# On the Casas Alvero conjecture

Christiaan van de Woestijne
Institut für Mathematik und Statistik
Montanuniversität Leoben, Austria

Czech and Slovak International Conference on Number Theory
Stará Lesná, 6 September 2011

# A question

Let $\alpha \in \mathbb{C}$ and let $P$ be the polynomial $(X-\alpha)^d$, for some positive integer $d$. Then, also

$$P^{(k)}(\alpha) = 0 \qquad (k = 1, \ldots, d-1).$$

In other words, all derivatives $P^{(k)}$ share one or more factors $X - \alpha$ with $P$.

Conversely, let $P = a_0X^d + a_1X^{d-1} + \ldots + a_{d-1}X + a_d$ be a polynomial with complex coefficients, and suppose that it shares a factor with its derivatives $P', P'', \ldots, P^{(d-1)}$. (Not $P^{(d)}$, of course.)

Question: do we have $P = a_0(X-\alpha)^d$ for some $\alpha \in \mathbb{C}$?

# A conjecture

Eduardo Casas-Alvero

Eduardo Casas Alvero (professor of mathematics at the Universitat de Barcelona) came across this question in 1998 and asked many people if they could prove it. In April of this year, in an interview on the Spanish amateur mathematics blog Gaussianos.com, he wrote:

> [...] mi impresión es que debe ser cierto, y esta impresión parece compartida por bastantes colegas. De todos modos no hay que fiarse: mi primera impresión fue que además de cierto era fácil y ya ves como estamos...

Thus, after 12 years, the question is still open and is now called the Casas Alvero conjecture.

# Results

Gema Diaz Toca (Murcia) and Laureano Gonzalez Vega (Santander) in 2005 were able to prove the conjecture for degrees up to 8 (published up to 7), using heavy computations.

In a joint effort by Hans-Christian Graf v. Bothmer (Hannover), Oliver Labs (Saarbrücken), Josef Schicho (Linz) and myself in 2006, we could prove the conjecture when the degree is a prime power, and some other related cases.

A different proof, and a nice introduction to the problem, is given by Jan Draisma and Johan P. de Jong in the current issue of the EMS Newsletter.

The smallest unknown cases are degrees 12, 20, 24 and 28.

Let us see some of the arguments used to get these results.

# More general formulation

Let $K$ be a field and $P \in K[X]$ of degree $d$. We define the $k$th Hasse derivative of $P$ as

$$P_k = \binom{d}{k} a_0 X^{d-k} + \binom{d-1}{k} a_1 X^{d-k-1} + \ldots + \binom{k}{k} a_k X^0.$$

We have $P_k = k! \cdot P^{(k)}$, so using this gives a stronger conjecture when char $K < d$.

Definition. The field $K$ has the Casas Alvero property for degree $d$ (written CA$(K, d)$) if every $P \in K[X]$ of degree $d$ that has a common factor with $P_1, \ldots, P_{d-1}$ has the form $P = c(X - \alpha)^d$ (over an algebraic closure $\bar{K}$ of $K$).

Simplifications: (i) $P$ monic; (ii) $P(0) = 0$; (iii) $K = \bar{K}$.

Thus, we must prove: if $P \in K[X]$, monic, $P(0) = 0$, has a common factor with $P_1, \ldots, P_{d-1}$, then $P = X^d$.

# Simple cases; number theory

(i) $d = 1$: is trivial.
(ii) $d = 2$: CA$(K, 2)$ holds for all $K$.
(iii) $d = 3$: CA$(K, 3)$ holds whenever characteristic is not 2.
(iv) $d = p + 1$, $p$ prime: CA$(K, d)$ is false in characteristic $p$.

Counterexample: $X^{p+1} - X^p$.

Theorem Suppose $p^e || d$, for a prime $p$. Then

CA$(K, d/p^e)$ implies CA$(K, d)$ in characteristic $p$.

To prove the theorem, we use the following well-known result.

Lemma (Kummer/Lucas). Suppose $p^e || n$. If $p^e \nmid k$, then if $v_p(k) < v_p(n)$, then $\binom{n}{k} \equiv 0 \pmod{p}$; if $p^e | k$, then

$$\binom{n}{k} \equiv \binom{n/p^e}{k/p^e} \pmod{p}.$$

# Proof of the theorem

Let $K$ be a perfect field of characteristic $p$, and suppose $P \in K[X]$ monic of degree $d = np^e$, where $p \nmid n$, and $P(0) = 0$.

Consider $P_{d-1} = \binom{np^e}{np^e-1} X + a_1$. The leading coefficient is 0 in $K$, so if $P$ has a factor in common with $P_{d-1}$, we have $a_1 = 0$.

Now $P_{d-2} = \binom{np^e}{np^e-2} X^2 + \binom{np^e-1}{np^e-2} a_1 X + a_2 = a_2$. It follows that $a_2 = 0$.

We continue like this. If $p^e \nmid k$, then we find $a_k = 0$; if $p^e | k$, then $a_k$ is free, as $P_{d-k}$ is divisible by $X$.

It follows that $P = Q^{p^e}$ for some $Q \in K[X]$, and $P_{kp^e} = Q_k^{p^e}$, so also $\gcd(Q, Q_k)$ is nontrivial for all $k$.

# Resultants

For polynomials $P$ and $Q$, let Res$(P, Q)$ be the resultant. Recall that Res$(P, Q) = 0$ iff $P$ and $Q$ have a common factor.

If $P = \sum_{i=0}^{d} a_{d-i} X^i$ and $Q = \sum_{i=0}^{e} b_{e-i} X^i$, then

$$\text{Res}(P, Q) \in \mathbb{Z}[a_0, \ldots, a_d, b_0, \ldots, b_e].$$

Examples:

(i) Res$(X + a, X + b) = a - b$;
(ii) the discriminant of a monic $P$ is Res$(P, P')$, up to sign.

