SYMPLECTIC REPRESENTATIONS OF SEMIDIRECT PRODUCTS

MARIA SABITOVA

Abstract. In this paper we study symplectic representations of groups of the form $(A \rtimes B) \rtimes C$, where A, B are finite cyclic groups of coprime orders, and C is an infinite cyclic group.

Introduction

The goal of the paper is to study symplectic representations of semidirect products G of the form $G = (A \rtimes B) \rtimes C$, where A, B are finite cyclic groups of coprime orders and C is an infinite cyclic group. Representations in question occur naturally in connection with elliptic curves over the field $\mathbb{Q}$ of rational numbers and, more generally, with abelian varieties over finite extensions of $\mathbb{Q}$. We now briefly explain the connection. Let E be an elliptic curve over $\mathbb{Q}$, i.e., E is given by an equation

$$y^2 = x^3 + ax + b, \tag{0.1}$$

where $a, b \in \mathbb{Z}$ and $4a^3+27b^2 \neq 0$. One says that E has good reduction at a prime number p, if, roughly speaking, after reducing a, b modulo p one still gets an elliptic curve, i.e., the resulting curve is smooth over the finite field $\mathbb{F}_p$ of p elements. One can also consider E as an elliptic curve over the field $\mathbb{Q}_p$ of p-adic numbers, i.e., given a fixed algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ in this case E consists of all points $P = (x, y) \in \overline{\mathbb{Q}}_p \times \overline{\mathbb{Q}}_p$ satisfying (0.1). It is known that there is a structure of an abelian group on E. Also, the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ acts on E via

$$\sigma \cdot (x, y) = (\sigma(x), \sigma(y)), \quad \forall \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p),\ (x, y) \in E,$$

and the action preserves the group structure on E. Let $l \in \mathbb{Z}$ be a prime number different from p and let E_{l^n}, $n \in \mathbb{N}$, denote the set of points $P \in E$ satisfying $l^n \cdot P = 0$ (with respect to the group structure on E written additively). We have group homomorphisms

$$E_{l^{n+1}} \longrightarrow E_{l^n}, \quad P \mapsto l \cdot P,\ P \in E_{l^{n+1}},$$

and hence we can form the inverse limit $T_l = \varprojlim_n E_{l^n}$. The group $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ acts on T_l via its action on E. Moreover, T_l is a module over the ring $\mathbb{Z}_l$ of l-adic integers, so that T_l is a $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-module over $\mathbb{Z}_l$. This gives a continuous (with respect to the standard topology on $\mathbb{Q}_l$ and the profinite topology on $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$) two-dimensional representation ρ of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ on $V_l = T_l \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ (via the trivial action of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ on $\mathbb{Q}_l$ and the

Date: September 9, 2013.

Supported by NSF grant DMS-0901230.

action of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ on T_l described above). One prefers to work with representations over $\mathbb{C}$ and there exist embeddings of $\mathbb{Q}_l$ into $\mathbb{C}$. However, given an embedding $\imath : \mathbb{Q}_l \hookrightarrow \mathbb{C}$, the representation of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ on $V_l \otimes_\imath \mathbb{C}$ is no longer continuous in general. It turns out that there is a big class of elliptic curves (namely, those with good reduction over a finite extension of $\mathbb{Q}_p$) such that the restriction of the representation of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ on $V_l \otimes_\imath \mathbb{C}$ to a subgroup is continuous. The subgroup in question is the so-called Weil group $\mathcal{W}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ of $\mathbb{Q}_p$, which is a semidirect product of the Galois group $I = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p^{unr})$ of an extension $\mathbb{Q}_p^{unr} \subset \overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ with an infinite cyclic group generated by a special element $\Phi \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. (More precisely, $\mathbb{Q}_p^{unr}$ is generated by all roots of unity of orders not divisible by p and Φ induces the action of the Frobenius $x \mapsto x^p$, $x \in \overline{\mathbb{F}}_p$, under the decomposition map $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \longrightarrow \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$.) It turns out that for elliptic curves with good reduction over a finite extension of $\mathbb{Q}_p$ the image of I under ρ is finite, so that the restriction of ρ to I can be considered as a representation of the Galois group of a finite Galois extension K of $\mathbb{Q}_p^{unr}$. It is known that $\mathrm{Gal}(K/\mathbb{Q}_p^{unr})$ is a semidirect product of a p-group with a finite cyclic group of order not divisible by p. In particular, if K is tamely ramified, i.e., the degree of K over $\mathbb{Q}_p^{unr}$ is not divisible by p, then $\mathrm{Gal}(K/\mathbb{Q}_p^{unr})$ is a finite cyclic group.

