Some extensions and applications of Eisenstein Irreducibility Criterion

Sudesh Kaur Khanduja
Department of Mathematics
Panjab University, Chandigarh
E-mail: skhand@pu.ac.in

Eisenstein Irreducibility Criterion. (1850)

Let $F(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$ *be a polynomial with coefficient in the ring* $\mathbb{Z}$ *of integers. Suppose that there exists a prime number* p *such that*

- a_0 *is not divisible by* p,
- a_i *is divisible by* p *for* $1 \leq i \leq n$,
- a_n *is not divisible by* p^2

$F(x)$ *is irreducible over the field* $\mathbb{Q}$ *of rational numbers.*

Example: Consider the pth cyclotomic polynomial $x^{p-1} + x^{p-2} + ... + x + 1 = x^p - 1/x - 1$ On changing x to $x+1$ it becomes $(x+1)^p - 1/(x+1-1) = x^{p-1} + \begin{pmatrix} p \\ 1 \end{pmatrix} x^{p-2} + ... + \begin{pmatrix} p \\ p-1 \end{pmatrix}$ and hence is irreducible over $\mathbb{Q}$.

This slick proof of the irreducibility for the pth cyclotomic polynomial was given by the Eisenstein,though its irreducibilty was proved by Gauss in 1799.

In 1906, Dumas proved the following generalization of this criterion.

Dumas Criterion. *Let* $F(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$ *be a polynomial with coefficients in* $\mathbb{Z}$. *Suppose there exists a prime* p *whose exact power* p^{r_i} *dividing* a_i *(where* $r_i = \infty$ *if* $a_i = 0$*),* $0 \leq i \leq n$*, satisfy*

- $r_0 = 0$,
- $(r_i/i) > (r_n/n)$ *for* $1 \leq i \leq n-1$ *and*
- *gcd*$(r_n,\ n)$ *equals 1.*

Then $F(x)$ *is irreducible over* $\mathbb{Q}$.

Example : x^3+3x^2+9x+9 is irreducible over $\mathbb{Q}$.

Note that Eisenstein's criterion is a special case of Dumas Criterion with $r_n = 1$.

For a given prime number p, let v_p stand for the mapping $v_p : Q^* \longrightarrow Z$ defined as follows. Write any non zero rational number $x = p^r\frac{a}{b}, p \nmid ab$. Set $v_p(x) = r$. Then

(i) $v_p(xy) = v_p(x) + v_p(y)$
(ii) $v_p(x+y) \geq min\{v_p(x), v_p(y)\}$.

Set $v_p(0) = \infty$. v_p is called the p-adic valuation of $\mathbb{Q}$.

Dumas Criterion. *Let* $F(x) = a_0x^n + a_1x^{n-1} + ... + a_n$ *be a polynomial with coefficients in* $\mathbb{Z}$*. Suppose there exists a prime number* p *such that* $v_p(a_0) = 0$, $v_p(a_i)/i > v_p(a_n)/n$ *for* $1 \leq i \leq n-1$ *and* $v_p(a_n)$ *is coprime to* n*, then* $F(x)$ *is irreducible over* $\mathbb{Q}$*.*

In 1923, Dumas criterion was extended to polynomials over more general fields namely, fields with discrete valuations by Kürschák. Indeed it was the Hungarian Mathematician JOSEPH KÜRSCHÁK who formulated the formal definition of the notion of valuation of a field in 1912.

Definition :A real valuation v of a field K is a mapping $v : K^* \longrightarrow \mathbb{R}$ satisfying

(i) $v(xy) = v(x) + v(y)$
(ii) $v(x + y) \geq min\{v_(x), v(y)\}$
(iii) $v(0) = \infty$.

$v(K^*)$ is called the value group of v. A real valuation is said to be discrete if $v(K^*)$ is isomorphic to $\mathbb{Z}$.

In 1931, Krull generalized the above notion of valuation.

