\prod\limits_{1\leq i<j\leq n}\left(X_i - X_j\right)} \in A\left[X_1, X_2, \ldots, X_n\right]$ is a symmetric polynomial.

We shall prove Corollary 9.9 later. When the integers $a_1, a_2, \ldots, a_n$ in Corollary 9.9 satisfy $a_1 > a_2 > \cdots > a_n$, the quotient $\dfrac{\det F}{\prod\limits_{1\leq i<j\leq n}\left(X_i - X_j\right)}$ is known as a *Schur polynomial* (see, e.g., [GriRei18, Corollary 2.6.6] or [Macdon95, Chapter I, (3.1)]).

**Example 9.10.** For this example, set $n = 3$ and $a_1 = 4$ and $a_2 = 2$ and $a_3 = 0$ in Corollary 9.9. Then, the matrix $F$ is

$$F = \begin{pmatrix} X_1^4 & X_1^2 & X_1^0 \\ X_2^4 & X_2^2 & X_2^0 \\ X_3^4 & X_3^2 & X_3^0 \end{pmatrix} = \begin{pmatrix} X_1^4 & X_1^2 & 1 \\ X_2^4 & X_2^2 & 1 \\ X_3^4 & X_3^2 & 1 \end{pmatrix},$$

and its determinant is

$$\det F = \det \begin{pmatrix} X_1^4 & X_1^2 & 1 \\ X_2^4 & X_2^2 & 1 \\ X_3^4 & X_3^2 & 1 \end{pmatrix} = X_1^4X_2^2 - X_1^4X_3^2 - X_1^2X_2^4 + X_1^2X_3^4 + X_2^4X_3^2 - X_2^2X_3^4$$
$$= (X_1 - X_2)(X_1 - X_3)(X_2 - X_3)(X_1 + X_2)(X_1 + X_3)(X_2 + X_3).$$

Thus, $\det F$ is clearly divisible by $(X_1 - X_2)(X_1 - X_3)(X_2 - X_3) = \prod_{1 \le i < j \le n} (X_i - X_j)$, and moreover the quotient

$$\frac{\det F}{\prod_{1 \le i < j \le n} (X_i - X_j)} = (X_1 + X_2)(X_1 + X_3)(X_2 + X_3)$$

is a symmetric polynomial. (This is a somewhat unusual example, since $F$ is a Vandermonde determinant in this case: for general choices of $a_1, a_2, a_3$, you should not expect the quotient $\dfrac{\det F}{\prod_{1 \le i < j \le n} (X_i - X_j)}$ to have a nice factorization.)

To construct the factorial Schur polynomials, we need another notation:

**Definition 9.11.** Let $A$ be a commutative ring. Let $a \in A$ and $k \in \mathbb{N}$. Then, $a^{\underline{k}}$ shall denote the element $a(a-1)(a-2)\cdots(a-k+1) = \prod_{i=0}^{k-1} (a-i)$ of $A$. (This element is called the *k-th lower factorial* or the *k-th falling factorial* of $a$.)

For example, if $A$ is any commutative ring and $a \in A$, then

$$a^{\underline{0}} = 1, \qquad a^{\underline{1}} = a, \qquad a^{\underline{2}} = a(a-1), \qquad a^{\underline{3}} = a(a-1)(a-2).$$

**Corollary 9.12.** Let $A$ be a commutative ring. Let $n \in \mathbb{N}$. Consider the polynomial ring $A[X_1, X_2, \ldots, X_n]$ in the $n$ indeterminates $X_1, X_2, \ldots, X_n$ over $A$. Let $a_1, a_2, \ldots, a_n$ be $n$ nonnegative integers.

Let $F$ be the $n \times n$-matrix $\left( (X_i)^{\underline{a_j}} \right)_{1 \le i \le n,\ 1 \le j \le n}$ over $A[X_1, X_2, \ldots, X_n]$. Then, the polynomial $\det F$ is divisible by $\prod_{1 \le i < j \le n} (X_i - X_j)$, and the quotient $\dfrac{\det F}{\prod_{1 \le i < j \le n} (X_i - X_j)} \in A[X_1, X_2, \ldots, X_n]$ is a symmetric polynomial.

**Example 9.13.** For this example, set $n = 3$ and $a_1 = 3$ and $a_2 = 2$ and $a_3 = 0$ in Corollary 9.12. Then, the matrix $F$ is

$$F = \begin{pmatrix} X_1^{\underline{3}} & X_1^{\underline{2}} & X_1^{\underline{0}} \\ X_2^{\underline{3}} & X_2^{\underline{2}} & X_2^{\underline{0}} \\ X_3^{\underline{3}} & X_3^{\underline{2}} & X_3^{\underline{0}} \end{pmatrix} = \begin{pmatrix} X_1(X_1-1)(X_1-2) & X_1(X_1-1) & 1 \\ X_2(X_2-1)(X_2-2) & X_2(X_2-1) & 1 \\ X_3(X_3-1)(X_3-2) & X_3(X_3-1) & 1 \end{pmatrix},$$

and its determinant is

$$\begin{aligned} \det F &= \det \begin{pmatrix} X_1(X_1-1)(X_1-2) & X_1(X_1-1) & 1 \\ X_2(X_2-1)(X_2-2) & X_2(X_2-1) & 1 \\ X_3(X_3-1)(X_3-2) & X_3(X_3-1) & 1 \end{pmatrix} \\ &= (X_1-X_2)(X_1-X_3)(X_2-X_3) \\ &\qquad (X_1X_2+X_1X_3+X_2X_3-X_1-X_2-X_3+1). \end{aligned}$$

This, again, is a polynomial that is divisible by $(X_1-X_2)(X_1-X_3)(X_2-X_3) = \prod_{1\le i<j\le n}(X_i-X_j)$, and the quotient $(X_1X_2+X_1X_3+X_2X_3-X_1-X_2-X_3+1)$ is again symmetric.

