A resultant formula for several polynomials. Variants of Hensel's Lemma.

Juliane Deißler

February 18, 2013

Contents

Chapter 0

Introduction

Let R be a discrete valuation ring and $\pi \in R$ a generator of its maximal ideal.

In this introduction, by a polynomial we understand a monic polynomial, unless mentioned otherwise.

0.1 Gauss and Hensel

The following assertion of Hensel's Lemma is essentially found e.g. in NEUKIRCH **[8,** II.(4.6)]. Let $f(X)$ be a polynomial in $R[X]$ whose discriminant does not vanish and that splits into two factors $g_1(X), g_2(X) \in R[X]$ modulo a certain power of π; i.e. $f(X) \equiv_{\pi^s} g_1(X) \cdot g_2(X)$ for some $s \geq 1$. In addition, the images $\overline{g_1(X)}$, $\overline{g_2(X)}$ of $g_1(X)$, $g_2(X)$ under the residue class map $R[X] \to {}^{R}\!/_{\pi}[X]$ are supposed to be coprime in ${}^{R}\!/_{\pi}[X]$. Then there exist polynomials $\tilde{g}_1(X), \tilde{g}_2(X) \in R[X]$ congruent to $g_1(X)$, $g_2(X)$ modulo π^s such that $f(X) \equiv_{\pi^{2s}} \tilde{g}_1(X) \cdot \tilde{g}_2(X)$; cf. Lemma 27. Below, we will call this well-known version the "classical version of Hensel's Lemma".

Although the name "classical version of Hensel's Lemma" is obvious nowadays, historically the assertion above can be traced back to GAUSS. It is mentioned first in a manuscript that GAUSS called *Disquisitiones Generales de Congruentiis* **[3,** §374], which was published only after his death in 1863 by RICHARD DEDEKIND.

GUENTHER FREI conjectures in *The Unpublished Section Eight* **[2,** §2.2.4] that KRONECKER was the first one who quotes Gauss's *Disquisitiones Generales de Congruentiis*. In addition, he conjectures that HERMANN KÜHNE knew Kronecker's *Grundzuege* where the *Disquisitiones Generales de Congruentiis* are mentioned. Furthermore, it would be very possible that HENSEL who was the editor of the "Crelle-Journal" at this time knew of Kühne's explanations including the relevant thoughts of GAUSS.

The first time that Hensel's Lemma appears in the papers of HENSEL is in *Neue Grundlagen der Arithmetik* **[5,** §4, p. 80] in 1904 in the following way. Let again $f(X)$ be a polynomial in $R[X]$ whose discriminant does not vanish. Let $f(X)$ be congruent to the product of two polynomials $g_1(X), g_2(X) \in R[X]$ modulo π^s with s bigger than the valuation t of the discriminant of $f(X)$. In addition, let twice the valuation of the resultant t'' of $g_1(X)$, $g_2(X)$ be smaller than the valuation

of the discriminant of $f(X)$, i.e. $2t'' < t$. Then there exist polynomials $\overset{\vee}{g}_1(X), \overset{\vee}{g}_2(X) \in R[X]$ such that $f(X) = \overset{\vee}{g}_1(X) \cdot \overset{\vee}{g}_2(X)$, such that $\overset{\vee}{g}_1(X)$ is congruent to $g_1(X)$ modulo $\pi^{s-t''}$ and such that $\overset{\vee}{g}_2(X)$ is congruent to $g_2(X)$ modulo $\pi^{s-t''}$.

Note that already in this version the resultant of the polynomials $g_1(X)$, $g_2(X)$ occurs. This version is often named Hensel-Rychlík Lemma after the Czech mathematician Karel Rychlík who published a generalised version in 1919.

The state of the art concerning Hensel's Lemma and henselian rings can be found in Ribenboim [**9**]. Historical remarks may be found in Rouquette [**10,** § 2.3]. The state of the art concerning resultants can be found in [**4,** Part III, Chapter 12, 13].

0.2 Results

In this diploma thesis we concentrate on the Hensel-Rychlík Lemma. We generalise the assertion on a polynomial that splits into two factors to an assertion on a polynomial that splits into an arbitrary number of factors; cf. § 2.2. We work directly with lifts of factorisations into several factors and avoid having to iterate factorisations into two factors. For this purpose we define the resultant for several polynomials; cf. § 1.1.

0.2.1 Resultant of several polynomials

Let S be an integral domain. We define the resultant of several polynomials in $S[X]$ analogously to the definition of the resultant of two polynomials as a determinant of a certain matrix; cf. van der Waerden, [**11,** §34]. For n polynomials $g_{(1)}(X), \ldots, g_{(n)}(X) \in S[X]$, $n \geq 1$, the resultant $\operatorname{Res}(g_{(1)}, \ldots, g_{(n)})$ is given by the determinant of the matrix $A(g_{(1)}, \ldots, g_{(n)})$ whose entries are coefficients of products of the polynomials $g_{(1)}(X), \ldots, g_{(n)}(X)$ that omit respectively one of them; cf. Definition 1.

Considering the polynomials $g_{(1)}(X), \ldots, g_{(n)}(X)$ as having coefficients in a large enough field, we state in Lemma 3 that the resultant $\operatorname{Res}(g_{(1)}, \ldots, g_{(n)})$ is also given by a product of differences of zeroes of $g_{(1)}(X), \ldots, g_{(n)}(X)$. Writing the polynomials $g_{(1)}(X), \ldots, g_{(n)}(X)$ in linear factors, i.e. $g_{(k)}(X) =: \prod_{i \in [1, \deg g_{(k)}]} (X - \gamma_{(k)i})$ for $k \in [1, n]$, this means that

$$\operatorname{Res}(g_{(1)}, \ldots, g_{(n)}) \;=\; \prod_{1 \leq k < \ell \leq n} \; \prod_{(i,j) \in [1, \deg g_{(k)}] \times [1, \deg g_{(\ell)}]} (\gamma_{(k)i} \,-\, \gamma_{(\ell)j}) \,.$$

To prove this we consider the zeroes $\gamma_{(k)i}$ for $k \in [1, n]$ and $i \in [1, \deg g_{(k)}]$ as independent variables. Then we prove the assertion for these "independent zeroes". The actual assertion then follows by specialisation of the "independent zeroes" to the actual zeroes.

In particular, we have $\operatorname{Res}(g_{(1)}\,,\, \ldots\,,\, g_{(n)}) = \prod_{1 \leq k < \ell \leq n} \operatorname{Res}(g_{(k)}\,,\, g_{(\ell)})$. Since in our application below the matrix $A(g_{(1)}, \ldots, g_{(n)})$ used in our definition of the resultant is used in a crucial way, it would not have been possible to just work with the right hand side of this equation.

In § 1.2 we give some calculation rules for the resultant of several polynomials. Moreover, we show in § 1.3 how the resultant is connected with the discrminant.

0.2.2 Applications to Hensel's Lemma

0.2.2.1 General case

Knowing the resultant of several polynomials we generalise in Theorem 17 the Hensel-Rychlík Lemma from the case that $f(X)$ splits into two factors to the case that $f(X)$ splits into an arbitrary number of factors. So assume R to be complete and let $f(X), g_{(1)}(X), \dots, g_{(n)}(X)$, $n \geq 1$, be polynomials in $R[X]$ of degree ≥ 1 such that $f(X)$ is congruent to the product of $g_{(1)}(X), \dots, g_{(n)}(X)$ modulo π^s with s bigger than twice the valuation of the resultant of $g_{(1)}(X), \dots, g_{(n)}(X)$; i.e. $f(X) \equiv_{\pi^s} \prod_{k\in[1,n]} g_{(k)}(X)$ for $s \geq 2t'' + 1$ where t'' denotes the valuation of the resultant of $g_{(1)}(X), \dots, g_{(n)}(X)$. Then there exist polynomials $\breve{g}_{(1)}(X), \dots, \breve{g}_{(n)}(X)$ in $R[X]$ congruent, respectively, to $g_{(1)}(X), \dots, g_{(n)}(X)$ modulo $\pi^{s-t''}$ such that $f(X) = \prod_{k\in[1,n]} \breve{g}_{(k)}(X)$. In addition, the polynomials $\breve{g}_{(1)}(X), \dots, \breve{g}_{(n)}(X)$ are unique.

To prove Theorem 17 we use Lemma 16 which assures that we can lift the factors $g_{(1)}(X), \dots, g_{(n)}(X)$ step by step, which also works if the underlying discrete valuation ring is not complete. Then iterating Lemma 16 and passing to the limit in a complete discrete valuation ring yields the assertion of Theorem 17.

To prove Lemma 16 we construct polynomials $\tilde{g}_{(1)}(X), \dots, \tilde{g}_{(n)}(X)$ in $R[X]$ congruent to $g_{(1)}(X), \dots, g_{(n)}(X)$ modulo $\pi^{s-t''}$ in the following way. We suppose that $\tilde{g}_{(k)}(X) = g_{(k)}(X) + \pi^{s-t''}u_{(k)}(X)$ for certain, not necessarily monic polynomials $u_{(k)}(X) \in R[X]$ and $k \in [1, n]$ and we require that $f(X)$ is congruent to the product of these polynomials $\tilde{g}_{(1)}(X), \dots, \tilde{g}_{(n)}(X)$ as asserted in Lemma 16. Then we show that, in fact, there exist polynomials $u_{(1)}(X), \dots, u_{(n)}(X)$ that satisfy this requirement. Therefor we have to solve a matrix equation containing the matrix $A(g_{(1)}, \dots, g_{(n)})$. Knowing the determinant of this matrix, namely the resultant of $g_{(1)}(X), \dots, g_{(n)}(X)$, we can assure that the equation is solvable with solution $u_{(1)}(X), \dots, u_{(n)}(X)$. The main arguments of this proof we have learnt from Koch **[7,** 4.4.3, 4.4.4, 4.4.5].

In § 2.4.1 we assume that $f(X) \equiv_{\pi^s} g_{(1)}(X) \cdot g_{(2)}(X) \cdot g_{(3)}(X)$ to compare the result of a single application of Lemma 16 to three factors with the result of two subsequent applications of Lemma 16 to two factors. We determine that both methods are essentially equally good; cf. § 2.4.1.2 and § 2.4.1.3.

0.2.2.2 Particular case $f(X) \equiv_\pi X^M$

In § 2.3 we investigate our generalisation of the Hensel-Rychlík Lemma in the case $f(X) \equiv_\pi X^M$. So assume R to be complete. Let $f(X)$ be a polynomial in $R[X]$ with $\deg f = M$ and $f(X) \equiv_\pi X^M$. Let $g_{(1)}(X), \dots, g_{(n)}(X)$, $n \geq 1$, be polynomials in $R[X]$ of degree ≥ 1 ordered such that $\deg g_{(1)} \leq \cdots \leq \deg g_{(n)}$. We denote again by t'' the valuation of the resultant of $g_{(1)}(X), \dots, g_{(n)}(X)$. Moreover, we denote by t''' the valuation of the resultant of $g_{(1)}(X), \dots, g_{(n)}(X)$ minus $\sum_{j\in[1,n-1]} \big((n-j)\deg g_{(j)} - 1\big)$. Now, let $f(X)$ be congruent to the product of $g_{(1)}(X), \dots, g_{(n)}(X)$ modulo π^s with s bigger than $t'' + t'''$; i.e. suppose that $f(X) \equiv_{\pi^s} \prod_{k\in[1,n]} g_{(k)}(X)$ for $s \geq t'' + t''' + 1$. Then there exist polynomials $\breve{g}_{(1)}(X), \dots, \breve{g}_{(n)}(X)$ in $R[X]$ congruent to $g_{(1)}(X), \dots, g_{(n)}(X)$ modulo $\pi^{s-t'''}$ such that $f(X) = \prod_{k\in[1,n]} \breve{g}_{(k)}(X)$. In

addition, the polynomials $\breve{g}_{(1)}(X), \ldots, \breve{g}_{(n)}(X)$ are unique; cf. Theorem 23.

Like in the general case, we have a Lemma which assures that we can lift the factors $g_{(1)}(X), \ldots, g_{(n)}(X)$ step by step, which also works if the underlying discrete valuation ring is not complete; cf. Lemma 22.

The proofs of Lemma 22 and Theorem 23 are similar to the respective proofs in the general case. We refrained from attempting to produce an assertion that covers both the general Lemma 16 and the more particular Lemma 22, for it probably would have obscured Lemma 16.

In § 2.4.2 we assume that $f(X) \equiv_{\pi^s} g_{(1)}(X) \cdot g_{(2)}(X) \cdot g_{(3)}(X)$, $\deg g_{(1)} \leq \deg g_{(2)} \leq \deg g_{(3)}$, to compare the result of a single application of Lemma 22 to three factors with the result of two subsequent applications of Lemma 22 to two factors. Under the present hypothesis $f(X) \equiv_\pi X^M$, we determine that the former method yields a somewhat more precise result than the latter method; cf. § 2.4.2.2.

0.2.3 Illustration of the theory

To illustrate the theory we give some examples in § 4. For that we have converted the construction of the polynomials $\tilde{g}_{(1)}(X), \ldots, \tilde{g}_{(n)}(X)$ given in the proof of Lemma 16 into an algorithm; cf. § 4.1. We consider some polynomials in the complete discrete valuation ring $\mathbb{Z}_p$ for a prime number p, apply the algorithm to these polynomials using the computer algebra system Magma [**1**] and concentrate on the current precision s and certain observables, namely the deviation, the defect and the surplus; cf. § 4.1.

As a first example, we consider the polynomial $f(X) = X^3+X^2-2X+8$ in $\mathbb{Z}[X] \subseteq \mathbb{Z}_2[X]$, which goes back to Dedekind and is also used as an example in [**7,** §3.12, Einleitung zu §4, §4.4]. We start with the initial precision $s = 3$ and the initial factorisation $g_{(1)}(X) = X$, $g_{(2)}(X) = X + 2$, $g_{(3)}(X) = X + 7$. Then we iterate the algorithm a few times and document on the one hand the development of the factors $g_{(1)}(X)$, $g_{(2)}(X)$, $g_{(3)}(X)$ during the steps 1 to 6 and on the other hand the observables mentioned above in steps 1 to 10. We observe that the defect and the surplus are constant in steps 1 to 10 and that the defect is even maximal during these steps; cf. Example 31.

In § 4.5 we make a conjecture concerning the surplus.

0.2.4 Versions of Hensel's Lemma

We already talked about the classical version of Hensel's Lemma and the Hensel-Rychlík Lemma; cf. 0.1. In § 3.2 we consider the classical version. We derive it from Lemma 16, applied to the case $n = 2$. So the classical version of Hensel's Lemma follows from the Hensel-Rychlík Lemma.

Another version we derive from Lemma 16 is given in Corollary 24. There the valuation of the resultant, appearing in Lemma 16, is suitably replaced by the valuation of the discriminant of the polynomial to be factorised. The advantage is that the factors need not be known to get that parameter, the disadvantage is a loss of precision; cf. § 3.1.

In § 3.3 we concentrate on a version called Newton-Hensel. Let again $f(X)$ be a polynomial

in $R[X]$ and let w be an element of R such that $f'(w) \neq 0$. Under certain assumptions, in particular, completeness of R, Theorem 30 asserts that there exists a unique element $\check{w}$ in R such that $\check{w}$ is a zero of the polynomial $f(X)$, i.e. $f(\check{w}) = 0$.

Again, we have a Lemma which assures that we can lift the element w in R step by step, which also works if the underlying discrete valuation ring is not complete; cf. Lemma 29.

Iterating this Lemma 29 and passing to the limit in a complete discrete valuation ring yields Theorem 30.

In § 3.3.2 we compare Newton-Hensel with Hensel-Rychlík. That means that we compare Lemma 16 with Lemma 29. The result we get is that the lifted element yielded by Lemma 16 is congruent to the lifted element yielded by Lemma 29 modulo a certain power of π.

0.3 Notations and conventions

- Given a finite set M, we denote by $|M|$ the number of its elements.
- Let $\Delta(f)$ denote the discriminant of a univariate polynomial f.
- Given a commutative ring R and $a, b, r \in R$, we write $a \equiv_r b$ or $a = b + \mathrm{O}(r)$ for $a - b \in rR$.
- Given a discrete valuation ring R and a prime element $\pi \in R$. We write $\mathrm{v}_\pi(0) := \infty$.
- Given $a, b \in \mathbb{Z}$, we write $[a, b] := \{ z \in \mathbb{Z} : a \leq z \leq b \}$ for the interval in $\mathbb{Z}$ with endpoints a and b.
- Empty entries of a matrix are zero.
- Given $n \geq 0$, the unit matrix of size $n \times n$ is denoted by E_n.
- In a proof by contradiction, the actual contradiction is marked by the symbol $\lightning$.

Chapter 1

Resultants

Let $n \in \mathbb{Z}_{\geq 1}$.

1.1 Definition of the resultant

Let R be a commutative ring.

Definition 1. Suppose given monic polynomials

$$\begin{aligned} g_{(1)} &= g_{(1)}(X) &&= \sum_{i\in[0,m_{(1)}]} g_{(1)i}X^i \\ g_{(2)} &= g_{(2)}(X) &&= \sum_{i\in[0,m_{(2)}]} g_{(2)i}X^i \\ &&&\vdots \\ g_{(n)} &= g_{(n)}(X) &&= \sum_{i\in[0,m_{(n)}]} g_{(n)i}X^i \end{aligned}$$

in $R[X]$, where $m_{(k)} := \deg g_{(k)} \geq 1$ for $k \in [1,n]$.

Denote

$$\begin{aligned} M &:= \sum_{\ell\in[1,n]} m_{(\ell)} \\ M_{(k)} &:= \sum_{\ell\in[1,n]\smallsetminus\{k\}} m_{(\ell)} = M - m_{(k)} \end{aligned}$$

and

$$\prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X) =: \sum_{i\in[0,M_{(k)}]} a_{(k)i}X^i$$

for $k \in [1,n]$.

Write

$$A(g_{(1)},\dots,g_{(n)}) \;:=\; \left(\begin{array}{ccccccc}
a_{(1)0} & \cdots & \cdots & \cdots & a_{(1)M_{(1)}} & & \\
 & \ddots & & & & \ddots & \\
 & & a_{(1)0} & \cdots & \cdots & \cdots & a_{(1)M_{(1)}} \\
a_{(2)0} & \cdots & \cdots & \cdots & a_{(2)M_{(2)}} & & \\
 & \ddots & & & & \ddots & \\
 & & a_{(2)0} & \cdots & \cdots & \cdots & a_{(2)M_{(2)}} \\
\vdots & & \vdots & & \vdots & & \vdots \\
\vdots & & \vdots & & \vdots & & \vdots \\
a_{(n)0} & \cdots & \cdots & \cdots & a_{(n)M_{(n)}} & & \\
 & \ddots & & & & \ddots & \\
 & & a_{(n)0} & \cdots & \cdots & \cdots & a_{(n)M_{(n)}}
\end{array}\right) \begin{array}{l} \left.\begin{array}{l}\\\\\end{array}\right\} m_{(1)} \text{ rows} \\ \left.\begin{array}{l}\\\\\end{array}\right\} m_{(2)} \text{ rows} \\ \\ \\ \left.\begin{array}{l}\\\\\end{array}\right\} m_{(n)} \text{ rows} \end{array} \;\in\; R^{M\times M}\,.$$

We define

$$\mathrm{Res}(g_{(1)},\dots,g_{(n)}) \;:=\; \det A(g_{(1)},\dots,g_{(n)}) \;\in\; R$$

to be the *resultant* of $g_{(1)}(X)\,,\dots,\,g_{(n)}(X)$.

1.2 A formula for the resultant in terms of zeroes

Keep the notation of §1.1, but suppose R to be an integral domain.

Let K be the field of fractions of R. Let L be a splitting field for $\prod_{k\in[1,n]} g_{(k)}(X) \in K[X]$.

Write $g_{(k)}(X) =: \prod_{i\in[1,m_{(k)}]} (X-\gamma_{(k)i})$ in $L[X]$ for $k\in[1,n]$.

Notation 2. Write

$$m^{(k)} \;:=\; \sum_{\ell\in[1,k]} m_{(\ell)}$$

and

$$I^{(k)} \;:=\; [1,m^{(k)}]$$

for $k\in[0,n]$.

Write

$$I_{(k)} \;:=\; [m^{(k-1)}+1,m^{(k)}]$$

for $k\in[1,n]$.

Note that $m^{(k)}=|I^{(k)}|$ for $k\in[0,n]$ and $m_{(k)}=|I_{(k)}|$ for $k\in[1,n]$. Note that $M=m^{(n)}$.

Lemma 3. *Recall that* $g_{(k)}(X) = \prod_{i\in[1,m_{(k)}]} (X-\gamma_{(k)i})$ *in* $L[X]$ *for* $k\in[1,n]$.

We have

$$\text{(I)}\qquad \mathrm{Res}(g_{(1)},\dots,g_{(n)}) \;=\; \prod_{1\le k<\ell\le n} \;\prod_{(i,j)\in[1,m_{(k)}]\times[1,m_{(\ell)}]} (\gamma_{(k)i}-\gamma_{(\ell)j})\,.$$

This generalises the well-known assertion in the case $n = 2$; cf. e.g. [**11,** §35].

Proof. We divide the proof into steps.

These steps are roughly described as follows.

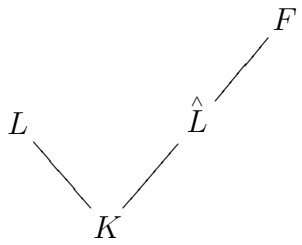
0. "Declaring" the zeroes $\gamma_{(i)j}$ of $g_{(i)}(X)$ to be independent variables $\hat{\gamma}_{(i)j}$.
1. Vanishing of the resultant if two zeroes "are identified".
2. In (I), but with the zeroes being "declared" to be independent variables, the right hand side divides the left hand side. Without this "declaration", this divisibility assertion would be meaningless.
3. Step 2 is continued with a comparison of coefficients to prove equality of the left hand side and the right hand side, still employing "declared independent zeroes".

   The actual equation (I) then follows by specialisation of the "declared independent zeroes" to the actual zeroes.

Step 0. Let

$$\hat{L} \;:=\; K[\underbrace{\hat{\gamma}_{(1)1}\,,\,\ldots\,,\,\hat{\gamma}_{(1)m_{(1)}}}\,,\underbrace{\hat{\gamma}_{(2)1}\,,\,\ldots\,,\,\hat{\gamma}_{(2)m_{(2)}}}\,,\;\;\ldots\ldots\;\,,\underbrace{\hat{\gamma}_{(n)1}\,,\,\ldots\,,\,\hat{\gamma}_{(n)m_{(n)}}}]$$

be a polynomial ring in M variables. Let F be its field of fractions.



For $\ell \in [1, n]$, let

$$\hat{g}_{(\ell)} \;=\; \hat{g}_{(\ell)}(X) \;:=\; \prod_{i\in[1,m_{(\ell)}]} (X - \hat{\gamma}_{(\ell)i}) \in \hat{L}[X].$$

For $k \in [1, n]$, denote

$$\prod_{\ell\in[1,n]\smallsetminus\{k\}} \hat{g}_{(\ell)}(X) =: \sum_{i\in[0,M_{(k)}]} \hat{a}_{(k)i} X^i\,.$$

Moreover, let

$$\hat{a}_{(k)i} := 0 \qquad \text{for } k \in [1, n] \text{ and } i \in \mathbb{Z} \smallsetminus [0, M_{(k)}].$$

Step 1. Suppose given κ, $\lambda \in [1, n]$ with $\kappa \neq \lambda$. Suppose given $\mu \in [1, m_{(\kappa)}]$ and $\nu \in [1, m_{(\lambda)}]$.

Consider the K-algebra homomorphism

$$\begin{array}{rcll}
\hat{L}[X] & \xrightarrow{\Psi} & \hat{L}[X] & \\
\hat{\gamma}_{(\kappa)\mu} & \longmapsto & \hat{\gamma}_{(\lambda)\nu} & \\
\hat{\gamma}_{(\kappa)i} & \longmapsto & \hat{\gamma}_{(\kappa)i} & \text{for } i \in [1, m_{(\kappa)}] \smallsetminus \{\mu\} \\
\hat{\gamma}_{(\ell)i} & \longmapsto & \hat{\gamma}_{(\ell)i} & \text{for } \ell \in [1, n] \smallsetminus \{\kappa\} \text{ and } i \in [1, m_{(\ell)}] \\
X & \longmapsto & X\,. &
\end{array}$$

Roughly speaking, Ψ only specialises $\hat{\gamma}_{(\kappa)\mu}$ to $\hat{\gamma}_{(\lambda)\nu}$.

We *claim* that $\mathrm{Res}(\Psi(\hat{g}_{(1)}), \ldots, \Psi(\hat{g}_{(n)})) = 0$.

> Of course, $\Psi(\hat{g}_{(\ell)}) = \hat{g}_{(\ell)}$ for $\ell \in [1,n] \smallsetminus \{\kappa\}$, but it will turn out to be convenient to apply Ψ everywhere; cf. Step 2.

Let $u(X) := \prod_{i \in [1, m_{(\lambda)}] \smallsetminus \{\nu\}} (X - \hat{\gamma}_{(\lambda)i})$. Let $v(X) := \prod_{i \in [1, m_{(\kappa)}] \smallsetminus \{\mu\}} (X - \hat{\gamma}_{(\kappa)i})$.

We have $u(X) \cdot \Psi(\hat{g}_{(\kappa)}(X)) = \big(\prod_{i \in [1, m_{(\kappa)}] \smallsetminus \{\mu\}} (X - \hat{\gamma}_{(\kappa)i}) \big) \cdot \big(\prod_{i \in [1, m_{(\lambda)}]} (X - \hat{\gamma}_{(\lambda)i}) \big) = v(X) \cdot \Psi(\hat{g}_{(\lambda)}(X))$,

and thus

$$\text{(II)} \quad u(X) \cdot \Psi\big(\hat{g}_{(\kappa)}(X) \cdot \prod_{\ell \in [1,n] \smallsetminus \{\kappa, \lambda\}} \hat{g}_{(\ell)}(X)\big) \;-\; v(X) \cdot \Psi\big(\hat{g}_{(\lambda)}(X) \cdot \prod_{\ell \in [1,n] \smallsetminus \{\kappa, \lambda\}} \hat{g}_{(\ell)}(X)\big) \;=\; 0.$$

We have

$$\Psi\Big(\prod_{\ell \in [1,n] \smallsetminus \{k\}} \hat{g}_{(\ell)}(X)\Big) \;=\; \sum_{i \in [0, M_{(k)}]} \Psi(\hat{a}_{(k)i}) X^i \qquad \text{for } k \in [1,n]\,.$$

Denote

$$\begin{aligned} u(X) &=: \sum_{i \in [0, m_{(\lambda)} - 1]} u_i X^i \\ v(X) &=: \sum_{i \in [0, m_{(\kappa)} - 1]} v_i X^i\,. \end{aligned}$$

Consider the coefficient in (II) that belongs to X^ι for $\iota \in [0, M-1]$. We have

$$\sum_{i \in [0, m_{(\lambda)} - 1]} u_i \, \Psi(\hat{a}_{(\lambda)\iota - i}) \;-\; \sum_{j \in [0, m_{(\kappa)} - 1]} v_j \, \Psi(\hat{a}_{(\kappa)\iota - j}) \;=\; 0.$$

So writing

$$U \;:=\; (0 \ldots 0 \underbrace{u_0 \ldots u_{m_{(\lambda)}-1}}_{\text{region } \lambda} 0 \ldots 0 \underbrace{-v_0 \ldots -v_{m_{(\kappa)}-1}}_{\text{region } \kappa} 0 \ldots 0)\,,$$

we have the following matrix equation with entries in F.

$$U \cdot \underbrace{\begin{pmatrix} \Psi(\hat{a}_{(1)0}) & \cdots & \cdots & \cdots & \Psi(\hat{a}_{(1)M_{(1)}}) & & \\ & \ddots & & & \ddots & & \\ & \Psi(\hat{a}_{(1)0}) & \cdots & \cdots & \cdots & \Psi(\hat{a}_{(1)M_{(1)}}) & \\ \Psi(\hat{a}_{(2)0}) & \cdots & \cdots & \cdots & \Psi(\hat{a}_{(2)M_{(2)}}) & & \\ & \ddots & & & \ddots & & \\ & \Psi(\hat{a}_{(2)0}) & \cdots & \cdots & \cdots & \Psi(\hat{a}_{(2)M_{(2)}}) & \\ \vdots & \vdots & & \vdots & \vdots & & \\ \vdots & \vdots & & \vdots & \vdots & & \\ \Psi(\hat{a}_{(n)0}) & \cdots & \cdots & \cdots & \Psi(\hat{a}_{(n)M_{(n)}}) & & \\ & \ddots & & & \ddots & & \\ & \Psi(\hat{a}_{(n)0}) & \cdots & \cdots & \cdots & \Psi(\hat{a}_{(n)M_{(n)}}) & \end{pmatrix}}_{= A(\Psi(\hat{g}_{(1)}), \ldots, \Psi(\hat{g}_{(n)}))} \;\begin{matrix} \} m_{(1)} \text{ rows} \\ \} m_{(2)} \text{ rows} \\ \\ \\ \\ \\ \} m_{(n)} \text{ rows} \end{matrix} \;=\; 0.$$

Since $u(X)$ and $v(X)$ are monic, thus nonzero, it follows that

$$\operatorname{Res}(\Psi(\hat{g}_{(1)}), \ldots, \Psi(\hat{g}_{(n)})) = \det A(\Psi(\hat{g}_{(1)}), \ldots, \Psi(\hat{g}_{(n)})) = 0.$$

This proves the *claim*.

Step 2.

Maintain the elements κ, $\lambda \in [1,n]$, $\mu \in [1, m_{(\kappa)}]$ and $\nu \in [1, m_{(\lambda)}]$ from Step 1.

By Step 1 we know that $\det A(\,\Psi(\hat{g}_{(1)}), \ldots, \Psi(\hat{g}_{(n)})\,) = \operatorname{Res}(\,\Psi(\hat{g}_{(1)}), \ldots, \Psi(\hat{g}_{(n)})\,) = 0$. Thus $\Psi(\det A(\,\hat{g}_{(1)}, \ldots, \hat{g}_{(n)}\,)) = 0$.

Consider the element $\det A(\,\hat{g}_{(1)}, \ldots, \hat{g}_{(n)}\,)$ of $\hat{L}$ as a polynomial in $\hat{\gamma}_{(\kappa)\mu}$, having coefficients in $K[\hat{\gamma}_{(1)1}, \ldots, \hat{\gamma}_{(\kappa-1)m_{(\kappa-1)}}, \hat{\gamma}_{(\kappa)1}, \ldots, \hat{\gamma}_{(\kappa)\mu-1}, \hat{\gamma}_{(\kappa)\mu+1}, \ldots, \hat{\gamma}_{(\kappa)m_{(\kappa)}}, \hat{\gamma}_{(\kappa+1)1}, \ldots, \hat{\gamma}_{(n)m_{(n)}}]$. By polynomial division, there exist polynomials $p = p(\hat{\gamma}_{(\kappa)\mu})$ and $q = q(\hat{\gamma}_{(\kappa)\mu})$ in $\hat{L}$ such that

$$\det A(\,\hat{g}_{(1)}, \ldots, \hat{g}_{(n)}\,) = (\hat{\gamma}_{(\kappa)\mu} - \hat{\gamma}_{(\lambda)\nu}) \cdot p(\hat{\gamma}_{(\kappa)\mu}) + q(\hat{\gamma}_{(\kappa)\mu})$$

and $\deg q(\hat{\gamma}_{(\kappa)\mu}) < \deg(\hat{\gamma}_{(\kappa)\mu} - \hat{\gamma}_{(\lambda)\nu}) = 1$.

Thus

$$q \in K[\hat{\gamma}_{(1)1}, \ldots, \hat{\gamma}_{(\kappa-1)m_{(\kappa-1)}}, \hat{\gamma}_{(\kappa)1}, \ldots, \hat{\gamma}_{(\kappa)\mu-1}, \hat{\gamma}_{(\kappa)\mu+1}, \ldots, \hat{\gamma}_{(\kappa)m_{(\kappa)}}, \hat{\gamma}_{(\kappa+1)1}, \ldots, \hat{\gamma}_{(n)m_{(n)}}],$$

i.e. it is constant in $\hat{\gamma}_{(\kappa)\mu}$. In particular, $\Psi(q) = q$.

Apply Ψ to the equation above.

$$\underbrace{\Psi(\det A(\,\hat{g}_{(1)}, \ldots, \hat{g}_{(n)}\,))}_{=0} = \underbrace{\Psi(\hat{\gamma}_{(\kappa)\mu} - \hat{\gamma}_{(\lambda)\nu})}_{=\hat{\gamma}_{(\lambda)\nu} - \hat{\gamma}_{(\lambda)\nu} = 0} \cdot \Psi(p(\hat{\gamma}_{(\kappa)\mu})) + \underbrace{\Psi(q)}_{=q}.$$

Hence $q = 0$. It follows that

$$\operatorname{Res}(\,\hat{g}_{(1)}, \ldots, \hat{g}_{(n)}\,) = \det A(\,\hat{g}_{(1)}, \ldots, \hat{g}_{(n)}\,) = (\hat{\gamma}_{(\kappa)\mu} - \hat{\gamma}_{(\lambda)\nu}) \cdot p(\hat{\gamma}_{(\kappa)\mu})\,.$$

Since κ, λ, μ and ν were chosen arbitrarily, we conclude that $\operatorname{Res}(\,\hat{g}_{(1)}, \ldots, \hat{g}_{(n)}\,)$ is divisible by $(\hat{\gamma}_{(k)i} - \hat{\gamma}_{(\ell)j})$ for $1 \le k < \ell \le n$ and $(i,j) \in [1, m_{(k)}] \times [1, m_{(\ell)}]$. So we obtain that

$$\underbrace{\prod_{1 \le k < \ell \le n} \prod_{(i,j) \in [1,m_{(k)}] \times [1,m_{(\ell)}]} (\hat{\gamma}_{(k)i} - \hat{\gamma}_{(\ell)j})}_{=:\ \operatorname{Res}_0(\hat{g}_{(1)}, \ldots, \hat{g}_{(n)})} \quad \text{divides} \quad \operatorname{Res}(\hat{g}_{(1)}, \ldots, \hat{g}_{(n)}),$$

since $\hat{L}$ is a unique factorisation domain; cf. **[11,** §30].

We shall show in Step 3 that $\operatorname{Res}_0(\hat{g}_{(1)}, \ldots, \hat{g}_{(n)}) = \operatorname{Res}(\hat{g}_{(1)}, \ldots, \hat{g}_{(n)})$.

Step 3.

Step 3.1. We observe that $\mathrm{Res}_0(\hat{g}_{(1)}\,,\,\ldots\,,\,\hat{g}_{(n)})$ is homogeneous of degree

$$\sum_{1\leq\, k\,<\,\ell\,\leq n} m_{(k)}m_{(\ell)} \;=:\; d\,.$$

Recall that $\hat{a}_{(k)s}$ is the coefficient of X^s in $\prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X)$ for $s\in[0,M_{(k)}]$ and zero elsewhere for $k\in[1,n]$; cf. Step 0. We have

$$\deg\hat{a}_{(k)s} \;=\; M_{(k)}-s \quad \text{for}\;\; s\,\in\,[0,M_{(k)}]\;\;\text{and}\;\;k\,\in\,[1,n].$$

Write

$$A(\,\hat{g}_{(1)}\,,\,\ldots\,,\,\hat{g}_{(n)}\,) \;=:\; (e_{s,t})_{s,t}\;\in\;\hat{L}^{M\times M}\,.$$

We *claim* that each nonzero Leibniz-summand in the determinant $\det A(\,\hat{g}_{(1)}\,,\,\ldots\,,\,\hat{g}_{(n)}\,) = \mathrm{Res}(\,\hat{g}_{(1)}\,,\,\ldots\,,\,\hat{g}_{(n)}\,)$ is homogeneous of degree d.

So consider one of them. Let $\tau\;\in\;\mathrm{S}_M$. We need to show that $e_{s,\tau(s)}$ is homogeneous and $\deg\big(\prod_{s\in[1,M]} e_{s,\tau(s)}\big)$ equals d.