By a Krull valuation of a field K we mean a mapping

$$v : K^* \to G$$

where G is a totally ordered (additively written) abelian group satisfying (i), (ii) and (iii). The pair (K, v) is called a valued field. The subring $\mathcal{R}_v = \{x \in K |\ v(x) \geqslant 0\}$ of K is called the valuation ring of v. It has a unique maximal ideal given by $\mathcal{M}_v = \{x \in K |\ v(x) > 0\}$. $R_v/\mathcal{M}_v$ is called the residue field of v. For any ξ belonging to R_v $\bar{\xi}$ will stand for the canonical homomorphism from R_v onto $R_v/\mathcal{M}_v$.

Example. Let v_x denote the x-adic valuation of the field $\mathbb{Q}(x)$ of rational functions in x trivial on $\mathbb{Q}$ and v_p denote the p-adic valuation of $\mathbb{Q}$. For any non-zero polynomial $f(x)$ belonging to $\mathbb{Q}(x)$, we shall denote by f^* the constant term of the polynomial $f(x)/x^{v_x(f(x))}$. Let v be the mapping from non-zero elements of $\mathbb{Q}(x)$ to $\mathbb{Z} \times \mathbb{Z}$ (lexicographically ordered) defined on $\mathbb{Q}[x]$ by

$$v(f(x)) = (v_x(f(x)), v_p(f^*)).$$

Then v gives a valuation on $\mathbb{Q}(x)$.

In 1997, Saha and S.K.K generalized the Eisenstein-Dumas-Kürschák criterion.

Theorem1.(-,Saha) *let v be a Krull valuation of a field K with value group G and $F(x) = a_0x^s + a_1x^{s-1} + ... + a_s$ be a polynomial over K. If*

- $v(a_0) = 0$,
- $v(a_i)/i \geq v(a_s)/s$ *for* $1 \leq i \leq s$ *and*
- *there does not exit any integer* $d > 1$ *dividing* s *such that* $v(a_s)/d \in G$,

then $F(x)$ is irreducible over K.

Definition. A polynomial which satisfies the hypothesis of Theorem 1 is called an Eisenstein-Dumas polynomial with respect to v.

Example: Let $F(X,Y) = g(Y)X^s + h(Y)$ be a polynomial over a field L in independent variables X, Y. If $g(Y), h(Y)$ have no common factors and $deg\ g(Y) - deg\ h(Y)$ is coprime to s,then $F(X,Y)$ is irreducible over L.

Verification: Regard $F(X,Y)/g(Y)$ as a polynomial in X with coefficients over the field $K = L(Y)$ with valuation on K defined by $v(a(Y)/b(Y)) = deg\ b(Y) - deg\ a(Y)$ and apply the criterion by Saha.
In 2001, S. Bhatia generalized Eisenstein's Irreducibility Criterion in a different direction.

Theorem 2. (–, S. Bhatia) *Let v be a valuation of a field K with value group the set of integers. Let $g(x) = x^m + a_1 x^{m-1} + \dots + a_m$ be a polynomial with coefficients in K such that $v(a_i)/i > v(a_m)/m$ for $1 \leq i \leq m-1$. Let r denote $gcd(v(a_m), m)$ and b be an element of K with $v(b) = v(a_m)/r$. Suppose that the polynomial $z^r + (a_m/b^r)^{-}$ in the indeterminate z is irreducible over the residue field of v. Then $g(x)$ is irreducible over K.*

Theorem 3. *Let $f(x)$ and $g(y)$ be non-constant polynomials with coefficients in a field k. Let c and c_0 denote respectively the leading coefficients of $f(x)$ and $g(y)$ and n, m their degrees. If $gcd(m, n) = r$ and if $z^r - (c_0/c)$ is irreducible over k, then so is $f(x) - g(y)$.*

The result of Theorem 3 has its roots in a theorem of Ehrenfeucht. In 1956, Ehrenfeucht proved that a polynomial $f_1(x_1) + ... + f_n(x_n)$ with complex coefficients is irreducible provided the degrees of $f_1(x_1), ...,$ $f_n(x_n)$ have greatest common divisor one.

