A resultant for Hensel's Lemma

Juliane Deißler

July 30, 2014

Let R be a complete discrete valuation ring with maximal ideal generated by π. Let $f(X) \in R[X]$ be a monic polynomial with nonzero discriminant $\Delta(f)$. Let $s \geq \mathrm{v}_\pi(\Delta(f)) + 1$. Suppose given a factorisation of $f(X)$ in $(R/\pi^s R)[X]$ into several factors, not necessarily coprime in $(R/\pi R)[X]$. We lift it uniquely to a factorisation of $f(X)$ in $R[X]$. This generalises the Hensel-Rychlík Lemma, which covers the case of two factors. We work directly with lifts of factorisations into several factors and avoid having to iterate factorisations into two factors. For this purpose we define a resultant for several polynomials in one variable as determinant of a generalised Sylvester matrix.

Contents

0 Introduction

In this introduction, by a polynomial we understand a monic polynomial.

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

MSC2010: 13B25.

0.1 Resultant of several polynomials

Classically, one defines the resultant of two polynomials in $R[X]$ as the determinant of their Sylvester matrix; cf. van der Waerden [**9,** §34].

Here, for polynomials $g_{(1)}(X), \ldots, g_{(n)}(X) \in R[X]$, where $n \geq 1$, the resultant $\mathrm{Res}(g_{(1)}, \ldots, g_{(n)})$ is defined to be the determinant of the generalised Sylvester matrix $\mathrm{Sylv}(g_{(1)}, \ldots, g_{(n)})$. This matrix contains the coefficients of the products $\prod_{j \in [1,n] \smallsetminus \{k\}} g_{(j)}(X)$, where $1 \leq k \leq n$, ordered in a similar way as in the classical Sylvester matrix; cf. Definition 3.

We obtain the product formula $\mathrm{Res}(g_{(1)}\,,\,\ldots\,,\,g_{(n)}) = \prod_{1 \leq k < \ell \leq n} \mathrm{Res}(g_{(k)}\,,\,g_{(\ell)})$, expressing our resultant as a product of classical resultants. Since in our application to Hensel lifting, the generalised Sylvester matrix $\mathrm{Sylv}(g_{(1)}, \ldots, g_{(n)})$ itself will appear, it would not have been possible to work only with this product formula.

Suppose given a polynomial $f(X) \in R[X]$ with discriminant $\Delta(f) \neq 0$. Let $s \geq \mathrm{v}_\pi(\Delta(f)) + 1$. As shall be explained in §0.2.1 below, we will start a Hensel lifting process with a factorisation $f(X) \equiv_{\pi^s} \prod_{k \in [1,n]} g_{(k)}(X)$, that is, with a factorisation of precision s, into factors $g_{(k)}(X)$, which are not necessarily coprime modulo π. In this context, the product formula for the resultant yields the inequality $2\,\mathrm{v}_\pi(\mathrm{Res}(g_{(1)}\,,\,\ldots\,,\,g_{(n)})) \leq \mathrm{v}_\pi(\Delta(f))$; cf. Proposition 9. Technically speaking, this inequality is the reason why we may start the process with said precision. In summary, the resultant machinery will supply our Hensel lifting process with a starting precision that depends only on the polynomial $f(X)$ to be factorised.

0.2 Applications to Hensel's Lemma

0.2.1 General case

Hensel's Lemma in the classical sense [**8,** 4.4.2] has, in rudimentary form, already been known to Gauss [**6,** §374]; cf. [**5,** §3.6]. Hensel developed a more sophisticated version [**7,** §4, p. 80], known today as Hensel-Rychlík Lemma. We generalise in Theorem 16 the Hensel-Rychlík Lemma from the case of two factors to the case of an arbitrary number of factors.

Let $f(X) \in R[X]$ such that $\Delta(f) \neq 0$. Let $s \geq \mathrm{v}_\pi(\Delta(f)) + 1$. Choose a factorisation

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

where $n \geq 1$, i.e. a factorisation modulo π^s into factors $g_{(k)}(X) \in R[X]$ of degree ≥ 1, which are not necessarily coprime modulo π. Write $t := \mathrm{v}_\pi(\mathrm{Res}(g_{(1)}\,,\,\ldots\,,\,g_{(n)}))$. Then there exist unique polynomials $\check{g}_{(1)}(X), \ldots, \check{g}_{(n)}(X)$ in $R[X]$ congruent, respectively, to $g_{(1)}(X), \ldots, g_{(n)}(X)$ modulo π^{s-t} such that

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

So to find a factorisation of a polynomial $f(X)$ in $R[X]$, we start with a factorisation of precision s, satisfying a lower bound depending only on $f(X)$, and lift it to a factorisation of $f(X)$ in $R[X]$. Here, to lift means to replace the old factors $g_{(k)}(X)$, factoring modulo π^s, by new factors $\check{g}_{(k)}(X)$, factoring exactly, such that the new factors are congruent to the old factors modulo π^{s-t}. Concerning the connection from new to old, s is the precision "one might hope for" – but from that we have to subtract t, which thus plays the role of a "potential defect"; this t, in turn, is bounded above depending only on $f(X)$, viz. $t \leq \mathrm{v}_\pi(\Delta(f))/2$. Such a defect actually occurs in examples, cf. § 3.

The inductive step of the proof of Theorem 16 is contained in Lemma 14. The arguments for that step I have learnt from KOCH [**8,** 4.4.3, 4.4.4, 4.4.5].

In Example 18 we suppose given a factorisation $f(X) \equiv_{\pi^s} g_{(1)}(X) \cdot g_{(2)}(X) \cdot g_{(3)}(X)$ into three factors, in order to compare the result of a single application of Lemma 14 to three factors with the result of two subsequent applications of Lemma 14 to two factors. We determine that both methods are essentially equally good.

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

In § 2.3 we investigate our generalisation of the Hensel-Rychlík Lemma in a particular case. Here, slightly better bounds than in the general case hold. Namely, the bound for the starting precision and the bound for the defect can be lowered somewhat, compared to the general case.

Let $f(X)$ be a polynomial in $R[X]$ with $\deg f =: M$ and $f(X) \equiv_\pi X^M$. Let $n \geq 1$ and $g_{(1)}(X), \ldots, g_{(n)}(X) \in R[X]$ of degree ≥ 1, ordered such that $\deg g_{(1)} \leq \cdots \leq \deg g_{(n)}$. Again, we write $t := \mathrm{v}_\pi(\mathrm{Res}(g_{(1)}, \ldots, g_{(n)}))$. Moreover, we write $t' := t - \sum_{j\in[1,n-1]} \big((n-j)(\deg g_{(j)}) - 1\big)$. Now, suppose that $f(X) \equiv_{\pi^s} \prod_{k\in[1,n]} g_{(k)}(X)$ for some $s \geq t + t' + 1$. Then there exist unique polynomials $\check{g}_{(1)}(X), \ldots, \check{g}_{(n)}(X) \in R[X]$ congruent, respectively, to $g_{(1)}(X), \ldots, g_{(n)}(X)$ modulo $\pi^{s-t'}$ such that $f(X) = \prod_{k\in[1,n]} \check{g}_{(k)}(X)$. Cf. Theorem 22.

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

Examples 25 and 26 show that $t' < t$ may occur.

The inductive step for the proof of Theorem 22 is contained in Lemma 21. In Example 23, we suppose given a factorisation $f(X) \equiv_{\pi^s} g_{(1)}(X) \cdot g_{(2)}(X) \cdot g_{(3)}(X)$ into three factors, ordered such that $\deg g_{(1)} \leq \deg g_{(2)} \leq \deg g_{(3)}$, in order to compare the result of a single application of Lemma 21 to three factors with the result of two subsequent applications of Lemma 21 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.