The situation can be generalized to an abelian variety $\mathcal{A}$ of dimension g (which is a higher dimensional analogue of an elliptic curve) over a finite extension of $\mathbb{Q}$. Assume for simplicity that $\mathcal{A}$ is defined over $\mathbb{Q}$. In the case of an abelian variety with good reduction over a finite extension of $\mathbb{Q}_p$ one obtains a $2g$-dimensional complex representation $\rho = \rho_p$ of a semidirect product G of the form $G = (A \rtimes B) \rtimes C$, where A is a p-group, B is a finite cyclic group of an order not divisible by p, and C is an infinite cyclic group. Moreover, there is a one-dimensional representation $\omega = \omega_p$ such that $\rho \otimes \omega$ is symplectic.

One of the main themes in arithmetic algebraic geometry is to study L- and ϵ-functions attached to algebraic varieties, in particular to an abelian variety $\mathcal{A}$ over $\mathbb{Q}$. Inseparable from the theory of L- and ϵ-functions is the notion of a root number—the ratio of an ϵ-function and its absolute value. The importance of studying root numbers lies in the fact that according to several famous conjectures in number theory they are believed to have deep connections to the arithmetic of the subject in question; for example, they may predict the existence of rational solutions to systems of polynomial equations. Moreover, root numbers are much easier to compute than L- and ϵ-functions. By definition, the root number of $\mathcal{A}$ is the product of root numbers $W(\rho_p)$ attached to representations ρ_p of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ over $\mathbb{Q}_l$, where p runs over all prime numbers and the twist of ρ_p by ω_p does not change $W(\rho_p)$.

Our motivation comes from the question of calculating root numbers of $\mathcal{A}$. For that one needs to understand representation ρ_p of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ over $\mathbb{Q}_l$ for an arbitrary prime number p. An important and the most difficult part of the case of a general abelian variety is the case of an abelian variety with good reduction over a finite extension of $\mathbb{Q}_p$. The simple case when K is tamely ramified, i.e., the p-part A of $\mathrm{Gal}(K/\mathbb{Q}_p^{unr})$ is trivial, was addressed in [3]. We now focus on a case when A is a cyclic group. Our main result is Proposition 3.2, which gives a description of symplectic representations of G.

The paper is organized as follows. In Section 1 we show that without loss of generality we can assume that C is finite (Lemma 1.1) and recall the Mackey method of small subgroups (Theorem 1.2). In Section 2 we consider the case when A is a finite abelian group and C is finite with all the other assumptions on G remaining the same (Lemma 2.1). Here we use Theorem 1.2 describing representations of a finite group G via representations of a fixed normal subgroup. Finally, in Section 3 we specialize to the case when A is cyclic (Proposition 3.2).

1. Representation theoretic facts

Lemma 1.1. *Let $C = \langle c \rangle$ be an infinite cyclic group generated by an element c and let E be a finite group. Let $G = E \rtimes C$ be a semi-direct product, where C acts on E via a homomorphism $\alpha : C \longrightarrow \mathrm{Aut}(E)$, and let $\mathrm{Ker}\,\alpha = \langle c^l \rangle$ for some $l \in \mathbb{N}$. Then every irreducible representation λ of G has the following form:*

$$\lambda = \lambda_0 \otimes \phi,$$

where λ_0 is an irreducible representation of G trivial on $\langle c^l \rangle$ and ϕ is a one-dimensional representation of G. In particular, every symplectic irreducible representation of G has finite image.

Proof. Since c^l is contained in the center of G and λ is an irreducible complex representation, by Schur's lemma $\lambda(c^l)$ acts as multiplication by a scalar $a \in \mathbb{C}^\times$. Define a one-dimensional representation ϕ of G as follows: ϕ is trivial on E and $\phi(c)$ equals an l-th root of a. Then $\lambda_0 = \lambda \otimes \phi^{-1}$ is trivial on $\langle c^l \rangle$ and $\lambda = \lambda_0 \otimes \phi$.