More generally, any sequence of $n + 1$ polynomials in $n$ variables has a well-defined resultant in the base field (ring) — it is nonzero if and only if the algebraic variety (scheme) defined by these polynomials is empty (has empty generic fibre). Projectively, one uses $n$ homogeneous polynomials in $n$ variables.

# The resultant variety

Let $R_k = \text{Res}(P, P_k)$, let $I(K,d) = (R_1, \ldots, R_{d-1})$, and let $V(K,d)$ be the algebraic variety

$$\left\{(a_1, \ldots, a_{d-1}) \in K^{d-1} \mid R_k(a_1, \ldots, a_{d-1}) = 0 \text{ for } k = 1, \ldots, d-1\right\}.$$

Note that if $(a_1, \ldots, a_{d-1}) \in V(K,d)$, then $(\lambda a_1, \ldots, \lambda^{d-1} a_{d-1}) \in V(K,d)$ for all $\lambda \in K$ — the ideal $I(K,d)$ is weighted homogeneous, if $a_i$ gets weight $i$.

Theorem. We have CA$(K,d)$ if and only if $V(K,d) = \{(0,0,\ldots,0)\}$.

By Hilbert's homogeneous Nullstellensatz, we find that CA$(K,d)$ holds if and only if $I(K,d)$ contains a power of $a_k$ for $k = 1, \ldots, d-1$. This can be verified in principle using Gröbner bases.

In practice: possible up to degree 8; for degree 12, impossible to compute the $R_k$!

# (Arithmetic) algebraic geometry

Resultants can be defined over $\mathbb{Z}$, so we can define the weighted projective $\mathbb{Z}$-scheme

$$X(d) \subseteq \mathbb{P}_{\mathbb{Z}}(1, 2, \ldots, d-1)$$

cut out by the equations $R_1, \ldots, R_{d-1}$.

Algebraic geometers tell me that the structure morphism

$$\phi : X(d) \to \operatorname{Spec} \mathbb{Z}$$

is projective, hence proper, hence closed, so

$$\phi(X(d)) \subseteq \operatorname{Spec} \mathbb{Z}$$

is closed. The complement of $\phi(X(d))$ is the set of points with empty fibre; it is open.

(Computing $\phi$ is very simple: we have $\phi(P) = P \cap \mathbb{Z}$.)

# (Arithmetic) algebraic geometry (2)

Note that

(i) CA($\overline{\mathbb{F}}_p, d$) $\iff$ $(p)$ has empty fibre;
(ii) CA($\overline{\mathbb{Q}}, d$) $\iff$ (0) has empty fibre.

Theorem If there exists a prime $p$ with CA($\overline{\mathbb{F}}_p, d$) true, then

(i) CA($K, d$) holds for all fields $K$ of characteristic 0;
(ii) for almost all primes $p$, CA($K, d$) holds for all fields of characteristic $p$.

Proof. If the complement of $\phi(X(d))$ is nonempty, it contains the generic point and almost all closed points.
Next, $X(d)$ is defined over $\mathbb{Z}$, so if it has no points over an algebraic closure of $\mathbb{Q}$ or $\mathbb{F}_p$, then there will be no points over bigger fields either. In other words: base change.

# Bad primes

In characteristic $p$, a counterexample to CA$(K, p+1)$ is given by $X^{p+1} - X^p$: every $P_k$ is divisible by either $X$ or $X-1$.

More generally, if the Casas Alvero conjecture holds for degree $d$ in characteristic 0, then there are only finitely many characteristics $p$ for which the conjecture is fails.

These can be found by computing (and factoring!) the multi-polynomial resultant of the ideal $I(\mathbb{Z}, d)$. They can be quite large.

For example, the Casas Alvero conjecture holds in characteristic 0 for degree 6. However, the polynomial

$$P = X^6 + 3144481702696843X^4 + X^3 + 2707944513497181X^2$$

is a counterexample in characteristic 7390044713023799.

# Other results

Draisma and De Jong (2011) gave a proof using valuation theory instead of algebraic geometry.

They also proved: given $(k_i, m_i)$ for $i = 1, \ldots, d-2$, with $1 \leq k_i \leq d-1$ and $1 \leq m_i \leq d-k_i$, there exists $P \in \mathbb{R}[X]$, having only real roots, such that the $m_i$-th root (counted in ascending order of the real line, with multiplicity) of $P_{k_i}$ is common with $P$, for all $i$.

Some easy applications of the Gauss-Lucas theorem are the following. If $P \in \mathbb{C}[X]$ violates the conjecture, then

(i) $P$ has at least 3 distinct roots (possibly at least 4);

(ii) $P$ has at most $d-1$ distinct roots.

# Conclusions

Using these techniques and variations thereof, we can prove CA$(K, d)$ for fields $K$ of characteristic 0 when $d$ is a prime power or twice a prime power, three times a power of an odd prime, four times a power of a prime greater than 7, etcetera. The smallest open cases are $d = 12$, 20, 24, and 28.

Literature:

(i) G. Diaz Toca and L. Gonzalez Vega, *On a conjecture about univariate polynomials and their roots.* In A. Dolzmann, A. Seidl, and T. Sturm (eds.), *Algorithmic Algebra and Logic 2005*, pages 83–90, Norderstedt, Germany, 2005.

(ii) H.C. Graf v. Bothmer, O. Labs, J. Schicho and C. van de Woestijne, *The Casas-Alvero conjecture for infinitely many degrees*, J.Alg. **316** (2007) 224–230.

(iii) J. Draisma and J.P. de Jong, *On the Casas-Alvero conjecture*, Newsletter of the EMS **80** (June 2011) 29–33.