0.3 Acknowledgements

To illustrate the theory we consider in § 3 some polynomials with cofficients in $\mathbb{Z}_p$ for a prime number p using the computer algebra system MAGMA [**1**].

I thank the referee of an earlier version for arguments that considerably simplified § 1 and for pointing out the reference [**4**]; cf. Remark 15.

0.4 Notations

- Given a, $b \in \mathbb{Z}$, we denote by $[a,b] := \{z \in \mathbb{Z} : a \le z \le b\} \subseteq \mathbb{Z}$ the integral interval.
- Given an integral domain R, a prime element $\pi \in R$ with $\pi \neq 0$ and $x \in R \smallsetminus \{0\}$, we denote $\mathrm{v}_\pi(x) := \max\{\, i \in \mathbb{Z}_{\ge 0} : \pi^i \text{ divides } x \,\}$. Moreover, $\mathrm{v}_\pi(0) := +\infty$.
- We denote by E_m the unit matrix of size $m \times m$.
- Given a commutative ring R and elements x, y, $u \in R$, we write $x \equiv_u y$ for $x - y \in uR$.
- For the zero polynomial 0, we put $\deg 0 := -\infty$.

1 Resultants

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

1.1 A lemma

Definition 1. *Suppose given $z \ge 0$. Suppose given $s \ge 0$. Suppose given $u(X) = \sum_{i \in [0,s]} u_i X^i$. Let*

$$B_{z,\,z+s}(u) \quad := \quad \begin{pmatrix} u_0 & u_1 & \cdots & \cdots & \cdots & u_s & & & & \\ & u_0 & u_1 & \cdots & \cdots & \cdots & u_s & & & \\ & & u_0 & u_1 & \cdots & \cdots & \cdots & u_s & & \\ & & & \ddots & \ddots & & & & \ddots & \\ & & & & u_0 & u_1 & \cdots & \cdots & \cdots & u_s \end{pmatrix} \quad \in \quad R^{z \times (z+s)}\ .$$

Lemma 2. *Suppose given $z \ge 0$. Suppose given s, $t \ge 0$. Suppose given $u(X) = \sum_{i \in [0,s]} u_i X^i$. Suppose given $v(X) = \sum_{i \in [0,t]} v_i X^i$. Then*

$$B_{z,\,z+s}(u) \cdot B_{z+s,\,z+s+t}(v) \;=\; B_{z,\,z+s+t}(uv)\ .$$

Proof. Write $u(X) = \sum_{i \ge 0} u_i X^i$ with $u_i = 0$ for $i \ge s+1$ and $v(X) = \sum_{i \ge 0} v_i X^i$ with $v_i = 0$ for $i \ge t+1$. Then $u(X) \cdot v(X) = \sum_{j \ge 0} \left(\sum_{i \in [0,j]} u_i v_{j-i} \right) X^j$.

Suppose given $p \in [1,z]$ and $q \in [1, z+s+t]$. If $p > q$, then the entry at position (p,q) is zero in the left hand side and in the right hand side matrix. If $p \le q$, then the entry at position (p,q) of $B_{z,\,z+s}(u) B_{z+s,\,z+s+t}(v)$ equals $\sum_{i \in [0,q-p]} u_i v_{q-p-i}$, which equals the entry at position (p,q) of $B_{z,\,z+s+t}(uv)$. □

1.2 A resultant

Let $n \in \mathbb{Z}_{\ge 1}$. Suppose given monic polynomials $g_{(k)} = g_{(k)}(X) = \sum\limits_{i \in [0, m_{(k)}]} g_{(k)i} X^i \in R[X]$, where $m_{(k)} := \deg g_{(k)} \ge 1$, for $k \in [1,n]$. Denote $M := \sum\limits_{j \in [1,n]} m_{(j)}$. Denote $M_{(k)} := M - m_{(k)}$ and

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

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

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

Definition 3. Let

$$\operatorname{Sylv}(g_{(1)},\ldots,g_{(n)}) \;:=\; \left(\begin{array}{cccccccc} a_{(1)0} & \cdots & \cdots & \cdots & a_{(1)M_{(1)}} & & \\ & \ddots & & & & \ddots & \\ & & a_{(1)0} & \cdots & \cdots & \cdots & a_{(1)M_{(1)}} \\ a_{(2)0} & \cdots & \cdots & \cdots & a_{(2)M_{(2)}} & & \\ & \ddots & & & & \ddots & \\ & & a_{(2)0} & \cdots & \cdots & \cdots & a_{(2)M_{(2)}} \\ \vdots & & \vdots & & \vdots & & \vdots \\ \vdots & & \vdots & & \vdots & & \vdots \\ a_{(n)0} & \cdots & \cdots & \cdots & a_{(n)M_{(n)}} & & \\ & \ddots & & & & \ddots & \\ & & a_{(n)0} & \cdots & \cdots & \cdots & a_{(n)M_{(n)}} \end{array}\right) \begin{array}{l} \left.\vphantom{\begin{array}{c}a\\a\\a\end{array}}\right\} m_{(1)} \text{ rows} \\ \left.\vphantom{\begin{array}{c}a\\a\\a\end{array}}\right\} m_{(2)} \text{ rows} \\ \vphantom{\begin{array}{c}a\\a\end{array}} \\ \left.\vphantom{\begin{array}{c}a\\a\\a\end{array}}\right\} m_{(n)} \text{ rows} \end{array} \;\in\; R^{M\times M}\,.$$

Let

$$\operatorname{Res}(g_{(1)},\ldots,g_{(n)}) \;:=\; \det \operatorname{Sylv}(g_{(1)},\ldots,g_{(n)}) \;\in\; R$$

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

Note that

$$\operatorname{Sylv}(g_{(1)},\ldots,g_{(n)}) \;=\; \left(\begin{array}{c} B_{m_{(1)},\,M}\left(\prod\limits_{j\in[1,n]\smallsetminus\{1\}} g_{(j)}(X)\right) \\ \hline B_{m_{(2)},\,M}\left(\prod\limits_{j\in[1,n]\smallsetminus\{2\}} g_{(j)}(X)\right) \\ \hline \vdots \\ \vdots \\ \hline B_{m_{(n)},\,M}\left(\prod\limits_{j\in[1,n]\smallsetminus\{n\}} g_{(j)}(X)\right) \end{array}\right)\,.$$

In the case $n = 1$, we have $\operatorname{Res}(g_{(1)}(X)) = 1$, for $\operatorname{Sylv}(g_{(1)}) = \mathrm{E}_{m_{(1)}}$.

In the case $n = 2$, our resultant coincides with the resultant found in the literature, e.g. in [**2,** §7.4, (4)], because it is obtained by a row and column reordering that leaves the determinant unchanged, for we need $m_{(1)}m_{(2)} + \lfloor\frac{m_{(1)}+m_{(2)}}{2}\rfloor + \lfloor\frac{m_{(1)}}{2}\rfloor + \lfloor\frac{m_{(2)}}{2}\rfloor \equiv_2 0$ transpositions.

Lemma 4 (cf. [**2,** §7.4, Th. 2.(iv), Cor.])**.** *Suppose given $u(X)$, $v(X)$, $w(X) \in R[X]$ monic.*

(1) *Choose a field C containing R as a subring such that $v(X) = \prod_{i\in[1,s]}(X-\alpha_i)$ and $w(X) = \prod_{j\in[1,t]}(X-\beta_j)$ in $C[X]$, where $s := \deg u$ and $t := \deg v$.*

Then $\operatorname{Res}(v,w) \;=\; \prod\limits_{(i,j)\,\in\,[1,s]\times[1,t]} (\alpha_i-\beta_j)\,.$

(2) *We have* $\operatorname{Res}(uv, w) = \operatorname{Res}(u, w) \cdot \operatorname{Res}(v, w)$.

