# Computing Galois groups by specialisation

Martin Bright[*]

24 March 2004

**Abstract**

The Galois group of an extension generated over $\mathbb{Q}$ by several fourth roots is obvious when those fourth roots are sufficiently general. If we wish to compute the Galois group in a collection of specific cases, though, generic algorithms become inefficient. We give an algorithm consisting mostly of linear algebra which computes not only the global Galois group but also the local decomposition groups, as subgroups of the generic Galois group.

## 1  Introduction

What is the Galois group of the field extension

$$\mathbb{Q}(\epsilon, \sqrt[4]{a_1}, \sqrt[4]{a_2}, \sqrt[4]{a_3})/\mathbb{Q}, \tag{1}$$

where $\epsilon$ is a primitive eighth root of unity and $a_i$ are given non-zero rational numbers?

This question arose when studying the cohomology of a family of surfaces over $\mathbb{Q}$ parametrised by the $a_i$, namely the diagonal quartics

$$a_0 X_0^4 + a_1 X_1^4 + a_2 X_2^4 + a_3 X_3^4 = 0.$$

Kummer theory tells us that, after adjoining a fourth root of unity $i$ to $\mathbb{Q}$, the rest of the extension is Abelian. Indeed, when the $a_i$ are "sufficiently general" (meaning that they are independent elements of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^4$), the answer is totally straightforward. However, naïvely to use a standard number theory package to compute anew the Galois group of this extension for each specific choice of the $a_i$ is extremely inefficient. The object of this note is to demonstrate a simple algorithm, essentially linear algebra, for finding the Galois group, and its action on the generators of the extension, for arbitrary $a_i$. We further show how to find the decomposition group at any prime.

We begin by fixing some notation. The Galois theory of étale extensions of rings, as described in [Grothendieck 1971, Exposé V], allows us to view this problem as one of specialisation. Let $A$ be the ring

$$A = \mathbb{Q}[s_1^\pm, s_2^\pm, s_3^\pm]$$

generated over $\mathbb{Q}$ by three transcendental elements $s_1, s_2, s_3$ and their inverses. Let $U = \operatorname{Spec} A$; then $U$ is the subset of three-dimensional affine space defined by $s_1 s_2 s_3 \neq 0$. The $\mathbb{Q}$-valued points of $U$ will correspond to triples $(a_1, a_2, a_3)$ of parameters in (1). Let $B$ be the ring

$$B = \mathbb{Q}(\epsilon)[t_1^{\pm}, t_2^{\pm}, t_3^{\pm}]$$

and let $V = \operatorname{Spec} B$. Define the map $\pi : V \to U$ by $t_i = s_i^4$. Then $\pi$ is étale. The automorphism group $G$ of $\pi$ is the same as that of the field extension $\mathbb{Q}(V)/\mathbb{Q}(U)$, which by Kummer theory is of order 256, generated by five elements as follows:

$$
\begin{aligned}
\sigma_1 &: t_1 \mapsto it_1 \\
\sigma_2 &: t_2 \mapsto it_2 \\
\sigma_3 &: t_3 \mapsto it_3 \\
\sigma_4 &: \sqrt{2} \mapsto -\sqrt{2} \\
\tau &: i \mapsto -i
\end{aligned}
\tag{2}
$$

where each generator fixes those of $\{t_1, t_2, t_3, \sqrt{2}, i\}$ not mentioned. The multiplication in $G$ is as follows: all the $\sigma_i$ commute with each other, and $\tau\sigma_i = \sigma_i^{-1}\tau$.

Let $a = (a_1, a_2, a_3)$ be a $\mathbb{Q}$-valued point of $U$. Then $\pi^{-1}a$ consists of finitely many points of $V$, which are permuted by the action of $G$; let $b$ be one such point. The *decomposition group* $G_b$ is by definition the stabiliser of $b$ in $G$; it is isomorphic in an obvious way to $\operatorname{Gal}(k(b)/k(a))$, which is the Galois group of the extension (1). A different choice of $b$ gives a conjugate decomposition group; this corresponds to a different choice of the various roots in the field extension. The problem is now, given $a$, to find $G_b$.