When the integers $a_1, a_2, \ldots, a_n$ in Corollary 9.12 satisfy $a_1 > a_2 > \cdots > a_n$, the quotient $\dfrac{\det F}{\prod_{1\le i<j\le n}(X_i-X_j)}$ is known as a *factorial Schur polynomial* (see, e.g., [CheLou93, Theorem 3.2][29]; for a more general result, see [BuMcNa14, Theorem 2]).

Instead of proving Corollary 9.9 and Corollary 9.12 separately, let us show a fact that generalizes them both:

**Corollary 9.14.** Let $A$ be a commutative ring. Let $n \in \mathbb{N}$. Consider the polynomial ring $A[X_1, X_2, \ldots, X_n]$ in the $n$ indeterminates $X_1, X_2, \ldots, X_n$ over $A$. Let $P_1, P_2, \ldots, P_n$ be $n$ polynomials in a single variable $T$ over the ring $A$.

Let $F$ be the $n \times n$-matrix $\left(P_j(X_i)\right)_{1\le i\le n,\ 1\le j\le n}$ over $A[X_1, X_2, \ldots, X_n]$. Then, the polynomial $\det F$ is divisible by $\prod_{1\le i<j\le n}(X_i-X_j)$, and the quotient $\dfrac{\det F}{\prod_{1\le i<j\le n}(X_i-X_j)} \in A[X_1, X_2, \ldots, X_n]$ is a symmetric polynomial.

*Proof of Corollary 9.14.* Define a polynomial $f \in A[X_1, X_2, \ldots, X_n]$ by $f = \det F$. (This is clearly well-defined, since the entries of the $n \times n$-matrix $F$ belong to $A[X_1, X_2, \ldots, X_n]$.) Note that

$$F = \left(P_j(X_i)\right)_{1\le i\le n,\ 1\le j\le n} = \left(P_v(X_u)\right)_{1\le u\le n,\ 1\le v\le n}$$

[29] Note that the lower factorial $a^{\underline{k}}$ is denoted by $(a)_k$ in [CheLou93].

(here, we have renamed the index $(i,j)$ as $(u,v)$).

We claim that the polynomial $f$ satisfies the following two properties:

*Property 1:* For every $(i,j) \in \{1,2,\ldots,n\}^2$ satisfying $i < j$, the result of substituting $X_j$ for $X_i$ in $f$ is 0.

*Property 2:* Each $\sigma \in S_n$ satisfies

$$f\left(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)}\right) = (-1)^{\sigma} f\left(X_1, X_2, \ldots, X_n\right).$$

[*Proof of Property 1:* Fix $(i,j) \in \{1,2,\ldots,n\}^2$ satisfying $i < j$.

The matrix $F$ satisfies $F = \left(P_v\left(X_u\right)\right)_{1 \le u \le n,\ 1 \le v \le n}$.

Hence, the $i$-th row of $F$ is $\left(P_1\left(X_i\right), P_2\left(X_i\right), \ldots, P_n\left(X_i\right)\right)$, whereas the $j$-th row of $F$ is $\left(P_1\left(X_j\right), P_2\left(X_j\right), \ldots, P_n\left(X_j\right)\right)$. If we substitute $X_j$ for $X_i$, then these two rows become equal (because $X_i$ and $X_j$ become equal upon this substitution). In other words, we have

$$\begin{aligned}&\left(\text{the result of substituting } X_j \text{ for } X_i \text{ in the } i\text{-th row of } F\right)\\ &= \left(\text{the result of substituting } X_j \text{ for } X_i \text{ in the } j\text{-th row of } F\right).\end{aligned}$$

Let $F'$ be the matrix obtained by substituting $X_j$ for $X_i$ in the matrix $F$. Thus,

$$\begin{aligned}&\left(\text{the } i\text{-th row of } F'\right)\\ &= \left(\text{the result of substituting } X_j \text{ for } X_i \text{ in the } i\text{-th row of } F\right)\\ &= \left(\text{the result of substituting } X_j \text{ for } X_i \text{ in the } j\text{-th row of } F\right)\end{aligned}$$

and

$$\begin{aligned}&\left(\text{the } j\text{-th row of } F'\right)\\ &= \left(\text{the result of substituting } X_j \text{ for } X_i \text{ in the } j\text{-th row of } F\right)\end{aligned}$$

(since the matrix $F'$ is obtained by substituting $X_j$ for $X_i$ in the matrix $F$). Comparing these two equalities, we conclude that (the $i$-th row of $F'$) = (the $j$-th row of $F'$). Hence, the matrix $F'$ has two equal rows (since $i < j$). Therefore, the determinant of $F'$ is 0. In other words, $\det\left(F'\right) = 0$.