Lemma 5. *We have* $\operatorname{Res}(g_{(1)}\,,\,\dots\,,\,g_{(n)}) \;=\; \prod_{1\le k<\ell\le n} \operatorname{Res}(g_{(k)}\,,\,g_{(\ell)})$.

Proof. We proceed by induction on $n \geq 1$; basing it at $n = 1$, where both sides equal 1. Suppose given $n \geq 2$. Suppose the assertion known for $n - 1$. Then

$$
\operatorname{Sylv}(g_{(1)},\dots,g_{(n)}) \;=\; \left(\begin{array}{c}
B_{m_{(1)},\,M}\Big(\prod_{j\in[1,n]\smallsetminus\{1\}} g_{(j)}(X)\Big) \\ \hline
B_{m_{(2)},\,M}\Big(\prod_{j\in[1,n]\smallsetminus\{2\}} g_{(j)}(X)\Big) \\ \hline
\vdots \\ \hline
B_{m_{(n)},\,M}\Big(\prod_{j\in[1,n]\smallsetminus\{n\}} g_{(j)}(X)\Big)
\end{array}\right)
$$

$$
\overset{\text{L. 2}}{=} \left(\begin{array}{c|c}
B_{m_{(1)},\,M_{(n)}}\Big(\prod_{j\in[1,n-1]\smallsetminus\{1\}} g_{(j)}(X)\Big) & \\ \hline
B_{m_{(2)},\,M_{(n)}}\Big(\prod_{j\in[1,n-1]\smallsetminus\{2\}} g_{(j)}(X)\Big) & \\ \hline
\vdots & \\ \hline
B_{m_{(n-1)},\,M_{(n)}}\Big(\prod_{j\in[1,n-1]\smallsetminus\{n-1\}} g_{(j)}(X)\Big) & \\ \hline
 & \mathrm{E}_{m_{(n)}}
\end{array}\right) \cdot \left(\begin{array}{c}
B_{M_{(n)},\,M}(g_{(n)}(X)) \\ \hline
B_{m_{(n)},\,M}\Big(\prod_{j\in[1,n-1]} g_{(j)}(X)\Big)
\end{array}\right) .
$$

Taking determinants, this yields

$$
\begin{array}{rcl}
\operatorname{Res}(g_{(1)}\,,\,\dots\,,\,g_{(n)}) & = & \operatorname{Res}(g_{(1)}\,,\,\dots\,,\,g_{(n-1)}) \cdot \operatorname{Res}(\prod_{j\in[1,n-1]} g_{(j)}\,,\,g_{(n)}) \\
& \overset{\text{L. 4.(2)}}{=} & \operatorname{Res}(g_{(1)}\,,\,\dots\,,\,g_{(n-1)}) \cdot \prod_{j\in[1,n-1]} \operatorname{Res}(g_{(j)}\,,\,g_{(n)}) \\
& \overset{\text{induction}}{=} & \Big(\prod_{1\le k<\ell\le n-1} \operatorname{Res}(g_{(k)}\,,\,g_{(\ell)})\Big) \cdot \Big(\prod_{j\in[1,n-1]} \operatorname{Res}(g_{(j)}\,,\,g_{(n)})\Big) \\
& = & \prod_{1\le k<\ell\le n} \operatorname{Res}(g_{(k)}\,,\,g_{(\ell)}) .
\end{array}
$$

□

Lemma 5 together with Lemma 4.(1) gives the

Corollary 6. *Write* $g_{(k)}(X) =: \prod_{i\in[1,m_{(k)}]} (X - \gamma_{(k)i})$ *in* $L[X]$ *for* $k \in [1, n]$.

We have

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

1.3 Resultants and discriminants

Denote by $\Delta(f)$ the discriminant of a polynomial $f(X) \in R[X]$.

Corollary 7. *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. Note that $\Delta(g_{(k)}) = \prod_{1\le i<j\le m_{(k)}} (\gamma_{(k)i} - \gamma_{(k)j})^2$ for $k \in [1,n]$; cf. [**9,** §33]. So

$$\begin{aligned}
&\Delta(g_{(1)} \cdot \ldots \cdot g_{(n)}) \\
&\quad = \Big(\prod_{k\in[1,n]} \prod_{1\le i<j\le m_{(k)}} (\gamma_{(k)i} - \gamma_{(k)j})^2\Big) \cdot \Big(\prod_{1\le k<\ell\le n} \prod_{(i,j)\in[1,m_{(k)}]\times[1,m_{(\ell)}]} (\gamma_{(k)i} - \gamma_{(\ell)j})^2\Big) \\
&\quad \overset{\text{C 6}}{=} \Big(\prod_{k\in[1,n]} \Delta(g_{(k)})\Big) \cdot \mathrm{Res}(g_{(1)}, \ldots, g_{(n)})^2 .
\end{aligned}$$

□

Remark 8. *Let $r \in R$. Suppose given monic polynomials $f(X)$, $\tilde{f}(X) \in R[X]$ such that $f(X) \equiv_r \tilde{f}(X)$. Then $\Delta(f) \equiv_r \Delta(\tilde{f})$.*

Proposition 9. *Let $f(X) \in R[X]$ be a monic polynomial with $\Delta(f) \neq 0$. Suppose that we have $f(X) \equiv_{\pi\Delta(f)} \prod_{k\in[1,n]} g_{(k)}(X)$. Then $\mathrm{Res}(g_{(1)}, \ldots, g_{(n)}) \neq 0$ and*

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

Proof. We have $\Delta(f) \overset{\text{R 8}}{\equiv}_{\pi\Delta(f)} \Delta(\prod_{k\in[1,n]} g_{(k)}) \overset{\text{C 7}}{=} \big(\prod_{k\in[1,n]} \Delta(g_{(k)})\big) \cdot \mathrm{Res}(g_{(1)}, \ldots, g_{(n)})^2$. □

Remark 10. *Let $r \in R$. Let $\tilde{g}_{(1)}(X), \ldots, \tilde{g}_{(n)}(X) \in R[X]$ 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. We may assume that r is not a unit in R. Then $\deg g_{(k)} = \deg \tilde{g}_{(k)}$ for $k \in [1,n]$. Hence $\mathrm{Sylv}(g_{(1)}, \ldots, g_{(n)}) \equiv_r \mathrm{Sylv}(\tilde{g}_{(1)}, \ldots, \tilde{g}_{(n)})$; cf. Definition 3. Taking determinants, we get $\mathrm{Res}(g_{(1)}, \ldots, g_{(n)}) \equiv_r \mathrm{Res}(\tilde{g}_{(1)}, \ldots, \tilde{g}_{(n)})$. □

2 Hensel

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

2.1 Linear Algebra tools

Suppose given $k \ge 1$. 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 $0 \le e_1 \le e_2 \le \cdots \le e_k$. Write $e := e_1 + \cdots + e_k = \mathrm{v}_\pi(\det(A))$. Choose $S, T \in \mathrm{GL}_k(R)$ such that $SAT = \mathrm{diag}(\pi^{e_1}, \ldots, \pi^{e_k}) =: D$. Suppose given $d_i \in \mathbb{Z}_{\ge 0}$ for $i \in [1,k]$ such that $d_1 \ge d_2 \ge \cdots \ge d_k$. Write $e' := e - (d_2 + \cdots + d_k)$.

Remark 11. *Suppose that for every $i \in [1,k]$, the element π^{d_i} divides each entry in column number i of A. Then $0 \le e_k \le e'$.*

Proof. Each $(k-1)\times(k-1)$-minor of A is divisible by $\pi^{d_k+\cdots+d_2}$. So $\pi^{d_k+\cdots+d_2}$ divides their greatest common divisor π^{e-e_k}. □

Lemma 12.