If this Leibniz-summand is nonzero, then $e_{s,\tau(s)}$ is homogeneous of degree

$$\deg e_{s,\tau(s)} \;=\; \deg\hat{a}_{(k)\,\tau(s)-s+m^{(k-1)}} \;=\; M_{(k)}-\tau(s)+s-m^{(k-1)}$$

for $s\in I_{(k)}$. Thus

$$\begin{aligned}
\deg\prod_{s\in[1,M]} e_{s,\tau(s)} \;&=\; \sum_{k\in[1,n]}\deg\prod_{s\in I_{(k)}} e_{s,\tau(s)}\\
&=\; \sum_{k\in[1,n]}\sum_{s\in I_{(k)}}\deg e_{s,\tau(s)}\\
&=\; \sum_{k\in[1,n]}\sum_{s\in I_{(k)}}(M_{(k)}-\tau(s)+s-m^{(k-1)})\\
&=\; \sum_{k\in[1,n]}\sum_{s\in I_{(k)}}(M_{(k)}-m^{(k-1)})+\sum_{k\in[1,n]}\sum_{s\in I_{(k)}}(-\tau(s)+s)\\
&=\; \sum_{k\in[1,n]} m_{(k)}(M_{(k)}-m^{(k-1)})+\sum_{s\in[1,M]}(-\tau(s)+s)\\
&=\; \sum_{k\in[1,n]} m_{(k)}(M_{(k)}-m^{(k-1)})\\
&=\; \sum_{k\in[1,n]} m_{(k)}\sum_{\ell\in[k+1,n]} m_{(\ell)}\\
&=\; \sum_{k\in[1,n]}\sum_{\ell\in[k+1,n]} m_{(k)}m_{(\ell)}\\
&=\; d\,.
\end{aligned}$$

This proves the *claim*.

So we have

$$\text{(III)} \qquad \mathrm{Res}(\hat{\hat{g}}_{(1)}\,,\,\ldots\,,\,\hat{\hat{g}}_{(n)}) \;=\; C\,\cdot\,\mathrm{Res}_0(\hat{\hat{g}}_{(1)}\,,\,\ldots\,,\,\hat{\hat{g}}_{(n)})$$

for some $C \in K$.

Step 3.2. Recall that

$$\begin{aligned}\mathrm{Res}_0(\hat{\hat{g}}_{(1)},\ldots,\hat{\hat{g}}_{(n)}) &= \prod_{1\leq k<\ell\leq n}\;\prod_{(i,j)\,\in\,[1,m_{(k)}]\times[1,m_{(\ell)}]}(\hat{\hat{\gamma}}_{(k)i}\,-\,\hat{\hat{\gamma}}_{(\ell)j})\;,\\ \mathrm{Res}(\hat{\hat{g}}_{(1)},\ldots,\hat{\hat{g}}_{(n)}) &= \det A(\hat{\hat{g}}_{(1)},\ldots,\hat{\hat{g}}_{(n)})\;;\end{aligned}$$

cf. Definition 1, and that

$$\mathrm{Res}(\hat{\hat{g}}_{(1)}\,,\,\ldots\,,\,\hat{\hat{g}}_{(n)}) \;=\; C\,\cdot\,\mathrm{Res}_0(\hat{\hat{g}}_{(1)}\,,\,\ldots\,,\,\hat{\hat{g}}_{(n)})\;;$$

cf. (III). We want to show that $C \stackrel{!}{=} 1$.

To this end, we consider a certain monomial Γ in $\mathrm{Res}(\hat{\hat{g}}_{(1)},\ldots,\hat{\hat{g}}_{(n)})$ and $\mathrm{Res}_0(\hat{\hat{g}}_{(1)},\ldots,\hat{\hat{g}}_{(n)})$ and compare its coefficients in these polynomials.

Suppose given $\ell \in [1, n-1]$. Given a monomial

$$\alpha \;:=\; c\prod_{k\in[1,n]}\;\prod_{i\in[1,m_{(k)}]}\hat{\hat{\gamma}}_{(k)i}^{\,w_{(k)i}}$$

in $\hat{\hat{L}}$, where $w_{(k)i} \in \mathbb{Z}_{\geq 0}$ and $c \in K \smallsetminus \{0\}$, we let

$$\deg_{(\ell)}(\alpha) \;:=\; \sum_{i\in[1,m_{(\ell)}]} w_{(\ell)i}$$

be the (ℓ)-*degree* of α.

Now we define the degree Deg of a monomial $\beta \in \hat{\hat{L}}$ to be

$$\mathrm{Deg}(\beta) \;:=\; (\deg_{(1)}(\beta)\,,\,\ldots\,,\,\deg_{(n-1)}(\beta)) \;\in\; (\mathbb{Z}_{\geq 0})^{\times(n-1)}$$

and, for $\ell \in [0, n-1]$, the degree $\mathrm{Deg}_{(\ell)}$ of a monomial $\beta \in \hat{\hat{L}}$ to be

$$\mathrm{Deg}_{(\ell)}(\beta) \;:=\; (\deg_{(1)}(\beta)\,,\,\ldots\,,\,\deg_{(\ell)}(\beta)\,,\,0\,,\,\ldots\,,\,0) \;\in\; (\mathbb{Z}_{\geq 0})^{\times(n-1)}\;.$$

We define a lexicographical order on $(\mathbb{Z}_{\geq 0})^{\times(n-1)}$ by

$$\begin{aligned}(k_1\,,\,\ldots\,,\,k_{n-1}) \,>\, (k'_1\,,\,\ldots\,,\,k'_{n-1}) \;\;:\Leftrightarrow\;\; & (k_1 \,>\, k'_1)\\ \vee\;\; & ((k_1 \,=\, k'_1) \wedge (k_2 \,>\, k'_2))\\ \vee\;\; & ((k_1 \,=\, k'_1) \wedge (k_2 \,=\, k'_2) \wedge (k_3 \,>\, k'_3))\\ \vee\;\; & \ldots\\ \vee\;\; & ((k_i \,=\, k'_i \text{ for } i \,\in\, [1, n-2]) \wedge (k_{n-1} \,>\, k'_{n-1}))\;.\end{aligned}$$

Abbreviate

$$\Gamma_{(k)} \;:=\; \prod_{i\in[1,m_{(k)}]}\hat{\hat{\gamma}}_{(k)i}$$

for $k \in [1,n]$. We want to compare coefficients of the monomial

$$\Gamma \;:=\; \prod_{k\in[1,n]} \Gamma_{(k)}^{m^{(k-1)}}$$

in $\mathrm{Res}_0(\hat g_{(1)},\dots,\hat g_{(n)})$ and $\mathrm{Res}(\hat g_{(1)},\dots,\hat g_{(n)})$.

Note that

$$\text{(IV)} \qquad \mathrm{Deg}(\Gamma) \;=\; (\underbrace{m^{(0)}}_{=0} m_{(1)}\,,\, m^{(1)}m_{(2)}\,,\,\dots\,,\, m^{(n-2)}m_{(n-1)})\;.$$

First we consider $\mathrm{Res}_0(\hat g_{(1)},\dots,\hat g_{(n)}) = \prod_{1\le k<\ell\le n} \prod_{(i,j)\in[1,m_{(k)}]\times[1,m_{(\ell)}]} (\hat\gamma_{(k)i} - \hat\gamma_{(\ell)j})$. Its Deg-minimal monomial, including coefficient, is given by

$$\prod_{1\le k<\ell\le n} \prod_{(i,j)\in[1,m_{(k)}]\times[1,m_{(\ell)}]} (-\hat\gamma_{(\ell)j})\;,$$

for replacing any factor $(-\hat\gamma_{(\ell)j})$ therein by a factor $\hat\gamma_{(k)i}$ with $k<\ell$ strictly raises the degree Deg.

We have

$$\begin{aligned}
\prod_{1\le k<\ell\le n} \prod_{(i,j)\in[1,m_{(k)}]\times[1,m_{(\ell)}]} (-\hat\gamma_{(\ell)j}) &= (-1)^{\sum_{1\le k<\ell\le n} m_{(k)}m_{(\ell)}} \prod_{1\le k<\ell\le n} \prod_{(i,j)\in[1,m_{(k)}]\times[1,m_{(\ell)}]} \hat\gamma_{(\ell)j} \\
&= (-1)^{\sum_{1\le k<\ell\le n} m_{(k)}m_{(\ell)}} \prod_{1\le k<\ell\le n} \Gamma_{(\ell)}^{m_{(k)}} \\
&= (-1)^{\sum_{\ell\in[1,n]}\sum_{k\in[1,\ell-1]} m_{(k)}m_{(\ell)}} \prod_{\ell\in[1,n]} \prod_{k\in[1,\ell-1]} \Gamma_{(\ell)}^{m_{(k)}} \\
&= (-1)^{\sum_{\ell\in[1,n]} m^{(\ell-1)}m_{(\ell)}} \prod_{\ell\in[1,n]} \Gamma_{(\ell)}^{m^{(\ell-1)}} \\
&= (-1)^{\sum_{\ell\in[1,n]} m^{(\ell-1)}m_{(\ell)}} \Gamma\;.
\end{aligned}$$

Now consider $\mathrm{Res}(\hat g_{(1)},\dots,\hat g_{(n)}) = \det A(g_{(1)},\dots,g_{(n)})$; cf. Definition 1. Its diagonal Leibniz-summand, belonging to $\mathrm{id}\in \mathrm{S}_M$, equals

$$\prod_{k\in[1,n]} \hat a_{(k)m^{(k-1)}}^{m_{(k)}}\;.$$

Recall that

$$\sum_{j\in[0,M_{(k)}]} \hat a_{(k)j} X^j \;=\; \prod_{\ell\in[1,n]\smallsetminus\{k\}} \hat g_{(\ell)}(X) \;=\; \prod_{\ell\in[1,n]\smallsetminus\{k\}} \prod_{i\in[1,m_{(\ell)}]} (X-\hat\gamma_{(\ell)i})\;.$$

So $\hat a_{(k)m^{(k-1)}}$ equals the sum of all products of $M_{(k)} - m^{(k-1)} = \sum_{\ell\in[k+1,n]} m_{(\ell)}$ factors of the form $(-\hat\gamma_{(\ell)i})$, where $\ell\in[1,n]\smallsetminus\{k\}$ and $i\in[1,m_{(\ell)}]$. Therefore the unique Deg-minimal monomial in $\hat a_{(k)m^{(k-1)}}$, including coefficient, is

$$\prod_{\ell\in[k+1,n]} \prod_{i\in[1,m_{(\ell)}]} (-\hat\gamma_{(\ell)i})\;,$$

for replacing a factor $(-\hat{\gamma}_{(\ell)i})$ therein by a factor $(-\hat{\gamma}_{(\ell')i'})$ with $\ell' \in [1, k-1]$ and $i' \in [1, m_{(\ell')}]$ strictly raises the degree Deg.

Thus the unique Deg-minimal monomial in $\prod\limits_{k\in[1,n]} \hat{a}_{(k)m^{(k-1)}}^{m_{(k)}}$ equals

$$\begin{aligned}
\prod_{k\in[1,n]} \prod_{\ell\in[k+1,n]} \prod_{i\in[1,m_{(\ell)}]} (-\hat{\gamma}_{(\ell)i})^{m_{(k)}} &= (-1)^{\sum\limits_{k\in[1,n]} \sum\limits_{\ell\in[k+1,n]} m_{(\ell)}m_{(k)}} \prod_{k\in[1,n]} \prod_{\ell\in[k+1,n]} \prod_{i\in[1,m_{(\ell)}]} \hat{\gamma}_{(\ell)i}^{m_{(k)}} \\
&= (-1)^{\sum\limits_{k\in[1,n]} \sum\limits_{\ell\in[k+1,n]} m_{(\ell)}m_{(k)}} \prod_{k\in[1,n]} \prod_{\ell\in[k+1,n]} \Gamma_{(\ell)}^{m_{(k)}} \\
&= (-1)^{\sum\limits_{1\le k<\ell\le n} m_{(\ell)}m_{(k)}} \prod_{1\le k<\ell\le n} \Gamma_{(\ell)}^{m_{(k)}} \\
&= (-1)^{\sum\limits_{\ell\in[1,n]} \sum\limits_{k\in[1,\ell-1]} m_{(\ell)}m_{(k)}} \prod_{\ell\in[1,n]} \prod_{k\in[1,\ell-1]} \Gamma_{(\ell)}^{m_{(k)}} \\
&= (-1)^{\sum\limits_{\ell\in[1,n]} m_{(\ell)}m^{(\ell-1)}} \prod_{\ell\in[1,n]} \Gamma_{(\ell)}^{m^{(\ell-1)}} \\
&= (-1)^{\sum\limits_{\ell\in[1,n]} m^{(\ell-1)}m_{(\ell)}} \Gamma \, .
\end{aligned}$$

So we have to show that the monomial Γ does not appear in another Leibniz-summand.

Recall that

$$A(\hat{g}_{(1)}, \ldots, \hat{g}_{(n)}) \;=\; (e_{s,t})_{s,t} \;\in\; \hat{L}^{M\times M} \, .$$

Suppose given $\tau \in \mathrm{S}_M$. Suppose that its Leibniz-summand $\prod\limits_{i\in[1,M]} e_{i,\tau(i)}$ in $\det A(\hat{g}_{(1)}, \ldots, \hat{g}_{(n)})$ contains a nonzero monomial $\tilde{\Gamma}$ that has degree

$$\text{(V)} \qquad \mathrm{Deg}(\tilde{\Gamma}) \;\le\; \mathrm{Deg}(\Gamma) \overset{\text{(IV)}}{=} (\underbrace{m^{(0)}}_{=0} m_{(1)}, m^{(1)}m_{(2)}, \ldots, m^{(n-2)}m_{(n-1)}) \, .$$

It suffices to show that $\tau \overset{!}{=} \mathrm{id}$.

> Note that then even $\tilde{\Gamma} = \Gamma$ will ensue by Deg-minimality of Γ as a monomial in the Leibniz-summand for id.

For $k \in [0, n-1]$, we denote by $\tilde{\Gamma}^{(k)}$ the subproduct of $\tilde{\Gamma}$ that consists of those factors of $\tilde{\Gamma}$ that appear as monomials in $e_{i,\tau(i)}$ for $i \in I^{(k)}$. Let $\tilde{\Gamma}^{(-1)} := 1$. So $\tilde{\Gamma}^{(-1)} = \tilde{\Gamma}^{(0)} = 1$.

We prove by *induction* on $k \in [0, n-1]$ that

1. $\tau(s) = s$ for $s \in I^{(k)}$,
2. $\tau(s) \ge s$ for $s \in I_{(k+1)}$,
3. $\mathrm{Deg}_{(k)}(\tilde{\Gamma}^{(k-1)}) = \mathrm{Deg}_{(k)}(\Gamma)$.

Putting $k = n-1$ then yields $\tau = \mathrm{id}$. In fact, *assume* that $\tau \neq \mathrm{id}$. Let $s' \in [1, M]$ be minimal such that $\tau(s') \neq s'$. Then $\tau(s') > s'$, and $\tau(s) = s$ for $s \in [1, s'-1]$. So there exists $s'' \in [s'+1, M]$ such that $\tau(s'') = s'$. But $s'' \overset{2.}{\le} \tau(s'') = s' < s''$, $\lightning$.

Base clause for $k = 0$:

We have $I^{(0)} = \emptyset$. We have $\mathrm{Deg}_{(0)}(\tilde{\Gamma}^{(-1)}) = (0, \dots, 0) = \mathrm{Deg}_{(0)}(\Gamma)$.

We have $\tau(s) \geq s$ for $s \in I_{(1)}$, since $e_{i,j} = 0$ for $i \in I_{(1)}$ and $j \in [1, i-1]$.

Induction step :

Suppose given $k \in [0, n-2]$. By induction assumption, we have

1. $\tau(s) = s$ for $s \in I^{(k)}$,
2. $\tau(s) \geq s$ for $s \in I_{(k+1)}$,
3. $\mathrm{Deg}_{(k)}(\tilde{\Gamma}^{(k-1)}) = \mathrm{Deg}_{(k)}(\Gamma)$.

We have

$$\mathrm{Deg}_{(k)}(\tilde{\Gamma}^{(k)}) \leq \mathrm{Deg}_{(k)}(\tilde{\Gamma}) \overset{\text{(V)}}{\leq} \mathrm{Deg}_{(k)}(\Gamma) \overset{3.}{=} \mathrm{Deg}_{(k)}(\tilde{\Gamma}^{(k-1)}) \leq \mathrm{Deg}_{(k)}(\tilde{\Gamma}^{(k)}) \ ,$$

whence

$$\text{(VI)} \qquad \mathrm{Deg}_{(k)}(\tilde{\Gamma}^{(k)}) = \mathrm{Deg}_{(k)}(\tilde{\Gamma}) = \mathrm{Deg}_{(k)}(\Gamma) \ .$$

We have to show that

1! $\tau(s) \overset{!}{=} s$ for $s \in I^{(k+1)}$,

2! $\tau(s) \overset{!}{\geq} s$ for $s \in I_{(k+2)}$,

3! $\mathrm{Deg}_{(k+1)}(\tilde{\Gamma}^{(k)}) \overset{!}{=} \mathrm{Deg}_{(k+1)}(\Gamma)$.

Using (VI), it suffices to show that

1! $\tau(s) \overset{!}{=} s$ for $s \in I_{(k+1)}$,

2! $\tau(s) \overset{!}{\geq} s$ for $s \in I_{(k+2)}$,

3! $\deg_{(k+1)}(\tilde{\Gamma}^{(k)}) \overset{!}{=} \deg_{(k+1)}(\Gamma)$.

We consider 3! first.

We *claim* that

$$(-1)^{Mm^{(k)} - \sum\limits_{\ell \in [1,k]} m^{(\ell)} m_{(\ell)}} \prod_{i \in [1,k]} \Big(\prod_{j \in [i+1,n]} \Gamma_{(j)} \Big)^{m_{(i)}} \overset{!}{=} \tilde{\Gamma}^{(k)} \ ,$$

i.e. that

$$(-1)^{\sum\limits_{\ell \in [1,k]} (M - m^{(\ell)}) m_{(\ell)}} (\Gamma_{(2)} \Gamma_{(3)} \cdots \Gamma_{(n)})^{m_{(1)}} \cdot (\Gamma_{(3)} \cdots \Gamma_{(n)})^{m_{(2)}} \cdot \ldots \cdot (\Gamma_{(k+1)} \cdots \Gamma_{(n)})^{m_{(k)}} \overset{!}{=} \tilde{\Gamma}^{(k)} \ .$$

We prove by *induction* on $\ell \in [1, k]$ that for $i \in I_{(\ell)}$, the monomial of $e_{i,\tau(i)} \overset{1.}{=} e_{i,i} = \hat{a}_{(\ell) m^{(\ell-1)}}$ that appears as a factor in $\tilde{\Gamma}$ equals $(-1)^{M - m^{(\ell)}} \Gamma_{(\ell+1)} \cdots \Gamma_{(n)}$.

This "inner" *induction* is needed to prove the claim, which in turn is part of the *induction step* of the "outer" *induction*.

Since $|I_{(\ell)}| = m_{(\ell)}$ for $\ell \in [1,k]$, this then will prove the claim.

Base clause $\ell = 1$:

Since $\hat{a}_{(1),m^{(0)}}$ is the constant coefficient of the polynomial

$$\prod_{\kappa\in[2,n]} \hat{g}_{(\kappa)}(X) \;=\; \prod_{\kappa\in[2,n]} \prod_{j\in[1,m_{(\kappa)}]} (X - \hat{\gamma}_{(\kappa)j}) \,,$$

it consists of only one summand, namely $(-1)^{M-m^{(1)}}\Gamma_{(2)}\cdots\Gamma_{(n)}$.

Induction step :

Suppose given $\ell \in [1, k-1]$.

Since, by induction assumption, $(-1)^{M-m^{(\lambda)}}\Gamma_{(\lambda+1)}\cdots\Gamma_{(n)}$ is the monomial of $\hat{a}_{(\lambda)m^{(\lambda-1)}}$ that appears as a factor in $\tilde{\Gamma}$ with multiplicity $m_{(\lambda)}$ for $\lambda \in [1, \ell-1]$, we have

$$\begin{aligned}
\tilde{\Gamma}^{(\ell-1)} &= \prod_{\lambda\in[1,\ell-1]} \big((-1)^{M-m^{(\lambda)}}\Gamma_{(\lambda+1)}\cdots\Gamma_{(n)}\big)^{m_{(\lambda)}} \\
&= (-1)^{\sum_{\lambda\in[1,\ell-1]}(M-m^{(\lambda)})m_{(\lambda)}} \big(\prod_{\lambda\in[1,\ell-1]} \big(\Gamma_{(\lambda+1)}\cdots\Gamma_{(\ell)}\big)^{m_{(\lambda)}}\big) \cdot \big(\prod_{\lambda\in[1,\ell-1]} \big(\Gamma_{(\ell+1)}\cdots\Gamma_{(n)}\big)^{m_{(\lambda)}}\big) \\
&= (-1)^{\sum_{\lambda\in[1,\ell-1]}(M-m^{(\lambda)})m_{(\lambda)}} \big(\Gamma_{(1)}^{m_{(1)}^{(0)}}\Gamma_{(2)}^{m_{(2)}^{(1)}}\cdots\Gamma_{(\ell)}^{m_{(\ell)}^{(\ell-1)}}\big) \cdot \big(\prod_{\lambda\in[1,\ell-1]} \big(\Gamma_{(\ell+1)}\cdots\Gamma_{(n)}\big)^{m_{(\lambda)}}\big),
\end{aligned}$$

whence

$$\deg_{(\lambda)}(\tilde{\Gamma}^{(\ell-1)}) \;=\; \deg_{(\lambda)}(\Gamma_{(\lambda)}^{m^{(\lambda-1)}}) \;=\; m^{(\lambda-1)}m_{(\lambda)} \;=\; \deg_{(\lambda)}(\Gamma)$$

for $\lambda \in [1, \ell-1]$.

Suppose given $i \in I_{(\ell)}$. Let φ be the monomial of $e_{i,\tau(i)} = e_{i,i} = \hat{a}_{(\ell)m^{(\ell-1)}}$ that appears as a factor in $\tilde{\Gamma}$. We have to show that $\varphi \stackrel{!}{=} (-1)^{M-m^{(\ell)}}\Gamma_{(\ell+1)}\cdots\Gamma_{(n)}$.

Suppose given $\lambda \in [1, \ell-1]$. Since $\mathrm{Deg}_{(k)}(\tilde{\Gamma}) = \mathrm{Deg}_{(k)}(\Gamma)$ by (VI), we in particular have $\deg_{(\lambda)}(\tilde{\Gamma}) = \deg_{(\lambda)}(\Gamma)$. Since $\deg_{(\lambda)}(\tilde{\Gamma}^{(\ell-1)}) = \deg_{(\lambda)}(\Gamma)$ by the consideration above, the monomial φ is not divisible by $\hat{\gamma}_{(\lambda)j}$ for $j \in [1, m_{(\lambda)}]$.

Recall that $\hat{a}_{(\ell)m^{(\ell-1)}}$ is the coefficient of $X^{m^{(\ell-1)}}$ of the polynomial

$$\prod_{\kappa\in[1,n]\smallsetminus\{\ell\}} \hat{g}_{(\kappa)}(X) \;=\; \prod_{\kappa\in[1,n]\smallsetminus\{\ell\}} \prod_{j\in[1,m_{(\kappa)}]} (X - \hat{\gamma}_{(\kappa)j}) \,.$$

Expanding this polynomial, the terms contributing to φ may not contain a factor $(-\hat{\gamma}_{(\kappa)j})$ with $\kappa \in [1, \ell-1]$. Thus the only term that contributes to φ is

$$\big(\prod_{\kappa\in[1,\ell-1]} \prod_{j\in[1,m_{(\kappa)}]} X\big) \cdot \big(\prod_{\kappa\in[\ell+1,n]} \prod_{j\in[1,m_{(\kappa)}]} (-\hat{\gamma}_{(\kappa)j})\big) \;=\; X^{m^{(\ell-1)}} \cdot (-1)^{M-m^{(\ell)}}\Gamma_{(\ell+1)}\cdots\Gamma_{(n)} \,,$$

whence the result for φ.

This concludes the *induction* needed for our claim and thus proves this *claim*.

Taking $(k+1)$-degrees, this claim yields

$$\begin{aligned}\deg_{(k+1)}(\tilde{\Gamma}^{(k)}) &= \deg_{(k+1)}\big((\Gamma_{(2)}\Gamma_{(3)}\cdots\Gamma_{(n)})^{m_{(1)}}\cdot(\Gamma_{(3)}\cdots\Gamma_{(n)})^{m_{(2)}}\cdot\ldots\cdot(\Gamma_{(k+1)}\cdots\Gamma_{(n)})^{m_{(k)}}\big)\\ &= \deg_{(k+1)}(\Gamma_{(k+1)}^{m_{(1)}+\cdots+m_{(k)}})\\ &= m^{(k)}m_{(k+1)}\\ &\overset{\text{(IV)}}{=} \deg_{(k+1)}(\Gamma)\,.\end{aligned}$$

So assertion 3! is shown.

We prove 2! in a stronger form, which will be needed for the proof of 1! later on.

Suppose given $x\in[1,n-k-1]$. Suppose given $s\in I_{(k+1+x)}$.

Let φ be the monomial of $e_{s,\tau(s)}$ that appears as a factor in $\tilde{\Gamma}$.

Since $\mathrm{Deg}_{(k)}(\tilde{\Gamma}^{(k)})\overset{\text{(VI)}}{=}\mathrm{Deg}_{(k)}(\tilde{\Gamma})$, we have $\deg_{(\ell)}(\varphi)=0$ for $\ell\in[1,k]$.

Since $\deg_{(k+1)}(\Gamma)\overset{\text{(V),(VI)}}{\geq}\deg_{(k+1)}(\tilde{\Gamma})\geq\deg_{(k+1)}(\tilde{\Gamma}^{(k)})\overset{3!}{=}\deg_{(k+1)}(\Gamma)$, we have $\deg_{(k+1)}(\tilde{\Gamma})=\deg_{(k+1)}(\tilde{\Gamma}^{(k)})$. Thus $\deg_{(k+1)}(\varphi)=0$.

Altogether, $\deg_{(\ell)}(\varphi)=0$ for $\ell\in[1,k+1]$.

Note that $e_{s,\tau(s)}=\hat{a}_{(k+1+x)\,\tau(s)-s+m^{(k+x)}}$ is the coefficient of $X^{\tau(s)-s+m^{(k+x)}}$ in

$$\prod_{\kappa\in[1,n]\smallsetminus\{k+1+x\}}\hat{g}_{(\kappa)}(X)\;=\;\prod_{\kappa\in[1,n]\smallsetminus\{k+1+x\}}\;\prod_{j\in[1,m_{(\kappa)}]}(X-\hat{\gamma}_{(\kappa)j})\,.$$

Expanding this polynomial, we see that φ is a monomial of a coefficient of

$$\Big(\prod_{\kappa\in[1,k+1]}\;\prod_{j\in[1,m_{(\kappa)}]}X\Big)\cdot\Big(\prod_{\kappa\in[k+2,n]\smallsetminus\{k+1+x\}}\;\prod_{j\in[1,m_{(\kappa)}]}(X-\hat{\gamma}_{(\kappa)j})\Big)\,.$$

In particular, $\tau(s)-s+m^{(k+x)}\geq m^{(k+1)}$. This is equivalent to

$$\text{(VII)}\qquad\qquad \tau(s)\;\geq\;s-m^{(k+x)}+m^{(k+1)}.$$

For $x=1$, assertion 2! is shown.

Now we do 1! by proof of contradiction. *Assume* that $\tau(s_1)\neq s_1$ for some $s_1\in I_{(k+1)}$. There exists $s_0\in I_{(k+1)}$ such that $\tau(s)=s$ for $s\in[1,s_0-1]$ and $\tau(s_0)>s_0$; cf. 2.

Let $\tilde{s}:=\tau^{-1}(s_0)$. Then $\tau(\tilde{s})=s_0$. We have $\tilde{s}\in[s_0+1,M]$; cf. 1.

If $\tilde{s}\in[s_0+1,m^{(k+1)}]\subseteq I_{(k+1)}$, then it follows that $s_0=\tau(\tilde{s})\overset{2.}{\geq}\tilde{s}\geq s_0+1$, $\lightning$.

If $\tilde{s}\in I_{(k+1+x)}$ for some $x\in[1,n-k-1]$, then it follows that

$$m^{(k+1)}\geq s_0=\tau(\tilde{s})\overset{\text{(VII)}}{\geq}\tilde{s}-m^{(k+x)}+m^{(k+1)}\geq(m^{(k+x)}+1)-m^{(k+x)}+m^{(k+1)}=m^{(k+1)}+1,\;\lightning\,.$$

So $\tau(s)=s$ for $s\in I_{(k+1)}$ and 1! is shown.

This concludes the *induction*.

So $\tilde{\Gamma} = \Gamma$ is shown. This proves that Γ appears only in the diagonal Leibniz-summand of $\det A(\hat{g}_{(1)}, \ldots, \hat{g}_{(n)}) = \mathrm{Res}(\hat{g}_{(1)}, \ldots, \hat{g}_{(n)})$. This then proves that $C = 1$, i.e. that

$$\mathrm{Res}(\hat{g}_{(1)}, \ldots, \hat{g}_{(n)}) \;=\; \mathrm{Res}_0(\hat{g}_{(1)}, \ldots, \hat{g}_{(n)}) \,.$$

Step 3.3. To obtain the statement of the lemma, we apply the K-algebra homomorphism

$$\begin{array}{rcl} \hat{L} & \stackrel{\rho}{\longrightarrow} & L \\ \hat{\gamma}_{(x)\kappa} & \longmapsto & \gamma_{(x)\kappa} \quad \text{for } x \in [1,n] \text{ and } \kappa \in [1, m_{(x)}] \end{array}$$

to the preceding equation. So

$$\begin{array}{rcl} \mathrm{Res}(g_{(1)}\,,\,\ldots\,,\,g_{(n)}) & = & \rho(\mathrm{Res}(\hat{g}_{(1)}\,,\,\ldots\,,\,\hat{g}_{(n)})) \\ & = & \rho(\mathrm{Res}_0(\hat{g}_{(1)}\,,\,\ldots\,,\,\hat{g}_{(n)})) \\ & = & \mathrm{Res}_0(g_{(1)}\,,\,\ldots\,,\,g_{(n)}) \\ & = & \displaystyle\prod_{1 \le k < \ell \le n} \; \prod_{(i,j) \in [1, m_{(k)}] \times [1, m_{(\ell)}]} (\gamma_{(k)i} - \gamma_{(\ell)j}). \end{array}$$

□

Corollary 4. *Recall that $g_{(1)}(X)\,,\,\ldots\,,\,g_{(n)}(X) \in R[X]$ are monic polynomials.*

We have

$$\mathrm{Res}(g_{(1)}\,,\,\ldots\,,\,g_{(n)}) \;=\; \prod_{1 \le k < \ell \le n} \mathrm{Res}(g_{(k)}\,,\,g_{(\ell)})$$

Proof. Recall that $g_{(i)}(X) = \displaystyle\prod_{j \in [1, m_{(i)}]} (X - \gamma_{(i)j})$ in $L[X]$.

By Lemma 3 we have

$$\begin{array}{rcl} \mathrm{Res}(g_{(1)}\,,\,\ldots\,,\,g_{(n)}) & = & \displaystyle\prod_{1 \le k < \ell \le n} \; \prod_{(i,j) \in [1, m_{(k)}] \times [1, m_{(\ell)}]} (\gamma_{(k)i} - \gamma_{(\ell)j}) \\ & = & \displaystyle\prod_{1 \le k < \ell \le n} \mathrm{Res}(g_{(k)}\,,\,g_{(\ell)}) \,. \end{array}$$

□

Remark 5. *Recall that $g_{(1)}(X)\,,\,\ldots\,,\,g_{(n)}(X) \in R[X]$ are monic polynomials.*

For $1 \le p < q \le n$, we have

$$\begin{array}{rcl} \mathrm{Res}(g_{(1)}, \ldots, g_{(p)}, \ldots, g_{(q)}, \ldots, g_{(n)}) & = & (-1)^{m_{(p)} m_{(q)} + \sum\limits_{\ell \in [p+1,\, q-1]} m_{(\ell)} (m_{(p)} + m_{(q)})} \\ & & \cdot\, \mathrm{Res}(g_{(1)}, \ldots, g_{(q)}, \ldots, g_{(p)}, \ldots, g_{(n)}) \,. \end{array}$$

Proof. By Lemma 3 we have

$$\mathrm{Res}(g_{(1)},\dots,g_{(p)},\dots,g_{(q)},\dots,g_{(n)})$$

$$\begin{aligned}
&\overset{\text{L 3}}{=} \prod_{1\le k<\ell\le n}\ \prod_{(i,j)\in[1,m_{(k)}]\times[1,m_{(\ell)}]}(\gamma_{(k)i}-\gamma_{(\ell)j})\\
&= \prod_{1\le k<\ell\le p-1}\ \prod_{(i,j)\in[1,m_{(k)}]\times[1,m_{(\ell)}]}(\gamma_{(k)i}-\gamma_{(\ell)j})\cdot\prod_{p+1\le k<\ell\le q-1}\ \prod_{(i,j)\in[1,m_{(k)}]\times[1,m_{(\ell)}]}(\gamma_{(k)i}-\gamma_{(\ell)j})\\
&\quad\cdot\prod_{q+1\le k<\ell\le n}\ \prod_{(i,j)\in[1,m_{(k)}]\times[1,m_{(\ell)}]}(\gamma_{(k)i}-\gamma_{(\ell)j})\cdot\prod_{1\le k<p<\ell\le n}\ \prod_{(i,j)\in[1,m_{(k)}]\times[1,m_{(\ell)}]}(\gamma_{(k)i}-\gamma_{(\ell)j})\\
&\quad\cdot\prod_{1\le k<p}\ \prod_{(i,j)\in[1,m_{(k)}]\times[1,m_{(p)}]}(\gamma_{(k)i}-\gamma_{(p)j})\cdot\prod_{p<\ell\le q}\ \prod_{(i,j)\in[1,m_{(p)}]\times[1,m_{(\ell)}]}(\gamma_{(p)i}-\gamma_{(\ell)j})\\
&\quad\cdot\prod_{q<\ell\le n}\ \prod_{(i,j)\in[1,m_{(p)}]\times[1,m_{(\ell)}]}(\gamma_{(p)i}-\gamma_{(\ell)j})\cdot\prod_{p+1\le k<q<\ell\le n}\ \prod_{(i,j)\in[1,m_{(k)}]\times[1,m_{(\ell)}]}(\gamma_{(k)i}-\gamma_{(\ell)j})\\
&\quad\cdot\prod_{p+1\le k<q}\ \prod_{(i,j)\in[1,m_{(k)}]\times[1,m_{(q)}]}(\gamma_{(k)i}-\gamma_{(q)j})\cdot\prod_{q<\ell\le n}\ \prod_{(i,j)\in[1,m_{(q)}]\times[1,m_{(\ell)}]}(\gamma_{(q)i}-\gamma_{(\ell)j})\\
&= \prod_{1\le k<\ell\le p-1}\ \prod_{(i,j)\in[1,m_{(k)}]\times[1,m_{(\ell)}]}(\gamma_{(k)i}-\gamma_{(\ell)j})\cdot\prod_{p+1\le k<\ell\le q-1}\ \prod_{(i,j)\in[1,m_{(k)}]\times[1,m_{(\ell)}]}(\gamma_{(k)i}-\gamma_{(\ell)j})\\
&\quad\cdot\prod_{q+1\le k<\ell\le n}\ \prod_{(i,j)\in[1,m_{(k)}]\times[1,m_{(\ell)}]}(\gamma_{(k)i}-\gamma_{(\ell)j})\cdot\prod_{1\le k<p<\ell\le n}\ \prod_{(i,j)\in[1,m_{(k)}]\times[1,m_{(\ell)}]}(\gamma_{(k)i}-\gamma_{(\ell)j})\\
&\quad\cdot\prod_{1\le k<p}\ \prod_{(i,j)\in[1,m_{(k)}]\times[1,m_{(p)}]}(\gamma_{(k)i}-\gamma_{(p)j})\\
&\quad\cdot(-1)^{\sum_{\ell\in[p+1,q]}m_{(p)}m_{(\ell)}}\cdot\prod_{p<\ell\le q}\ \prod_{(i,j)\in[1,m_{(\ell)}]\times[1,m_{(p)}]}(\gamma_{(\ell)i}-\gamma_{(p)j})\\
&\quad\cdot\prod_{q<\ell\le n}\ \prod_{(i,j)\in[1,m_{(p)}]\times[1,m_{(\ell)}]}(\gamma_{(p)i}-\gamma_{(\ell)j})\cdot\prod_{p+1\le k<q<\ell\le n}\ \prod_{(i,j)\in[1,m_{(k)}]\times[1,m_{(\ell)}]}(\gamma_{(k)i}-\gamma_{(\ell)j})\\
&\quad(-1)^{\sum_{k\in[p+1,q-1]}m_{(k)}m_{(q)}}\cdot\prod_{p+1\le k<q}\ \prod_{(i,j)\in[1,m_{(q)}]\times[1,m_{(k)}]}(\gamma_{(q)i}-\gamma_{(k)j})\\
&\quad\cdot\prod_{q<\ell\le n}\ \prod_{(i,j)\in[1,m_{(q)}]\times[1,m_{(\ell)}]}(\gamma_{(q)i}-\gamma_{(\ell)j})\\
&= (-1)^{\sum_{\ell\in[p+1,q]}m_{(p)}m_{(\ell)}}\cdot(-1)^{\sum_{k\in[p+1,q-1]}m_{(k)}m_{(q)}}\cdot\mathrm{Res}(g_{(1)},\dots,g_{(q)},\dots,g_{(p)},\dots,g_{(n)})\\
&= (-1)^{m_{(p)}m_{(q)}+\sum_{\ell\in[p+1,\,q-1]}m_{(\ell)}(m_{(p)}+m_{(q)})}\cdot\mathrm{Res}(g_{(1)},\dots,g_{(q)},\dots,g_{(p)},\dots,g_{(n)})
\end{aligned}$$

□

Remark 6. *Recall that* $g_{(1)}(X)\,,\,\ldots\,,\,g_{(n-1)}(X)\,\in\,R[X]$ *are monic polynomials.*

Let $\tilde{g}_{(n)}(X)$, $\tilde{\tilde{g}}_{(n)}(X)\,\in\,R[X]$ *be further monic polynomials.*

We have

$$\begin{aligned}&\mathrm{Res}(g_{(1)}\,,\,\ldots\,,\,g_{(n-1)}\,,\,\tilde{g}_{(n)})\cdot\mathrm{Res}(g_{(1)}\,,\,\ldots\,,\,g_{(n-1)}\,,\,\tilde{\tilde{g}}_{(n)})\\ =\;&\mathrm{Res}(g_{(1)}\,,\,\ldots\,,\,g_{(n-1)}\,,\,\tilde{g}_{(n)}\tilde{\tilde{g}}_{(n)})\cdot\mathrm{Res}(g_{(1)}\,,\,\ldots\,,\,g_{(n-1)})\,.\end{aligned}$$

Proof. Recall that K is the field of fractions of R.