But recall that $f = \det F$. Hence,

$$\begin{aligned}&\left(\text{the result of substituting } X_j \text{ for } X_i \text{ in } f\right)\\ &= \left(\text{the result of substituting } X_j \text{ for } X_i \text{ in } \det F\right)\\ &= \det \underbrace{\left(\text{the matrix obtained by substituting } X_j \text{ for } X_i \text{ in the matrix } F\right)}_{\substack{=F' \\ \text{(because this is how } F' \text{ was defined)}}}\\ &\qquad \left(\begin{array}{c}\text{because when a substitution is applied to all entries of the matrix,}\\ \text{the determinant of the matrix undergoes the same substitution}\end{array}\right)\\ &= \det\left(F'\right) = 0.\end{aligned}$$

In other words, the result of substituting $X_j$ for $X_i$ in $f$ is 0. This proves Property 1.]

[*Proof of Property 2:* Let $\sigma \in S_n$.

It is well-known that if we permute the rows of an $n \times n$-matrix according to the permutation $\sigma$, then the determinant of this matrix is multiplied by $(-1)^\sigma$. In other words, any $n \times n$-matrix $\left(b_{i,j}\right)_{1 \leq i \leq n,\ 1 \leq j \leq n}$ satisfies

$$\det\left(\left(b_{\sigma(i),j}\right)_{1 \leq i \leq n,\ 1 \leq j \leq n}\right) = (-1)^\sigma \det\left(\left(b_{i,j}\right)_{1 \leq i \leq n,\ 1 \leq j \leq n}\right)$$

[30]. Applying this to $\left(b_{i,j}\right)_{1 \leq i \leq n,\ 1 \leq j \leq n} = \left(P_j\left(X_i\right)\right)_{1 \leq i \leq n,\ 1 \leq j \leq n}$, we conclude that

$$\det\left(\left(P_j\left(X_{\sigma(i)}\right)\right)_{1 \leq i \leq n,\ 1 \leq j \leq n}\right) = (-1)^\sigma \det\left(\left(P_j\left(X_i\right)\right)_{1 \leq i \leq n,\ 1 \leq j \leq n}\right).$$

But $f = \det F = \det\left(\left(P_j\left(X_i\right)\right)_{1 \leq i \leq n,\ 1 \leq j \leq n}\right)$ (since $F = \left(P_j\left(X_i\right)\right)_{1 \leq i \leq n,\ 1 \leq j \leq n}$). Substituting $X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)}$ for $X_1, X_2, \ldots, X_n$ in this equality, we obtain

$$\begin{aligned} f\left(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)}\right) &= \det\left(\left(P_j\left(X_{\sigma(i)}\right)\right)_{1 \leq i \leq n,\ 1 \leq j \leq n}\right) \\ &= (-1)^\sigma \underbrace{\det\left(\left(P_j\left(X_i\right)\right)_{1 \leq i \leq n,\ 1 \leq j \leq n}\right)}_{= f = f(X_1, X_2, \ldots, X_n)} \\ &= (-1)^\sigma f\left(X_1, X_2, \ldots, X_n\right). \end{aligned}$$

This proves Property 2.]

We have now proven that $f$ satisfies both Properties 1 and 2. Hence, Proposition 9.6 shows that $f$ is divisible by $\prod_{1 \leq i < j \leq n}\left(X_i - X_j\right)$, and that the quotient $\dfrac{f}{\prod_{1 \leq i < j \leq n}\left(X_i - X_j\right)} \in A\left[X_1, X_2, \ldots, X_n\right]$ is a symmetric polynomial. In view of $f = \det F$, this rewrites as follows: $\det F$ is divisible by $\prod_{1 \leq i < j \leq n}\left(X_i - X_j\right)$, and the quotient $\dfrac{\det F}{\prod_{1 \leq i < j \leq n}\left(X_i - X_j\right)} \in A\left[X_1, X_2, \ldots, X_n\right]$ is a symmetric polynomial. This proves Corollary 9.14. $\square$

*Proof of Corollary 9.9.* Consider the polynomial ring $A\left[T\right]$ in a single variable $T$ over the ring $A$. For each $j \in \{1, 2, \ldots, n\}$, define a polynomial $P_j \in A\left[T\right]$ by $P_j =$

[30] See, for example, [Grinbe15, Lemma 6.17 **(a)**] (applied to $\left(b_{i,j}\right)_{1 \leq i \leq n,\ 1 \leq j \leq n}$, $\sigma$ and $\left(b_{\sigma(i),j}\right)_{1 \leq i \leq n,\ 1 \leq j \leq n}$ instead of $B$, $\kappa$ and $B_\kappa$) for a proof of this fact.

$T^{a_j}$. Thus, $P_1, P_2, \ldots, P_n$ are $n$ polynomials in a single variable $T$ over the ring $A$. Moreover, for each $i \in \{1, 2, \ldots, n\}$ and $j \in \{1, 2, \ldots, n\}$, we have

$$P_j(X_i) = (X_i)^{a_j} \qquad \left(\text{since } P_j = T^{a_j}\right).$$

Thus, we have $\left(P_j(X_i)\right)_{1 \le i \le n,\, 1 \le j \le n} = \left((X_i)^{a_j}\right)_{1 \le i \le n,\, 1 \le j \le n}$. But $F = \left((X_i)^{a_j}\right)_{1 \le i \le n,\, 1 \le j \le n}$ (by the definition of $F$). Comparing these two equalities, we obtain $F = \left(P_j(X_i)\right)_{1 \le i \le n,\, 1 \le j \le n}$. Thus, $F$ is the $n \times n$-matrix $\left(P_j(X_i)\right)_{1 \le i \le n,\, 1 \le j \le n}$ over $A[X_1, X_2, \ldots, X_n]$. Hence, Corollary 9.14 shows that the polynomial $\det F$ is divisible by $\prod_{1 \le i < j \le n} (X_i - X_j)$, and that the quotient $\dfrac{\det F}{\prod_{1 \le i < j \le n} (X_i - X_j)} \in A[X_1, X_2, \ldots, X_n]$ is a symmetric polynomial. This proves Corollary 9.9. □