Let $X$ be the following subgroup of $B^{\times}$:

$$X = \langle (1+i), \sqrt{2}, t_1, t_2, t_3 \rangle.$$

We write $Y$ for $X/(X \cap A^{\times})$, an Abelian group of order 512. Let $\mu_4$ denote the group of fourth roots of unity in $\bar{\mathbb{Q}}$. The action of $G$ on $X$ gives us a map

$$\phi : G \to \operatorname{Hom}(Y, \mu_4), \qquad g \mapsto (x \mapsto gx/x).$$

Note that $\phi$ is not a homomorphism, but rather a crossed homomorphism. Now let $\beta : B \to \bar{\mathbb{Q}}$ denote the evaluation map of the point $b$; then $\beta$ induces maps $Y \to \bar{\mathbb{Q}}^{\times}/\mathbb{Q}^{\times}$ and hence

$$\beta^* : \operatorname{Hom}(\bar{\mathbb{Q}}^{\times}/\mathbb{Q}^{\times}, \mu_4) \to \operatorname{Hom}(Y, \mu_4).$$

**Proposition 1.** *The decomposition group $G_b$ is described as*

$$G_b = \phi^{-1}(\operatorname{im} \beta^*).$$

## 2 Proof of Proposition 1

The following is easily checked:

**Lemma 2.** *The map $\phi$ is injective, and its image consists of those elements of $\operatorname{Hom}(Y, \mu_4)$ which take $(1+i)$ to either $1$ or $-i$.* $\qquad\square$

**Lemma 3.** *Let $H$ be any subgroup of $G$. Then $B^H$ is generated as an $A$-module by $X^H = X \cap B^H$.*

*Proof.* As an $A[G]$-module, $B$ splits as a direct sum of 128 submodules, each of the form

$$B_x = Ax + Aix$$

for some $x = t_1^{n_1} t_2^{n_2} t_3^{n_3} \sqrt{2}^{n_4}$. The $G$-action on $B_x$ factors through a subgroup of the dihedral group of order 8 generated by $x \mapsto ix$ and $i \mapsto -i$. It is easily checked that the fixed space of each subgroup of this dihedral group is one of

$$\{0\}, \quad B_x, \quad Ax, \quad Aix, \quad A(1+i)x, \quad A(1-i)x$$

all of which are generated by elements in $X$. $\qquad\square$

**Lemma 4.** *Let $a$ be a point of $U$, $b$ a point of $V$ lying above $a$, and $\beta : B \to \bar{\mathbb{Q}}$ the homomorphism corresponding to $b$. Then*

$$G_b = \mathrm{Stab}_G(X \cap \beta^{-1}(\mathbb{Q})).$$

*Here $\mathrm{Stab}_G(S)$ means the set of elements of $G$ fixing pointwise the set $S$.*

*Proof.* By Galois theory, $B^{G_b}$ is the largest subring of $B$ on which $\beta$ restricts to a $\mathbb{Q}$-valued point; in other words,

$$B^{G_b} = \beta^{-1}(\mathbb{Q}).$$

Furthermore, $G_b$ is precisely the stabiliser of $B^{G_b}$. But by Lemma 3, $B^{G_b}$ is generated as an $A$-module by

$$X^{G_b} = X \cap \beta^{-1}(\mathbb{Q})$$

and so the stabilisers are the same. $\qquad\square$

*of Proposition 1.* The stabiliser of $X \cap \beta^{-1}(\mathbb{Q})$ consists of those $g \in G$ such that $gx/x = 1$ for all $x$ in that set; in other words,

$$G_b = \phi^{-1} \ker(\mathrm{Hom}(Y, \mu_4) \to \mathrm{Hom}(\ker(Y \xrightarrow{\beta} \bar{\mathbb{Q}}^\times/\mathbb{Q}^\times), \mu_4)).$$

But Hom is left exact, so the sequence

$$\mathrm{Hom}(\bar{\mathbb{Q}}^\times/\mathbb{Q}^\times, \mu_4) \xrightarrow{\beta^*} \mathrm{Hom}(Y, \mu_4) \to \mathrm{Hom}(\ker(Y \xrightarrow{\beta} \bar{\mathbb{Q}}^\times/\mathbb{Q}^\times), \mu_4)) \to 0$$

is exact, giving the result. $\qquad\square$

# 3  Implementation

Proposition 1 is very easy to apply in practice. We assume that the $a_i$ are sufficiently small that they may easily be factorised. We may replace $\bar{\mathbb{Q}}^\times/\mathbb{Q}^\times$ by a finite subgroup, in which $\beta(Y)$ is contained.

If $k$ is a global field and $S$ a finite set of primes of $k$ including all of the infinite primes, let $k_S$ denote the group of $S$-units of $k$.

