Twisting Commutative Algebraic Groups

TWISTING COMMUTATIVE ALGEBRAIC GROUPS

B. MAZUR, K. RUBIN, AND A. SILVERBERG

Abstract. If V is a commutative algebraic group over a field k, $\mathcal{O}$ is a commutative ring that acts on V, and $\mathcal{I}$ is a finitely generated free $\mathcal{O}$-module with a right action of the absolute Galois group of k, then there is a commutative algebraic group $\mathcal{I} \otimes_{\mathcal{O}} V$ over k, which is a twist of a power of V. These group varieties have applications to cryptography (in the cases of abelian varieties and algebraic tori over finite fields) and to the arithmetic of abelian varieties over number fields. For purposes of such applications we devote this article to making explicit this tensor product construction and its basic properties.

Introduction

In this paper we study twists of powers of commutative algebraic groups. We have been using and proving special cases of these results elsewhere, and believe that it would be useful to have a complete theory and complete proofs in the literature in one place. Examples of applications of these twists that already appear in the literature include: to polarizations on abelian varieties [H], to cryptography ([F, RS1] in the case of abelian varieties over finite fields and [RS2] in the case of algebraic tori over finite fields), to constructing abelian varieties over number fields with Shafarevich-Tate groups of nonsquare order [St], and to bounding below the Selmer rank of abelian varieties over dihedral extensions of number fields [MR].

Suppose V is a commutative algebraic group over a field k, $\mathcal{O}$ is a commutative ring that acts on V, and $\mathcal{I}$ is a finitely generated free $\mathcal{O}$-module with a right action of the absolute Galois group G_k of k. We will define a commutative algebraic group over k that we will denote $\mathcal{I} \otimes_{\mathcal{O}} V$, which is a twist of a power of V.

The general theory underlying the construction of $\mathcal{I} \otimes_{\mathcal{O}} V$ is given in the standard sources discussing the homological algebra of tensor products of sheaves for the étale topology (see [GV], particularly Proposition 12.7 on p. 205). In that language, $\mathcal{I} \otimes_{\mathcal{O}} V$ is a tensor product in the category of sheaves on the big étale site over $\mathrm{Spec}(k)$. This tensor product construction was introduced by Serre (§2 of [Se1]) in the case where V is an elliptic curve with complex multiplication by $\mathcal{O}$ and $\mathcal{I}$ is a projective $\mathcal{O}$-module with trivial Galois action. It is discussed in detail by Conrad (§7 of [C]) in the case where V is a group scheme with $\mathcal{O}$-action and $\mathcal{I}$ is a projective $\mathcal{O}$-module with trivial Galois action. Our main objective is to record, in some detail and in a usable way, the basic features regarding the operation of tensoring an abelian group scheme over k endowed with a ring $\mathcal{O}$ of operators (viewing the group scheme as a sheaf for the big étale topology over $\mathrm{Spec}(k)$) with a locally constant sheaf over $\mathrm{Spec}(k)$ of free $\mathcal{O}$-modules of finite rank, noting that the new sheaf given by this tensor product construction is again representable as a group scheme over k with an $\mathcal{O}$-action. To effectively make use of this construction

Mazur is supported by NSF grant DMS-0403374, Rubin by NSF grant DMS-0457481, and Silverberg by NSA grant H98230-05-1-0044.

in our applications, we found that we must pin things down very explicitly. For ease of reading we provide in this article a largely self-contained treatment.

In §1 and §2, following Milne [Mi] who dealt with the case of abelian varieties, we give a concrete definition of $\mathcal{I} \otimes_{\mathcal{O}} V$, and we prove some important properties. Some basic examples are given in Examples 1.5. Our construction is functorial in both $\mathcal{I}$ and V (Theorem 1.8), and if $\mathcal{I}$ decomposes (up to finite index) as $\oplus_i \mathcal{J}_i$, then $\mathcal{I} \otimes_{\mathcal{O}} V$ is isogenous to $\oplus_i (\mathcal{J}_i \otimes V)$ (see Corollary 2.5). Theorem 2.2 describes the action of G_k on the torsion points of $\mathcal{I} \otimes_{\mathcal{O}} V$. We include a more general explicit construction of $\mathcal{I} \otimes_{\mathcal{O}} V$, without the assumption that $\mathcal{I}$ is a free $\mathcal{O}$-module, in an appendix.

If L is a finite Galois extension of k and $G := \mathrm{Gal}(L/k)$, then $\mathbb{Z}[G] \otimes_{\mathbb{Z}} V$ is the restriction of scalars $\mathrm{Res}^L_k V$. Theorem 4.5 shows that $\mathrm{Res}^L_k V$ is isogenous to $\oplus_\rho (\mathcal{I}_\rho \otimes_{\mathbb{Z}} V)$, where ρ runs through the irreducible rational representations of G and $\mathcal{I}_\rho$ is the intersection of $\mathbb{Z}[G]$ with the ρ-isotypic component of $\mathbb{Q}[G]$. In §5 we restrict to the case where L/k is abelian, which is the case of interest in many of the applications. Similar results were obtained by Diem and Naumann [DN] in the case of abelian varieties. In §6 we study cases where $\mathrm{Gal}(L/k)$ is a semi-direct product, which are needed for the applications in [MR]. We study finite group actions on $\mathcal{I} \otimes_{\mathcal{O}} V$ in §7; these results have cryptographic significance in the case of algebraic tori.

We thank Dick Gross for drawing our attention to Conrad's paper [C].

Notation. Let $\mathbb{Z}^+$ denote the set of positive integers. If k is a field, k^{s} will denote a separable closure of k and $G_k := \mathrm{Gal}(k^{\mathrm{s}}/k)$. In this paper "ring" will always mean ring with identity, and "commutative algebraic group" will always mean a commutative algebraic group variety (not necessarily connected).

If $n \in \mathbb{Z}^+$, let $\boldsymbol{\mu}_n$ denote the group of n-th roots of unity in $\bar{\mathbb{Q}}$. If G is a finite group, then $\mathbb{Z}[G]$ will denote the group ring, except that $\mathbb{Z}[\boldsymbol{\mu}_n]$ denotes the ring of integers of the cyclotomic field $\mathbb{Q}(\boldsymbol{\mu}_n)$.

Suppose k is a field and $\mathcal{O}$ is a commutative ring. We consider two categories:

- $\mathbf{FMod}_{\mathcal{O}}(k)$ is the category whose objects are finitely generated free $\mathcal{O}$-modules with a continuous *right* action of G_k, and whose morphisms are G_k-equivariant $\mathcal{O}$-module homomorphisms (the modules are given the discrete topology, so a continuous G_k-action is one that factors through a finite extension of k).
- $\mathbf{CAG}_{\mathcal{O}}(k)$ is the category whose objects are commutative algebraic groups V over k with an action of $\mathcal{O}$, i.e., a ring homomorphism $\mathcal{O} \to \mathrm{End}_k(V)$, and whose morphisms are $\mathcal{O}$-equivariant homomorphisms defined over k.

If $\mathcal{I}, \mathcal{J} \in \mathbf{FMod}_{\mathcal{O}}(k)$ we will view $\mathrm{Hom}_{\mathcal{O}}(\mathcal{I}, \mathcal{J})$ as a left G_k-module, where for $f \in \mathrm{Hom}_{\mathcal{O}}(\mathcal{I}, \mathcal{J})$, $\gamma \in G_k$, and $x \in \mathcal{I}$, we define $(f^\gamma)(x) = f(x\gamma)\gamma^{-1}$. View $\mathcal{O} \in \mathbf{FMod}_{\mathcal{O}}(k)$ with trivial G_k-action.

1. Twisting commutative algebraic groups

Fix a field k and a commutative ring $\mathcal{O}$. In this section we construct a functor $\mathbf{FMod}_{\mathcal{O}}(k) \times \mathbf{CAG}_{\mathcal{O}}(k) \to \mathbf{CAG}_{\mathcal{O}}(k)$, which we will denote by $(\mathcal{I}, V) \mapsto \mathcal{I} \otimes_{\mathcal{O}} V$. This construction appears in §2 of [Mi] when V is an abelian variety.

Definition 1.1. Suppose $V \in \mathbf{CAG}_{\mathcal{O}}(k)$ and $\mathcal{I} \in \mathbf{FMod}_{\mathcal{O}}(k)$. Define the *$\mathcal{I}$-twist* $\mathcal{I} \otimes_{\mathcal{O}} V$ of V as follows. Let $d = \mathrm{rank}_{\mathcal{O}}(\mathcal{I})$, and fix an $\mathcal{O}$-module isomorphism

$j : \mathcal{O}^d \xrightarrow{\sim} \mathcal{I}$. The homomorphism $\mathcal{O} \to \mathrm{End}_k(V)$ induces

$$H^1(k, \mathrm{GL}_d(\mathcal{O})) \longrightarrow H^1(k, \mathrm{Aut}_k(V^d)) \longrightarrow H^1(k, \mathrm{Aut}_{k^s}(V^d)),$$

and we let $c_{\mathcal{I}} \in H^1(k, \mathrm{Aut}_{k^s}(V^d))$ be the image of the cocycle $(\gamma \mapsto j^{-1} \circ j^\gamma)$ under this composition. Define $\mathcal{I} \otimes_{\mathcal{O}} V$ to be the twist of V^d by the cocycle $c_{\mathcal{I}}$. Namely, by Corollaire to Proposition 5 on p. 131 in §III-1.3 of [Se3] (see also §3.1 of [V]), there is a pair $(\mathcal{I} \otimes_{\mathcal{O}} V, \phi)$ (unique up to isomorphism) where $\mathcal{I} \otimes_{\mathcal{O}} V \in \mathbf{CAG}_{\mathcal{O}}(k)$ and $\phi : V^d \xrightarrow{\sim} \mathcal{I} \otimes_{\mathcal{O}} V$ is an isomorphism defined over k^s such that for every $\gamma \in G_k$,

$$c_{\mathcal{I}}(\gamma) = \phi^{-1} \circ \phi^\gamma. \tag{1.1}$$

Remark 1.2. Suppose L is a separable extension of k and G_L acts trivially on $\mathcal{I}$. Then $j^\gamma = j$ for all $\gamma \in G_L$, so $c_{\mathcal{I}}(\gamma) = 1$, so $\phi^\gamma = \phi$ by (1.1). Thus the isomorphism $\phi : V^d \xrightarrow{\sim} \mathcal{I} \otimes_{\mathcal{O}} V$ is defined over L.

If we choose a different $\mathcal{O}$-module isomorphism $j' : \mathcal{O}^d \xrightarrow{\sim} \mathcal{I}$ in Definition 1.1, then $j' = j \circ \alpha$ for some $\alpha \in \mathrm{GL}_d(\mathcal{O})$. The cocycles $\gamma \mapsto j^{-1} j^\gamma$ and $\gamma \mapsto (j')^{-1}(j')^\gamma = \alpha^{-1} j^{-1} j^\gamma \alpha^\gamma$ represent the same class in $H^1(k, \mathrm{GL}_d(\mathcal{O}))$, so they give rise to the same class $c_{\mathcal{I}} \in H^1(k, \mathrm{Aut}_{k^s}(V^d))$. Thus $\mathcal{I} \otimes_{\mathcal{O}} V$ is independent of the choice of j.

