Newton polygons

Bill Casselman
University of British Columbia
cass@math.ubc.ca

Newton polygons are associated to polynomials with coefficients in a discrete valuation ring, and they give information about the valuations of roots. There are several applications, among them to the structure of Dieudonné modules, the ramification of local field extensions, and the desingularization of algebraic curves in $\mathbb{P}^2$.

As an exception to a common practice of attribution, Newton polygons were originally introduced by Isaac Newton himself, and how he used them is not so different from how they are used now. He wanted to solve polynomial equations $f(x, y) = 0$ for y as a series in fractional powers of x. For example, to solve $y^n = x$ we write simply $y = x^{1/n}$, and

$$\text{to solve} \quad y^n = 1 + x \quad \text{set} \quad y = \sum\nolimits_0 \binom{1/n}{k} x^k \,.$$

Newton sketched the procedure he had come up with in a letter to Oldenburg. It is quite readable (see p. 126 of [Newton:1959] for the original Latin, p. 145 for an English translation). The diagram he exhibits is not essentially different from the ones drawn today. Newton polygons are perfectly and appropriately named—they are non-trivial, and introduced by Newton. This thread became eventually a method related to desingularizing algebraic curves over $\mathbb{C}$ (explained in Chaper IV of [Walker:1950]).

My original motivation in writing this essay was to understand the theory of crystals, particularly §5 of Chapter IV of [Demazure:1970]. But since then I have come across other applications. One recent one is the account in [Lubin:2012] of ramification groups and what Serre has called the *Herbrand function* in terms of Newton polygons. Another is the computation of splitting fields of polynomials defined over local fields, for example in [Romano:2000], [Greve-Pauli:2013], and [Milstead et al.:2018]. I shall take these topics up elsewhere.

Contents

Throughout, let

$$\begin{aligned} \mathfrak{o} &= \text{ a complete discrete valuation ring} \\ \mathfrak{k} &= \text{ its quotient field} \\ \mathfrak{p} &= \text{ the maximal ideal of } \mathfrak{o} \\ \mathbb{F} &= \text{ the quotient } \mathfrak{o}/\mathfrak{p} \\ \varpi &= \text{ a generator of } \mathfrak{p} \\ \overline{\mathfrak{k}} &= \text{ an algebraic closure of } \mathfrak{k} \\ \operatorname{ord}(x) &= n \text{ if } x = u\varpi^n \text{ with } u \text{ in } \mathfrak{o}^\times . \end{aligned}$$

Write $x \equiv_n y$ to mean $x - y \in \mathfrak{p}^n$.

For $\mathfrak{l}$ a finite extension of $\mathfrak{k}$, let $\mathfrak{o}_\mathfrak{l}$ be its ring of integers, $\mathfrak{p}_\mathfrak{l}$ its prime ideal. Then $\mathfrak{p}_\mathfrak{l}^e = \mathfrak{p}$, where e is the ramification degree of $\mathfrak{l}/\mathfrak{k}$. The homomorphism ord from $\mathfrak{k}^\times$ to $\mathbb{Z}$ may be extended to one from $\mathfrak{l}^\times$ to $(1/e)\mathbb{Z}$, and then in turn to one from all of $\overline{\mathfrak{k}}^\times$ to $\mathbb{Q}$. This extension also satisfies the conditions that

$$\begin{array}{ll} \text{(oa)} & \mathrm{ord}\,(x+y) \ge \min(\mathrm{ord}\,(x), \mathrm{ord}\,(y)) \\ \text{(ob)} & \mathrm{ord}\,(x+y) = \min(\mathrm{ord}\,(x), \mathrm{ord}\,(y)) \ \text{ if } \ \mathrm{ord}\,(x) \ne \mathrm{ord}\,(y)\,. \end{array}$$

Part I. Polynomials

1. Introduction

Suppose $P(x) = p_n x^n + p_{n-1}x^{n-1} + \cdots + p_0$ to be a non-zero polynomial of degree n in $\mathfrak{k}[x]$.

If α lies in $\overline{\mathfrak{k}}$, what can we say about $\mathrm{ord}\,(P(\alpha))$?

The condition (oa) implies that all we can say in general is that

$$\mathrm{ord}\,P(\alpha) \ge \mathrm{ord}\,(p_k) + k\,\mathrm{ord}\,(\alpha)$$

for all k. But (ob) tells us that

$$\mathrm{ord}\,\big(P(\alpha)\big) = \min\nolimits_k\big(\mathrm{ord}\,(p_k) + k\,\mathrm{ord}\,(\alpha)\big)$$

if there is a unique k such that $\mathrm{ord}\,(p_k) + k\,\mathrm{ord}\,(\alpha)$ is minimum.

These assertions can be characterized geometrically. Let Σ_P be the set of points $P_k = (k, \mathrm{ord}\,(p_k))$ in the (x, y) plane for all k in $\mathbb{Z}$, with the convention that $\mathrm{ord}\,(0) = \infty$. Let $\mathcal{C}_P$ be the convex hull of Σ_P. Its boundary is called the **Newton polygon** of the polynomial f. It will have vertical sides contained in the line $x = 0$ and $x = n$. At lower left lies the corner $(0, \mathrm{ord}\,(p_0))$ and at lower right $(n, \mathrm{ord}\,(p_n))$. The set $\mathcal{C}_P$ will be stable under vertical shifts upwards, and is bounded below. Therefore (1) every linear function

$$y + \lambda x$$

in the (x, y)-plane will have a minimum value on it, and (2) the region $\mathcal{C}_P$ is determined by the functions of this form that are non-negative on it.

This minimum value will in general be at a unique vertex $(k, \mathrm{ord}\,(c_k))$, but for certain **exceptional** λ the minimum value will be taken along all of an edge of $\mathcal{C}_P$. The exceptional values of λ coincide with the negative slopes of the edges of $\mathcal{C}_P$, and there are hence a finite number.

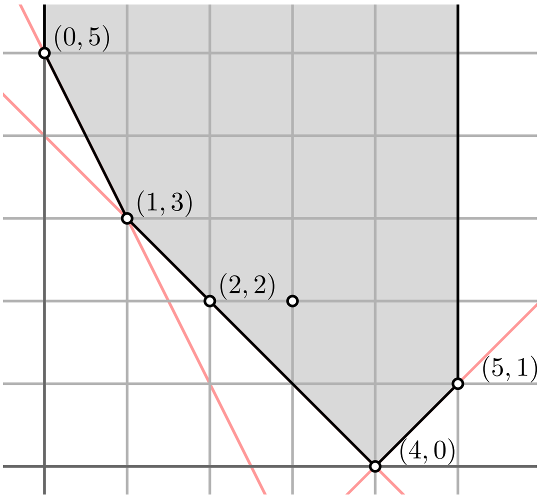
1.1. Lemma. *If $\mathrm{ord}\,(\alpha)$ is unexceptional, then*

$$\mathrm{ord}\,(P(\alpha)) = \min\nolimits_k\big(\mathrm{ord}\,(p_k) + k\,\mathrm{ord}\,(\alpha)\big)\,.$$

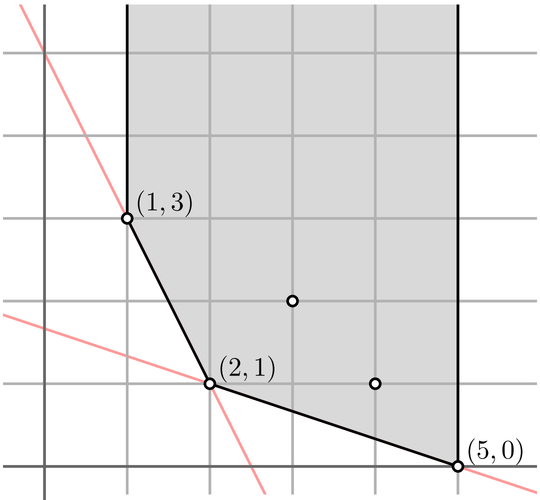
In particular, if $\mathrm{ord}\,(\alpha)$ is unexceptional, $\mathrm{ord}\,(P(\alpha)$ is finite. Therefore:

1.2. Corollary. *If $P(\alpha) = 0$ then $\mathrm{ord}\,(\alpha)$ is the negative slope of one of the bottom edges of the Newton polygon of P.*

Here are two examples of Newton polygons:



$P(x) = p^5 + p^3x + p^2x^2 + p^2x^3 - x^4 + px^5$



$P(x) = p^3x + px^2 + p^2x^3 - px^4 + x^5$

For the moment, Corollary 1.2 the main consequence of our discussion. It might not seem complete, since I have not shown that every occurring slope is the order of a root. There is one case in which this should be clear. Since in between $x = i$ and $x = i + 1$ the slope doesn't change, there are at most n distinct slopes. If the orders of the roots are all different, then they must coincide exactly with the set of slopes. Less obvious is the main fact about Newton polygons: *the orders of the roots and the negatives of the slopes of the Newton polygon coincide, even counting multiplicity.* We'll see why in the next section.

From now on, let $\textsc{np}_P$ be the function on the range $[0, n]$ whose graph is the bottom of the Newton polygon of P.

2. The main theorem

Since the valuation of $\mathfrak{k}$ extends canonically to $\overline{\mathfrak{k}}$, one can define by exactly the same formula the Newton polygon of any polynomial f in $\overline{\mathfrak{k}}[X]$. For each $i \geq 1$, let λ_i be its slope between $x = i - 1$ and $x = i$—i.e. the slope of the i-th segment, reading left to right. The **slope sequence** of f is the n-tuple $(\lambda_1, \lambda_2, \ldots, \lambda_n)$. By definition of convexity, $\lambda_i \leq \lambda_{i+1}$. In the figure on the left above, the slope sequence is $(-2, -1, -1, -1, 1)$ and on the right it is $(-2, -1/3, -1/3, -1/3)$.

We have seen in the previosu section that if α is a root of $P(x)$ then $-\mathrm{ord}\,(\alpha)$ is the negative of one of the slopes on the Newton polygon. If the slopes of the are all different, this implies that the orders of the roots are exactly these negative slopes. This leaves up in the air what happens when some of the slopes have multiplicity. This turns out not to be a probem:

2.1. Theorem. *Suppose that*

$$P = c \cdot \prod (x - \alpha_i)$$

lies in $\overline{\mathfrak{k}}[X]$*. Arrange the* α_i *in decreasing magnitude, so that*

$$\mu_1 = \mathrm{ord}\,(\alpha_1) \leq \mu_2 = \mathrm{ord}\,(\alpha_2) \leq \ldots \leq \mu_n = \mathrm{ord}\,(\alpha_n)\,.$$

Then the slope sequence of the Newton polygon is

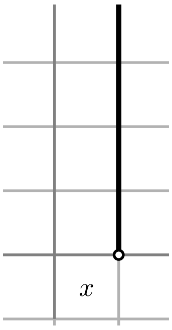
$$-\mu_n, -\mu_{n-1}, \ldots\,, -\mu_1\,.$$

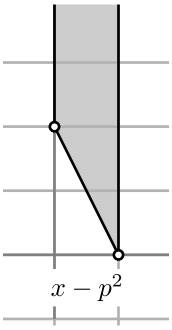
In another formulation, suppose $P = \prod_1^n (x - \alpha)$. Suppose x in $[k - 1, k]$ with $1 \leq k \leq n$. Then

$$\textsc{np}(x) = \sum\nolimits_{k+1}^{n} \mathrm{ord}\,(\alpha_i) + (k - x)\,\mathrm{ord}\,(\alpha_k)\,.$$

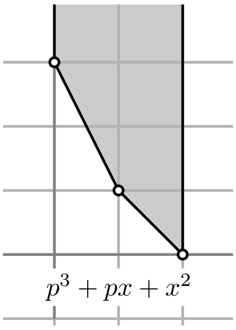
The reason for the choice of indexing should become clear in a moment. Before beginning the proof, let's look at a few examples.

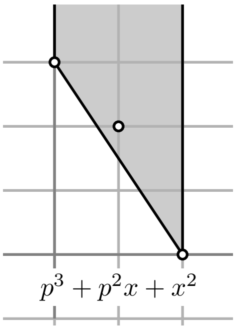
- Suppose $P = x - \alpha$. Its polygon is the segment between $(0, \operatorname{ord}(\alpha))$ and $(1, 0)$, and the claim is trivial.





- Now suppose $P = (x - \alpha)(X - \beta) = x^2 - (\alpha + \beta)x + \alpha\beta$, with $\operatorname{ord}(\alpha) \geq \operatorname{ord}(\beta)$. The constant term is $\alpha\beta$, so one point on the polygon is $(0, \operatorname{ord}(\alpha) + \operatorname{ord}(\beta))$. Another is $(2, 0)$. Otherwise, there are two cases: (1) $\operatorname{ord}(\alpha) > \operatorname{ord}(\beta)$, (2) $\operatorname{ord}(\alpha) = \operatorname{ord}(\beta)$. In the first $\operatorname{ord}(\alpha + \beta) = \operatorname{ord}(\beta)$, and so there are two distinct slopes. In the second, $\operatorname{ord}(\alpha + \beta) \geq \operatorname{ord}(\alpha) = \operatorname{ord}(\beta) =$ (say) λ, and the polygon is the single segment from $(0, 2\lambda)$ to $(2, 0)$.





Proof of the Theorem. One may as well assume $c = 1$, since multiplying P by c only shifts $\mathcal{C}_P$ vertically by $\operatorname{ord}(c)$. For each subset I of $[1, n]$ let

$$\alpha_I = \prod_{i \in I} \alpha_i \,.$$

So now

$$P(x) = \sum_0^n p_i x^i$$

with $p_0 = 1$ and

$$p_k = \sum_{|I|=n-k} \alpha_I \,.$$

For example, $p_n = \prod_1^n \alpha_i$. Let

$$\begin{aligned} M_k &= \min\nolimits_{|I|=k} \operatorname{ord}(\alpha_I) \\ &= \operatorname{ord}(\alpha_1 \ldots \alpha_k) \\ &= \mu_1 + \cdots + \mu_k \,, \end{aligned}$$

with the convention that $M_0 = 0$. The corner of the Newton polygon at the far left is $(0, M_n)$, that far right is $(n, 0)$. The assertion of the Theorem is that the bottom of the Newton polygon is the polygonal path connecting all the points (k, M_{n-k}). I'll call this path Γ_P. This will follow from the following two claims, together with basic facts about convex regions: (1) the path Γ_P lies (weakly) below the Newton polygon; (2) its vertices (i.e. its extremal points) lie on the Newton polygon.