(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 that for every $i \in [1, k]$, the element π^{d_i} divides each entry in column number i of A. 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). Write $yT =: (\pi^{e_k} z_1, \ldots, \pi^{e_k} z_k)$, where $z_i \in R$ for $i \in [1, k]$. Let $x := (\pi^{e_k-e_1} z_1, \ldots, \pi^{e_k-e_k} z_k)S \in R^{1\times k}$. So $xA = xS^{-1}DT^{-1} = (\pi^{e_k-e_1} z_1, \ldots, \pi^{e_k-e_k} z_k)DT^{-1} = yTT^{-1} = y$.
Ad (3). By Remark 11 we have $e' \geq e_k$, so that the assertion follows with (1). □

Lemma 13.

(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 that for every $i \in [1, k]$, the element π^{d_i} divides each entry in column number i of A. 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). We have $xA = xS^{-1}DT^{-1} \in R^{1\times k}\pi^u$, whence $xS^{-1}D \in R^{1\times k}\pi^u$. Denote $xS^{-1} =: (z_1, \ldots, z_k) \in R^{1\times k}$. So $xS^{-1}D = (\pi^{e_1} z_1, \ldots, \pi^{e_k} z_k)$. Hence $z_i \in R\pi^{u-e_i} \subseteq R\pi^{u-e_k}$ for $i \in [1, k]$. So $xS^{-1} = (z_1, \ldots, z_k) \in R^{1\times k}\pi^{u-e_k}$. Hence $x \in R^{1\times k}\pi^{u-e_k}S = R^{1\times k}\pi^{u-e_k}$.
Ad (3). By Remark 11 we have $e' \geq e_k$, so that the assertion follows with (1). □

2.2 General case

Let $f(X) \in R[X]$ be a monic polynomial such that $\Delta(f) \neq 0$. 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. Denote $t := \mathrm{v}_\pi(\mathrm{Res}(g_{(1)}, \ldots, g_{(n)}))$. Write $m_{(k)} := \deg g_{(k)}$ and $M_{(k)} := M - m_{(k)}$ for $k \in [1, n]$.
Let $s \geq \mathrm{v}_\pi(\Delta(f)) + 1$. Suppose that $f(X) \equiv_{\pi^s} \prod_{k\in[1,n]} g_{(k)}(X)$.
Note that t is finite and that $s \geq 2t + 1$; cf. Proposition 9.
(Actually, we could also suppose only the condition $s \geq 2t+1$. However, $2t+1$ depends on the factors $g_{(1)}(X), \ldots, g_{(n)}(X)$, whereas $\mathrm{v}_\pi(\Delta(f)) + 1$ depends only on $f(X)$.)

Lemma 14 (cf. [**7,** p. 81])**.**

(1) *There exist monic polynomials $\tilde{g}_{(1)}(X), \ldots, \tilde{g}_{(n)}(X) \in R[X]$ such that $\tilde{g}_{(k)}(X) \equiv_{\pi^{s-t}} g_{(k)}(X)$ 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* $\tilde{g}_{(1)}(X)\,, \dots, \tilde{g}_{(n)}(X)$, $\tilde{h}_{(1)}(X)\,, \dots, \tilde{h}_{(n)}(X) \in R[X]$ *such that* $\tilde{g}_{(k)}(X) \equiv_{\pi^{s-t}} g_{(k)}(X)$ *and* $\tilde{h}_{(k)}(X) \equiv_{\pi^{s-t}} g_{(k)}(X)$ *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 § 1. The arguments I have learnt from Koch [**8,** Satz 4.4.3, Hilfssatz 4.4.4, Hilfssatz 4.4.5].

Proof. Ad (1). *Existence of admissible lift.*
We make the ansatz $\tilde{g}_{(k)}(X) = g_{(k)}(X) + \pi^{s-t}u_{(k)}(X)$ 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 $b(X) \overset{!}{\equiv}_{\pi^{s-t}} \sum_{k\in[1,n]} u_{(k)}(X) \cdot \prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X)$. So it suffices to find $u_{(k)}(X) \in R[X]$ for $k \in [1,n]$ as above such that $b(X) \overset{!}{=} \sum_{k\in[1,n]} u_{(k)}(X) \cdot \prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X)$.
Writing $b(X) =: \sum_{i\geq 0} \beta_i X^i$, $\prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X) =: \sum_{i\geq 0} a_{(k)i}X^i$, $u_{(k)}(X) =: \sum_{i\geq 0} u_{(k)i}X^i$ 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

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

such that

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

Note that $(\beta_0 \ \dots \ \beta_{M-1}) \in \pi^t R^{1\times M}$ since $b(X) \equiv_{\pi^t} 0$. So U exists as required by Lemma 12.(2).

Valuation of resultant. Since $\tilde{g}_{(k)}(X) \equiv_{\pi^{s-t}} g_{(k)}(X)$ for $k \in [1,n]$, Remark 10 implies that $\mathrm{Res}(\tilde{g}_{(1)}, \dots, \tilde{g}_{(n)}) \equiv_{\pi^{s-t}} \mathrm{Res}(g_{(1)}, \dots, g_{(n)})$. Since $s-t \geq t+1 = \mathrm{v}_\pi(\mathrm{Res}(g_{(1)}, \dots, g_{(n)}))+1$, this implies $\mathrm{v}_\pi(\mathrm{Res}(\tilde{g}_{(1)}, \dots, \tilde{g}_{(n)})) = \mathrm{v}_\pi(\mathrm{Res}(g_{(1)}, \dots, g_{(n)})) = t$.

Ad (2). Writing $\tilde{g}_{(k)}(X) =: g_{(k)}(X) + \pi^{s-t}u_{(k)}(X)$ and $\tilde{h}_{(k)}(X) =: g_{(k)}(X) + \pi^{s-t}v_{(k)}(X)$ 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 $u_{(k)}(X) \overset{!}{\equiv}_{\pi^{s-2t-r}} v_{(k)}(X)$ for $k \in [1,n]$. We have

$$\begin{aligned} \prod_{k\in[1,n]} g_{(k)}(X) + \pi^{s-t} \sum_{k\in[1,n]} u_{(k)}(X) \cdot \prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X) &\equiv_{\pi^{2(s-t)}} \prod_{k\in[1,n]} (g_{(k)}(X) + \pi^{s-t}u_{(k)}(X)) \\ = \prod_{k\in[1,n]} \tilde{g}_{(k)}(X) &\equiv_{\pi^{2(s-t)-r}} \prod_{k\in[1,n]} \tilde{h}_{(k)}(X) \\ = \prod_{k\in[1,n]} (g_{(k)}(X) + \pi^{s-t}v_{(k)}(X)) &\equiv_{\pi^{2(s-t)}} \prod_{k\in[1,n]} g_{(k)}(X) + \pi^{s-t} \sum_{k\in[1,n]} v_{(k)}(X) \cdot \prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X) \, . \end{aligned}$$

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

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

we have to show that $W \overset{!}{\in} \pi^{s-2t-r}R^{1\times M}$. From $(*)$, we obtain $W \cdot \mathrm{Sylv}(g_{(1)}, \dots, g_{(n)}) \in \pi^{s-t-r}R^{1\times M}$. Note that $s-t-r \geq t = \mathrm{v}_\pi(\det \mathrm{Sylv}(g_{(1)}, \dots, g_{(n)}))$. So we can infer by Lemma 13.(2) that $W \in \pi^{s-2t-r}R^{1\times M}$. □

Remark 15. In [**4**, App. B], the same method is used as in Lemma 14.(1). Since in [**4**, App. B], the discriminant of $f(X)$ is not invoked, the necessary starting precision depends on the factorisation chosen there; namely, it is assumed, using our notation and context, that for some $\tau \geq 0$, the congruence $U \cdot \mathrm{Sylv}(g_{(1)}, \dots, g_{(n)}) \equiv_{\pi^{\tau+1}} (\pi^\tau, 0, \dots, 0)$ is solvable for some $U \in R^{1\times M}$ in order to be able to use a factorisation $f(X) \equiv_{\pi^{2\tau+1}} \prod_{k\in[1,n]} g_{(k)}(X)$. This condition is satisfied if $\mathrm{Res}(g_{(1)}, \dots, g_{(n)})$ divides π^τ, and so, using Proposition 9, it is satisfied if $\Delta(f)$ divides $\pi^{2\tau}$.

