Revista Colombiana de Matemáticas
Vol. XXI (1987), págs. 141-146

A SIMPLE PROOF OF A GENERALIZATION OF EISENSTEIN'S IRREDUCIBILITY CRITERION

by

Nelo D. ALLAN(*)

Abstract. We present a simple proof of Königsberg's Criterion, [K] p.69 and also present families of irreducible polynomials over some fields. In particular, if $(n,h) = 1$, $a_o,\ldots,a_{n-1} \in Z$ = ring of integers and p is a primer not dividing a_o, then $f(x) = x^n - p^h(a_o + a_1 + \ldots + a_{n-1}x^{n-1})$ is irreducible over the rationals. Also if k is any field, then $F(x,y) = x^n - ay^h + \sum_{t=1}^{n-1} a_t x^t y^{\lambda(t)}$, $a, a_t \in k$, $\lambda(t) \in Z$ $a \neq 0$, and $n\lambda(t)+ht > nh$, is irreducible in $k[x,y]$.

This is an expository note which has as objective to give a simple up-to-date, elementary proof of Konigsberg's generalization of the Eisenstein's Irreducibility criterion.

Let k be a complete discrete valuation field with ring of integers R, valuation ν and prime π. Let $F(x) \in R[x]$ be a minic polynomial; we want to find conditions under which F(x) is irreducible. We let $F(x) = \sum_{i=o}^{n} a_i' x^{n-i}$, $a_o' = 1$, and we set $a_i' = \pi^{\lambda(i)} a_i$, with $\nu(a_i) = 0$ if $a_i' \neq 0$ and $\lambda(i) \in Z$. In the car-

(*) This research has been fully supported by the reciprocity agreement NSERC-CNP$_q$. (Canada-Brazil).

tesian plane we plot the Newton Polygon, $P(F)$, of F. It consists of the lower part of the boundary of the convex hull of the points $\{(i,\lambda(i)) | i = 0,\dots,n,\ a_i \neq 0\}$.

A necessary condition for the irreducibility of F is that $P(F)$ consists of a single segment E joining $(n,0)$ to $(0,h)$ for $h = \lambda(n)$. We set $n = um$, $h = vm$, with $(u,v) = 1$, and look at the polynomial F_o formed by the terms whose corresponding points lie on E. Roughly speaking we erase the positive powers of π out of F_o and replace x^u by X; if the new polynomial $F^*(X)$ is irreducible mod π, then f is irreducible. Clearly, we can immediately construct families of irreducible polynomials, one of them $x^n - \pi^h H(x)$, $\pi \nmid H(0)$, $(n,h) = 1$, and degree of $H =: d^oH \leqslant n-1$. If $h = 1$ we get the Eisenstein's criterion. This criterion follows easily from [W] and puts in evidence the fact that Newton's polygons give a better understanding of the Einsentein's criterion: it is a first stage of a process that if we parallel to the theory of singularities of a curve, it corresponds to the usual stages of separating branches of a curve, at a singular point (see [M] and also [A]).

It is well known that if F is irreducible, then its polygon is a segment (see [W], p.74). Hence a necessary condition in order to have the irreducibility of F is that $P(F) = E$ be a segment, which we shall assume not to be parallel to the x-axis. Consequently its end points are $\{(0,h),(n,0)\}$, $h = \lambda(n)$ and again writting $n = um$, $h = vm$, $(u,v) = 1$, then the equations of the line ℓ_o support of E is $xv + uy = muv$. We write $F(x) = F_o(x) + F_1(x) + \dots$, with $F_j(x)$ being the sum of the terms of F whose corresponding points lie on the line $\ell_j = \ell(m,j)$: $xv + yu = muv + j$; thus

$$F_o(x) := F_o(x,\pi) = x^{mu} + \sum_{t=1}^{m} a''_t x^{u(m-t)} \pi^{ut}, \quad a''_t = a_{mt}$$

can be regarded as a homogeneous (v,u)-weighted form in (x,π), of total weight muv. The same is true form F_j but now the total weight is $muv + j$.

We shall denote by $\bar{k}$ the residue class field of k and then we shall associate to F a polynomial F^* of m-th degree in $\bar{k}[X]$ defined by

$$F^*(X) = X^m + \sum_{t=1}^{m} \bar{a}_{t''} X^{m-t}.$$

where $\bar{a}$ denotes the reduction of a mod π. If G(X) is another monic polynomial in R[x] such that P(G) is a segment E' parallel to E, then G decomposes as sum $G = G_0 + G_1 + \ldots$ of polynomials G_j which can be also regarded as weighted forms in (x,π) with respective weights (v,u), say of total degree $suv + j$. Using the same procedure, we arrive at polynomial G^* of degree s in $\bar{k}[X]$. Now it is easy to verify that P(FG) is also a segment parallel to E, and because we are working with some sort of weighted forms, $(FG)_0 \equiv F_0G_0 \bmod \pi$, and hence $(FG)^* = F^*G^*$. (For, the corresponding points of F_jG_t all lie in the union of all $\ell(m+s\ ,\ j+t+ku)$).