*Proof of Corollary 9.12.* Consider the polynomial ring $A[T]$ in a single variable $T$ over the ring $A$. For each $j \in \{1, 2, \ldots, n\}$, define a polynomial $P_j \in A[T]$ by $P_j = T^{\underline{a_j}}$. Thus, $P_1, P_2, \ldots, P_n$ are $n$ polynomials in a single variable $T$ over the ring $A$. Moreover, for each $i \in \{1, 2, \ldots, n\}$ and $j \in \{1, 2, \ldots, n\}$, we have

$$\begin{aligned} P_j(X_i) &= X_i (X_i - 1)(X_i - 2) \cdots (X_i - a_j + 1) \\ &\qquad \left( \begin{array}{c} \text{since } P_j = T^{\underline{a_j}} = T(T-1)(T-2)\cdots(T-a_j+1) \\ \text{(by the definition of } T^{\underline{a_j}}\text{)} \end{array} \right) \\ &= (X_i)^{\underline{a_j}} \qquad \left( \begin{array}{c} \text{since } (X_i)^{\underline{a_j}} = X_i (X_i - 1)(X_i - 2) \cdots (X_i - a_j + 1) \\ \text{(by the definition of } (X_i)^{\underline{a_j}}\text{)} \end{array} \right). \end{aligned}$$

Thus, we have $\left(P_j(X_i)\right)_{1 \le i \le n,\, 1 \le j \le n} = \left((X_i)^{\underline{a_j}}\right)_{1 \le i \le n,\, 1 \le j \le n}$. But $F = \left((X_i)^{\underline{a_j}}\right)_{1 \le i \le n,\, 1 \le j \le n}$ (by the definition of $F$). Comparing these two equalities, we obtain $F = \left(P_j(X_i)\right)_{1 \le i \le n,\, 1 \le j \le n}$. Thus, $F$ is the $n \times n$-matrix $\left(P_j(X_i)\right)_{1 \le i \le n,\, 1 \le j \le n}$ over $A[X_1, X_2, \ldots, X_n]$. Hence, Corollary 9.14 shows that the polynomial $\det F$ is divisible by $\prod_{1 \le i < j \le n} (X_i - X_j)$, and that the quotient $\dfrac{\det F}{\prod_{1 \le i < j \le n} (X_i - X_j)} \in A[X_1, X_2, \ldots, X_n]$ is a symmetric polynomial. This proves Corollary 9.12. □

# 10. More about power series

In this Section, we return to the study of the ring $A[[X]]$ of formal power series.

## 10.1. Regular and nilpotent elements in general

We begin with proving some general properties of nilpotency and regularity in commutative rings. We begin with fairly obvious ones:

**Corollary 10.1.** Let $A$ be a commutative ring. Let $r$ be a regular element of $A$. Let $n \in \mathbb{N}$. Then, the element $r^n$ of $A$ is regular.

*Proof of Corollary 10.1.* Apply Proposition 2.3 to $G = \{1, 2, \ldots, n\}$ and $a_g = r$. □

**Proposition 10.2.** Let $A$ be a commutative ring. Let $a \in A$ and $b \in A$ be two elements of $A$ such that the element $ab$ of $A$ is regular. Then, $a \in A$ is regular.

*Proof of Proposition 10.2.* Every $x \in A$ satisfying $ax = 0$ satisfies $(ab)\, x = b \underbrace{ax}_{=0} = 0$, thus $x = 0$ (since $ab$ is regular). In other words, $a$ is regular. This proves Proposition 10.2. □

Next, let us recall a basic identity: If $A$ is a commutative ring, and if $a$ and $b$ are any elements of $A$, and if $m \in \mathbb{N}$, then

$$(a - b) \sum_{i=0}^{m-1} a^i b^{m-1-i} = a^m - b^m. \tag{59}$$

Now, we shall prove a surprisingly general property of regularity:

**Proposition 10.3.** Let $A$ be a commutative ring. Let $r$ be a regular element of $A$. Let $a$ be a nilpotent element of $A$. Then, the element $r - a$ of $A$ is regular.

*Proof of Proposition 10.3.* The element $a$ of $A$ is nilpotent. In other words, there exists some $m \in \mathbb{N}$ such that $a^m = 0$ (by the definition of "nilpotent"). Consider this $m$.

Corollary 10.1 (applied to $n = m$) shows that the element $r^m$ of $A$ is regular.

But (59) (applied to $r$ and $a$ instead of $a$ and $b$) yields

$$(r - a) \sum_{i=0}^{m-1} r^i b^{m-1-i} = r^m - \underbrace{a^m}_{=0} = r^m.$$

Hence, the element $(r - a) \sum_{i=0}^{m-1} r^i b^{m-1-i}$ is regular (since the element $r^m$ is regular).