The first follows immediately from the inequality

$$\mathrm{ord}\,(p_k) \ge \min_{|I|=k} \mathrm{ord}\,(\alpha_I) = M_k\,.$$

For the second, it suffices to show that the actual vertices of Γ_P are points of the Newton polygon. So I ask, what is the shape of the path Γ_P? The segment from $(n-k, M_k)$ to $(n-k+1, M_{k-1})$ has slope $\mathrm{ord}\,(\alpha_k)$. The vertices of Γ_P are therefore the points $(n-k, M_k)$ for which $\mathrm{ord}\,(\alpha_{k+1}) > \mathrm{ord}\,(\alpha_k)$. But then $\mathrm{ord}\,(\alpha_{k+1}) > \mathrm{ord}\,(\alpha_j)$ for all $j \le k$, and $\mathrm{ord}\,(p_{n-k}) = M_k$, so that $(n-k, M_k)$ is a vertex of $\mathcal{C}_P$. ▯

As an immediate consequence:

2.2. Corollary. *Suppose $P(x)$ and $Q(x)$ to be polynomials in $\overline{\mathfrak{k}}[x]$. Suppose that* $\mathrm{ord}\,(\alpha) \ge \mathrm{ord}\,(\beta)$ *whenever α is a root of $P(x)$ and β is a root of Q. Then the Newton polygon of PQ is obtained by joining shifted copies of the Newton polygons of f and g, first f and then g, so as to make a continuous path.*

In other words, let k, ℓ be the degrees of P, Q. Then

$$\mathrm{NP}_{PQ}(x) = \begin{cases} \mathrm{NP}_P(x) + \mathrm{ord}\,(q_0) & \text{if } 0 \le x \le k \\ \mathrm{NP}_Q(x-k) & \text{if } k \le x \le p+q. \end{cases}$$

2.3. Corollary. *Suppose the bottom of the Newton polygon of the polynomial $P(x)$ in $\mathfrak{k}[x]$ is a single line segment from* $(0, \mathrm{ord}\,(p_0)$ *to $(n, 0)$ that does not contain any integral nodes (i, m). Then P is irreducible in $\mathfrak{k}[x]$.*

Because according to the previous corollary, if $P = QR$ then the Newton polygon of P would be the join of those of Q and R at an integral node. ▯

And in turn a consequence. Recall that an **Eisenstein polynomial** is one of the form $x^n + \sum_i x^i$ with all p_i in $\mathfrak{o}$, $\mathrm{ord}\,(p_i) \ge 1$ for all i, and $\mathrm{ord}\,(p_0) = 1$.

2.4. Corollary. *Every Eisenstein polynomial is irreducible in $\mathfrak{k}[x]$.*

An amusing consequence:

2.5. Corollary. *A rational number that is an algebraic integer is an integer.*

Proof Because it is an integer in every $\mathbb{Q}_p$. ▯

COMPUTATION. The proof gives absolutely no idea of how to find explicit solutions, and in fact this is a task that depends on the particular field $\mathfrak{k}$. There is, however, one tool that is ubiquitous. For every element of x in $\mathfrak{o}$ let $\overline{x}$ be its image in $\mathbb{F}$, and for every polynomial P in $\mathfrak{o}[x]$, let $\overline{P}$ be its image in $\mathbb{F}[x]$.

2.6. Proposition. (Hensel's Lemma) *Suppose P to be in $\mathfrak{o}[x]$. If a in $\mathfrak{o}$ satisfies $\overline{P}(\overline{a}) = 0$ and $\overline{P}'(\overline{a}) \ne 0$, then there exists a unique α in $\mathfrak{o}$ such that $P(\alpha) = 0$ and $\overline{\alpha} = \overline{a}$.*

Proof. This follows directly from the $\mathfrak{p}$-adic version of the method of Newton-Raphson for solving equations:

2.7. Lemma. *Suppose that $f(a) \equiv_n 0$ and that $f'(a)$ is a unit in $\mathfrak{o}^\times$. Then*

$$b = a - \frac{f(a)}{f'(a)}$$

satisfies $f(b) \equiv_{2n} 0$.

Proof. From Taylor's series:

$$\begin{aligned} f\left(a - \frac{f(a)}{f'(a)}\right) &= f(a) - f'(a)\cdot\frac{f(a)}{f'(a)} + \left(\frac{f(a)}{f'(a)}\right)^2 (\ldots) \\ &= O(\varpi^{2n})\,. \end{aligned}$$

▯

Verifying the assumption on $\overline{P}'(\overline{a})$ can be done by computing the gcd of $\overline{P}(x)$ and $\overline{P}'(x)$, since this will contain as factors all $x - \overline{a}$ with $\overline{a}$ a root of multiplicity greater than one, and factorization in finite fields is well known to be entirely feasible.

The convergence is quadratic, but in practice it is often more convenient to proceed linearly. In this version of the process, one starts with some x_1 in $\mathfrak{o}$ such that $f(x_1) \equiv_1 0$ and then calculates in succession some x_n in $\mathfrak{o}$ (effectively modulo $\mathfrak{p}^n$) such that $f(x_n) \equiv_n 0$. Explicitly:

(2.8)
$$x_{n+1} = x_n - C \cdot f(x_n) \equiv_n x_n \,,$$

with $C \equiv 1/f'(x_1)$. The solution is therefore determined by what I call **Hensel data**: (i) a polynomial $f(x)$ in $\mathfrak{k}[x]$ and (ii) a root x_1 of $f(x)$ modulo $\mathfrak{p}$ such that $f'(x_0) \not\equiv 0$ modulo $\mathfrak{p}$.

Example. Let $\mathfrak{k} = \mathbb{Q}_2$ and
$$P(x) = x^3 + 2x + 1 \,.$$
Then $P'(a) = 3x^2 + 2$ and
$$\overline{P}(x) - x \cdot \overline{P}'(x) = 1$$
so that Hensel's Lemma may be applied to all roots modulo 2—for example 1. Therefore we set $x_1 = 1$ in $\mathbb{Z}/(2)$. For subsequent values of x_n we may identify $\mathbb{Z}/(2^n)$ with $[0, 2^n - 1]$, and take θ to be just the obvious embedding. For example, since $f(1) = 4 \equiv 0 \bmod 2^2$, we have also $x_2 = 1$. For the rest, note that $-1/f'(x_1) = -1/5 \equiv 1$ modulo 2, so
$$x_3 = 1 + f(x_2) = 1 + 4 = 5 \,.$$
Sure enough, $f(5) = 125 + 10 + 1 = 136 \equiv 0$ modulo 8. A few more initial values of x_n:
$$x_1 = 1, \ x_2 = 1, \ x_3 = 5, \ 13, \ 29, \ 29, \ 29, \ 157, \ 157, \ 669, \ 669, \ 2717, \ \ldots$$

Remark. [Jorza:(undated)] explains an algorithm that amounts to a converse to Corollary 2.2: *the partition of the Newton polygon of a polynomial in $\mathfrak{k}[x]$ into edges of distinct slopes corresponds to a factorization of the polygon in $\mathfrak{k}[x]$.*

3. Newton's example

Suppose now $\mathfrak{k}$ to be an algebraically closed field of characteristic 0, $\mathfrak{k} = \mathfrak{k}(\!(x)\!)$ (formal Laurent series in t with coefficients in $\mathfrak{k}$). The argument leading to the following result is suggested implicitly in a letter from Newton to Oldenburg, in which he introduces 'his' polygons. This result also plays an important role in the explicit desingularization of algebraic curves, as explained in [Walker:1950]). But Newton's writing on the subject leaves much to be desired, and the modern version originates in a more extensive exposition by the nineteenth century French mathematician Puiseux.

