Newton Polygons and Factoring polynomials over Local Fields

Andrei Jorza

March 8, 2005

1 Generalities

Let K be a number field. We have seen that a finite place of K is a valuation $v : K \to \mathbb{Z} \cup \{\infty\}$ such that $v(xy) = v(x) + v(y), v(x + y) \geq \min(v(x), v(y))$ and $v(0) = \infty$. This defines the metric $|x|_v = q_v^{-v(x)}$ where $q_v = \#k_v$ the size of the residue field $k_v = \mathcal{O}_v/\wp_v$. Here K_v is the completion of K at v, $\mathcal{O}_v$ is the ring of integers of K_v and $\wp_v$ is the maximal ideal of the local ring $\mathcal{O}_v$.

Let v be a finite place. Let $f(x) \in K_v[x]$ be a polynomial $f(x) = f_0 + f_1x + \cdots + f_nx^n$. The Newton polygon $NP(f)$ is the lower convex hull of the points $\{(0, \infty), (n, \infty)\} \cup \{P_i = (i, v(f_i))|i = 0, 1, \ldots, n\}$. The $NP(f)$ is a polygonal like formed by two vertical lines together with a set of lines of various slopes.

Proposition 1.1. *Let f be a polynomial of degree n. If u is a root of f then there exists a segment in $NP(f)$ of slope equal to $-v(u)$.*

Proof. We have $f_0 + f_1u + \cdots + f_nu^n = 0$. If $\min v(f_iu^i)$ is uniquely attained, then the nonarchimedean property of v would imply that $v(f_0 + f_1u + \cdots + f_nu^n) = \min(v(f_iu^i)) = v(0) = \infty$ which cannot be. So $\exists i \neq j$ such that $v(f_iu^i) = v(f_ju^j)$. But this corresponds to the line of slope $-v(u)$ through P_i and P_j. The valuation $v(f_iu^i)$ is the place where this line intersects the vertical axis and the fact that this valuation is minimal implies that all the points on $NP(f)$ are on or above this line. So this line contains a segment of $NP(f)$ which proves the lemma. $\square$

Example 1.2. Let p be a prime number and let $f(x) = x^3 + px^2 + px + p^2 \in \mathbb{Q}_p[x]$. According to the theory this will have one root of valuation 1 and two roots of valuation 1/2.

Proposition 1.3. *Let $f, g \in K_v[x]$ be two polynomials ($f = f_0 + \cdots + f_dx^d, g = g_0 + \cdots + g_ex^e$) such that all the slopes of $NP(f)$ are less or equal to all the slopes of $NP(g)$. Then $NP(fg)$ is obtained by adjoining $NP(f)$ and $NP(g)$ in the following explicit manner (here we interpret*

$NP(f)$ as a piecewise linear function in x)

$$NP(fg)(x) = \begin{cases} NP(f)(x) + NP(g)(0), x \in [0, d] \\ NP(f)(d) + NP(g)(x-d), x \in [d, d+e] \end{cases}$$

Example 1.4. $f(x) = x^3 + px^2 + px + p^2, g(x) = px^2 + x + 1$ and

$$(fg)(x) = px^5 + (p^2+1)x^4 + (p^2+p+1)x^3 + px^2 + px + p^2.$$

Proof. $(fg)(x) = \sum_0^{d+e} h_i x^i$ where $h_i = \sum f_j g_{i-j}$. If $i \in [0, d]$ then

$$v(h_i) = v(g_0 f_i + \cdots + g_j f_{i-j} + \cdots)$$

and $v(g_0 f_i) = v(g_0) + v(f_i) \geq NP(g)(0) + NP(f)(i)$ with equality if $NP(f)(i) = v(f_i)$. For $j > 0$ we still have $v(g_j f_{i-j}) \geq NP(g)(j) + NP(f)(i-j) > NP(g)(0) + NP(f)(i)$ because of the slope condition ($\Longleftrightarrow NP(g)(j) - NP(g)(0) > NP(f)(i) - NP(f)(i-j)$). This takes care of the case $i \in [0, d]$.

Now assume that $i \in [d, d+e]$. Then $h_i = f_d g_{i-d} + \cdots + f_{d-j} g_{i+j-d} + \cdots$ and the proof is similar. □

2 Factorization

This is a very nice theorem since it tells you that you can compose Newton polygons when multiplying polynomials. Can we go the other way around? The answer is yes. But first we need a technical lemma:

Lemma 2.1. *Let $c \in \mathbb{R}$. Write $v_c(f) = \min(v(f_i) + ic)$. Then $v_c(fg) = v_c(f) + v_c(g), v_c(f+g) \geq \min(v_c(f), v_c(g))$.*

