Universidad de Concepción
Dirección de Postgrado
Facultad de Ciencias Físicas y Matemáticas -Programa de Magíster en Matemática

Potencias en subsucesiones de progresiones aritméticas en anillos de funciones y un problema de indecidibilidad

(Powers in subsequences of arithmetic progressions in rings of functions and a problem of undecidability)

NATALIA CRISTINA GARCÍA FRITZ
CONCEPCIÓN-CHILE
2011

Profesor Guía: Xavier Vidaux
Dpto. de Matemática, Facultad de Ciencias Físicas y Matemáticas
Universidad de Concepción

Introduction and Main Results

This thesis consists of two main theorems (Theorems 2 and 6) on the arithmetic of polynomials and some consequences in Mathematical Logic.

A simple corollary of our first main theorem, inspired by a paper on powers in arithmetic progressions by Hajdu [10], states in particular that given any field F

the quantity $a\lambda+b$, where a and b are coprime polynomials in $F[t]$, cannot be a power in $F[t]$ for more than $M = 4$ distinct values of $\lambda \in F$, unless both a and b have zero derivative.

Here by *power*, we mean *a k-th power for some $k \geq 2$*. This corollary was actually our very first result and inspired the rest of the thesis. On the one hand, one could naturally try to generalize it in the following ways:

1. Is the condition on coprimality really necessary? If not, how *small* should the degree of the greatest common divisor of a and b be in order to ensure the existence of an M (guessing that the more a and b have factors in common, the bigger should be M);

2. What about other rings of functions? (such that subrings of function fields, rings of analytic or meromorphic functions, ...)

3. What about considering expressions of the form $a\lambda^2 + b\lambda + c$ instead of $a\lambda + b$? What about higher powers?

In the work presented here, we deal with generalizations of type 1 (Theorem 2) and of type 3 (Theorem 6).

On the other hand, the statement above and its possible generalizations *should* say something about the first order language $\mathcal{L}_P = \{0, 1, +, P\}$ (or languages containing $\mathcal{L}_P$), where P is a unary relation symbol and $P(x)$ is interpreted as "x is a power".

Though to the best of our knowledge this language has not been previously studied by logicians (though Macintyre's language [12] is somewhat related to it, as it contains a predicate P^k for each $k \geq 2$ interpreted as "$P^k(x)$ if and only if x is a k-th power"), the study of consecutive powers and powers in arithmetic progression over the integers has a long history. In 1640, Fermat conjectured that there does not exist four squares in arithmetic progression, and this was proved later on by Euler. A few centuries

later, in 1844, Catalan [3] conjectured that the only consecutive powers are 8 and 9. In 1997, Darmon and Merel [6] proved that there does not exist three k-th powers in arithmetic progression with k greater than or equal to 3, completing the study of arithmetic progressions formed by powers with the same exponent. Nowadays, the study is focusing in arithmetic progressions formed by powers without the restriction of having the same exponent. In 2004, Hajdu [10] proved under the ABC conjecture that if

$$(x_1^{l_1}, x_2^{l_2}, \ldots, x_k^{l_k})$$

is an arithmetic progression with x_1 and x_2 coprime and $l_i \geq 2$ for every i, then k and $\max\{l_i\}$ are bounded (not depending on the x_i). He also proves, unconditionally, that if there exists a constant C greater than every l_i, then k is bounded.

Let us introduce some notation before we state our main results.

Notation 1. *1. If F is a field, we denote by $\tilde{F}$ the algebraic closure of F.*

2. *If a is a polynomial, we will write a' for the formal derivative of a and* $\deg(a)$ *for the degree of a.*

3. *If a and b are polynomials over a field F, we write* $\gcd(a,b)$ *for the (monic) greatest common divisor of a and b in F, and* $\operatorname{lcm}(a,b)$ *for the (monic) least common multiple of a and b in F.*

4. *If r is a real number, the notation $\lceil r \rceil$ will refer to the ceiling function applied to r (this is the smallest integer which is greater than or equal to r).*

5. *Given $a, b \in F[t]$, we will write*

$$\gamma(a,b) = \frac{\deg(\gcd(a,b))}{\max\{\deg(a), \deg(b)\}}$$

and refer to it as to the index of coprimality of a and b. *Observe that $0 \leq \gamma(a,b) \leq 1$ measures precisely how far are a and b of being coprime: the closer $\gamma(a,b)$ is to 0, the less factors a and b have in common, and the closer $\gamma(a,b)$ is to 1, the more factors a and b have in common. Note that $\gamma(a,b)$ does not vary with the base field considered (as the greatest common divisor depends only on the prime field of F).*