3.1. Theorem. *The union of the fields $\mathfrak{k}(\!(x^{1/n})\!)$ is an algebraic closure of $\mathfrak{k}$.*

Of course Newton didn't state it this way. In his case the domain of coefficients concerned wasn't even specified explicitly, but he presumably knew only about real numbers. Here is a roughly equivalent formulation, closer to what Newton had in mind:

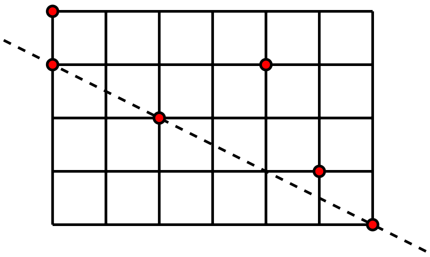
3.2. Corollary. *Suppose $P(x, y)$ to be in $\mathfrak{k}[x, y]$, monic in y of degree n. There exist n series α_i in some $\mathfrak{k}[\![x^{1/m}]\!]$ such that*
$$P(x, y) = \prod (y - \alpha_i) \,.$$

The most subtle point is that one m suffices for all roots. I'll postpone the proof to the next section, but in this one go through one relatively simple example—essentially that in Newton's letter.

Suppose we want to solve

$$y^6 - 5xy^5 + x^3y^4 - 7x^2y^2 + 6x^3 + x^4 = 0\,.$$

Newton plots the exponents (m, n) of each term $(x^n y^m)$ occurring, and considers the bottom of their convex hull. This is equivalent to what we have done earlier. The diagram that arises (which is basically just a copy of Newton's) is this :



Newton then solves the equation obtained by summing just the terms on the line $y + (1/2)x = 3$. This gives us

$$y^6 - 7x^2y^2 + 6x^3 = 0\,,$$

which we can solve explicitly. It is a cubic equation in $Y = y^2$, but more significantly it is homogeneous of weoight 3 in x and y if we assign y a weight of $1/2$, x a weight of 1. This allows us to perform a transformation particular to the case of power series. The equation has homogeneity degree 3 (which is also the y-intercept of the line under consideration). so we divide it by x^3 to get

$$(y/\sqrt{x})^6 - 7(y/\sqrt{x})^2 + 6 = 0\,,$$

or

(3.3)
$$Y^6 - 7Y^2 + 6 = (Y^2-1)(Y^2-2)(Y^2+3) = 0 \qquad (Y = y/\sqrt{x})\,.$$

The solutions are $Y = \pm 1, \pm\sqrt{2}, \pm\sqrt{-3}$.

We now divide the original equation by x^3, getting

$$\frac{y^6}{x^3} - \frac{5y^5}{x^2} + y^4 - \frac{7y^2}{x} + 6 + x = 0\,.$$

Setting $Y = y/\sqrt{x}$ (as before) and also $X = \sqrt{X}$ this becomes

(3.4)
$$f(Y) = \boldsymbol{Y^6} - 5XY^5 + X^4Y^4 \boldsymbol{- 7Y^2} + (\boldsymbol{6} + X) = 0\,.$$

The point of this is that reduced modulo (X) this is the part that is emphasized, which is the same as (3.3). The roots of the reduction are distinct, so we may apply Hensel's Lemma. For the original equation we therefore have solutions which are formal series in $\sqrt{x}$ with leading terms

$$y = \pm\sqrt{x}, \quad \pm\sqrt{2x}, \quad \pm\sqrt{-3x}\,.$$

For Newton only the first four were to be considered, since he excluded imaginary numbers. What Newton says is that these leading terms solve the equation 'very nearly', including almost no details but adding a bit later the remark, "Here some difficulties will sometimes arise . . . " It's hard to know exactly what he meant.

Hensel's Lemma will give a series solution of (3.4) of the form

$$c_0 + c_1X + c_2X^2 + \cdots\,,$$

in which c_0 is a root of (3.3) and we can find the rest of the coefficients inductively.

What we have done so far is illustrated here by the fact that the constant term in (3.4) vanishes if $Y = 1$.

We have

$$f'(1) = 6 - 25X + 4X^4 - 14 = -8 - 25X + 4X^4\,,$$

which is a unit in the ring $\mathbb{R}[[X]]$. Its inverse is

$$\frac{1}{-8-25X} \equiv -\frac{1}{8}\cdot(1 + (25/8)X) \bmod (X^2)\,.$$

We therefore have

$$Y_1 = Y_0 - \frac{f(Y_0)}{f'(Y_0)} = 1 - \frac{-4X}{-8+25X} = 1 - (1/2)X + O(X^2)$$

and sure enough $f(Y_1) = O(X^2)$. Continuing, we get

$$Y = 1 - (1/2)X + (29/16)X^2 - (1197/128)X^3 + (58993/1024)X^4 - (3203393/8192)X^5 + \cdots$$

or

$$y = \sqrt{x}(1 - (1/2)\sqrt{x} + (29/16)x - (1197/128)x^{3/2} + (58993/1024)x^2 - (3203393/8192)x^{5/2} + \cdots$$

Remark. There is no simple generalization of this Theorem when $\mathfrak{k}$ is a finite extension of $\mathbb{Q}_p$, and the algebraic closure of $\mathfrak{k}$ in that case is quite complicated. More curious is the case in which $\mathfrak{k}$ itself has characteristic $p > 0$. As Chevalley had already pointed out a while ago, $y^p - y - 1/x$ has no solution in fractional power series in x. [Kedlaya:1999], [Kedlaya:2001], and other papers referred to there tell the really remarkable story of how to fix things up in that case.

4. Puiseux expansions

In this section I'll sketch a proof of Theorem 3.1, along with a few related items. The proof will amount to a reasonably practical algorithm, under the assumption that one knows how to find and describe all roots of any polynomial in $\mathfrak{k}[x]$. Of course this an entirely unreasonable assumption, but I imagine one could find a substitute assumption that uses only factorization in $\mathfrak{k}[x]$ into irreducibles.

What is going to develop is by far simplest if one knows that $f(x, y) = 0$ has only simple roots. If

$$f(x,y) = \prod\nolimits_i (y - \alpha_i(x))^{m_i}$$

and some $m_i > 1$, then the gcd $g(x, y)$ of $f(x, y)$ and $\partial f(x, y)/\partial y$ will have $y - \alpha_i(x)$ as common factor, and in particular $g(x, y)$ will be a non-trivial polynomial in y. But in any case the quotient $f(x, y)/g(x, y)$ will always have the same roots as $f(x, y)$, and they will be simple. So *from now on I assume that $f(x, y) = 0$ has only simple roots.*

The example in the previous section is too simple to indicate what problems can arise. For a general equation $P(x, y) = 0$ it is true that all solutions can be expanded in formal fractional power series in some $\mathfrak{k}[[x^{1/n}]]$, but it may not be apparent at first what n is. Finding the common denominator in the expansion may take several iterations of a relatively simple process. As in Newton's example, the point of the iterations is to reduce the problem to one in which Hensel's Lemma can be applied.

I am going to describe an algorithm with input a polynomial $f(x, y)$ in $\mathfrak{k}[x, y]$ and output amounting to a list of all of its roots, specified in a very particular way. Each root, if described completely, will be an infinite formal power series

(4.1) $$y = c_1x^{\gamma_1} + c_2x^{\gamma_2} + c_3x^{\gamma_3} + \cdots$$

in which the $c_i \neq 0$ are complex numbers, and the γ_i are rational numbers such that

$$\gamma_1 < \gamma_2 < \gamma_3 < \quad \ldots \quad .$$

Of course it is impractical to specify the series completely. The algorithm will tell how to compute the terms in the series, inductively, one by one. Let

$$\lambda_1 = \gamma_1, \quad \lambda_i = \gamma_i - \gamma_{i-1} \ (i \geq 2) .$$

And let

$$\begin{aligned} y_N &= c_1 x^{\gamma_1} + c_2 x^{\gamma_2} + \cdots + c_N x^{\gamma_N} \\ w_N &= x^{\lambda_N}(c_N + x^{\lambda_{N+1}} c_{N+1} + \cdots) \end{aligned}$$

so that

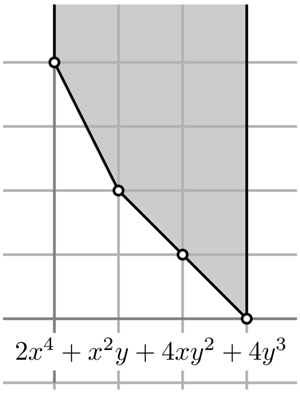
$$\begin{aligned} w_1 &= y \\ y &= y_N + x^{\gamma_N} w_{N+1} \\ w_N &= x^{\lambda_N}(c_N + w_{N+1}) . \end{aligned}$$

The algorithm will amount to a series of steps. In each step, we start with the equation satisfied by w_N. Then the possible values of λ_N are determined from the slopes of the Newton polygon of the equation, the possible values of c_N for each slope are determined by examining the homogeneous equation associated to that slope, and then the equation satisfied by w_{N+1} is derived. At that point, we do the next step.

