Proc. Indian Acad. Sci. (Math. Sci.), Vol. 109, No. 3, August 1999, pp. 231–239.

Equations of similitude

SHREERAM S ABHYANKAR and PAUL A LOOMIS

Mathematics Department, Purdue University, West Lafayette, IN 47907, USA
E-mail: ram@cs.purdue.edu; loomisp@math.purdue.edu

MS received 8 September 1998; revised 3 December 1998

Abstract. A general technique is developed to enlarge the Galois group of an equation from a subgroup of a finite classical isometry group towards the corresponding similitude group.

Keywords. Galois group; equation; isometry; similitude.

1. Introduction

In [Ab3, Ab4, Ab5], explicit equations were given whose Galois groups were the symplectic, orthogonal, and unitary groups $\mathrm{Sp}(2m,q)$, $\Omega^-(2m,q)$, and $\mathrm{SU}(2m-1,q')$, where $m>1$ is an integer and $q>1$ is a power of a prime p; in the unitary case $q=q'^2$ where $q'>1$ is a power of p. We shall now modify these equations so as to enlarge their Galois groups towards the corresponding similitude groups $\mathrm{GSp}(2m,q)$, $\mathrm{GO}^-(2m,q)$, and $\mathrm{GU}(2m-1,q')$. In § 2 we shall review the definitions of these finite classical groups. In § 3 we shall refine the composite polynomial lemma (2.4) of [Ab2] describing the Galois group of the composition of two polynomials. In § 4, the enlargement principle will be deduced as a consequence of this. In § 5, 6, and 7, the said principle will be applied to get the modified equations in the symplectic, orthogonal, and unitary cases respectively.

2. Review of classical groups

Recall that for any integer $n>0$, the general linear group $\mathrm{GL}(n,q)$ is the group of all nonsingular n by n matrices over the field $\mathrm{GF}(q)$ of cardinality q. Likewise, for an n-dimensional $\mathrm{GF}(q)$-vector-space V, the group of all $\mathrm{GF}(q)$-linear bijections $V\to V$ is denoted by $\mathrm{GL}(V)$. Moreover, for any basis $\beta=(\beta_1,\ldots,\beta_n)$ of V, we get a $\mathrm{GF}(q)$-linear bijection $\Lambda_\beta: V\to \mathrm{GF}(q)^n$ given by $\Lambda_\beta(\alpha_1\beta_1+\cdots+\alpha_n\beta_n)=(\alpha_1,\ldots,\alpha_n)$ for all $\alpha_1,\ldots,\alpha_n$ in $\mathrm{GF}(q)$, and this induces an isomorphism $\Lambda_\beta^*:\mathrm{GL}(V)\to\mathrm{GL}(n,q)$. Likewise, any $\mathrm{GF}(q)$-linear bijection $\Lambda: V\to V^\sharp$, where $V^\sharp$ is any other n-dimensional $\mathrm{GF}(q)$-vector-space, induces an isomorphism $\Lambda^*:\mathrm{GL}(V)\to\mathrm{GL}(V^\sharp)$. By $\mathrm{HL}(V)$ we denote the group of all homotheties of V, i.e., members of $\mathrm{GL}(V)$ of the form $v\mapsto\gamma v$ with $0\neq\gamma\in\mathrm{GF}(q)$, and by $\Theta_V:\mathrm{GL}(V)\to\mathrm{PGL}(V)$ we denote the canonical epimorphism where $\mathrm{PGL}(V)=\mathrm{GL}(V)/\mathrm{HL}(V)$. Likewise, by $\mathrm{HL}(n,q)$ we denote the group of all nonsingular n by n scalar matrices over $\mathrm{GF}(q)$, and by $\Theta_n:\mathrm{GL}(n,q)\to\mathrm{PGL}(n,q)$ we denote the canonical epimorphism where $\mathrm{PGL}(n,q)=\mathrm{GL}(n,q)/\mathrm{HL}(n,q)$. For any sub-

Abhyankar's work was partly supported by NSF grant DMS 97-32592 and NSA grant MDA 904-97-1-0010, and Loomis's work was partly supported by a Sloan Doctoral Dissertation Fellowship.