Let $\tilde{L}$ be a splitting field for $\tilde{g}_{(n)}(X)\cdot\tilde{\tilde{g}}_{(n)}(X)\cdot\prod_{j\in[1,n-1]}g_{(j)}(X)\,\in\,K[X]$.

Write $\tilde{g}_{(n)}(X)\,=:\,\prod\limits_{j\in[1,\tilde{m}_{(n)}]}(X-\tilde{\gamma}_{(i)j})$ and $\tilde{\tilde{g}}_{(n)}(X)\,=:\,\prod\limits_{j\in[1,\tilde{\tilde{m}}_{(n)}]}(X-\tilde{\tilde{\gamma}}_{(i)j})$ in $L[X]$.

By Lemma 3, we have

$$\begin{aligned}&\mathrm{Res}(g_{(1)}\,,\,\ldots\,,\,g_{(n-1)}\,,\,\tilde{g}_{(n)})\cdot\mathrm{Res}(g_{(1)}\,,\,\ldots\,,\,g_{(n-1)}\,,\,\tilde{\tilde{g}}_{(n)})\\ =\;&\prod_{1\le k<\ell\le n-1}\;\prod_{(i,j)\,\in\,[1,m_{(k)}]\times[1,m_{(\ell)}]}(\gamma_{(k)i}\,-\,\gamma_{(\ell)j})\cdot\prod_{1\le k\le n-1}\;\prod_{(i,j)\,\in\,[1,m_{(k)}]\times[1,\tilde{m}_{(n)}]}(\gamma_{(k)i}\,-\,\tilde{\gamma}_{(n)j})\\ &\cdot\prod_{1\le k<\ell\le n-1}\;\prod_{(i,j)\,\in\,[1,m_{(k)}]\times[1,m_{(\ell)}]}(\gamma_{(k)i}\,-\,\gamma_{(\ell)j})\cdot\prod_{1\le k\le n-1}\;\prod_{(i,j)\,\in\,[1,m_{(k)}]\times[1,\tilde{\tilde{m}}_{(n)}]}(\gamma_{(k)i}\,-\,\tilde{\tilde{\gamma}}_{(n)j})\\ =\;&\mathrm{Res}(g_{(1)}\,,\,\ldots\,,\,g_{(n-1)}\,,\,\tilde{g}_{(n)}\tilde{\tilde{g}}_{(n)})\cdot\mathrm{Res}(g_{(1)}\,,\,\ldots\,,\,g_{(n-1)})\,.\end{aligned}$$

□

Example 7. Recall that $g_{(1)}(X)\in R[X]$ is a monic polynomial. Suppose given $w\in R$. Then

$$\mathrm{Res}(X-w,\,g_{(1)}(X))\;=\;\prod_{i\in[1,m_{(1)}]}(w-\gamma_{(1)i})\;=\;g_{(1)}(w)\,.$$

1.3 The resultant and the discriminant

Let R be an integral domain. Let $\pi\neq 0$ be a prime element of R.

Let K be the field of fractions of R.

Corollary 8. *Let* $g_{(1)}(X)\,,\,\ldots\,,\,g_{(n)}(X)\,\in\,R[X]$ *be monic polynomials.*

Denote $m_{(k)}:=\deg(g_{(k)})$ *for* $k\in[1,n]$.

We have

$$\Delta(g_{(1)}\cdot\ldots\cdot g_{(n)})\;=\;\Big(\prod_{k\in[1,n]}\Delta(g_{(k)})\Big)\cdot\mathrm{Res}(g_{(1)},\,\ldots\,,g_{(n)})^2\,.$$

Proof. Let L be a splitting field for $\prod\limits_{k\in[1,n]}g_{(k)}(X)\,\in\,K[X]$. Write $g_{(k)}(X)\,=:\,\prod\limits_{i\in[1,m_{(k)}]}(X-\gamma_{(k)i})$, in $L[X]$, for $k\in[1,n]$.

Note that $\Delta(g_{(k)})=\prod\limits_{1\le i<j\le m_{(k)}}(\gamma_{(k)i}-\gamma_{(k)j})^2$ for $k\in[1,n]$; cf. **[11,** §33].

So

$$\begin{aligned}\Delta(g_{(1)} \cdot \ldots \cdot g_{(n)}) \\ &= \Big(\prod_{k\in[1,n]} \prod_{1\le i<j\le m_{(k)}} (\gamma_{(k)i} - \gamma_{(k)j})^2\Big) \cdot \Big(\prod_{1\le k<\ell\le n} \prod_{(i,j)\in[1,m_{(k)}]\times[1,m_{(\ell)}]} (\gamma_{(k)i} - \gamma_{(\ell)j})^2\Big) \\ &\overset{\text{Lem. 3}}{=} \Big(\prod_{k\in[1,n]} \Delta(g_{(k)})\Big) \cdot \mathrm{Res}(g_{(1)}, \ldots, g_{(n)})^2 .\end{aligned}$$

□

Remark 9. *Let $r \in R$. Let $f(X), \tilde{f}(X) \in R[X]$ monic polynomials such that $f(X) \equiv_r \tilde{f}(X)$. Then*

$$\Delta(f) \equiv_r \Delta(\tilde{f}).$$

Proof. Write $f(X) =: \sum_{i\in[0,\mu]} f_i X^i$ and $\tilde{f}(X) =: \sum_{i\in[0,\mu]} \tilde{f}_i X^i$. By assumption, we have $f_i \equiv_r \tilde{f}_i$ for all $i \in [0,\mu]$.

By [**11,** §33], the discriminant Δ is an integer polynomial

$$P(X_0, \ldots, X_\mu) = \sum z_{\nu_0,\ldots,\nu_\mu} X_0^{\nu_0} \cdots X_\mu^{\nu_\mu} \in \mathbb{Z}[X_0, \ldots, X_\mu]$$

in the coefficients of its argument. So we have

$$\begin{aligned}\Delta(f) &= P(f_0, \ldots, f_\mu) \\ \Delta(\tilde{f}) &= P(\tilde{f}_0, \ldots, \tilde{f}_\mu)\end{aligned}$$

For each monomial that occurs in P, we get

$$\underbrace{z_{\nu_0,\ldots,\nu_\mu}}_{\in\mathbb{Z}} f_0^{\nu_0} \ldots f_\mu^{\nu_\mu} \equiv_r \underbrace{z_{\nu_0,\ldots,\nu_\mu}}_{\in\mathbb{Z}} \tilde{f}_0^{\nu_0} \ldots \tilde{f}_\mu^{\nu_\mu}.$$

So for the sum of these monomials we have

$$\Delta(f) = P(f_0, \ldots, f_\mu) \equiv_r P(\tilde{f}_0, \ldots, \tilde{f}_\mu) = \Delta(\tilde{f}).$$

□

Remark 10. *Let $f(X), g_{(1)}(X), \ldots, g_{(n)}(X) \in R[X]$ be monic polynomials with $\Delta(f) \neq 0$, such that*

$$f(X) \equiv_{\pi\Delta(f)} \prod_{k\in[1,n]} g_{(k)}(X) .$$

Then

$$2\, \mathrm{v}_\pi(\mathrm{Res}(g_{(1)}, \ldots, g_{(n)})) \le \mathrm{v}_\pi(\Delta(f)) .$$

Proof. Since $f(X) \equiv_{\pi\Delta(f)} \prod_{k\in[1,n]} g_{(k)}(X)$, we have $\Delta(f) \equiv_{\pi\Delta(f)} \Delta(\prod_{k\in[1,n]} g_{(k)})$; cf. Remark 9. Thus

$$\Delta(f) \equiv_{\pi\Delta(f)} \Delta(\prod_{k\in[1,n]} g_{(k)}) \overset{\text{C 8}}{=} \Big(\prod_{k\in[1,n]} \Delta(g_{(k)})\Big) \cdot \mathrm{Res}(g_{(1)}, \ldots, g_{(n)})^2 .$$

So there exists $x \in R$ such that

$$\big(\prod_{k\in[1,n]} \Delta(g_{(k)}) \big) \cdot \mathrm{Res}(g_{(1)}\,,\,\ldots\,,\,g_{(n)})^2 \;=\; \Delta(f) + x\pi\Delta(f) \;=\; \Delta(f)(1+x\pi).$$

Denoting $m := \mathrm{v}_\pi(\mathrm{Res}(g_{(1)}\,,\,\ldots\,,\,g_{(n)}))$, we get that π^{2m} divides the left hand side, and thus also $\Delta(f)$. Hence $2m \,\leq\, \mathrm{v}_\pi(\Delta(f))$. □

Remark 11. *Let $r \in R$.*

Let $g_{(1)}(X)\,,\,\ldots\,,\,g_{(n)}(X)\,,\,\tilde{g}_{(1)}(X)\,,\,\ldots\,,\,\tilde{g}_{(n)}(X) \,\in\, R[X]$ be monic polynomials such that

$$g_{(k)}(X) \;\equiv_r\; \tilde{g}_{(k)}(X)$$

for $k \in [1,n]$. Then

$$\mathrm{Res}(g_{(1)}\,,\,\ldots\,,\,g_{(n)}) \;\equiv_r\; \mathrm{Res}(\tilde{g}_{(1)}\,,\,\ldots\,,\,\tilde{g}_{(n)})\,.$$

Proof. Note that $\deg g_{(k)} = \deg \tilde{g}_{(k)}$ for $k \in [1,n]$. Hence

$$A(g_{(1)},\ldots,g_{(n)}) \;\equiv_r\; A(\tilde{g}_{(1)},\ldots,\tilde{g}_{(n)})\,;$$

cf. Definition 1. Taking determinants, this yields

$$\mathrm{Res}(g_{(1)}\,,\,\ldots\,,\,g_{(n)}) \;\equiv_r\; \mathrm{Res}(\tilde{g}_{(1)}\,,\,\ldots\,,\,\tilde{g}_{(n)})\,.$$

□

Chapter 2

Hensel

2.1 Linear Algebra

Let R be a discrete valuation ring.

Let $\pi \in R$ be a generator of the maximal ideal of R.

Suppose given $k \geq 1$. Suppose given $A \in R^{k \times k}$ such that $\det(A) \neq 0$.

Let $\pi^{e_1}, \ldots, \pi^{e_k}$ be the elementary divisors of A, ordered such that $0 \leq e_1 \leq e_2 \leq \cdots \leq e_k$.

Write $e := e_1 + \cdots + e_k = \mathrm{v}_\pi(\det(A))$.

Remark 12. *Suppose given $d_i \in \mathbb{Z}_{\geq 0}$ for $i \in [1,k]$ such that $d_1 \geq d_2 \geq \cdots \geq d_k$ and such that for every $i \in [1,k]$, the element π^{d_i} divides each entry in column number i of A.*

Then $e_k \leq e' := e - (d_2 + \cdots + d_k)$.

Proof. We *claim* that

$$d_k + \cdots + d_{k-j+1} \overset{!}{\leq} e_1 + \cdots + e_j \quad \text{for } j \in [1,k].$$

Suppose given $\ell \in [1,k]$.

Recall that an $\ell \times \ell$ - minor of A is the determinant of a $\ell \times \ell$ - submatrix of A.

Recall that for $i \in [1,k]$ the element π^{d_i} divides each entry in column number i of A and

$$d_k \leq d_{k-1} \leq \cdots \leq d_1 \, .$$

So the determinant of each $\ell \times \ell$ - submatrix of A is divisible by $\pi^{d_k + \cdots + d_{k-\ell+1}}$.

Recall that $\pi^{e_1}, \ldots, \pi^{e_k}$ are the elementary divisors of A. So $\prod_{i \in [1,\ell]} \pi^{e_i}$ is the greatest common divisor of the $\ell \times \ell$ - minors of A; cf. [**6,** Th. 3.9].

Since $\pi^{d_k + \cdots + d_{k-\ell+1}}$ divides all $\ell \times \ell$ - minors of A and $\prod_{i \in [1,\ell]} \pi^{e_i}$ is their greatest common divisor, it follows that $\pi^{d_k + \cdots + d_{k-\ell+1}}$ divides $\prod_{i \in [1,\ell]} \pi^{e_i}$.

Hence

$$d_k + \cdots + d_{k-\ell+1} \ \leq \ e_1 + \cdots + e_\ell$$

This proves the *claim.*

Recall that

$$e = e_1 + \cdots + e_k \ .$$

So

$$\begin{array}{rcl} e_k & = & e - (e_1 + \cdots + e_{k-1}) \\ & \underset{\text{Claim}}{\leq} & e - (d_k + \cdots + d_{k-(k-1)+1}) \\ & = & e - (d_k + \cdots + d_2) \\ & = & e' \ . \end{array}$$

□

Lemma 13.

(1) *Suppose given $y \in \pi^{e_k} R^{1\times k}$. Then there exists $x \in R^{1\times k}$ such that $xA = y$.*

(2) *Suppose given $y \in \pi^{e} R^{1\times k}$. Then there exists $x \in R^{1\times k}$ such that $xA = y$.*

(3) *Suppose given $d_i \in \mathbb{Z}_{\geq 0}$ for $i \in [1,k]$ such that $d_1 \geq d_2 \geq \cdots \geq d_k$ and such that for every $i \in [1,k]$, the element π^{d_i} divides each entry in column number i of A.*

Write $e' := \mathrm{v}_\pi(\det(A)) - (d_2 + \cdots + d_k)$. We have $e' \geq 0$.

Suppose given $y \in \pi^{e'} R^{1\times k}$. Then there exists $x \in R^{1\times k}$ such that $xA = y$.

Proof. Ad (1).

Recall that $\pi^{e_1}, \ldots, \pi^{e_k}$ are the elementary divisors of A. So there exist $S, T \in \mathrm{GL}_k(R)$ such that

$$SAT \ = \ \begin{pmatrix} \pi^{e_1} & & \\ & \ddots & \\ & & \pi^{e_k} \end{pmatrix} \ =: \ D \ .$$

Recall that $y \in \pi^{e_k} R^{1\times k}$. So $yT \in \pi^{e_k} R^{1\times k}$.

Let

$$yT \ = \ (\pi^{e_k} z_1 \, , \, \ldots \, , \, \pi^{e_k} z_k) \ \text{ for } z_i \in R, \, i \in [1,k] \ .$$

Denote

$$\tilde{x} \ := \ (\pi^{e_k - e_1} z_1 \, , \, \ldots \, , \, \pi^{e_k - e_k} z_k) \ \in \ R^{1\times k} \ .$$

So

$$\tilde{x} D \ = \ yT \ .$$

Denote $x := \tilde{x}S \in R^{1\times k}$.

Then

$$\begin{aligned} xA &= xS^{-1}DT^{-1} \\ &= \tilde{x}DT^{-1} \\ &= yTT^{-1} \\ &= y\ . \end{aligned}$$

Ad (2). Recall that $e := e_1 + \cdots + e_k$. So $e \geq e_k$.

So

$$y \in \pi^e R^{1\times k} \subseteq \pi^{e_k} R^{1\times k}\ .$$

The assertion follows with (1).

Ad (3). By Remark 12 we have $e' \geq e_k \geq 0$.

So

$$y \in \pi^{e'} R^{1\times k} \subseteq \pi^{e_k} R^{1\times k}\ .$$

The assertion follows with (1). □

Lemma 14.

(1) *Suppose given $u \geq e_k$ and $x \in R^{1\times k}$ such that $xA \in R^{1\times k}\pi^u$. Then $x \in R^{1\times k}\pi^{u-e_k}$.*

(2) *Suppose given $u \geq e$ and $x \in R^{1\times k}$ such that $xA \in R^{1\times k}\pi^u$. Then $x \in R^{1\times k}\pi^{u-e}$.*

(3) *Suppose given $d_i \in \mathbb{Z}_{\geq 0}$ for $i \in [1,k]$ such that $d_1 \geq d_2 \geq \cdots \geq d_k$ and such that for every $i \in [1,k]$, the element π^{d_i} divides each entry in column number i of A.*

Write $e' := \mathrm{v}_\pi(\det(A)) - (d_2 + \cdots + d_k)$. We have $e' \geq 0$.

Suppose given $u \geq e'$ and $x \in R^{1\times k}$ such that $xA \in R^{1\times k}\pi^u$. Then $x \in R^{1\times k}\pi^{u-e'}$.

Proof. Ad (1).

Recall that $\pi^{e_1}, \ldots, \pi^{e_k}$ are the elementary divisors of A. So there exist $S, T \in \mathrm{GL}_k(R)$ such that

$$SAT \ = \ \begin{pmatrix} \pi^{e_1} & & \\ & \ddots & \\ & & \pi^{e_k} \end{pmatrix} \ =: \ D\ .$$

Recall that $xA \in R^{1\times k}\pi^u$.

So we have

$$xA \ = \ xS^{-1}DT^{-1} \ \in \ R^{1\times k}\pi^u\ .$$

It follows that

$$xS^{-1}D \ \in \ R^{1\times k}\pi^u T \ = \ R^{1\times k}\pi^u\ .$$

Denote

$$xS^{-1} =: (z_1, \ldots, z_k) \in R^{1\times k} .$$

So

$$xS^{-1}D = (\pi^{e_1}z_1, \ldots, \pi^{e_k}z_k) \in R^{1\times k}\pi^u .$$

Recall that $e_1 \leq e_2 \leq \cdots \leq e_k$.

So for $i \in [1,k]$ it follows that

$$z_i \in R\pi^{u-e_i} \subseteq R\pi^{u-e_k} .$$

Hence

$$xS^{-1} = (z_1, \ldots, z_k) \in R^{1\times k}\pi^{u-e_k} .$$

So

$$x \in R^{1\times k}\pi^{u-e_k}S = R^{1\times k}\pi^{u-e_k} .$$

Ad (2).

Recall that $e := e_1 + \cdots + e_k$. So we have $u \geq e \geq e_k$.

By (1) it follows that $x \in R^{1\times k}\pi^{u-e_k}$.

Since $e \geq e_k$, we have

$$x \in R^{1\times k}\pi^{u-e_k} \subseteq R^{1\times k}\pi^{u-e} .$$

Ad (3).

Remark 12 yields $e' \geq e_k \geq 0$. So we have $u \geq e' \geq e_k$.

By (1) it follows that $x \in R^{1\times k}\pi^{u-e_k}$.

Since $e' \geq e_k$, we have

$$x \in R^{1\times k}\pi^{u-e_k} \subseteq R^{1\times k}\pi^{u-e'} .$$

□

2.2 Lifting factorisations

Let R be a discrete valuation ring.

Let $\pi \in R$ be a generator of the maximal ideal of R.

Remark 15 (cf. [**5,** p. 79])**.** *Let $f(X) \in R[X]$ be a monic polynomial such that $\Delta(f) \neq 0$.*

Let $n \geq 1$. Let $g_{(1)}(X), \ldots, g_{(n)}(X) \in R[X]$ be monic polynomials of degree ≥ 1.

Denote

$$t := \mathrm{v}_\pi(\Delta(f)) , \qquad t'' := \mathrm{v}_\pi(\mathrm{Res}(g_{(1)}, \ldots, g_{(n)})) .$$

Suppose that

$$f(X) \equiv_{\pi^{t+1}} \prod_{k\in[1,n]} g_{(k)}(X) .$$

Then

$$t \;\geq\; 2t'' \,.$$

Proof. Since $f(X) \equiv_{\pi^{t+1}} \prod_{k\in[1,n]} g_{(k)}(X)$ and $t+1 = \mathrm{v}_\pi(\pi\Delta(f))$, we obtain

$$2t'' \;=\; 2\,\mathrm{v}_\pi(\mathrm{Res}(g_{(1)}\,,\,\ldots\,,\,g_{(n)})) \overset{\text{R. 10}}{\leq} \mathrm{v}_\pi(\Delta(f)) \;=\; t\,.$$

□

Lemma 16 (cf. [**5,** p. 81])**.** *Recall that R is a discrete valuation ring with maximal ideal πR.*

Let $f(X) \in R[X]$ be a monic polynomial. Write $M := \deg f$.

Let $n \geq 1$. Let $g_{(1)}(X)\,,\,\ldots\,,\,g_{(n)}(X) \in R[X]$ be monic polynomials of degree ≥ 1.

Suppose that $\mathrm{Res}(g_{(1)}\,,\,\ldots\,,\,g_{(n)}) \neq 0$. *Denote* $t'' := \mathrm{v}_\pi(\mathrm{Res}(g_{(1)}\,,\,\ldots\,,\,g_{(n)}))$.

Let $s \geq 2t''+1$. Suppose that

$$f(X) \equiv_{\pi^s} \prod_{k\in[1,n]} g_{(k)}(X)\,.$$

(Note that we may replace the condition $s \geq 2t''+1$ by the condition $s > t := \mathrm{v}_\pi(\Delta(f))$ if $\Delta(f) \neq 0$; cf. Remark 15.)

(1) *There exist monic polynomials $\tilde{g}_{(1)}(X)\,,\,\ldots\,,\,\tilde{g}_{(n)}(X) \in R[X]$ such that*

$$\tilde{g}_{(k)}(X) \;\equiv_{\pi^{s-t''}}\; g_{(k)}(X) \quad \textit{for } k \in [1,n]$$

and

$$f(X) \;\equiv_{\pi^{2(s-t'')}} \prod_{k\in[1,n]} \tilde{g}_{(k)}(X)\,.$$

We call such a tuple $(\tilde{g}_{(k)}(X))_k$ of polynomials an admissible lift *of $(g_{(k)}(X))_k$ with respect to s.*

We have

$$\mathrm{v}_\pi(\mathrm{Res}(\tilde{g}_{(1)}\,,\,\ldots\,,\,\tilde{g}_{(n)})) \;=\; t''$$

for any admissible lift $(\tilde{g}_{(k)}(X))_k$ of $(g_{(k)}(X))_k$ with respect to s.

(2) *Suppose given $r \in [0, s-2t'']$.*

Suppose given monic polynomials $\tilde{g}_{(1)}(X)\,,\,\ldots\,,\,\tilde{g}_{(n)}(X)$, $\tilde{h}_{(1)}(X)\,,\,\ldots\,,\,\tilde{h}_{(n)}(X) \in R[X]$ such that

$$\tilde{g}_{(k)}(X) \;\equiv_{\pi^{s-t''}}\; g_{(k)}(X) \quad \textit{for } k \in [1,n]\,,$$
$$\tilde{h}_{(k)}(X) \;\equiv_{\pi^{s-t''}}\; g_{(k)}(X) \quad \textit{for } k \in [1,n]$$

and

$$\prod_{k\in[1,n]} \tilde{g}_{(k)}(X) \;\equiv_{\pi^{2(s-t'')-r}} \prod_{k\in[1,n]} \tilde{h}_{(k)}(X)\,.$$

Then

$$\tilde{g}_{(k)}(X) \equiv_{\pi^{2s-3t''-r}} \tilde{h}_{(k)}(X)$$

for $k \in [1,n]$.

In particular, considering the case $r = 0$*, two admissible lifts with respect to* s *as in* (1) *are mutually congruent modulo* $\pi^{2s-3t''}R[X]$.

In the following proof, we shall use the notation of Definition 1.

The arguments we have learnt from Koch, [**7,** Satz 4.4.3, Hilfssatz 4.4.4, Hilfssatz 4.4.5].

Proof. Ad (1). *Existence of admissible lift.*

We make the ansatz

$$\tilde{g}_{(k)}(X) = g_{(k)}(X) + \pi^{s-t''}u_{(k)}(X) \quad \text{for } k \in [1,n]$$

with $u_{(k)}(X) \in R[X]$ and $\deg u_{(k)} < \deg g_{(k)} = m_{(k)}$ for $k \in [1,n]$.

Thus we require that

$$\begin{aligned} f(X) &\overset{!}{\equiv}_{\pi^{2(s-t'')}} \prod_{k\in[1,n]} \tilde{g}_{(k)}(X) \\ &= \prod_{k\in[1,n]} (g_{(k)}(X) + \pi^{s-t''}u_{(k)}(X)) \\ &\equiv_{\pi^{2(s-t'')}} \prod_{k\in[1,n]} g_{(k)}(X) + \pi^{s-t''} \sum_{k\in[1,n]} u_{(k)}(X) \cdot \prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X) \,. \end{aligned}$$

Let $b(X) := \pi^{t''-s}(f(X) - \prod_{k\in[1,n]} g_{(k)}(X))$. Since $f(X) \equiv_{\pi^s} \prod_{k\in[1,n]} g_{(k)}(X)$, we get $b(X) \equiv_{\pi^{t''}} 0$.

So our requirement reads

$$b(X) \overset{!}{\equiv}_{\pi^{s-t''}} \sum_{k\in[1,n]} u_{(k)}(X) \cdot \prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X) \,.$$

Therefore it suffices to find polynomials $u_{(k)}(X) \in R[X]$ for $k \in [1,n]$ as above that satisfy the equation

$$b(X) \overset{!}{=} \sum_{k\in[1,n]} u_{(k)}(X) \cdot \prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X) \,.$$

Writing

$$\begin{aligned} b(X) &=: \sum_{i\geq 0} \beta_i X^i \\ \prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X) &=: \sum_{i\geq 0} a_{(k)i} X^i \\ u_{(k)}(X) &=: \sum_{i\geq 0} u_{(k)i} X^i \end{aligned}$$

for $k \in [1,n]$, where β_i , $a_{(k)i}$, $u_{(k)i} \in R$ for $i \geq 0$, a comparison of coefficients shows that it suffices to find

$$U := (\underbrace{u_{(1)\,0} \ldots u_{(1)\,m_{(1)}-1}}\ \underbrace{u_{(2)\,0} \ldots u_{(2)\,m_{(2)}-1}}\ \ldots\ \underbrace{u_{(n)\,0} \ldots u_{(n)\,m_{(n)}-1}}) \in R^{1\times M}$$

such that

$$U \cdot \underbrace{\begin{pmatrix}
a_{(1)0} & \cdots & \cdots & \cdots & a_{(1)M_{(1)}} & & \\
 & \ddots & & & & \ddots & \\
 & & a_{(1)0} & \cdots & \cdots & \cdots & a_{(1)M_{(1)}} \\
a_{(2)0} & \cdots & \cdots & \cdots & a_{(2)M_{(2)}} & & \\
 & \ddots & & & & \ddots & \\
 & & a_{(2)0} & \cdots & \cdots & \cdots & a_{(2)M_{(2)}} \\
\vdots & & \vdots & & \vdots & & \vdots \\
\vdots & & \vdots & & \vdots & & \vdots \\
a_{(n)0} & \cdots & \cdots & \cdots & a_{(n)M_{(n)}} & & \\
 & \ddots & & & & \ddots & \\
 & & a_{(n)0} & \cdots & \cdots & \cdots & a_{(n)M_{(n)}}
\end{pmatrix}}_{= A(g_{(1)}, \ldots, g_{(n)})}
\begin{matrix}
\left.\begin{matrix} \\ \\ \\ \end{matrix}\right\} m_{(1)} \text{ rows} \\
\left.\begin{matrix} \\ \\ \\ \end{matrix}\right\} m_{(2)} \text{ rows} \\
\\ \\ \\
\left.\begin{matrix} \\ \\ \\ \end{matrix}\right\} m_{(n)} \text{ rows}
\end{matrix}
\stackrel{!}{=} (\beta_0 \ldots \beta_{M-1}).$$

Recall that $\det A(g_{(1)}, \ldots, g_{(n)}) = \mathrm{Res}(g_{(1)}, \ldots, g_{(n)})$; cf. Definition 1. In particular, we have $t'' = \mathrm{v}_\pi(\det A(g_{(1)}, \ldots, g_{(n)}))$.

Note that $(\beta_0 \ldots \beta_{M-1}) \in \pi^{t''} R^{1\times M}$ since $b(X) \equiv_{\pi^{t''}} 0$. So U exists as required by Lemma 13.(2).

Valuation of resultant. Since $\tilde{g}_{(k)}(X) \equiv_{\pi^{s-t''}} g_{(k)}(X)$ for $k \in [1, n]$, Remark 11 implies that

$$\mathrm{Res}(\tilde{g}_{(1)}, \ldots, \tilde{g}_{(n)}) \equiv_{\pi^{s-t''}} \mathrm{Res}(g_{(1)}, \ldots, g_{(n)}) .$$

Since $s - t'' \geq t'' + 1 = \mathrm{v}_\pi(\mathrm{Res}(g_{(1)}, \ldots, g_{(n)})) + 1$, this implies

$$\mathrm{v}_\pi(\mathrm{Res}(\tilde{g}_{(1)}, \ldots, \tilde{g}_{(n)})) = \mathrm{v}_\pi(\mathrm{Res}(g_{(1)}, \ldots, g_{(n)})) = t'' .$$

Ad (2).

Writing

$$\begin{aligned} \tilde{g}_{(k)}(X) &=: g_{(k)}(X) + \pi^{s-t''} u_{(k)}(X) \\ \tilde{h}_{(k)}(X) &=: g_{(k)}(X) + \pi^{s-t''} v_{(k)}(X) \end{aligned}$$

for $k \in [1, n]$, where $u_{(k)}(X)$, $v_{(k)}(X) \in R[X]$, we obtain $\deg u_{(k)}(X) < \deg g_{(k)}(X) = m_{(k)}$, since $\tilde{g}_{(k)}(X)$ and $g_{(k)}(X)$ are monic polynomials of the same degree; likewise, we obtain $\deg v_{(k)}(X) < m_{(k)}$.

We have to show that $u_{(k)}(X) \stackrel{!}{\equiv}_{\pi^{s-2t''-r}} v_{(k)}(X)$ for $k \in [1, n]$.

We have

$$\begin{aligned}
& \prod_{k\in[1,n]} g_{(k)}(X) + \pi^{s-t''} \sum_{k\in[1,n]} u_{(k)}(X) \cdot \prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X) \\
\equiv_{\pi^{2(s-t'')}} \quad & \prod_{k\in[1,n]} (g_{(k)}(X) + \pi^{s-t''} u_{(k)}(X)) \\
= \quad & \prod_{k\in[1,n]} \tilde{g}_{(k)}(X) \\
\equiv_{\pi^{2(s-t'')-r}} \quad & \prod_{k\in[1,n]} \tilde{h}_{(k)}(X) \\
= \quad & \prod_{k\in[1,n]} (g_{(k)}(X) + \pi^{s-t''} v_{(k)}(X)) \\
\equiv_{\pi^{2(s-t'')}} \quad & \prod_{k\in[1,n]} g_{(k)}(X) + \pi^{s-t''} \sum_{k\in[1,n]} v_{(k)}(X) \cdot \prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X) \, .
\end{aligned}$$

The difference yields

$$\sum_{k\in[1,n]} (u_{(k)}(X) - v_{(k)}(X)) \cdot \prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X) \ \equiv_{\pi^{s-t''-r}} \ 0 \, .$$

Writing

$$w_{(k)}(X) \ := \ u_{(k)}(X) - v_{(k)}(X)$$

for $k \in [1,n]$, this reads

$$(*) \qquad \sum_{k\in[1,n]} w_{(k)}(X) \cdot \prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X) \ \equiv_{\pi^{s-t''-r}} \ 0 \, .$$

Writing

$$w_{(k)}(X) \ =: \ \sum_{i\geq 0} w_{(k)i} X^i$$

for $k \in [1,n]$, and

$$W \ := \ (\underbrace{w_{(1)\,0} \ \ldots \ w_{(1)\,m_{(1)}-1}}\ \underbrace{w_{(2)\,0} \ \ldots \ w_{(2)\,m_{(2)}-1}}\ \ \ldots \ \ \underbrace{w_{(n)\,0} \ \ldots \ w_{(n)\,m_{(n)}-1}}) \ \in \ R^{1\times M} \, ,$$

we have to show that $W \overset{!}{\in} \pi^{s-2t''-r} R^{1\times M}$. From $(*)$, we obtain

$$W \cdot A(g_{(1)} \, , \, \ldots \, , \, g_{(n)}) \ \in \ \pi^{s-t''-r} R^{1\times M} \, .$$

Note that $s - t'' - r \geq t'' = \mathrm{v}_\pi(\det A(g_{(1)} \, , \, \ldots \, , \, g_{(n)}))$. So we can infer by Lemma 14.(2) that $W \in \pi^{s-2t''-r} R^{1\times M}$.

□

Theorem 17. *Recall that R is a discrete valuation ring with maximal ideal πR.*

Suppose R to be complete.

Let $f(X) \in R[X]$ be a monic polynomial.

Let $n \geq 1$. Let $g_{(1)}(X) \, , \, \ldots \, , \, g_{(n)}(X) \in R[X]$ be monic polynomials of degree ≥ 1.

Suppose that $\mathrm{Res}(g_{(1)} \, , \, \ldots \, , \, g_{(n)}) \neq 0$. Denote $t'' := \mathrm{v}_\pi(\mathrm{Res}(g_{(1)} \, , \, \ldots \, , \, g_{(n)}))$.

Let $s \geq 2t'' + 1$. Suppose that

$$f(X) \equiv_{\pi^s} \prod_{k\in[1,n]} g_{(k)}(X) \, .$$

Then there exist unique monic polynomials $\overset{\vee}{g}_{(1)}(X), \ldots, \overset{\vee}{g}_{(n)}(X) \in R[X]$ *such that*

$$\overset{\vee}{g}_{(k)}(X) \equiv_{\pi^{s-t''}} g_{(k)}(X) \quad \text{for } k \in [1,n]$$

and

$$f(X) = \prod_{k\in[1,n]} \overset{\vee}{g}_{(k)}(X) .$$

(Note that we may replace the condition $s \geq 2t''+1$ *by the condition* $s > t := \mathrm{v}_\pi(\Delta(f))$ *if* $\Delta(f) \neq 0$*; cf. Remark* 15*.)*

Proof. Existence. Since R is complete, by Remark 74 it suffices to show that there exist monic polynomials $\tilde{g}_{(1)}(X), \ldots, \tilde{g}_{(n)}(X) \in R[X]$ such that

$$f(X) \equiv_{\pi^{s+1}} \prod_{k\in[1,n]} \tilde{g}_{(k)}(X) ,$$

$$\tilde{g}_{(k)}(X) \equiv_{\pi^{s-t''}} g_{(k)}(X) \quad \text{for } k \in [1,n]$$

and

$$\mathrm{v}_\pi(\mathrm{Res}(\tilde{g}_{(1)}, \ldots, \tilde{g}_{(n)})) = t'' .$$

This follows from Lemma 16.(1) since $2(s-t'') \geq s+1$.

