(*February 19, 2005*)

Newton polygons

Paul Garrett garrett@math.umn.edu http://www.math.umn.edu/˜garrett/

Let k be the field of fractions of a discrete valuation ring $\mathbf{o}$, with *ord*-function ord, and suppose that $\mathbf{o}$ and k are *complete*. Let

$$f(x) = x^n + c_{n-1}x^{n-1} + \ldots + c_2x^2 + c_1x + c_0$$

be in $k[x]$. Consider piecewise-linear convex (bending upward) functions P on the interval $[0, n]$ such that for each integer i

$$P(i) \leq \text{ord } c_i$$

Let N be the *maximum* among these, and let $i_1 < \ldots < i_m$ be the integer indices such that we have *equality*

$$N(i_j) = \text{ord } c_{i+j}$$

The line segements

$$\ell_j = \text{ line segment connecting } N(i_j) \text{ and } N(i_{j+1})$$

form the **Newton polygon** attached to f.

Theorem: Suppose that the roots of f generate a separable extension of k. Let m_j be the negative of the slope of ℓ_j, and let p_j be the length of the projection of ℓ_j to the horizontal axis. Then there are exactly p_j roots of f in k_{sep} with ord equal to m_j.

Proof: Let $\nu_1 < \ldots < \nu_m$ be the distinct ords of the roots, and suppose that there are exactly μ_i roots with ord ν_i. Let σ_j be the j^{th} symmetric function of the roots, so $c_i = \pm\sigma_i$.

Let $\rho_1, \ldots, \rho_{\mu_1}$ be the roots with largest ord. Since

$$\sigma_{\mu_1} = \rho_1 \ldots \rho_{\mu_1} + (\text{other products})$$

where the other products of μ_1 factors have strictly smaller ords. By the ultrametric inequality,

$$\text{ord}(\sigma_{\mu_1}) = \text{ord}(\rho_1 \ldots \rho_{\mu_1}) = \mu_1\nu_1$$

Similarly, let $\tau_1, \ldots, \tau_{\mu_2}$ be the second-largest batch of roots, namely, roots with ord ν_2. Then

$$\sigma_{\mu_1+\mu_2} = \rho_1 \ldots \rho_{\mu_1}\tau_1 \ldots \tau_{\mu_2} + (\text{other products})$$

where all the other products have strictly smaller ord. Again by the ultrametric inequality

$$\text{ord}(\sigma_{\mu_1+\mu_2}) = \text{ord}(\rho_1 \ldots \rho_{\mu_1}\tau_1 \ldots \tau_{\mu_2}) = \mu_1\nu_1 + \mu_2\nu_2$$

Generally,

$$\text{ord}(\sigma_{\mu_1+\ldots+\mu_j}) = \mu_1\nu_1 + \ldots + \mu_j\nu_j$$

Therefore, the line segment connecting $N(n - \mu_1 - \ldots - \mu_j)$ and $N(n - \mu_1 - \ldots - \mu_{j+1})$ has slope $-\nu j + 1$ and the projecting to the horizontal axis has length μ_{j+1}.

On the other hand, for

$$\mu_1\nu_1 + \ldots + \mu_j\nu_j < M < \mu_1\nu_1 + \ldots + \mu_{j+1}\nu_{j+1}$$

by the ultrametric inequality

$$\text{ord}M \geq \min(\text{ord of products of } M \text{ roots}) = \mu_1\nu_1 + \ldots + \mu_j\nu_j + (M - \mu_1 - \ldots - \mu_j)\nu_{j+1}$$

That is, $N(n - M)$ lies on or above the line segment connecting the two points $N(n - \mu_1 - \ldots - \mu_j)$ and $N(n - \mu_1 - \ldots - \mu_{j+1})$. ///

Corollary: *(Irreducibility criterion)* Let f be monic of degree n over an ultrametric local field k as above. Suppose that the Newton polygon consists of a single line segment of slope $-a/n$ where a is relatively prime to n. Then f is irreducible in $k[x]$.

Proof: By the theorem, there are n roots of ord a/n. Since a is prime to n, the field $k(\alpha)$ generated over k by any one of these roots has ramification index divisible by n, by the following lemma, for example. But $[k(\alpha) : k] \leq n$, so the field extension degree is exactly n. ///

Lemma: Let α belong to the separable closure of the ultrametric field k, and suppose that $\text{ord}\alpha = a/n$ with a relatively prime to n. Then $k(\alpha)$ has ramification index divisible by n (and, thus n divides $[k(\alpha) : k]$).