If L/k is a Galois extension, V is a commutative algebraic group over k, $\mathcal{I} \in \mathbf{FMod}_{\mathcal{O}}(k)$, and A is a commutative k-algebra, let $\gamma \in G_k$ act on $A \otimes_k L$ as $1 \otimes \gamma$ and on $\mathcal{I} \otimes_{\mathcal{O}} (V(A \otimes_k L))$ as $\gamma^{-1} \otimes (1 \otimes \gamma)$.

Lemma 1.3. *Suppose $\mathcal{I} \in \mathbf{FMod}_{\mathcal{O}}(k)$, $V \in \mathbf{CAG}_{\mathcal{O}}(k)$, and L is a Galois extension of k such that G_L acts trivially on $\mathcal{I}$. Fix an $\mathcal{O}$-module isomorphism $j : \mathcal{O}^d \xrightarrow{\sim} \mathcal{I}$, and let $\phi : V^d \xrightarrow{\sim} \mathcal{I} \otimes_{\mathcal{O}} V$ be as in Definition 1.1. Then for every commutative k-algebra A, the composition*

$$(\mathcal{I} \otimes_{\mathcal{O}} V)(A \otimes_k L) \xrightarrow{\sim} \mathcal{I} \otimes_{\mathcal{O}} (V(A \otimes_k L))$$

of the sequence of $\mathcal{O}$-module isomorphisms

$$(\mathcal{I} \otimes_{\mathcal{O}} V)(A \otimes_k L) \xrightarrow{\phi^{-1}} V^d(A \otimes_k L) \xrightarrow{\sim} \mathcal{O}^d \otimes_{\mathcal{O}} (V(A \otimes_k L)) \xrightarrow{j \otimes 1} \mathcal{I} \otimes_{\mathcal{O}} (V(A \otimes_k L))$$

is a G_k-equivariant $\mathcal{O}$-module isomorphism that is independent of j and is functorial in A, V, $\mathcal{I}$, and L.

Proof. Remark 1.2 shows that ϕ is defined over L, and therefore $\phi(V^d(A \otimes_k L)) = (\mathcal{I} \otimes_{\mathcal{O}} V)(A \otimes_k L)$. The G_k-equivariance of the composition and the independence of j follow from (1.1) and the definition of $c_{\mathcal{I}}$. The functoriality is clear. □

Theorem 1.4. *Suppose $\mathcal{I} \in \mathbf{FMod}_{\mathcal{O}}(k)$ and $V \in \mathbf{CAG}_{\mathcal{O}}(k)$. Let L be a Galois extension of k such that G_L acts trivially on $\mathcal{I}$. Then $\mathcal{I} \otimes_{\mathcal{O}} V$ represents the functor on commutative k-algebras $A \mapsto (\mathcal{I} \otimes_{\mathcal{O}} (V(A \otimes_k L)))^{\mathrm{Gal}(L/k)}$. More precisely, for every commutative k-algebra A, the isomorphism of Lemma 1.3 restricts to a functorial group isomorphism*

$$(\mathcal{I} \otimes_{\mathcal{O}} V)(A) \cong (\mathcal{I} \otimes_{\mathcal{O}} (V(A \otimes_k L)))^{\mathrm{Gal}(L/k)}.$$

Proof. This follows directly from Lemma 1.3, since $(A \otimes_k L)^{G_k} = A$ and G_L acts trivially on $\mathcal{I}$ and L. □

Examples 1.5. (i) Suppose $0 \leq d \in \mathbb{Z}$, and $\mathcal{I} = \mathcal{O}^d$ with trivial Galois action. Then $\mathcal{I} \otimes_{\mathcal{O}} V = V^d$.

(ii) Suppose χ is a quadratic character of G_k, and $\mathcal{I}$ is a free, rank-one $\mathbb{Z}$-module with G_k acting via χ. Then $\mathcal{I} \otimes_{\mathbb{Z}} V$ is the quadratic twist of V by χ. More generally, if $\mathcal{O} = \mathbb{Z}[\boldsymbol{\mu}_n]$, $\chi : G_k \to \boldsymbol{\mu}_n$ is a homomorphism, and $\mathcal{I}$ is a free, rank-one $\mathcal{O}$-module with G_k acting via χ, then $\mathcal{I} \otimes_{\mathcal{O}} V$ is the twist of V by χ^{-1} (in this case the cocycle $c_{\mathcal{I}}$ is χ^{-1}).

(iii) Suppose $V = \mathbb{G}_m$, the multiplicative group, and $\mathcal{I}$ is a free $\mathbb{Z}$-module. Then $\mathcal{I} \otimes_{\mathbb{Z}} V$ is the algebraic torus whose character module $\mathrm{Hom}(\mathcal{I} \otimes_{\mathbb{Z}} V, \mathbb{G}_m)$ is $\mathrm{Hom}(\mathcal{I}, \mathbb{Z})$. See Corollary 1.10 below, and Example 6 in §3.4 of [V].

(iv) If L/k is a finite Galois extension then $\mathcal{O}[\mathrm{Gal}(L/k)] \otimes_{\mathcal{O}} V = \mathrm{Res}_k^L V$ (see Proposition 4.1 below).

Proposition 1.6. *Suppose $\mathcal{I}, \mathcal{J} \in \mathbf{FMod}_{\mathcal{O}}(k)$ and $V, W \in \mathbf{CAG}_{\mathcal{O}}(k)$.*

(i) *There is a functorial G_k-equivariant $\mathcal{O}$-module isomorphism*

$$\mathrm{Hom}_{\mathcal{O}}(\mathcal{I}, \mathcal{J}) \otimes_{\mathcal{O}} \mathrm{Hom}_{k^{\mathrm{s}}}(V, W) \xrightarrow{\sim} \mathrm{Hom}_{k^{\mathrm{s}}}(\mathcal{I} \otimes_{\mathcal{O}} V, \mathcal{J} \otimes_{\mathcal{O}} W).$$

(ii) *The isomorphism of (i) restricts to an injective homomorphism*

$$\mathrm{Hom}_{\mathcal{O}[G_k]}(\mathcal{I}, \mathcal{J}) \otimes_{\mathcal{O}} \mathrm{Hom}_k(V, W) \hookrightarrow \mathrm{Hom}_k(\mathcal{I} \otimes_{\mathcal{O}} V, \mathcal{J} \otimes_{\mathcal{O}} W).$$

Proof. Fix $\mathcal{O}$-module isomorphisms $\mathcal{O}^n \cong \mathcal{I}$ and $\mathcal{O}^m \cong \mathcal{J}$. These isomorphisms induce (see Definition 1.1) isomorphisms $V^n \xrightarrow{\sim} \mathcal{I} \otimes_{\mathcal{O}} V$ and $W^m \xrightarrow{\sim} \mathcal{J} \otimes_{\mathcal{O}} W$ defined over k^{s}, which induce isomorphisms

$$\begin{aligned}\mathrm{Hom}_{\mathcal{O}}(\mathcal{I}, \mathcal{J}) \otimes_{\mathcal{O}} \mathrm{Hom}_{k^{\mathrm{s}}}(V, W) &\xrightarrow{\sim} M_{m\times n}(\mathcal{O}) \otimes_{\mathcal{O}} \mathrm{Hom}_{k^{\mathrm{s}}}(V, W) \\ &\xrightarrow{\sim} M_{m\times n}(\mathrm{Hom}_{k^{\mathrm{s}}}(V, W)) \xrightarrow{\sim} \mathrm{Hom}_{k^{\mathrm{s}}}(V^n, W^m) \xrightarrow{\sim} \mathrm{Hom}_{k^{\mathrm{s}}}(\mathcal{I} \otimes_{\mathcal{O}} V, \mathcal{J} \otimes_{\mathcal{O}} W).\end{aligned}$$

The proof of G_k-equivariance is similar to the proof of G_k-equivariance in Lemma 1.3. This proves (i), and (ii) follows since G_k acts trivially on $\mathrm{Hom}_{\mathcal{O}[G_k]}(\mathcal{I}, \mathcal{J}) \otimes_{\mathcal{O}} \mathrm{Hom}_k(V, W)$. □

Corollary 1.7. *Suppose $\mathcal{I}, \mathcal{J} \in \mathbf{FMod}_{\mathcal{O}}(k)$ and $V \in \mathbf{CAG}_{\mathcal{O}}(k)$.*

(i) *The isomorphism of Proposition 1.6(i) with $W = V$ and the identity map in $\mathrm{Hom}_k(V, W)$ gives a functorial G_k-equivariant $\mathcal{O}$-module homomorphism*

$$\mathrm{Hom}_{\mathcal{O}}(\mathcal{I}, \mathcal{J}) \longrightarrow \mathrm{Hom}_{k^{\mathrm{s}}}(\mathcal{I} \otimes_{\mathcal{O}} V, \mathcal{J} \otimes_{\mathcal{O}} V).$$

(ii) *The map of (i) restricts to a homomorphism*

$$\mathrm{Hom}_{\mathcal{O}[G_k]}(\mathcal{I}, \mathcal{J}) \longrightarrow \mathrm{Hom}_k(\mathcal{I} \otimes_{\mathcal{O}} V, \mathcal{J} \otimes_{\mathcal{O}} V).$$

(iii) *If the map $\mathcal{O} \to \mathrm{End}_k(V)$ is injective, then the maps in (i) and (ii) are injective.*

Proof. Assertions (i) and (ii) follow directly from Proposition 1.6. For (iii), tensoring the injection $\mathcal{O} \hookrightarrow \mathrm{End}_k(V)$ with the free $\mathcal{O}$-module $\mathrm{Hom}_{\mathcal{O}}(\mathcal{I}, \mathcal{J})$ shows that $\mathrm{Hom}_{\mathcal{O}}(\mathcal{I}, \mathcal{J}) \hookrightarrow \mathrm{Hom}_{\mathcal{O}}(\mathcal{I}, \mathcal{J}) \otimes_{\mathcal{O}} \mathrm{End}_k(V)$ is injective. Now (iii) follows from the injectivity in Proposition 1.6. □

If $f \in \mathrm{Hom}_{\mathcal{O}}(\mathcal{I}, \mathcal{J})$ we will often write f_V for the image of f under the map of Corollary 1.7(i).

Theorem 1.8. *The map $(\mathcal{I}, V) \mapsto \mathcal{I} \otimes_{\mathcal{O}} V$ is a functor from $\mathbf{FMod}_{\mathcal{O}}(k) \times \mathbf{CAG}_{\mathcal{O}}(k)$ to $\mathbf{CAG}_{\mathcal{O}}(k)$.*

Proof. This follows directly from Proposition 1.6(ii). □

Corollary 1.9. *Suppose $\mathcal{I}, \mathcal{J} \in \mathbf{FMod}_{\mathcal{O}}(k)$, $V \in \mathbf{CAG}_{\mathcal{O}}(k)$, and $k \subseteq F \subseteq k^{\mathrm{s}}$. If $\mathcal{I}$ and $\mathcal{J}$ are isomorphic as $\mathcal{O}[G_F]$-modules, then the group varieties $\mathcal{I} \otimes_{\mathcal{O}} V$ and $\mathcal{J} \otimes_{\mathcal{O}} V$ are isomorphic over F.*

Proof. If $f : \mathcal{I} \to \mathcal{J}$ is a G_F-equivariant isomorphism, then the image of f under the functorial map of Corollary 1.7(i) is an isomorphism over F from $\mathcal{I} \otimes_{\mathcal{O}} V$ to $\mathcal{J} \otimes_{\mathcal{O}} V$. □

Corollary 1.10. *If $\mathcal{I} \in \mathbf{FMod}_{\mathbb{Z}}(k)$, then* $\mathrm{Hom}_{k^{\mathrm{s}}}(\mathcal{I} \otimes_{\mathbb{Z}} \mathbb{G}_m, \mathbb{G}_m) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathcal{I}, \mathbb{Z})$.