We can now state our main theorem:

THEOREM. *Assume that* $f \equiv x^n \bmod p$, *that the Newton polygon of the monic polynomial* $F(x) \in R[x]$ *is a segment, and that the form* F^* *is irreducible. Then* F *is irreducible in* R[x].

Proof. In fact, let us assume that F is reducible say $F = \Pi F_i$, F_i nonconstant irreducible, which, by Gauss' lemma, we may assume that $F_i \in R[x]$. Now as remarked before, the diagram of F_i is segment. If $\tilde{k}$ is the splitting field of F, $\tilde{\nu}$ is the unique extension of ν to $\tilde{k}$, and $\alpha \in \tilde{k}$ is a root of F, then $\tilde{\nu}(\alpha)$ = -slope of E. Consequently, if $P(F_i) = E_i$ and α_i is any root of F_i, then $\tilde{\nu}(\alpha_i)$ = -slope of E = -slope of E_i. Consequently all E_i are parallel to E and $F^* = \Pi F_i^*$. As F_i are non constant, F_i^* are non trivial proper divisor of F^* and this is a contradiction. Therefore F is irreducible.

Since irreducibility over $\mathbb{Z}_p$, the ring of the p-adic integers, p prime, implies irreducibility over the ring of integers $\mathbb{Z}$, we have:

COROLLARY. *Let* $a_i \in \mathbb{Z}$, *be such that* $F^*(X) = X^m + \sum a_i X^{m-1}$

is irreducible mod p. *We let* u, v *be relatively prime,* (u,v) = 1. *Let* $H(x) = \sum_{i=o}^{n-1} b_i x^i p^{\lambda(i)} \in \mathbb{Z}[x]$ *be such that* $\lambda(i) > 0$ *and if* $b_i \neq 0$, $iv + \lambda(i)u > muv$. *Then*

$$F(x) = x^{um} + \sum a_i x^{u(m-i)} p^{iv} + H(x)$$

is irreducible.

We close our note with five remarks:

REMARK 1. The condition (n,h) = 1 is already sufficient for the irreducibility of F, because m = 1 and then F^* is linear. (See [V], p.77, Ex.1).

REMARK 2. Our last corollary can be applied to a more general situation, namely the case where R^* is a Dedekind domain, p is a primer and R its p-adic completion.

REMARK 3. Another case where our theorem applies is when $R = L[[Y]]$ is the formal power series ring in one variable over a field L, and (n,h) = 1

$$F(x,y) = ax^n - by^h + H(x,y) \in L|x,y|$$

with $a,b \in L$, $ab \neq 0$, and

$$H(x,y) = \sum \{a_{ij} x^i y^j \mid hi + jn > hn,\ i < n,\ a_{ij} \in L\}.$$

F is irreducible in R[x] and a fortiori in $L[x,y] \subset R[x]$.

REMARK 4. We let ν_o be the valuation u.v. It was observed by Rella (see (R)) that we have an extension ν_1 of ν_o to k[x] by setting $\nu_1(x) = \nu$. The residue class ring of ν_1 is $\bar{k}[x]$ where X is the image of $x^u \pi^{-\nu}$. In our case $\nu_1(F_j) = muv + j$ hence the image of $\pi^{-muv} F(x)$ coincides with $F^*(X)$.

REMARK 5. It is also easily seen that in the case where N is prime all the irreducible polynomials of degree N are either obtained by lifting the irreducibles of $\bar{k}[x]$ or up to a linear change of variables, by considering polinonials as in Remark 3 with $\pi = y$. If in Remark 3, L is formally real and N is odd the same holds for the irreducible germs at the origin.

Finally a next step generalization, the Dumas Criterion comes when in the corollary we replace x by a polynomial w(x), irreducible mod p. (see [A], [M] and [V]).

BIBLIOGRAPHY

[A] Allan, N., *Irreducible Polynomials over complete discrete Valuation Rings*, (To appear).

[W] Weiss, E., *Algebraic Number Theory*, New York, 1963.

[K] Königsberger, L., *Ueber die Eisensteinschen Satz von der Irreduzibilität Algebraischer Gleichungen*, Journal fur die Mathematik, vol. 115 (1895), 53-78.

[M] MacLane, S., *The Schönemann-Eisenstein Irreducibility Criteria in Terms de Prime Ideals*, Trans. Amer. Math. Society (1938), 226-239.

[R] Rella, T., *Ordnungsbestimmungen in Integrität Bereichen und Newtonsche Polynome*, Journal für die Mathematik, vol. 158, 1927, 33-48.

[V] Van der Waerden, B.L., *Modern Algebra*, Vol. 1, 2nd Edition, Ungar, N.Y., 1949, 76-77.

*

Departamento de Matemática
Universidade Estadual de Campinas
Caixa Postal 1170
13100 Campinas, SP, Brasil.

(Recibido en octubre de 1986).