Proof. Let $v_c(f) = v(f_i) + ic, v_c(g) = v(g_j) + jc$. So $v_c(f) + v_c(g) = v(f_i g_j) + (i+j)c \leq v(\sum f_u g_{i+j-u}) + (i+j)c) \leq v_c(fg)$ because $v(h_i) \geq \min v(f_j) + v(g_{i-j})$. In the other direction, $v_c(fg) \leq v(h_{i+j}) + (i+j)c = v(\sum f_{i-k} g_{j+k}) + (i+j)c$. If $k \neq 0$ then $v(f_{i-k} g_{j+k}) + (i+j)c > v_c(f) + v_c(g)$ by choice of i and j. So $v(\sum f_{i-k} g_{j+k}) + (i+j)c = v(f_i g_j) + (i+j)c = v_c(f) + v_c(g)$. □

Lemma 2.2. *This essentially bounds the quantities in the division with remainder. Let $f, h \in K_v[x]$ with $\deg f = d$ and $v_c(f) = v(f_d) + dc$. Write $h = qf + r$ division with remainder. Then $v_c(q) \geq v_c(h) - v_c(f)$ which in turn implies that $v_c(r) \geq v_c(h)$.*

Proof. If h has degree n and let $\deg f = d$; write $q = q_0 + \cdots + q_{n-d} x^{n-d}$. If we show by induction on i that $v_c(q_{n-d-i} x^{n-d-i}) \geq v_c(h) - v_c(f)$ then we are done.

For each $i \leq n-d$ there is no contribution from r in the formula for h_{n-i} so $h_{n-i}x^{n-i} = f_d q_{n-d-i} x^{n-i} + f_{d-1} q_{n-d-i+1} x^{n-i} + \cdots$.

Note that $v_c(f_d q_{n-d-i} x^{n-i}) = v_c(f) + v_c(q_{n-d-i} x^{n-i-d})$ by the hypothesis on f. Also, from the inductive hypothesis we get that $v_c(q_{n-d-(i-j)} x^{n-d-(i-j)}) \geq v_c(h) - v_c(f)$ which implies that $v_c(f_{d-j} q_{n-d-i+j} x^{n-i}) \geq v_c(h)$. So

$$v_c(f_d q_{n-d-i} x^{n-i}) = v_c(h_{n-i} x^{n-i} - \sum_{j>0} f_{d-j} q_{n-d-i+j} x^{n-i}) \geq v_c(H),$$

which implies the result for i given the result for $i-j$ for $j>0$.

Now $v_c(r) = v_c(h - fq) \geq \min(v_c(h), v_c(f) + v_c(q)) = v_c(h)$.

$\square$

The reason why this technical lemma is important is that it gives an algorithmic way to approximate factorizations of polynomials.

Theorem 2.3. *Let $h \in K_v[x]$ be a polynomial of degree $d+e$ and let d be a point of discontinuity in $NP(h)$. We saw in Proposition 1.3 that such Newton polygons arise when h is the product of a polynomial of degree d and one of degree e. This theorem states that each h arise in such manner.*

Proof. As mentioned, the prood will be algorithmic. Let $f_0 = h_0 + \cdots h_d x^d$, the first d terms in the expansion of h and let $g_0 = 1$. Choose c such that $v_c(h) = v_c(h_d x^d)$ and such that d is the smallest index with this property ($v_c(h) \neq v_c(h_i x^i), i > d$).

Now $v_c(h - f_0 g_0) = \varepsilon > 0$ and $v_c(f_0) = v_c(h)$. We'll construct f_i, g_i such that $\deg f_i = d, \deg g_i \leq n-d$, $v_c(f_i) = v_c(h)$, $v_c(f_i - f_{i+1}) \geq v_c(h) + i\varepsilon$, $v_c(g_i - g_{i-1}) \geq i\varepsilon$ and finally $v_c(h - f_i g_i) \geq v_c(h) + (i+1)\varepsilon$. Clearly this implies that $f_i \to f, g_i \to g, f_i g_i \to fg, h$ so $h = fg$.

Write $h - f_i g_i = q f_i + r$, division with remainder. Take $f_{i+1} = f_i + r, g_{i+1} = g_i + q$. Let's show that the conditions are satisfied. The conditions on the degrees are clearly satisfied.

Now $v_c(f_{i+1} - f_i) = v_c(r) \geq v_c(h - f_i g_i)$ and $v_c(g_{i+1} - g_i) = v_c(q) \geq v_c(h - f_i g_i) - v_c(f_i)$ by Lemma 2.2. In particular this shows that $v_c(f_{i+1}) = v_c(f_i) = v_c(h)$.

By the inductive hypothesis we have $v_c(h - f_i g_i) \geq v_c(h) + (i+1)\varepsilon$ so we have $v_c(r) \geq v_c(h) + (i+1)\varepsilon$ which implies that $v_c(f_{i+1} - f_i) \geq v_c(h) + (i+1)\varepsilon$, the first condition. Also $v_c(q) \geq v_c(h) + (i+1)\varepsilon - v_c(f_i) = (i+1)\varepsilon$ and so $v_c(g_{i+1} - g_i) \geq (i+1)\varepsilon$.

