Irreducible Polynomials

Sudesh K. Khanduja

Indian Institute of Science Education and Research,

Mohali (Chandigarh), India
email: skhanduja@iisermohali.ac.in

Field medalist 2014

Maryam Mirzakhani (May 1977)

The word polynomial is derived from the Greek word "poly" meaning many and Latin word "nomial" meaning term. A polynomial is an expression involving a sum of terms in one or more variables multiplied by coefficients.

- $4x^3 + \frac{7}{3}x^2 - \frac{2}{7}x + 1$ is a polynomial in one variable.
- $9\sqrt{2}x^3y^2 + 6x^2y + 5xy + \sqrt{3}$ is a polynomial in two variables.

The degree of a polynomial $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$ is defined to be n if $a_n \neq 0$. The degree of the polynomial $\sum a_{ij}x^iy^j$ in two variables x, y is defined to be $\max\{i + j | a_{ij} \neq 0\}$

A polynomial of degree $n \geq 1$ with coefficients in a field F is said to be irreducible over F if it cannot be written as a product of two non constant polynomials over F of degree less than n.

- Every polynomial of degree one is irreducible.
- The polynomial $x^2 + 1$ is irreducible over $\mathbb{R}$ but reducible over $\mathbb{C}$.
- Irreducible polynomials are the building blocks of all polynomials.

The Fundamental Theorem of Algebra (Gauss, 1797).

Every polynomial $f(x)$ with complex coefficients can be factored into linear factors over the complex numbers.

Gauss used an alternative formulation that avoided the notion of complex numbers, considering the polynomials $f(x)\bar{f}(x)$ and proved that each irreducible polynomial over real numbers has degree one or two.

Carl Friedrich Gauss (1777–1855)

- Interestingly over $\mathbb{Q}$ for each number $n \geq 1$, one can easily construct infinitely many irreducible polynomials of degree n.

Eisenstein Irreducibility Criterion (1850).

Let $F(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial with coefficient in the ring $\mathbb{Z}$ of integers. Suppose that there exists a prime number p such that

- *a_n is not divisible by p,*
- *a_i is divisible by p for $0 \leq i \leq n-1$,*
- *a_0 is not divisible by p^2*

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

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

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

Dumas Criterion.

Let $F(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$ 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

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

Definition.

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

(i) $v_p(ab) = v_p(a) + v_p(b)$

(ii) $v_p(a + b) \geq min\{v_p(a), v_p(b)\}$.

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

Using the p-adic valuation v_p of the field $\mathbb{Q}$, Dumas criterion can be restated as:

Dumas Criterion.

Let $F(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial with coefficients in $\mathbb{Z}$. Suppose there exists a prime number p such that $v_p(a_n) = 0$, $v_p(a_i)/n - i > v_p(a_0)/n$ for $1 \leq i \leq n-1$ and $v_p(a_0)$ 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 $v : K^* \to \mathbb{R}$ satisfying

(i) $v(ab) = v(a) + v(b)$
(ii) $v(a+b) \geq min\{v(a), v(b)\}$
(iii) $v(0) = \infty$.

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

Example.

Let R be U.F.D with quotient field K. and π be a prime element of R. We denote the π-adic valuation of K defined for any non-zero $\alpha \in R$ by $v_\pi(\alpha) = r$, where $\alpha = \pi^r\beta, \beta \in R$, π does not divide β. It can be extended to K in a canonical manner.

Definition: Krull valuation

A Krull valuation v of a field K is a mapping, i.e., $v : K^* \to G$ where G is a totally ordered (additively written) abelian group satisfying (i) $v(ab) = v(a) + v(b)$ (ii) $v(a+b) \geq min\{v(a), v(b)\}$. The pair (K, v) is called a valued field. The subring $R_v = \{a \in K|\ v(a) \geqslant 0\}$ of K with unique maximal ideal $\mathcal{M}_v = \{a \in K|\ v(a) > 0\}$ is called the valuation ring of v.

Example Krull valuation.

Let v_x denote the x-adic valuation of the field $\mathbb{Q}(x)$ of rational functions in an indeterminate x trivial on $\mathbb{Q}$. For any non-zero polynomial $g(x)$ belonging to $\mathbb{Q}(x)$, we shall denote $g^{(0)}$ the constant term of the polynomial $g(x)/x^{v_x(g(x))}$. Let p be any rational prime. 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

$$v(g(x)) = (v_x(g(x)), v_p(g^{(0)})).$$

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

Theorem 1. (-, J. Saha, 1997)

Let v be a Krull valuation of a field K with value group G and $F(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial over K. If

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

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

Definition.