Uniqueness. Suppose given monic polynomials $\overset{\vee}{g}_{(1)}(X), \ldots, \overset{\vee}{g}_{(n)}(X) \in R[X]$ such that

$$\overset{\vee}{g}_{(k)}(X) \equiv_{\pi^{s-t''}} g_{(k)}(X) \quad \text{for } k \in [1,n]$$

and

$$f(X) = \prod_{k\in[1,n]} \overset{\vee}{g}_{(k)}(X) ,$$

and monic polynomials $\overset{\vee}{h}_{(1)}(X), \ldots, \overset{\vee}{h}_{(n)}(X) \in R[X]$ such that

$$\overset{\vee}{h}_{(k)}(X) \equiv_{\pi^{s-t''}} g_{(k)}(X) \quad \text{for } k \in [1,n]$$

and

$$f(X) = \prod_{k\in[1,n]} \overset{\vee}{h}_{(k)}(X) .$$

We have to show that $\overset{\vee}{g}_{(k)}(X) \overset{!}{=} \overset{\vee}{h}_{(k)}(X)$ for $k \in [1,n]$.

Note that $\mathrm{v}_\pi(\mathrm{Res}(\overset{\vee}{g}_{(1)}, \ldots, \overset{\vee}{g}_{(n)})) = t'' = \mathrm{v}_\pi(\mathrm{Res}(\overset{\vee}{h}_{(1)}, \ldots, \overset{\vee}{h}_{(n)}))$ by Lemma 16.(1).

Let $s_1 := s$. Both $(\overset{\vee}{h}_{(k)}(X))_k$ and $(\overset{\vee}{g}_{(k)}(X))_k$ are admissible lifts of $(\overset{\vee}{g}_{(k)}(X))_k$ with respect to s_1 in the sense of Lemma 16.(1), since

$$\begin{array}{rll}
f(X) & \equiv_{\pi^{s_1}} & \prod_{k\in[1,n]} \overset{\vee}{g}_{(k)}(X) \\
\overset{\vee}{h}_{(k)}(X) & \equiv_{\pi^{s_1-t''}} & \overset{\vee}{g}_{(k)}(X) \quad \text{for } k \in [1,n] \\
f(X) & \equiv_{\pi^{2(s_1-t'')}} & \prod_{k\in[1,n]} \overset{\vee}{h}_{(k)}(X) \\
\overset{\vee}{g}_{(k)}(X) & \equiv_{\pi^{s_1-t''}} & \overset{\vee}{g}_{(k)}(X) \quad \text{for } k \in [1,n] \\
f(X) & \equiv_{\pi^{2(s_1-t'')}} & \prod_{k\in[1,n]} \overset{\vee}{g}_{(k)}(X) .
\end{array}$$

So Lemma 16.(2) yields

$$\overset{\vee}{h}_{(k)}(X) \equiv_{\pi^{2(s_1-t'')-t''}} \overset{\vee}{g}_{(k)}(X) \qquad \text{for } k \in [1,n].$$

The idea is to use this congruence to replace the second congruence in the array above, and to iterate this procedure.

Let $s_2 := 2(s_1 - t'')$. Note that $s_2 = s_1 + (s_1 - 2t'') > s_1$. Both $(\overset{\vee}{h}_{(k)}(X))_k$ and $(\overset{\vee}{g}_{(k)}(X))_k$ are admissible lifts of $(\overset{\vee}{g}_{(k)}(X))_k$ with respect to s_2 in the sense of Lemma 16.(1), since

$$\begin{array}{rll} f(X) & \equiv_{\pi^{s_2}} & \prod_{k\in[1,n]} \overset{\vee}{g}_{(k)}(X) \\ \overset{\vee}{h}_{(k)}(X) & \equiv_{\pi^{s_2-t''}} & \overset{\vee}{g}_{(k)}(X) \quad \text{for } k \in [1,n] \\ f(X) & \equiv_{\pi^{2(s_2-t'')}} & \prod_{k\in[1,n]} \overset{\vee}{h}_{(k)}(X) \\ \overset{\vee}{g}_{(k)}(X) & \equiv_{\pi^{s_2-t''}} & \overset{\vee}{g}_{(k)}(X) \quad \text{for } k \in [1,n] \\ f(X) & \equiv_{\pi^{2(s_2-t'')}} & \prod_{k\in[1,n]} \overset{\vee}{g}_{(k)}(X)\,. \end{array}$$

So Lemma 16.(2) yields

$$\overset{\vee}{h}_{(k)}(X) \equiv_{\pi^{2(s_2-t'')-t''}} \overset{\vee}{g}_{(k)}(X) \qquad \text{for } k \in [1,n].$$

Let $s_3 := 2(s_2 - t'')$. Note that $s_3 = s_2 + (s_2 - 2t'') > s_2 + (s_1 - 2t'') > s_2$. Continue as above.

This yields a strictly increasing sequence $(s_\ell)_{\ell\geq 1}$ of integers such that

$$\overset{\vee}{h}_{(k)}(X) \equiv_{\pi^{s_\ell-t''}} \overset{\vee}{g}_{(k)}(X) \qquad \text{for } k \in [1,n] \text{ and } \ell \geq 1.$$

Hence

$$\overset{\vee}{h}_{(k)}(X) = \overset{\vee}{g}_{(k)}(X) \qquad \text{for } k \in [1,n].$$

□

Remark 18. The case $n = 2$ of Theorem 17, i.e. the case of a factorisation of $f(X)$ into two factors $g_{(1)}(X)$ and $g_{(2)}(X)$ modulo π^s, is due to HENSEL; cf. **[5,** p. 80, 81].

Translated to our notation, he starts right away with $s > t$. He writes in the statement on **[5,** p. 80, l. 8] that $\overset{\vee}{g}_{(1)}(X)$ and $\overset{\vee}{g}_{(2)}(X)$ are "Näherungswerte" of $g_{(1)}(X)$ and $g_{(2)}(X)$. In the proof, on **[5,** p. 81, l. 7], he makes this precise and shows that actually $\overset{\vee}{g}_{(1)}(X) \equiv_{\pi^{s-t''}} g_{(1)}(X)$ and $\overset{\vee}{g}_{(2)}(X) \equiv_{\pi^{s-t''}} g_{(2)}(X)$.

2.3 Lifting factorisations in the case $f(X) \equiv_\pi X^M$

Let R be a discrete valuation ring. Let $\pi \in R$ be a generator of the maximal ideal of R.

Remark 19. *Suppose given a monic polynomial $f(X) \in R[X]$. Write $M := \deg(f)$. Suppose that $f(X) \equiv_\pi X^M$.*

Let $n \geq 1$. Let $g_{(1)}(X), \ldots, g_{(n)}(X) \in R[X]$ be monic polynomials of degree ≥ 1. Write $m_{(k)} := \deg(g_{(k)})$ for $k \in [1,n]$.

Suppose that

$$f(X) \equiv_\pi \prod_{k\in[1,n]} g_{(k)}(X) \ .$$

Then $g_{(k)}(X) \equiv_\pi X^{m_{(k)}}$ *for* $k \in [1,n]$.

Proof. Recall that R is a discrete valuation ring and $\pi \in R$ is a generator of the maximal ideal of R. So R/π is a field and $R/\pi[X]$ is a unique factorisation domain.

So we have

$$X^M \ \equiv_\pi \ \underbrace{X \cdot X \cdot \cdots \cdot X \cdot X}_{M \text{ times}} \ .$$

Note that

$$X^M \ \equiv_\pi \ f(X) \ \equiv_\pi \ \prod_{k\in[1,n]} g_{(k)}(X) \ .$$

Since we can decompose X^M in $R/\pi[X]$ only into powers of X we have

$$g_{(k)}(X) \ \equiv_\pi \ X^{a_k}$$

for $a_k \in \mathbb{Z}_{\geq 1}$ and $k \in [1,n]$.

Since for $k \in [1,n]$ the polynomials $g_{(k)}(X)$ are monic it follows that

$$a_k \ = \ \deg g_{(k)} \ =: \ m_{(k)} \quad \text{for } k \in [1,n].$$

So

$$g_{(k)}(X) \ \equiv_\pi \ X^{m_{(k)}} \quad \text{for } k \in [1,n].$$

□

Lemma 20. *Let* $\ell \geq 1$. *Let* $h_{(1)}(X), \ldots, h_{(\ell)}(X) \in R[X]$ *be monic polynomials of degree* ≥ 1.

Write $\chi_{(k)} := \deg(h_{(k)})$ *for* $k \in [1,\ell]$. *Write* $\chi := \sum_{k\in[1,\ell]} \chi_{(k)}$. *Suppose the ordering to be chosen such that* $\chi_{(1)} \leq \chi_{(2)} \leq \cdots \leq \chi_{(\ell)}$.

Suppose that $h_{(k)}(X) \equiv_\pi X^{\chi_{(k)}}$ *for* $k \in [1,\ell]$.

Write $\prod_{k\in[1,\ell]} h_{(k)}(X) =: \sum_{i\in[0,\chi]} b_i X^i$ *with* $b_i \in R$ *for* $i \in [0,\chi]$.

Then

$$\mathrm{v}_\pi(b_i) \ \geq \ \ell - \max\{\, j \in [0,\ell] \ : \ \chi_{(1)} + \cdots + \chi_{(j)} \leq i \,\}$$

for $i \in [0,\, \chi]$.

Proof. Write $h_{(k)}(X) =: \sum_{i\in[0,\chi_{(k)}]} h_{(k)i} X^i$ for $k \in [1,\ell]$, where $h_{(k)i} \in R$ for $i \in [0,\chi_{(k)}]$. We have

$$b_i \ = \ \sum_{\substack{i_{(k)}\in[0,\chi_{(k)}] \\ \text{for } k\in[1,\ell], \\ i_{(1)}+\cdots+i_{(\ell)}=i}} \ \prod_{k\in[1,\ell]} h_{(k)i_{(k)}} \ .$$

So it suffices to show that

$$\mathrm{v}_\pi\Big(\prod_{k\in[1,\ell]} h_{(k)i_{(k)}}\Big) \overset{!}{\geq} \ell - \max\{\, j\in[0,\ell] \,:\, \chi_{(1)}+\cdots+\chi_{(j)}\leq i\,\}$$

for all occurring summands. Since $\mathrm{v}_\pi(h_{(k)i_{(k)}})\geq 1$ if $i_{(k)}\in[0,\chi_{(k)}-1]$, it remains to show that for such a summand, we have

$$|\{\, k\in[1,\ell] \,:\, i_{(k)}=\chi_{(k)}\,\}| \overset{!}{\leq} \max\{\, j\in[0,\ell] \,:\, \chi_{(1)}+\cdots+\chi_{(j)}\leq i\,\}\,.$$

Assume that

$$|\{\, k\in[1,\ell] \,:\, i_{(k)}=\chi_{(k)}\,\}| > \max\{\, j\in[0,\ell] \,:\, \chi_{(1)}+\cdots+\chi_{(j)}\leq i\,\}\,,$$

whereas $i_{(1)}+\cdots+i_{(\ell)} = i$. Write $H := \{\, k\in[1,\ell] \,:\, i_{(k)}=\chi_{(k)}\,\}\subseteq[1,\ell]$.

Then $\ell\geq|H|>\max\{\, j\in[0,\ell] \,:\, \chi_{(1)}+\cdots+\chi_{(j)}\leq i\,\}$, whence $\chi_{(1)}+\cdots+\chi_{(|H|)}>i$. So

$$\begin{array}{rcll} i &=& i_{(1)}+\cdots+i_{(\ell)} & \\ &=& (\sum_{k\in H} i_{(k)}) + (\sum_{k\in[1,\ell]\smallsetminus H} i_{(k)}) & \\ &\geq& \sum_{k\in H} i_{(k)} & \\ &=& \sum_{k\in H} \chi_{(k)} & \\ &\geq& \sum_{k\in[1,|H|]} \chi_{(k)} & \qquad (\text{using } \chi_{(1)}\leq\chi_{(2)}\leq\cdots\leq\chi_{(\ell)}) \\ &>& i & \lightning \end{array}$$

□

Lemma 21. *Let $n\geq 1$. Let $g_{(1)}(X),\,\ldots\,,g_{(n)}(X)\in R[X]$ be monic polynomials of degree ≥ 1.*

We shall use the notation of Definition 1. In particular, we write $m_{(k)}=\deg(g_{(k)})$ for $k\in[1,n]$.
Assume that $\mathrm{Res}(g_{(1)},\,\ldots\,,g_{(n)}) = \det A(g_{(1)},\,\ldots\,,g_{(n)})$ is nonzero.

Suppose that $g_{(k)}(X)\equiv_\pi X^{m_{(k)}}$ for $k\in[1,n]$.

Suppose the ordering of the polynomials to be chosen such that $m_{(1)}\leq m_{(2)}\leq\cdots\leq m_{(n)}$.

Write

$$e' := \mathrm{v}_\pi\big(\mathrm{Res}(g_{(1)},\,\ldots\,,g_{(n)})\big) - \sum_{j\in[1,n-1]} \big((n-j)m_{(j)}-1\big)\,.$$

We have $e'\geq 0$.

(1) *Suppose given $y\in\pi^{e'}R^{1\times M}$. Then there exists $x\in R^{1\times M}$ such that $xA(g_{(1)},\,\ldots\,,g_{(n)})=y$.*

(2) *Suppose given $u\geq e'$ and $x\in R^{1\times M}$ such that $xA(g_{(1)},\,\ldots\,,g_{(n)})\in R^{1\times M}\pi^u$.*
Then $x\in R^{1\times M}\pi^{u-e'}$.

Proof. Recall that $\prod_{j\in[1,n]\smallsetminus\{k\}} g_{(j)}(X) =: \sum_{i\in[0,M_{(k)}]} a_{(k)i}X^i$ for $k\in[1,n]$.

Suppose given $i\in[1,M]$. Write

$$d_i := (n-1) - \max\{\, j\in[0,n-1] \,:\, m_{(1)}+\cdots+m_{(j)} \le i-1 \,\}\,.$$

Note that $d_\xi \ge d_\eta$ for $1\le\xi\le\eta\le M$. By Lemma 20, we have

$$\mathrm{v}_\pi(a_{(k)i-1}) \;\ge\; d_i$$

for $k\in[1,n]$, since the sequence of degrees of the polynomials $g_{(j)}(X)$, with $g_{(k)}(X)$ omitted, is entrywise bounded below by the sequence of degrees of the polynomials $g_{(j)}(X)$, i.e. by the sequence of the $m_{(j)}$.

It follows that

$$\mathrm{v}_\pi(a_{(k)\xi-1}) \;\ge\; d_\xi \;\ge\; d_i$$

for $k\in[1,n]$ and $\xi\in[1,i]$. Hence π^{d_i} divides column number i of $A(g_{(1)},\ldots,g_{(n)})$; cf. Definition 1.

We have

$$\begin{aligned}
&d_2+\cdots+d_M\\
&\quad= \textstyle\sum_{i\in[2,M]}\big((n-1)-\max\{\, j\in[0,n-1] \,:\, m_{(1)}+\cdots+m_{(j)}\le i-1\,\}\big)\\
&\quad= (M-1)(n-1)-\textstyle\sum_{i\in[2,M]}\max\{\, j\in[0,n-1] \,:\, m_{(1)}+\cdots+m_{(j)}\le i-1\,\}\\
&\quad= (M-1)(n-1)-\textstyle\sum_{i\in[1,M-1]}\max\{\, j\in[0,n-1] \,:\, m_{(1)}+\cdots+m_{(j)}\le i\,\}\\
&\quad= (M-1)(n-1)-\textstyle\sum_{j\in[1,n-1]} j\cdot|\,[\,m_{(1)}+\cdots+m_{(j)}\,,\,m_{(1)}+\cdots+m_{(j)}+m_{(j+1)}-1\,]\,|\\
&\quad= (M-1)(n-1)-\textstyle\sum_{j\in[1,n-1]} jm_{(j+1)}\\
&\quad= (M-1)(n-1)-\textstyle\sum_{j\in[1,n]} (j-1)m_{(j)}\\
&\quad= (M-1)(n-1)+M-\textstyle\sum_{j\in[1,n]} jm_{(j)}\\
&\quad= 1+nM-n-\textstyle\sum_{j\in[1,n]} jm_{(j)}\\
&\quad= 1+\textstyle\sum_{j\in[1,n]}\big((n-j)m_{(j)}-1\big)\\
&\quad= \textstyle\sum_{j\in[1,n-1]}\big((n-j)m_{(j)}-1\big)\,,
\end{aligned}$$

whence

$$\mathrm{v}_\pi(\det A(g_{(1)},\ldots,g_{(n)}))-(d_2+\cdots+d_M) \;=\; e'\,.$$

So assertion (1) follows by Lemma 13.(3), assertion (2) follows by Lemma 14.(3); moreover, we have $e'\ge 0$. □

Now we shall adapt Lemma 16 to our particular situation $f(X)\equiv_\pi X^M$, improving the assertions at some points. We refrain from attempting to produce an assertion that covers both Lemma 16 and Lemma 22, for it probably would have obscured Lemma 16.

Similar comments apply to Theorem 17 and Theorem 23.

Lemma 22. *Recall that R is a discrete valuation ring with maximal ideal πR.*

Let $f(X) \in R[X]$ be a monic polynomial. Write $M := \deg f$. Suppose that $f(X) \equiv_\pi X^M$.

Let $n \geq 1$. Suppose given monic polynomials $g_{(1)}(X), \ldots, g_{(n)}(X) \in R[X]$ having degree ≥ 1. Write $m_{(k)} := \deg(g_{(k)})$ for $k \in [1,n]$. Suppose the ordering to be chosen such that $m_{(1)} \leq m_{(2)} \leq \cdots \leq m_{(n)}$.

Suppose that $\mathrm{Res}(g_{(1)}, \ldots, g_{(n)}) \neq 0$. Denote

$$\begin{aligned} t'' &:= \mathrm{v}_\pi\big(\mathrm{Res}(g_{(1)}, \ldots, g_{(n)})\big) \\ t''' &:= e' := \mathrm{v}_\pi\big(\mathrm{Res}(g_{(1)}, \ldots, g_{(n)})\big) - \textstyle\sum_{j\in[1,n-1]} \big((n-j)m_{(j)} - 1\big) \end{aligned}$$

cf. Lemma 21.

Let $s \geq t'' + t''' + 1$. Suppose that

$$f(X) \equiv_{\pi^s} \prod_{k\in[1,n]} g_{(k)}(X) .$$

(Note that we may replace the condition $s \geq t'' + t''' + 1$ by the condition $s > t := \mathrm{v}_\pi(\Delta(f))$ if $\Delta(f) \neq 0$; cf. Remark 15*.)*

(1) *There exist monic polynomials $\tilde{g}_{(1)}(X), \ldots, \tilde{g}_{(n)}(X) \in R[X]$ such that*

$$\tilde{g}_{(k)}(X) \equiv_{\pi^{s-t'''}} g_{(k)}(X) \quad \text{for } k \in [1,n]$$

and

$$f(X) \equiv_{\pi^{2(s-t''')}} \prod_{k\in[1,n]} \tilde{g}_{(k)}(X) .$$

We call such a tuple $(\tilde{g}_{(k)}(X))_k$ of polynomials an admissible lift *of $(g_{(k)}(X))_k$ with respect to s.*

We have

$$\mathrm{v}_\pi(\mathrm{Res}(\tilde{g}_{(1)}, \ldots, \tilde{g}_{(n)})) = t''$$

for any admissible lift $(\tilde{g}_{(k)}(X))_k$ of $(g_{(k)}(X))_k$ with respect to s.

(2) *Suppose given $r \in [0, s-2t''']$.*

Suppose given monic polynomials $\tilde{g}_{(1)}(X), \ldots, \tilde{g}_{(n)}(X)$, $\tilde{h}_{(1)}(X), \ldots, \tilde{h}_{(n)}(X) \in R[X]$ such that

$$\begin{aligned} \tilde{g}_{(k)}(X) &\equiv_{\pi^{s-t'''}} g_{(k)}(X) \quad \text{for } k \in [1,n] , \\ \tilde{h}_{(k)}(X) &\equiv_{\pi^{s-t'''}} g_{(k)}(X) \quad \text{for } k \in [1,n] \end{aligned}$$

and

$$\prod_{k\in[1,n]} \tilde{g}_{(k)}(X) \equiv_{\pi^{2(s-t''')-r}} \prod_{k\in[1,n]} \tilde{h}_{(k)}(X) .$$

Then

$$\tilde{g}_{(k)}(X) \equiv_{\pi^{2s-3t'''-r}} \tilde{h}_{(k)}(X)$$

for $k \in [1,n]$.

In particular, considering the case $r = 0$, two admissible lifts with respect to s as in (1) *are mutually congruent modulo $\pi^{2s-3t'''}R[X]$.*

In the following proof, we shall use the notation of Definition 1.

Proof. By Remark 19, we have $g_{(k)}(X) \equiv_\pi X^{m_{(k)}}$ for $k \in [1,n]$.

Ad (1). *Existence of admissible lift.*

We make the ansatz

$$\tilde{g}_{(k)}(X) \;=\; g_{(k)}(X) + \pi^{s-t'''} u_{(k)}(X) \quad \text{for } k \in [1,n]$$

with $u_{(k)}(X) \in R[X]$ and $\deg u_{(k)} < \deg g_{(k)} = m_{(k)}$ for $k \in [1,n]$.

Thus we require that

$$\begin{aligned} f(X) \;&\overset{!}{\equiv}_{\pi^{2(s-t''')}}\; \prod_{k\in[1,n]} \tilde{g}_{(k)}(X) \\ &= \prod_{k\in[1,n]} (g_{(k)}(X) + \pi^{s-t'''} u_{(k)}(X)) \\ &\equiv_{\pi^{2(s-t''')}}\; \prod_{k\in[1,n]} g_{(k)}(X) + \pi^{s-t'''} \sum_{k\in[1,n]} u_{(k)}(X) \cdot \prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X)\,. \end{aligned}$$

Let $b(X) := \pi^{t'''-s}(f(X) - \prod_{k\in[1,n]} g_{(k)}(X))$. Since $f(X) \equiv_{\pi^s} \prod_{k\in[1,n]} g_{(k)}(X)$, we get $b(X) \equiv_{\pi^{t'''}} 0$.

So our requirement reads

$$b(X) \;\overset{!}{\equiv}_{\pi^{s-t'''}} \sum_{k\in[1,n]} u_{(k)}(X) \cdot \prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X)\,.$$

Therefore it suffices to find polynomials $u_{(k)}(X) \in R[X]$ for $k \in [1,n]$ as above that satisfy the equation

$$b(X) \;\overset{!}{=} \sum_{k\in[1,n]} u_{(k)}(X) \cdot \prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X)\,.$$

Writing

$$\begin{aligned} b(X) \;&=:\; \sum_{i\geq 0} \beta_i X^i \\ \prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X) \;&=:\; \sum_{i\geq 0} a_{(k)i} X^i \\ u_{(k)}(X) \;&=:\; \sum_{i\geq 0} u_{(k)i} X^i \end{aligned}$$

for $k \in [1,n]$, where $\beta_i\,,\, a_{(k)i}\,,\, u_{(k)i} \in R$ for $i \geq 0$, a comparison of coefficients shows that it suffices to find

$$U \;:=\; (\underbrace{u_{(1)\,0} \;\ldots\; u_{(1)\,m_{(1)}-1}}\;\; \underbrace{u_{(2)\,0} \;\ldots\; u_{(2)\,m_{(2)}-1}}\;\; \ldots \;\; \underbrace{u_{(n)\,0} \;\ldots\; u_{(n)\,m_{(n)}-1}}) \;\in\; R^{1\times M}$$

such that

$$U \cdot \underbrace{\left(\begin{array}{ccccccc}
a_{(1)0} & \cdots & \cdots & \cdots & a_{(1)M_{(1)}} & & \\
 & \ddots & & & & \ddots & \\
 & & a_{(1)0} & \cdots & \cdots & \cdots & a_{(1)M_{(1)}} \\
a_{(2)0} & \cdots & \cdots & \cdots & a_{(2)M_{(2)}} & & \\
 & \ddots & & & & \ddots & \\
 & & a_{(2)0} & \cdots & \cdots & \cdots & a_{(2)M_{(2)}} \\
\vdots & & \vdots & & \vdots & & \vdots \\
\vdots & & \vdots & & \vdots & & \vdots \\
a_{(n)0} & \cdots & \cdots & \cdots & a_{(n)M_{(n)}} & & \\
 & \ddots & & & & \ddots & \\
 & & a_{(n)0} & \cdots & \cdots & \cdots & a_{(n)M_{(n)}}
\end{array}\right)}_{= A(g_{(1)}, \ldots, g_{(n)})}
\begin{array}{l}
\left.\begin{array}{l}\\ \\ \\ \end{array}\right\} m_{(1)} \text{ rows} \\
\left.\begin{array}{l}\\ \\ \\ \end{array}\right\} m_{(2)} \text{ rows} \\
\\ \\ \\
\left.\begin{array}{l}\\ \\ \\ \end{array}\right\} m_{(n)} \text{ rows}
\end{array}
\stackrel{!}{=} (\beta_0 \ \ldots \ \beta_{M-1}).$$

Note that $(\beta_0 \ \ldots \ \beta_{M-1}) \in \pi^{t'''} R^{1\times M}$ since $b(X) \equiv_{\pi^{t'''}} 0$. So U exists as required by Lemma 21.(1).

Valuation of resultant. Since $\tilde{g}_{(k)}(X) \equiv_{\pi^{s-t'''}} g_{(k)}(X)$ for $k \in [1,n]$, Remark 11 implies that

$$\mathrm{Res}(\tilde{g}_{(1)}, \ldots, \tilde{g}_{(n)}) \equiv_{\pi^{s-t'''}} \mathrm{Res}(g_{(1)}, \ldots, g_{(n)}) .$$

Since $s - t''' \geq t'' + 1 = \mathrm{v}_\pi(\mathrm{Res}(g_{(1)}, \ldots, g_{(n)})) + 1$, this implies

$$\mathrm{v}_\pi(\mathrm{Res}(\tilde{g}_{(1)}, \ldots, \tilde{g}_{(n)})) = \mathrm{v}_\pi(\mathrm{Res}(g_{(1)}, \ldots, g_{(n)})) = t'' .$$

Ad (2).

Writing

$$\begin{aligned} \tilde{g}_{(k)}(X) &=: g_{(k)}(X) + \pi^{s-t'''} u_{(k)}(X) \\ \tilde{h}_{(k)}(X) &=: g_{(k)}(X) + \pi^{s-t'''} v_{(k)}(X) \end{aligned}$$

for $k \in [1,n]$, where $u_{(k)}(X)$, $v_{(k)}(X) \in R[X]$, we obtain $\deg u_{(k)}(X) < \deg g_{(k)}(X) = m_{(k)}$, since $\tilde{g}_{(k)}(X)$ and $g_{(k)}(X)$ are monic polynomials of the same degree; likewise, we obtain $\deg v_{(k)}(X) < m_{(k)}$.

We have to show that $u_{(k)}(X) \stackrel{!}{\equiv}_{\pi^{s-2t'''-r}} v_{(k)}(X)$ for $k \in [1,n]$.

We have

$$\begin{aligned}
& \prod_{k\in[1,n]} g_{(k)}(X) + \pi^{s-t'''} \sum_{k\in[1,n]} u_{(k)}(X) \cdot \prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X) \\
\equiv_{\pi^{2(s-t''')}} \quad & \prod_{k\in[1,n]} (g_{(k)}(X) + \pi^{s-t'''} u_{(k)}(X)) \\
= \quad & \prod_{k\in[1,n]} \tilde{g}_{(k)}(X) \\
\equiv_{\pi^{2(s-t''')-r}} \quad & \prod_{k\in[1,n]} \tilde{h}_{(k)}(X) \\
= \quad & \prod_{k\in[1,n]} (g_{(k)}(X) + \pi^{s-t'''} v_{(k)}(X)) \\
\equiv_{\pi^{2(s-t''')}} \quad & \prod_{k\in[1,n]} g_{(k)}(X) + \pi^{s-t'''} \sum_{k\in[1,n]} v_{(k)}(X) \cdot \prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X) \ .
\end{aligned}$$

The difference yields

$$\sum_{k\in[1,n]} (u_{(k)}(X) - v_{(k)}(X)) \cdot \prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X) \ \equiv_{\pi^{s-t'''-r}} \ 0 \ .$$

Writing

$$w_{(k)}(X) \ := \ u_{(k)}(X) - v_{(k)}(X)$$

for $k \in [1,n]$, this reads

$$(*) \qquad \sum_{k\in[1,n]} w_{(k)}(X) \cdot \prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X) \ \equiv_{\pi^{s-t'''-r}} \ 0 \ .$$

Writing

$$w_{(k)}(X) \ =: \ \sum_{i\geq 0} w_{(k)i} X^i$$

for $k \in [1,n]$, and

$$W \ := \ (\underbrace{w_{(1)\,0} \ \ldots \ w_{(1)\,m_{(1)}-1}}\ \underbrace{w_{(2)\,0} \ \ldots \ w_{(2)\,m_{(2)}-1}}\ \ \ldots \ \ \underbrace{w_{(n)\,0} \ \ldots \ w_{(n)\,m_{(n)}-1}}) \ \in \ R^{1\times M} \ ,$$

we have to show that $W \overset{!}{\in} \pi^{s-2t'''-r} R^{1\times M}$. From $(*)$, we obtain

$$W \cdot A(g_{(1)} \, , \, \ldots \, , \, g_{(n)}) \ \in \ \pi^{s-t'''-r} R^{1\times M} \ .$$

Note that $s - t''' - r \geq t''' = e'$. So we can infer by Lemma 21.(2) that $W \in \pi^{(s-t'''-r)-t'''} R^{1\times M} = \pi^{s-2t'''-r} R^{1\times M}$. □

Theorem 23. *Recall that R is a discrete valuation ring with maximal ideal πR.*

Suppose R to be complete.

Let $f(X) \in R[X]$ be a monic polynomial. Write $M := \deg(f)$. Suppose that $f(X) \equiv_\pi X^M$.

Let $n \geq 1$. Suppose given monic polynomials $g_{(1)}(X) \, , \, \ldots \, , \, g_{(n)}(X) \in R[X]$ having degree ≥ 1. Write $m_{(k)} := \deg(g_{(k)})$ for $k \in [1,n]$. Suppose the ordering to be chosen such that $m_{(1)} \leq m_{(2)} \leq \cdots \leq m_{(n)}$.

Suppose that $\mathrm{Res}(g_{(1)}\,,\,\ldots\,,\,g_{(n)}) \neq 0$. *Denote*

$$\begin{aligned} t'' &:= \mathrm{v}_\pi\big(\mathrm{Res}(g_{(1)}\,,\,\ldots\,,\,g_{(n)})\big) \\ t''' &:= \mathrm{v}_\pi\big(\mathrm{Res}(g_{(1)}\,,\,\ldots\,,\,g_{(n)})\big) - \textstyle\sum_{j\in[1,n-1]}\big((n-j)m_{(j)}-1\big)\,. \end{aligned}$$

Let $s \geq t'' + t''' + 1$.

Suppose that

$$f(X) \equiv_{\pi^s} \prod_{k\in[1,n]} g_{(k)}(X)\,.$$

Then there exist unique monic polynomials $\overset{\vee}{g}_{(1)}(X)\,,\,\ldots\,,\,\overset{\vee}{g}_{(n)}(X) \in R[X]$ *such that*

$$\overset{\vee}{g}_{(k)}(X) \equiv_{\pi^{s-t'''}} g_{(k)}(X) \quad \textit{for } k \in [1,n]$$

and

$$f(X) = \prod_{k\in[1,n]} \overset{\vee}{g}_{(k)}(X)\,.$$

(Note that we may replace the condition $s \geq t'' + t''' + 1$ *by the condition* $s > t := \mathrm{v}_\pi(\Delta(f))$ *if* $\Delta(f) \neq 0$*; cf. Remark* 15.*)*

Proof. Existence. Since R is complete, by Remark 74 it suffices to show that there exist monic polynomials $\tilde{g}_{(1)}(X)\,,\,\ldots\,,\,\tilde{g}_{(n)}(X) \in R[X]$ such that

$$f(X) \equiv_{\pi^{s+1}} \prod_{k\in[1,n]} \tilde{g}_{(k)}(X)\,,$$

$$\tilde{g}_{(k)}(X) \equiv_{\pi^{s-t'''}} g_{(k)}(X) \quad \text{for } k \in [1,n]$$

and

$$\mathrm{v}_\pi(\mathrm{Res}(\tilde{g}_{(1)}\,,\,\ldots\,,\,\tilde{g}_{(n)})) = t''\,.$$

This follows from Lemma 22.(1) since $2(s-t''') \geq s+1$.

Uniqueness. Suppose given monic polynomials $\overset{\vee}{g}_{(1)}(X)\,,\,\ldots\,,\,\overset{\vee}{g}_{(n)}(X) \in R[X]$ such that

$$\overset{\vee}{g}_{(k)}(X) \equiv_{\pi^{s-t'''}} g_{(k)}(X) \quad \text{for } k \in [1,n]$$

and

$$f(X) = \prod_{k\in[1,n]} \overset{\vee}{g}_{(k)}(X)\,,$$

and monic polynomials $\overset{\vee}{h}_{(1)}(X)\,,\,\ldots\,,\,\overset{\vee}{h}_{(n)}(X) \in R[X]$ such that

$$\overset{\vee}{h}_{(k)}(X) \equiv_{\pi^{s-t'''}} g_{(k)}(X) \quad \text{for } k \in [1,n]$$

and

$$f(X) = \prod_{k\in[1,n]} \overset{\vee}{h}_{(k)}(X)\,.$$

We have to show that $\overset{\vee}{g}_{(k)}(X) \overset{!}{=} \overset{\vee}{h}_{(k)}(X)$ for $k \in [1,n]$.

Note that $\mathrm{v}_\pi(\mathrm{Res}(\overset{\vee}{g}_{(1)}, \ldots, \overset{\vee}{g}_{(n)})) = t'' = \mathrm{v}_\pi(\mathrm{Res}(\overset{\vee}{h}_{(1)}, \ldots, \overset{\vee}{h}_{(n)}))$ by Lemma 22.(1).

Let $s_1 := s$. Both $(\overset{\vee}{h}_{(k)}(X))_k$ and $(\overset{\vee}{g}_{(k)}(X))_k$ are admissible lifts of $(\overset{\vee}{g}_{(k)}(X))_k$ with respect to s_1 in the sense of Lemma 22.(1), since

$$\begin{array}{rll} f(X) & \equiv_{\pi^{s_1}} & \prod_{k\in[1,n]} \overset{\vee}{g}_{(k)}(X) \\ \overset{\vee}{h}_{(k)}(X) & \equiv_{\pi^{s_1-t'''}} & \overset{\vee}{g}_{(k)}(X) \quad \text{for } k \in [1,n] \\ f(X) & \equiv_{\pi^{2(s_1-t''')}} & \prod_{k\in[1,n]} \overset{\vee}{h}_{(k)}(X) \\ \overset{\vee}{g}_{(k)}(X) & \equiv_{\pi^{s_1-t'''}} & \overset{\vee}{g}_{(k)}(X) \quad \text{for } k \in [1,n] \\ f(X) & \equiv_{\pi^{2(s_1-t''')}} & \prod_{k\in[1,n]} \overset{\vee}{g}_{(k)}(X)\ . \end{array}$$

So Lemma 22.(2) yields

$$\overset{\vee}{h}_{(k)}(X) \equiv_{\pi^{2(s_1-t''')-t'''}} \overset{\vee}{g}_{(k)}(X) \qquad \text{for } k \in [1,n].$$

Let $s_2 := 2(s_1 - t''')$. Note that $s_2 = s_1 + (s_1 - 2t''') > s_1$. Both $(\overset{\vee}{h}_{(k)}(X))_k$ and $(\overset{\vee}{g}_{(k)}(X))_k$ are admissible lifts of $(\overset{\vee}{g}_{(k)}(X))_k$ with respect to s_2 in the sense of Lemma 22.(1), since

$$\begin{array}{rll} f(X) & \equiv_{\pi^{s_2}} & \prod_{k\in[1,n]} \overset{\vee}{g}_{(k)}(X) \\ \overset{\vee}{h}_{(k)}(X) & \equiv_{\pi^{s_2-t'''}} & \overset{\vee}{g}_{(k)}(X) \quad \text{for } k \in [1,n] \\ f(X) & \equiv_{\pi^{2(s_2-t''')}} & \prod_{k\in[1,n]} \overset{\vee}{h}_{(k)}(X) \\ \overset{\vee}{g}_{(k)}(X) & \equiv_{\pi^{s_2-t'''}} & \overset{\vee}{g}_{(k)}(X) \quad \text{for } k \in [1,n] \\ f(X) & \equiv_{\pi^{2(s_2-t''')}} & \prod_{k\in[1,n]} \overset{\vee}{g}_{(k)}(X)\ . \end{array}$$

So Lemma 22.(2) yields

$$\overset{\vee}{h}_{(k)}(X) \equiv_{\pi^{2(s_2-t''')-t'''}} \overset{\vee}{g}_{(k)}(X) \qquad \text{for } k \in [1,n].$$

Let $s_3 := 2(s_2 - t''')$. Note that $s_3 = s_2 + (s_2 - 2t''') > s_2 + (s_1 - 2t''') > s_2$. Continue as above.