Proof. Apply Proposition 1.6(i) with $\mathcal{J} = \mathcal{O} = \mathbb{Z}$ and $V = W = \mathbb{G}_m$. □

2. Properties of the twists $\mathcal{I} \otimes_{\mathcal{O}} V$

For this section, fix a field k, a commutative ring $\mathcal{O}$, and a commutative algebraic group $V \in \mathbf{CAG}_{\mathcal{O}}(k)$.

Theorem 2.1. *Suppose $\mathcal{I} \in \mathbf{FMod}_{\mathcal{O}}(k)$. Then:*

(i) *$\mathcal{I} \otimes_{\mathcal{O}} V$ is a commutative algebraic group of dimension* $\mathrm{rank}_{\mathcal{O}}(\mathcal{I}) \dim(V)$,
(ii) *$\mathcal{I} \otimes_{\mathcal{O}} V$ is connected if and only if V is connected.,*
(iii) *if L is a separable extension of k and G_L acts trivially on $\mathcal{I}$, then $\mathcal{I} \otimes_{\mathcal{O}} V$ is isomorphic over L to $V^{\mathrm{rank}_{\mathcal{O}}(\mathcal{I})}$.*

Proof. Fix a separable extension L/k such that G_L acts trivially on $\mathcal{I}$. Since $\mathcal{I}$ is isomorphic as a G_L-module to $\mathcal{O}^{\mathrm{rank}_{\mathcal{O}}(\mathcal{I})}$, $\mathcal{I} \otimes_{\mathcal{O}} V$ is isomorphic over L to $\mathcal{O}^{\mathrm{rank}_{\mathcal{O}}(\mathcal{I})} \otimes_{\mathcal{O}} V = V^{\mathrm{rank}_{\mathcal{O}}(\mathcal{I})}$ by Corollary 1.9, giving (iii). The remaining assertions follow easily. □

Suppose $n \in \mathbb{Z}^+$. If B is an abelian group, let $B[n]$ denote the subgroup of elements of order dividing n in B. If W is a commutative algebraic group over k, let $W[n]$ denote the G_k-module $W(k^{\mathrm{s}})[n]$, and if ℓ is a prime let

$$T_\ell(W) := \varprojlim_m W[\ell^m],$$

the ℓ-adic Tate module of W.

Theorem 2.2. *Suppose $\mathcal{I} \in \mathbf{FMod}_{\mathcal{O}}(k)$, $n \in \mathbb{Z}^+$, and ℓ is prime. Then there are G_k-equivariant isomorphisms (with $\gamma \in G_k$ acting on the right-hand sides as $\gamma^{-1} \otimes \gamma$), functorial in $\mathcal{I}$ and V,*

(i) $(\mathcal{I} \otimes_{\mathcal{O}} V)(k^{\mathrm{s}}) \cong \mathcal{I} \otimes_{\mathcal{O}} (V(k^{\mathrm{s}}))$,
(ii) $(\mathcal{I} \otimes_{\mathcal{O}} V)[n] \cong \mathcal{I} \otimes_{\mathcal{O}} (V[n])$,
(iii) $T_\ell(\mathcal{I} \otimes_{\mathcal{O}} V) \cong \mathcal{I} \otimes_{\mathcal{O}} (T_\ell(V))$.

Proof. (See Proposition 6(b) of [Mi].) The first assertion follows from Lemma 1.3 with $A = k$ and $L = k^{\mathrm{s}}$. Since $\mathcal{I}$ is a free $\mathcal{O}$-module,

$$(\mathcal{I} \otimes_{\mathcal{O}} (V(k^{\mathrm{s}})))[n] \cong \mathcal{I} \otimes_{\mathcal{O}} (V[n]),$$

so (ii) follows from (i), and (iii) follows by taking the inverse limit of (ii) with $n = \ell^m$. □

Lemma 2.3. *Suppose $\mathcal{I}, \mathcal{J} \in \mathbf{FMod}_{\mathcal{O}}(k)$ with $\mathcal{I} \subseteq \mathcal{J}$ and $\mathcal{J}/\mathcal{I}$ is free (as an $\mathcal{O}$-module). Then the induced sequence of commutative algebraic groups over k*

$$0 \longrightarrow \mathcal{I} \otimes_{\mathcal{O}} V \longrightarrow \mathcal{J} \otimes_{\mathcal{O}} V \longrightarrow (\mathcal{J}/\mathcal{I}) \otimes_{\mathcal{O}} V \longrightarrow 0$$

is exact.

Proof. Since $\mathcal{J}/\mathcal{I}$ is free, there is an $\mathcal{O}$-module isomorphism $\mathcal{J} \cong \mathcal{I} \oplus (\mathcal{J}/\mathcal{I})$. It follows by Corollary 1.9 that $\mathcal{J} \otimes_{\mathcal{O}} V \cong (\mathcal{I} \otimes_{\mathcal{O}} V) \oplus ((\mathcal{J}/\mathcal{I}) \otimes_{\mathcal{O}} V)$ over k^{s}, so the sequence of the lemma is a (split) exact sequence over k^{s}. But then the sequence is exact over k. □

Define a *k-isogeny* in $\mathbf{CAG}_{\mathcal{O}}(k)$ or in $\mathbf{FMod}_{\mathcal{O}}(k)$ to be a k-morphism whose kernel and cokernel are annihilated by some positive integer.

Lemma 2.4. *If $\mathcal{I}, \mathcal{J} \in \mathbf{FMod}_{\mathcal{O}}(k)$ and $s : \mathcal{I} \to \mathcal{J}$ is a k-isogeny, then the induced map $s_V : \mathcal{I} \otimes_{\mathcal{O}} V \to \mathcal{J} \otimes_{\mathcal{O}} V$ is a k-isogeny.*

Proof. Suppose $n \in \mathbb{Z}^+$ is such that $n \cdot \ker(s) = 0$ and $n \cdot \mathrm{coker}(s) = 0$. Then there is a k-isogeny $t : \mathcal{J} \to \mathcal{I}$ such that $t \circ s$ and $s \circ t$ are both multiplication by n^2, so $s_V \circ t_V \in \mathrm{End}_k(\mathcal{J} \otimes_{\mathcal{O}} V)$ and $t_V \circ s_V \in \mathrm{End}_k(\mathcal{I} \otimes_{\mathcal{O}} V)$ are both multiplication by n^2. Therefore s_V is a k-isogeny. □

Corollary 2.5. *Suppose $\mathcal{I}, \mathcal{J}_1, \dots, \mathcal{J}_t \in \mathbf{FMod}_{\mathcal{O}}(k)$, and $\mathcal{I} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \oplus_{i=1}^{t} (\mathcal{J}_i \otimes_{\mathbb{Z}} \mathbb{Q})$ as $\mathcal{O}[G_k]$-modules. Then $\mathcal{I} \otimes_{\mathcal{O}} V$ is k-isogenous to $\oplus_{i=1}^{t} (\mathcal{J}_i \otimes_{\mathcal{O}} V)$.*

Proof. In this case $\mathcal{I}$ is k-isogenous to $\oplus_i \mathcal{J}_i$, so by Lemma 2.4, $\mathcal{I} \otimes_{\mathcal{O}} V$ is k-isogenous to $(\oplus_i \mathcal{J}_i) \otimes_{\mathcal{O}} V \cong \oplus_i (\mathcal{J}_i \otimes_{\mathcal{O}} V)$. □

Proposition 2.6. *Suppose $\mathcal{I}, \mathcal{J} \in \mathbf{FMod}_{\mathcal{O}}(k)$. Then there is a natural isomorphism $(\mathcal{I} \otimes_{\mathcal{O}} \mathcal{J}) \otimes_{\mathcal{O}} V \cong \mathcal{I} \otimes_{\mathcal{O}} (\mathcal{J} \otimes_{\mathcal{O}} V)$ over k.*

Proof. Suppose A is a commutative k-algebra. Then applying Theorem 1.4 and Lemma 1.3 with $L = k^{\mathrm{s}}$ (suppressing the subscripts $\mathcal{O}$ and k from the tensor products)

$$\begin{aligned}(\mathcal{I} \otimes (\mathcal{J} \otimes V))(A) &\cong (\mathcal{I} \otimes ((\mathcal{J} \otimes V)(A \otimes k^{\mathrm{s}})))^{G_k} \\ &\cong (\mathcal{I} \otimes (\mathcal{J} \otimes (V(A \otimes k^{\mathrm{s}})))^{G_k} \\ &= ((\mathcal{I} \otimes \mathcal{J}) \otimes (V(A \otimes k^{\mathrm{s}})))^{G_k} \\ &\cong ((\mathcal{I} \otimes \mathcal{J}) \otimes V)(A).\end{aligned}$$

These isomorphisms are functorial in A, so the proposition follows from a variant of the Yoneda Lemma (see for example Proposition VI-2 of [EH]). □

3. Annihilator modules

The results of this section will be used in §4 and §7.

Fix a finite Galois extension L/k, a commutative ring $\mathcal{O}$, and a commutative algebraic group $V \in \mathbf{CAG}_{\mathcal{O}}(k)$, and let $G := \mathrm{Gal}(L/k)$. Let $\mathbf{FMod}_{\mathcal{O}}(L/k)$ denote the full subcategory of $\mathbf{FMod}_{\mathcal{O}}(k)$ whose objects are the $\mathcal{O}[G_k]$-modules in $\mathbf{FMod}_{\mathcal{O}}(k)$ on which G_L acts trivially.

Definition 3.1. For $\mathcal{I} \in \mathbf{FMod}_{\mathcal{O}}(L/k)$, define a left $\mathcal{O}[G]$-module

$$\hat{\mathcal{I}} := \mathrm{Hom}_{\mathcal{O}[G]}(\mathcal{I}, \mathcal{O}[G])$$

with $\mathcal{O}[G]$ acting by $(\alpha \cdot f)(x) = \alpha \cdot f(x)$ for every $\alpha \in \mathcal{O}[G]$, $f \in \hat{\mathcal{I}}$, and $x \in \mathcal{I}$. Also define an $\mathcal{O}$-module homomorphism $\pi : \mathcal{O}[G] \to \mathcal{O}$ by $\pi(\sum_{g \in G} a_g g) = a_1$.

Part (i) of the following lemma shows that $\hat{\mathcal{I}}$ is independent of the choice of L.