A polynomial with coefficients from a valued field (K, v) which satisfies the hypothesis of Theorem 1 is called an Eisenstein-Dumas polynomial with respect to v.

In 2001, S. Bhatia generalized Eisenstein - Dumas Irreducibility Criterion in a different direction.

Theorem 2 (–, S. Bhatia)

Let $F(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_0$ 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

- $r_n = 0$,
- $(r_i/n - i) > (r_0/n)$ *for* $1 \leq i \leq n-1$ *and*
- $gcd(r_0,\ n) = d$ *and the polynomial* $a_n x^d + a_0/p^{r_0}$ *is irreducible modulo* p.

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

Example: Let p be a prime congruent 3 modulo 4. Let b_0, b_2, b_3 be integers with b_0 congruent 1 mod p. The polynomial $x^4 + b_3 p x^3 + b_2 p^2 x^2 + b_0 p^2$ is irreducible over $\mathbb{Q}$.

Theorem 3 (–, S. Bhatia).

Let $f(x)$ and $g(y)$ be non-constant polynomials with coefficients in a field K. Let a and b denote respectively the leading coefficients of $f(x)$ and $g(y)$ and m, n their degrees. If $gcd(m, n) = r$ and if $z^r - (b/a)$ 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 $f_1(x_1) + \cdots + f_n(x_n)$ with complex coefficients is irreducible provided the degrees of $f_1(x_1), \ldots, f_n(x_n)$ have greatest common divisor one. In 1964, Tverberg extended this result by showing that when $n \geq 3$, then $f_1(x_1) + \cdots + f_n(x_n)$ belonging to $K[x_1, \ldots, x_n]$ is irreducible over any field K of characteristic zero in case the degree of each f_i is positive. He also proved that $f_1(x_1) + f_2(x_2)$ is irreducible over any field provided degrees of f_1 and f_2 are coprime.

The following more general result was obtained for Generalized Difference Polynomials jointly with A. J. Engler in 2008.

Recall that a polynomial $P(x, y)$ is said to be a generalized difference polynomial (with respect to x) of the type (n, m) if $P(x, y) = ax^m + \sum_{i=1}^{m} P_i(y)x^{m-i}$, where $a \in K^*, m \geq 1,\ n = \deg P_m(y) \geq 1$ and $\deg P_i(y) < ni/m$ for $1 \leq i \leq m-1$.

Theorem 4. (-, A. J. Engler, 2008)

Let $P(x, y) = ax^m + P_1(y)x^{m-1} + \ldots + P_m(y)$ be a generalized difference polynomial of the type (n, m) over a field K. Let r be the greatest common divisor of m, n and b be the leading coefficient of $P_m(y)$. Then the number of irreducible factors of $P(x, y)$ over K (counting multiplicities if any) does not exceed the number of K-irreducible factors of the polynomial $x^r + \frac{b}{a}$

Proof of Theorem 4.

Let

$$P(x,y) = aF_1(x,y)...F_s(x,y) \tag{1}$$

be a factorization of $P(x,y)$ as a product of irreducible factors over K. Let x be given the weight n and y the weight m. Let $H_i(x,y)$ denote the sum of those monomials occurring in $F_i(x,y)$ which have the highest weight, then $H_i(x,y)$ is a non-constant polynomial. Denote $\frac{b}{a}$ by $-u$. Keeping in mind the definition of a generalized difference polynomial and comparing the terms of highest weight on both sides of (1), it can be easily seen that

$$x^m - uy^n = H_1(x,y)...H_s(x,y). \tag{2}$$

Let p denote the characteristic of K or 1 according as char of K is positive or zero.

Let ξ be a primitive r_1-th root of unity, where $r = p^t r_1$, p does not divide r_1. The integers $\frac{m}{r}$ and $\frac{n}{r}$ will be denoted by m_1, n_1 respectively. Choose c belonging to the algebraic closure K^{alg} of K such that $c^r = u$. Rewrite (2) as

$$x^m - uy^n = \prod_{i=1}^{r}(x^{m_1} - c\xi^i y^{n_1}) = H_1(x,y)...H_s(x,y). \qquad (3)$$

Recall that a polynomial of the type $x^j - dy^k$ is irreducible over K^{alg}, where j, k are co-prime.Consequently each K-irreducible factor of $x^m - uy^n$ will be a polynomials in x^{m_1}, y^{n_1} and thus will be arise from a K-irreducible factor of $x^r - uy^r$ and hence from that of $x^r - u$. This proves the theorem in view of (3).