This yields a strictly increasing sequence $(s_\ell)_{\ell\geq 1}$ of integers such that

$$\overset{\vee}{h}_{(k)}(X) \equiv_{\pi^{s_\ell-t'''}} \overset{\vee}{g}_{(k)}(X) \qquad \text{for } k \in [1,n] \text{ and } \ell \geq 1.$$

Hence

$$\overset{\vee}{h}_{(k)}(X) = \overset{\vee}{g}_{(k)}(X) \qquad \text{for } k \in [1,n].$$

□

2.4 Hensel with three factors vs. iteration of Hensel with two factors

2.4.1 General case

2.4.1.1 Situation

Given a factorisation of a polynomial into three factors modulo a power of π, we want to improve on its precision in two ways, on the one hand by a direct application of Lemma 16.(1) for *three*

factors, on the other hand by an iterated application of Lemma 16.(1) for *two* factors.

Let R be a discrete valuation ring.

Let $\pi \in R$ be a generator of the maximal ideal of R.

Let $f(X) \in R[X]$ be a monic polynomial.

Let $g_{(1)}(X)\,,\, g_{(2)}(X)\,,\, g_{(3)}(X) \in R[X]$ be monic polynomials of degree ≥ 1.

Suppose that $\mathrm{Res}(g_{(1)}\,,\, g_{(2)}\,,\, g_{(3)}) \neq 0$. Denote

$$t'' \;:=\; \mathrm{v}_\pi(\mathrm{Res}(g_{(1)}\,,\, g_{(2)}\,,\, g_{(3)}))\;.$$

We denote

$$\begin{aligned} t''_0 \;&:=\; \mathrm{v}_\pi(\mathrm{Res}(g_{(2)}\,,\, g_{(3)}))\;, \\ t''_1 \;&:=\; \mathrm{v}_\pi(\mathrm{Res}(g_{(1)}\,,\, g_{(2)}g_{(3)}))\;. \end{aligned}$$

We have

$$\begin{aligned} \mathrm{Res}(g_{(1)}\,,\, g_{(2)}\,,\, g_{(3)}) \;&\overset{\text{C 4}}{=}\; \mathrm{Res}(g_{(1)}\,,\, g_{(2)}) \cdot \mathrm{Res}(g_{(1)}\,,\, g_{(3)}) \cdot \mathrm{Res}(g_{(2)}\,,\, g_{(3)}) \\ &\overset{\text{R 6}}{=}\; \mathrm{Res}(g_{(1)}\,,\, g_{(2)}g_{(3)}) \cdot \mathrm{Res}(g_{(2)}\,,\, g_{(3)})\;. \end{aligned}$$

It follows that

$$\begin{aligned} t'' \;&=\; \mathrm{v}_\pi(\mathrm{Res}(g_{(1)}\,,\, g_{(2)}\,,\, g_{(3)})) \\ &=\; \mathrm{v}_\pi(\mathrm{Res}(g_{(1)}\,,\, g_{(2)}g_{(3)}) \cdot \mathrm{Res}(g_{(2)}\,,\, g_{(3)})) \\ &=\; \mathrm{v}_\pi(\mathrm{Res}(g_{(1)}\,,\, g_{(2)}g_{(3)})) + \mathrm{v}_\pi(\mathrm{Res}(g_{(2)}\,,\, g_{(3)})) \\ &=\; t''_1 + t''_0\;. \end{aligned}$$

Let $s \geq 2t'' + 1$.

Suppose that

$$f(X) \equiv_{\pi^s} g_{(1)}(X) \cdot g_{(2)}(X) \cdot g_{(3)}(X)\;.$$

2.4.1.2 Existence

Now we can apply Lemma 16.(1) to this factorisation into *three* factors modulo π^s, to obtain monic polynomials $\tilde{g}_{(1)}(X)\,,\, \tilde{g}_{(2)}(X)\,,\, \tilde{g}_{(3)}(X) \in R[X]$ such that

(i)
$$\begin{aligned} \tilde{g}_{(k)}(X) \;&\equiv_{\pi^{s-t''}} \quad g_{(k)}(X) \quad \text{for } k \in [1,3] \\ f(X) \;&\equiv_{\pi^{2(s-t'')}} \; \tilde{g}_{(1)}(X) \cdot \tilde{g}_{(2)}(X) \cdot \tilde{g}_{(3)}(X)\,. \end{aligned}$$

We can also apply Lemma 16.(1) to the factorisation of $f(X)$ into the *two* factors $g_{(1)}(X)$ and $g_{(2)}(X) \cdot g_{(3)}(X)$ modulo π^s. Doing so, we shall obtain an improved factorisation of $f(X)$ into, say, $\tilde{h}_{(1)}(X)$ and $\tilde{h}_{(2)}(X)$, where $\tilde{h}_{(1)}(X)$ is congruent to $g_{(1)}(X)$ and where $\tilde{h}_{(2)}(X)$ is congruent to $g_{(2)}(X) \cdot g_{(3)}(X)$, modulo a certain power of π. Then we can apply Lemma 16.(1) to this factorisation of $\tilde{h}_{(2)}(X)$ into the *two* factors $g_{(2)}(X)$ and $g_{(3)}(X)$ modulo said power of π.

We want to compare the results of both methods, i.e. of the above single application of Lemma 16.(1) for three factors on the one hand, of two subsequent applications of Lemma 16.(1) for two factors on the other hand.

So we have

$$(\star) \qquad f(X) \equiv_{\pi^s} g_{(1)}(X) \cdot (g_{(2)}(X) \cdot g_{(3)}(X)) \; .$$

To apply Lemma 16.(1) to the factorisation $(\star)$ into *two* factors modulo π^s we have to assure that

1. $\mathrm{Res}(g_{(1)} \, , \, g_{(2)}g_{(3)}) \overset{!}{\neq} 0$,
2. $s \overset{!}{\geq} 2t_1'' + 1$.

1. We have seen above that $\mathrm{Res}(g_{(1)} \, , \, g_{(2)}g_{(3)})$ divides $\mathrm{Res}(g_{(1)} \, , \, g_{(2)} \, , \, g_{(3)})$.

Since $\mathrm{Res}(g_{(1)} \, , \, g_{(2)} \, , \, g_{(3)}) \neq 0$ it follows that $\mathrm{Res}(g_{(1)} \, , \, g_{(2)}g_{(3)}) \neq 0$.

2. Since

$$t'' = t_1'' + t_0''$$

it follows that

$$t'' \geq t_1'' \; .$$

So we have

$$s \geq 2t'' + 1 \geq 2t_1'' + 1 \; .$$

By 1. and 2. we are allowed to apply Lemma 16.(1) to $(\star)$. This yields monic polynomials $\tilde{h}_{(1)}(X) \, , \, \tilde{h}_{(2)}(X) \in R[X]$ such that

$$\begin{aligned} \tilde{h}_{(1)}(X) &\equiv_{\pi^{s-t_1''}} g_{(1)}(X) \; , \\ \tilde{h}_{(2)}(X) &\equiv_{\pi^{s-t_1''}} g_{(2)}(X) \cdot g_{(3)}(X) \; , \\ f(X) &\equiv_{\pi^{2(s-t_1'')}} \tilde{h}_{(1)}(X) \cdot \tilde{h}_{(2)}(X) \; . \end{aligned}$$

Now we want to apply Lemma 16.(1) to

$$\tilde{h}_{(2)}(X) \equiv_{\pi^{s-t_1''}} g_{(2)}(X) \cdot g_{(3)}(X) \; .$$

So we have to assure that

3. $\mathrm{Res}(g_{(2)} \, , \, g_{(3)}) \overset{!}{\neq} 0$,
4. $s - t_1'' \overset{!}{\geq} 2t_0'' + 1$.

3. We have seen above that $\mathrm{Res}(g_{(2)} \, , \, g_{(3)})$ divides $\mathrm{Res}(g_{(1)} \, , \, g_{(2)} \, , \, g_{(3)})$.

Since $\mathrm{Res}(g_{(1)} \, , \, g_{(2)} \, , \, g_{(3)}) \neq 0$ it follows that $\mathrm{Res}(g_{(2)} \, , \, g_{(3)}) \neq 0$.

4. Recall that

$$t'' \;=\; t''_1 + t''_0 \,.$$

So

$$s \;\geq\; 2t'' + 1 \;=\; 2t''_1 + 2t''_0 + 1 \;\geq\; t''_1 + 2t''_0 + 1 \,.$$

Hence

$$s - t''_1 \;\geq\; 2t''_0 + 1 \,.$$

By 3. and 4. we are allowed to apply Lemma 16.(1) to $\tilde{h}_{(2)}(X) \equiv_{\pi^{s-t''_1}} g_{(2)}(X) \cdot g_{(3)}(X)$. This yields monic polynomials $\tilde{\tilde{g}}_{(2)}(X)\,,\ \tilde{\tilde{g}}_{(3)}(X) \in R[X]$ such that

$$\begin{array}{rcl} \tilde{\tilde{g}}_{(2)}(X) & \equiv_{\pi^{(s-t''_1)-t''_0}} & g_{(2)}(X) \\ \tilde{\tilde{g}}_{(3)}(X) & \equiv_{\pi^{(s-t''_1)-t''_0}} & g_{(3)}(X) \end{array}$$

and

$$\tilde{h}_{(2)}(X) \;\equiv_{\pi^{2((s-t''_1)-t''_0)}}\; \tilde{\tilde{g}}_{(2)}(X) \cdot \tilde{\tilde{g}}_{(3)}(X) \,.$$

Altogether, the two subsequent applications of Lemma 16.(1) for two factors yield

$$(\mathrm{ii}_1) \qquad \begin{array}{rcl} \tilde{h}_{(1)}(X) & \equiv_{\pi^{s-t''_1}} & g_{(1)}(X) \\ \tilde{\tilde{g}}_{(2)}(X) & \equiv_{\pi^{s-t''_1-t''_0}} & g_{(2)}(X) \\ \tilde{\tilde{g}}_{(3)}(X) & \equiv_{\pi^{s-t''_1-t''_0}} & g_{(3)}(X) \end{array}$$

and

$$(\mathrm{ii}_2) \qquad \begin{array}{rcl} f(X) & \equiv_{\pi^{2(s-t''_1)}} & \tilde{h}_{(1)}(X) \cdot \tilde{h}_{(2)}(X) \\ & \equiv_{\pi^{2(s-t''_1-t''_0)}} & \tilde{h}_{(1)}(X) \cdot \tilde{\tilde{g}}_{(2)}(X) \cdot \tilde{\tilde{g}}_{(3)}(X) \,. \end{array}$$

Comparing the result (i) of Lemma 16.(1) for three factors with the result $(\mathrm{ii}_1\,, \mathrm{ii}_2)$ of two subsequent applications of Lemma 16.(1) for two factors, both methods essentially yield a precision of $s - t''$ for the factors and a precision of $2(s - t'')$ for the product decomposition.

2.4.1.3 Uniqueness

Suppose given monic polynomials $\tilde{g}_{(1)}(X)\,,\ \tilde{g}_{(2)}(X)\,,\ \tilde{g}_{(3)}(X) \in R[X]$ and monic polynomials $\tilde{G}_{(1)}(X)\,,\ \tilde{G}_{(2)}(X)\,,\ \tilde{G}_{(3)}(X) \in R[X]$ such that that

$$\begin{array}{rcll} \tilde{g}_{(k)}(X) & \equiv_{\pi^{s-t''}} & g_{(k)}(X) & \text{for } k \in [1,3] \\ f(X) & \equiv_{\pi^{2(s-t'')}} & \tilde{g}_{(1)}(X) \cdot \tilde{g}_{(2)}(X) \cdot \tilde{g}_{(3)}(X) & \\ \tilde{G}_{(k)}(X) & \equiv_{\pi^{s-t''}} & g_{(k)}(X) & \text{for } k \in [1,3] \\ f(X) & \equiv_{\pi^{2(s-t'')}} & \tilde{G}_{(1)}(X) \cdot \tilde{G}_{(2)}(X) \cdot \tilde{G}_{(3)}(X) \,. & \end{array}$$

By Lemma 16.(2), we obtain

$$\tilde{g}_{(k)}(X) \;\equiv_{\pi^{2s-3t''}}\; \tilde{G}_{(k)}(X)$$

for $k \in [1,3]$.

We can also apply Lemma 16.(2) twice to respective factorisations into two polynomials.

Suppose given monic polynomials $\tilde{h}_{(1)}(X)\,,\,\tilde{h}_{(2)}(X) \in R[X]$ and monic polynomials $\tilde{H}_{(1)}(X)\,,\,\tilde{H}_{(2)}(X) \in R[X]$ such that

$$\begin{aligned}
\tilde{h}_{(1)}(X) &\equiv_{\pi^{s-t_1''}} g_{(1)}(X)\\
\tilde{h}_{(2)}(X) &\equiv_{\pi^{s-t_1''}} g_{(2)}(X)\cdot g_{(3)}(X)\\
f(X) &\equiv_{\pi^{2(s-t_1'')}} \tilde{h}_{(1)}(X)\cdot\tilde{h}_{(2)}(X)\\
\tilde{H}_{(1)}(X) &\equiv_{\pi^{s-t_1''}} g_{(1)}(X)\\
\tilde{H}_{(2)}(X) &\equiv_{\pi^{s-t_1''}} g_{(2)}(X)\cdot g_{(3)}(X)\\
f(X) &\equiv_{\pi^{2(s-t_1'')}} \tilde{H}_{(1)}(X)\cdot\tilde{H}_{(2)}(X)\,.
\end{aligned}$$

Lemma 16.(2) yields

$$\begin{aligned}
\tilde{h}_{(1)}(X) &\equiv_{\pi^{2s-3t_1''}} \tilde{H}_{(1)}(X)\\
\tilde{h}_{(2)}(X) &\equiv_{\pi^{2s-3t_1''}} \tilde{H}_{(2)}(X)\,.
\end{aligned}$$

Suppose given monic polynomials $\tilde{\tilde{g}}_{(2)}(X)\,,\,\tilde{\tilde{g}}_{(3)}(X) \in R[X]$ and monic polynomials $\tilde{\tilde{G}}_{(2)}(X)\,,\,\tilde{\tilde{G}}_{(3)}(X) \in R[X]$ such that

$$\begin{aligned}
\tilde{\tilde{g}}_{(2)}(X) &\equiv_{\pi^{(s-t_1'')-t_0''}} g_{(2)}(X)\\
\tilde{\tilde{g}}_{(3)}(X) &\equiv_{\pi^{(s-t_1'')-t_0''}} g_{(3)}(X)\\
\tilde{h}_{(2)}(X) &\equiv_{\pi^{2((s-t_1'')-t_0'')}} \tilde{\tilde{g}}_{(2)}(X)\cdot\tilde{\tilde{g}}_{(3)}(X)\\
\tilde{\tilde{G}}_{(2)}(X) &\equiv_{\pi^{(s-t_1'')-t_0''}} g_{(2)}(X)\\
\tilde{\tilde{G}}_{(3)}(X) &\equiv_{\pi^{(s-t_1'')-t_0''}} g_{(3)}(X)\\
\tilde{H}_{(2)}(X) &\equiv_{\pi^{2((s-t_1'')-t_0'')}} \tilde{\tilde{G}}_{(2)}(X)\cdot\tilde{\tilde{G}}_{(3)}(X)\,.
\end{aligned}$$

We have

$$\tilde{\tilde{g}}_{(2)}(X)\cdot\tilde{\tilde{g}}_{(3)}(X) \equiv_{\pi^{2((s-t_1'')-t_0'')}} \tilde{h}_{(2)}(X) \equiv_{\pi^{2s-3t_1''}} \tilde{H}_{(2)}(X) \equiv_{\pi^{2(s-t_1''-t_0'')}} \tilde{\tilde{G}}_{(2)}(X)\cdot\tilde{\tilde{G}}_{(3)}(X)\,.$$

Case $t_1'' \leq 2t_0''$ *.*

We get

$$\tilde{\tilde{g}}_{(2)}(X)\cdot\tilde{\tilde{g}}_{(3)}(X) \equiv_{\pi^{2((s-t_1'')-t_0'')}} \tilde{\tilde{G}}_{(2)}(X)\cdot\tilde{\tilde{G}}_{(3)}(X)$$

Lemma 16.(2) yields

$$\begin{aligned}
\tilde{\tilde{g}}_{(2)}(X) &\equiv_{\pi^{2(s-t_1'')-3t_0''}} \tilde{\tilde{G}}_{(2)}(X)\\
\tilde{\tilde{g}}_{(3)}(X) &\equiv_{\pi^{2(s-t_1'')-3t_0''}} \tilde{\tilde{G}}_{(3)}(X)\,.
\end{aligned}$$

Altogether, we have

$$\begin{aligned}
\tilde{h}_{(1)}(X) &\equiv_{\pi^{2s-3t_1''}} \tilde{H}_{(1)}(X)\\
\tilde{\tilde{g}}_{(2)}(X) &\equiv_{\pi^{2s-2t_1''-3t_0''}} \tilde{\tilde{G}}_{(2)}(X)\\
\tilde{\tilde{g}}_{(3)}(X) &\equiv_{\pi^{2s-2t_1''-3t_0''}} \tilde{\tilde{G}}_{(3)}(X)\,.
\end{aligned}$$

So if $t_0'' = t''$ or if $t_1'' = t''$, then the non-iterated method and the iterated method are equally precise, otherwise the iterated method is more precise.

Case $t_1'' > 2t_0''$.

We get

$$\tilde{\tilde{g}}_{(2)}(X) \cdot \tilde{\tilde{g}}_{(3)}(X) \equiv_{\pi^{2s-3t_1''}} \tilde{\tilde{G}}_{(2)}(X) \cdot \tilde{\tilde{G}}_{(3)}(X)$$

Lemma 16.(2), with $r := t_1'' - 2t_0''$, yields

$$\begin{aligned} \tilde{\tilde{g}}_{(2)}(X) &\equiv_{\pi^{2(s-t_1'')-3t_0''-r}} \tilde{\tilde{G}}_{(2)}(X) \\ \tilde{\tilde{g}}_{(3)}(X) &\equiv_{\pi^{2(s-t_1'')-3t_0''-r}} \tilde{\tilde{G}}_{(3)}(X) \ . \end{aligned}$$

Altogether, we have

$$\begin{aligned} \tilde{h}_{(1)}(X) &\equiv_{\pi^{2s-3t_1''}} \tilde{H}_{(1)}(X) \\ \tilde{\tilde{g}}_{(2)}(X) &\equiv_{\pi^{2s-3t_1''-t_0''}} \tilde{\tilde{G}}_{(2)}(X) \\ \tilde{\tilde{g}}_{(3)}(X) &\equiv_{\pi^{2s-3t_1''-t_0''}} \tilde{\tilde{G}}_{(3)}(X) \ . \end{aligned}$$

So if $t_1'' = t''$, then the non-iterated method and the iterated method are equally precise, otherwise the iterated method is more precise.

2.4.2 The case $f(X) \equiv_\pi X^M$

2.4.2.1 Situation

Suppose given a polynomial that is congruent to a power of X modulo π. Given a factorisation of this polynomial into three factors modulo a power of π, we want to improve on its precision in two ways, on the one hand by a direct application of Lemma 22.(1) for *three* factors, on the other hand by an iterated application of Lemma 22.(1) for *two* factors.

Let R be a discrete valuation ring.

Let $\pi \in R$ be a generator of the maximal ideal of R.

Let $f(X) \in R[X]$ be a monic polynomial. Write $M := \deg(f)$. Suppose that $f(X) \equiv_\pi X^M$.

Let $g_{(1)}(X)$, $g_{(2)}(X)$, $g_{(3)}(X) \in R[X]$ be monic polynomials of degree $m_{(k)} := \deg(g_{(k)}) \geq 1$ for $k \in [1,3]$. We have $g_{(k)}(X) \equiv_\pi X^{m_{(k)}}$ for $k \in [1,3]$; cf. Remark 19.

Suppose that $m_{(1)} \leq m_{(2)} \leq m_{(3)}$.

Suppose that $\mathrm{Res}(g_{(1)}\,,\, g_{(2)}\,,\, g_{(3)}) \neq 0$.

Denote

$$\begin{aligned} t'' &:= \mathrm{v}_\pi(\mathrm{Res}(g_{(1)}\,,\, g_{(2)}\,,\, g_{(3)})) \\ t''' &:= \mathrm{v}_\pi(\mathrm{Res}(g_{(1)}\,,\, g_{(2)}\,,\, g_{(3)})) - 2m_{(1)} - m_{(2)} + 2 \ . \end{aligned}$$

We denote

$$\begin{aligned} t_0'' &:= \mathrm{v}_\pi(\mathrm{Res}(g_{(2)}\,,\, g_{(3)}))\ , & t_0''' &:= \mathrm{v}_\pi(\mathrm{Res}(g_{(2)}\,,\, g_{(3)})) - m_{(2)} + 1\ , \\ t_1'' &:= \mathrm{v}_\pi(\mathrm{Res}(g_{(1)}\,,\, g_{(2)}g_{(3)}))\ , & t_1''' &:= \mathrm{v}_\pi(\mathrm{Res}(g_{(1)}\,,\, g_{(2)}g_{(3)})) - m_{(1)} + 1\ . \end{aligned}$$

We have

$$\begin{array}{rcl} \mathrm{Res}(g_{(1)}\,,\,g_{(2)}\,,\,g_{(3)}) & \overset{\text{C 4}}{=} & \mathrm{Res}(g_{(1)}\,,\,g_{(2)})\cdot\mathrm{Res}(g_{(1)}\,,\,g_{(3)})\cdot\mathrm{Res}(g_{(2)}\,,\,g_{(3)}) \\ & \overset{\text{R 6}}{=} & \mathrm{Res}(g_{(1)}\,,\,g_{(2)}g_{(3)})\cdot\mathrm{Res}(g_{(2)}\,,\,g_{(3)})\,. \end{array}$$

It follows that

$$\begin{array}{rcl} t'' & = & \mathrm{v}_\pi(\mathrm{Res}(g_{(1)}\,,\,g_{(2)}\,,\,g_{(3)})) \\ & = & \mathrm{v}_\pi(\mathrm{Res}(g_{(1)}\,,\,g_{(2)}g_{(3)})\cdot\mathrm{Res}(g_{(2)}\,,\,g_{(3)})) \\ & = & \mathrm{v}_\pi(\mathrm{Res}(g_{(1)}\,,\,g_{(2)}g_{(3)}))+\mathrm{v}_\pi(\mathrm{Res}(g_{(2)}\,,\,g_{(3)})) \\ & = & t''_1+t''_0 \end{array}$$

and

$$\begin{array}{rcl} t''' & = & t''-2m_{(1)}-m_{(2)}+2 \\ & = & t''_1+t''_0-2m_{(1)}-m_{(2)}+2 \\ & = & (t''_1-m_{(1)}+1)+(t''_0-m_{(2)}+1)-m_{(1)} \\ & = & t'''_1+t'''_0-m_{(1)}\,. \end{array}$$

Let $s \geq 2t''+1$.

Suppose that

$$f(X) \equiv_{\pi^s} g_{(1)}(X)\cdot g_{(2)}(X)\cdot g_{(3)}(X)\,.$$

Note that $s \geq 2t''+1 \geq t''+t'''+1$.

2.4.2.2 Existence

So we can apply Lemma 22.(1) to this factorisation into *three* factors modulo π^s, to obtain monic polynomials $\tilde{g}_{(1)}(X)\,,\,\tilde{g}_{(2)}(X)\,,\,\tilde{g}_{(3)}(X) \in R[X]$ such that

(iii)
$$\begin{array}{rcll} \tilde{g}_{(k)}(X) & \equiv_{\pi^{s-t'''}} & g_{(k)}(X) & \text{for } k\in[1,3] \\ f(X) & \equiv_{\pi^{2(s-t''')}} & \tilde{g}_{(1)}(X)\cdot\tilde{g}_{(2)}(X)\cdot\tilde{g}_{(3)}(X)\,. & \end{array}$$

We can also apply Lemma 22.(1) to the factorisation of $f(X)$ into the *two* factors $g_{(1)}(X)$ and $g_{(2)}(X)\cdot g_{(3)}(X)$ modulo π^s. Doing so, we shall obtain an improved factorisation of $f(X)$ into, say, $\tilde{h}_{(1)}(X)$ and $\tilde{h}_{(2)}(X)$, where $\tilde{h}_{(1)}(X)$ is congruent to $g_{(1)}(X)$ and where $\tilde{h}_{(2)}(X)$ is congruent to $g_{(2)}(X)\cdot g_{(3)}(X)$, modulo a certain power of π. Then we can apply Lemma 22.(1) to this factorisation of $\tilde{h}_{(2)}(X)$ into the *two* factors $g_{(2)}(X)$ and $g_{(3)}(X)$ modulo said power of π.

We want to compare the results of both methods, i.e. of the above single application of Lemma 22.(1) for three factors on the one hand, of two subsequent applications of Lemma 22.(1) for two factors on the other hand.

So we have

($\star\star$)
$$f(X) \equiv_{\pi^s} g_{(1)}(X)\cdot(g_{(2)}(X)\cdot g_{(3)}(X))\,.$$

To apply Lemma 22.(1) to the factorisation $(\star\star)$ into *two* factors modulo π^s we have to assure that

1. $\mathrm{Res}(g_{(1)}\,,\,g_{(2)}g_{(3)}) \overset{!}{\neq} 0$,
2. $s \overset{!}{\geq} t_1'' + t_1''' + 1$.

1. We have seen above that $\mathrm{Res}(g_{(1)}\,,\,g_{(2)}g_{(3)})$ divides $\mathrm{Res}(g_{(1)}\,,\,g_{(2)}\,,\,g_{(3)})$.

Since $\mathrm{Res}(g_{(1)}\,,\,g_{(2)}\,,\,g_{(3)}) \neq 0$ it follows that $\mathrm{Res}(g_{(1)}\,,\,g_{(2)}g_{(3)}) \neq 0$.

2. Since

$$t'' = t_1'' + t_0''$$

it follows that

$$t'' \geq t_1''\,.$$

So we have

$$s \geq 2t''+1 \geq 2t_1''+1 \geq t_1''+t_1'''+1\,.$$

By 1. and 2. we are allowed to apply Lemma 22.(1) to $(\star\star)$. This yields monic polynomials $\tilde{h}_{(1)}(X)\,,\,\tilde{h}_{(2)}(X) \in R[X]$ such that

$$\begin{aligned} \tilde{h}_{(1)}(X) &\equiv_{\pi^{s-t_1'''}} g_{(1)}(X)\,, \\ \tilde{h}_{(2)}(X) &\equiv_{\pi^{s-t_1'''}} g_{(2)}(X)\cdot g_{(3)}(X)\,, \\ f(X) &\equiv_{\pi^{2(s-t_1''')}} \tilde{h}_{(1)}(X)\cdot\tilde{h}_{(2)}(X)\,. \end{aligned}$$

Now we want to apply Lemma 22.(1) to

$$\tilde{h}_{(2)}(X) \equiv_{\pi^{s-t_1'''}} g_{(2)}(X)\cdot g_{(3)}(X)\,.$$

So we have to assure that

3. $\mathrm{Res}(g_{(2)}\,,\,g_{(3)}) \overset{!}{\neq} 0$,
4. $s - t_1''' \overset{!}{\geq} t_0'' + t_0''' + 1$.

3. We have seen above that $\mathrm{Res}(g_{(2)}\,,\,g_{(3)})$ divides $\mathrm{Res}(g_{(1)}\,,\,g_{(2)}\,,\,g_{(3)})$.

Since $\mathrm{Res}(g_{(1)}\,,\,g_{(2)}\,,\,g_{(3)}) \neq 0$ it follows that $\mathrm{Res}(g_{(2)}\,,\,g_{(3)}) \neq 0$.

4. Recall that

$$t'' = t_1'' + t_0''\,.$$

So

$$s \geq 2t''+1 \geq 2t''-m_{(2)}-m_{(1)}+3-t_1'' = (2t_0''-m_{(2)}+1)+(t_1''-m_{(1)}+1)+1 = (t_0''+t_0''')+t_1'''+1\,.$$

Hence

$$s - t_1''' \;\geq\; t_0'' + t_0''' + 1 \,.$$

By 3. and 4. we are allowed to apply Lemma 22.(1) to $\tilde{h}_{(2)}(X) \equiv_{\pi^{s-t_1'''}} g_{(2)}(X) \cdot g_{(3)}(X)$. This yields monic polynomials $\tilde{\tilde{g}}_{(2)}(X)\,,\, \tilde{\tilde{g}}_{(3)}(X) \in R[X]$ such that

$$\begin{array}{lll} \tilde{\tilde{g}}_{(2)}(X) & \equiv_{\pi^{(s-t_1''')-t_0'''}} & g_{(2)}(X) \\ \tilde{\tilde{g}}_{(3)}(X) & \equiv_{\pi^{(s-t_1''')-t_0'''}} & g_{(3)}(X) \end{array}$$

and

$$\tilde{h}_{(2)}(X) \;\equiv_{\pi^{2((s-t_1''')-t_0''')}}\; \tilde{\tilde{g}}_{(2)}(X) \cdot \tilde{\tilde{g}}_{(3)}(X) \,.$$

Altogether, the two subsequent applications of Lemma 22.(1) for two factors yield

$$(\mathrm{iv}_1) \qquad \begin{array}{lll} \tilde{h}_{(1)}(X) & \equiv_{\pi^{s-t_1'''}} & g_{(1)}(X) \\ \tilde{\tilde{g}}_{(2)}(X) & \equiv_{\pi^{s-t_1'''-t_0'''}} & g_{(2)}(X) \\ \tilde{\tilde{g}}_{(3)}(X) & \equiv_{\pi^{s-t_1'''-t_0'''}} & g_{(3)}(X) \end{array}$$

and

$$(\mathrm{iv}_2) \qquad \begin{array}{lll} f(X) & \equiv_{\pi^{2(s-t_1''')}} & \tilde{h}_{(1)}(X) \cdot \tilde{h}_{(2)}(X) \\ & \equiv_{\pi^{2(s-t_1'''-t_0''')}} & \tilde{h}_{(1)}(X) \cdot \tilde{\tilde{g}}_{(2)}(X) \cdot \tilde{\tilde{g}}_{(3)}(X) \,. \end{array}$$

Comparing the result (iii) of Lemma 22.(1) for three factors with the result $(\mathrm{iv}_1\,, \mathrm{iv}_2)$ of two subsequent applications of Lemma 22.(1) for two factors, the former method yields a precision of $s - t'''$ for the factors and a precision of $2(s - t''')$ for the product decomposition, the latter method yields a precision of $s - t_0''' - t_1'''$ for the factors and a precision of $2(s - t_0''' - t_1''')$ for the product decomposition. Since $t''' = t_1''' + t_0''' - m_{(1)} < t_1''' + t_0'''$, the former method yields a higher precision.

Chapter 3

Miscellanea

3.1 Using the discriminant only

We derive the following corollary, in which, roughly, the resultant is replaced by the discriminant. In general, this will cause loss of precision.

We neglect the question of uniqueness.

Corollary 24. *Let R be a complete discrete valuation ring.*

Let $\pi \in R$ be a generator of the maximal ideal of R.

Let $f(X) \in R[X]$ be a monic polynomial such that $\Delta(f) \neq 0$.

Denote $t := \mathrm{v}_\pi(\Delta(f))$. Denote $t' := \lfloor \frac{t}{2} \rfloor$.

Let $s \geq t+1$. Let $g_{(1)}(X), \ldots, g_{(n)}(X) \in R[X]$ be monic polynomials of degree ≥ 1 such that

$$f(X) \equiv_{\pi^s} \prod_{k \in [1,n]} g_{(k)}(X) \, .$$

Then there exist monic polynomials $\overset{\vee}{g}_{(1)}(X), \ldots, \overset{\vee}{g}_{(n)}(X) \in R[X]$ such that

$$\overset{\vee}{g}_{(k)}(X) \equiv_{\pi^{s-t'}} g_{(k)}(X) \quad \text{for } k \in [1,n] \, .$$

and

$$f(X) = \prod_{k \in [1,n]} \overset{\vee}{g}_{(k)}(X).$$

Proof. We have $t \geq 2t''$ by Remark 15. Hence $s \geq t+1 \geq 2t''+1$, so that we may apply Theorem 17.

Since $\frac{t}{2} \geq t''$, we have $t' = \lfloor \frac{t}{2} \rfloor \geq t''$, whence $s - t' \leq s - t''$. So the monic polynomials $\overset{\vee}{g}_{(1)}(X), \ldots, \overset{\vee}{g}_{(n)}(X) \in R[X]$ satisfying

$$\overset{\vee}{g}_{(k)}(X) \equiv_{\pi^{s-t''}} g_{(k)}(X) \quad \text{for } k \in [1,n]$$

and

$$f(X) = \prod_{k \in [1,n]} \overset{\vee}{g}_{(k)}(X)$$

also satisfy

$$\overset{\vee}{g}_{(k)}(X) \equiv_{\pi^{s-t'}} g_{(k)}(X) \quad \text{for } k \in [1,n] \,,$$

as required. □

It might be useful to have the following version of Lemma 16 not involving resultants. Over a complete discrete valuation ring, it follows from Corollary 24; conversely, an iteration of Lemma 25 yields Corollary 24.

Lemma 25. *Let R be a discrete valuation ring.*

Let $\pi \in R$ be a generator of the maximal ideal of R.

Let $f(X) \in R[X]$ be a monic polynomial such that $\Delta(f) \neq 0$.

Denote $t := \mathrm{v}_\pi(\Delta(f))$. Denote $t' := \lfloor \frac{t}{2} \rfloor$.

Let $n \geq 1$. Let $g_{(1)}(X), \ldots, g_{(n)}(X) \in R[X]$ be monic polynomials of degree ≥ 1.

Let $s \geq t+1$.

Suppose that

$$f(X) \equiv_{\pi^s} \prod_{k \in [1,n]} g_{(k)}(X) \,.$$

Then there exist monic polynomials $\tilde{g}_{(1)}(X), \ldots, \tilde{g}_{(n)}(X) \in R[X]$ such that

$$\tilde{g}_{(k)}(X) \equiv_{\pi^{s-t'}} g_{(k)}(X) \quad \textit{for } k \in [1,n]$$

and

$$f(X) \equiv_{\pi^{2(s-t')}} \prod_{k \in [1,n]} \tilde{g}_{(k)}(X) \,.$$

Proof. Since $s > t$, Lemma 16 gives monic polynomials $g_{(1)}(X), \ldots, g_{(n)}(X) \in R[X]$ such that

$$\tilde{g}_{(k)}(X) \equiv_{\pi^{s-t''}} g_{(k)}(X) \quad \text{for } k \in [1,n]$$

and

$$f(X) \equiv_{\pi^{2(s-t'')}} \prod_{k \in [1,n]} \tilde{g}_{(k)}(X) \,.$$

By Remark 15 we know that

$$t \geq 2t'' \,,$$

whence $\frac{t}{2} \geq t''$, which, together with $t'' \in \mathbb{Z}$, yields

$$t' \geq t'' \,.$$

Hence the assertion is shown. □

3.2 Hensel's lemma, classical version

We derive the classical version of Hensel's Lemma from Lemma 16. More precisely speaking, we derive the inductive step for Hensel's Lemma in the version found e.g. in **[8,** (II.4.6)].

Lemma 26. *Let $\ell \,|\, k$ be an extension of fields with ℓ algebraically closed.*

Let $h_{(1)}(X)$, $h_{(2)}(X)$ be polynomials in $k[X]$.

Then $h_{(1)}(X)$, $h_{(2)}(X)$ are coprime in $k[X]$ if and only if $h_{(1)}(X)$, $h_{(2)}(X)$ are coprime in $\ell[X]$.

This is also a consequence of Euclid's algorithm. We give a direct argument.

Proof. First we show that

$$h_{(1)}(X),\, h_{(2)}(X) \text{ are coprime in } k[X] \quad \overset{!}{\Leftarrow} \quad h_{(1)}(X),\, h_{(2)}(X) \text{ are coprime in } \ell[X]\ .$$

We *assume* that $h_{(1)}(X)$, $h_{(2)}(X)$ have a common factor of degree ≥ 1 in $k[X]$.

Then they also have a common factor of degree ≥ 1 in $\ell[X]$. $\lightning$

So they are coprime in $k[X]$.