Thus, Proposition 10.2 (applied to $r - a$ and $\sum_{i=0}^{m-1} r^i b^{m-1-i}$ instead of $a$ and $b$) shows that $r - a \in A$ is regular. This proves Proposition 10.3. □

## 10.2. More regular power series

Let us now resume studying formal power series in $A[[X]]$. We begin with an essentially trivial fact:

**Proposition 10.4.** Let $A$ be a commutative ring. Then:
**(a)** The element $X$ of $A[[X]]$ is regular.
**(b)** Let $n \in \mathbb{N}$. Then, the element $X^n$ of $A[[X]]$ is regular.

*Proof of Proposition 10.4.* **(a)** The quickest way to prove this is by applying Proposition 6.1 to $a = 0$ (since 0 is nilpotent). Alternatively, you can prove this directly: If $x \in A[[X]]$ is such that $Xx = 0$, then it is easily seen that $x = 0$ (since the coefficients of $Xx$ are precisely the coefficients of $x$, just shifted by one degree); in other words, $X$ is regular. Either way, Proposition 10.4 **(a)** is proven.

**(b)** Proposition 10.4 **(a)** shows that the element $X$ of $A[[X]]$ is regular. Hence, Corollary 10.1 (applied to $A[[X]]$ and $X$ instead of $A$ and $r$) yields that the element $X^n$ of $A[[X]]$ is regular. This proves Proposition 10.4 **(b)**. □

We can now apply Proposition 10.3 to rings of power series:

**Corollary 10.5.** Let $A$ be a commutative ring. Let $n \in \mathbb{N}$. Let $p \in A[[X]]$ be a formal power series such that $X^n - p$ is nilpotent. Then, $p \in A[[X]]$ is regular.

*Proof of Corollary 10.5.* Proposition 10.4 **(b)** yields that the element $X^n$ of $A[[X]]$ is regular. Meanwhile, the element $X^n - p$ of $A[[X]]$ is nilpotent (by assumption). Hence, Proposition 10.3 (applied to $A[[X]]$, $X^n$ and $X^n - p$ instead of $A$, $r$ and $a$) yields that the element $X^n - (X^n - p)$ of $A[[X]]$ is regular. In other words, the element $p$ of $A[[X]]$ is regular (since $X^n - (X^n - p) = p$). This proves Corollary 10.5. □

We can now re-prove Proposition 6.1:

*Second proof of Proposition 6.1.* Recall that $A$ is a subring of $A[[X]]$. We know that $a$ is nilpotent. In other words, $X^1 - (X - a)$ is nilpotent (since $\underbrace{X^1}_{=X} - (X - a) = X - (X - a) = a$). Thus, Corollary 10.5 (applied to $n = 1$ and $p = X - a$) yields that $X - a \in A[[X]]$ is regular. This proves Proposition 6.1 again. (Of course, this second proof of Proposition 6.1 is circular if you have used Proposition 6.1 in proving Proposition 10.4; thus, for it to be valid, you need a proof of Proposition 10.4 that is independent on Proposition 6.1.) □

## 10.3. Intermezzo on sums of nilpotents

We next prove a standard fact about nilpotent elements in commutative rings:

**Proposition 10.6.** Let $A$ be a commutative ring. Let $a$ and $b$ be two nilpotent elements of $A$. Then, the element $a + b$ of $A$ is nilpotent.

*Proof of Proposition 10.6.* The element $a$ of $A$ is nilpotent. In other words, there exists some $p \in \mathbb{N}$ such that $a^p = 0$ (by the definition of "nilpotent"). Consider this $p$.

The element $b$ of $A$ is nilpotent. In other words, there exists some $q \in \mathbb{N}$ such that $b^q = 0$ (by the definition of "nilpotent"). Consider this $q$.

Every $k \in \{0, 1, \ldots, p\}$ satisfies

$$b^{p+q-k} = 0. \tag{60}$$

[*Proof of (60):* Let $k \in \{0, 1, \ldots, p\}$. Then, $k \leq p$, so that $p - k \geq 0$. Hence, $b^{q+(p-k)} = \underbrace{b^q}_{=0} b^{p-k} = 0$. In view of $q + (p-k) = p + q - k$, this rewrites as $b^{p+q-k} = 0$. This proves (60).]

Every $k \in \{p+1, p+2, \ldots, p+q\}$ satisfies

$$a^k = 0. \tag{61}$$

[*Proof of (61):* Let $k \in \{p+1, p+2, \ldots, p+q\}$. Thus, $k \geq p+1 \geq p$ and therefore $k - p \geq 0$. Hence, $a^{p+(k-p)} = \underbrace{a^p}_{=0} a^{k-p} = 0$. In view of $p + (k-p) = k$, this rewrites as $a^k = 0$. This proves (61).]

Recall that the ring $A$ is commutative. Hence, the binomial formula yields

$$\begin{aligned}
(a+b)^{p+q} &= \sum_{k=0}^{p+q} \binom{p+q}{k} a^k b^{p+q-k} \\
&= \sum_{k=0}^{p} \binom{p+q}{k} a^k \underbrace{b^{p+q-k}}_{\substack{=0 \\ \text{(by (60))}}} + \sum_{k=p+1}^{p+q} \binom{p+q}{k} \underbrace{a^k}_{\substack{=0 \\ \text{(by (61))}}} b^{p+q-k} \\
&\qquad \text{(here, we have split the sum at } k = p \text{, since } 0 \leq p \leq p+q\text{)} \\
&= \underbrace{\sum_{k=0}^{p} \binom{p+q}{k} a^k \cdot 0}_{=0} + \underbrace{\sum_{k=p+1}^{p+q} \binom{p+q}{k} \cdot 0 b^{p+q-k}}_{=0} = 0 + 0 = 0.
\end{aligned}$$

Hence, there exists a $k \in \mathbb{N}$ such that $(a+b)^k = 0$ (namely, $k = p+q$). In other words, the element $a+b$ of $A$ is nilpotent (by the definition of "nilpotent"). This proves Proposition 10.6. □

**Corollary 10.7.** Let $A$ be a commutative ring. Let $a$ and $b$ be two nilpotent elements of $A$. Then, the element $a - b$ of $A$ is nilpotent.

