ARTICLE IN PRESS YJABR:16716

Journal of Algebra ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Black Box Galois representations

Alejandro Argáez-García, John Cremona *

ARTICLE INFO

Article history:
Received 18 October 2017
Available online xxxx
Communicated by Bruno Salvy

Keywords:
Galois representations
Elliptic curves
Automorphic forms

ABSTRACT

We develop methods to study 2-dimensional 2-adic Galois representations ρ of the absolute Galois group of a number field K, unramified outside a known finite set of primes S of K, which are presented as *Black Box* representations, where we only have access to the characteristic polynomials of Frobenius automorphisms at a finite set of primes. Using suitable finite test sets of primes, depending only on K and S, we show how to determine the determinant $\det \rho$, whether or not ρ is residually reducible, and further information about the size of the *isogeny graph* of ρ whose vertices are homothety classes of stable lattices. The methods are illustrated with examples for $K = \mathbb{Q}$, and for K imaginary quadratic, ρ being the representation attached to a Bianchi modular form.
These results form part of the first author's thesis [2].

1. Introduction

Let K be a number field. Denote by $\overline{K}$ the algebraic closure of K and by $G_K = \mathrm{Gal}(\overline{K}/K)$ the absolute Galois group of K. By an *ℓ-adic Galois representation* of K we mean a continuous representation $\rho\colon G_K \to \mathrm{Aut}(V)$, where V is a finite-dimensional vector space over $\mathbb{Q}_\ell$, which is unramified outside a finite set of primes of K. Such representations arise throughout arithmetic geometry, where typically V is a cohomology

* Corresponding author.
E-mail address: j.e.cremona@warwick.ac.uk (J. Cremona).

https://doi.org/10.1016/j.jalgebra.2018.05.017
0021-8693/© 2018 Published by Elsevier Inc.

space attached to an algebraic variety. For example, modularity of elliptic curves over K can be interpreted as a statement that the 2-dimensional Galois representation arising from the action of G_K on the ℓ-adic Tate module of the elliptic curve is equivalent, as a representation, to a representation attached to a suitable automorphic form over K. In this 2-dimensional context and with $\ell = 2$, techniques have been developed by Serre [15], Faltings, Livné [13] and others to establish such an equivalence using only the characteristic polynomial of $\rho(\sigma)$ for a *finite* number of elements $\sigma \in G_K$. Here the ramified set of primes S is known in advance and the Galois automorphisms σ which are used in the Serre–Faltings–Livné method have the form $\sigma = \operatorname{Frob}\mathfrak{p}$ where $\mathfrak{p}$ is a prime not in S, so that ρ is unramified at $\mathfrak{p}$.

Motivated by such applications, in this paper we study Galois representations of K as "Black Boxes" where both the base field K and the finite ramified set S are specified in advance, and the only information we have about ρ is the characteristic polynomial of $\rho(\operatorname{Frob}\mathfrak{p})$ for certain primes $\mathfrak{p}$ not in S; we may specify these primes, but only finitely many of them. Using such a Black Box as an oracle, we seek to give algorithmic answers to questions such as the following (see the following section for definitions):

- Is ρ irreducible? Is ρ trivial, or does it have trivial semisimplification?
- What is the determinant character of ρ?
- What is the residual representation $\overline{\rho}$? Is it irreducible, trivial, or with trivial semisimplification?
- How many lattices in V (up to homothety) are stable under ρ – in other words, how large is the isogeny class of ρ?

In the case where $\dim V = 2$ and $\ell = 2$, we give substantial answers to these questions in the following sections. In Section 2 we recall basic facts about Galois representations and introduce key ideas and definitions, for arbitrary finite dimension and arbitrary prime ℓ. From Section 3 on, we restrict to $\ell = 2$, first considering the case of one-dimensional representations (characters); these are relevant in any dimension since $\det\rho$ is a character. Although in the applications $\det\rho$ is always a power of the ℓ-adic cyclotomic character of G_K, we will not assume this, and in fact the methods of Section 3 may be used to prove that the determinant of a Black Box Galois representation has this form. From Section 4 we restrict to 2-dimensional 2-adic representations, starting with the question of whether the residual representation $\overline{\rho}$ is or is not irreducible (over $\mathbb{F}_2$), and what is its splitting field (see Section 2 for definitions); a complete solution is given for both these questions, which we can express as answering the question of whether or not the isogeny class of ρ consists of only one element. In Section 5 we consider further the residually reducible case and determine whether or not the isogeny class of ρ contains a representative with trivial residual representation, or equivalently whether the size of the class is 2 or greater. In Section 6 we assume that ρ is trivial modulo 2^k for some $k \geq 1$ and determine the reduction of ρ

Please cite this article in press as: A. Argáez-García, J. Cremona, Black Box Galois representations, J. Algebra (2018), https://doi.org/10.1016/j.jalgebra.2018.05.017