Question

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

In 2010, Anuj Bishnoi characterized such polynomials using distinguished pairs and the following result was deduced as a corollary which extends a result of M.Juras.

Theorem 5.

Let $g(x) = \sum_{i=0}^{n} a_i x^i$ be a monic polynomial of degree n with coefficients in a valued field (K, v). Suppose that the characteristic of the residue field of v does not divide n. 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 $g(x - \frac{a_{n-1}}{n})$.

Classical Schönemann Irreducibility Criterion(1846).

If a polynomial $g(x)$ belonging to $\mathbb{Z}[x]$ has the form $g(x) = f(x)^n + pM(x)$ where p is a prime numberand $M[x] \in \mathbb{Z}[x]$ has degree less than $n \deg f(x)$ such that
• $f(x)$ belonging to $\mathbb{Z}[x]$ is a monic polynomial which is irreducible modulo p and
• $f(x)$ is co-prime to $M(x)$ modulo p,
then $g(x)$ is irreducible in $\mathbb{Q}[x]$.

Eisenstein's Criterion is easily seen to be a particular case of Schönemann Criterion by setting $f(x) = x$. A polynomial satisfying the hypothesis of the Schönemann Irreducibility Criterion is called a Schönemann polynomial with respect to v_p and $f(x)$.

f(x)-expension

If $f(x)$ is a fixed monic polynomial with co-efficients from an integral domain R,than each $g(x) \in R[x]$ can be uniquely written as $\sum g_i(x)f(x)^i$, $\deg g_i(x) < \deg f(x)$,referred to as the $f(x)$-expansion of $g(x)$.

It can be easily verified that a monic polynomial $g(x)$ belonging to $\mathbb{Z}[x]$ is a Schönemann polynomial w.r.t v_p and $f(x)$ if and only if the $f(x)$-expansion of $g(x)$ given by $g(x) = \sum_{i=0}^{n} g_i(x)f(x)^i$, $\deg g_i(x) <$ $\deg f(x)$, satisfies the following three conditions:
(i) $g_n(x) = 1$;
(ii) p divides the content of each polynomial $g_i(x)$ for $0 \leqslant i < n$;
(iii) p^2 does not divide the content of $g_0(x)$.
This reformulation led to the generalization of Schönemann Criterion to polynomials with coefficients in arbitrary valued fields.

Gaussian prolongation

Let v be a valuation of K. We shall denote by v^x the Gaussian prolongation of v to $K(x)$ defined on $K[x]$ by

$$v^x\Big(\sum_i a_i x^i\Big) = \min_i\{v(a_i)\}, a_i \in K.$$

Restatement of classical Schönemann Irreducibility Criterion.

Let $f(x)$ belonging to $\mathbb{Z}[x]$ is a monic polynomial which is irreducible modulo p and $g(x)$ belonging to $\mathbb{Z}[x]$ be a polynomial whose $f(x)$-expansion $\sum_{i=0}^{n} g_i(x)f(x)^i$ satisfies

(i) $g_n(x) = 1$;
(ii) $v_p^x(g_i(x)) \geq 1, 0 \leq i \leq n-1$;
(iii) $v_p^x(g_0(x)) = 1$.
Then $g(x)$ is irreducible over $\mathbb{Q}$.

Theorem 6. Generalized Schönemann Irreducibility Criterion. (-, J. Saha, R. Brown; 1997,2008)

Let v be a Krull valuation of a field K with value group G and valuation ring R_v having maximal ideal M_v. Let $f(x)$ belonging to $R_v[x]$ be a monic polynomial which is irreducible modulo M_v. Assume that $g(x)$ belonging to $R_v[x]$ is a polynomial whose $f(x)$-expansion $\sum_{i=0}^{n} g_i(x)f(x)^i$ satisfies (i) $g_n(x)=1$, (ii) $\frac{v^x(g_i(x))}{n-i} \geqslant \frac{v^x(g_0(x))}{n} > 0$ for $0 \leqslant i \leqslant n-1$ and (iii) $v^x(g_0(x)) \notin dG$ for any number $d>1$ dividing n. Then $g(x)$ is irreducible over K.

A polynomial $g(x)$ satisfying conditions (i), (ii), (iii) of the above Theorem 6 will be referred to as a Generalized Schönemann polynomial with respect to v and $f(x)$.

In 2011, Ramneek extended Generalized Schönemann Irreducibility Criterion and obtained the following result.