Lemma 3.2. (i) *For each $\mathcal{K} \in \mathbf{FMod}_{\mathcal{O}}(L/k)$, the map $f \mapsto \pi \circ f$ defines an isomorphism of left G_k-modules*

$$\hat{\mathcal{K}} \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{O}}(\mathcal{K}, \mathcal{O}).$$

(ii) *If $\mathcal{I}, \mathcal{J} \in \mathbf{FMod}_{\mathcal{O}}(L/k)$, $\mathcal{I} \subseteq \mathcal{J}$, and $\mathcal{J}/\mathcal{I}$ is a projective $\mathcal{O}$-module, then the canonical sequence $0 \to \widehat{\mathcal{J}/\mathcal{I}} \to \hat{\mathcal{J}} \to \hat{\mathcal{I}} \to 0$ is exact.*

Proof. For (i), see for example Proposition VI.3.4 of [B]. Assertion (ii) follows from (i), since the exact sequence of $\mathcal{O}$-modules $0 \to \mathcal{I} \to \mathcal{J} \to \mathcal{J}/\mathcal{I} \to 0$ splits if $\mathcal{J}/\mathcal{I}$ is projective. □

Lemma 3.3. *Suppose $\mathcal{I}, \mathcal{J} \in \mathbf{FMod}_{\mathcal{O}}(L/k)$, $\mathcal{I} \subseteq \mathcal{J}$, and $\mathcal{J}/\mathcal{I}$ is a free $\mathcal{O}$-module. Then*

$$\mathcal{I} \otimes_{\mathcal{O}} V = \bigcap_{f \in \widehat{\mathcal{J}/\mathcal{I}}} \ker(f_V : \mathcal{J} \otimes_{\mathcal{O}} V \to \mathcal{O}[G] \otimes_{\mathcal{O}} V),$$

where f_V is the image of f under the map

$$\mathrm{Hom}_{\mathcal{O}[G]}(\mathcal{J}/\mathcal{I}, \mathcal{O}[G]) \hookrightarrow \mathrm{Hom}_{\mathcal{O}[G]}(\mathcal{J}, \mathcal{O}[G]) \longrightarrow \mathrm{Hom}_k(\mathcal{J} \otimes_{\mathcal{O}} V, \mathcal{O}[G] \otimes_{\mathcal{O}} V)$$

coming from Corollary 1.7(ii).

Proof. Choose an $\mathcal{O}$-basis $\{f_1, \ldots, f_d\}$ of $\mathrm{Hom}_{\mathcal{O}}(\mathcal{J}/\mathcal{I}, \mathcal{O})$. For every i let $\phi_i \in \widehat{\mathcal{J}/\mathcal{I}}$ be the inverse image of f_i under the isomorphism of Lemma 3.2(i) (with $\mathcal{K} = \mathcal{J}/\mathcal{I}$), so $\pi \circ \phi_i = f_i$, with π defined in Definition 3.1. Then there is a commutative diagram of $\mathcal{O}$-modules, with the top line an exact sequence of $\mathcal{O}[G]$-modules

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{J}/\mathcal{I} & \xrightarrow{\oplus \phi_i} & \mathcal{O}[G]^d & \longrightarrow & \mathcal{C} & \longrightarrow & 0. \\ & & & \searrow^{\oplus f_i}_{\cong} & \downarrow{\scriptstyle \pi^d} & & & & \\ & & & & \mathcal{O}^d & & & & \end{array} \tag{3.1}$$

Then $(\oplus f_i)^{-1} \circ \pi^d$ gives a splitting of the top exact sequence, so $\mathcal{C}$ is isomorphic as an $\mathcal{O}$-module to the kernel of π^d, which is free. Therefore we can apply Lemma 2.3 both to the top line of (3.1) and to the exact sequence $0 \to \mathcal{I} \to \mathcal{J} \to \mathcal{J}/\mathcal{I} \to 0$ to obtain an exact sequence

$$0 \to \mathcal{I} \otimes_{\mathcal{O}} V \to \mathcal{J} \otimes_{\mathcal{O}} V \xrightarrow{\oplus(\phi_i)_V} (\mathcal{O}[G] \otimes_{\mathcal{O}} V)^d \to \mathcal{C} \otimes_{\mathcal{O}} V \to 0.$$

By Lemma 3.2(i), $\phi_1, \ldots, \phi_d$ generate $\widehat{\mathcal{J}/\mathcal{I}}$, so

$$\mathcal{I} \otimes_{\mathcal{O}} V = \ker(\oplus(\phi_i)_V) = \cap_{f \in \widehat{\mathcal{J}/\mathcal{I}}} \ker(f_V).$$

□

Definition 3.4. If $\mathcal{I}$ is a right ideal of $\mathcal{O}[G]$, let $\mathcal{I}^{\perp}$ denote the left annihilator of $\mathcal{I}$, i.e., $\mathcal{I}^{\perp}$ is the left ideal of $\mathcal{O}[G]$ defined by

$$\mathcal{I}^{\perp} := \{\alpha \in \mathcal{O}[G] : \alpha \mathcal{I} = 0\}.$$

A (right or left) ideal $\mathcal{I}$ of $\mathcal{O}[G]$ is *saturated* if $\mathcal{O}[G]/\mathcal{I}$ is a projective $\mathcal{O}$-module.

A finitely generated $\mathbb{Z}$-module is projective (or equivalently, free) if and only if it is torsion-free. Thus when $\mathcal{O} = \mathbb{Z}$, intersecting with $\mathbb{Z}[G]$ (inversely, tensoring with $\mathbb{Q}$) gives a one-to-one correspondence between the ideals of $\mathbb{Q}[G]$ and the saturated ideals of $\mathbb{Z}[G]$.

Lemma 3.5. *Let $\lambda : \mathcal{O}[G] \to \widehat{\mathcal{O}[G]}$ be the ring isomorphism that sends $\alpha \in \mathcal{O}[G]$ to left multiplication by α. Then:*

(i) *If $\mathcal{I}$ is a right ideal of $\mathcal{O}[G]$ then the restriction of λ induces an isomorphism*
$$\mathcal{I}^\perp \xrightarrow{\sim} \widehat{\mathcal{O}[G]/\mathcal{I}}.$$
(ii) *If $\mathcal{I}$ is a saturated right ideal of $\mathcal{O}[G]$, then $\mathcal{I} = \{\alpha \in \mathcal{O}[G] : \mathcal{I}^\perp \cdot \alpha = 0\}$.*
(iii) *If $\mathcal{I}$ is a saturated two-sided ideal of $\mathcal{O}[G]$, then λ induces an isomorphism $\mathcal{O}[G]/\mathcal{I}^\perp \xrightarrow{\sim} \mathrm{End}_{\mathcal{O}[G]}(\mathcal{I})$ (and $\mathrm{End}_{\mathcal{O}[G]}(\mathcal{I}) = \hat{\mathcal{I}}$).*

Proof. Suppose $\mathcal{I}$ is a right ideal of $\mathcal{O}[G]$. The map $\widehat{\mathcal{O}[G]} \to \mathcal{O}[G]$ defined by $f \mapsto f(1)$ is a right and left inverse of λ. Thus λ is an isomorphism and there is a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{I}^\perp & \longrightarrow & \mathcal{O}[G] & \longrightarrow & \mathcal{O}[G]/\mathcal{I}^\perp & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\lambda} & & \downarrow{\scriptstyle\lambda}{\scriptstyle\cong} & & \downarrow{\scriptstyle\lambda} & & \\ 0 & \longrightarrow & \widehat{\mathcal{O}[G]/\mathcal{I}} & \longrightarrow & \widehat{\mathcal{O}[G]} & \longrightarrow & \hat{\mathcal{I}} & & \end{array} \tag{3.2}$$

where the right-hand vertical map is injective by definition of $\mathcal{I}^\perp$. The snake lemma shows that the left-hand vertical map is an isomorphism, which proves (i).

Now suppose $\mathcal{I}$ is saturated. If $\beta \in \mathcal{O}[G] - \mathcal{I}$, then there is an $\mathcal{O}$-module homomorphism from $\mathcal{O}[G]/\mathcal{I}$ to $\mathcal{O}$ that is nonzero on β. Now (ii) follows from (i), along with Lemma 3.2(i) with $\mathcal{K} = \mathcal{O}[G]/\mathcal{I}$.

Since $\mathcal{I}$ is saturated, by Lemma 3.2(ii) the bottom right-hand map of (3.2) is surjective, and hence the right-hand vertical map is an isomorphism. If $\mathcal{I}$ is a two-sided ideal, then $\lambda(\mathcal{O}[G]/\mathcal{I}^\perp) \subseteq \mathrm{End}_{\mathcal{O}[G]}(\mathcal{I}) \subseteq \hat{\mathcal{I}}$, so equality must hold and the proof of (iii) is complete. □

4. Decomposing the restriction of scalars

In this section we decompose the restriction of scalars of a commutative algebraic group. Theorems 4.5, 5.2, and 5.5 were proved by Diem and Naumann in §3.4 and §3.5 of [DN] in the case of abelian varieties.

Fix a finite Galois extension L/k, a commutative ring $\mathcal{O}$, and a commutative algebraic group $V \in \mathbf{CAG}_{\mathcal{O}}(k)$, and let $G := \mathrm{Gal}(L/k)$. Let $\mathrm{Res}^L_k V$ denote the Weil restriction of scalars of V from L to k (see for example §1.3 of [W] or §3.12 of [V]). Then for every commutative k-algebra A there is an isomorphism, functorial in A,
$$(\mathrm{Res}^L_k V)(A) \cong V(A \otimes_k L). \tag{4.1}$$

Proposition 4.1. *$\mathcal{O}[G] \otimes_{\mathcal{O}} V \cong \mathrm{Res}^L_k V$ over k.*

Proof. Let $\mathcal{O}^G := \oplus_{g\in G}\mathcal{O}$, $V^G := \oplus_{g\in G} V$, and for $g \in G$ let $p_g : V^G \to V$ be the projection onto the g component. Using the $\mathcal{O}$-module isomorphism $j : \mathcal{O}^G \to \mathcal{O}[G]$ defined by $j((x_g)) = \sum_g x_g g^{-1}$, Definition 1.1 gives a pair $(\mathcal{O}[G] \otimes_{\mathcal{O}} V, \phi)$ where $\phi : V^G \xrightarrow{\sim} \mathcal{O}[G] \otimes_{\mathcal{O}} V$ is an isomorphism over L. Let $\eta := p_1 \circ \phi^{-1} : \mathcal{O}[G] \otimes_{\mathcal{O}} V \to V$. The cocycle $c_{\mathcal{O}[G]} \in H^1(k, \mathrm{Aut}_{k^s}(V^G))$ of Definition 1.1 satisfies $p_h \circ c_{\mathcal{O}[G]}(g) = p_{g^{-1}h}$ for every $g, h \in G$, so (using (1.1)),
$$\eta^g = p_1 \circ (\phi^{-1})^g = p_1 \circ c_{\mathcal{O}[G]}(g)^{-1} \circ \phi^{-1} = p_g \circ \phi^{-1}.$$

Therefore $\oplus\eta^g : \mathcal{O}[G] \otimes_{\mathcal{O}} V \to V^G$ is an isomorphism (it's equal to ϕ^{-1}), so by the definition of $\mathrm{Res}^L_k V$ in §1.3 of [W], $\mathcal{O}[G] \otimes_{\mathcal{O}} V \cong \mathrm{Res}^L_k V$ over k. □

For the rest of this section we will take $\mathcal{O} = \mathbb{Z}$ and write simply "$\otimes$" in place of "$\otimes_{\mathbb{Z}}$". The functorial map of Corollary 1.7(ii) (with $\mathcal{I} = \mathcal{J} = \mathbb{Z}[G]$) and Proposition 4.1 give natural ring homomorphisms

$$\mathbb{Z}[G] \cong \mathrm{End}_{\mathbb{Z}[G]}(\mathbb{Z}[G]) \to \mathrm{End}_k(\mathbb{Z}[G] \otimes V) \xrightarrow{\sim} \mathrm{End}_k(\mathrm{Res}^L_k V). \tag{4.2}$$

If $\alpha \in \mathbb{Z}[G]$, then we denote its image under (4.2) by $\alpha_V \in \mathrm{End}_k(\mathrm{Res}^L_k V)$.