*Proof of Corollary 10.7.* The element $b$ of $A$ is nilpotent. In other words, there exists some $q \in \mathbb{N}$ such that $b^q = 0$ (by the definition of "nilpotent"). Consider this $q$. Then, $(-b)^q = (-1)^q \underbrace{b^q}_{=0} = 0$. Hence, there exists a $k \in \mathbb{N}$ such that $(-b)^k = 0$ (namely, $k = q$). In other words, the element $-b$ of $A$ is nilpotent (by the definition of "nilpotent"). Hence, Proposition 10.6 (applied to $-b$ instead of $b$) shows that the element $a + (-b)$ of $A$ is nilpotent (since $a$ is nilpotent). In other words, the element $a - b$ of $A$ is nilpotent (since $a + (-b) = a - b$). This proves Corollary 10.7. □

## 10.4. Nilpotent power series have nilpotent coefficients

In Definition 3.1 **(a)**, we have introduced the notation $[X^n]\, p$ for the coefficient of $X^n$ in a polynomial $p \in A[X]$. We can extend this notation to formal power series $p \in A[[X]]$ in the obvious way:

**Definition 10.8.** Let $A$ be a commutative ring.

If $p \in A[[X]]$ is a formal power series in some indeterminate $X$ over $A$, and if $n \in \mathbb{N}$, then $[X^n]\, p$ will denote the coefficient of $X^n$ in $p$. For example,

$$\left[X^3\right]\left(1 + X + X^2 + X^3 + \cdots\right) = 1;$$
$$\left[X^4\right]\left(1 + 2X + 3X^2 + 4X^3 + \cdots\right) = 5.$$

Clearly, every formal power series $p \in A[[X]]$ satisfies $p = \sum\limits_{n \in \mathbb{N}} \left([X^n]\, p\right) X^n$. (Here, $\sum\limits_{n \in \mathbb{N}} \left([X^n]\, p\right) X^n$ is a well-defined infinite sum.)

Clearly, Definition 10.8 extends Definition 3.1 **(a)**.

Our next goal is a necessary criterion for the nilpotency of a formal power series:

**Theorem 10.9.** Let $A$ be a commutative ring. Let $g \in A[[X]]$ be nilpotent. Then, $[X^n]\, g$ is nilpotent for each $n \in \mathbb{N}$.

In other words, each coefficient of a nilpotent formal power series in $A[[X]]$ must be nilpotent.

Note that the converse of Theorem 10.9 does not hold in general. (See [EleRos12] and [Fields71] for counterexamples.)

Before we prove Theorem 10.9, we state a few simple lemmas. First, we recall the rules for adding and multiplying formal power series:

**Proposition 10.10.** Let $A$ be a commutative ring. Let $n \in \mathbb{N}$.

**(a)** Every $p \in A[[X]]$ and $q \in A[[X]]$ satisfy $[X^n]\,(p+q) = [X^n]\, p + [X^n]\, q$.

**(b)** Every $\lambda \in A$ and $p \in A[[X]]$ satisfy $[X^n]\,(\lambda p) = \lambda\, [X^n]\, p$.

**(c)** Every $p \in A[[X]]$ and $q \in A[[X]]$ satisfy $[X^n]\,(pq) = \sum\limits_{k=0}^{n} \left(\left[X^k\right] p\right) \cdot \left(\left[X^{n-k}\right] q\right)$.

**Corollary 10.11.** Let $A$ be a commutative ring.

**(a)** Every $p \in A[[X]]$ and $q \in A[[X]]$ satisfy $\left[X^0\right](pq) = \left(\left[X^0\right] p\right) \cdot \left(\left[X^0\right] q\right)$.

**(b)** Every $p \in A[[X]]$ and $n \in \mathbb{N}$ satisfy $\left[X^0\right](p^n) = \left(\left[X^0\right] p\right)^n$.

*Proof of Corollary 10.11.* **(a)** This follows easily from Proposition 10.10 **(c)**.

**(b)** This follows by induction on $n$ (using Corollary 10.11 **(a)** in the induction step). □

Now we can easily prove the particular case of Theorem 10.9 for $n = 0$:

**Lemma 10.12.** Let $A$ be a commutative ring. Let $g \in A[[X]]$ be nilpotent. Then, $[X^0] g$ is nilpotent.

*Proof of Lemma 10.12.* We have assumed that $g$ is nilpotent. In other words, there exists an $n \in \mathbb{N}$ such that $g^n = 0$ (by the definition of "nilpotent"). Consider this $n$. Now, Corollary 10.11 **(b)** (applied to $p = g$) yields $[X^0](g^n) = ([X^0] g)^n$. Hence, $([X^0] g)^n = [X^0] \underbrace{(g^n)}_{=0} = [X^0] 0 = 0$. Thus, there exists a $k \in \mathbb{N}$ such that $([X^0] g)^k = 0$ (namely, $k = n$). In other words, $[X^0] g$ is nilpotent (by the definition of "nilpotent"). This proves Lemma 10.12. □

In order to get a grip on the other coefficients of a nilpotent formal power series, we need a few more basic results. We begin with a general property of regular and nilpotent elements:

**Lemma 10.13.** Let $A$ be a commutative ring. Let $r \in A$ and $a \in A$ be such that $ra$ is nilpotent and $r$ is regular. Then, $a$ is nilpotent.