Before I try to explain the general algorithm, I'll look at another example, one that should make things somewhat clearer. (I take it from [Didier et al.:2008], although how I deal with it will differ from how they do.) Let

$$P(x) = 4y^3 + 4xy^2 + x^2y + 2x^4 .$$

Its Newton polygon looks like this:



According to Theorem 2.1, its roots have orders 2, 1, 1. What are the corresponding power series solutions?

(a) Let's look first for the solution of order 2. That is to say, in the format of (4.1) its leading term is of the form c_1x^2.

Following Newton, we look first at the terms of the equation whose vertices lies on the edge from $(0, 4)$ to $(1, 2)$:

$$x^2y + 2x^4 = 0 .$$

This is homogeneous of degree 4, if we assign y weight 2. If we divide this by x^4 we get the homogeneous equation of degree 0

$$\frac{y}{x^2} + 2 = 0 .$$

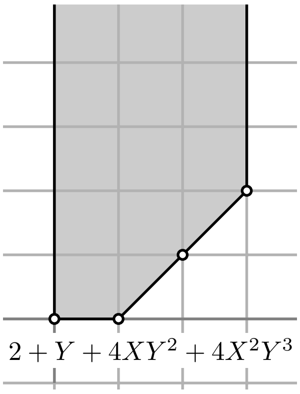
If we divide the whole equation by x^4 to get

$$4\,\frac{y^3}{x^4} + 4\,\frac{y^2}{x^3} + \frac{y}{x^2} + 2 = 4x^2\,\frac{y^3}{x^6} + 4x\,\frac{y^2}{x^4} + \frac{y}{x^2} + 2 == 0$$

If we set $Y = y/x^2$, $X = x$ this becomes

$$F(X,Y) = 4X^2Y^3 + 4XY^2 + Y + 2 = 0\,.$$

Its Newton polygon is this:



In other words, I have **flattened** the edge under consideration in the original Newton polygon. The new Newton polygon is strictly decreasing at the left of the flat segment (which is vacant in this example), strictly increasing to its right.

Its reduction modulo (X) is $Y + 2 = 0$. The root $Y = -2$ has multiplicity one. In the end, we get a solution

$$y = x^2\,Y(x) = x^2(-2 + w_1)$$

in which $Y = -2 + w$ is a series in x with $Y(0) = -2$ satisfying

$$F(X,Y) = 4x^2Y^3 + 4xY^2 + Y + 2 = 0\,,$$

which we can solve by applying Hensel's Lemma.

(b) Now we look at the edge from $(1,2)$ to $(3,0)$, lying on the line with slope -1 and y-intercept $(0,3)$. The corresponding homogeneous subexpression is

$$4y^3 + 4xy^2 + x^2y\,.$$

It is homogeneous of weighted degree 3, since the line passing through the nodes under consideration is $j + i = 3$. We therefore divide the original equation by x^3, getting

$$4\,\frac{y^3}{x^3} + 4\,\frac{y^2}{x^2} + \frac{y}{x} + 2x = 0\,,$$

or, setting $Y = y/x$, $X = x$:

(4.2) $$F(X,Y) = 4Y^3 + 4Y^2 + Y + 2X = 0\,.$$

The reduced equation is

$$4Y^3 + 4Y^2 + Y = 0$$

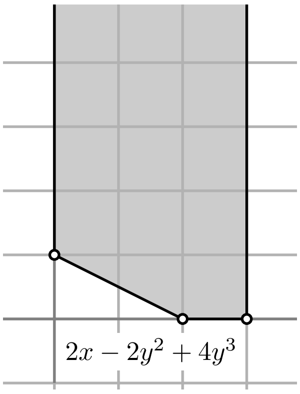
with solutions $Y = 0, -1/2, -1/2$. We can ignore the root 0 because we are now looking for a solution whose constant term does not vanish. It is in effect a shadow of the first solution we have found. So we are now looking at a root $-1/2$ of multiplicity 2. Because it has multiplicity 2, we cannot apply Hensel's Lemma. All we know is that we are looking for a pair of solutions of the form

$$Y = -1/2 + y_1 \quad (y_1 = o(1))$$

in which y_1 is a fractional power series of order more than 0. We substitute this expression for Y into (4.2) to derive an equation for y_1. This gives us the equation

$$2x_1 - 2y_1^2 + 4y_1^3 = 0\,.$$

Its Newton polygon is



We require that $y_1 = o(1)$, so we ignore the last segment. The homogeneous equation for the first segment is

$$2y_1^2 - 2x_1 = 0$$

with y-intercept 1, so we divide the (new) original equation by x to get

$$2 - 2\,\frac{y_1^2}{x} + 4\,\frac{y_1^3}{x} = 2 - 2\,\frac{y_1^2}{x} + 4x^{1/2}\,\frac{y_1^3}{x^{3/2}} = 2 - 2Y_1^2 + 4x_1Y_1^3 \quad (Y_1 = y_1/\sqrt{x}, x_1 = \sqrt{x})\,.$$

Now we can apply Hensel's Lemma. It gives us two solutions corresponding to the two roots ±1 of the reduced equation, leading finally to solutions of the original equation:

$$y = x(-1/2 + \sqrt{x}\,Y(x_1)) = x(-1/2 + \sqrt{x}(-1 + w_3)\,,$$

with $Y(x_1)$ a power series in $x_1 = \sqrt{x}$, such that $Y(0) = \pm 1$, satisfying the equation

$$2 - 2Y^2 + 4x_1Y^3 = 0\,.$$

With examples in view, I can now describe the general algorithm. The ultimate goal is to find all of its solutions, in the form of fractional power series

$$y = c_1x^{\lambda_1} + c_2x^{\lambda_1+\lambda_2} + c_3x^{\lambda_1+\lambda_2+\lambda_3} + \cdots \tag{4.3}$$

with all $c_i \neq 0$, all rational numbers $\lambda_i > 0$. Of course we cannot expect to find a formula for all terms, but we shall instead describe an algorithm for finding, in principle, arbitrarily many. This algorithm takes place in stages, in each of which another term in (4.3) is determined.

One point that causes some difficulty, as we have seen already in the last example, is that different solutions can start out with the same initial terms. Nonetheless, since we have arranged things so that $f(x,y)=0$ has only simple roots, sooner or later solution series will diverge.