Now we show that

$$h_{(1)}(X),\, h_{(2)}(X) \text{ are coprime in } k[X] \quad \overset{!}{\Rightarrow} \quad h_{(1)}(X),\, h_{(2)}(X) \text{ are coprime in } \ell[X]\ .$$

We *assume* that $h_{(1)}(X)$, $h_{(2)}(X)$ have a common factor $c(X)$ of degree ≥ 1 in $\ell[X]$.

Since ℓ is algebraically closed, $c(X)$ has a root $\xi \in \ell$. Let $\mu_\xi(X) \in k[X]$ be its minimal polynomial over k. We have

$$\begin{aligned} h_{(1)}(\xi) &= 0\ , \\ h_{(2)}(\xi) &= 0\ . \end{aligned}$$

It follows that $\mu_\xi(X)$ is a factor of both $h_{(1)}(X)$ and $h_{(2)}(X)$.

Since $\deg \mu_\xi \geq 1$ it follows that $h_{(1)}(X)$, $h_{(2)}(X)$ are not coprime in $k[X]$. $\lightning$

So $h_{(1)}(X)$, $h_{(2)}(X)$ are coprime in $\ell[X]$. □

Lemma 27 (Hensel, **[5,** p. 81], **[3,** §374], cf. e.g. **[8,** (II.4.6)])**.**

Let R be a discrete valuation ring. Let $\pi \in R$ be a generator of the maximal ideal of R.

Given $u(X) \in R[X]$, we denote by $\overline{u(X)} \in {}^{R}\!/_{\pi}[X]$ its image under the residue class map $R[X] \to {}^{R}\!/_{\pi}[X]$.

Let $f(X) \in R[X]$ be a monic polynomial such that $\Delta(f) \neq 0$.

Let $s \geq 1$. Let $g_{(1)}(X)\,,\, g_{(2)}(X) \in R[X]$ be monic polynomials of degree ≥ 1 such that

$$f(X) \equiv_{\pi^s} g_{(1)}(X) \cdot g_{(2)}(X)$$

and such that $\overline{g_{(1)}(X)}\,,\, \overline{g_{(2)}(X)}$ are coprime in ${}^{R}\!/_{\pi}[X]$.

Then there exist monic polynomials $\tilde{g}_{(1)}(X)\,,\ \tilde{g}_{(2)}(X) \in R[X]$ *such that*

$$\begin{aligned} \tilde{g}_{(1)}(X) &\equiv_{\pi^s} g_{(1)}(X)\,, \\ \tilde{g}_{(2)}(X) &\equiv_{\pi^s} g_{(2)}(X)\,. \end{aligned}$$

and

$$f(X) \equiv_{\pi^{2s}} \tilde{g}_{(1)}(X) \cdot \tilde{g}_{(2)}(X)\,.$$

Proof. Let E be an algebraic closure of ${}^{R}\!/_{\pi}$.

Denote

$$\mathrm{Res}(g_{(1)}\,,\ g_{(2)}) =: \mathrm{Res}_R(g_{(1)}\,,\ g_{(2)})$$

the resultant of $g_{(1)}\,,\ g_{(2)}$ in R.

Likewise we define $\mathrm{Res}_{R/\pi}(\overline{g_{(1)}}\,,\ \overline{g_{(2)}})$ and $\mathrm{Res}_E(\overline{g_{(1)}}\,,\ \overline{g_{(2)}})$.

Note that

$$\mathrm{Res}_{R/\pi}(\overline{g_{(1)}}\,,\ \overline{g_{(2)}}) \ = \ \overline{\mathrm{Res}_R(g_{(1)}\,,\ g_{(2)})}\,.$$

Since $\overline{g_{(1)}(X)}\,,\ \overline{g_{(2)}(X)}$ are coprime in ${}^{R}\!/_{\pi}[X]$ we know by Lemma 26 that $\overline{g_{(1)}(X)}\,,\ \overline{g_{(2)}(X)}$ are also coprime in $E[X]$.

So

$$\begin{aligned} \mathrm{Res}_{R/\pi}(\overline{g_{(1)}}\,,\ \overline{g_{(2)}}) &= \overline{\mathrm{Res}_R(g_{(1)}\,,\ g_{(2)})} \\ &= \mathrm{Res}_E(\overline{g_{(1)}}\,,\ \overline{g_{(2)}}) \\ &\neq 0\,. \end{aligned}$$

So we have

$$\mathrm{Res}_R(g_{(1)}\,,\ g_{(2)}) \not\equiv_{\pi} 0\,.$$

So

$$t'' := \mathrm{v}_{\pi}(\mathrm{Res}_R(g_{(1)}\,,\ g_{(2)})) \ = \ 0.$$

Since $s \geq 1 \ = \ 2t''+1$, Lemma 16 yields that there exist monic polynomials $\tilde{g}_{(1)}(X)\,,\ \tilde{g}_{(2)}(X) \in R[X]$ such that

$$\begin{aligned} \tilde{g}_{(1)}(X) &\equiv_{\pi^s} g_{(1)}(X)\,, \\ \tilde{g}_{(2)}(X) &\equiv_{\pi^s} g_{(2)}(X) \end{aligned}$$

and

$$f(X) \equiv_{\pi^{2s}} \tilde{g}_{(1)}(X) \cdot \tilde{g}_{(2)}(X)\,.$$

□

3.3 Newton-Hensel

3.3.1 Lifting roots

Remark 28. *Let R be a commutative ring.*

Let $w \in R$. Let $f(X) \in R[X]$.

Then we have the first degree Taylor expansion

$$f(X) \;=\; f(w) + (X-w)f'(w) + \mathrm{O}((X-w)^2)\;.$$

Proof. We consider $f(X) - f(w)$. By polynomial division by $(X-w)$ we have

$$f(X) - f(w) \;=\; (X-w)h(X) + r$$

for a polynomial $h(X) \in R[X]$ and $r \in R$.

Evaluation at w yields $r \;=\; 0$.

So we have

$$f(X) \;=\; f(w) + (X-w)h(X)\;.$$

Now we consider $h(X)$. Likewise, we have

$$h(X) \;=\; h(w) + (X-w)k(X)\;.$$

for a polynomial $k(X) \in R[X]$.

Hence

$$f(X) \;=\; f(w) + (X-w)h(w) + (X-w)^2k(X)\;.$$

Deriving yields

$$f'(X) \;=\; h(w) + 2(X-w)k(X) + (X-w)^2k'(X)\;.$$

Evaluation at w yields $h(w) \;=\; f'(w)$.

So

$$f(X) \;=\; f(w) + (X-w)f'(w) + \mathrm{O}((X-w)^2)\;.$$

□

Lemma 29. *Let R be a discrete valuation ring, with maximal ideal generated by $\pi \in R$.*

Let $f(X) \in R[X]$ be a polynomial. Let $w \in R$ be such that $f'(w) \neq 0$. Suppose given $d \in \mathbb{Z}$ such that

$$(\triangleright) \qquad \mathrm{v}_\pi\left(\frac{f(w)}{f'(w)}\right) \;=\; \mathrm{v}_\pi(f(w)) - \mathrm{v}_\pi(f'(w)) \;\geq\; d \;>\; \mathrm{v}_\pi(f'(w)) \;=:\; a \;\geq\; 0\;.$$

Note that

$$f(w) \;\equiv_{\pi^{2a}}\; 0\;.$$

Then there exists $\tilde{w} \in R$, unique modulo $\pi^{2d-a}R$, such that

$$\begin{aligned} \tilde{w} &\equiv_{\pi^d} w \,, \\ f(\tilde{w}) &\equiv_{\pi^{2d}} 0 \,. \end{aligned}$$

We call such an element $\tilde{w} \in R$ an admissible lift *of $w \in R$ with respect to d.*

In addition, for any admissible lift $\tilde{w}$ of $w \in R$ with respect to d we have

$$\mathrm{v}_\pi(f(\tilde{w})) > \mathrm{v}_\pi(f(w)) \quad \textit{if} \quad d = \mathrm{v}_\pi(f(w)) - \mathrm{v}_\pi(f'(w)) \,,$$

and we have

$$\mathrm{v}_\pi(f(\tilde{w})) > 2\,\mathrm{v}_\pi(f'(\tilde{w})) = 2\,\mathrm{v}_\pi(f'(w)) \,.$$

Proof. For *existence,* we let

$$\tilde{w} := w - \frac{f(w)}{f'(w)} \,.$$

Note that $\tilde{w} \equiv_{\pi^d} w$.

We have

$$\begin{aligned} f(\tilde{w}) &= f(w - \tfrac{f(w)}{f'(w)}) \\ &\overset{\text{R. 28}}{=} f(w) - \tfrac{f(w)}{f'(w)} f'(w) + \mathrm{O}((\tfrac{f(w)}{f'(w)})^2) \\ &= 0 + \mathrm{O}((\tfrac{f(w)}{f'(w)})^2). \end{aligned}$$

So

$$f(\tilde{w}) \equiv_{\pi^{2d}} 0 \,.$$

Now we show *uniqueness* modulo $\pi^{2d-a}R$.

Recall that

$$\begin{aligned} \tilde{w} &\equiv_{\pi^d} w \,, \\ f(\tilde{w}) &\equiv_{\pi^{2d}} 0 \,. \end{aligned}$$

Suppose given $\hat{w} \in R$ such that

$$\begin{aligned} \hat{w} &\equiv_{\pi^d} w \,, \\ f(\hat{w}) &\equiv_{\pi^{2d}} 0 \,. \end{aligned}$$

We have to show that

$$\tilde{w} \overset{!}{\equiv}_{\pi^{2d-a}} \hat{w} \,.$$

Let $\tilde{z} \in R$ be such that

$$\tilde{w} = w + \pi^d \tilde{z} \,.$$

So

$$\begin{aligned} f(\tilde{w}) &= f(w + \pi^d \tilde{z}) \\ &\overset{\text{R. 28}}{=} f(w) + \pi^d \tilde{z} f'(w) + \mathrm{O}(\pi^{2d}) \,. \end{aligned}$$

So

$$f(\tilde{w}) \equiv_{\pi^{2d}} f(w) + \pi^d \tilde{z} f'(w) \,.$$

Likewise, for $\hat{\tilde{w}} = w + \pi^d \hat{\tilde{z}}$, where $\hat{\tilde{z}} \in R$, we have

$$f(\hat{\tilde{w}}) \equiv_{\pi^{2d}} f(w) + \pi^d \hat{\tilde{z}} f'(w) \,.$$

So we have

$$f(w) + \pi^d \tilde{z} f'(w) \equiv_{\pi^{2d}} f(\tilde{w}) \equiv_{\pi^{2d}} 0 \equiv_{\pi^{2d}} f(\hat{\tilde{w}}) \equiv_{\pi^{2d}} f(w) + \pi^d \hat{\tilde{z}} f'(w) \,.$$

It follows that

$$\pi^d \tilde{z} f'(w) \equiv_{\pi^{2d}} \pi^d \hat{\tilde{z}} f'(w) \,.$$

So

$$\tilde{z} f'(w) \equiv_{\pi^d} \hat{\tilde{z}} f'(w) \,.$$

So

$$\tilde{z} \equiv_{\pi^{d-a}} \hat{\tilde{z}} \,.$$

Hence

$$\tilde{w} = w + \pi^d \tilde{z} \equiv_{\pi^{2d-a}} w + \pi^d \hat{\tilde{z}} = \hat{\tilde{w}} \,.$$

Finally, we show that the *additional assertions* hold for an element $\hat{\tilde{w}} \in R$ such that

$$(*) \qquad \hat{\tilde{w}} \equiv_{\pi^d} w \,,$$
$$(**) \qquad f(\hat{\tilde{w}}) \equiv_{\pi^{2d}} 0 \,.$$

Again, we write $\hat{\tilde{w}} = w + \pi^d \hat{\tilde{z}}$, where $\hat{\tilde{z}} \in R$; cf. $(*)$.

If $d = \mathrm{v}_\pi(f(w)) - \mathrm{v}_\pi(f'(w))$, then

$$\begin{aligned} \mathrm{v}_\pi(f(\hat{\tilde{w}})) &\overset{(**)}{\geq} 2d \\ &= 2\big(\mathrm{v}_\pi(f(w)) - \mathrm{v}_\pi(f'(w))\big) \\ &= \mathrm{v}_\pi(f(w)) + \big(\mathrm{v}_\pi(f(w)) - 2\,\mathrm{v}_\pi(f'(w))\big) \\ &\overset{(\triangleright)}{>} \mathrm{v}_\pi(f(w)) \,; \end{aligned}$$

note that $f(w) \neq 0$.

We have

$$\begin{aligned} f'(\hat{\tilde{w}}) &= f'(w + \pi^d \hat{\tilde{z}}) \\ &\overset{\text{R. 28}}{=} f'(w) + \pi^d \hat{\tilde{z}} f''(w) + \mathrm{O}((\pi^d \hat{\tilde{z}})^2) \,. \end{aligned}$$

Note that $d > a = \mathrm{v}_\pi(f'(w))$. It follows that $f'(\hat{\tilde{w}}) \equiv_{\pi^d} f'(w) \not\equiv_{\pi^d} 0$.

So $\mathrm{v}_\pi(f'(\hat{\tilde{w}})) = \mathrm{v}_\pi(f'(w)) < d$.

Hence

$$\mathrm{v}_\pi(f(\hat{\tilde{w}})) \overset{(**)}{\geq} 2d > 2\,\mathrm{v}_\pi(f'(\hat{\tilde{w}})) = 2\,\mathrm{v}_\pi(f'(w)) \,.$$

□

Theorem 30. *Let R be a complete discrete valuation ring. Let $\pi \in R$ be a generator of the maximal ideal of R.*

Let $f(X) \in R[X]$ be a polynomial. Let $w \in R$ be such that $f'(w) \neq 0$ and

$$\mathrm{v}_\pi(f(w)) \;>\; 2\,\mathrm{v}_\pi(f'(w))\;.$$

Write

$$d \;:=\; \mathrm{v}_\pi(f(w)) - \mathrm{v}_\pi(f'(w))\;.$$

Then there exists a unique element $\overset{\vee}{w} \in R$ such that

$$\begin{aligned} \overset{\vee}{w} &\equiv_{\pi^d} w\;, \\ f(\overset{\vee}{w}) &= 0\;. \end{aligned}$$

In addition, we have

$$\mathrm{v}_\pi(f'(\overset{\vee}{w})) \;=\; \mathrm{v}_\pi(f'(w))\;.$$

Proof. We show *existence* of $\overset{\vee}{w}$.

We want to construct a sequence $(w_i)_{i\geq 1}$ in R and a sequence $(d_i)_{i\geq 1}$ in $\mathbb{Z}_{\geq 0}$ such that $w_1 = w$ and $d_1 = d$ and such that

$$\begin{aligned} d_i &< d_{i+1} \\ w_i &\equiv_{\pi^{d_i}} w_{i+1} \\ f(w_{i+1}) &\equiv_{\pi^{2d_i}} 0 \\ \mathrm{v}_\pi(f'(w_{i+1})) &= \mathrm{v}_\pi(f'(w_i)) \end{aligned}$$

for $i \geq 1$.

Then, letting

$$\overset{\vee}{w} \;:=\; \lim_i w_i\;,$$

we have

$$\overset{\vee}{w} \;=\; \lim_i w_i \;\overset{\text{R. 69}}{\equiv_{\pi^d}}\; \lim_i w_1 \;=\; w_1 \;=\; w$$

and

$$f(\overset{\vee}{w}) \;=\; f(\lim_i w_i) \;\overset{\text{R. 71}}{=}\; \lim_i f(w_i) \;\overset{\text{R. 67}}{=}\; 0\;.$$

Furthermore, we have

$$\mathrm{v}_\pi(f'(\overset{\vee}{w})) \;=\; \mathrm{v}_\pi(f'(\lim_i w_i)) \;\overset{\text{R. 71}}{=}\; \mathrm{v}_\pi(\lim_i f'(w_i)) \;\overset{\text{R. 66}}{=}\; \lim_i \mathrm{v}_\pi(f'(w_i)) \;=\; \mathrm{v}_\pi(f'(w))\;.$$

So we have to construct such a sequence.

Let $w_1 := w$ and $d_1 := d$.

Step 1. It follows by Lemma 29 that there exists $w_2 \in R$ such that

$$\begin{aligned} w_2 &\equiv_{\pi^{d_1}} w_1\;, \\ f(w_2) &\equiv_{\pi^{2d_1}} 0 \end{aligned}$$

and

$$\begin{aligned} \mathrm{v}_\pi(f(w_2)) &> \mathrm{v}_\pi(f(w_1)) \,, \\ \mathrm{v}_\pi(f(w_2)) &> 2\,\mathrm{v}_\pi(f'(w_2)) = 2\,\mathrm{v}_\pi(f'(w_1)) \,. \end{aligned}$$

We define

$$d_2 := \mathrm{v}_\pi(f(w_2)) - \mathrm{v}_\pi(f'(w_2)) \,.$$

Then

$$\begin{aligned} d_2 &= \mathrm{v}_\pi(f(w_2)) - \mathrm{v}_\pi(f'(w_2)) \\ &> \mathrm{v}_\pi(f(w_1)) - \mathrm{v}_\pi(f'(w_2)) \\ &= \mathrm{v}_\pi(f(w_1)) - \mathrm{v}_\pi(f'(w_1)) \\ &= d_1 \,. \end{aligned}$$

Step 2. It follows by Lemma 29 that there exists $w_3 \in R$ such that

$$\begin{aligned} w_3 &\equiv_{\pi^{d_2}} w_2 \,, \\ f(w_3) &\equiv_{\pi^{2d_2}} 0 \end{aligned}$$

and

$$\begin{aligned} \mathrm{v}_\pi(f(w_3)) &> \mathrm{v}_\pi(f(w_2)) \,, \\ \mathrm{v}_\pi(f(w_3)) &> 2\,\mathrm{v}_\pi(f'(w_3)) = 2\,\mathrm{v}_\pi(f'(w_2)) \,. \end{aligned}$$

We define

$$d_3 := \mathrm{v}_\pi(f(w_3)) - \mathrm{v}_\pi(f'(w_3)) \,.$$

Then

$$\begin{aligned} d_3 &= \mathrm{v}_\pi(f(w_3)) - \mathrm{v}_\pi(f'(w_3)) \\ &> \mathrm{v}_\pi(f(w_2)) - \mathrm{v}_\pi(f'(w_3)) \\ &= \mathrm{v}_\pi(f(w_2)) - \mathrm{v}_\pi(f'(w_2)) \\ &= d_2 \,. \end{aligned}$$

Steps ≥ 3. Continue as above.

We show *uniqueness* of $\overset{\vee}{w}$.

Suppose given $\overset{\vee}{w} \in R$ such that

$$\begin{aligned} \overset{\vee}{w} &\equiv_{\pi^d} w \,, \\ f(\overset{\vee}{w}) &= 0 \,. \end{aligned}$$

and $\overset{\vee\vee}{w} \in R$ such that

$$\begin{aligned} \overset{\vee\vee}{w} &\equiv_{\pi^d} w \\ f(\overset{\vee\vee}{w}) &= 0 \,. \end{aligned}$$

We have to show that $\overset{\vee}{w} \overset{!}{=} \overset{\vee\vee}{w}$.

Write $a := \mathrm{v}_\pi(f'(w))$. Both $\overset{\vee}{w}$ and $\overset{\vee\vee}{w}$ are admissible lifts of w with respect to d in the sense of Lemma 29. Therefore $\mathrm{v}_\pi(f'(\overset{\vee}{w})) = a = \mathrm{v}_\pi(f'(\overset{\vee\vee}{w}))$ by Lemma 29.

Let $d_1 := d$. Both $\overset{\vee}{w}$ and $\overset{\vee\vee}{w}$ are admissible lifts of $\overset{\vee}{w}$ with respect to d_1 in the sense of Lemma 29, since

$$\begin{aligned} \overset{\vee}{w} &\equiv_{\pi^{d_1}} \overset{\vee}{w} , \\ f(\overset{\vee}{w}) &\equiv_{\pi^{2d_1}} 0 , \\ \overset{\vee\vee}{w} &\equiv_{\pi^{d_1}} \overset{\vee}{w} , \\ f(\overset{\vee\vee}{w}) &\equiv_{\pi^{2d_1}} 0 . \end{aligned}$$

So Lemma 29 yields

$$\overset{\vee}{w} \equiv_{\pi^{2d_1-a}} \overset{\vee\vee}{w} .$$

Let $d_2 := 2d_1 - a$. Note that $d_2 = d_1 + (d_1 - a) > d_1 > a$. Both $\overset{\vee}{w}$ and $\overset{\vee\vee}{w}$ are admissible lifts of $\overset{\vee}{w}$ with respect to d_2 in the sense of Lemma 29, since

$$\begin{aligned} \overset{\vee}{w} &\equiv_{\pi^{d_2}} \overset{\vee}{w} , \\ f(\overset{\vee}{w}) &\equiv_{\pi^{2d_2}} 0 , \\ \overset{\vee\vee}{w} &\equiv_{\pi^{d_2}} \overset{\vee}{w} , \\ f(\overset{\vee\vee}{w}) &\equiv_{\pi^{2d_2}} 0 . \end{aligned}$$

So Lemma 29 yields

$$\overset{\vee}{w} \equiv_{\pi^{2d_2-a}} \overset{\vee\vee}{w} .$$

Let $d_3 := 2d_2 - a$. Note that $d_3 = d_2 + (d_2 - a) > d_2 > a$. Continue as above.

This yields a strictly increasing sequence $(d_\ell)_{\ell \geq 1}$ of integers such that

$$\overset{\vee}{w} \equiv_{\pi^{d_\ell}} \overset{\vee\vee}{w} \qquad \text{for } \ell \geq 1.$$

Hence

$$\overset{\vee}{w} = \overset{\vee\vee}{w} .$$

□

3.3.2 Comparison of Hensel and Newton-Hensel

Let R be a discrete valuation ring. Let $\pi \in R$ be a generator of the maximal ideal of R.

Let $f(X) \in R[X]$ be a monic polynomial with $\deg f \geq 2$. Let $w \in R$ be such that $f(w) \neq 0$. Write

$$\begin{aligned} s &:= \mathrm{v}_\pi(f(w)) , \\ t'' &:= \mathrm{v}_\pi(f'(w)) . \end{aligned}$$

Suppose that

$$s > 2t'' .$$

1. We want to apply Hensel, i.e. Lemma 16, to lift w.

By polynomial division, we have $f(X) = (X - w) \cdot g_{(2)}(X) + f(w) \equiv_{\pi^s} (X - w) \cdot g_{(2)}(X)$ for some monic polynomial $g_{(2)}(X) \in R[X]$.

Write $g_{(1)}(X) := X - w$. Then

$$f(X) \equiv_{\pi^s} g_{(1)}(X) \cdot g_{(2)}(X) \, .$$

Since

$$f'(X) \equiv_{\pi^s} g_{(1)}(X) \cdot g'_{(2)}(X) + g'_{(1)}(X) \cdot g_{(2)}(X) = (X - w) \cdot g'_{(2)}(X) + g_{(2)}(X) \, ,$$

we have

$$f'(w) \equiv_{\pi^s} g_{(2)}(w) \, .$$

Since $t'' < s$, this implies

$$t'' = \mathrm{v}_\pi(f'(w)) = \mathrm{v}_\pi(g_{(2)}(w)) \overset{\text{Ex. } 7}{=} \mathrm{v}_\pi(\mathrm{Res}(X - w, \, g_{(2)}(X))) = \mathrm{v}_\pi(\mathrm{Res}(g_{(1)}, \, g_{(2)})) \, .$$

In particular, this resultant does not vanish.

Lemma 16.(1) yields monic polynomials $\tilde{g}_{(1)}(X) \, , \, \tilde{g}_{(2)}(X) \in R[X]$ with the following properties.

- $X - \hat{w} := \tilde{g}_{(1)}(X) \equiv_{\pi^{s-t''}} g_{(1)}(X) = X - w$
- $\tilde{g}_{(2)}(X) \equiv_{\pi^{s-t''}} g_{(2)}(X)$
- $f(X) \equiv_{\pi^{2(s-t'')}} \tilde{g}_{(1)}(X) \cdot \tilde{g}_{(2)}(X) = (X - \hat{w}) \cdot \tilde{g}_{(2)}(X)$

In particular, comparing the constant coefficients resp. plugging in $\hat{w}$, we obtain

- $\hat{w} \equiv_{\pi^{s-t''}} w$,
- $f(\hat{w}) \equiv_{\pi^{2(s-t'')}} 0$.

2. We want to apply Newton-Hensel, i.e. Lemma 29, to lift w.

Since $2t'' < s$, we have $f'(w) \neq 0$.

Write

$$d := \mathrm{v}_\pi(f(w)) - \mathrm{v}_\pi(f'(w)) = s - t'' \, .$$

By assumption, we have $d > \mathrm{v}_\pi(f'(w)) = t''$.

Lemma 29 yields an admissible lift $\tilde{w} \in R$ of w with respect to d, i.e. we have the following properties.

- $\tilde{w} \equiv_{\pi^d} w$
- $f(\tilde{w}) \equiv_{\pi^{2d}} 0$

The admissible lift is uniquely determined modulo $\pi^{2d-t''}R$.

3. Comparison of Hensel and Newton-Hensel via Newton-Hensel.

Recall that $d = s - t''$.

So

- $\hat{\hat{w}} \equiv_{\pi^d} w$,
- $f(\hat{\hat{w}}) \equiv_{\pi^{2d}} 0$.

So both $\hat{\hat{w}}$ from 1. and $\tilde{w}$ from 2. are admissible lifts of w with respect to d. The uniqueness from 2. now guarantees that

$$\hat{\hat{w}} \equiv_{\pi^{2d-t''}} \tilde{w} .$$

4. Comparison of Hensel and Newton-Hensel via Hensel.

We want to use the uniqueness assertion of Lemma 16.(2) to recover the result in 3.

Recall that $d = s - t''$ and that

- $X - \hat{\hat{w}} = \tilde{g}_{(1)}(X) \equiv_{\pi^{s-t''}} g_{(1)}(X) = X - w$,
- $\tilde{g}_{(2)}(X) \equiv_{\pi^{s-t''}} g_{(2)}(X)$,
- $f(X) \equiv_{\pi^{2(s-t'')}} \tilde{g}_{(1)}(X) \cdot \tilde{g}_{(2)}(X) = (X - \hat{\hat{w}}) \cdot \tilde{g}_{(2)}(X)$.

On the other hand, polynomial division yields

$$f(X) = (X - \tilde{w}) \cdot \tilde{h}_{(2)}(X) + f(\tilde{w}) \equiv_{\pi^{2d}} (X - \tilde{w}) \cdot \tilde{h}_{(2)}(X) .$$

Writing $\tilde{h}_{(1)}(X) := X - \tilde{w}$, we have

$$f(X) \equiv_{\pi^{2d}} \tilde{h}_{(1)}(X) \cdot \tilde{h}_{(2)}(X)$$

We have $\tilde{w} \equiv_{\pi^d} w \equiv_{\pi^d} \hat{\hat{w}}$, and so

$$\tilde{h}_{(1)}(X) = X - \tilde{w} \equiv_{\pi^d} X - w.$$

Moreover,

$$\tilde{h}_{(1)}(X) \cdot \tilde{h}_{(2)}(X) \equiv_{\pi^{2d}} f(X) \equiv_{\pi^{2d}} \tilde{g}_{(1)}(X) \cdot \tilde{g}_{(2)}(X) .$$

So

$$\begin{aligned} \tilde{g}_{(1)}(X) \cdot \tilde{h}_{(2)}(X) &\equiv_{\pi^d} (X - w) \cdot \tilde{h}_{(2)}(X) \\ &\equiv_{\pi^d} \tilde{h}_{(1)}(X) \cdot \tilde{h}_{(2)}(X) \\ &\equiv_{\pi^d} \tilde{g}_{(1)}(X) \cdot \tilde{g}_{(2)}(X) \\ &\equiv_{\pi^d} \tilde{g}_{(1)}(X) \cdot g_{(2)}(X) . \end{aligned}$$

Since $\tilde{g}_{(1)}(X) = X - \hat{\hat{w}}$ is not a zero divisor in ${}^{R}\!/_{\pi^d}[X]$, we conclude that

$$\tilde{h}_{(2)}(X) \equiv_{\pi^d} g_{(2)}(X) .$$

So we may apply Lemma 16.(2) with $r := 0$ to get

$$\tilde{g}_{(1)}(X) \equiv_{\pi^{2d-t''}} \tilde{h}_{(1)}(X) ,$$

i.e.

$$\hat{\hat{w}} \equiv_{\pi^{2d-t''}} \tilde{w} .$$

Chapter 4

Examples

4.1 Construction of examples

To illustrate Theorem 17 we consider some polynomials in the complete discrete valuation ring $\mathbb{Z}_p$ for a prime number p. We turn Lemma 16 into an algorithm and iterate it a few times. Given a polynomial in $\mathbb{Z}[X] \subseteq \mathbb{Z}_p[X]$ and a factor decomposition in $\mathbb{Z}[X]$ to a certain p-adic precision, this algorithm returns a factor decomposition in $\mathbb{Z}[X]$ to a higher p-adic precision.

We use the notation of Lemma 16.

We choose the initial precision to be $t + 1$.

Let s be the current precision.

Write

$$\begin{aligned} g_{(k)}(X) &=: \sum_{j \in [0, m_{(k)}]} c_{(k)j} X^j \\ \tilde{g}_{(k)}(X) &=: \sum_{j \in [0, m_{(k)}]} \tilde{c}_{(k)j} X^j \end{aligned}$$

for $k \in [1, n]$, where $c_{(k)j}\,,\ \tilde{c}_{(k)j} \in \mathbb{Z}$.

Let the *deviation* be

$$s' := \min \{ \mathrm{v}_\pi(c_{(k)j} - \tilde{c}_{(k)j}) : k \in [1, n],\ j \in [0, m_{(k)}] \} .$$

By Lemma 16, we have $s' \geq s - t''$.

Let the *defect* be $s - s'$. The defect is bounded above by t''.

Let

$$\begin{aligned} f(X) &=: \sum_{j \in [0, M]} \lambda_j X^j \\ \prod_{k \in [1, n]} \tilde{g}_{(k)}(X) &=: \sum_{j \in [0, M]} \mu_j X^j \end{aligned}$$

where $\lambda_j\,,\ \mu_j \in \mathbb{Z}$.

Let the (maximal possible) precision for the subsequent step be

$$\tilde{s} := \min \{ \mathrm{v}_\pi(\lambda_j - \mu_j) : j \in [0, M] \} .$$

By Lemma 16, we have $\tilde{s} \geq 2(s - t'')$. Recall that $2s' \geq 2(s - t'')$.

Let the *surplus* be $\tilde{s} - 2s'$; cf. Conjecture 59 below.

In the examples below we will concentrate on the following observables.

- The current p-adic precision s, resulting from the initial data resp. the previous step.
- The deviation.
- The defect.
- The surplus.

We use the computer algebra system MAGMA [**1**] (student version of V2.16-13) and the following code.

```
Z := Integers();
Q := FieldOfFractions(Z);
PQ<X> := PolynomialRing(Q);
p := 5;                                        // prime number under consideration

f := PQ!(X^6 - 6*X^3 - 6*X^2 - 5*X + 2);      // polynomial f(X) under considera-
                                               // tion; cf. Example 55 below
t := Valuation(Discriminant(f),p);             // t

R := pAdicRing(p,t+1);
PR<X> := PolynomialRing(R);
g_fac := Factorisation(PR!f);
g := &cat[[PQ!g_fac[i][1] : j in [1..g_fac[i][2]]] : i in [1..#g_fac]];
n := #g;
M := Degree(f);                                //  M
m := [Degree(u) : u in g];                     // m_(1),...,m_(n)
mm := [0] cat [&+[m[i] : i in [1..k]] : k in [1..n]];
                                               // m^(0),...,m^(n)
print "initial decomposition:", [g[i] : i in [1..n]];
f_approx := &*[PQ!g[i] : i in [1..n]];         // product of g_(1),...,g_(n)

s := t+1;                                      // current precision

MS := RMatrixSpace(Rationals(),M,M);           // calculation of valuation of
                                               // discriminant
A := MS!0;
for k in [1..n] do
 a := Coefficients(&*[g[i] : i in [1..n] | i ne k]);
 for j in [1..m[k]] do
  for r in [0..#a-1] do
```

```
   A[mm[k]+j,j+r] := a[r+1];                //  A(g_(1),...,g_(n))
  end for;
 end for;
end for;
tt := Valuation(Determinant(A),p);        // t''

while f ne f_approx do
 b := p^(tt-s)*PQ!(f - &*g);
 beta := Coefficients(b);
 VS := RMatrixSpace(Rationals(),1,M);
 betavec := VS!0;
 for i in [1..#beta] do
  betavec[1,i] := beta[i];
 end for;
                                          //  (beta_0,...,beta_{M-1})
 MS := RMatrixSpace(Rationals(),M,M);
 A := MS!0;
 for k in [1..n] do
  a := Coefficients(&*[g[i] : i in [1..n] | i ne k]);
  for j in [1..m[k]] do
   for r in [0..#a-1] do
    A[mm[k]+j,j+r] := a[r+1];              //  A(g_(1),...,g_(n))
   end for;
  end for;
 end for;

 print "valuation of resultant = ", Valuation(Determinant(A),p);
                                          // returns  v_pi( Res(g_(1),...,g_(n)) ),
                                          // known to be equal to  t''

 U := betavec * A^-1;
 u := [&+[U[1,mm[k] + i + 1] * (PQ!X)^i : i in [0..m[k]-1]] : k in [1..n]];
 gg := [g[k] + p^(s-tt)*u[k] : k in [1..n]];
                                          //  g~_(1),...,g~_(n)

 cdg := &cat[Coefficients(gg[i] - g[i]) : i in [1..n]];
                                          // ask for variation of new factors
 min_val_cdg := Minimum([Valuation(cdg[i],p) : i in [1..#cdg]]);
 print "deviation = ", min_val_cdg;       // returns deviation s~

 print "defect = ", s - min_val_cdg, "(bounded above by", tt, ")";
                                          // returns defect s - s~ (<= t'')

 f_approx := &*[PQ!gg[i] : i in [1..n]];  // product of g~_(1),...,g~_(n)
```

```
 c := Coefficients(f - f_approx);
 s := Minimum([Valuation(c[i],p) : i in [1..#c]]);
 print "s = ",s;                                  // returns the "new" s for the next
                                                  // induction step (the "best" s we
                                                  // can get, the increment from
                                                  // "old" s to "new" s can be greater
                                                  // than 1)
 print "surplus = ", s - 2*min_val_cdg;
 g := [PQ!PolynomialRing(pAdicRing(p,s))!gg[i] : i in [1..n]];
                                                  // choice of inverse image
 print "g = ", g;                                 // returns the list g̃_(1), ..., g̃_(n)
                                                  // of the factors of the output
                                                  // factorisation of this step,
                                                  // which is the input factorisation
                                                  // of the next step
end while;
```

The factorisations modulo powers of p and the observed parameters depend on the choice of the inverse images in the last but one step; cf. Examples 35, 36 below. Therefore, in some examples we shall record not only the observed parameters, but also the lifted decompositions of $f(X)$ modulo some powers of p that result from the choices made by Magma.

If $f(X) \equiv_\pi X^M$ and the degrees of the factors $g_{(k)}(X)$ are sorted increasingly, then this algorithm is at the same time an implementation of the proof of Lemma 22, carrying an extra factor $\pi^{t''-t'''}$ along, which appears on both sides of the equation $U \cdot A(g_{(1)}\,,\,\ldots\,,\,g_{(n)}) = (\beta_0\,\ldots\,\beta_{M-1})$, as the reader may check by comparison with the proof of Lemma 16. In this case, the defect $s - s'$ is bounded above by t'''; cf. Lemma 22.

In the Examples 48, 49 below, we raise the initial precision from $t+1$ a bit. This will be indicated there.

4.2 Examples for $p = 2$

Example 31. We consider the polynomial

$$f(X) = X^3 + X^2 - 2X + 8$$

at $p = 2$.

This polynomial is also used as an example in [**7,** §3.12, Einleitung zu §4, §4.4].

We start with initial precision $s = 3$.