Proposition 4.2. *If $\mathcal{I}$ is a saturated right ideal of $\mathbb{Z}[G]$, then:*

(i) $\mathcal{I} \otimes V = \bigcap_{\alpha \in \mathcal{I}^\perp} \ker(\alpha_V : \mathrm{Res}^L_k V \to \mathrm{Res}^L_k V)$.

(ii) *For every commutative k-algebra A there is a functorial isomorphism*

$$(\mathcal{I} \otimes V)(A) \cong \{v \in V(A \otimes_k L) : \mathcal{I}^\perp \cdot v = 0\}.$$

(iii) *If further $\mathcal{I}$ is a two-sided ideal, then there is a natural injective ring homomorphism*

$$(\mathbb{Z}[G]/\mathcal{I}^\perp) \otimes \mathrm{End}_k(V) \hookrightarrow \mathrm{End}_k(\mathcal{I} \otimes V).$$

Proof. By Lemma 3.5(i), $\widehat{\mathbb{Z}[G]/\mathcal{I}} \cong \mathcal{I}^\perp$. By Lemma 3.3 (with $\mathcal{J} = \mathbb{Z}[G]$) and Proposition 4.1, we have (i). Assertion (ii) follows from (i) and (4.1).

If $\mathcal{I}$ is a two-sided ideal, then $\mathbb{Z}[G]/\mathcal{I}^\perp \xrightarrow{\sim} \mathrm{End}_{\mathbb{Z}[G]}(\mathcal{I})$ by Lemma 3.5(iii). Now (iii) follows from Proposition 1.6(ii) (with $\mathcal{J} = \mathcal{I}$ and $W = V$). □

The group ring $\mathbb{Q}[G]$ is semisimple, and decomposes into a direct sum of minimal two-sided ideals

$$\mathbb{Q}[G] = \bigoplus_{\rho} \mathbb{Q}[G]_\rho \tag{4.3}$$

indexed by the irreducible rational representations ρ of G. Here $\mathbb{Q}[G]_\rho$ is the ρ-isotypic component of $\mathbb{Q}[G]$, i.e., the sum of all left ideals of $\mathbb{Q}[G]$ isomorphic to ρ.

Definition 4.3. If ρ is an irreducible finite-dimensional rational representation of G_k, choose a finite Galois extension L/k such that ρ factors through $G := \mathrm{Gal}(L/k)$, define

$$\mathcal{I}_\rho := \mathbb{Q}[G]_\rho \cap \mathbb{Z}[G] \in \mathbf{FMod}_{\mathcal{O}}(k),$$

and define the *ρ-twist of V* by

$$V_\rho := \mathcal{I}_\rho \otimes V.$$

Remark 4.4. Note that $\mathcal{I}_\rho$ is well-defined up to $\mathbb{Z}[G_k]$-isomorphism, independent of the choice of L, and therefore V_ρ is well-defined up to isomorphism over k. Since $\mathbb{Q}[G]_\rho$ is a $\mathbb{Q}$-vector space, $\mathcal{I}_\rho$ is a saturated ideal of $\mathbb{Z}[G]$.

Theorem 4.5. *Suppose L/k is a finite Galois extension, V is a commutative algebraic group over k, and $G := \mathrm{Gal}(L/k)$. Then $\mathrm{Res}^L_k V$ is isogenous over k to $\oplus_\rho V_\rho$, direct sum over all irreducible rational representations of G.*

Proof. This follows from Proposition 4.1, (4.3), and Corollary 2.5 with $\mathcal{I} = \mathbb{Z}[G]$ and with $\{\mathcal{J}_1, \ldots, \mathcal{J}_t\} = \{\mathcal{I}_\rho : \rho \text{ an irreducible rational representation of } G\}$. □

5. Abelian twists

Fix a finite abelian extension L/k and a commutative algebraic group V over k, and let $G = \mathrm{Gal}(L/k)$ and $\mathcal{O} = \mathbb{Z}$.

The irreducible rational representations of G are in one-to-one correspondence with the cyclic extensions of k in L. (See for example exercise 13.1 of [Se2].) Namely, if ρ is an irreducible rational representation let F_ρ be the fixed field of the kernel of ρ, and if F is a cyclic extension of k in L let ρ_F (or $\rho_{F/k}$, if we need to specify the field k) denote the unique irreducible rational representation of G with kernel $\mathrm{Gal}(L/F)$. If $[F : k] = d$ then $\dim \rho_F = \varphi(d)$, where φ is the Euler φ-function.

Definition 5.1. Suppose F is a cyclic extension of k in L, and ρ_F is the corresponding irreducible rational representation of G. Let $\mathbb{Q}[G]_F$ denote the ρ_F-isotypic component of $\mathbb{Q}[G]$, and let

$$\mathcal{I}_F := \mathbb{Q}[G]_F \cap \mathbb{Z}[G], \qquad V_F := \mathcal{I}_F \otimes V$$

(these were denoted $\mathbb{Q}[G]_{\rho_F}$, $\mathcal{I}_{\rho_F}$, and V_{ρ_F} in (4.3) and Definition 4.3). When necessary to specify the ground field k, we will write $\mathcal{I}_{F/k}$ and $V_{F/k}$. Let R_F denote the maximal order of the field $\mathbb{Q}[G]_F$.

By Remark 4.4, $\mathcal{I}_F$ and V_F are well-defined up to isomorphism, independent of the choice of field L containing F, and $\mathcal{I}_F$ is saturated in $\mathbb{Z}[G]$.

The following result is a special case of Theorem 4.5.

Theorem 5.2. *If L/k is a finite abelian extension and V is a commutative algebraic group over k, then $\mathrm{Res}_k^L V$ is isogenous over k to $\oplus_F V_F$, direct sum over all cyclic extensions F of k in L.*

If $k \subseteq F \subseteq L$, let

$$N_{L/F} := \sum_{g \in \mathrm{Gal}(L/F)} g \in \mathbb{Z}[G].$$

Define

$$\Omega_L := \{\text{fields } F : k \subseteq F \subsetneq L\} \quad \supseteq \quad \Omega'_L := \{F : k \subseteq F \subsetneq L, [L : F] \text{ prime}\}.$$

Then every element of Ω_L is a subfield of some element of Ω'_L, and we define

$$W_L := \bigcap_{F \in \Omega_L} \ker(N_{L/F,V}) = \bigcap_{F \in \Omega'_L} \ker(N_{L/F,V}) \subseteq \mathrm{Res}_k^L V,$$

where $N_{L/F,V} \in \mathrm{End}_k(\mathrm{Res}_k^L V)$ is the image of $N_{L/F}$ under (4.2). We will see in Theorem 5.8(i) below that if L/k is cyclic, then $W_L = V_L$. In the non-cyclic case we have the following.

Proposition 5.3. *If L/k is abelian but not cyclic, then* $\dim(W_L) = 0$.

Proof. Since L/k is not cyclic, there are a prime p and a field M such that $k \subseteq M \subset L$ and $\mathrm{Gal}(L/M) \cong (\mathbb{Z}/p\mathbb{Z})^2$. Since there are exactly $p+1$ degree p extensions of M in L, in $\mathbb{Z}[G]$ we have the identity

$$\sum_{M \subsetneq F \subsetneq L} N_{L/F} = p + N_{L/M}.$$

Since W_L is in the kernel of all the norm maps in this identity, it follows that W_L is contained in the kernel of multiplication by p, so $\dim(W_L) = 0$. □

Suppose for the rest of this section that L/k is cyclic. Theorems 5.5, 5.8, and 5.9 below are our main results about V_L in the cyclic case. Let $r := |G| = [L : k]$, and fix a generator τ of G. For $d \in \mathbb{Z}^+$ let $\Phi_d \in \mathbb{Z}[x]$ denote the d-th cyclotomic polynomial, and let $\Psi_d(x) := (x^d - 1)/\Phi_d(x) \in \mathbb{Z}[x]$.

Lemma 5.4. (i) *$\mathcal{I}_L = \Psi_r(\tau)\mathbb{Z}[G]$ and $\mathcal{I}_L^\perp = \Phi_r(\tau)\mathbb{Z}[G]$.*

(ii) *Every isomorphism $\chi : G \xrightarrow{\sim} \boldsymbol{\mu}_r$ induces a ring isomorphism $R_L \xrightarrow{\sim} \mathbb{Z}[\boldsymbol{\mu}_r]$. This ring isomorphism is G-equivariant, with $g \in G$ acting on $\mathbb{Z}[\boldsymbol{\mu}_r]$ as multiplication by $\chi(g)$.*

(iii) *The projection $\mathbb{Q}[G] \twoheadrightarrow \mathbb{Q}[G]_L$ given by (4.3) induces a G-module isomorphism $\mathbb{Z}[G]/\mathcal{I}_L^\perp \xrightarrow{\sim} R_L$.*

(iv) *$\mathcal{I}_L = \prod_{primes\ \ell \mid r}(\zeta_\ell - 1)R_L$, where for each prime ℓ dividing r, ζ_ℓ is a primitive ℓ-th root of unity in R_L.*

Proof. Let $S = \mathbb{Q}[x]/(x^r - 1)\mathbb{Q}[x]$. Since G is cyclic of order r, the homomorphism $\eta : \mathbb{Q}[G] \to S$ that takes τ to x is a $\mathbb{Q}[G]$-module isomorphism, where τ acts on S as multiplication by x. Since $\mathbb{Q}[G]_L \cong \mathbb{Q}[x]/\Phi_r(x)\mathbb{Q}[x] \cong \Psi_r(x)S \subseteq S$ as $\mathbb{Q}[G]$-modules, and $\mathbb{Q}[G]$ (and hence S) has a unique $\mathbb{Q}[G]$-submodule isomorphic to $\mathbb{Q}[G]_L$, we have $\eta(\mathbb{Q}[G]_L) = \Psi_r(x)S$. It follows that the isomorphism $\eta : \mathbb{Z}[G] \cong \mathbb{Z}[x]/(x^r - 1)\mathbb{Z}[x]$ maps $\mathcal{I}_L$ (resp., $\mathcal{I}_L^\perp$) isomorphically onto the ideal generated by $\Psi_r(x)$ (resp., by $\Phi_r(x)$). Both assertions of (i) now follow.

If $\chi : G \xrightarrow{\sim} \boldsymbol{\mu}_r$ is an isomorphism, then $\tau \mapsto x \mapsto \chi(\tau)$ induces isomorphisms $\mathbb{Q}[G]_L \xrightarrow{\sim} \mathbb{Q}[x]/\Phi_r(x)\mathbb{Q}[x] \xrightarrow{\sim} \mathbb{Q}(\boldsymbol{\mu}_r)$. The composition maps the maximal order R_L isomorphically to the maximal order $\mathbb{Z}[\boldsymbol{\mu}_r]$, giving (ii).