At the start of each stage, we are given a polynomial $f(x,y)$, and we wish to find $c\neq 0$, $\lambda>0$ such that $y=cx^\lambda$ is an approximate root. Suppose that

$$f(x,y)=\sum c_{i,j}x^jy^i\,.$$

Since we want $\lambda>0$, we consider one by one the edges of its Newton polygon that have a negative slope. Suppose that the edge we are consiering lies in the line $\beta+\lambda\alpha=\mu$. Here μ is the β-intercept of the line, and $\lambda=k/\ell$ with k, ℓ relatively prime. Thus for all monomials x^jy^i we have

$$j+(k/\ell)i\geq\mu,\quad \text{or}\ j\ell+ki\geq\ell\mu\,,$$

and on the edge

$$j+(k/\ell)i=\mu\,.$$

We now divide the original equation by x^μ. This determines a new equation

$$\sum c_{i,j}x^{j-\mu}y^i==\sum c_{i,j}x^{j+(k/\ell)i-\mu}y^i/x^{(k/\ell)i}=0\,.$$

We now introduce new variables

$$x_*=x^{1/\ell},\quad Y=y/x^\lambda=y/x_*^k\,.$$

The equation becomes

$$f(x,y)=x^\mu\Big(\sum c_{i,j}X^{j\ell+ki-\mu\ell}Y^i\Big)=0\,.$$

Because the line $\beta+\lambda\alpha=\mu$ lies weakly below all nodes (i,j), the exponent of X is always a non-negative integer. It vanishes along the line itself, and the corresponding terms therefore give rise to an equation with constant coefficients—i.e. homogeneous of degree 0. This is the reduction of the new equation modulo (X). If c is a root of multiplicity one, we are in a situation in which Hensel's Lemma is applicable. Otherwise, we set $Y=c+y_*$ with $y_*=o(1)$ and find the equation $f_*(x_*,y_*)=0$ satisfied by y_* (subject to $y_*=o(1)$). The algorithm now loops with f_* replacing f. At the start we have

$$f(x,0)=O(x^\mu)$$

and at the end we have

$$f(x,cx^\lambda)=O(x^{\mu+1/\ell})\,.$$

Things therefore improve in each loop through this step, and it follows that in the end we have a true root if only we know:

4.4. Lemma. *Eventually* $\ell=1$.

Proof. We have to consider more carefully what is changing as the algorithm proceeds. When we start one of these steps, we are looking at the strictly decreasing part of the Newton polygon of a polynomial of degree n, and then we consider in turn each of several edges with distinct slopes. I call the **admissible span** of the polygon the with of its decreasing part, and the **span** of an edge is its width. The span of one of the edges we are looking at is at most the admissible span of the polygon.

After flattening, we are looking at an equation

$$Y^r(Y-c)^m\Phi(Y)+x_*R(x_*,Y)=0\,.$$

Here r is the left coordinate of the flat segment, and its right hand end is the sum of r, m, and the degree–say d—of $\Phi(Y)$. The sum $m+d$ is at most the admissible span of the polygon before flattening.

In the next phase, we set $Y = c + y_*$, getting a new equation for y_*:

$$(c + y_*)^r y_*^m \Phi(c + y_*) + x_* R(x_*, c + y_*) \, .$$

Its Newton polygon first touches the x_*-axis at $(m, 0)$, so its admissible span is exactly m. *The admissible span of the new Newton polygon is strictly less than what we started with, unless the edge under consideration has span m, in which acse it remains the same.*

In particular, the admissible span does not increase, and any chain of stpes must result in an infinite sequence of constant values, say L, of the admissible span. At each step the polynomial $F(0, Y)$ has a single root of multiplicity L. In this chain, the Newton polygon will always be a single edge of width L.

The single edge will intersect the lattice $\mathbb{Z}^2$ is a number of points with horizontal spacing δ, so that we can factor $L = \Lambda\delta$. The 'constant' polynomial $F(0, Y)$ appearing in the loop will be a polynomial in Y^δ:

$$F(0, Y) = \Phi(Y^\delta) \, .$$

We can factor Φ into linear factors $Z - d$, and then

$$F(0, Y) = \prod (Y^\delta - d) \, .$$

But if $\delta > 1$ this will give a smaller span in the next loop. Hence $\delta = 1$. Thus the left hand vertex of the Newton polygon is some multiple of L, and hence ℓ is always 1 from some point on.

Furthermore, L must also be eventually 1, or we would have roots of the original equation that are not simple. Hence:

4.5. Lemma. *Eventually we arrive at an equation to which we can apply Hensel's Lemma.*

You can continue looping in this way as long as you wish, at least in principale, but in practice you can speed things up slightly by following the method demostrated earlier when Hensel's Lemma becomes applicable. It hence makes sense to have as output of the algorithm a list of the solutions as initial series together with Hensel data characterizing subsequent computation.

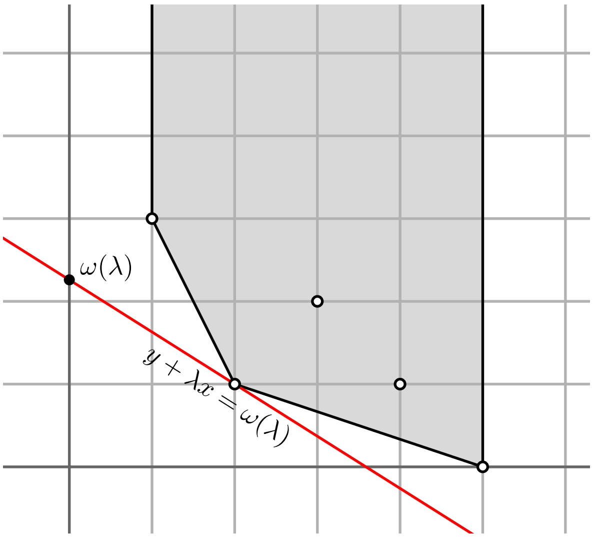
5. Duality

In this section I follow closely the Appendix of [Lubin:2013].

If Ω is any closed convex region in $\mathbb{R}^2$, its dual Ω^* is the set of all (a, b, c) in $\mathbb{R}^3$ such that $ax + by + c \geq 0$ on Ω. It is a convex cone. The region Ω then consists of all (x, y) such that $ax + by + c \geq 0$ for all (a, b, c) in Ω^*.

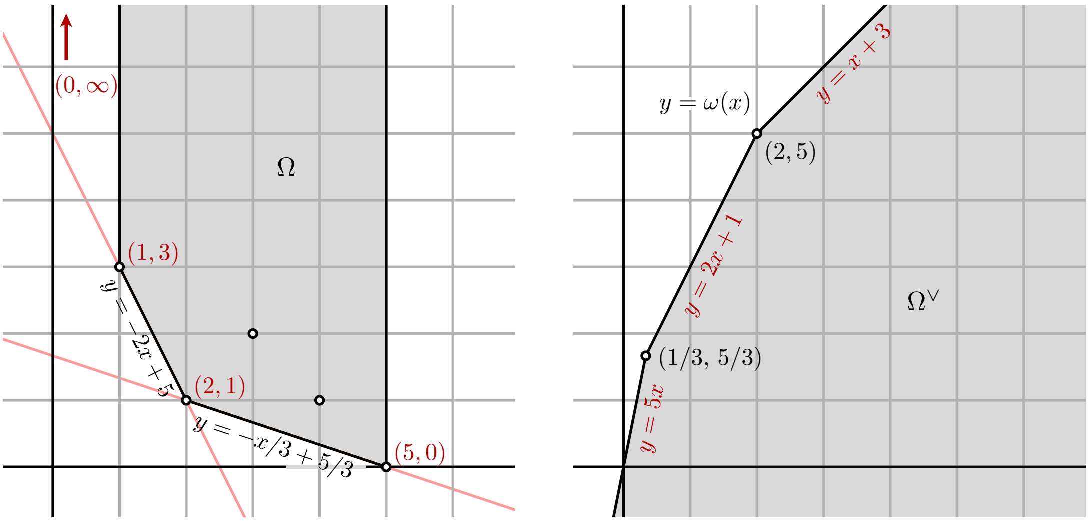
For us, the region Ω will be $\mathcal{C}_P$, and in this case a slight variation will be convenient. To the set $\mathcal{C}_P$ is associated the set $\mathcal{C}_P^\vee$ of all (λ, c) with the property that $\mathcal{C}_P$ is contained in the region $y + \lambda x - c \geq 0$. It is a essentially a slice through the three-dimensional dual, taking into account a change in sign, and it is also convex. It is not closed, because it won't contain any functions of x alone.