We consider the development of the factors $g_{(1)}(X)$, $g_{(2)}(X)$, $g_{(3)}(X)$ during steps 1 to 6, starting with the initial factorisation during step 1.

step 1	$g_{(1)}(X) = X$
	$g_{(2)}(X) = X + 2$
	$g_{(3)}(X) = X + 7$
step 2	$g_{(1)}(X) = X + 12$
	$g_{(2)}(X) = X + 14$
	$g_{(3)}(X) = X + 7$
step 3	$g_{(1)}(X) = X + 52$
	$g_{(2)}(X) = X + 54$
	$g_{(3)}(X) = X + 23$
step 4	$g_{(1)}(X) = X + 980$
	$g_{(2)}(X) = X + 470$
	$g_{(3)}(X) = X + 599$
step 5	$g_{(1)}(X) = X + 167380$
	$g_{(2)}(X) = X + 224214$
	$g_{(3)}(X) = X + 132695$
step 6	$g_{(1)}(X) = X + 1339592148$
	$g_{(2)}(X) = X - 4836725802$
	$g_{(3)}(X) = X + 3497133655$

We obtain the following results in the first 10 steps. The defect is bounded above by $t'' = 1$.

step	current precision s	deviation s'	defect	surplus
1	3	2	1	0
2	4	3	1	0
3	6	5	1	0
4	10	9	1	0
5	18	17	1	0
6	34	33	1	0
7	66	65	1	0
8	130	129	1	0
9	258	257	1	0
10	514	513	1	0

The defect seems to be constant with value 1. The surplus seems to be constant with value 0. We observe that the defect is maximal.

Note that in step 1, the precision grows only by 1; cf. Lemma 25.

Example 32. We consider the polynomial

$$f(X) = X^5 - 3X^2 + X - 3$$

at $p = 2$. We start with initial precision $s = 5$.

We consider the development of the factors $g_{(1)}(X)$ and $g_{(2)}(X)$ during steps 1 to 6, starting with the initial factorisation during step 1.

step 1	$g_{(1)}(X) = X^2 + 22X + 29$ $g_{(2)}(X) = X^3 + 10X^2 + 7X + 1$
step 2	$g_{(1)}(X) = X^2 + 438X + 861$ $g_{(2)}(X) = X^3 + 586X^2 + 519X + 289$
step 3	$g_{(1)}(X) = X^2 + 201142X + 102237$ $g_{(2)}(X) = X^3 + 847434X^2 + 794119X + 477473$
step 4	$g_{(1)}(X) = X^2 + 251921633718X + 311299247965$ $g_{(2)}(X) = X^3 - 251921633718X^2 - 495014109689X + 194909784353$
step 5	$g_{(1)}(X) = X^2 - 270217790319937134063178X - 54492371411137001098051 5$ $g_{(2)}(X) = X^3 + 270217790319937134063178X^2 + 421158365255857157709319X$ $- 13413327363756387157372 7$
step 6	$g_{(1)}(X) = X^2 + 116184103518671414448200427670327657267801378450 2X$ $-889614967501437839019879131291973122959543107 5$ $g_{(2)}(X) = X^3 - 116184103518671414448200427670327657267801378450 2X^2$ $+ 123265486076297715444438036145045917106971424307 9X$ $- 254604116792662003423810497290610860675602888415$

We obtain the following results in the first 10 steps. The defect is bounded above by $t'' = 0$.

step	current precision s	deviation s'	defect	surplus
1	5	5	0	0
2	10	10	0	0
3	20	20	0	0
4	40	40	0	0
5	80	80	0	1
6	161	161	0	0
7	322	322	0	0
8	644	644	0	3
9	1291	1291	0	1
10	2583	2583	0	0

Example 33. We consider the polynomial

$$f(X) \;=\; X^{10} + 3X^5 + 2X^3 + X^2 + 3X - 2$$

at $p = 2$. We start with initial precision $s = 10$.

We consider the development of the factors $g_{(1)}(X)$, ..., $g_{(5)}(X)$ during steps 1 to 4, starting with the initial factorisation during step 1.

step 1	$g_{(1)}(X) = X + 198$ $g_{(2)}(X) = X^2 + 308X + 863$ $g_{(3)}(X) = X^2 + 214X + 719$ $g_{(4)}(X) = X^2 + 949X + 425$ $g_{(5)}(X) = X^3 + 379X^2 + 766X + 413$
step 2	$g_{(1)}(X) = X + 63686$ $g_{(2)}(X) = X^2 + 187188X + 14687$ $g_{(3)}(X) = X^2 + 234198X + 92367$ $g_{(4)}(X) = X^2 + 86965X + 154025$ $g_{(5)}(X) = X^3 + 214395X^2 + 178942X + 252317$
step 3	$g_{(1)}(X) = X - 24530323258$ $g_{(2)}(X) = X^2 + 4237482804X - 811320993$ $g_{(3)}(X) = X^2 + 23559377622X + 6353938639$ $g_{(4)}(X) = X^2 - 3594955851X - 28305630807$ $g_{(5)}(X) = X^3 + 328418683X^2 + 6572129022X + 25297148317$
step 4	$g_{(1)}(X) = X + 10327978227227752646$ $g_{(2)}(X) = X^2 + 1144098589728048975 88X - 363420929239795091105$ $g_{(3)}(X) = X^2 + 180813564266353234646X - 100058002576128775985$ $g_{(4)}(X) = X^2 + 176420897432331178933X + 393619519059755948457$ $g_{(5)}(X) = X^3 - 481972298898717063813X^2 - 536752069698591737090X$ $+ 303003932483942341021$

We obtain the following results in the first 10 steps. The defect is bounded above by $t'' = 2$.

step	current precision s	deviation s'	defect	surplus
1	10	9	1	0
2	18	18	0	0
3	36	35	1	0
4	70	69	1	0
5	138	137	1	0
6	274	273	1	0

step	current precision s	deviation s'	defect	surplus
7	546	545	1	0
8	1090	1089	1	0
9	2178	2177	1	0
10	4354	4353	1	0

We observe that the defect seems to be eventually constant with value 1. The surplus seems to be constant with value 0.

Example 34. We consider the polynomial

$$f(X) \;=\; X^{10} - 3X^5 + 3X^4 - 2X^3 - 2X^2 - 3X - 2$$

at $p = 2$. We start with initial precision $s = 3$, for which we have the initial factorisation into the factors

$$\begin{aligned} g_{(1)}(X) &= X + 6 \\ g_{(2)}(X) &= X + 5 \\ g_{(3)}(X) &= X + 3 \\ g_{(4)}(X) &= X^3 + 4X^2 + 5X + 5 \\ g_{(5)}(X) &= X^4 + 6X^3 + 7X + 3\,. \end{aligned}$$

We obtain the following results in the first 16 steps. The defect is bounded above by $t'' = 1$.

step	current precision s	deviation s'	defect	surplus
1	3	3	0	0
2	6	6	0	0
3	12	12	0	0
4	24	24	0	0
5	48	48	0	0
6	96	96	0	0
7	192	192	0	0
8	384	383	1	0
9	766	765	1	0
10	1530	1529	1	0
11	3058	3057	1	0
12	6114	6113	1	0
13	12226	12225	1	0

step	current precision s	deviation s'	defect	surplus
14	24450	24449	1	0
15	48898	48897	1	0
16	97794	97793	1	0

We observe that the defect seems to be eventually constant with value 1. The surplus seems to be constant with value 0.

Example 35. We consider the polynomial

$$f(X) = X^5 + 3X^2 - 3X + 3$$

at $p = 2$. We start with initial precision $s = 5$.

We consider the development of the factors $g_{(1)}(X)$ and $g_{(2)}(X)$ during steps 1 to 6, starting with the initial factorisation during step 1.

step 1	$g_{(1)}(X) = X^2 + 14X + 21$ $g_{(2)}(X) = X^3 + 18X^2 + 15X + 23$
step 2	$g_{(1)}(X) = X^2 + 1518X + 1333$ $g_{(2)}(X) = X^3 + 530X^2 + 1039X + 1879$
step 3	$g_{(1)}(X) = X^2 + 2678254X + 734517$ $g_{(2)}(X) = X^3 + 1516050X^2 + 3773455X + 3252055$
step 4	$g_{(1)}(X) = X^2 + 981553700334X - 969776876235$ $g_{(2)}(X) = X^3 - 981553700334X^2 + 5362836673551X + 3109471493975$
step 5	$g_{(1)}(X) = X^2 + 13685657801432377892017713 4X + 662832354847452086326531 09$ $g_{(2)}(X) = X^3 - 13685657801432377892017713 4X^2 + 637828420283861750320711 83X$ $+ 12949023479342753096673672 7$
step 6	$g_{(1)}(X) = X^2 + 824220678029113832562081071371447801152187218185988 94X$ $- 856980319605578481334196012439686147220285639741139 95$ $g_{(2)}(X) = X^3 - 824220678029113832562081071371447801152187218185988 94X^2$ $- 229187902787981212042334078514639304246392089365985 13X$ $- 604333949486002452348234473287400426822770809455494 81$

We obtain the following results in the first 12 steps. The defect is bounded above by $t'' = 0$.

step	current precision s	deviation s'	defect	surplus
1	5	5	0	1
2	11	11	0	0
3	22	22	0	0

step	current precision s	deviation s'	defect	surplus
4	44	44	0	0
5	88	88	0	1
6	177	178	0	0
7	356	357	-1	2
8	716	716	-1	1
9	1433	1433	0	1
10	2867	2868	0	0
11	5736	5736	-1	0
12	11472	11472	0	0

We observe that the defect is negative in certain steps.

Example 36. We consider the polynomial

$$f(X) = X^5 + 3X^2 - 3X + 3$$

at $p = 2$. We start with initial precision $s = 5$.

This is the same polynomial as in Example 35. We will vary the inverse images chosen in the last but one step of the algorithm, to the effect that the factors $g_{(k)}(X)$ will change, and so will all of the observed parameters.

We consider the development of the factors $g_{(1)}(X)$ and $g_{(2)}(X)$ during steps 1 to 6, starting with the initial factorisation during step 1.

step 1	$g_{(1)}(X) = X^2 + 14X + 21$ $g_{(2)}(X) = X^3 + 18X^2 + 15X + 23$
step 2	$g_{(1)}(X) = X^2 + 1518X + 3381$ $g_{(2)}(X) = X^3 + 530X^2 + 1039X + 3927$
step 3	$g_{(1)}(X) = X^2 + 2678254X + 13317429$ $g_{(2)}(X) = X^3 + 5710354X^2 + 7967759X + 15834967$
step 4	$g_{(1)}(X) = X^2 - 51795004432914X + 86991153345845$ $g_{(2)}(X) = X^3 + 51795004432914X^2 + 5362836673551X + 196623517982551$
step 5	$g_{(1)}(X) = X^2 + 942140687265467584066360881 4X + 2668199408012042111896382 3925$ $g_{(2)}(X) = X^3 - 942140687265467584066360881 4X^2 + 6827528616710763124816332 95X$ $+ 1715116577496740631082969 4807$
step 6	$g_{(1)}(X) = X^2 - 3478185148689606014439618676053238914721109630785835061 0X$ $+ 4792022823738461826034396131400152285620386318989474665 49$ $g_{(2)}(X) = X^3 + 3478185148689606014439618676053238914721109630785835061 0X^2$ $+ 1911558999327408369589995582291496067260130662834677729 43X$ $+ 5677291644958632217765327501118608124880605676880790567 27$

We obtain the following results in the first 12 steps. The defect is bounded above by $t'' = 0$.

step	current precision s	deviation s'	defect	surplus
1	5	5	0	1
2	11	11	0	1
3	23	23	0	1
4	47	47	0	0
5	94	94	0	0
6	188	188	0	0
7	376	376	0	3
8	755	755	0	0
9	1510	1510	0	0
10	3020	3020	0	0
11	6040	6040	0	1
12	12081	12081	0	0

Cf. the table in the preceding Example 35, dealing with the same polynomial.

Example 37. We consider the polynomial

$$f(X) = X^{10} - 3X^5 - 3X^4 - 2X^3 + 3X^2 - 3X - 1$$

at $p = 2$. We start with initial precision $s = 9$, for which we have the initial factorisation into the factors

$$\begin{aligned} g_{(1)}(X) &= X^2 + 100X + 359 \\ g_{(2)}(X) &= X^3 + 375X^2 + 183X + 143 \\ g_{(3)}(X) &= X^5 + 37X^4 + 191X^3 + 365X^2 + 66X + 71. \end{aligned}$$

We obtain the following results in the first 13 steps. The defect is bounded above by $t'' = 2$.

step	current precision s	deviation s'	defect	surplus
1	9	8	1	0
2	16	16	0	0
3	32	31	1	0
4	62	62	0	0
5	124	124	0	0
6	248	247	1	0

step	current precision s	deviation s'	defect	surplus
7	494	494	0	0
8	988	988	0	0
9	1976	1976	0	0
10	3952	3951	1	0
11	7902	7901	1	0
12	15802	15802	0	0
13	31604	31604	0	0

The defect seems to be non-periodic. The surplus seems to be constant with value 0.

Example 38. We consider the polynomial

$$f(X) \;=\; X^{10} - 3X^5 - 3X^4 - 2X^3 - X^2 - 3X + 3$$

at $p = 2$. We start with initial precision $s = 9$, for which we have the initial factorisation into the factors

$$\begin{aligned} g_{(1)}(X) &= X^2 + 28X + 375 \\ g_{(2)}(X) &= X^3 + 215X^2 + 199X + 123 \\ g_{(3)}(X) &= X^5 + 269X^4 + 231X^3 + 177X^2 + 394X + 239\ . \end{aligned}$$

We obtain the following results in the first 13 steps. The defect is bounded above by $t'' = 2$.

step	current precision s	deviation s'	defect	surplus
1	9	8	1	0
2	16	16	0	0
3	32	31	1	0
4	62	61	1	0
5	122	122	0	0
6	244	244	0	0
7	488	488	0	0
8	976	975	1	0
9	1950	1950	0	0
10	3900	3900	0	0
11	7800	7799	1	0
12	15598	15597	1	0
13	31194	31194	0	0

The defect does not seem to show a regular behaviour, whereas the surplus seems to be constant with value 0.

Example 39. We consider the polynomial

$$f(X) \;=\; X^8 + 3072X^2 + 16384$$

at $p = 2$. We start with initial precision $s = 103$, for which we have the initial factorisation into the factors

$$\begin{aligned} g_{(1)}(X) &= X + 480683502420016498820359772498 0 \\ g_{(2)}(X) &= X - 480683502420016498820359772498 0 \\ g_{(3)}(X) &= X^6 - 109306212419814278046624855998 4X^4 \\ &\quad -4943636030726675686411786481408X^2 - 434114347446031754105233109094 4. \end{aligned}$$

We obtain the following results in the first 10 steps. The defect is bounded above by $t'' = 23$. Since $f(X) \equiv_2 X^8$, the defect is even bounded above by $t''' = 22$.

step	current precision s	deviation s'	defect	surplus
1	103	100	3	0
2	200	196	4	0
3	392	387	5	0
4	774	773	1	0
5	1546	1537	9	0
6	3074	3071	3	0
7	6142	6135	7	0
8	12270	12267	3	0
9	24534	24527	7	0
10	49054	49051	3	0

The defect does not seem to show a regular behaviour, whereas the surplus seems to be constant with value 0.

Example 40. We consider the polynomial

$$f(X) \;=\; X^8 + 3072X^2 + 49152$$

at $p = 2$. We start with initial precision $s = 103$, for which we have the initial factorisation into the factors

$$\begin{aligned} g_{(1)}(X) &= X^2 - 45183253138908130722393783278 56 \\ g_{(2)}(X) &= X^3 + 365684051531283273805999838977 2X^2 \\ &\quad -3029064992395295772940018582304X + 955005618431619133244515494176 \\ g_{(3)}(X) &= X^3 - 365684051531283273805999838977 2X^2 \\ &\quad -3029064992395295772940018582304X - 955005618431619133244515494176. \end{aligned}$$

We obtain the following results in the first 10 steps. The defect is bounded above by $t'' = 38$. Since $f(X) \equiv_2 X^8$, the defect is even bounded above by $t''' = 33$.

step	current precision s	deviation s'	defect	surplus
1	103	95	8	0
2	190	187	3	0
3	374	371	3	0
4	742	741	1	0
5	1482	1475	7	0
6	2950	2947	3	0
7	5894	5893	1	0
8	11786	11779	7	0
9	23558	23555	3	0
10	47110	47107	3	0

The defect does not seem to show a regular behaviour, except for seemingly eventually having values in $\{1, 3, 7\}$, whereas the surplus seems to be constant with value 0.

4.3 Examples for $p = 3$

Example 41. We consider the polynomial

$$f(X) \;=\; X^3 + X^2 - X + 17$$

at $p = 3$. We start with initial precision $s = 3$.

We consider the development of the factors $g_{(1)}(X)$, $g_{(2)}(X)$, $g_{(3)}(X)$ during steps 1 to 6, starting with the initial factorisation during step 1.

step 1	$g_{(1)}(X) = X + 22$ $g_{(2)}(X) = X + 16$ $g_{(3)}(X) = X + 17$
step 2	$g_{(1)}(X) = X + 49$ $g_{(2)}(X) = X + 475$ $g_{(3)}(X) = X + 206$
step 3	$g_{(1)}(X) = X + 42574$ $g_{(2)}(X) = X + 4606$ $g_{(3)}(X) = X + 11870$
step 4	$g_{(1)}(X) = X + 372543349$ $g_{(2)}(X) = X + 73382830$ $g_{(3)}(X) = X + 328914800$

step 5	$g_{(1)}(X) = X - 7088836743567680$
	$g_{(2)}(X) = X + 4687989319796947$
	$g_{(3)}(X) = X + 2400847423770734$
step 6	$g_{(1)}(X) = X + 153893879658084666895915951639 3$
	$g_{(2)}(X) = X + 359818658350036450642759160294 8$
	$g_{(3)}(X) = X - 513712538008121117538675111934 0$

We obtain the following results in the first 10 steps. The defect is bounded above by $t'' = 1$.

step	current precision s	deviation s'	defect	surplus
1	3	3	0	0
2	6	5	1	0
3	10	9	1	0
4	18	17	1	0
5	34	33	1	0
6	66	65	1	0
7	130	129	1	0
8	258	257	1	0
9	514	513	1	0
10	1026	1025	1	0

The defect seems to be eventually constant with value 1. The surplus seems to be constant with value 0.

Example 42. We consider the polynomial

$$f(X) = X^6 - X^4 - 6X^3 - 4X^2 + 6X - 5$$

at $p = 3$. We start with initial precision $s = 7$, for which we have the initial factorisation into the factors

$$\begin{aligned} g_{(1)}(X) &= X + 193 \\ g_{(2)}(X) &= X + 418 \\ g_{(3)}(X) &= X^2 + 160X + 388 \\ g_{(4)}(X) &= X^2 + 1416X + 88. \end{aligned}$$

We obtain the following results in the first 10 steps. The defect is bounded above by $t'' = 2$.

step	current precision s	deviation s'	defect	surplus
1	7	5	2	0
2	10	8	2	0
3	16	14	2	0

step	current precision s	deviation s'	defect	surplus
4	28	26	2	0
5	52	50	2	0
6	100	98	2	0
7	196	194	2	0
8	388	386	2	0
9	772	770	2	0
10	1540	1538	2	0

The defect seems to be constant with value 2, assuming its upper bound. The surplus seems to be constant with value 0.

Example 43. We consider the polynomial

$$f(X) = X^{10} - 243X^2 + 236196$$

at $p = 3$. We start with initial precision $s = 61$, for which we have the initial factorisation into the factors

$$\begin{aligned} g_{(1)}(X) &= X^2 - 1304211831974468171155230 0219 \\ g_{(2)}(X) &= X^8 + 1304211831974468171155230 0219X^6 - 5603241534654939981270859 0278X^4 \\ &\quad +1108734947610472709411868 2187X^2 + 5147473462895057364480039 2019. \end{aligned}$$

We obtain the following results in the first 11 steps. The defect is bounded above by $t'' = 10$. Since $f(X) \equiv_3 X^{10}$, the defect is even bounded above by $t''' = 9$.

step	current precision s	deviation s'	defect	surplus
1	61	61	0	0
2	122	117	5	0
3	234	234	0	0
4	468	463	5	0
5	926	926	0	0
6	1852	1847	5	0
7	3694	3694	0	1
8	7389	7384	5	0
9	14768	14768	0	0
10	29536	29531	5	0
11	59062	59062	0	0

The defect seems to be periodic.

Example 44. We consider the polynomial

$$f(X) = X^{10} + 54X - 243$$

at $p = 3$. We start with initial precision $s = 46$, for which we have the initial factorisation into the factors

$$\begin{aligned} g_{(1)}(X) &= X + 1254845291302170687078 \\ g_{(2)}(X) &= X^3 + 34391148802997285953 29X^2 + 20979122552691595182 84X \\ &\quad + 2387878303991212496958 \\ g_{(3)}(X) &= X^6 + 4168977948050601813522X^5 + 3414335924445189447372X^4 \\ &\quad - 4695237998019536297 10X^3 - 3733781694469525960542X^2 \\ &\quad + 2741122263554615006433X + 3057293995913895085035. \end{aligned}$$

We obtain the following results in the first 10 steps. The defect is bounded above by $t'' = 13$. Since $f(X) \equiv_3 X^{10}$, the defect is even bounded above by $t''' = 10$.

step	current precision s	deviation s'	defect	surplus
1	46	43	3	0
2	86	86	0	0
3	172	169	3	0
4	338	336	2	0
5	672	671	1	0
6	1342	1340	2	0
7	2680	2679	1	0
8	5358	5356	2	0
9	10712	10711	1	0
10	21422	21420	2	0

The defect seems to be eventually periodic. The surplus seems to be constant with value 0.

Example 45. We consider the polynomial

$$f(X) = X^{10} - 81X^3 - 81X^2 - 729$$

at $p = 3$. We start with initial precision $s = 47$.

We consider the development of the factors $g_{(1)}(X)$, ..., $g_{(4)}(X)$ during steps 1 to 3, starting with the initial factorisation during step 1.

step 1	$g_{(1)}(X) = X^2 + 12476944095490426480470X - 1827344990806843265208$ $g_{(2)}(X) = X^2 + 11518164134498883612837X - 12549192272943808130988$ $g_{(3)}(X) = X^2 - 12773699960698996533003X + 9393800803929134496474$ $g_{(4)}(X) = X^4 - 11221408269290313560304X^3 - 13772989526932563242294X^2$ $+ 6835699768973000181444X + 947509305312943983276$
step 2	$g_{(1)}(X) = X^2 + 368207490382041805893628621819338729275289 99X$ $- 916244767344391614554214440980172287935101 16$ $g_{(2)}(X) = X^2 - 277261219531483993108945527466032937862299 50X$ $- 291527411655902047313240170888143858718501686$ $g_{(3)}(X) = X^2 + 427355500659942511785229103689015435437460 20X$ $+ 129174542220527722811394650759681492356179021$ $g_{(4)}(X) = X^4 - 518301771510500324569912198042321226850450 69X^3$ $- 310935444659398389059157508266271062110634234X^2$ $- 112957315355865865126419592237912544154306729X$ $+ 762721859326053211606998197935283610557397$
step 3	$g_{(1)}(X) = X^2 - 605530929980921660332245016906262173086430328368742930472184361$ $85420971015221857399431 1X$ $+ 918926257469138886460314038887305156968527094049781390041951308060 92$ 5288617133009893775 $g_{(2)}(X) = X^2 - 369868036870631621880839969214336444736844751753786276981911243902 2$ $93329411539036368303X$ $- 145643038384702576548519246014016296841671032377956934590931977586310$ 65713212604431968 $g_{(3)}(X) = X^2 + 233666271795760139053133361773706784522988036161900433192477822 0$ $60047620773937457457413 2X$ $- 246734803358080184235065809342398992208062154686495179362558122869 64$ 21429683703706552171 $g_{(4)}(X) = X^4 - 136126375110604810831824863161646922740660528149647512447068261$ $48439731681759798472115 18X^3$ $- 206346843405541203798544553027752563222393203581480667752973981190658$ $67922720565499398 14X^2$ $+ 148790794853483852003901684335044551123177762468777949446884221282 17$ $49540492433306914356X$ $+ 308496030839379767632955227064666461026707595977052367282835137341 4$ 525331518388254410666

Here, linebreaks within the coefficients have not been marked.

We obtain the following results in the first 12 steps. The defect is bounded above by $t'' = 18$. Since $f(X) \equiv_3 X^{10}$, the defect is even bounded above by $t''' = 9$.

step	current precision s	deviation s'	defect	surplus
1	47	47	0	0
2	94	92	2	0
3	184	183	1	0
4	366	365	1	1
5	731	729	2	0
6	1458	1458	0	0
7	2916	2915	1	0
8	5830	5829	1	1
9	11659	11657	2	1
10	23315	23314	1	1
11	46629	46627	2	0
12	93254	93253	1	0

Example 46. We consider the polynomial

$$f(X) = X^{24} + 531441X^4 + 531441$$

at $p = 3$. We start with initial precision $s = 301$, for which we have the initial factorisation into the factors

$$\begin{aligned}
g_{(1)}(X) &= X^4 + 14724340788178134468602169629772161096878074740071686087025456851825017837 \\
&\quad 364402715632580564561503823223852911353633300356150742086651378447097 0X^2 \\
&\quad -134673399860164952991074852935458232488015158715254166032786719208542941262090 \\
&\quad 794861453991303805126404787629525118667078587150413177025416305 30 \\
g_{(2)}(X) &= X^4 - 14724340788178134468602169629772161096878074740071686087025456851825017 8 \\
&\quad 373644027156325805645615038232238529113536333003561507420866513784470970X^2 \\
&\quad -134673399860164952991074852935458232488015158715254166032786719208542941 26 \\
&\quad 209079486145399130380512640478762952511866707858715041317702541630530 \\
g_{(3)}(X) &= X^8 - 62942469501026597767591231977176276190897020816815178805910850728180625835 \\
&\quad 990237634124872720415893813970667048997521316706755048931584880492700X^6 \\
&\quad -381420207040120764995320213468103479030354625984773199300878813624609864847563 \\
&\quad 77515847494960712069527462736826329199717957000303873582308805587X^4 \\
&\quad +991101794055664064799809916911611862489257036046149283841323481526112806202 0 \\
&\quad 326913441412862546062480595951148238801022561618590311462904029127X^2 \\
&\quad -80331493820623699708496779868282809371116563747245822593957133701905353703 20 \\
&\quad 131073404613089525652743243502486090233743965972429961763121157251 0
\end{aligned}$$

$$
\begin{aligned}
g_{(4)}(X) \;=\;& X^8 + 62942469501026597767591231977176276190897020816815178805910850728180625835990237634124872720415893813970667048997521316706755048931584880492700X^6 \\
&-38142020704012076499532021346810347903035462598477319930087881362460986484756377515847494960712069527462736826329199717957000303873582308805587X^4 \\
&-99110179405566406479980991691161186248925703604614928384132348152611280620203269134414128625460624805959511482388010225616185903114629040291 27X^2 \\
&-80331493820623699708496779868282809371116563747245822593957133701905353703201310734046130895256527432435024860902337439659724299617631211572510.
\end{aligned}
$$

Here, linebreaks within the coefficients have not been marked.

We obtain the following results in the first 10 steps. The defect is bounded above by $t'' = 112$. Since $f(X) \equiv_3 X^{24}$, the defect is even bounded above by $t''' = 71$.

step	current precision s	deviation s'	defect	surplus
1	301	296	5	0
2	592	592	0	0
3	1184	1178	6	0
4	2356	2353	3	0
5	4706	4705	1	0
6	9410	9406	4	0
7	18812	18809	3	0
8	37618	37616	2	0
9	75232	75231	1	0
10	150462	150457	5	0

The defect seems to be unperiodic. The surplus seems to be constant with value 0.

4.4 Examples for $p = 5$

Example 47. We consider the polynomial

$$f(X) = X^8 + X^7 + X^6 - 7X^5 - 2X^4 - 2X^3 + 6X^2 + 6X + 6$$

at $p = 5$. We start with initial precision $s = 6$.

We consider the development of the factors $g_{(1)}(X)$ and $g_{(2)}(X)$ during steps 1 to 6, starting with the initial factorisation during step 1.

step 1	$g_{(1)}(X) = X^2 + 12828X + 13401$
	$g_{(2)}(X) = X^6 + 2798X^5 + 106X^4 + 3602X^3 + 13661X^2 + 1913X + 13981$
step 2	$g_{(1)}(X) = X^2 + 25075328X + 27310276$
	$g_{(2)}(X) = X^6 + 219065298X^5 + 49265731X^4 + 20378602X^3 + 97216786X^2 + 44767538X$ $+ 168404606$
step 3	$g_{(1)}(X) = X^2 - 7379844457346547X - 11525498507845974$
	$g_{(2)}(X) = X^6 + 7379844457346548X^5 - 7563817821828019X^4 + 15329971211784852X^3$ $+ 5360665624560536X^2 + 26040840620939413X - 19943609206595394$
step 4	$g_{(1)}(X) = X^2 + 11936727647072475410620900945032 8X - 13460364196882151480535136445647 24$
	$g_{(2)}(X) = X^6 - 11936727647072475410620900945032 7X^5 - 15707463666486780719101312983905 19X^4$ $- 12450705332192045296910859171213 98X^3 + 74072521678935337602716953081053 6X^2$ $+ 53776092755757662277774857992378 8X + 68080936943281755837212565668585 6$
step 5	$g_{(1)}(X) = X^2 - 52470468459504744579233037600586547682762934932594373114850823465 47X$ $- 30367332962987097427778704257867992271100728041060682157145722990 99$
	$g_{(2)}(X) = X^6 + 52470468459504744579233037600586547682762934932594373114850823465 48X^5$ $+ 55664106756183317352619039995346297113847918652702494323369633282 31X^4$ $- 61938756389751113975573816000695414290653649693739260915375772776 48X^3$ $+ 51931224694053674959076673558928128517763878760819488726285151855 36X^2$ $+ 57646684484717905699196034913085574351265611887017152841572713300 38X$ $+ 33001790064530214035415730161272598466510480559276142955875707483 56$
step 6	$g_{(1)}(X) = X^2 - 10677900254920587690854693998545400435937161647779940338625521507744$ $06995485505559148005012302577833266298096455507089569457319085184 22X$ $- 42944655235434308633528577318782825355156413990431410919093585777260685 1$ $02333044493673331336557414927983542792000376101354228242522 24$
	$g_{(2)}(X) = X^6 + 10677900254920587690854693998545400435937161647779940338625521507744$ $06995485505559148005012302577833266298096455507089569457319085184 23X^5$ $- 18784007206703372994836187497587830749138682006351924329513255144287062 95$ $22841350306516450471199696989693442350851115174704778515187394X^4$ $- 10486334078937092086306206518576027904336899751682245228338560580981397 87$ $67282625667703991310604765112481317854577155097890243631965148X^3$ $- 17488587164688837971993616152482049530617869066380391423333450485512 4857$ $96846167494126777856814137718114744894697033267677205532270508 9X^2$ $+ 13091338148026411152976534867706488568595635980086349863181215303484007 9$ $38046812875528576156197806136259262020104248466711597489828316 3X$ $- 38544210800342953639425160333309594482479150654214477820131917250437896$ $61040319178645717414293203949491170916935605151852725886987828 94$

Here, linebreaks within the coefficients have not been marked.

We obtain the following results in the first 15 steps. The defect is bounded above by $t'' = 0$.

step	current precision s	deviation s'	defect	surplus
1	6	6	0	0
2	12	12	0	0
3	24	24	0	0
4	48	48	0	0
5	96	96	0	0
6	193	193	0	1
7	386	386	0	0
8	772	772	0	0
9	1544	1544	0	0
10	3088	3088	0	0
11	6176	6176	0	0
12	12352	12352	0	0
13	24704	24704	0	0
14	49408	49408	0	0
15	98816	98816	0	0

The defect seems to be constant with value 0.

Example 48. We consider the polynomial

$$f(X) = X^8 + X^4 + 5X^3 + X^2 - 2X + 3$$

at $p = 5$. The valuation t of its discriminant equals 0.

We start with initial precision $s = 5$ $(> t + 1)$.

We consider the development of the factors $g_{(1)}(X)$ and $g_{(2)}(X)$ during steps 1 to 5, starting with the initial factorisation during step 1.

step 1	$g_{(1)}(X) = X + 2678$ $g_{(2)}(X) = X^7 + 447X^6 + 2934X^5 + 2123X^4 + 2107X^3 + 1209X^2 + 2924X + 776$
step 2	$g_{(1)}(X) = X + 5615178$ $g_{(2)}(X) = X^7 + 4150447X^6 + 9127934X^5 + 6286498X^4 + 9186482X^3 + 8610584X^2$ $+ 8859174X + 900776$
step 3	$g_{(1)}(X) = X + 30097427490178$ $g_{(2)}(X) = X^7 - 30097427490178X^6 + 14052987643559X^5 + 6347232848998X^4$ $+ 45739345123982X^3 - 33239796076916X^2 - 4896993093951X$ $- 12793348708599$

step 4	$g_{(1)}(X) = X - 619520783612888756332275447$ $g_{(2)}(X) = X^7 + 619520783612888756332275447X^6 - 19542098336218693393463408 16X^5$ $+ 23569302845629755549965208 73X^4 - 25348722248927612674908135 18X^3$ $+ 39349076523184443908191574 59X^2 + 71813798825616346848542167 4X$ $- 10876957389600881717666773 49$
step 5	$g_{(1)}(X) = X + 30789449742415249093673722950308622757326586872047436517 8$ $g_{(2)}(X) = X^7 - 30789449742415249093673722950308622757326586872047436517 8X^6$ $+ 52262327363840820833270663086160605930507292495370456059X^5$ $- 39725222713563242215285290725424468086772832235760113537 7X^4$ $- 91817401850569154993050791836393466063436427310831112601 8X^3$ $+ 19358464478600284610015692050576624453055855288080939183 4X^2$ $- 20245633911529642450613405134581988869799428114766531451X$ $+ 77602627724531590072464347156601803898186606081504972890 1$

We obtain the following results in the first 14 steps. The defect is bounded above by $t'' = 0$.

step	current precision s	deviation s'	defect	surplus
1	5	5	0	0
2	10	10	0	0
3	20	20	0	0
4	40	40	0	2
5	82	82	0	0
6	164	164	0	1
7	329	329	0	0
8	658	658	0	0
9	1316	1316	0	0
10	2632	2632	0	1
11	5265	5265	0	2
12	10532	10532	0	0
13	21064	21064	0	0
14	42128	42128	0	0

The defect seems to be constant with value 0, whereas the surplus seems to be non-periodic.

Example 49. We consider the polynomial

$$f(X) = X^{10} - 2X^5 - 2X^4 + X^3 + 3X^2 - 3X + 3$$

at $p = 5$. The valuation t of its discriminant equals 0.

We start with initial precision $s = 6$ ($> t + 1$).

We consider the development of the factors $g_{(1)}(X)$ and $g_{(2)}(X)$ during steps 1 to 4, starting with the initial factorisation during step 1.

step 1	$g_{(1)}(X) = X + 9758$ $g_{(2)}(X) = X^9 + 5867X^8 + 15439X^7 + 2488X^6 + 3346X^5 + 5980X^4 + 6533X^3 + 987X^2 + 9482X + 5891$
step 2	$g_{(1)}(X) = X - 5851552742$ $g_{(2)}(X) = X^9 + 5851552742X^8 - 2221187686X^7 - 13406419387X^6 - 7214309154X^5 + 10736537230X^4 - 11602946592X^3 - 8929577138X^2 + 14798087607X + 12999412141$
step 3	$g_{(1)}(X) = X - 1963549745336662099617$ $g_{(2)}(X) = X^9 + 1963549745336662099617X^8 - 1413636760622338375186X^7 + 2254176923204367018113X^6 - 1680427973548474074779X^5 - 1032566939137212681520X^4 - 2271480125194708415342X^3 - 2138946050423968639638X^2 + 785796165206448478232X - 189622104307782090035 9$
step 4	$g_{(1)}(X) = X + 28625481978418765095927674831030214921972 58$ $g_{(2)}(X) = X^9 - 28625481978418765095927674831030214921972 58X^8 + 92785805367767044711424802607727944096716 89X^7 - 10794283425533751284198443960360120828294387X^6 + 92399664233452904605138642173500865483147 1X^5 + 41853240692228960794106976033108017521622 30X^4 + 21799484536720176447206745080530584654127 83X^3 + 35948331952708427795886093044340425840947 37X^2 - 19475578983860853559143433885576939421467 68X - 88683292292611083795754574722065604869159 84$

We obtain the following results in the first 13 steps. The defect is bounded above by $t'' = 0$.

step	current precision s	deviation s'	defect	surplus
1	6	6	0	3
2	15	15	0	1
3	31	31	0	0
4	62	62	0	0
5	124	124	0	1
6	249	249	0	1
7	499	499	0	1

step	current precision s	deviation s'	defect	surplus
8	999	999	0	0
9	1998	1998	0	0
10	3996	3996	0	0
11	7992	7992	0	0
12	15984	15984	0	0
13	31968	31968	0	0

The defect seems to be constant with value 0.