Using (i) and (ii), there is a commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \Phi_r(x)\mathbb{Z}[x]/(x^r-1)\mathbb{Z}[x] & \longrightarrow & \mathbb{Z}[x]/(x^r-1)\mathbb{Z}[x] & \longrightarrow & \mathbb{Z}[x]/\Phi_r(x)\mathbb{Z}[x] & \longrightarrow & 0 \\
 & & \cong\uparrow\eta & & \cong\uparrow\eta & & \cong\uparrow & & \\
0 & \longrightarrow & \mathcal{I}_L^\perp & \longrightarrow & \mathbb{Z}[G] & \xrightarrow{\lambda} & R_L & \longrightarrow & 0
\end{array}$$

with vertical isomorphisms, where the map λ is induced by $\mathbb{Q}[G] \twoheadrightarrow \mathbb{Q}[G]_L$. Since the top row is exact, so is the bottom row, giving (iii).

Let μ denote the Möbius function. Then

$$\Psi_r(x) = (x^r - 1)/\Phi_r(x) = \prod_{d \mid r, d \neq 1} (x^{r/d} - 1)^{-\mu(d)}. \tag{5.1}$$

In $\mathbb{Z}[x]/\Phi_r(x)\mathbb{Z}[x]$, x is a primitive r-th root of unity, so $x^{r/d}$ has order d, so $x^{r/d} - 1$ is a unit in $\mathbb{Z}[x]/\Phi_r(x)\mathbb{Z}[x]$ unless d is a prime power. When $d \neq 1$ is a prime power, $\mu(d) = -1$ if d is prime, and $\mu(d) = 0$ otherwise. By (i), $\eta(\mathcal{I}_L)$ is generated by $\Psi_r(x)$, so by (5.1), the ideal $\lambda(\mathcal{I}_L)$ of R_L is generated by $\prod_{\ell \mid r}(\zeta_\ell - 1)$. Since $\mathcal{I}_L \subseteq \mathbb{Q}[G]_L$, λ is the identity map on $\mathcal{I}_L$. This proves (iv). □

Theorem 5.5. *Suppose L/k is a cyclic extension of degree r, and V is a commutative algebraic group over k. Then:*

(i) *V_L is a commutative algebraic group of dimension $\varphi(r)\dim(V)$.*

(ii) *If V is connected then V_L is connected.*

(iii) *V_L is isomorphic over L to $V^{\varphi(r)}$.*

(iv) *There is an injective ring homomorphism $R_L \otimes \mathrm{End}_k(V) \hookrightarrow \mathrm{End}_k(V_L)$.*

Proof. Parts (i), (ii), and (iii) follow from Theorem 2.1, since $\operatorname{rank}_{\mathbb{Z}} \mathcal{I}_L = \dim \rho_L = \varphi(r)$. Part (iv) follows from Proposition 4.2(iii) and Lemma 5.4(iii). □

Lemma 5.6. *The ideal of $\mathbb{Z}[x]/(x^r-1)\mathbb{Z}[x]$ generated by $\Phi_r(x)$ is also generated by each of the following sets*

(i) $\{(x^r-1)/(x^d-1) : d \mid r, d \neq r\}$,
(ii) $\{(x^r-1)/(x^{r/\ell}-1) : \ell \mid r,\ \ell \text{ prime}\}$.

Proof. The identity $x^r - 1 = \prod_{d|r} \Phi_d(x)$ shows that $\Phi_r(x)$ divides $(x^r-1)/(x^d-1)$ for every divisor $d < r$ of r. On the other hand, Theorem 1 of [dB] or [Re] shows that $\Phi_r(x)$ is a $\mathbb{Z}[x]$-linear combination of $\{(x^r-1)/(x^d-1) : d \mid r, d \neq r\}$. This proves (i). Every element in the set (i) is divisible by one of the elements in its subset (ii), so this completes the proof. □

Lemma 5.7. *Each of the sets $\{\Phi_r(\tau)\}$, $\{N_{L/F} : F \in \Omega_L\}$, $\{N_{L/F} : F \in \Omega'_L\}$ generates the ideal $\mathcal{I}_L^{\perp} \subseteq \mathbb{Z}[G]$.*

Proof. If $k \subseteq F \subseteq L$ and $[F : k] = d$, then $N_{L/F}$ goes to $(x^r-1)/(x^d-1)$ under the isomorphism $\mathbb{Z}[G] \xrightarrow{\sim} \mathbb{Z}[x]/(x^r-1)\mathbb{Z}[x]$. Thus by Lemma 5.6, the three sets of this lemma generate the same ideal of $\mathbb{Z}[G]$. By Lemma 5.4(i), this ideal is $\mathcal{I}_L^{\perp}$. □

Recall that if $\alpha \in \mathbb{Z}[G]$, then $\alpha_V \in \operatorname{End}_k(\operatorname{Res}_k^L V)$ denotes its image under (4.2).

Theorem 5.8. *Suppose L/k is a cyclic extension of degree r, and V is a commutative algebraic group over k. Then:*

(i) $V_L = \cap_{F \in \Omega_L} \ker(N_{L/F,V}) = \cap_{F \in \Omega'_L} \ker(N_{L/F,V}) = \ker(\Phi_r(\tau)_V) \subseteq \operatorname{Res}_k^L V$, *where τ is any generator of $\operatorname{Gal}(L/k)$.*
(ii) *If A is a commutative k-algebra, then*

$$V_L(A) \cong \{\alpha \in V(A \otimes_k L) : N_{L/F}(\alpha) = 0 \text{ for every } F \in \Omega_L\}.$$

In particular,

$$V_L(k) \cong \{\alpha \in V(L) : N_{L/F}(\alpha) = 0 \text{ for every } F \in \Omega_L\}.$$

Both assertions also hold with Ω_L replaced by Ω'_L.

Proof. Assertion (i) (resp., (ii)) follows from Lemma 5.7 and Proposition 4.2(i) (resp., (ii)). □

Theorem 5.9. *Suppose L/k is a cyclic extension of degree r, and V is a commutative algebraic group over k. Suppose that ℓ is prime and $g \in G_k$. Let d be the order of the restriction of g to $G := \operatorname{Gal}(L/k)$. If the characteristic polynomial of g acting on $T_\ell(V)$ is $\prod_i (X - \alpha_i)$ with $\alpha_i \in \bar{\mathbb{Q}}_\ell$, then the characteristic polynomial of g acting on $T_\ell(V_L)$ is*

$$\prod_{i,\zeta} (X - \alpha_i \zeta)^{\varphi(r)/\varphi(d)}$$

where ζ runs through all primitive d-th roots of unity.

Proof. By Lemma 5.4(ii), the eigenvalues of the generator $\tau \in G$ acting on $\mathcal{I}_L \otimes \mathbb{Q} = R_L \otimes \mathbb{Q}$ are exactly the primitive r-th roots of unity in $\bar{\mathbb{Q}}$, each with multiplicity one. It follows that the eigenvalues of g acting on $\mathcal{I}_L$ are the primitive d-th roots of unity, each with multiplicity $\varphi(r)/\varphi(d)$. The result now follows from the isomorphism $T_\ell(V_L) \cong \mathcal{I}_L \otimes T_\ell(V)$ of Theorem 2.2(iii). □

Proposition 5.10. *Suppose L/k is cyclic, F and M are extensions of k in L, $F \cap M = k$, and $L = FM$. If V is a commutative algebraic group over k, then $(V_F)_M \cong V_L$ over k.*

Proof. Let $d = [F : k]$ and $e = [M : k]$. Then $de = r$. Since L/k is cyclic, d and e are relatively prime. By Lemma 5.4(ii,iv), there are isomorphisms of $\mathbb{Z}[G]$-modules $\mathcal{I}_F \cong \mathbb{Z}[\boldsymbol{\mu}_d]$, $\mathcal{I}_M \cong \mathbb{Z}[\boldsymbol{\mu}_e]$, and $\mathcal{I}_L \cong \mathbb{Z}[\boldsymbol{\mu}_r]$, where the chosen generator τ of G acts on the right-hand sides as multiplication by ζ_d, ζ_e, and ζ_r, respectively, and where the roots of unity are chosen so that $\zeta_d\zeta_e = \zeta_r$. Then the natural map $\mathbb{Z}[\boldsymbol{\mu}_d] \otimes_{\mathbb{Z}} \mathbb{Z}[\boldsymbol{\mu}_e] \xrightarrow{\sim} \mathbb{Z}[\boldsymbol{\mu}_r]$ is an isomorphism of $\mathbb{Z}[G]$-modules. Hence $\mathcal{I}_L \cong \mathcal{I}_M \otimes_{\mathbb{Z}} \mathcal{I}_F$, and the proposition follows from Proposition 2.6. □

Remark 5.11. Suppose $k \subseteq F \subseteq L$. Let $N_{L/F} : \mathbb{Z}[G] \to \mathbb{Z}[G]$ denote multiplication by $\sum_{h \in \mathrm{Gal}(L/F)} h$. Then $N_{L/F}$ factors as

$$N_{L/F} : \mathbb{Z}[G] \xrightarrow{R_{L/F}} \mathbb{Z}[\mathrm{Gal}(F/k)] \xhookrightarrow{\iota_{L/F}} \mathbb{Z}[G]$$

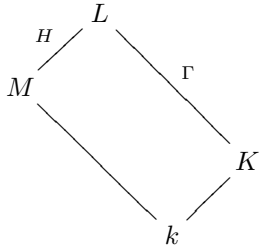
where $R_{L/F}$ is the natural projection map. Since $\ker(R_{L/F})$ and $\mathrm{coker}(\iota_{L/F})$ are torsion-free, Lemma 2.3 shows that the induced maps $R_{L/F,V}$ and $\iota_{L/F,V}$ in the composition

$$N_{L/F,V} : \mathrm{Res}^L_k V \xrightarrow{R_{L/F,V}} \mathrm{Res}^F_k V \xhookrightarrow{\iota_{L/F,V}} \mathrm{Res}^L_k V \tag{5.2}$$

are surjective and injective, respectively. In [RS1, RS2, RS3], the primitive subgroup of $\mathrm{Res}^L_k V$ corresponding to L was defined to be $T_L := \cap_{k \subseteq F \subsetneq L} \ker(R_{L/F,V})$. By (5.2), $\ker(R_{L/F,V}) = \ker(N_{L/F,V})$. So when L/k is cyclic, $T_L = V_L = W_L$ (the last equality by Theorem 5.8(i)).

6. Semidirect products

Suppose for this section that L/k is a finite Galois extension, and $G := \mathrm{Gal}(L/k)$ is a semidirect product $\Gamma \rtimes H$ of a normal cyclic subgroup $\Gamma = \mathrm{Gal}(L/K)$ of order r by a subgroup $H = \mathrm{Gal}(L/M)$. There is a diagram



and we view $\mathbb{Z}[\Gamma]$ and $\mathbb{Z}[H]$ as subrings of $\mathbb{Z}[G]$, so $\mathbb{Z}[G] = \mathbb{Z}[\Gamma]\mathbb{Z}[H] = \mathbb{Z}[H]\mathbb{Z}[\Gamma]$. Let $\rho_{L/K}$ be the (unique) irreducible faithful rational representation of Γ, and $\mathbb{Q}[\Gamma]_{L/K}$ the $\rho_{L/K}$-isotypic component of $\mathbb{Q}[\Gamma]$. Let $\mathcal{I}_L = \mathcal{I}_{L/K} \subseteq \mathbb{Z}[\Gamma]$ be the ideal $\mathbb{Q}[\Gamma]_{L/K} \cap \mathbb{Z}[\Gamma]$ of Definition 5.1, so $\mathcal{I}_L \in \mathbf{FMod}_{\mathbb{Z}}(K)$.