Proof: Let ϖ be a local parameter in the extension $k(\alpha)$. Then

$$\text{ord}\varpi = \frac{1}{e}$$

where e is the ramification index of the extension. Since α differs by a unit from some integer power of ϖ,

$$\frac{a}{n} = \text{ord}\alpha \in \frac{1}{e} \cdot \mathbf{Z}$$

That is, $ea \in n\mathbf{Z}$. Since a is prime to n, it must be that n divides e, which divides the field extension degree in general. ///

Corollary: *(Eisenstein's criterion)* Let f be monic of positive degree over a principal ideal domain R. Let E be the field of fractions of R. Let π be a prime element of R dividing all the coefficients of f (apart from the leading one, that of x^n), and suppose that π^2 does *not* divide the constant coefficient. Then f is irreducible in $E[x]$.

Proof: Let k be the π-adic completion of E, and $\mathbf{o}$ the valuation ring in k. In fact, f is irreducible in $k[x]$. The hypothesis implies that the Newton polygon consists of a single segment connecting $(0, 1)$ and $(n, 0)$, with slope $-1/n$. Thus, by the previous corollary, f is irreducible in $k[x]$. ///

Corollary: In the situation of the theorem, the polynomial f factors over k into polynomials f_i of degrees d_i, where all roots of f_i have ord $-m_i$. Let $m_i = a_i/d_i$, if a_i is relatively prime to d_i then f_i is *irreducible* over k and any root of f_i generates a totally ramified extension of k.

Proof: If α, β are Galois conjugates, then their ords are the same. Thus, the set of roots with a given ord is stable under Galois. That is, the monic factor f_i of f with these as roots has coefficients in the ground field k. If the ord of α is of the form a/M with numerator prime to M then α generates an extension of degree divisible by M, by the lemma above. Thus, f_i is irreducible if in lowest terms $-m_i$ has denominator d_i. ///

Remark: In this last corollary there is not conclusion about the irreducibility of the factor f_i if the denominator of $-m_i$ (in lowest terms) is not the maximum possible, d_i. That is, we reach a sharp conclusion only for totally ramified extensions.

Corollary: If the Newton polygon has a line segment of slope -1 and length 1, then there is a factor $x - \alpha$ of $f(x)$ with $\alpha \in k$.

Proof: The previous results show that there is a factor $x - \alpha$ with $\text{ord}\alpha = 1$. If α were not in k, then it would have a Galois conjugate $\beta \neq \alpha$ with the same ord, which is excluded by the hypothesis. ///

Example: Consider

$$f(x) = x^5 + 2x^2 + 4$$

over $\mathbf{Q}_2$. The Newton polygon has two pieces, one with slope $-1/3$ and length 3, the other with slope $-1/2$ and length 2. Thus, over $\mathbf{Q}_2$ this quintic factors into an irreducible cubic and an irreducible quadratic.

Example: Consider a slight alteration of the previous, to

$$f(x) = x^5 + 2x + 4$$

over $\mathbf{Q}_2$. Not the Newton polygon has two pieces, one with slope $-1/4$ and length 4, the other with slope -1 and length 1. Thus, over $\mathbf{Q}_2$ this quintic factors into an irreducible quartic and has a linear factor in k.

Example: Consider the formal power series ring $\mathbf{o} = \mathbf{C}[[z]]$ and its field of fractions k. Use the ord function

$$\mathrm{ord}(c_n z^n + c_{n+1} z^{n+1} + \ldots) = 2^{-n}$$

(with $c_n \neq 0$). The non-zero prime ideal in $\mathbf{o}$ is generated by z. Let

$$f(w) = w^3 - zw + z$$

By Eisenstein's criterion this is irreducible. The extension generated by a root is totally ramified over k, that is, the Riemann surface is *triply branched* at 0.

Example: By contrast, consider

$$f(w) = w^3 - zw + z^2$$

The Newton polygon has two pieces, revealing two roots with ord 1/2 and one with ord 1. Thus, there is a root w in k. Thus, at 0 the Riemann surface of this polynomial has a doubly-branched part and a separate sheet.