*Proof of Lemma 10.13.* We have assumed that $ra$ is nilpotent. In other words, there exists an $n \in \mathbb{N}$ such that $(ra)^n = 0$ (by the definition of "nilpotent"). Consider this $n$. Then, $r^n a^n = (ra)^n = 0$.

Corollary 10.1 shows that the element $r^n$ of $A$ is regular. In other words, every $x \in A$ satisfying $r^n x = 0$ satisfies $x = 0$. Applying this to $x = a^n$, we obtain $a^n = 0$ (since $r^n a^n = 0$). Hence, $a$ is nilpotent.

This proves Lemma 10.13. □

**Corollary 10.14.** Let $A$ be a commutative ring. Let $g \in A[[X]]$ be such that $Xg$ is nilpotent. Then, $g$ is nilpotent.

*Proof of Corollary 10.14.* Proposition 10.4 **(a)** shows that the element $X$ of $A[[X]]$ is regular. Hence, Lemma 10.13 (applied to $A[[X]]$, $X$ and $g$ instead of $A$, $r$ and $a$) yields that $g$ is nilpotent. This proves Corollary 10.14. □

**Corollary 10.15.** Let $A$ be a commutative ring. Let $g \in A[[X]]$. Define a formal power series $\widetilde{g} \in A[[X]]$ by $\widetilde{g} = \sum_{n \in \mathbb{N}} ([X^{n+1}] g) \cdot X^n$. Then:

**(a)** We have $g = [X^0] g + X\widetilde{g}$.

**(b)** We have $[X^k] g = [X^{k-1}] \widetilde{g}$ for each positive integer $k$.

**(c)** If $g$ is nilpotent, then $\widetilde{g}$ is nilpotent.

*Proof of Corollary 10.15.* **(a)** Every formal power series $f \in A[[X]]$ satisfies $f = \sum_{n \in \mathbb{N}} ([X^n] f) \cdot X^n$ (since $[X^0] f, [X^1] f, [X^2] f, \ldots$ are the coefficients of $f$). Applying

this to $f = g$, we obtain

$$g = \sum_{n \in \mathbb{N}} \left( \left[ X^n \right] g \right) \cdot X^n = \left( \left[ X^0 \right] g \right) \cdot \underbrace{X^0}_{=1} + \underbrace{\sum_{n \in \{1,2,3,\ldots\}} \left( \left[ X^n \right] f \right) \cdot X^n}_{\substack{= \sum_{n \in \mathbb{N}} \left( \left[ X^{n+1} \right] g \right) \cdot X^{n+1} \\ \text{(here, we have substituted } n+1 \\ \text{for } n \text{ in the sum)}}}$$

(here, we have split off the addend for $n = 0$ from the sum)

$$= \left[ X^0 \right] g + \sum_{n \in \mathbb{N}} \left( \left[ X^{n+1} \right] g \right) \cdot \underbrace{X^{n+1}}_{= XX^n} = \left[ X^0 \right] g + \underbrace{\sum_{n \in \mathbb{N}} \left( \left[ X^{n+1} \right] g \right) \cdot XX^n}_{= X \sum_{n \in \mathbb{N}} \left( \left[ X^{n+1} \right] g \right) \cdot X^n}$$

$$= \left[ X^0 \right] g + X \underbrace{\sum_{n \in \mathbb{N}} \left( \left[ X^{n+1} \right] g \right) \cdot X^n}_{= \widetilde{g}} = \left[ X^0 \right] g + X\widetilde{g}.$$

This proves Corollary 10.15 **(a)**.

**(b)** We have $\widetilde{g} = \sum_{n \in \mathbb{N}} \left( \left[ X^{n+1} \right] g \right) \cdot X^n$. Thus, the coefficients of the power series $\widetilde{g}$ are $\left[ X^1 \right] g$, $\left[ X^2 \right] g$, $\left[ X^3 \right] g$, .... In other words, for each $n \in \mathbb{N}$, we have $\left[ X^n \right] \widetilde{g} = \left[ X^{n+1} \right] g$. Substituting $k - 1$ for $n$ in this result, we obtain the following: For each $k \in \{1, 2, 3, \ldots\}$, we have $\left[ X^{k-1} \right] \widetilde{g} = \left[ X^k \right] g$. This proves Corollary 10.15 **(b)**.

**(c)** Assume that $g$ is nilpotent. Thus, Lemma 10.12 shows that $\left[ X^0 \right] g$ is nilpotent. Hence, Corollary 10.7 (applied to $A[[X]]$, $g$ and $\left[ X^0 \right] g$ instead of $A$, $a$ and $b$) shows that the element $g - \left[ X^0 \right] g$ of $A[[X]]$ is nilpotent.

