Problems and results on polynomials

Andrzej Schinzel
Académie des Sciences de Pologne, Varsovie

January 25, 1993

[summary by Philippe Dumas]

The aim of the talk is to survey some problems on factorization of polynomials, polynomials with sparse powers, and irreducibility of binomials and trinomials.

1. Factorization of binomials

In 1895 Vahlen gave a necessary and sufficient condition for the reducibility of a binomial:

the binomial $X^n - a$ is reducible over $\mathbb{Q}$ iff
- $a = b^p$ with p a prime number which divides n and b is rational,
- or $a = -4\,b^4$, the number n is a multiple of 4 and b is rational.

Capelli extended the result two years later to the fields of characteristic 0 and Rédei treated the case of a positive characteristic. These results give the following theorem.

Theorem 1 (Capelli theorem). *The binomial $X^n - a$ has at least one irreducible factor whose number of nonzero coefficients is less or equal to three.*

One cannot improve the result since

$$X^4 + 4 = (X^2 - 2\,X + 2)(X^2 + 2\,X + 2).$$

2. Ritt theorems

Another type of factorization uses the composition instead of the product and Ritt published in 1922 an important work about the subject. At first if a complex polynomial f is prime and may be written $f = g \circ h$ then g or h has degree 1. Next the existence of such a factorization is obvious but there is no uniqueness because $g \circ h = (g \circ l) \circ (l^{[-1]} \circ h)$ if l has degree 1 and $l^{[-1]}$ is the functional inverse of l. One may hope for a result of quasi-uniqueness modulo linear functions, but the next example shows this is not the case.

$$\begin{aligned} f_1 &= X^r P(X)^n, & f_2 &= X^n, \\ g_1 &= X^n, & g_2 &= X^r P(X^n), \\ f_1 \circ f_2 &= g_1 \circ g_2 = X^{rn} P(X^n)^n. \end{aligned}$$

Ritt showed the following theorem for the complex number field $\mathbb{C}$.

Theorem 2 (First Ritt theorem). *If a polynomial f admits the two factorizations*

$$f = f_1 \circ \cdots \circ f_r = g_1 \circ \cdots \circ g_s$$

then the two sequences of degrees

$$\deg f_1, \ldots, \deg f_r; \quad \deg g_1, \ldots, \deg g_s$$

have the same length and include the same terms.

In 1974 Dorey and Whaples extended the theorem to any field under the condition that the degree of f does not divide the characteristic (otherwise it is wrong).

Ritt also proved the difficult result which follows.

THEOREM 3 (SECOND RITT THEOREM). *There are only two cases which give an equality*

$$f_1 \circ f_2 = g_1 \circ g_2$$

with

$$\deg f_1 = \deg g_2 = m, \quad \deg f_2 = \deg g_1 = n$$

and $(n, m) = 1$. *The first is that of the example above and the second is*

$$\begin{aligned} f_1 &= D_m, \quad f_2 = D_n \\ g_1 &= D_n, \quad g_2 = D_m \end{aligned}$$

where D_k *is defined by*

$$D_k(X + X^{-1}) = X^k + X^{-k}.$$

Polynomials D_k are connected to Chebychev polynomials but they are defined even in characteristic 2 contrary to the latter. Zannier proved last year that the theorem is right for all algebraically closed fields in all characteristic under the condition that the derivatives f_1', f_2', g_1', g_2' are not the zero polynomial.

3. Polynomials with sparse powers

In 1947 Rényi built a polynomial of degree 23 the square of which has fewer nonzero coefficients than the polynomial itself. That looks paradoxical but Erdös proved that there exist an infinity of polynomials f the number of nonzero coefficients of which, $N(f)$, satisfies

$$N(f^2) < N(f)^c$$

with $c < 1$. Verdenius computed in 1949 a possible value of c,

$$c = \frac{\log 8}{\log 13},$$

using Erdös proof. Coppersmith and Davenport gave analogous results

$$N(f^k) < N(f)^c$$

but without improvement of the constant c. They proved that for each polynomial F there are positive constants C and c with $c < 1$ such that for any integer $N \geq 1$ there is a polynomial f, whose degree is N, such that $N = N(f) - 1$ (the polynomial f is complete) and

$$N(F(f)) < C\, N(f)^c.$$

On the other hand Schinzel proved in 1987 that

$$N(f^2) \gg \log\log N(f).$$

The proof is valid for $N(f^k)$ too, but does not give an inequality. One could look for an inequality

$$N(F(f)) > \varphi(N(f)),$$

where F is a polynomial like $F(x) = x^3 - x$.