The region $\mathcal{C}_P$ is taken into itself by a vertical upwards shift, and consequently $\mathcal{C}_P^\vee$ is taken into itself by a vertical shift downwards. There exists for each λ a maximum value of c such that (λ, c) lies in $\mathcal{C}_P^\vee$, since some shift upwards of a line with finite slope will eventually intersect $\mathcal{C}_P$. Define $\omega_P(\lambda)$ to be that value of c. It is also the minimum value of $y + \lambda x$ on $\mathcal{C}_P$, and the y-intercept of that highest line.



5.1. Theorem. *The set $\mathcal{C}_P^\vee$ is the same as the set of points lying on or below the graph of $\omega(\lambda)$.*

Vertices of $\mathcal{C}_P$ correspond to bounding lines in the dual figure, and vice-versa. In figures, with $P(x) = x^5 - px^4 + p^2x^3 + p^3x$:



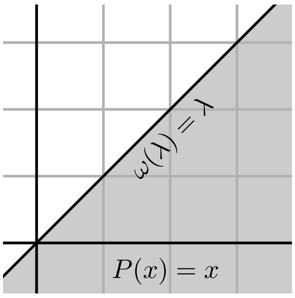
In these figures, one encounters in $\mathcal{C}_P$ the lines $y = -x/3 + 5/3$, $y = -2x + 5$ reading right to left, and in $\mathcal{C}_P^\vee$ the vertices $(1/3, 5/3)$, $(2, 5)$, reading left to right.

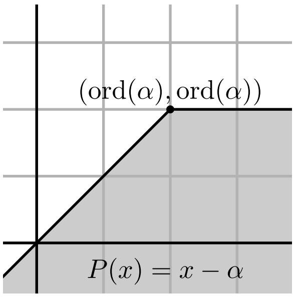
Here are some basic examples:

5.2. Lemma. *(a) If $P(x) = x$ then $\omega_P(\lambda) = \lambda$ for all λ. (b) If $P(x) = x - \alpha$ with $\alpha \neq 0$, then*

$$\omega_P(\lambda) = \begin{cases} \lambda & \text{if } \lambda \le \operatorname{ord}(\alpha) \\ \operatorname{ord}(\alpha) & \text{otherwise.} \end{cases}$$

In figures:





I put into one package a number of important facts about the dual polygons:

5.3. Theorem. *Suppose P, Q to be in $\overline{\mathfrak{k}}[[x]]$.*

(a) If $\mathrm{ord}\,(x)$ is unexceptional for P, then

$$\mathrm{ord}\,(P(x)) = \omega_P(\mathrm{ord}\,(x))\,.$$

(b) If P and Q are two polynomials in $\overline{\mathfrak{k}}[X]$, then $\omega_{PQ} = \omega_P + \omega_Q$.
(c) If $P(0) = 0$, the function ω_P is an invertible piece-wise linear map from $[0, \infty)$ to itself.
(d) The function ω is linear between exceptional values, and if λ is unexceptional then its slope is equal to the number of roots α of P with $\mathrm{ord}\,(\alpha) \geq \lambda$.
(e) Suppose $Q(0) = 0$. Then

$$\omega_{P \circ Q} = \omega_P \circ \omega_Q\,.$$

Note that (a) determines completely the function ω_P, since it is continuous.

Proof. Item (a) is just a reformulation of .

Item (b) follows from (a).

Item (c) follows from the interpretation of $\omega(\lambda)$ as y-intercept.

Item (d) follows from (b) and Lemma 5.2.

Only item (e) requires a bit of work, but follows without too much trouble from (a).

Part II. Power series

6. The Weierstrass preparation theorem

The material in this section is well known. I have found §4.2 of [Castillo:2008] particularly clear.

Let $x \mapsto \overline{x}$ be the ring homomorphism from $\mathfrak{o}$ to $\mathfrak{o}/\mathfrak{p}$. A series

$$f(T) = f_0 + f_1 T + f_2 T^2 + \cdots$$

in $\mathfrak{o}[[T]]$ will be called here **admissible** if one of its coefficients is a unit in $\mathfrak{o}$.

6.1. Lemma. (Weierstrass division) *Suppose f, g in $\mathfrak{o}[[T]]$ with f admissible. Let n be least such that $f_n \in \mathfrak{o}^\times$. There exist q in $\mathfrak{o}[[T]]$ and r in $\mathfrak{o}[T]$ of degree $< n$ such that*

$$g = fq + r\,.$$

Proof. I shall exhibit an algorithm computing successively a series q_n and a polynomial r_n such that

$$\begin{aligned} g &\equiv f q_n + r_n \text{ modulo } \mathfrak{p}^{n+1} \\ q_{n+1} &\equiv q_n \text{ modulo } \mathfrak{p}^{n+1} \\ r_{n+1} &\equiv r_n \text{ modulo } \mathfrak{p}^{n+1} . \end{aligned}$$

INITIALIZATION. What are the initial q_0 and r_0? Because of the definition of n, we can write

$$f = \rho + T^n \sigma$$

with ρ a polynomial of degree $< n$ whose reduction modulo $\mathfrak{p}$ vanishes, and σ in $\mathfrak{o}[[T]]^\times$. Reducing modulo $\mathfrak{p}$ we now have

$$\overline{f} = T^n \overline{\sigma} .$$

Since σ is a unit in $\mathfrak{o}[[T]]$ it is invertible, so also have

$$T^n = \overline{f}\,\overline{\sigma}^{-1} .$$

We can also write

$$g = r_0 + T^n s_0$$

with r_0 a polynomial of degree $< n$ and s_0 in $\mathfrak{o}[[T]]$. But then

$$\begin{aligned} \overline{g} &= \overline{r}_0 + T^n\,\overline{s}_0 \\ &= \overline{r}_0 + \overline{f}\cdot\overline{\sigma}^{-1}\overline{s}_0 \\ &= \overline{r}_0 + \overline{f}\cdot\overline{q}_0 \quad (q_0 = \sigma^{-1} s_0) \end{aligned}$$

or

$$g = f\cdot q_0 + r_0 + \varpi g_1, \quad g_1 = \frac{g - f\cdot q_0 - r_0}{\varpi} .$$

INDUCTION. Now proceed by induction, applying the same process to each get in turn

$$\begin{aligned} g_n \quad &= r_n + T^n s_n \\ q_{n+1} &= \overline{\sigma}^{-1} s_n \\ g_{n+1} &= \frac{g_n - f\cdot q_n - r_n}{\varpi} \end{aligned}$$

with

$$g = (r_0 + r_1\varpi + \cdots + r_n\varpi^n) + f(q_0 + q_1\varpi + \cdots + q_n\varpi^n) + \varpi^{n+1} g_{n+1}$$

at each stage. ∎

A polynomial $P(X)$ in $\mathfrak{o}[X]$ is said to be **distinguished** if it is monic, say of degree n, and the coefficients of $P(X) - X^n$ lie in $\mathfrak{p}$.