In this section we will show (Theorem 6.3 below) that the commutative algebraic group $V_{L/K} = \mathcal{I}_L \otimes V \in \mathbf{CAG}_{\mathbb{Z}}(K)$ of Definition 5.1 has a model over k of the form $\mathcal{J}_L \otimes V \in \mathbf{CAG}_{\mathbb{Z}}(k)$ for a suitable right ideal $\mathcal{J}_L$ of $\mathbb{Z}[G]$. This is needed for the applications in [MR], in the case where G is a dihedral group of order $2r$.

Define

$$N_H := \sum_{h \in H} h \in \mathbb{Z}[H] \subseteq \mathbb{Z}[G].$$

Lemma 6.1. *The abelian group $\mathcal{J}_L := N_H \mathcal{I}_L$ is a saturated right ideal of $\mathbb{Z}[G]$.*

Proof. For $h \in H$, the representation $\rho^h_{L/K}$ of Γ defined by $\rho^h_{L/K}(\gamma) = \rho_{L/K}(h\gamma h^{-1})$ is an irreducible faithful rational representation of Γ, so $\rho^h_{L/K} \cong \rho_{L/K}$. Hence $h\mathcal{I}_L h^{-1} = \mathcal{I}_L$ in $\mathbb{Q}[G]$, so for $h \in H$ and $\gamma \in \Gamma$ we have

$$N_H \mathcal{I}_L h = N_H h \mathcal{I}_L = N_H \mathcal{I}_L, \quad N_H \mathcal{I}_L \gamma = N_H \mathcal{I}_L,$$

so $N_H \mathcal{I}_L \mathbb{Z}[G] = N_H \mathcal{I}_L$. Since $\mathcal{I}_L \subseteq \mathbb{Z}[\Gamma]$ is saturated, $\mathcal{J}_L \subseteq \mathbb{Z}[G]$ is saturated. □

Definition 6.2. Define $V_{L/k} := \mathcal{J}_L \otimes V$ where $\mathcal{J}_L := N_H \mathcal{I}_L$ as in Lemma 6.1. This definition depends on the subgroup H of G; if necessary we will denote $V_{L/k}$ by $V_{L/k,H}$. Theorem 6.3 below shows that if H' is another subgroup with $G = \Gamma \rtimes H'$, then $V_{L/k,H'}$ is isomorphic to $V_{L/k,H}$ over K.

Theorem 6.3. *Over K there is an isomorphism $V_{L/k} \cong V_{L/K}$, where $V_{L/K}$ (resp., $V_{L/k}$) is given by Definition 5.1 (resp., Definition 6.2).*

Proof. Left multiplication by N_H is an isomorphism $\mathcal{I}_L \to \mathcal{J}_L$ of right G_K-modules. By Corollary 1.9 with $F = K$, $V_{L/K} = V_{\mathcal{I}_L}$ is isomorphic over K to $V_{L/k} = V_{\mathcal{J}_L}$. □

7. Finite group actions on $\mathcal{I} \otimes V$

In this section we study the action of symmetric groups on the group varieties $\mathcal{I} \otimes V$. When V is an algebraic torus, these results provide insights into some known cryptosystems (see [RS2, RS3]).

Fix a finite Galois extension L/k and let $G := \mathrm{Gal}(L/k)$ (and $\mathcal{O} = \mathbb{Z}$). Fix also a commutative algebraic group V over k that is not isogenous to the trivial group, i.e., so that the natural map $\mathbb{Z} \to \mathrm{End}_k(V)$ is injective. If $\sigma \in \mathrm{End}_{\mathbb{Z}}(\mathbb{Z}[G])$, let $\sigma_V \in \mathrm{End}_L(\mathrm{Res}^L_k V)$ denote the endomorphism given by the functorial map of Corollary 1.7(i) (with $\mathcal{I} = \mathcal{J} = \mathbb{Z}[G]$). If $\mathcal{I}$ is a saturated right ideal of $\mathbb{Z}[G]$, view $\mathcal{I} \otimes V \subseteq \mathrm{Res}^L_k V$ via Lemma 2.3 (with $\mathcal{J} = \mathbb{Z}[G]$) and Proposition 4.1.

Lemma 7.1. *Suppose that $\mathcal{I}$ is a saturated right ideal of $\mathbb{Z}[G]$, and $\sigma \in \mathrm{End}_{\mathbb{Z}}(\mathbb{Z}[G])$. Then the following are equivalent:*

(i) $\sigma(\mathcal{I}) \subseteq \mathcal{I}$.
(ii) $\sigma_V(\mathcal{I} \otimes V) \subseteq \mathcal{I} \otimes V$.

Proof. If $\sigma(\mathcal{I}) \subseteq \mathcal{I}$ then $\sigma|_{\mathcal{I}} \in \mathrm{End}_{\mathbb{Z}}(\mathcal{I})$. By the functoriality of $\mathcal{I} \mapsto \mathcal{I} \otimes V$, we have $\sigma_V|_{\mathcal{I} \otimes V} \in \mathrm{End}_L(\mathcal{I} \otimes V)$. Thus (i) ⇒ (ii).

Conversely, suppose $\sigma_V(\mathcal{I} \otimes V) \subseteq \mathcal{I} \otimes V$ and let $\lambda : \mathbb{Z}[G] \to \mathrm{End}_{\mathbb{Z}}(\mathbb{Z}[G])$ denote the map that sends $\alpha \in \mathbb{Z}[G]$ to left multiplication by α. Suppose $\alpha \in \mathcal{I}$ and $\beta \in \mathcal{I}^\perp$. Then $\alpha\mathbb{Z}[G] \subseteq \mathcal{I}$, so $\alpha_V \in \mathrm{End}_k(\mathrm{Res}^L_k V)$ factors through $\mathcal{I} \otimes V$, i.e., $\alpha_V(\mathrm{Res}^L_k V) \subseteq \mathcal{I} \otimes V$. Therefore

$$(\lambda(\beta) \circ \sigma \circ \lambda(\alpha))_V(\mathrm{Res}^L_k V) = \beta_V(\sigma_V(\alpha_V(\mathrm{Res}^L_k V))) \subseteq \beta_V(\mathcal{I} \otimes V) = 0$$

by Proposition 4.2(i). By Corollary 1.7(iii), the map $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}[G]) \to \mathrm{End}_{k^s}(\mathrm{Res}^L_k V)$ is injective, so $\lambda(\beta) \circ \sigma \circ \lambda(\alpha) = 0$, and thus $\beta \cdot \sigma(\alpha) = (\lambda(\beta) \circ \sigma \circ \lambda(\alpha))(1) = 0$. Therefore $\mathcal{I}^\perp \sigma(\mathcal{I}) = 0$, so $\sigma(\mathcal{I}) \subseteq \mathcal{I}$ by Proposition 3.5(ii). Thus (ii) ⇒ (i). □

Let Σ_H denote the group of permutations of a set H. If $\sigma \in \Sigma_G$, let $\hat{\sigma} \in \mathrm{Aut}_{\mathbb{Z}}(\mathbb{Z}[G])$ denote the automorphism induced by σ, and let $\hat{\sigma}_V \in \mathrm{Aut}_L(\mathrm{Res}^L_k V)$ denote the corresponding automorphism of $\mathrm{Res}^L_k V$.

Lemma 7.2. *Suppose that L/k is cyclic and $\sigma \in \Sigma_G$. Then the restriction of $\hat{\sigma}_V$ to V_L is an automorphism of V_L if and only if*

(*) *for every $g \in G$ and subgroup $H \subseteq G$ of prime order, $\sigma(gH) = \sigma(g)H$.*

Proof. Since σ has finite order, the restriction of $\hat{\sigma}_V$ to V_L is an automorphism if and only if $\hat{\sigma}_V(V_L) \subseteq V_L$, which by Lemma 7.1 happens if and only if $\hat{\sigma}(\mathcal{I}_L) \subseteq \mathcal{I}_L$. Write $G = G_1 \times \cdots \times G_t$ where each G_i is of prime power order, $|G_i| = p_i^{r_i}$, ordered so that $p_1 < \ldots < p_t$. For $1 \leq i \leq t$, let H_i be the subgroup of G_i of order p_i, and let $N_{H_i} = \sum_{h \in H_i} h \in \mathbb{Z}[G]$. By Lemma 5.7,

$$\mathcal{I}_L^{\perp} = \sum_{i=1}^{t} \mathbb{Z}[G] N_{H_i}. \tag{7.1}$$

If σ satisfies (*) then $\hat{\sigma}(N_{H_i}\alpha) = N_{H_i} \cdot \hat{\sigma}(\alpha)$ for every $\alpha \in \mathbb{Z}[G]$ and every i, so

$$\mathcal{I}_L^{\perp} \cdot \hat{\sigma}(\mathcal{I}_L) = \sum_i \mathbb{Z}[G] N_{H_i} \cdot \hat{\sigma}(\mathcal{I}_L) = \sum_i \mathbb{Z}[G] \cdot \hat{\sigma}(N_{H_i} \cdot \mathcal{I}_L) = 0,$$

since $N_{H_i} \cdot \mathcal{I}_L = 0$ for all i. By Proposition 3.5(ii) we conclude that $\hat{\sigma}(\mathcal{I}_L) \subseteq \mathcal{I}_L$, so by Lemma 7.1, $\hat{\sigma}_V|_{V_L} \in \mathrm{Aut}(V_L)$.

Conversely, suppose (*) fails to hold for some H. Take j minimal so that there is a $\gamma \in G$ with $\sigma(\gamma H_j) \neq \sigma(\gamma)H_j$. Replacing σ by $\tau_{\sigma(\gamma)^{-1}} \circ \sigma \circ \tau_\gamma$ (where $\tau_g \in \Sigma_G$ is left multiplication by $g \in G$) we may assume without loss of generality that $\sigma(1) = 1$, $\sigma(H_j) \neq H_j$, and $\sigma(gH_i) = \sigma(g)H_i$ for all $g \in G$ and $i < j$. It follows that $\sigma^{-1}(gH_i) = \sigma^{-1}(g)H_i$ for all $g \in G$ and $i < j$, so

$$\sigma^{-1}(g \prod_{i<j} H_i) = \sigma^{-1}(g) \prod_{i<j} H_i \quad \text{for every } g \in G. \tag{7.2}$$

Let $\pi_i : G \to G_i$ be the projection map. For $1 \leq i \leq t$, fix $1 \neq \delta_i \in H_i$ such that

$$\delta_i \notin \begin{cases} \pi_i(\sigma^{-1}(H_j)) & \text{if } i > j, \\ \sigma^{-1}(H_j) & \text{if } i = j, \\ \pi_i(\sigma^{-1}(H_j) \cap \delta_j \prod_{i<j} H_i) & \text{if } 1 < i < j. \end{cases}$$

The first is possible since $p_i > p_j$ if $i > j$; the second since $\sigma(H_j) \neq H_j$; and the third because it follows from (7.2) that the elements of $\sigma^{-1}(H_j)$ lie in distinct cosets of $\prod_{i<j} H_i$, and $|H_i| = p_i \geq 3$ if $i > 1$.