In 1964, Tverberg extended this result by showing that when $n \geq 3$, then $f_1(x_1) + ... + f_n(x_n)$ belonging to $K[x_1, ..., x_n]$ is irreducible over any field K of characteristic zero in case the degree of each f_i is positive. Of course this result is false when characteristic of K is $p > 0$. Note that if a polynomial F can be written as $F = (g_1(x_1))^p + (g_2(x_2))^p + ... + (g_n(x_n))^p + c[g_1(x_1) + g_2(x_2) + ... + g_n(x_n)]$ where c is in K and each $g_i(x_i)$ is in $K[x_i]$, then it is reducible over K.

In 1966, Tverberg proved that the converse of the above simple fact holds in the particular case when $n = 3$ and K is an algebraically closed field of characteristic $p > 0$. In 1982, Schinzel extended Tverberg's result by showing that this converse holds for any $n \geq 3$. In 2004, Amrit Pal has given a proof of Schinzel's result which is shorter and entirely different from Schinzel's proof.

Question: *When is a translate* $g(x+a)$ *of a given polynomial* $g(x)$ *with coefficients in a valued field* (K, v) *an Eisenstein-Dumas polynomial with respect to* v*?*

In 2009, we have characterized such polynomials using distinguished pairs.

Theorem 4 (-, Anuj Bishnoi). *Let* v *be a henselian Krull valuation of a field* K*. Let* $g(x)$ *belonging to* $R_v[x]$ *be a monic polynomial of degree* e *having a root* θ*. Then for an element* a *of* K*,* $g(x + a)$ *is an Eisenstein-Dumas polynomial with respect to* v *if and only if* (θ, a) *is a distinguished pair and* $K(\theta)/K$ *is a totally ramified extension of degree* e*.*

The following result which generalizes a result of M. Juras [12] proved in 2006 has been quickly deduced from the above theorem.

Theorem 5. *Let* $g(x) = \sum_{i=0}^{e} a_i x^i$ *be a monic polynomial with coefficients in a henselian valued field* (K, v)*. Suppose that the characteristic of the residue field of* v *does not divide* e*. If there exists an element* b *belonging to* K *such that* $g(x+b)$ *is an Eisenstein-Dumas polynomial with respect to* v*, then so is* $g(x - \frac{a_{e-1}}{e})$*.*

Classical Schönemann Irreducibility Criterion.(1846) *If a polynomial $F(x)$ belonging to $\mathbb{Z}[x]$ has the form $F(x) = \phi(x)^s + pM(x)$ where p is a prime number,*

- *$\phi(x)$ belonging to $\mathbb{Z}[x]$ is a monic polynomial which is irreducible modulo p,*
- *$\phi(x)$ is co-prime to $M(x)$ modulo p, and*
- *the degree of $M(x)$ is less than the degree of $F(x)$,*

then $F(x)$ is irreducible in $\mathbb{Q}[x]$.

Eisenstein's Criterion is easily seen to be a particular case of Schönemann Criterion by setting $\phi(x) = x$.

In 1997, Saha gave a generalization of Classical Schönemann Irreducibility Criterion using the theory of prolongations of a valuation defined on K to a simple transcendental extension of K which was initiated by MacLane and developed further by Popescu at el. In 2008, Ron Brown has given a different proof of Saha's result.

Recently, we have extended the Generalized Schönemann-Eisenstein Irreducibility Criterion.

Theorem 6. (-, R. Khassa) *Let v be a discrete valuation of K with value group $\mathbb{Z}$ and π be an element of K with $v(\pi) = 1$.*

Let $f(x)$ belonging to $R_v[x]$ be a monic polynomial of degree m such that $\bar{f}(x)$ is irreducible over $R_v/\mathcal{M}_v$. Let $F(x)$ belonging to $R_v[x]$ be a monic polynomial having $f(x)$-expansion $\sum_{i=0}^{n} A_i(x)f(x)^i$. Assume that there exists $s \leqslant n$ such that π does not divide the content of $A_s(x)$, π divides the content of each $A_i(x), 0 \leqslant i \leqslant s-1$ and π^2 does not divide the content of $A_0(x)$. Then $F(x)$ has an irreducible factor of degree sm over the completion $(\hat{K}, \hat{v})$ of (K, v) which is a Schönemann polynomial with respect to $\hat{v}$ and $f(x)$.