4. Factorization of trinomials

Schinzel studied the reducibility of the trinomial

$$X^n + A\,X^m + B.$$

He gave a complete result for the case when $A,\ B \in \mathbb{K}(y)$ and an incomplete result for the case $A,\ B \in \mathbb{K}$, where $\mathbb{K}$ is an algebraic number field. Then the problem is almost solved for finite extensions.

The trinomial is reducible if and only if the reciprocal trinomial $B\,X^n + A\,X^{n-m} + 1$ is reducible so one may suppose that $n \geq 2\,m$. The first theorem concerns fields $\mathbb{K}(y)$ where y is a vector of variables, $\mathbb{K}$ is a field of characteristic $\kappa \geq 0$ which does not divide the product $nm(n-m)$ and we call n_1 and m_1 the quotients $n/(n,m)$ and $m/(n,m)$ respectively.

THEOREM 4 (FIRST SCHINZEL THEOREM). *If A and B are in $\mathbb{K}(y)^*$ and $A^{-n}B^{n-m}$ is not in $\mathbb{K}$ then the trinomial $X^n + A\,X^m + B$ is reducible over $\mathbb{K}(y)$ if and only if*

- *$X^{n_1} + A\,X^{m_1} + B$ has a proper factor of degree less than or equal to 2,*
- *or there exists an integer l such as satisfies the two following conditions: first $\{n/l,\ m/l\}$, which we call $\{\nu,\ \mu\}$, is one of $\{6,\ 1\}$, $\{6,\ 2\}$, $\{7,\ 1\}$, $\{8,\ 2\}$, $\{8,\ 4\}$, $\{9,\ 3\}$, $\{10,\ 2\}$, $\{10,\ 4\}$, $\{12,\ 2\}$, $\{12,\ 3\}$, $\{12,\ 4\}$, $\{15,\ 5\}$ or of the type $\{2\,p,\ p\}$ with p a prime number; next*

$$A = u^{\nu-\mu}A_{\nu,\mu}(v), \qquad B = u^{\nu}B_{\nu,\mu}(v),$$

where $u,\ v$ are in $\mathbb{K}(y)$ and polynomials $A_{\nu,\mu}$, $B_{\nu,\mu}$ are given in Table 1.

$\nu,\ \mu$	$A_{\nu,\mu}$	$B_{\nu,\mu}$
$2\,p,\ p$	$-[(1+\sqrt{1-4\,v}/2]^p - [(1-\sqrt{1-4\,v}/2]^p$	v^p
$6,\ 1$	$8\,v(v^2+1)$	$(v^2+4\,v-1)(v^2-4\,v-1)$
$6,\ 2$	$4\,(v+1)$	$-v^2$
$7,\ 1$	$-(2\,v+1)^4(4\,v^2-3\,v+1)$ $\times\,(v^3-2\,v^2-v+1)$	$v(2\,v-1)(2\,v+1)^5$ $\times\,(3\,v-2)(v^2-v-1)$
$8,\ 2$	$-v^2+8\,v-8$	$4\,(v-1)^2$
$8,\ 4$	$2\,v^2-8\,v+4$	v^4
$9,\ 3$	$v^3-81\,v+243$	$27\,(v-3)^3$
$10,\ 2$	$4\,v^3-8\,v+4$	$-(v^2-4\,v+2)^2$
$10,\ 4$	$v^5(-v^3+8\,v-8)$	$-4\,v^8(v-1)^4$
$12,\ 2$	$1024\,(v-4)^8(2\,v-3)$ $\times\,(v^2-6\,v+6)(3\,v^2-3\,v+1)$	$1024\,(v-4)^{10}(v^3-8\,v+8)$
$12,\ 3$	$-729\,v(v-1)^7(2\,v-1)$ $\times\,(3v^2-6\,v+2)(3\,v^2-3\,v+1)$	$729\,(v-1)^9(3\,v^3-3\,v+1)$
$12,\ 4$	$512\,(2\,v-1)(2\,v^2+2\,v-1)$ $\times\,(2\,v^2-2\,v+1)$	$1024\,(2\,v^2-4\,v+1)^4$
$15,\ 5$	$5\,(5\,v-5)^7(5\,v^4-5\,v^3-5\,v^2+5\,v-1)$ $\times\,(5\,v^4-10\,v^3+100\,v^2-5\,v+1)$	$(5\,v-5)^{10}(5\,v^2-5\,v+1)^5$

TABLE 1. Trinomials $X^{\nu l} + u^{\nu-\mu}A_{\nu,\mu}(v)\,X^{\mu l} + u^{\nu}B_{\nu,\mu}(v)$ are reducible.