Theorem 16. *Suppose R to be a complete discrete valuation ring. Recall that $f(X) \in R[X]$ is a monic polynomial with $\Delta(f) \neq 0$, that $s \geq \mathrm{v}_\pi(\Delta(f))+1$, that $f(X) \equiv_{\pi^s} \prod_{k\in[1,n]} g_{(k)}(X)$ and that $t = \mathrm{v}_\pi(\mathrm{Res}(g_{(1)}, \dots, g_{(n)}))$.*

Then there exist unique monic polynomials $\check{g}_{(1)}(X), \dots, \check{g}_{(n)}(X) \in R[X]$ such that $\check{g}_{(k)}(X) \equiv_{\pi^{s-t}} g_{(k)}(X)$ for $k \in [1,n]$ and $f(X) = \prod_{k\in[1,n]} \check{g}_{(k)}(X)$.

Proof. Existence. Since R is complete, it suffices to show that there exist monic polynomials $\tilde{g}_{(1)}(X)\,,\,\dots\,,\,\tilde{g}_{(n)}(X) \in R[X]$ such that $f(X) \equiv_{\pi^{s+1}} \prod_{k\in[1,n]} \tilde{g}_{(k)}(X)$ and $\tilde{g}_{(k)}(X) \equiv_{\pi^{s-t}} g_{(k)}(X)$ for $k \in [1,n]$, and $\mathrm{v}_\pi(\mathrm{Res}(\tilde{g}_{(1)}\,,\,\dots\,,\,\tilde{g}_{(n)})) = t$. This follows by Lemma 14.(1) as $2(s-t) \geq s+1$.

Uniqueness. Given $\check{g}_{(1)}(X),\dots,\check{g}_{(n)}(X),\check{h}_{(1)}(X),\dots,\check{h}_{(n)}(X) \in R[X]$, all monic, such that $\check{g}_{(k)}(X) \equiv_{\pi^{s-t}} g_{(k)}(X) \equiv_{\pi^{s-t}} \check{h}_{(k)}(X)$ for $k \in [1,n]$ and $\prod_{k\in[1,n]} \check{g}_{(k)}(X) = f(X) = \prod_{k\in[1,n]} \check{h}_{(k)}(X)$, we have to show that $\check{g}_{(k)}(X) \overset{!}{=} \check{h}_{(k)}(X)$ for $k \in [1,n]$.

Note that $\mathrm{v}_\pi(\mathrm{Res}(\check{g}_{(1)}\,,\,\dots\,,\,\check{g}_{(n)})) = t = \mathrm{v}_\pi(\mathrm{Res}(\check{h}_{(1)}\,,\,\dots\,,\,\check{h}_{(n)}))$ by Lemma 14.(1).

Let $s_1 := s$. Both $(\check{h}_{(k)}(X))_k$ and $(\check{g}_{(k)}(X))_k$ are admissible lifts of $(\check{g}_{(k)}(X))_k$ with respect to s_1 in the sense of Lemma 14.(1), since $\check{h}_{(k)}(X) \equiv_{\pi^{s_1-t}} \check{g}_{(k)}(X)$ for $k \in [1,n]$ and the other required congruences are verified using equalities. So Lemma 14.(2) yields $\check{h}_{(k)}(X) \equiv_{\pi^{2(s_1-t)-t}} \check{g}_{(k)}(X)$ for $k \in [1,n]$.

Let $s_2 := 2(s_1-t)$. Note that $s_2 = s_1 + (s_1 - 2t) > s_1$. Both $(\check{h}_{(k)}(X))_k$ and $(\check{g}_{(k)}(X))_k$ are admissible lifts of $(\check{g}_{(k)}(X))_k$ with respect to s_2, since $\check{h}_{(k)}(X) \equiv_{\pi^{s_2-t}} \check{g}_{(k)}(X)$ for $k \in [1,n]$. So Lemma 14.(2) yields $\check{h}_{(k)}(X) \equiv_{\pi^{2(s_2-t)-t}} \check{g}_{(k)}(X)$ 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 $\check{h}_{(k)}(X) \equiv_{\pi^{s_\ell-t}} \check{g}_{(k)}(X)$ for $k \in [1,n]$ and $\ell \geq 1$. Hence $\check{h}_{(k)}(X) = \check{g}_{(k)}(X)$ for $k \in [1,n]$. □

Remark 17. The case $n = 2$ of Theorem 16, 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. [**7,** p. 80, 81].

Translated to our notation, he starts with $s > \mathrm{v}_\pi(\Delta(f))$. He writes in the statement on [**7,** p. 80, l. 8] that $\check{g}_{(1)}(X)$ and $\check{g}_{(2)}(X)$ are "Näherungswerte" of $g_{(1)}(X)$ and $g_{(2)}(X)$. In the proof, on [**7,** p. 81, l. 7], he makes this precise and shows that actually $\check{g}_{(1)}(X) \equiv_{\pi^{s-t}} g_{(1)}(X)$ and $\check{g}_{(2)}(X) \equiv_{\pi^{s-t}} g_{(2)}(X)$.

Example 18. Suppose that $n = 3$. Write $t_0 := \mathrm{v}_\pi(\mathrm{Res}(g_{(2)}\,,\,g_{(3)}))$, $t_1 := \mathrm{v}_\pi(\mathrm{Res}(g_{(1)}\,,\,g_{(2)}g_{(3)}))$. Corollary 6 gives $\mathrm{Res}(g_{(1)}\,,\,g_{(2)}\,,\,g_{(3)}) = \mathrm{Res}(g_{(1)}\,,\,g_{(2)}g_{(3)}) \cdot \mathrm{Res}(g_{(2)}\,,\,g_{(3)})$, whence $t = t_1 + t_0$. In particular, t_0 and t_1 are finite.

We can apply Lemma 14.(1) to $f(X) \equiv_{\pi^s} g_{(1)}(X) \cdot g_{(2)}(X) \cdot g_{(3)}(X)$ to obtain monic polynomials $\tilde{g}_{(1)}(X)\,,\,\tilde{g}_{(2)}(X)\,,\,\tilde{g}_{(3)}(X) \in R[X]$ such that

$$\text{(i)} \qquad \tilde{g}_{(k)}(X) \equiv_{\pi^{s-t}} g_{(k)}(X) \text{ for } k \in [1,3]\,, \quad f(X) \equiv_{\pi^{2(s-t)}} \tilde{g}_{(1)}(X) \cdot \tilde{g}_{(2)}(X) \cdot \tilde{g}_{(3)}(X)\,.$$

We can also apply Lemma 14.(1) first to the factorisation $f(X) \equiv_{\pi^s} g_{(1)}(X) \cdot (g_{(2)}(X) \cdot g_{(3)}(X))$ and then to the resulting factorisation of the second factor into $g_{(2)}(X) \cdot g_{(3)}(X)$ modulo a certain power of π.

