Journal of Symbolic Computation 71 (2015) 73–97

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

# Computing Galois groups of polynomials (especially over function fields of prime characteristic)

Nicole Sutherland

*Computational Algebra Group, School of Mathematics and Statistics, University of Sydney, Australia*

ARTICLE INFO

*Article history:*
Received 27 June 2014
Accepted 25 September 2014
Available online 2 October 2014

*MSC:*
11R32

*Keywords:*
Galois groups
Function fields

ABSTRACT

We describe a general algorithm for the computation of Galois groups of polynomials over global fields from the point of view of using it to compute Galois groups of polynomials over function fields with prime characteristic, including characteristic 2 in which some invariants which are efficient to use in other characteristics are invariant for too large a group. We state new invariants for most of these situations when the characteristic is 2. We also describe the use of this algorithm for computing Galois groups of reducible polynomials over both number fields and function fields.

## 1. Introduction

There are a number of algorithms available for computing Galois groups and some of these algorithms have been known for some time. Chronologically each algorithm published has increased the degrees of the polynomials it accepts as input. A limitation on degrees has been due to the use of tabulated information. Geißler (2003) provides an algorithm for Galois groups of polynomials of degree at most 23 over $\mathbb{Q}$ and $k(t)$. This was the most recent work on algorithms for Galois groups when Fieker and Klüners (2014) developed their algorithm for Galois groups of polynomials. Unlike most previous algorithms the algorithm of Fieker and Klüners (2014) is not degree restricted (Hulpke, 1999, is not degree restricted either, however, it usually cannot determine the Galois group uniquely), and it can compute the Galois group of any polynomial over any algebraic number field or algebraic function field (including of course $\mathbb{Q}$ and $k(t)$ for $k = \mathbb{F}_q, \mathbb{Q}$). It has been implemented in Magma

*E-mail address:* nicole.sutherland@sydney.edu.au.

http://dx.doi.org/10.1016/j.jsc.2014.09.043
0747-7171/© 2014 Elsevier Ltd. All rights reserved.

(Cannon et al., 2010) V2.13 for polynomials over $\mathbb{Q}$ and in V2.14 for polynomials over number fields and $\mathbb{Q}(t)$.

We describe here the algorithm of Fieker and Klüners (2014) which we have implemented in Magma (Cannon et al., 2010) for polynomials over $\mathbb{F}_q(t)$ (V2.16) and global algebraic function fields (simple extensions of $\mathbb{F}_q(t)$) (V2.17). This is the first implementation, of which we know, of an algorithm for computing Galois groups over global function fields which is not restricted by the degree of the polynomial. It is also the first algorithm (that we know of) which uses the computation of subfields (and in particular the generating subfields as introduced by van Hoeij et al., 2011) of global function fields in calculating the Galois group. This algorithm is based on Stauduhar (1973).

A particular difficulty in generalizing (Fieker and Klüners, 2014) is that the invariants they provide for some groups $G$ and $H$ are $S_n$-invariant when the characteristic is 2 and so are never $G$-relative $H$-invariants (Definition 2). For such groups $G$ and $H$ we state in this paper (Section 3.5) some new polynomials which are $G$-relative $H$-invariant when the characteristic is 2. These invariants are a key part of the paper.

We will first give an overall view of the algorithm and then expand on the details from the point of view of using this algorithm to compute Galois groups of polynomials over global function fields. We also mention how this algorithm can be used to compute Galois groups of reducible polynomials over algebraic number fields and global algebraic function fields.

We begin with some definitions.

**Definition 1.** The *Galois group*, $\mathrm{Gal}(f)$, of a polynomial $f$ over a field $F$ is the automorphism group of $S_f/F$ where $S_f$ is the splitting field of $f$ over $F$.

When $f$ is irreducible over $F$ and of degree $n$ we compute Galois groups as transitive subgroups of $S_n$.

Invariants and resolvents are an important part of our algorithm. We define invariants and resolvents here and discuss the uses of the different types later. Let $R$ be a commutative unitary domain and $I(x_1, \dots x_n) \in R[x_1, \dots x_n]$. A permutation $\tau \in S_n$ acts on $I$ by permuting $x_1 \dots, x_n$ and we write $I^\tau$ for this action.

**Definition 2.** A polynomial $I(x_1, \dots, x_n) \in R[x_1, \dots, x_n]$ such that $I^\tau = I$ for all $\tau \in H$ for some group $H \subseteq S_n$ is said to be *$H$-invariant*.

An $H$-invariant polynomial $I(x_1, \dots, x_n) \in R[x_1, \dots, x_n]$ is a *$G$-relative $H$-invariant* polynomial if $I^\tau \neq I$ for all $\tau \in G \setminus H$, $H \subset G \subseteq S_n$, that is, for the stabilizer in $G$ we have $\mathrm{Stab}_G\, I = H$.

For a $G$-relative $H$-invariant polynomial $I$ we can compute a $G$-relative $H$-invariant *resolvent polynomial*

$$Q_{(G,H)}(y) = \prod_{\tau \in G//H} \big(y - I^\tau(x_1, \dots, x_n)\big),$$

where $G//H$ denotes a system of representatives for the right cosets $H\tau$ of $G/H$. If $G = S_n$ then we call $Q$ an *absolute resolvent*, otherwise we call $Q$ a *relative resolvent*.

An $S_n$-relative $H$-invariant is a $G$-relative $H$-invariant and a $G$-relative $H$-invariant is an $H$-invariant but the converse is not always true.

We recall the definition of a block system as found in Geißler and Klüners (2000, Definition 2.14), as it is crucial to the definition of a number of our special invariants.

**Definition 3.** Let $G$ be a transitive permutation group acting on a finite set $\Omega$. A subset $\emptyset \neq \Delta \subset \Omega$ is called a *block* if $\Delta \cap \Delta^\sigma \in \{\emptyset, \Delta\}$ for all $\sigma \in G$. The orbit of a block $\Delta$ under $G$ is called a *block system*.

The blocks we use will be subsets of $\Omega = \{\text{roots of } f\}$. A block system of a group $G$ is a block system for the transitive subgroups of $G$ but the converse does not always hold.