Assume now that λ is symplectic. Then λ and its contragredient representation have the same character, which implies that for any $g \in G$ we have

$$\phi(g) \cdot \mathrm{tr}\,\lambda_0(g) = \phi(g)^{-1} \cdot \mathrm{tr}\,\lambda_0(g^{-1}).$$

Taking into account that λ_0 is trivial on $\langle c^l \rangle$, the above equation for $g = c^l$ gives $\phi(c^{2l}) = 1$, i.e., λ can be considered as an irreducible symplectic representation of the finite group $H = G/\langle c^{2l} \rangle \cong E \rtimes C/\langle c^{2l} \rangle$. □

Let G be a finite group and let $N \subseteq G$ be a normal subgroup. The group G acts on the set $\hat{N}$ of isomorphism classes of complex irreducible representations σ of N in the following way: if $\sigma : N \longrightarrow \mathrm{GL}_m(\mathbb{C})$, then $g\sigma : N \longrightarrow \mathrm{GL}_m(\mathbb{C})$ is given by

$$g\sigma(n) = \sigma(g^{-1}ng),\ g \in G,\ n \in N.$$

For $\sigma \in \hat{N}$ we denote by G_σ the stabilizer of σ in G, i.e.,

$$G_\sigma = \{g \in G \,|\, g\sigma \cong \sigma\}.$$

Theorem 1.2 (Mackey method of small subgroups (cf. [1], p. 153, Thm. 6.2))**.** *Let $\sigma \in \hat{N}$ and let $\tau \in \hat{G_\sigma}$ be an irreducible component of $\operatorname{Ind}_N^{G_\sigma} \sigma$. Then $\operatorname{Ind}_{G_\sigma}^G \tau$ is an irreducible representation of G. Moreover, any irreducible representation of G can be obtained in this way. More precisely, let $\lambda \in \hat{G}$ and let $\sigma \in \hat{N}$ be an irreducible component of $\operatorname{Res}_N^G \lambda$. Then there exists an irreducible component $\tau \in \hat{G_\sigma}$ of $\operatorname{Ind}_N^{G_\sigma} \sigma$ such that $\lambda \cong \operatorname{Ind}_{G_\sigma}^G \tau$.*

Proof. Let us show first that $\operatorname{Ind}_{G_\sigma}^G \tau$ is irreducible or, equivalently, $\langle \operatorname{Ind}_{G_\sigma}^G \tau, \operatorname{Ind}_{G_\sigma}^G \tau \rangle = 1$, where $\langle \cdot\,, \cdot \rangle$ denotes the inner product of representations. Using the Frobenius reciprocity theorem we have $\langle \operatorname{Ind}_{G_\sigma}^G \tau, \operatorname{Ind}_{G_\sigma}^G \tau \rangle = \langle \tau, \operatorname{Res}_{G_\sigma}^G \left(\operatorname{Ind}_{G_\sigma}^G \tau\right) \rangle$ and we need to show that τ appears only once in the decomposition of $\mu = \operatorname{Res}_{G_\sigma}^G \left(\operatorname{Ind}_{G_\sigma}^G \tau\right)$ into irreducibles. Let W and V denote representation spaces of μ and τ, respectively, and assume that $W = V^n \oplus V'$, where $n \geq 2$ and V' is a $\mathbb{C}[G_\sigma]$-submodule of W.

Let s be the index $[G : G_\sigma]$ of G_σ in G and let $h_1, \dots, h_s \in G$ denote a set of left coset representatives of G_σ in G with $h_1 = 1$. Then $W = h_1 V \oplus \cdots \oplus h_s V$ and

$$h_1 V \oplus \cdots \oplus h_s V = V^n \oplus V', \quad n \geq 2. \tag{1.1}$$

Let U be a representation space of σ and let $g_1, \dots, g_t \in G_\sigma$ be a set of left coset representatives of N in G_σ. Then $\operatorname{Ind}_N^{G_\sigma} \sigma = g_1 U \oplus \cdots \oplus g_t U$. Note that each $g_i U$ is an N-module and it follows from the definition of G_σ that as N-modules all $g_i U$ are isomorphic to each other. Since τ is a subrepresentation of $\operatorname{Ind}_N^{G_\sigma} \sigma$, this implies $\operatorname{Res}_N^{G_\sigma} \tau \cong \sigma^r$ for some $r \geq 1$. Thus from (1.1) we get $h_1 U^r \oplus \cdots \oplus h_s U^r \cong U^{rn} \oplus V'$, where each $h_j U$ is an N-module and this is an isomorphism of N-modules. Since $n \geq 2$ and $h_1 = 1$, by the uniqueness of decomposition of a module into simple modules we conclude that there exists $h_k \neq 1$ such that $h_k U \cong U$ and hence $h_k \in G_\sigma$. This contradicts the assumptions that h_k is a representative of G_σ in G and $h_k \neq 1$.