We have $s \geq 2t+1 \geq 2t_1+1$. So Lemma 14.(1) gives monic polynomials $\tilde{h}_{(1)}(X)\,,\,\tilde{h}_{(2)}(X) \in R[X]$ such that

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

We have $s - t_1 \geq 2t + 1 - t_1 = t_1 + 2t_0 + 1 \geq 2t_0 + 1$. So Lemma 14.(1) gives monic polynomials

$\tilde{\tilde{g}}_{(2)}(X)\,,\ \tilde{\tilde{g}}_{(3)}(X)\ \in\ R[X]$ such that

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

Altogether, the two subsequent applications of Lemma 14.(1) for two factors yield

$$\text{(ii)}\qquad \begin{array}{l}\tilde{h}_{(1)}(X)\ \equiv_{\pi^{s-t_1}}\ g_{(1)}(X)\ ,\ \ \tilde{\tilde{g}}_{(2)}(X)\ \equiv_{\pi^{s-t_1-t_0}}\ g_{(2)}(X)\ ,\ \ \tilde{\tilde{g}}_{(3)}(X)\ \equiv_{\pi^{s-t_1-t_0}}\ g_{(3)}(X)\\ f(X)\ \equiv_{\pi^{2(s-t_1)}}\ \tilde{h}_{(1)}(X)\cdot\tilde{h}_{(2)}(X)\ \equiv_{\pi^{2(s-t_1-t_0)}}\ \tilde{h}_{(1)}(X)\cdot\tilde{\tilde{g}}_{(2)}(X)\cdot\tilde{\tilde{g}}_{(3)}(X)\ .\end{array}$$

Comparing the result (i) of Lemma 14.(1) for three factors with the result (ii) of two subsequent applications of Lemma 14.(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.

2.3 Case $f(X) \equiv_\pi X^M$

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 $g_{(1)}(X),\ldots,g_{(n)}(X)\in R[X]$ with degree ≥ 1. Write $m_{(k)} := \deg(g_{(k)})$ and $M_{(k)} := M - m_{(k)}$ for $k\in[1,n]$. Suppose the ordering to be chosen such that $m_{(1)}\leq m_{(2)}\leq\cdots\leq m_{(n)}$ and that $\mathrm{Res}(g_{(1)},\ldots,g_{(n)})\neq 0$. Let $t := \mathrm{v}_\pi\big(\mathrm{Res}(g_{(1)},\ldots,g_{(n)})\big)$, $t' := e' := \mathrm{v}_\pi\big(\mathrm{Res}(g_{(1)}\,,\,\ldots\,,\,g_{(n)})\big) - \sum_{j\in[1,n-1]}\big((n-j)m_{(j)}-1\big)$. Let $s\geq t+t'+1$. Suppose that $f(X)\equiv_{\pi^s}\prod\limits_{k\in[1,n]} g_{(k)}(X)$. We remark that $g_{(k)}(X)\equiv_\pi X^{m_{(k)}}$ for $k\in[1,n]$.
(Note that we may replace $s\geq t+t'+1$ by $s\geq \mathrm{v}_\pi(\Delta(f))+1$ if $\Delta(f)\neq 0$; cf. Proposition 9.)

Lemma 19. *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 $b_i = \sum_{i_{(k)}\in[0,\chi_{(k)}]\text{ for }k\,\in\,[1,\ell],\ i_{(1)}+\cdots+i_{(\ell)}\,=\,i}\ \prod_{k\in[1,\ell]} h_{(k)i_{(k)}}$. 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 $|\{\,k\in[1,\ell]\ :\ i_{(k)}=\chi_{(k)}\,\}|\ >\ \max\{\,j\in[0,\ell]\ :\ \chi_{(1)}+\cdots+\chi_{(j)}\leq i\,\}$. 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, using $\chi_{(1)}\leq\chi_{(2)}\leq\cdots\leq\chi_{(\ell)}$, we get $i = i_{(1)}+\cdots+i_{(\ell)} = (\sum_{k\in H} i_{(k)})+(\sum_{k\in[1,\ell]\smallsetminus H} i_{(k)})\geq\sum_{k\in H} i_{(k)} = \sum_{k\in H}\chi_{(k)}\geq\sum_{k\in[1,|H|]}\chi_{(k)} > i$. *Contradiction.* □

Lemma 20.

(1) *We have $e'\geq 0$.*

(2) *Given $y\in\pi^{e'}R^{1\times M}$, there exists $x\in R^{1\times M}$ such that $x\,\mathrm{Sylv}(g_{(1)}\,,\,\ldots\,,\,g_{(n)}) = y$.*

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

Proof. Write $\prod\limits_{j\in[1,n]\smallsetminus\{k\}} g_{(j)}(X) \;=:\; \sum\limits_{i\in[0,M_{(k)}]} a_{(k)i}X^i$ for $k \in [1,n]$.

Suppose given $i \in [1,M]$. Write $d_i \;:=\; (n-1) - \max\{\, j\in[0,n-1] \,:\, m_{(1)}+\dots+m_{(j)} \leq i-1\,\}$. Note that $d_\xi \geq d_\eta$ for $1 \leq \xi \leq \eta \leq M$. By Lemma 19, we have $\mathrm{v}_\pi(a_{(k)i-1}) \;\geq\; d_i$ 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 $\mathrm{v}_\pi(a_{(k)\xi-1}) \;\geq\; d_\xi \;\geq\; d_i$ for $k \in [1,n]$ and $\xi \in [1,i]$. Hence π^{d_i} divides column number i of $\mathrm{Sylv}(g_{(1)}\,,\,\dots\,,\,g_{(n)})$; cf. Definition 3.

We have

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

whence $\mathrm{v}_\pi(\det \mathrm{Sylv}(g_{(1)}\,,\,\dots\,,\,g_{(n)})) - (d_2+\dots+d_M) \;=\; e'$. So assertion (2) follows by Lemma 12.(3), assertion (3) follows by Lemma 13.(3); moreover, assertion (1) follows by Remark 11. □

Lemma 21.

(1) *There exist monic polynomials* $\tilde{g}_{(1)}(X),\dots,\tilde{g}_{(n)}(X) \in R[X]$ *such that* $\tilde{g}_{(k)}(X) \equiv_{\pi^{s-t'}} g_{(k)}(X)$ *for* $k \in [1,n]$ *and* $f(X) \equiv_{\pi^{2(s-t')}} \prod\limits_{k\in[1,n]} \tilde{g}_{(k)}(X)$.

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* $\mathrm{v}_\pi(\mathrm{Res}(\tilde{g}_{(1)}\,,\,\dots\,,\,\tilde{g}_{(n)})) \;=\; t$ *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* $\tilde{g}_{(1)}(X)\,,\,\dots\,,\,\tilde{g}_{(n)}(X)$, $\tilde{h}_{(1)}(X),\dots,\tilde{h}_{(n)}(X) \in R[X]$ *such that* $\tilde{g}_{(k)}(X) \equiv_{\pi^{s-t'}} g_{(k)}(X)$ *and* $\tilde{h}_{(k)}(X) \equiv_{\pi^{s-t'}} g_{(k)}(X)$ *for* $k \in [1,n]$ *and* $\prod\limits_{k\in[1,n]} \tilde{g}_{(k)}(X) \equiv_{\pi^{2(s-t')-r}} \prod\limits_{k\in[1,n]} \tilde{h}_{(k)}(X)$. *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 § 1.