If $S \subseteq \{1, \cdots, t\}$, let $\delta_S = \prod_{i \in S} \delta_i$. Note that $\delta_S = 1$ if and only if $S = \emptyset$. We claim that if $\sigma(\delta_S) \in H_j$, then either $S = \emptyset$, or else $S = \{1, j\}$ and $j \neq 1$ (in which case $\delta_S = \delta_1\delta_j$). To prove the claim, suppose $S \neq \emptyset$ (so $\delta_S \neq 1$) and $\sigma(\delta_S) \in H_j$. Then $\pi_i(\delta_S) \in \pi_i(\sigma^{-1}(H_j))$. Note that $\pi_i(\delta_S)$ is δ_i if $i \in S$ and is 1 otherwise. By our constraints on the δ_i, if $i > j$ then $i \notin S$. If $j \notin S$, then applying (7.2) with $g = 1$ gives $\sigma(\delta_S) \in (\prod_{i<j} H_i) \cap H_j = \{1\}$, contradicting that $\sigma(1) = 1$ and $\delta_S \neq 1$. Thus $j \in S$, and again by our constraints, if $1 < i < j$ then $i \notin S$. Since $\sigma(\delta_j) \notin H_j$, we cannot have $S = \{j\}$. We have thus proved the claim.

Let $\alpha := \prod_{i=1}^{t}(1 - \delta_i) = \sum_S (-1)^{|S|}\delta_S \in \mathbb{Z}[G]$, with S running over subsets of $\{1, \cdots, t\}$. By the claim above, $\hat{\sigma}(\alpha) = \sum_S (-1)^{|S|}\sigma(\delta_S) = 1 + \sum_{g \notin H_j} a_g g$ or $1 + \sigma(\delta_1\delta_j) + \sum_{g \notin H_j} a_g g$ with $a_g \in \mathbb{Z}$. It follows that $N_{H_j} \cdot \hat{\sigma}(\alpha) \neq 0$, since the

coefficient of the identity element is either 1 or 2, so $\hat{\sigma}(\alpha) \notin \mathcal{I}_L$ by Lemma 5.7. Since $\delta_i \in H_i$, we have $N_{H_i}(1-\delta_i) = 0$ for all i. Thus by (7.1), $\mathcal{I}_L^{\perp}\alpha = 0$, so by Proposition 3.5(ii), $\alpha \in \mathcal{I}_L$. Therefore $\hat{\sigma}(\mathcal{I}_L) \not\subseteq \mathcal{I}_L$, so by Lemma 7.1, $\hat{\sigma}_V(V_L) \not\subseteq V_L$. □

If $|G|$ is squarefree, and H is a subgroup of G, then there is a unique subgroup $J \subseteq G$ such that $G = H \times J$, and this decomposition induces an inclusion $\Sigma_H \subseteq \Sigma_G$.

Theorem 7.3. *Suppose L/k is cyclic of squarefree degree, $|G| = p_1 \cdots p_t$ with distinct primes p_i, H_i is the subgroup of G of order p_i, and $\sigma \in \Sigma_G$. Then $\hat{\sigma}_V|_{V_L} \in \mathrm{Aut}(V_L)$ if and only if $\sigma \in \prod_{i=1}^{t} \Sigma_{H_i} (\subseteq \Sigma_G)$.*

Proof. Suppose $\sigma \in \prod_i \Sigma_{H_i}$. It is easy to see that for every $g \in G$ and every i, $\sigma(gH_i) = \sigma(g)H_i$. By Lemma 7.2, $\hat{\sigma}_V|_{V_L} \in \mathrm{Aut}(V_L)$.

Conversely, suppose $\hat{\sigma}_V|_{V_L} \in \mathrm{Aut}(V_L)$. By Lemma 7.2, $\sigma(gH_i) = \sigma(g)H_i$ for all $g \in G$ and all i. Let $\pi_i : G \to H_i$ denote the projection, and let $\sigma_i = \sigma|_{H_i} : H_i \to G$. Let $\tau_i = \pi_i \circ \sigma_i \in \Sigma_{H_i}$. It follows easily that $\sigma = \prod_{i=1}^{t} \tau_i \circ \pi_i \in \sigma \in \prod_i \Sigma_{H_i}$. □

Appendix. More general construction

Although in the above discussion we restrict to the case of free $\mathcal{O}$-modules $\mathcal{I}$, the tensor product construction $(\mathcal{I}, V) \mapsto \mathcal{I} \otimes_{\mathcal{O}} V$ in the appropriate category of sheaves for the étale topology (as alluded to in the introduction) is quite general. Moreover, this more general construction can also be formulated in fairly concrete terms. For example, suppose that $\mathcal{O}$ is a commutative noetherian ring, $V \in \mathbf{CAG}_{\mathcal{O}}(k)$, and $\mathcal{I}$ is a finitely generated $\mathcal{O}$-module with a continuous right action of G_k, but do not assume that $\mathcal{I}$ is a free $\mathcal{O}$-module. Let L be a finite Galois extension of k such that G_L acts trivially on $\mathcal{I}$, and let $G := \mathrm{Gal}(L/k)$. Since $\mathcal{O}$ is noetherian, there is an $\mathcal{O}[G]$-presentation of $\mathcal{I}$, i.e., an exact sequence

$$\mathcal{O}[G]^a \xrightarrow{\psi} \mathcal{O}[G]^b \longrightarrow \mathcal{I} \longrightarrow 0$$

of right $\mathcal{O}[G]$-modules. By basic properties of the functor $V \mapsto \mathrm{Res}_k^L V$ (or for example, by Corollary 1.7(ii) and Proposition 4.1), ψ induces a k-homomorphism

$$\psi_V : (\mathrm{Res}_k^L V)^a \to (\mathrm{Res}_k^L V)^b,$$

and we can define

$$\mathcal{I} \otimes_{\mathcal{O}} V := \mathrm{coker}(\psi_V) \in \mathbf{CAG}_{\mathcal{O}}(k).$$

One can show that this definition is independent of the choice of L and of the presentation of $\mathcal{I}$, and it agrees with Definition 1.1 if $\mathcal{I}$ is a free $\mathcal{O}$-module. Further, without the assumption that the $\mathcal{O}$-modules are free, Theorem 1.8, Corollaries 1.9, 1.10, and 2.5, and Lemma 2.4 all remain true verbatim, Proposition 1.6 and Corollary 1.7 hold if $\mathcal{I}$ and $\mathcal{J}$ are projective $\mathcal{O}$-modules, Theorem 2.2 holds if $\mathcal{I}$ is a projective $\mathcal{O}$-module, and Lemma 2.3 holds if $\mathcal{I}/\mathcal{J}$ is a projective $\mathcal{O}$-module.

This definition of $\mathcal{I} \otimes_{\mathcal{O}} V$ is essentially the same as Conrad's definition of his $\mathcal{I} \otimes_{\mathcal{O}[G]} \mathrm{Res}_k^L V$ in Theorem 7.2 of [C], using the action of $\mathcal{O}[G]$ on $\mathrm{Res}_k^L V$ given by (4.2) above.

References

[B] K. Brown, Cohomology of groups, Graduate Texts in Mathematics **87**, Springer, New York, 1982.

[C] B. Conrad, *Gross-Zagier revisited*, in Heegner points and Rankin L-series, Math. Sci. Res. Inst. Pub. **49**, Cambridge Univ. Press, Cambridge, 2004, 67–163.

[dB] N. G. de Bruijn, *On the factorization of cyclic groups*, Nederl. Akad. Wetensch. Proc. Ser. A **56** (= Indagationes Math. **15**) (1953), 370–377.

[DN] C. Diem, N. Naumann, *On the structure of Weil restrictions of abelian varieties*, J. Ramanujan Math. Soc. **18** (2003), 153–174.

[EH] D. Eisenbud, J. Harris, The geometry of schemes, Graduate Texts in Mathematics **197**, Springer, New York, 2000.

[F] G. Frey, *Applications of arithmetical geometry to cryptographic constructions*, in Finite fields and applications (Augsburg, 1999), Springer, Berlin, 2001, 128–161.

[GV] A. Grothendieck, J-L. Verdier, exposé IV of *Théorie des topos et cohomologie étale des schémas. Tome 1: Théorie des topos*, Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964 (SGA 4), eds. M. Artin, A. Grothendieck, J-L. Verdier, Lecture Notes in Math. **269**, Springer, Berlin-New York, 1972.

[H] E. Howe, *Isogeny classes of abelian varieties with no principal polarizations*, in Moduli of abelian varieties (Texel Island, 1999), Progress in Math. **195**, Birkhäuser, Basel, 2001, 203–216.

[MR] B. Mazur, K. Rubin, *Finding large Selmer rank via an arithmetic theory of local constants*, to appear in Annals of Mathematics, `http://arxiv.org/abs/math/0512085`

[Mi] J. S. Milne, *On the arithmetic of abelian varieties*, Invent. Math. **17** (1972), 177–190.

[Re] L. Rédei, *Über das Kreisteilungspolynom*, Acta Math. Acad. Sci. Hungar. **5** (1954), 27–28.

[RS1] K. Rubin, A. Silverberg, *Supersingular abelian varieties in cryptology*, in Advances in Cryptology — CRYPTO 2002, Lect. Notes in Comp. Sci. **2442**, Springer, Berlin, 2002, 336–353.

[RS2] K. Rubin, A. Silverberg, *Algebraic tori in cryptography*, in High Primes and Misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams, Fields Institute Communications Series **41**, AMS, Providence, RI, 2004, 317–326.

[RS3] K. Rubin, A. Silverberg, *Using primitive subgroups to do more with fewer bits*, in Proceedings of Algorithmic Number Theory, 6th International Symposium, ANTS-VI, Lect. Notes in Comp. Sci. **3076**, Springer, Berlin, 2004, 18–41.

[Se1] J-P. Serre, *Complex multiplication*, in Algebraic Number Theory, eds. J. W. S. Cassels and A. Fröhlich, Thompson Book Co., Washington, DC, 1967, 292–296.

[Se2] J-P. Serre, Linear representations of finite groups, Graduate Texts in Mathematics **42**, Springer, New York, 1977.

[Se3] J-P. Serre, Cohomologie galoisienne, cinquième édition, révisée et complétée, Lecture Notes in Math. **5**, Springer, Berlin, 1994.

[St] W. A. Stein, *Shafarevich-Tate groups of nonsquare order*, in Modular curves and abelian varieties, Progr. Math. **224**, Birkhäuser, Basel, 2004, 277–289.

[V] V. E. Voskresenskiĭ, Algebraic groups and their birational invariants, Translations of Mathematical Monographs **179**, AMS, Providence, RI, 1998.

[W] A. Weil, Adeles and algebraic groups, Progress in Math. **23**, Birkhäuser, Boston, 1982.

Department of Mathematics, Harvard University, Cambridge, MA 02138 USA
E-mail address: `mazur@math.harvard.edu`

Department of Mathematics, University of California Irvine, Irvine, CA 92697 USA
E-mail address: `krubin@uci.edu`

Department of Mathematics, University of California Irvine, Irvine, CA 92697 USA
E-mail address: `asilverb@uci.edu`