Assume now that $\lambda \in \hat{G}$ and $\sigma \in \hat{N}$ is an irreducible component of $\operatorname{Res}_N^G \lambda$. Then by the Frobenious reciprocity theorem $\langle \operatorname{Res}_{G_\sigma}^G \lambda, \operatorname{Ind}_N^{G_\sigma} \sigma \rangle = \langle \operatorname{Res}_N^G \lambda, \sigma \rangle \neq 0$ and hence $\operatorname{Res}_{G_\sigma}^G \lambda$ and $\operatorname{Ind}_N^{G_\sigma} \sigma$ have a common irreducible component $\tau \in \hat{G_\sigma}$. By the previous paragraph $\operatorname{Ind}_{G_\sigma}^G \tau$ is irreducible and $\langle \operatorname{Ind}_{G_\sigma}^G \tau, \lambda \rangle = \langle \tau, \operatorname{Res}_{G_\sigma}^G \lambda \rangle \neq 0$. Since λ is irreducible, this implies $\lambda \cong \operatorname{Ind}_{G_\sigma}^G \tau$. ◻

2. The case when A is abelian.

Lemma 2.1. *Let A be a finite abelian group of order e, let $B = \langle b \rangle$ be a finite cyclic group of order k prime to e, and let $C = \langle c \rangle$ be a finite cyclic group. Let $E = A \rtimes B$ be a semi-direct product with B acting on A and let $G = E \rtimes C$ be a semi-direct product, where C acts on E. Let ψ_1 be a (one-dimensional) representation of A, let $\Gamma = A \rtimes \langle b^x \rangle$ denote the stabilizer of ψ_1 in E, and let ψ_2 be a (one-dimensional) representation of $\langle b^x \rangle$. Then both ψ_1 and ψ_2 can be extended to representations of Γ and denote $\phi = \psi_1 \otimes \psi_2 \in \hat{\Gamma}$. Let $E \rtimes \langle c^s \rangle$ be the stabilizer of $\operatorname{Ind}_\Gamma^E \phi$ in G. Then there exist i and a one-dimensional representation μ of $F = \langle A, b^x, c^s b^i \rangle$ such that*

- $c^s b^i \phi = \phi$,

- $\mathrm{Res}_\Gamma^F \mu = \phi$,
- $\sigma = \mathrm{Ind}_F^G \mu$ *is irreducible, and*
- $|\overline{c^s b^i}| = |c^s|$, *where* $\overline{c^s b^i}$ *denotes the image of* $c^s b^i$ *in* F/Γ *or, equivalently,*

$$[E \rtimes \langle c^s \rangle : F] = x.$$

Moreover, every irreducible representation σ *of* G *can be obtained in this way.*

Proof. Note that since k is prime to e, A is normal in G. Let λ be an irreducible representation of $E = A \rtimes B$. Using Theorem 1.2, λ can be constructed from one-dimensional representation ψ_1 of A in the following way. Let Γ denote the stabilizer of ψ_1 in E. Then $\Gamma = A \rtimes \langle b^x \rangle$ for some non-negative integer $x < k$ and let ψ_2 be a one-dimensional representation of $\langle b^x \rangle$. Then ψ_1 and ψ_2 can be extended to representations of Γ via

$$\begin{aligned} \psi_1(b^{xv}a) &= \psi_1(a), \quad a \in A, \\ \psi_2(b^{xv}a) &= \psi_2(b^{xv}), \end{aligned}$$

and $\lambda = \mathrm{Ind}_\Gamma^E(\psi_1 \otimes \psi_2)$ ([4], p. 62, Prop. 25). Let $\phi = \psi_1 \otimes \psi_2$ and let G_λ denote the stabilizer of λ in G. Then $G_\lambda = E \rtimes \langle c^s \rangle$ for some s, i.e., $c^s\lambda \cong \lambda$ or, equivalently, $\langle c^s\lambda, \lambda \rangle = 1$. Note that Γ is normal in G and $\{1, b, \ldots, b^{x-1}\}$ is a system of representatives for the left cosets of Γ in E. Hence

$$\mathrm{Res}_\Gamma^E(c^s\lambda) \cong c^s\phi \oplus c^s b\phi \oplus \cdots \oplus c^s b^{x-1}\phi$$

and by the Frobenius reciprocity theorem we have

$$1 = \langle c^s\lambda, \lambda \rangle = \langle \mathrm{Res}_\Gamma^E(c^s\lambda), \phi \rangle = \sum_{i=0}^{x-1} \langle c^s b^i \phi, \phi \rangle.$$