Theorem 7. (-, R. Khassa)

Let v be a henselian Krull valuation of a field K with value group G and valuation ring R_v having maximal ideal $\mathcal{M}_v$. Let $f(x)$ belonging to $R_v[x]$ be a monic polynomial of degree m which is irreducible modulo M_v and $A(x)$ belonging to $R_v[x]$be a monic polynomial with $f(x)$-expansion $\sum\limits_{i=0}^{n} A_i(x)f(x)^i$. Assume that there exists $s \leqslant n$ such that (i) $v^x(A_s(x)) = 0$, (ii) $\frac{v^x(A_i(x))}{s-i} \geqslant \frac{v^x(A_0(x))}{s} > 0$ for $0 \leqslant i \leqslant s-1$ and (iii) $v^x(A_0(x)) \notin dG$ for any number $d > 1$ dividing s. Then $A(x)$ has an irreducible factor $g(x)$ of degree sm over K such that $g(x)$ is a Generalized Schönemann polynomial with respect to v and $f(x)$; moreover the $f(x)$-expansion of $g(x) = f(x)^s + g_{s-1}(x)f(x)^{s-1} + \ldots + g_0(x)$ satisfies $v^x(g_0(x)) = v^x(A_0(x))$.

A special case of her previous result is following:

Theorem 8. (-, R. Khassa.)

Let v be a discrete valuation of K with value group $\mathbb{Z}$, valuation ring R_v having maximal ideal M_v generated by π. Let $f(x)$ belonging to $R_v[x]$ be a monic polynomial of degree m which is irreducible modulo M_v. Let $A(x)$ 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 $A(x)$ 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 $f(x)$.

Motivation

Let $g(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ *be a monic polynomial with coefficients in* $\mathbb{Z}$ *such that* p *does not divide* a_s, p *divides each* a_i *for* $0 \leqslant i \leqslant s-1$ *and* p^2 *does not divide* a_0. *Then* $g(x)$ *has an irreducible factor of degree* $\geq s$ *over* $\mathbb{Z}$.

Theorem 9 (-, R. Khassa)

Let $g(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ *be a monic polynomial with coefficients in* $\mathbb{Z}$ *such that* p *does not divide* a_s, p *divides each* a_i *for* $0 \leqslant i \leqslant s-1$ *and* p^2 *does not divide* a_0. *Then* $g(x)$ *has an irreducible factor of degree* s *over* p*-adic integers which is an Eisenstein polynomial with respect to* p.

Akira's Criterion(1982).

Let $F(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ belonging to $\mathbb{Z}[x]$ be a polynomial satisfying the following conditions for a prime p and an index $s \leqslant n-1$.

(i) $p|a_i$ for $0 \leqslant i \leqslant s-1$, $p^2 \nmid a_0, p \nmid a_s$.

(ii) The polynomial $x^{n-s} + a_{n-1}x^{n-s-1} + \ldots + a_s$ is irreducible modulo p.

(iii) No divisor of a_0 co-prime to p is congruent to a_s modulo p.

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

Example.

The polynomial $x^5 + ax^4 - 3x^3 + bx^2 + cx + 7$ is irreducible over $\mathbb{Q}$ for any choice of integers a, b, c all divisible by 7.

Theorem 10. Generalized Akira's Criterion (-, R. Khassa)

Let R_0 be an integrally closed domain with quotient field K and v be a discrete valuation of K with R_v containing R_0. Let $F(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ belonging to $R_0[x]$ be a polynomial satisfying the following conditions for an index $s \leqslant n-1$.

(i) $v(a_s) = 0$ and $v(a_i) > 0$ for $0 \leqslant i \leqslant s-1$, and $v(a_0) = 1$.

(ii) The polynomial $x^{n-s} + a_{n-1}x^{n-s-1} + \ldots + a_s$ is irreducible Modulo M_v over the residue field of v.

(iii) $d \not\equiv a_s$ modulo M_v for any divisor d of a_0 in R_0.

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

Proof of G.A.C.

Applying Theorem 9, we see that $F(x)$ has an irreducible factor $g(x)$ of degree s over the completion $(\hat{K}, \hat{v})$ of (K, v), which is an Eisenstein polynomial with respect to $\hat{v}$. Write $F(x) = g(x)h(x)$, where $g(x) = x^s + b_{s-1}x^{s-1} + \ldots + b_0$, $h(x) = x^{n-s} + c_{n-s-1}x^{n-s-1} + \ldots + c_0$. In view of the hypothesis, $F(x) \equiv x^s(x^{n-s} + a_{n-1}x^{n-s-1} + \ldots + a_s)$ modulo M_v, so $\bar{h}(x) = x^{n-s} + \bar{a}_{n-1}x^{n-s-1} + \ldots + \bar{a}_s$, which is given to be irreducible over the residue field of v. Hence $h(x)$ is also irreducible over $\hat{K}$. Note that $\bar{c}_0 = \bar{a}_s \neq \bar{0}$ by hypothesis. If $F(x)$ were reducible over K, then $g(x)$ and $h(x)$ being irreducible over $\hat{K}$, would belong to $R_0[x]$ and consequently the equality $a_0 = b_0c_0$ would contradict assumption (iii) of the corollary for the divisor c_0 belonging to R_0 of a_0.