**Definition 5.** For any field $k$, define

$$\sqrt[4]{k} := \{x \in \bar{k}^\times \mid x^4 \in k\}.$$

If $k$ is a global field and $S$ a finite set of primes in $k$, define

$$\sqrt[4]{k_S} := \{x \in \bar{k}^\times \mid x^4 \in k_S\}.$$

It is clear that the image of $\beta : Y \to \bar{\mathbb{Q}}^\times/\mathbb{Q}^\times$ lies in $\sqrt[4]{\mathbb{Q}_S}/\mathbb{Q}_S$, where $S$ is the set of primes dividing the $a_i$ together with $2$ and $\infty$.

The structure of $\sqrt[4]{k}/k^\times$ is straightforward:

**Lemma 6.** *Let $k$ be a field.*

- *If $k$ contains a primitive fourth root of unity, then $\sqrt[4]{k}/k^\times$ is isomorphic to $k^\times/(k^\times)^4$.*

- *If $k$ does not contain a primitive fourth root of unity, then there is an exact sequence*

$$0 \to \mu_4/\mu_2 \to \sqrt[4]{k}/k^\times \to k^\times/(k^\times)^4 \to 0.$$

*If $k$ is a global field and $S$ a finite set of primes of $k$ including all the infinite primes, then the statements hold if we replace $k^\times$ by $k_S$.*

*Proof.* The sequence

$$0 \to \mu_4 \to \sqrt[4]{k} \xrightarrow{x \mapsto x^4} k^\times \to 0$$

is exact, by definition of $\sqrt[4]{k}$. Taking the tensor product with $\mathbb{Z}/4\mathbb{Z}$ gives a (not very) long exact sequence:

$$0 \to k^\times[4] \to \mu_4 \to \sqrt[4]{k}/k^\times \to k^\times/(k^\times)^4 \to 0$$

which proves both cases. Replacing $k^\times$ by $k_S$ changes nothing. $\qquad\square$

## 3.1 Computing the global Galois group

The algorithm for computing the Galois group of the extension (1) is now as follows.

1. Factorise the $a_i$ and let $S$ be the set of primes dividing any of them, together with $2$ and $\infty$.

2. Construct the finite Abelian groups $Y$ and $\sqrt[4]{\mathbb{Q}_S}/\mathbb{Q}_S$, together with the map $\beta$ between them defined by $t_i \mapsto \sqrt[4]{a_i}$ (with some arbitrary choice of fourth roots).

3. Apply the functor $\mathrm{Hom}(\cdot, \mu_4)$ to get

$$\mathrm{Hom}(\sqrt[4]{\mathbb{Q}_S}/\mathbb{Q}_S, \mu_4) \xrightarrow{\beta^*} \mathrm{Hom}(Y, \mu_4).$$

4. Compute (generators for) the image of $\beta^*$.

5. Compute generators for $\phi^{-1}(\operatorname{im}\beta^*)$.

All these steps are easily accomplished using a computer algebra system such as MAGMA [Bosma et al. 1997]. An implementation is available on the author's web site [Bright 2003].

The final step merits some explanation. It is clear how to write down a left inverse for $\phi$ and hence compute the inverse image of any element. As $\phi$ is not a homomorphism, it is not immediately clear how to compute the inverse image of a subgroup. But $G$ is quite close to being Abelian, in that it has an Abelian subgroup $G'$ of index 2, generated by the $\sigma_i$. On $G'$, $\phi$ restricts to a homomorphism. The image $\phi(G')$ consists of those elements of $\operatorname{Hom}(Y, \mu_4)$ whose kernel contains $(1+i)$.

**Lemma 7.** *Let $H$ be a subgroup of $\operatorname{Hom}(Y, \mu_4)$. A set of generators for $\phi^{-1}H$ is given by*

- *the inverse images of a set of generators for $H \cap \phi(G')$, together with*

- *the inverse image of any element $h$ of $H$ such that $h(1+i) = -i$, if such an element exists.*

*Proof.* Since $G'$ is of index 2, any subgroup $I$ of $G$ is generated by $I \cap G'$ together with any one element of $I$ not contained in $G'$. $\qquad\square$

If there is an element $h$ in $H$ with $h(1+i) = -i$, then either such an element or its inverse must occur in any set of generators of $H$. We can thus compute $\phi^{-1}H$ easily from a set of generators for $H$.