The theorem presents a complete analogy with Capelli's theorem in which there is an exceptional case $a = -4\,b^4$ and an infinite sequence of exceptions corresponding to $a = b^p$. The proof rests on the existence of a lower bound for the genus of a certain algebraic curve except in a finite number of cases. Once this bound is known, the problem is solved by a method of indeterminate coefficients.

Schinzel gave a theorem for the algebraic function fields but it is too technical to be cited here and another theorem for the algebraic number fields (finite extension of $\mathbb{Q}$). The latter is rather complicated and we only comment it. Like the first Schinzel theorem it gives a criterion to recognize reducible polynomials. The criterion is the disjunction of four conditions. The first two are similar to those of the preceding theorem. The third one looks like the second one with a list of pairs, $\{7,\ 2\}$, $\{7,\ 3\}$, $\{8,\ 1\}$, $\{9,\ 1\}$, $\{14,\ 2\}$, $\{21,\ 7\}$ and formulae

$$A = u^{\nu-\mu} A_{\nu,\mu}(v,w), \quad B = u^{\nu} B_{\nu,\mu}(v,w),$$

but here (v,w) is a point on an elliptic curve $E_{\nu,\mu}(\mathbb{K})$. All curves but one (namely $E_{7,2}$, whose equation is $w^2 = v^3 + 16\,v^2 + 64\,v + 80$) are given by their canonical form of Weierstrass. For example, the curve $E_{7,3}$ is defined by the equation $w^2 = v^3 - 675\,v + 13662$. In the end the fourth condition uses all pairs of integers and formulae

$$A = u^{\nu-\mu} A_0, \quad B = u^{\nu} B_0,$$

where (A_0, B_0) lies in a finite set $F_{\nu,\mu}(\mathbb{K})$. However the proof does not furnish a way to compute $F_{\nu,\mu}(\mathbb{K})$ for it is based on Falting's theorem which is ineffective.

For the rational number field $\mathbb{K} = \mathbb{Q}$ one knows twenty exceptional trinomials which are reducible but do not satisfy any one of the first three conditions. Among those is the polynomial

$$X^8 + 3\,X^3 - 1 = (X^3 + X - 1)(X^5 - X^3 + X^2 + X + 1).$$

One may expect that for each algebraic field $\mathbb{K}$ there is only a finite number of exceptions. That conjecture is very difficult to prove; it suffices to think of Fermat theorem in which there is only one simple curve and one parameter. Here the curves are complicated and there are several parameters.

If the conjecture is right there exists constant $C_1(\mathbb{K})$ such that a reducible trinomial $X^n + A\,X^m + B$ satisfies the first condition (it has a proper factor of degree less than or equal to 2) or the condition $n_1 \leq C_1(\mathbb{K})$. For $\mathbb{K} = \mathbb{Q}$ it needs $C_1(\mathbb{K}) \geq 17$ as shows the example

$$X^{17} + 103X + 56 = (X^3 - X^2 + X + 1)(X^{14} + X^{13} - 2\,X^{11} - \cdots + 9\,X^2 + 47\,X + 56).$$

As another consequence of the conjecture there exists constant $C_2(\mathbb{K})$ such that every polynomial has an irreducible factor with at most $C_2(\mathbb{K})$ nonzero coefficients. Breman asserts the constant has value greater than or equal to 8. Moreover Chauder and Schinzel gave an explicit example of this.

Bibliography

[1] Coppersmith (D.) and Davenport (J.). – Polynomials whose powers are sparse. *Acta Arithmetica*, vol. LVIII, n° 1, 1991.
[2] Schinzel (A.). – *Selected topics on polynomials.* – Ann Arbor, 1982.
[3] Schinzel (A.). – On the number of terms of a power of a polynomial. *Acta Arithmetica*, vol. 49, 1987, pp. 55–70.
[4] Schinzel (A.). – On reducible trinomials. *Dissertationes Mathematicae*, 1993. – To appear.
[5] Zannier (U.). – Ritt's second theorem in arbitrary characteristic. *Journal für die reine und angewandte Mathematik*, 1993. – To appear.