Theorem 11. (Weintraub, 2013)

Let $F(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$ belonging to $\mathbb{Z}[x]$ be a polynomial and suppose there is a prime p which does not divide a_n, p divides a_i for $i = 0, \cdots, n-1$ and for some k with $0 \leq k \leq n-1, p^2$ does not divide a_k. Let k_0 be the smallest such value of k. If $F(x) = g(x)h(x)$ is a factorization in $\mathbb{Z}[x]$, then $\min(\deg g(x), \deg h(x)) \leq k_0$. In particular, for a primitive polynomial $F(x)$ if $k_0 = 0$ then $F(x)$ is irreducible over $\mathbb{Z}$.

Remark: The polynomial $x^{2k+m} + p^2 x^{k+m} + (p^3 - p^2)x^m + px^k + p^2$ with $k_0 = k \geq 1$ is reducible having factorization $(x^k + p)(x^{k+m} + (p^2 - p)x^m + p)$.

Observation: The hypothesis of above theorem implies that k_0 be the smallest index such that $\min\left\{\frac{v_p(a_i)}{n-i} | 0 \leq i \leq n-1\right\} = \frac{v_p(a_{k_0})}{n-k_0} = \frac{1}{n-k_0}$.

Theorem 12. (-, B. Tarar, 2015)

Let v be a valuation of a field K with valuation ring R_v. Let $F(x) = \sum_{i=0}^{n} a_i x^i \in R_v[x]$ be a polynomial with $v(a_n) = 0$. Let k_0 be the smallest index such that $\min\left\{\frac{v(a_i)}{n-i} \middle| 0 \le i \le n-1\right\} = \frac{v(a_{k_0})}{n-k_0} > 0$. If $v(a_{k_0}), n-k_0$ are co-prime, then for any factorization of $F(x)$ as $g(x)h(x)$ in $K[x]$, $\min\{\deg g(x), \deg h(x)\} \le k_0$.

Theorem 13. (-, B. Tarar, 2015)

Let v be a valuation of a field K with valuation ring R_v having maximal ideal M_v. Let $f(x)$ belonging to $R_v[x]$ be a monic polynomial of degree m which is irreducible modulo M_v and $A(x)$ belonging to $R_v[x]$ be a monic polynomial with $f(x)$-expansion $\sum_{i=0}^{n} A_i(x)f(x)^i, A_n(x) = 1$. Let k_0 be the smallest integer such that
$\min\left\{\frac{v^x(A_i(x))}{n-i} | 0 \le i \le n-1\right\} = \frac{v^x(A_{k_0}(x))}{n-k_0} > 0$. If $v^x(A_{k_0}(x)), n-k_0$ are co-prime, then for any factorization of $A(x)$ as $g(x)h(x)$ in $K[x]$, $\min\{\deg g(x), \deg h(x)\} \le k_0 m$.

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 für 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 für 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 J. 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] K. Aghigh and S. K. Khanduja, On the main invariant of elements algebraic over a henselian valued field, *Proc. Edinburgh Math. Soc.* 45 (2002) 219-227.

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

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

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

[18] A. J. Engler and S. K. Khanduja, On Irreducible factors of the polynomial f(x)-g(y), *International Journal of Mathematics*, 21:4 (2010) 407-418.

[19] A. Bishnoi and S. K. Khanduja, On Eisenstein-Dumas and Generalized Schönemann polynomials., *Comm. Algebra*, 38:9 (2010) 3163-3173.

[20] R. Khassa and S. K. Khanduja, A generalization of Eisenstein-Schönemann Irreducibility Criterion, *Manuscripta Mathematica* 134 (2011) 215-224.

[21]S. H. Weintraub, A mild generalization of Eisenstein's criterion, Proc. Amer. Math. Soc. 141, No. 4, 1159-1160 (2013)

[22] S. K. Khanduja, B. Tarar, Reformulation of Hensel's Lemma and extension of a theorem of Ore (submitted for publication to).

Jayanti Datta

Saurabh Bhatia

Ramneek Khassa

Bablesh Tarar

Thank You