Theorem 7. *Let* $(K, v), \pi$ *be as above and* $F(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ *be a polynomial over* R_v *satisfying the following conditions for an index* $s \leqslant n-1$.
(i) $\pi | a_i$ *for* $0 \leqslant i \leqslant s-1$, $\pi^2 \nmid a_0, \pi \nmid a_s$.
(ii) The polynomial $x^{n-s} + \bar{a}_{n-1}x^{n-s-1} + \ldots + \bar{a}_s$ *is irreducible over the residue field of* v.
(iii) $\bar{d} \neq \bar{a}_s$ *for any divisor* d *of* a_0 *in* R_v.
Then $F(x)$ *is irreducible over* K.

Gotthold Max Eisenstein
Born: 16 April 1823 in Berlin, Germany
Died: 11 Oct 1852 in Berlin, Germany

What attracted me so strongly and exclusively to mathematics, apart from the actual content, was particularly the specific nature of the mental processes by which mathematical concepts are handled. This way of deducing and discovering new truths from old ones, and the extraordinary clarity and self-evidence of the theorems, the ingeniousness of the ideas ... had an irresistible fascination for me. Beginning from the individual theorems, I grew accustomed to delve more deeply into their relationships and to grasp whole theories as a single entity. That is how I conceived the idea of mathematical beauty ...

References

1. T. Schönemann, Von denjenigen Moduln, Welche Potenzen von Primzahlen sind, *Journal für die Reine und Angew. Math.* 32 (1846) 93-105.
2. G. Eisenstein, Über die Irreduzibilitat und einige andere Eigenschaften der Gleichungen, *Journal fü die Reine und Angew. Math.*, 39 (1850) 160-179.
3. G. Dumas, Sur quelques cas d'irreductibilite des polynomes à coefficients rationnels, *Journal de Math. Pures et Appliqus*, 6 (1906) 191-258.
4. J. Kürschák, Irreduzible Formen, *Journal fü die Reine und Angew. Math.*, 152 (1923) 180-191.
5. S. Maclane, The Schönemann - Eisenstein irreducibility criterion in terms of prime ideals, *Trans. Amer. Math. Soc.*, 43 (1938) 226-239.
6. A. Ehrenfeucht, Kryterium absolutnej nierozkladalnosci wielomianow, *Prace Math.*, 2 (1956) 167-169.

7. H. Tverberg, A remark on Ehrenfeucht's criterion for irreducibility of polynomials, *Prace Mat.*, 8 (1964) 117-118.
8. H. Tverberg, On the irreducibility of polynomials $f(x) + g(y) + h(z)$. *Quart. J. Math.*, 17 (1966) 364-366.
9. A. Schinzel, Reducibility of polynomials in several variables II. Pacific J. Math. *118* (1985), 531-563.
10. V.Alexandru, N. Popescu and A. Zaharescu, A theorem of characterizaton of residual transcendental extension of a valuation, *J. Math. Kyoto Univ.*, 28 (1988) 579-592.
11.S. K. Khanduja and Jayanti Saha, On a generalization of Eisenstein's irreducibility criterion, *Mathematika,* 44 (1997) 37-41.
12. P.Ribenboim, The Theory of Classical Valuations,*Springer Verlag*,1999.

13. S. Bhatia and S. K. Khanduja, Difference polynomials and their generalizations, *Mathematika,* 48 (2001), 293-299.

14. A. P. Singh and S. K. Khanduja, An extension of the irreducibility criteria of Ehrenfeucht and Tverberg, *Communications in Algebra,* 32 (2004) 579-588.

15. M. Jur*áš*, A note on Eisenstein's criterion for irreducibility of polynomials , JP Jour. Algebra, Number Theory, and Appl., 5(3) (2005), 603 608.

16. R. Brown ,Roots of Schönemann Polynomials in Henselian extension fields, *Indian J. Pure and Applied Mathematics* 39(5) (2008) 403-410.

17. Anuj Bishnoi and S. K. Khanduja, On Eisenstein-Dumas and Generalized Schönemann polynomials., *Comm. Algebra* 2010 (to appear).

18. R. Khassa and S.K. Khanduja, A generalization of Eisenstein-Schönemann Irreducibility Criterion (Preprint)

THANK YOU