Proof. Ad (1). *Existence of admissible′ lift.* We make the ansatz $\tilde{g}_{(k)}(X) \;=\; g_{(k)}(X) + \pi^{s-t'}u_{(k)}(X)$ 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

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

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 $b(X) \overset{!}{\equiv}_{\pi^{s-t'}} \sum_{k\in[1,n]} u_{(k)}(X) \cdot \prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X)$. So it suffices to find $u_{(k)}(X) \in R[X]$ for $k \in [1,n]$ as above such that $b(X) \overset{!}{=} \sum_{k\in[1,n]} u_{(k)}(X) \cdot \prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X)$.
Writing $b(X) =: \sum_{i\geq 0} \beta_i X^i$, $\prod_{\ell\in[1,n]\smallsetminus\{k\}} g_{(\ell)}(X) =: \sum_{i\geq 0} a_{(k)i} X^i$, $u_{(k)}(X) =: \sum_{i\geq 0} u_{(k)i} X^i$ 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

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

such that $U \cdot \mathrm{Sylv}(g_{(1)}, \dots, g_{(n)}) \overset{!}{=} (\beta_0 \dots \beta_{M-1})$. Note that $(\beta_0 \dots \beta_{M-1}) \in \pi^{t'} R^{1\times M}$ since $b(X) \equiv_{\pi^{t'}} 0$. So U exists as required by Lemma 20.(2).
Valuation of resultant. Since $\tilde{g}_{(k)}(X) \equiv_{\pi^{s-t'}} g_{(k)}(X)$ for $k \in [1,n]$, Remark 10 implies that $\mathrm{Res}(\tilde{g}_{(1)}, \dots, \tilde{g}_{(n)}) \equiv_{\pi^{s-t'}} \mathrm{Res}(g_{(1)}, \dots, g_{(n)})$. Since $s - t' \geq t + 1 = \mathrm{v}_\pi(\mathrm{Res}(g_{(1)}, \dots, g_{(n)})) + 1$, this implies $\mathrm{v}_\pi(\mathrm{Res}(\tilde{g}_{(1)}, \dots, \tilde{g}_{(n)})) = \mathrm{v}_\pi(\mathrm{Res}(g_{(1)}, \dots, g_{(n)})) = t$.
Ad (2). Writing $\tilde{g}_{(k)}(X) =: g_{(k)}(X) + \pi^{s-t'} u_{(k)}(X)$ and $\tilde{h}_{(k)}(X) =: g_{(k)}(X) + \pi^{s-t'} v_{(k)}(X)$ 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 $u_{(k)}(X) \overset{!}{\equiv}_{\pi^{s-2t'-r}} v_{(k)}(X)$ for $k \in [1,n]$. We have

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

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

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

we have to show that $W \overset{!}{\in} \pi^{s-2t'-r} R^{1\times M}$. From $(*)$, we obtain $W \cdot \mathrm{Sylv}(g_{(1)}, \dots, g_{(n)}) \in \pi^{s-t'-r} R^{1\times M}$. Note that $s - t' - r \geq t' = e'$. So we can infer by Lemma 20.(3) that $W \in \pi^{(s-t'-r)-t'} R^{1\times M} = \pi^{s-2t'-r} R^{1\times M}$. □

Theorem 22. *Suppose R to be a complete discrete valuation ring. Recall that $f(X) \in R[X]$ is a monic polynomial, that $M = \deg f$, that $f(X) \equiv_\pi X^M$, that $g_{(1)}(X), \dots, g_{(n)}(X) \in R[X]$ are* *monic polynomials, that* $t = \mathrm{v}_\pi\big(\operatorname{Res}(g_{(1)},\ldots,g_{(n)})\big)$*, that* $m_{(k)} = \deg(g_{(k)})$ *for* $k \in [1,n]$*, ordered such that* $m_{(1)} \leq \cdots \leq m_{(n)}$ *, that* $t' = \mathrm{v}_\pi\big(\operatorname{Res}(g_{(1)}\,,\,\ldots\,,\,g_{(n)})\big) - \sum_{j\in[1,n-1]}\big((n-j)m_{(j)}-1\big)$*, that* $s \geq t+t'+1$ *and that* $f(X) \equiv_{\pi^s} \prod\limits_{k\in[1,n]} g_{(k)}(X)$*.*

Then there exist unique monic polynomials $\overset{\vee}{g}_{(1)}(X)\,,\,\ldots\,,\,\overset{\vee}{g}_{(n)}(X) \in R[X]$ *such that* $\overset{\vee}{g}_{(k)}(X) \equiv_{\pi^{s-t'}} g_{(k)}(X)$ *for* $k\in[1,n]$ *and* $f(X) = \prod\limits_{k\in[1,n]} \overset{\vee}{g}_{(k)}(X)$ *.*

Proof. Existence. Since R is complete, it suffices to show that there exist monic polynomials $\tilde g_{(1)}(X),\ldots,\tilde g_{(n)}(X) \in R[X]$ such that $f(X) \equiv_{\pi^{s+1}} \prod\limits_{k\in[1,n]} \tilde g_{(k)}(X)$ and $\tilde g_{(k)}(X) \equiv_{\pi^{s-t'}} g_{(k)}(X)$ for $k\in[1,n]$, and $\mathrm{v}_\pi(\operatorname{Res}(\tilde g_{(1)},\ldots,\tilde g_{(n)})) = t$. This follows from Lemma 21.(1) since $2(s-t') \geq s+1$.

Uniqueness. Given $\overset{\vee}{g}_{(1)}(X),\ldots,\overset{\vee}{g}_{(n)}(X)\,,\,\overset{\vee}{h}_{(1)}(X),\ldots,\overset{\vee}{h}_{(n)}(X) \in R[X]$, all monic, such that $\overset{\vee}{g}_{(k)}(X) \equiv_{\pi^{s-t'}} g_{(k)}(X) \equiv_{\pi^{s-t'}} \overset{\vee}{h}_{(k)}(X)$ for $k\in[1,n]$ and $\prod\limits_{k\in[1,n]} \overset{\vee}{g}_{(k)}(X) = f(X) = \prod\limits_{k\in[1,n]} \overset{\vee}{h}_{(k)}(X)$, we have to show that $\overset{\vee}{g}_{(k)}(X) \overset{!}{=} \overset{\vee}{h}_{(k)}(X)$ for $k\in[1,n]$.

Note that $\mathrm{v}_\pi(\operatorname{Res}(\overset{\vee}{g}_{(1)}\,,\,\ldots\,,\,\overset{\vee}{g}_{(n)})) = t = \mathrm{v}_\pi(\operatorname{Res}(\overset{\vee}{h}_{(1)}\,,\,\ldots\,,\,\overset{\vee}{h}_{(n)}))$ by Lemma 21.(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 21.(1), since $\overset{\vee}{h}_{(k)}(X) \equiv_{\pi^{s_1-t'}} \overset{\vee}{g}_{(k)}(X)$ for $k\in[1,n]$ and the other required congruences are verified using equalities. So Lemma 21.(2) yields $\overset{\vee}{h}_{(k)}(X) \equiv_{\pi^{2(s_1-t')-t'}} \overset{\vee}{g}_{(k)}(X)$ 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, since $\overset{\vee}{h}_{(k)}(X) \equiv_{\pi^{s_2-t'}} \overset{\vee}{g}_{(k)}(X)$ for $k\in[1,n]$. So Lemma 21.(2) yields $\overset{\vee}{h}_{(k)}(X) \equiv_{\pi^{2(s_2-t')-t'}} \overset{\vee}{g}_{(k)}(X)$ 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 $\overset{\vee}{h}_{(k)}(X) \equiv_{\pi^{s_\ell-t'}} \overset{\vee}{g}_{(k)}(X)$ for $k\in[1,n]$ and $\ell\geq 1$. Hence $\overset{\vee}{h}_{(k)}(X) = \overset{\vee}{g}_{(k)}(X)$ for $k\in[1,n]$. □

Example 23. Suppose that $n=3$ and $s\geq 2t+1$. Write $t_0 := \mathrm{v}_\pi(\operatorname{Res}(g_{(2)}\,,\,g_{(3)}))$ and $t_1 := \mathrm{v}_\pi(\operatorname{Res}(g_{(1)}\,,\,g_{(2)}g_{(3)}))$. Lemma 6 gives $\operatorname{Res}(g_{(1)}\,,\,g_{(2)}\,,\,g_{(3)}) = \operatorname{Res}(g_{(1)}\,,\,g_{(2)}g_{(3)})\cdot\operatorname{Res}(g_{(2)}\,,\,g_{(3)})$, whence $t = t_1+t_0$. In particular, t_0 and t_1 are finite.

