Simplifying polynomials in one variable using quadratic form theory.

University of British Colombia

Sylvain Gaulhiac, under the supervision of Zinovy Reichstein

Summer 2014

Research Report

This summer I worked with Professor Zinovy Reichstein at UBC on a project concerning the simplification of a polynomial in one variable using quadratic form theory. More precisely, we try to simplify the minimal polynomial of a generator of a finite separable field extension, in a 'general' framework. It is related to the isotropy or anisotropy of the trace form over a finite separable extension. We used quadratic form theory, Galois theory, finite group theory and general algebra. This problem can also be tackled using methods from algebraic geometry like invariant theory.

Let $n \geq 3$ be an integer, and k a field. One can define the field $K = k(a_1, \ldots, a_n)$ where $a_1, \ldots, a_n$ are algebraically independent variables over k.

Let $P(X) = X^n + a_1 X^{n-1} + \ldots + a_n \in K[X]$ be the 'general polynomial' of degree n. P is an irreducible polynomial over K, so that

$$L := \frac{K[X]}{(P)}$$

is a field.

If X_1 denotes the image of X over the natural projection $K[X] \to L$, then $L = K(X_1)$, the degree of the field extension L/K is n, and P is the minimal polynomial of X over K. Let Y be another generator of L over K, and $Q := X^n + b_1 X^{n-1} + b_2 X^{n-2} + \ldots + b_n \in K[X]$ its minimal polynomial. The question we ask here is whether one can find Y such that $b_1 = b_2 = 0$.

Furthermore, we have :

$$\begin{cases} tr(Y) = -b_1 \\ tr(Y^2) = {b_1}^2 - 2b_2 \end{cases}$$

Therefore, if $\mathrm{char}(K) \neq 2$, the condition $b_1 = b_2 = 0$ is equivalent to

$$tr(Y) = tr(Y^2) = 0$$

The aim of the work is to prove the following result :

THEOREM 0.1. *Let k be a field such that* $\mathrm{char}(k) \nmid 2n$*, and let K and L the fields defined as above. Let write $n = \sum_{i=1}^{r} 2^{n_i}$ with $n_i \neq n_j$ when $i \neq j$. Then there exists a generator y of L over K such that $tr_{L/K}(y) = tr_{L/K}(y^2) = 0$ if and only if the polynomial system*

$$\sum_{i=1}^{r} 2^{n_i} y_i^2 = 0$$

$$\sum_{i=1}^{r} 2^{n_i} y_i = 0$$

has a non zero solution $(y_1, \ldots, y_r)$ in k^r.

COROLLARY 0.2. *Let k be a field such that* $\mathrm{char}(k) \nmid 2n$*, and let K and L be as above.*

1. *If n can be written $n = 2^m$ or $n = 2^{m_1} + 2^{m_2}$, with $m, m_1, m_2 \in \mathbb{N}$ then the answer is negative : it is impossible to find a generator Y satisfying the condition $tr_{L/K}(Y) = tr_{L/K}(Y^2) = 0$.*
2. *Otherwise, when k contains the quadratic closure of its prime subfield (i.e. when k contains a square root of every element of its prime subfield) there exists a generator $Y \in L^*$ such that $b_1 = b_2 = 0$, which is equivalent to $tr(Y) = tr(Y^2) = 0$.*

BIBLIOGRAPHY

[Lam] T.Y. LAM.— *Introduction to quadratic forms over fields*, Graduate Studies in Mathematics Volume 67, American Mathematical Society.

[Rei] Z. REICHSTEIN.— *On a theorem of Hermite and Joubert*, Canad. J. Math. 51 (1999), 69-95.

[K-R] Z. REICHSTEIN and D.S. KANG.— *Trace forms of Galois field extensions in the presence of roots of unity*, J. reine angew. Math. 549 (2002), 79-89.

SYLVAIN GAULHIAC, STUDENT AT THE ECOLE NORMALE SUPÉRIEURE DE RENNES.