Example 50. We consider the polynomial

$$f(X) = X^{10} - 5X^5 + 5X^4 - 2X^3 + 2X^2 - 5X + 5$$

at $p = 5$. We start with initial precision $s = 4$, for which we have the initial factorisation into the factors

$$\begin{aligned} g_{(1)}(X) &= X^2 + 565 \\ g_{(2)}(X) &= X + 366 \\ g_{(3)}(X) &= X + 396 \\ g_{(4)}(X) &= X^3 + 540X^2 + 146X + 506 \\ g_{(5)}(X) &= X^3 + 573X^2 + 577X + 272. \end{aligned}$$

We obtain the following results in the first 10 steps. The defect is bounded above by $t'' = 1$.

step	current precision s	deviation s'	defect	surplus
1	4	3	1	0
2	6	5	1	0
3	10	9	1	0
4	18	17	1	0
5	34	33	1	0
6	66	65	1	0
7	130	129	1	0
8	258	257	1	0
9	514	513	1	0
10	1026	1025	1	0

The defect seems to be constant with value 1. The surplus seems to be constant with value 0.

Example 51. We consider the polynomial

$$f(X) = X^{10} - 5X^5 + 2X^4 - 3X^3 - 5X^2 - 5X - 5$$

at $p = 5$. We start with initial precision $s = 7$, for which we have the initial factorisation into the factors

$$\begin{aligned} g_{(1)}(X) &= X^3 + 32960X^2 + 27750X + 53060 \\ g_{(2)}(X) &= X + 2537 \\ g_{(3)}(X) &= X + 36187 \\ g_{(4)}(X) &= X + 24719 \\ g_{(5)}(X) &= X^4 + 59847X^3 + 45029X^2 + 50382X + 14882. \end{aligned}$$

We obtain the following results in the first 10 steps. The defect is bounded above by $t'' = 2$.

step	current precision s	deviation s'	defect	surplus
1	7	5	2	0
2	10	8	2	0
3	16	14	2	0
4	28	26	2	0
5	52	50	2	0
6	100	98	2	0
7	196	194	2	0
8	388	386	2	0
9	772	770	2	0
10	1540	1538	2	0

The defect seems to be constant with value 2, assuming its upper bound. The surplus seems to be constant with value 0.

Example 52. We consider the polynomial

$$f(X) = X^5 + X^4 - X^3 - X^2 + 15625$$

at $p = 5$. We start with initial precision $s = 13$, for which we have the initial factorisation into the factors

$$\begin{aligned} g_{(1)}(X) &= X - 272453000 \\ g_{(2)}(X) &= X + 28328000 \\ g_{(3)}(X) &= X^2 - 183124998X - 61062499 \\ g_{(4)}(X) &= X + 427249999. \end{aligned}$$

We obtain the following results in the first 10 steps. The defect is bounded above by $t'' = 3$.

step	current precision s	deviation s'	defect	surplus
1	13	13	0	0
2	26	24	2	0
3	48	45	3	0
4	90	87	3	0
5	174	171	3	0
6	342	339	3	0
7	678	675	3	0
8	1350	1347	3	0
9	2694	2691	3	0
10	5382	5379	3	0

The defect seems to be eventually constant with value 3, assuming its upper bound. The surplus seems to be constant with value 0.

Example 53. We consider the polynomial

$$f(X) = X^{10} + 2X^5 - 2X^4 - 5X^3 + 4X^2 + 2X - 5$$

at $p = 5$. We start with initial precision $s = 7$, for which we have the initial factorisation into the factors

$$\begin{aligned} g_{(1)}(X) &= X + 48635 \\ g_{(2)}(X) &= X + 56492 \\ g_{(3)}(X) &= X + 6742 \\ g_{(4)}(X) &= X^7 + 44381X^6 + 59132X^5 + 1103X^4 + 36075X^3 + 77735X^2 + 17688X + 25683. \end{aligned}$$

We obtain the following results in the first 10 steps. The defect is bounded above by $t'' = 3$.

step	current precision s	deviation s'	defect	surplus
1	7	4	3	0
2	8	5	3	0
3	10	7	3	0
4	14	11	3	0
5	22	19	3	0
6	38	35	3	0

step	current precision s	deviation s'	defect	surplus
7	70	67	3	0
8	134	131	3	0
9	262	259	3	0
10	518	515	3	0

The defect seems to be constant with value 3, assuming its upper bound. The surplus seems to be constant with value 0.

Note that in step 1, the precision grows only by 1.

Example 54. We consider the polynomial

$$f(X) = X^8 + 5^8$$

at $p = 5$. We start with initial precision $s = 57$, for which we have the initial factorisation into the factors

$$\begin{aligned} g_{(1)}(X) &= X^4 + 322978802526335719458155848243791925437 5 \\ g_{(2)}(X) &= X^4 - 322978802526335719458155848243791925437 5. \end{aligned}$$

We obtain the following results in the first 10 steps. The defect is bounded above by $t'' = 16$. Since $f(X) \equiv_5 X^8$, the defect is even bounded above by $t''' = 13$.

step	current precision s	deviation s'	defect	surplus
1	57	57	0	0
2	114	110	4	0
3	220	216	4	0
4	432	428	4	0
5	856	852	4	0
6	1704	1700	4	0
7	3400	3396	4	0
8	6792	6788	4	0
9	13576	13572	4	0
10	27144	27140	4	0

The defect seems to be eventually constant with value 4. The surplus seems to be constant with value 0.

Example 55. We consider the polynomial

$$f(X) = X^6 - 6X^3 - 6X^2 - 5X + 2$$

at $p = 5$. We start with initial precision $s = 4$, for which we have the initial factorisation into the factors

$$\begin{aligned} g_{(1)}(X) &= X + 97 \\ g_{(2)}(X) &= X^2 + 589X + 344 \\ g_{(3)}(X) &= X^3 + 564X^2 + 619X + 589. \end{aligned}$$

We obtain the following results in the first 10 steps. The defect is bounded above by $t'' = 1$.

step	current precision s	deviation s'	defect	surplus
1	4	4	0	0
2	8	8	0	0
3	16	15	1	0
4	30	30	0	0
5	60	59	1	0
6	118	118	0	0
7	236	235	1	0
8	470	470	0	0
9	940	939	1	0
10	1878	1878	0	0

The defect seems to show eventually a periodic behaviour. The surplus seems to be constant with value 0.

Example 56. We consider the polynomial

$$f(X) = X^8 - 4X^5 - X^4 + 3X^3 - X^2 - 4X + 1$$

at $p = 5$. We start with initial precision $s = 7$, for which we have the initial factorisation into the factors

$$\begin{aligned} g_{(1)}(X) &= X + 46886 \\ g_{(2)}(X) &= X + 11288 \\ g_{(3)}(X) &= X^2 + 62726X + 34569 \\ g_{(4)}(X) &= X + 29884 \\ g_{(5)}(X) &= X^3 + 5466X^2 + 1745X + 73242. \end{aligned}$$

We obtain the following results in the first 10 steps. The defect is bounded above by $t'' = 2$.

step	current precision s	deviation s'	defect	surplus
1	7	5	2	0
2	10	10	0	0
3	20	20	0	0
4	40	39	1	0
5	78	77	1	0
6	154	153	1	0
7	306	305	1	0
8	610	610	0	0
9	1220	1218	2	0
10	2436	2436	0	0

The defect seems to show a non-periodic behaviour. The surplus seems to be constant with value 0.

Example 57. We consider the polynomial

$$f(X) = X^{10} + 5X^4 + 2X^3 - 2X^2 + 4X + 5$$

at $p = 5$. We start with initial precision $s = 7$, for which we have the initial factorisation into the factors

$$\begin{aligned} g_{(1)}(X) &= X + 73145 \\ g_{(2)}(X) &= X + 30378 \\ g_{(3)}(X) &= X^2 + 13441X + 63539 \\ g_{(4)}(X) &= X + 55514 \\ g_{(5)}(X) &= X^2 + 19353X + 74958 \\ g_{(6)}(X) &= X^3 + 42544X^2 + 61381X + 39536. \end{aligned}$$

We obtain the following results in the first 10 steps. The defect is bounded above by $t'' = 2$.

step	current precision s	deviation s'	defect	surplus
1	7	5	2	0
2	10	9	1	0
3	18	18	0	0
4	36	34	2	0
5	68	67	1	0
6	134	133	1	0

step	current precision s	deviation s'	defect	surplus
7	266	265	1	0
8	530	529	1	0
9	1058	1057	1	0
10	2114	2114	0	0

The defect seems to show a non-periodic behaviour. The surplus seems to be constant with value 0.

Example 58. We consider the polynomial

$$f(X) = X^8 + 15625X^5 - 15625X^3 - 781250X - 390625$$

at $p = 5$. We start with initial precision $s = 57$, for which we have the initial factorisation into the factors

$$\begin{aligned}
g_{(1)}(X) &= X - 202863311574511330893387561435448614489 5 \\
g_{(2)}(X) &= X - 675463496491321688393531645821676989040 \\
g_{(3)}(X) &= X + 212919704789644146376401307639078756951 5 \\
g_{(4)}(X) &= X + 333752639092427103957708870036174845345 \\
g_{(5)}(X) &= X^2 + 650117238910327529702042488934985953375X \\
&\quad -119665318737239593726127820684931083295 0 \\
g_{(6)}(X) &= X^2 - 408970313662761100096357175185785234300X \\
&\quad -132699697907708527305448713466564403955 0.
\end{aligned}$$

We obtain the following results in the first 10 steps. The defect is bounded above by $t'' = 26$. Since $f(X) \equiv_5 X^8$, the defect is even bounded above by $t''' = 15$.

step	current precision s	deviation s'	defect	surplus
1	57	57	0	0
2	114	112	2	2
3	226	223	3	0
4	446	445	1	0
5	890	889	1	0
6	1778	1777	1	0
7	3554	3553	1	0
8	7106	7106	0	0
9	14212	14210	2	0
10	28420	28419	1	0

The defect seems to show a non-periodic behaviour. The surplus seems to be eventually constant with value 0.

4.5 A conjecture concerning the surplus

Since the observed surplus was nonnegative throughout, the examples in §4.2, §4.3 and §4.4 lend evidence to Conjecture 59 below.

We use the notation of Lemma 16.

Suppose given a prime $p \in \mathbb{Z}$. Suppose that $R = \mathbb{Z}_p$ and $\pi = p$.

Recall that

$$\begin{aligned} g_{(k)}(X) &= \sum_{j\in[0,m_{(k)}]} c_{(k)j} X^j \\ \tilde{g}_{(k)}(X) &= \sum_{j\in[0,m_{(k)}]} \tilde{c}_{(k)j} X^j \ , \end{aligned}$$

where $c_{(k)j}\,,\ \tilde{c}_{(k)j} \ \in \ \mathbb{Z}$ for $k \in [1,n]$ and $j \in [0, m_{(k)}]$, and that the deviation is given by

$$s' \ = \ \min\{\, \mathrm{v}_\pi(c_{(k)j} - \tilde{c}_{(k)j}) \ : \ k \in [1,n],\ j \in [0, m_{(k)}] \,\} \ .$$

Recall that

$$\begin{aligned} f(X) &= \sum_{j\in[0,M]} \lambda_j X^j \\ \prod_{k\in[1,n]} \tilde{g}_{(k)}(X) &= \sum_{j\in[0,M]} \mu_j X^j \end{aligned}$$

where $\lambda_j\,,\ \mu_j \ \in \ \mathbb{Z}$, and that

$$\tilde{s} \ = \ \min\,\{\, \mathrm{v}_\pi(\lambda_j - \mu_j) \ : \ j \in [0, M] \,\} \ .$$

Conjecture 59. *We have*

$$\tilde{s} \ \geq \ 2s' \ ,$$

i.e.

$$f(X) \ \equiv_{\pi^{2s'}} \ \prod_{k\in[1,n]} \tilde{g}_{(k)}(X) \ .$$

Remark 60. By Lemma 16 we have

$$f(X) \ \equiv_{\pi^{2(s-t'')}} \ \prod_{k\in[1,n]} \tilde{g}_{(k)}(X)$$

and

$$s - t'' \ \leq \ s' \ .$$

So if the defect $s - s'$ equals its upper bound t'', then $2(s - t'') = 2s'$, so that Conjecture 59 does not yield anything new in this case.

Appendix A

Complete discrete valuation rings

We collect some well-known basic facts.

Let R be a discrete valuation ring. Let $\pi \in R$ be a generator of the maximal ideal of R.

Definition 61. Let $(a_i)_{i\geq 1}$ be a sequence in R.

(1) Let $\mathrm{v}_\pi(r)$ denote the valuation at π of the element $r \in R$.

(2) We say $(a_i)_{i\geq 1}$ is *convergent* in R with *limit* $a \in R$ if

$$\forall\, M \in \mathbb{N}\ \ \exists\, N \in \mathbb{N}\ :\ \mathrm{v}_\pi(a_i - a) > M \quad \text{for } i \geq N.$$

Remark 62. *Let $(a_i)_{i\geq 1}$ be a convergent sequence in R. Then its limit is unique.*

Proof. Suppose that there exist two limits a and a' of the sequence $(a_i)_{i\geq 1}$.

We have

$$\begin{aligned} \mathrm{v}_\pi(a - a') &= \mathrm{v}_\pi\big((a - a_i) + (a_i - a')\big) \\ &\geq \min\left\{\mathrm{v}_\pi(a - a_i)\,,\, \mathrm{v}_\pi(a_i - a')\right\} \end{aligned}$$

Let $M \in \mathbb{N}$.

We have to show that there exists $N \in \mathbb{N}$ such that

$$\min\left\{\mathrm{v}_\pi(a - a_i)\,,\, \mathrm{v}_\pi(a_i - a')\right\} \ > \ M \quad \text{for } i \geq N.$$

Since $(a_i)_{i\geq 1}$ is convergent with limit a there exists $N_a \in \mathbb{N}$ such that

$$\mathrm{v}_\pi(a - a_i) \ > \ M \quad \text{for } i \geq N_a\,.$$

Since $(a_i)_{i\geq 1}$ is convergent with limit a' there exists $N_{a'} \in \mathbb{N}$ such that

$$\mathrm{v}_\pi(a_i - a') \ > \ M \quad \text{for } i \geq N_{a'}\,.$$

For $N := \max\left\{N_a\,,\, N_{a'}\right\}$ it follows that

$$\min\left\{\mathrm{v}_\pi(a - a_i)\,,\, \mathrm{v}_\pi(a_i - a')\right\} \ > \ M \quad \text{for } i \geq N.$$

So $\mathrm{v}_\pi(a - a') > M$ for $i \geq N$.

Hence $a = a'$. □

Definition 63. Let R be a discrete valuation ring. Let $\pi \in R$ be a generator of the maximal ideal of R.

Let $(a_i)_{i\geq 1}$ be a convergent sequence in R with limit $a \in R$.

We denote the limit a of the sequence $(a_i)_{i\geq 1}$ by $\lim\limits_{i\geq 1} a_i$, i.e.

$$a \;=:\; \lim_{i\geq 1} a_i \;.$$

Definition 64. Let $(a_i)_{i\geq 1}$ be a sequence in R.

(1) We call $(a_i)_{i\geq 1}$ a *Cauchy sequence* in R if

$$\forall\, M \in \mathbb{N} \;\; \exists\, N \in \mathbb{N} \;:\; \mathrm{v}_\pi(a_i - a_j) > M \quad \text{for } i,j \geq N.$$

(2) We say R is *complete* if every Cauchy sequence in R is convergent in R.

Remark 65. *For convergent sequences $(a_i)_{i\geq 1}$ and $(b_i)_{i\geq 1} \in R$ we have*

$$\begin{aligned} (1)\quad \lim_{i\geq 1}(a_i + b_i) &= \lim_{i\geq 1} a_i + \lim_{i\geq 1} b_i \;, \\ (2)\quad \lim_{i\geq 1}(a_i \cdot b_i) &= \lim_{i\geq 1} a_i \cdot \lim_{i\geq 1} b_i \;. \end{aligned}$$

Proof. Denote $\lim\limits_{i\geq 1} a_i =: a$ and $\lim\limits_{i\geq 1} b_i =: b$.

Ad (1).

We have

$$\begin{aligned} \mathrm{v}_\pi\big((a_i + b_i) - (a + b)\big) &= \mathrm{v}_\pi\big((a_i - a) + (b_i - b)\big) \\ &\geq \min\left\{\mathrm{v}_\pi(a_i - a)\,,\, \mathrm{v}_\pi(b_i - b)\right\} \;. \end{aligned}$$

Let $M \in \mathbb{N}$.

We have to show that there exists $N \in \mathbb{N}$ such that

$$\min\left\{\mathrm{v}_\pi(a_i - a)\,,\, \mathrm{v}_\pi(b_i - b)\right\} \;>\; M \quad \text{for } i \geq N.$$

Since $(a_i)_{i\geq 1}$ is convergent there exists $N_a \in \mathbb{N}$ such that

$$\mathrm{v}_\pi(a_i - a) \;>\; M \quad \text{for } i \geq N_a \,.$$

Since $(b_i)_{i\geq 1}$ is convergent there exists $N_b \in \mathbb{N}$ such that

$$\mathrm{v}_\pi(b_i - b) \;>\; M \quad \text{for } i \geq N_b \,.$$

For $N := \max\left\{N_a\,,\, N_b\right\}$ it follows that

$$\min\left\{\mathrm{v}_\pi(a_i - a)\,,\, \mathrm{v}_\pi(b_i - b)\right\} \;>\; M \quad \text{for } i \geq N.$$

So $\mathrm{v}_\pi\big((a_i + b_i) - (a + b)\big) > M$ for $i \geq N$.

Hence $\lim\limits_{i\geq 1}(a_i + b_i) = \lim\limits_{i\geq 1} a_i + \lim\limits_{i\geq 1} b_i$.

Ad (2).

We have

$$\begin{aligned} \mathrm{v}_\pi\big((a_i \cdot b_i) - (a \cdot b)\big) &= \mathrm{v}_\pi\big((a_i - a)b_i + a(b_i - b)\big) \\ &\geq \min\left\{\mathrm{v}_\pi\big((a_i - a)b_i\big)\,,\, \mathrm{v}_\pi\big(a(b_i - b)\big)\right\} \end{aligned}$$

Let $M \in \mathbb{N}$.

We have to show that there exists $N \in \mathbb{N}$ such that

$$\min\left\{\mathrm{v}_\pi\big((a_i - a)b_i\big)\,,\, \mathrm{v}_\pi\big(a(b_i - b)\big)\right\} \;>\; M \quad \text{for } i \geq N.$$

Note that

$$\begin{aligned} \mathrm{v}_\pi\big((a_i - a)b_i\big) &= \mathrm{v}_\pi(a_i - a) + \underbrace{\mathrm{v}_\pi(b_i)}_{\geq 0} \;\geq\; \mathrm{v}_\pi(a_i - a)\,, \\ \mathrm{v}_\pi\big(a(b_i - b)\big) &= \underbrace{\mathrm{v}_\pi(a)}_{\geq 0} + \mathrm{v}_\pi(b_i - b) \;\geq\; \mathrm{v}_\pi(b_i - b)\,. \end{aligned}$$

So we have

$$\min\left\{\mathrm{v}_\pi\big((a_i - a)b_i\big)\,,\, \mathrm{v}_\pi\big(a(b_i - b)\big)\right\} \;\geq\; \min\left\{\mathrm{v}_\pi(a_i - a)\,,\, \mathrm{v}_\pi(b_i - b)\right\}.$$

Since $(a_i)_{i\geq 1}$ is convergent there exists $N_a \in \mathbb{N}$ such that

$$\mathrm{v}_\pi(a_i - a) \;>\; M \quad \text{for } i \geq N_a\,.$$

Since $(b_i)_{i\geq 1}$ is convergent there exists $N_b \in \mathbb{N}$ such that

$$\mathrm{v}_\pi(b_i - b) \;>\; M \quad \text{for } i \geq N_b\,.$$

For $N := \max\left\{N_a\,,\, N_b\right\}$ it follows that

$$\min\left\{\mathrm{v}_\pi\big((a_i - a)b_i\big)\,,\, \mathrm{v}_\pi\big(a(b_i - b)\big)\right\} \;\geq\; \min\left\{\mathrm{v}_\pi(a_i - a)\,,\, \mathrm{v}_\pi(b_i - b)\right\} \;>\; M \quad \text{for } i \geq N.$$

So $\mathrm{v}_\pi\big((a_i \cdot b_i) - (a \cdot b)\big) > M$ for $i \geq N$.

Hence $\lim\limits_{i\geq 1}(a_i \cdot b_i) = \lim\limits_{i\geq 1} a_i \cdot \lim\limits_{i\geq 1} b_i$. □

Remark 66. *Let $(a_i)_{i\geq 1}$ be a convergent sequence in R.*

Then

$$\lim_{i\geq 1} \mathrm{v}_\pi(a_i) \;=\; \mathrm{v}_\pi(\lim_{i\geq 1} a_i)\,.$$

Note that $(\mathrm{v}_\pi(a_i))_{i\geq 1}$ on the lefthand side of the asserted equation is a sequence in $\mathbb{Z}_{\geq 0}$. We understand the limit in $\mathbb{Z}$ as the limit in $\mathbb{R}$ and $\mathbb{Z} \subseteq \mathbb{R}$. So either there exists $k \in \mathbb{N}$ such that $(\mathrm{v}_\pi(a_i))_{i\geq 1}$ is constant for $i \geq k$ or $\lim\limits_{i\geq 1} \mathrm{v}_\pi(a_i) = \infty$.

Proof. Denote $a := \lim_{i\geq 1} a_i$.

First we consider the case $\mathrm{v}_\pi(a) < \infty$.

Since $(a_i)_{i\geq 1}$ is convergent with limit a, we have

$$\forall\, M \in \mathbb{N}\ \exists\, N \in \mathbb{N}\ :\ \mathrm{v}_\pi(a_i - a) > M \quad \text{for } i \geq N.$$

It follows that

$$a\ \equiv_{\pi^M}\ a_i$$

for $i \geq N$. So there exists $r_i \in R$ such that

$$a_i\ =\ a + \pi^M r_i$$

for $i \geq N$, whence

$$\mathrm{v}_\pi(a_i)\ =\ \mathrm{v}_\pi(a + \pi^M r_i)\ .$$

Since $\mathrm{v}_\pi(a)$ is finite, we may choose $M > \mathrm{v}_\pi(a)$ to obtain

$$\mathrm{v}_\pi(a + \pi^M r_i)\ =\ \min\left\{\, \mathrm{v}_\pi(a)\,,\, \mathrm{v}_\pi(\pi^M r_i)\right\}\ =\ \min\left\{\, \mathrm{v}_\pi(a)\,,\, M + \mathrm{v}_\pi(r_i)\right\}\ =\ \mathrm{v}_\pi(a)$$

for $i \geq N$.

So

$$\mathrm{v}_\pi(a_i)\ =\ \mathrm{v}_\pi(a)$$

for $i \geq N$.

Hence

$$\lim_{i\geq 1} \mathrm{v}_\pi(a_i)\ =\ \mathrm{v}_\pi(a)\ =\ \mathrm{v}_\pi(\lim_{i\geq 1} a_i)\ .$$

Now we consider the case $\mathrm{v}_\pi(a) = \infty$.

So $a = 0$.

Since $(a_i)_{i\geq 1}$ is convergent with limit $a = 0$, we have

$$\forall\, M \in \mathbb{N}\ \exists\, N \in \mathbb{N}\ :\ \mathrm{v}_\pi(a_i) > M \quad \text{for } i \geq N.$$

So

$$\lim_{i\geq 1} \mathrm{v}_\pi(a_i)\ =\ \infty\ .$$

Hence

$$\lim_{i\geq 1} \mathrm{v}_\pi(a_i)\ =\ \mathrm{v}_\pi(\lim_{i\geq 1} a_i)\ .$$

□

Remark 67. *Let $(a_i)_{i\geq 1}$ be a sequence in R with $\mathrm{v}_\pi(a_i) < \mathrm{v}_\pi(a_{i+1})$ for $i \geq 1$.*

Then $\lim_{i\geq 1} a_i = 0$.

Proof. By assumption we have $\mathrm{v}_\pi(a_i) \to \infty$ for $i \to \infty$.

So for every $M \in \mathbb{N}$ there exists $N \in \mathbb{N}$ such that $\mathrm{v}_\pi(a_i - 0) = \mathrm{v}_\pi(a_i) > M$ for $i \geq N$. □

Remark 68. *Suppose R to be complete.*

Let $(c_i)_{i\geq 1}$ be a sequence in R. Let $x \in \mathbb{Z}_{\geq 0}$. Suppose that $(\pi^x c_i)_{i\geq 1}$ converges. Then $(c_i)_{i\geq 1}$ converges, and

$$\lim_{i\geq 1} \pi^x c_i \;=\; \pi^x \lim_{i\geq 1} c_i$$

Proof. In view of Remark 65.(2), it suffices to show that $(c_i)_{i\geq 1}$ converges. Since R is complete, it suffices to show that $(c_i)_{i\geq 1}$ is a Cauchy sequence.

Write $d := \lim_{i\geq 1} \pi^x c_i$.

Suppose given $M \in \mathbb{N}$. There exists $N \in \mathbb{N}$ such that $\mathrm{v}_\pi(\pi^x c_i - d) > M + x$ for $i \geq N$.

For $i,\, j \geq N$, we obtain

$$\begin{aligned}
\mathrm{v}_\pi(c_i - c_j) &= \mathrm{v}_\pi(\pi^x c_i - \pi^x c_j) - x \\
&= \mathrm{v}_\pi\big((\pi^x c_i - d) + (d - \pi^x c_j)\big) - x \\
&\geq \min\left\{ \mathrm{v}_\pi(\pi^x c_i - d)\,,\, \mathrm{v}_\pi(d - \pi^x c_j)\right\} - x \\
&> (M + x) - x \\
&= M\,.
\end{aligned}$$

□

Remark 69. *Suppose R to be complete.*

Let $(a_i)_{i\geq 1}$, $(b_i)_{i\geq 1}$ be convergent sequences in R.

Let $x \in \mathbb{Z}_{\geq 0}$.

Suppose that

$$a_i \;\equiv_{\pi^x}\; b_i \quad \forall i \;\geq\; 1\,.$$

Then

$$\lim_{i\geq 1} a_i \;\equiv_{\pi^x}\; \lim_{i\geq 1} b_i\,.$$

Proof. Since $a_i \equiv_{\pi^x} b_i$ for $i \geq 1$, there exists an element $c_i \in R$ such that

$$a_i \;=\; b_i + \pi^x c_i \quad \forall i \;\geq\; 1\,.$$

It follows that

$$\lim_{i\geq 1} a_i \;=\; \lim_{i\geq 1} (b_i + \pi^x c_i)$$

Since $(a_i)_{i\geq 1}$, $(b_i)_{i\geq 1}$ are convergent it follows that $(\pi^x c_i)_{i\geq 1}$ is convergent. By Remark 68, the sequence $(c_i)_{i\geq 1}$ is convergent, and we have $\lim_{i\geq 1} \pi^x c_i = \pi^x \lim_{i\geq 1} c_i$. So by Remark 65 we have

$$\lim_{i\geq 1} a_i \;=\; \lim_{i\geq 1} b_i + \lim_{i\geq 1} \pi^x c_i \;=\; \lim_{i\geq 1} b_i + \pi^x \lim_{i\geq 1} c_i \;\equiv_{\pi^x}\; \lim_{i\geq 1} b_i\,.$$

□

Definition 70. Let R be a discrete valuation ring. Let $\pi \in R$ be a generator of the maximal ideal of R.

Let $f(X)$, $g(X)$ be polynomials in $R[X]$ and let $(p_i(X))_{i\geq 1}$ be a sequence of polynomials in $R[X]$.

Denote

$$\begin{aligned} f(X) &=: \sum_{\alpha\geq 0} f_\alpha X^\alpha \ , \\ g(X) &=: \sum_{\alpha\geq 0} g_\alpha X^\alpha \ , \\ p_i(X) &=: \sum_{\alpha\geq 0} p_{i,\alpha} X^\alpha \quad \text{for } i \geq 1. \end{aligned}$$

(1) Suppose given $s \geq 0$. Recall that the polynomials $f(X)$ and $g(X)$ are congruent modulo π^s if $f(X) - g(X) \in \pi^s R[X]$, i.e. if $f_\alpha \equiv_{\pi^s} g_\alpha$ for $\alpha \geq 0$.

(2) We say $(p_i(X))_{i\geq 1}$ is *convergent* in $R[X]$ with *limit* $f(X) \in R[X]$ if the sequence of coefficients $(p_{i,\alpha})_{i\geq 1}$ is convergent with limit f_α for $\alpha \geq 0$.

Remark 71. Suppose given a convergent sequence $(a_i)_{i\geq 1}$ in R. Suppose given $f(X) \in R[X]$.

Remark 65.$(1, 2)$ yields

$$\lim_{i\geq 1} f(a_i) \ = \ f(\lim_{i\geq 1} a_i) \ .$$

In that sense, $f(X)$ is *continuous.*

Remark 72. *Suppose R to be complete.*

Let $(n_i)_{i\geq 1}$ be a sequence in $\mathbb{Z}_{\geq 0}$ with $n_i < n_{i+1}$ $\forall i \geq 1$.

Let $d \in \mathbb{Z}_{\geq 0}$.

Let $(p_i(X))_{i\geq 1}$ be a sequence in $R[X]$ such that $\deg p_i \leq d$ and such that

$$p_i(X) \ \equiv_{\pi^{n_i}} \ p_j(X) \ \ \textit{for } i < j.$$

Then the sequence $(p_i(X))_{i\geq 1}$ is convergent.

If all $p_i(X)$ are monic, then so is their limit.

Proof. Let

$$p_i(X) \ =: \sum_{\alpha\geq 0} p_{i,\alpha} X^\alpha \quad \text{for } i \geq 1.$$

Suppose given $\alpha \geq 0$. Since $p_i(X) \equiv_{\pi^{n_i}} p_j(X)$ for $i < j$, we have

$$\mathrm{v}_\pi(p_{i,\alpha} - p_{j,\alpha}) \ \geq \ n_i$$

for $i \leq j$.

Suppose given $M \in \mathbb{N}$. Choose $N \in \mathbb{N}$ such that $n_N \geq M$. For $i, \, j \, \geq \, N$, we get

$$\begin{aligned} \mathrm{v}_\pi(p_{i,\alpha} - p_{j,\alpha}) &= \mathrm{v}_\pi(p_{i,\alpha} - p_{N,\alpha} + p_{N,\alpha} - p_{j,\alpha}) \\ &\geq \min \left\{ \mathrm{v}_\pi(p_{i,\alpha} - p_{N,\alpha}) \, , \, \mathrm{v}_\pi(p_{N,\alpha} - p_{j,\alpha}) \right\} \\ &\geq \min \left\{ n_N \, , \, n_N \right\} \\ &\geq M \ . \end{aligned}$$

So the sequence $(p_{i,\alpha})_{i\geq 1}$ is Cauchy, hence convergent. Write $\hat{p}_\alpha := \lim_{i\geq 1} p_{i,\alpha}$.

Note that $p_{i,\alpha} = 0$ for $\alpha \geq d$ and $i \geq 1$, so that $\hat{p}_\alpha = 0$ for $\alpha \geq d$.

Let

$$\hat{p}(X) \ := \ \sum_{\alpha\geq 0} \hat{p}_\alpha X^\alpha \ .$$

Suppose given $M \in \mathbb{N}$. For $\alpha \in [0,d]$, there exists $N_\alpha \in \mathbb{N}$ such that

$$\mathrm{v}_\pi(p_{i,\alpha} - \hat{p}_\alpha) \ > \ M \quad \text{for } i \geq N_\alpha \ .$$

Let $N := \max\left\{ N_\alpha \ : \ \alpha \in [0,d] \right\}$. Then

$$p_i(X) \ \equiv_{\pi^M} \ \hat{p}(X) \quad \text{for } i \geq N \ .$$

Hence $\hat{p}(X)$ is the limit of the sequence $(p_i(X))_{i\geq 1}$. □

Remark 73. *Suppose R to be complete.*

Let $(n_i)_{i\geq 1}$ be a sequence in $\mathbb{Z}_{\geq 0}$ with $n_i < n_{i+1}$ $\forall i \geq 1$.

Let $f(X)$ be a polynomial in $R[X]$.

Let $(p_i(X))_{i\geq 1}$ be a sequence in $R[X]$ such that

$$f(X) \ \equiv_{\pi^{n_i}} \ p_i(X) \ \ \textit{for } i \geq 1.$$

Then the sequence $(p_i(X))_{i\geq 1}$ is convergent with limit $f(X)$.

Proof. Let

$$\begin{aligned} f(X) \ &=: \ \sum_{\alpha\geq 0} f_\alpha X^\alpha \ , \\ p_i(X) \ &=: \ \sum_{\alpha\geq 0} p_{i,\alpha} X^\alpha \quad \text{for } i \geq 1. \end{aligned}$$

Since $f(X) \equiv_{\pi^{n_i}} p_i(X)$ for $i \geq 1$ we have

$$\mathrm{v}_\pi(f_\alpha - p_{i,\alpha}) \ \geq \ n_i$$

for $i \geq 1$ and $\alpha \geq 0$.

Since $n_i < n_{i+1}$ for $i \geq 1$ we have $\mathrm{v}_\pi(f_\alpha - p_{i,\alpha}) \to \infty$ for $i \to \infty$. So the sequence $(p_{i,\alpha})_{i\geq 1}$ is convergent with limit f_α for $\alpha \geq 0$. So the sequence $(p_i(X))_{i\geq 1}$ is convergent with limit $f(X)$.

□

Remark 74. *Suppose R to be complete.*

Let $(n_i)_{i\geq 1}$ be a sequence in $\mathbb{Z}_{\geq 0}$ with $n_i < n_{i+1}$ $\forall i \geq 1$.

Let $(m_i)_{i\geq 1}$ be a sequence in $\mathbb{Z}_{\geq 0}$ with $m_i < m_{i+1}$ $\forall i \geq 1$.

Let $f(X)$ be a polynomial in $R[X]$.

Let $(p_{1,i}(X))_{i\geq 1}\,,\ \ldots\,,\ (p_{n,i}(X))_{i\geq 1}$ *be sequences in* $R[X]$ *of constant degree with*

$$p_{s,i}(X)\ \equiv_{\pi^{n_i}}\ p_{s,j}(X)\ \ \textit{for}\ i<j\ ,$$

such that

$$f(X)\ \equiv_{\pi^{m_i}}\ \prod_{s\in[1,n]}\ p_{s,i}(X)$$

for $i\geq 1$.

By Remark 72, *these sequences converge, and we may write* $\hat{p}_s(X):=\lim\limits_{i\geq 1} p_{s,i}(X)$.

If all $p_{s,i}(X)$ *are monic, then so are their limits* $\hat{p}_s(X)$.

Then

$$f(X)\ =\ \prod_{s\in[1,n]}\ \hat{p}_s(X)\ .$$

Proof. We have

$$\begin{aligned} f(X) &\overset{\text{R 73}}{=} \lim_{i\geq 1}\prod_{s\in[1,n]} p_{s,i}(X)\\ &\overset{\text{R 65(2)}}{=} \prod_{s\in[1,n]}\lim_{i\geq 1} p_{s,i}(X)\\ &= \prod_{s\in[1,n]}\ \hat{p}_s(X)\ . \end{aligned}$$

□

References

[1] Bosma, W.; Cannon, J.J.; Fieker, C.; Steel, A. (eds.), *Handbook of Magma functions,* Edition 2.16, 2010; cf. magma.maths.usyd.edu.au, magma.maths.usyd.edu.au/calc.

[2] Frei, G., *The Unpublished Section Eight: On the Way to Function Fields over a Finite Field,* in: The Shaping of Arithmetic after C. F. Gauss's Disquisitiones Arithmeticae, Springer, 2007.

[3] Gauss, C.F., *Werke,* Band II, zweiter Abdruck, 1876.

[4] Gelfand, I.M.; Kapranov, M.M.; Zelevinsky, A.V., *Discriminants, Resultants and Multidimensional Determinants,* Birkhäuser, 1994.

[5] Hensel, K., *Neue Grundlagen der Arithmetik,* J. Reine Angew. Math. 127, p. 51–84, 1904.

[6] Jacobson, N., *Basic Algebra I,* 2nd ed., Freeman, 1985.

[7] Koch, H., *Zahlentheorie,* Vieweg, 1997.

[8] Neukirch, J., *Algebraic Number Theory,* transl. N. Schappacher, Springer, 1999.

[9] Ribenboim, P., *Equivalent forms of Hensel's Lemma,* Expo. Math. 3, p. 3–24, 1985.

[10] Rouquette, P., *History of Valuation Theory, Part I,* in: Valuation Theory and its applications, Vol. I, Fields Institute Communication Series, Vol. 32, p. 291–355, 2002.

[11] van der Waerden, B. L., *Algebra,* Springer Grundlehren, 5. Aufl., 1960.