Denote $t' := t - 2m_{(1)} - m_{(2)} + 2$, $t'_0 := t_0 - m_{(2)} + 1$ and $t'_1 := t_1 - m_{(1)} + 1$. So $s \geq 2t+1 \geq t+t'+1$ and $t' = t'_1 + t'_0 - m_{(1)}$.

We can apply Lemma 21.(1) to $f(X) \equiv_{\pi^s} g_{(1)}(X)\cdot g_{(2)}(X)\cdot g_{(3)}(X)$ to obtain monic polynomials $\tilde g_{(1)}(X)\,,\,\tilde g_{(2)}(X)\,,\,\tilde g_{(3)}(X) \in R[X]$ such that

(i$'$) $\quad \tilde g_{(k)}(X) \equiv_{\pi^{s-t'}} g_{(k)}(X)$ for $k\in[1,3]$, $\quad f(X) \equiv_{\pi^{2(s-t')}} \tilde g_{(1)}(X)\cdot\tilde g_{(2)}(X)\cdot\tilde g_{(3)}(X)$.

We can also apply Lemma 21.(1) first to the factorisation $f(X) \equiv_{\pi^s} g_{(1)}(X)\cdot(g_{(2)}(X)\cdot g_{(3)}(X))$ and then to the resulting factorisation of the second factor into $g_{(2)}(X)\cdot g_{(3)}(X)$ modulo a certain power of π.

We have $s \geq 2t+1 \geq 2t_1+1 \geq t_1+t'_1+1$. So Lemma 21.(1) gives monic polynomials $\tilde h_{(1)}(X)\,,\,\tilde h_{(2)}(X) \in R[X]$ such that

$$\tilde h_{(1)}(X) \equiv_{\pi^{s-t'_1}} g_{(1)}(X)\,,\quad \tilde h_{(2)}(X) \equiv_{\pi^{s-t'_1}} g_{(2)}(X)\cdot g_{(3)}(X)\,,\quad f(X) \equiv_{\pi^{2(s-t'_1)}} \tilde h_{(1)}(X)\cdot\tilde h_{(2)}(X)\,.$$

We have $s \geq 2t+1 \geq 2t-m_{(2)}-m_{(1)}+3-t_1 = (2t_0-m_{(2)}+1)+(t_1-m_{(1)}+1)+1 = (t_0+t'_0)+t'_1+1$ and thus $s-t'_1 \geq t_0+t'_0+1$. So Lemma 21.(1) gives monic polynomials $\tilde{\tilde{g}}_{(2)}(X)\,,\, \tilde{\tilde{g}}_{(3)}(X) \in R[X]$ such that

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

Altogether, the two subsequent applications of Lemma 21.(1) for two factors yield

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

Comparing the result (i$'$) of Lemma 21.(1) for three factors with the result (ii$'$) of two subsequent applications of Lemma 21.(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.

3 Examples

To illustrate Theorem 16 we consider some polynomials in the complete discrete valuation ring $\mathbb{Z}_p$ for a prime number p. 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, the method of the proof of Lemma 14 gives a factor decomposition in $\mathbb{Z}[X]$ to a higher p-adic precision. We use the notation of Lemma 14.

Write $g_{(k)}(X) =: \sum_{j\in[0,m_{(k)}]} c_{(k)j}X^j$ and $\tilde{g}_{(k)}(X) =: \sum_{j\in[0,m_{(k)}]} \tilde{c}_{(k)j}X^j$ for $k \in [1,n]$, where $c_{(k)j}\,,\tilde{c}_{(k)j} \in \mathbb{Z}$.

Write $f(X) - \prod_{k\in[1,n]} g_{(k)}(X) =: \sum_{j\in[0,M]} w_jX^j$, where $w_j \in \mathbb{Z}$. Let s be the current precision, i.e.

$$s \;:=\; \min\,\{\,\mathrm{v}_\pi(w_j) \;:\; j\in[0,M]\,\}\;.$$

In the respective initial step of the examples below, we ensure that $s \geq \mathrm{v}_p(\Delta(f))+1$. Write

$$s' \;:=\; \min\,\{\,\mathrm{v}_\pi(c_{(k)j}-\tilde{c}_{(k)j}) \;:\; k\in[1,n],\; j\in[0,m_{(k)}]\,\}\;.$$

By Lemma 14, we have $s' \geq s-t$. Let the *defect* be $s-s'$. The defect is bounded above by t. If $f(X) \equiv_\pi X^M$ and the degrees of the factors $g_{(k)}(X)$ are sorted increasingly, then the defect $s-s'$ is bounded above by t'; cf. Lemma 21.

The following examples have been calculated using Magma [**1**].

Example 24. We consider the polynomial

$$f(X) = X^3+X^2-2X+8$$

at $p=2$; it has been used as an example by Dedekind and Koch; cf. [**3,** p. 225], [**8,** §3.12, introduction to §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	defect $s - s'$
1	3	1
2	4	1
3	6	1
4	10	1
5	18	1
6	34	1
7	66	1
8	130	1
9	258	1
10	514	1

The defect seems to be constant with value 1. We observe that the defect is maximal. Note that in step 1, the precision grows only by 1.

Example 25.

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

$$\begin{aligned} g_{(1)}(X) &= X + 4806835024200164988203597724980 \\ g_{(2)}(X) &= X - 4806835024200164988203597724980 \\ g_{(3)}(X) &= X^6 - 10930621241981427804662485599984X^4 \\ &\quad -4943636030726675686411786481408X^2 \\ &\quad -4341143474460317541052331090944. \end{aligned}$$

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	defect $s - s'$
1	103	3
2	200	4
3	392	5
4	774	1
5	1546	9
6	3074	3
7	6142	7
8	12270	3
9	24534	7
10	49054	3

Example 26.

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

$$\begin{aligned}
g_{(1)}(X) &= X + 125484529130217068707 8 \\
g_{(2)}(X) &= X^3 + 343911488029972859532 9X^2 \\
&\quad +209791225526915951828 4X \\
&\quad +238787830399121249695 8 \\
g_{(3)}(X) &= X^6 + 416897794805060181352 2X^5 \\
&\quad +341433592444518944737 2X^4 \\
&\quad -469523799801953629710X^3 \\
&\quad -373378169446952596054 2X^2 \\
&\quad +274112226355461500643 3X \\
&\quad +305729399591389508503 5.
\end{aligned}$$

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	defect $s - s'$
1	46	3
2	86	0
3	172	3
4	338	2
5	672	1
6	1342	2
7	2680	1
8	5358	2
9	10712	1
10	21422	2

The defect seems to be eventually periodic.

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.

[2] Cohn, P.M., *Algebra,* Vol. 1, Wiley, 1982.

[3] Dedekind, R. *Gesammelte Mathematische Werke,* Band 1, Vieweg, 1930.

[4] Ford, D.; Pauli, S.; Roblot, X.-F., *A fast algorithm for polynomial factorization over* $\mathbb{Q}_p$, J. Th. Nombres Bordeaux 14 (1), p. 151–169, 2002.

[5] 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.

[6] Gauss, C.F., *Werke,* Band II, zweiter Abdruck, 1876.

[7] Hensel, K., *Neue Grundlagen der Arithmetik,* J. Reine Angew. Math. 127, p. 51–84, 1904.

[8] Koch, H., *Zahlentheorie,* Vieweg, 1997.

[9] van der Waerden, B. L., *Algebra,* Springer Grundlehren, 5. Aufl., 1960.

Juliane Deißler
University of Stuttgart
Fachbereich Mathematik
Pfaffenwaldring 57
D-70569 Stuttgart
juliane.deissler@mint-kolleg.de