But Corollary 10.15 **(a)** yields $g = \left[ X^0 \right] g + X\widetilde{g}$; thus, $g - \left[ X^0 \right] g = X\widetilde{g}$. Hence, $X\widetilde{g}$ is nilpotent (since $g - \left[ X^0 \right] g$ is nilpotent). Therefore, Corollary 10.14 (applied to $\widetilde{g}$ instead of $g$) yields that $\widetilde{g}$ is nilpotent. This proves Corollary 10.15 **(c)**. □

We are now ready to prove Theorem 10.9:

*Proof of Theorem 10.9.* We shall prove Theorem 10.9 by induction on $n$:

*Induction base:* If $A$ is a commutative ring, and if $g \in A[[X]]$ is nilpotent, then $\left[ X^0 \right] g$ is nilpotent (by Lemma 10.12). In other words, Theorem 10.9 holds for $n = 0$. This completes the induction base.

*Induction step:* Let $k$ be a positive integer. Assume that Theorem 10.9 holds for $n = k - 1$. We must prove that Theorem 10.9 holds for $n = k$.

We have assumed that Theorem 10.9 holds for $n = k - 1$. In other words, the following statement holds:

> *Statement 1:* Let $A$ be a commutative ring. Let $g \in A[[X]]$ be nilpotent. Then, $\left[ X^{k-1} \right] g$ is nilpotent.

Now, we must prove that Theorem 10.9 holds for $n = k$. In other words, we must prove the following statement:

*Statement 2:* Let $A$ be a commutative ring. Let $g \in A\left[\left[X\right]\right]$ be nilpotent. Then, $\left[X^k\right] g$ is nilpotent.

[*Proof of Statement 2:* Define a formal power series $\widetilde{g} \in A\left[\left[X\right]\right]$ by $\widetilde{g} = \sum\limits_{n \in \mathbb{N}} \left(\left[X^{n+1}\right] g\right) \cdot X^n$. Then, Corollary 10.15 **(c)** shows that $\widetilde{g}$ is nilpotent. Hence, Statement 1 (applied to $\widetilde{g}$ instead of $g$) yields that $\left[X^{k-1}\right] \widetilde{g}$ is nilpotent. But Corollary 10.15 **(b)** yields $\left[X^k\right] g = \left[X^{k-1}\right] \widetilde{g}$. Hence, $\left[X^k\right] g$ is nilpotent (since $\left[X^{k-1}\right] \widetilde{g}$ is nilpotent). This proves Statement 2.]

So we have proven Statement 2. In other words, we have proven that Theorem 10.9 holds for $n = k$. This completes the induction step. Thus, Theorem 10.9 is proven. □

TODO!

# References

[BieLou89] L. C. Biedenharn, J. D. Louck, *A new class of symmetric polynomials defined in terms of tableaux*, Advances in Applied Mathematics, Volume 10, Issue 4, December 1989, pp. 396–438.
https://doi.org/10.1016/0196-8858(89)90023-7

[BuMcNa14] Daniel Bump, Peter J. McNamara and Maki Nakasuji, *Factorial Schur Functions and the Yang-Baxter Equation*, arXiv:1108.3087v3.
https://arxiv.org/abs/1108.3087v3

[CheLou93] William Y. C. Chen and James D. Louck, *The factorial Schur function*, J. Math. Phys. 34, 4144 (1993).
http://dx.doi.org/10.1063/1.530032

[EGHLSVY11] Pavel Etingof, Oleg Golberg, Sebastian Hensel, Tiankai Liu, Alex Schwendner, Dmitry Vaintrob, Elena Yudovina, *Introduction to Representation Theory*, Student Mathematical Library #59, AMS 2011.
A draft of this book can be found on the arXiv as arXiv:0901.0827v5.

[EleRos12] Georges Elencwajg, Julian Rosen and others, *Answers to math.stackexchange question #187952 ("A non-nilpotent formal power series with nilpotent coefficients")*.
https://math.stackexchange.com/q/187952

[Fields71] David E. Fields, *Zero divisors and nilpotent elements in power series rings*, Proc. Amer. Math. Soc. **27** (1971), pp. 427–433. https://doi.org/10.1090/S0002-9939-1971-0271100-6

[Garrett09] Paul Garrett, *Abstract Algebra*, lecture notes, 2009.
http://www.math.umn.edu/~garrett/m/algebra/notes/Whole.pdf

[Grinbe15] Darij Grinberg, *Notes on the combinatorial fundamentals of algebra*, 10 January 2019.
http://www.cip.ifi.lmu.de/~grinberg/primes2015/sols.pdf
The numbering of theorems and formulas in this link might shift when the project gets updated; for a "frozen" version whose numbering is guaranteed to match that in the citations above, see https://github.com/darijgr/detnotes/releases/tag/2019-01-10 .

[GriRei18] Darij Grinberg, Victor Reiner, *Hopf algebras in Combinatorics*, version of 11 May 2018, arXiv:1409.8356v5.
See also http://www.cip.ifi.lmu.de/~grinberg/algebra/HopfComb-sols.pdf for a version that gets updated.

[Knapp2016] Anthony W. Knapp, *Basic Algebra*, Digital Second Edition, 2016.
http://www.math.stonybrook.edu/~aknapp/download.html

[LLPT95] D. Laksov, A. Lascoux, P. Pragacz, and A. Thorup, *The LLPT Notes*, edited by A. Thorup, 1995,
http://www.math.ku.dk/~thorup/notes/sympol.pdf .

[Macdon95] I. G. Macdonald, *Symmetric Functions and Hall Polynomials*, Oxford University Press, 2nd edition 1995.