## 3.2 Computing local Galois groups

The algorithm may be extended to compute the decomposition group of the extension (1) at a prime $p$, as a subgroup of the global Galois group. Note that some care needs to be taken to use the same choice of fourth roots as when computing the global Galois group. We simply replace $\beta$ by the composite map

$$Y \xrightarrow{\beta} \sqrt[4]{\mathbb{Q}_S}/\mathbb{Q}_S \to \sqrt[4]{\mathbb{Q}_p}/\mathbb{Q}_p^\times.$$

Here the last group is again finite and can be computed by MAGMA using Lemma 6 (see Bright [2003]).

# 4 Example

As an example, we will compute the Galois group over $\mathbb{Q}$ of

$$K = \mathbb{Q}(\epsilon, \sqrt[4]{-4}, \sqrt[4]{3}, \sqrt[4]{24})$$

together with its action on $K$.

The group $Y$ is generated by the five elements

$$(1+i), \sqrt{2}, t_1, t_2, t_3$$

and an element of $\operatorname{Hom}(Y, \mu_4)$ will be written as a row vector containing the images of these generators, for example $(1, 1, i, -1, i)$.

The set $S$ of primes contains $\infty$, 2 and 3; Lemma 6 shows that $\sqrt[4]{\mathbb{Q}_S}/\mathbb{Q}_S$ is isomorphic to $(\mathbb{Z}/4\mathbb{Z})^3$, generated by $\epsilon$ and fourth roots of 2 and 3. Again, an element of $\mathrm{Hom}(\sqrt[4]{\mathbb{Q}_S}/\mathbb{Q}_S, \mu_4)$ will be written as a row vector.

The map $\beta : Y \to \sqrt[4]{\mathbb{Q}_S}/\mathbb{Q}_S$ is as follows:

$$(1+i) \mapsto \epsilon \times \sqrt[4]{2}^2 \qquad \sqrt{2} \mapsto \sqrt[4]{2}^2$$
$$t_1 \mapsto \epsilon \times \sqrt[4]{2}^2 \qquad t_2 \mapsto \sqrt[4]{3}$$
$$t_3 \mapsto \sqrt[4]{2}^3 \times \sqrt[4]{3}.$$

We can use this to write down the dual map $\beta^*$:

$$(i,0,0) \mapsto x_1 = (i,1,i,1,1)$$
$$(0,i,0) \mapsto x_2 = (-1,-1,-1,1,-i)$$
$$(0,0,i) \mapsto x_3 = (1,1,1,i,1).$$

Finally we find generators for $\phi^{-1}(\mathrm{im}\,\beta^*)$ using Lemma 7. The image of $\beta^*$ is generated by the three elements $x_1, x_2, x_3$ above. Now $\phi(G')$ consists of those elements which take $(1+i)$ to 1, that is, which have 1 as the first component of their row vector. It is clear that the intersection of this with $\mathrm{im}\,\beta^*$ is generated by $x_1^2 x_2$ and $x_3$, giving two generators of the Galois group. From the second part of Lemma 7, $x_1^{-1}$ provides a third generator. We have shown that $\phi^{-1}(\mathrm{im}\,\beta^*)$ is generated by

$$\sigma_4 \sigma_1^{-1}, \quad \sigma_2, \quad \tau \sigma_3.$$

In other words, a set of generators for $\mathrm{Gal}(K/\mathbb{Q})$ is given by

$$g_1 : \sqrt[4]{-4} \mapsto -i\sqrt[4]{-4}, \quad \sqrt{2} \mapsto -\sqrt{2}$$
$$g_2 : \sqrt[4]{3} \mapsto i\sqrt[4]{3}$$
$$g_3 : \sqrt[4]{24} \mapsto -i\sqrt[4]{24}, \quad i \mapsto -i.$$

This group is easily checked to be of order 32. Further calculations show that the decomposition group at 2 is the whole of this group, and that the decomposition group at 3 is dihedral of order 8.

# References

W. Bosma, J. Cannon, and C. Playoust. The MAGMA algebra system I: The user language. *Journal of Symbolic Computation*, 3/4(24):235–265, 1997.

M. J. Bright. Implementation of algorithm for computing galois groups by specialisation, 2003. `http://www.boojum.org.uk/maths/quartic-surfaces/galspec.magma`.

A. Grothendieck. *Séminaire de Géometrie Algébrique du Bois-Marie SGA 1: Revêtements Étales et Groupe Fondamental*. Number 224 in Lecture Notes in Mathematics. Springer-Verlag, 1971.