This implies that there exists i such that $c^s b^i$ is in the stabilizer of ϕ in G_λ. Denote by F the stabilizer of ϕ in G_λ. Thus $\langle A, b^x, c^s b^i \rangle \subseteq F$ and it is easy to check that the reverse inclusion also holds. Consequently, $F = \langle A, b^x, c^s b^i \rangle$ and as a result F/Γ is cyclic. We will make use of the following lemma:

Lemma 2.2 ([2], p. 97, Exc. (6.17))**.** *Let* N *be a normal subgroup of a finite group* G *such that* G/N *is cyclic. If* $\sigma \in \hat{N}$ *and* $G_\sigma = G$, *then* σ *can be extended to an irreducible representation of* G.

Proof. Assume $\sigma : N \longrightarrow \mathrm{GL}_m(\mathbb{C})$ and let $c \in G$ be a preimage of a generator of G/N under the quotient map, so that $G = \langle N, c \rangle$. Since $G_\sigma = G$, we have $c\sigma \cong \sigma$. In other words, there exists $\phi \in \mathrm{GL}_m(\mathbb{C})$ such that

$$\sigma(c^{-1}nc) = \phi^{-1}\sigma(n)\phi, \quad \forall n \in N. \tag{2.1}$$

Let k be the order of c in G/N, i.e., k is the smallest positive integer satisfying $c^k \in N$. Then $\sigma(c^k)\phi^{-k}$ commutes with $\sigma(n)$ for any $n \in N$ and since σ is irreducible, by Schur's lemma $\sigma(c^k)\phi^{-k} = \lambda I$, where $\lambda \in \mathbb{C}$ and $I \in \mathrm{GL}_m(\mathbb{C})$ is the identity matrix. Denote by $\lambda^{1/k} \in \mathbb{C}$ an arbitrary k-th root of λ. Define $\tilde{\sigma} : G \longrightarrow \mathrm{GL}_m(\mathbb{C})$ as

$$\begin{aligned}\tilde{\sigma}(n) &= \sigma(n), \quad \forall n \in N,\\ \tilde{\sigma}(c) &= \lambda^{1/k}\phi.\end{aligned}$$

In particular, we have $\tilde{\sigma}(c)^k = \sigma(c^k)$. Since N is normal in G, every $g \in G$ can be written (not necessarily in a unique way) as $g = nc^s$, where $n \in N$ and $s \in \mathbb{Z}$. We define

$$\tilde{\sigma}(g) = \tilde{\sigma}(n)\tilde{\sigma}(c)^s.$$

We now check that $\tilde{\sigma}$ is a well-defined representation of G. First, we show that $\tilde{\sigma}(g)$ does not depend on the choice of n and s. Suppose $g = n'c^t$ for $n' \in N$, $t \in \mathbb{Z}$, so that $c^{s-t} \in N$ and hence $s - t$ is divisible by k by the choice of k. We have

$$\tilde{\sigma}(n^{-1}n') = \sigma(n^{-1}n') = \sigma(c^{s-t}) = \sigma(c^k)^{\frac{s-t}{k}} = \tilde{\sigma}(c)^{s-t},$$

which implies $\tilde{\sigma}(nc^s) = \tilde{\sigma}(n'c^t)$. Second, we check that $\tilde{\sigma} : G \longrightarrow \mathrm{GL}_m(\mathbb{C})$ is a homomorphism. Let $g_1 = n_1c^a, g_2 = n_2c^b \in G$, where $n_1, n_2 \in N$ and $a, b \in \mathbb{Z}$. We have

$$\begin{aligned}\tilde{\sigma}(g_1g_2) &= \tilde{\sigma}(n_1c^an_2c^{-a}c^{b+a}) =\\ &= \sigma(n_1c^an_2c^{-a})\tilde{\sigma}(c)^{b+a} = \sigma(n_1)\sigma(c^an_2c^{-a})(\lambda^{1/k})^{b+a}\phi^{b+a},\end{aligned} \tag{2.2}$$

where $\sigma(c^an_2c^{-a}) = \phi^a\sigma(n_2)\phi^{-a}$ by (2.1). Thus (2.2) becomes

$$\tilde{\sigma}(g_1g_2) = (\lambda^{1/k})^{b+a}\sigma(n_1)\phi^a\sigma(n_2)\phi^b = \tilde{\sigma}(g_1)\tilde{\sigma}(g_2).$$