6.2. Proposition. (Weierstrass preparation theorem) *Suppose f to be admissible in $\mathfrak{o}[[X[[$, and let n be the least n such that f_n is in $\mathfrak{o}^\times$. There exist a unique distinguished polynomial $P(X)$ of degree n and g in $\mathfrak{k}[[X]]^\times$ such that $f = P\cdot g$.*

Proof. Apply the previous Lemma to f and $g = T^n$, giving

$$T^n = f\cdot q + r$$

with r a polynomial of degree $< n$. Reducing modulo $\mathfrak{p}$ we see that

$$\overline{r} = T^n - \overline{q}\overline{f}\,.$$

But by hypothesis $\overline{f}$ is divisible by T^n, so $\overline{r}$ is also divisible by T^n. Hence $\overline{r} \equiv 0$, and r is divisible by ϖ. Set

$$P = T^n - r\,.$$

Since $T^n = \overline{f}\overline{q}$, q lies in $\mathfrak{o}[[T]]^\times$. The polynomial P is distinguished, and

$$f = P \cdot q \qquad \blacksquare$$

This already an interesting result even if f is a polynomial. It then factors f into a polynomial all of whose roots α agree with those of f that satisfy $|\alpha| < 1$ and a series with no roots in that region.

Example. Let

$$f(T) = 1 + pT\,.$$

It is already a unit in $\mathfrak{o}[[T]]$, so $P = 1$, $g = f$.

Example. Let

$$f(T) = p - (1 + p^2)T + pT^2 = (T - p)(pT - 1)\,.$$

here $P = T - p$ and $g = -1 + pT$.

Example. Let

$$f(T) = p - T + pT^2\,.$$

This has the same Newton polygon as the last example, but the Weierstrass factorization is not simple. We can solve for the roots according to the formula

$$\alpha = \frac{1 \pm \sqrt{1 - 4p^2}}{2p}\,.$$

The square roots converges in $\mathbb{Z}_p$ since it can be written in terms of the binomial series (also due to Newton!) as

$$(1 - 4p^2)^\gamma = 1 - \gamma \cdot (4p^2) + \frac{\gamma(\gamma - 1)}{2} \cdot (4p^2)^2 - \cdots\,.$$

with $\gamma = 1/2$.

One of the roots, say α, is integral. The other is $\beta = 1/\alpha$. The explicit formula in this case will tell us that $\operatorname{ord}(\alpha) = 1$, and that $p\beta$ is a unit. We now have the Weierstrass factorization

$$f(T) = p(T - \alpha)(T - \beta) = (T - \alpha)(pT - p\beta)\,.$$

7. Newton polygons of power series

If $f(T)$ is a power series in $\mathfrak{o}[[T]]$ and x is in $\overline{\mathfrak{k}}$ with $\operatorname{ord}(x) > 0$, then $f(x)$ converges. It therefore makes sense to refer to the roots α of f with $|\alpha| < 1$. If f has the Weierstrass factorization $f = P \cdot g$, then those roots agree with the roots of P. One can define the Newton polygon of f in the usual way, but if one is interested in only the roots α with $|\alpha| < 1$, it also seems reasonable to define a variant of the Newton polygon in which only those roots appear. This is exactly what [Lubin:2013] does. He defines the Newton polygon of an admissible power series to be given by the monotonically decreasing part of what might be called the 'normal' Newton polygon, together with the horizontal line tacked on at the end. Thus if n is the least n such that f_n is a unit, the Newton polygon will have a horizontal line from $(n, 0)$ off to ∞. Up to the point $(n, 0)$ this will agree with the Newton polygon of P.

Similarly, the dual polygon will be the top of the dual of the new Newton polygon. It will be the same as the old one in the positive quadrant, but will now be bounded on the left by the ray from $(0, 0)$ to $(0, -\infty)$. This is the dual polygon illustrated in Lubin's paper.

The main result along these lines is that Theorem 5.3 holds as well if the polynomials are replaced by the series introduced here.

I include here a simple application of these ideas to the arithmetic of algebraic extensiuons. Suppose $\mathfrak{l}/\mathfrak{k}$ to be a totally ramified separable extension, $\varpi_{\mathfrak{l}}$ and $\varpi_{\mathfrak{k}}$ prime ideal generators. We may write

$$\varpi_{\mathfrak{k}} = \sum_{m=e} c_m \varpi_{\mathfrak{l}}^m$$

with c_e a unit in $\mathfrak{o}_{\mathfrak{k}}$. (One may even choose the c_m to be Teichmüller representatives.) Let

$$f(x) = \sum_{m=e} c_m x^m \, .$$

Weiersrass' preparation theorem allows to write

$$f(x) - \varpi_{\mathfrak{k}} = P(x) \cdot u(x)$$

in which $P(x)$ is a monic polynomial of degree e, $u(x)$ an invertible power series in $\mathfrak{o}[[x]]$.

7.1. Proposition. *In these circumstances, the polynomial P is the irreducible polynomial over $\mathfrak{k}$ whose root is $\varpi_{\mathfrak{l}}$.*

Part III. References

1. Hugo Castillo, 'Kubota-Leopoldt p-adic L-functions', Ph. D. thesis available at

`http://algant.eu/documents/theses/`

2. Claude Chevalley, **Introduction to the theory of algebraic functions of one variable**, American Mathematical Society, 1951.

3. Chris Christensen, 'Newton's method for recovering affected equations', *The College Mathematics Journal* **27** (1996), 330–340.

4. Michel Demazure, **Lectures on *p*-divisible groups**, *Lecture Notes in Mathematics* **332**, 1972.

5. Annie K. Didier, Kevin M. Sonnanburg, and Nicholas J. Willis, 'How to compute a Puiseux expansion', preprint dated 2008, avail at

`https://arxiv.org/abs/0807.4674`

6. Christian Greve and Sebastian Pauli, 'Ramification polygons, splitting fields, and Galois groups of Eisenstein polynomials', *International Journal of Number Theory* **8** (2012), 1401–1424.

7. Andrei Jorza, 'Newton polygons and factoring polynomials over local fields', preprint (undated) at https://wstein.org/129-05/section/m129-section-newton-polygons/newton_polygons.pdf

8. Kiran S. Kedlaya, ‘Power series and p-adic algebraic closures’, arXiv:9906030.

9. ——, ‘The algebraic closure of the power series field in positive characteristic’, *Proceedings of the American Mathematical Society* **12** (2001), 3461–3470.

10. ——, ‘Finite automata and algebraic extensions of function fields’, arXiv:math/0410375.

11. Jonathan Lubin, ‘Elementary analytic methods in higher ramification theory’, *Journal of Number Theory* **133** (2013), 983–999.

12. Jonathan Milstead, Sebastian Pauli, Brian Sinclair, ‘Constructing splitting fields of polynomials over local fields’, pp. 101-124 in [Rychtář et al.:2018].

13. Isaac Newton, letter from Newton to Oldenburg dated October 24, 1696, pp. 110–161 in **The Correspondence of Isaac Newton**, edited by H. W. Turnbull, Cambridge University Press, 1960.

14. David Romano, ‘Galois groups of strongly Eisenstein polynomials’, Ph. D. thesis, UC Berkeley, 2000.

15. Jan Rychtář, Maya Chhetri, Sat Gupta, Ratnasingham Shivaji (editors), **Collaborative Mathematics and Statistics Research** (Topics from the 9th Annual UNCG Regional Mathematics and Statistics Conference), in the series *Springer Proceedings in Mathematics & Statistics* **109**, Springer, 2018

16. Robert Walker, **Algebraic curves**, Princeton Press, 1950. Reissued by Dover Publications.