Lastly, $v_c(h - (f_i + r)(g_i + q)) = v_c(h - f_i g_i - f_i q - r g_i - rq) = v_c(r - r g_i - rq) = v_c(r) + v_c(1 - g_i - q)$ but this is $\geq v_c(h) + (i+1)\varepsilon + \min(v_c(1 - g_i), v_c(q))$. The condition on g_i implies that $v_c(1 - g_i) \geq \varepsilon$ and $v_c(q) \geq (i+1)\varepsilon$. So we get what we want. $\square$

Problem 2.4. Let $f \in K_v[x]$ such that $NP(f)$ consists of one segment that contains no other lattice points. Then f is irreducible.

Proof. Assume it is reducible. Then $f = gh$ and each roots of g, h has to have the same valuation as f so the NP of g and h have the same slope as that of f. But then we can put $NP(g)$ at the top of $NP(f)$ and we get a lattice point on $NP(f)$. So f is irreducible. $\square$

Problem 2.5. Factor the following polynomials $x^3 + 5x + 25, x^3 + 5x^2 + 25 \in \mathbb{Q}_5[x]$.

3 Galois Groups

Let L_w/K_v be a Galois extension.

Lemma 3.1. *Let $\alpha, \beta \in L_w$ such that $v(\beta - \sigma\alpha) < v(\sigma\alpha - \alpha)$ for any $\sigma \in \mathrm{Gal}(L_w/K_v) \setminus \mathrm{Gal}(L_w/K_v(\alpha))$. Prove that $\alpha \in K_v(\beta)$.*

Proof. Let $\sigma \in \mathrm{Gal}(L_w/K_v(\beta))$. We want to show that $\sigma\alpha = \alpha$ which is enough to prove the lemma. Assume that $\sigma\alpha \neq \alpha$ so $v(\alpha - \sigma\alpha) > v(\beta - \sigma\alpha) = v(\sigma(\beta - \alpha)) = v(\beta - \alpha) = v(\beta - \sigma\alpha + \sigma\alpha - \alpha) \geq \min(v(\beta - \sigma\alpha), v(\alpha - \sigma\alpha)) = v(\alpha - \sigma\alpha)$ which is a contradiction. $\square$

Theorem 3.2 (Krasner). *Let $f \in K_v[x]$ be a monic irreducible polynomial of degree d. Let $x_1, \ldots, x_d$ be the roots of f and let $\varepsilon = \max_{i \neq j} v(x_i - x_j)/2$ and let $C = \max(d\varepsilon, v(f_i))$. Assume that g is a polynomial of degree d in $K_v[x]$ such that $v_0(f - g) > C$. Then g is irreducible and $K_v[x]/(f) \cong K_v[x]/(g)$. (This essentially says that the two Galois groups are equal.)*

Proof. Since $C > v(f_i)$ the Newton polygon says that $f \cong g \pmod{p_v}$ so if g factors by Hensel's lemma f factors. (I won't prove Hensel's lemma here.) So assume g is irreducible.

Let $y_1, \ldots, y_d$ be the roots of g. By dimension count enough to show that $y_i \in K_v(x_j)$. For this it is enough by Lemma 3.1 to show that there exist i and j such that for all k we have $v(y_i - x_j) > v(x_k - x_j)$, for then $v(y_i - x_j) > v(x_k - x_j) \geq \min(v(x_k - y_i), v(y_i - x_j)) = v(x_k - y_i)$ which gives the result.

Now, $v(f(y_j)) = v(f(y_j) - g(y_j)) = v(\sum(f_i - g_i)y_j^i) = \lambda = \begin{cases} C \\ C + nv(y_j) \end{cases}$. But here the polynomials are monic so $v(y_i) \geq 0$ so $C \leq v(f(y_j)) = v(\prod(y_j - x_k)) = \sum v(y_i - x_k)$. For at least one k we have $v(y_j - x_k) \geq C/d > \varepsilon$ so the hypotheses are satisfied. $\square$

Example 3.3. Let $K/\mathbb{Q}_3$ be the extension defined by the polynomial $f(x) = x^4 - 10x^2 + 27x + 1$. Find $\mathrm{Gal}(K/\mathbb{Q}_3)$.

Proof. The idea is that $g(x) = x^4 - 10x^2 + 1$ has roots $\pm\sqrt{2} + \pm\sqrt{3}$ so the Galois group of g is $(\mathbb{Z}/2\mathbb{Z})^2$.

So now all we need is that f and g satisfy the hypotheses of Theorem 3.2.

We start out with g instead of f. Would like to have $C = v_0(f - g) = 3$. Then $C > v(g_i) = 0$ so the only inequality we want to check is that $C > 4\varepsilon$. But $\varepsilon = 1/2$ so the hypotheses are satisfied. $\square$