Clearly, $\tilde{\sigma}$ is irreducible and extends σ. $\square$

By Lemma 2.2 there exists a one-dimensional representation μ of F such that $\mathrm{Res}^F_\Gamma \mu = \phi$ and μ is an irreducible component of $\mathrm{Ind}^F_\Gamma \phi$. First, applying Theorem 1.2 to G_λ with a normal subgroup Γ, $\phi \in \hat{\Gamma}$, and an irreducible component μ of $\mathrm{Ind}^F_\Gamma \phi$, we conclude that $\mathrm{Ind}^{G_\lambda}_F \mu$ is irreducible. Second, applying Theorem 1.2 to G with a normal subgroup E, $\lambda \in \hat{E}$, and an irreducible component $\mathrm{Ind}^{G_\lambda}_F \mu$ of $\mathrm{Ind}^{G_\lambda}_E \lambda$, we conclude that $\mathrm{Ind}^G_F \mu = \mathrm{Ind}^G_{G_\lambda} \mathrm{Ind}^{G_\lambda}_F \mu$ is also irreducible.

Conversely, let $\sigma \in \hat{G}$ and let λ be an irreducible component of $\mathrm{Res}^G_E \sigma$. Then in the notation of the proof used above, $\lambda = \mathrm{Ind}^E_\Gamma \phi$ and it is enough to show that there exists an extension μ of ϕ to F such that $\sigma \cong \mathrm{Ind}^G_F \mu$. Note that by Lemma 2.2 there exists $\tilde{\lambda} \in \hat{G}_\lambda$ that extends λ and hence every irreducible component of $\mathrm{Ind}^{G_\lambda}_E \lambda$ has the form $\tilde{\lambda} \otimes \psi$, where ψ is a one-dimensional representation of $\langle c^s \rangle$ considered as a representation of G_λ via inflection. By Theorem 1.2, without loss of generality we can assume that $\sigma \cong \mathrm{Ind}^G_{G_\lambda} \tilde{\lambda}$. Now we will use Theorem 1.2 applied to G_λ with the normal subgroup Γ and $\tilde{\lambda}$. Namely, note that every irreducible component of $\mathrm{Res}^{G_\lambda}_\Gamma \tilde{\lambda}$ has the form $b^j\phi$ and every irreducible component of $\mathrm{Ind}^F_\Gamma \phi$ has the form $\mu \otimes \kappa$, where κ is a one-dimensional representation of $\langle \overline{c^sb^i} \rangle$ considered as a representation of F via inflection. By Theorem 1.2, without loss of generality we can assume that $\tilde{\lambda}$ is obtained from ϕ and μ via $\tilde{\lambda} \cong \mathrm{Ind}^{G_\lambda}_F \mu$ and hence

$\sigma \cong \mathrm{Ind}_F^G \mu$. Moreover, it follows that $x = \dim \tilde{\lambda} = [G_\lambda : F]$, hence $[F : \Gamma] = [G_\lambda : E]$ and $|\overline{c^s b^i}| = |c^s|$. □

Remark 2.3. Note that if A is cyclic, then F is normal in G (see the subsection below). This is not true for a general abelian A. For example, let $A \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $B \cong \mathbb{Z}/3\mathbb{Z}$, and $C \cong \mathbb{Z}/2\mathbb{Z}$. Denote by a_1, a_2 generators of A with the group operation written multiplicatively and define

$$\begin{array}{rcll} c^{-1}bc & = & b^2, & \\ b^{-1}a_1b & = & a_2, & b^{-1}a_2b = a_1a_2, \\ c^{-1}a_1c & = & a_1, & c^{-1}a_2c = a_1a_2, \\ \psi_1(a_1) & = & 1, & \psi_1(a_2) = -1. \end{array}$$

It is easy to check that $G = (A \rtimes B) \rtimes C$ is well defined, $\Gamma = A$ and $c\psi_1 = \psi_1$. Thus $F = \langle A, c\rangle$ and F is not normal in G. Indeed, $bcb^{-1} = cb \notin F$.

3. The case when A is cyclic.

In what follows we will write an action of a cyclic group $\langle b\rangle$ on a group A in the form $b^{-1}ab$, $a \in A$. Since B is cyclic, it is well defined, and it is more convenient for applications to representations. Thus we multiply elements in a semi-direct product $A \rtimes \langle b\rangle$ as follows

$$(a_1, b_1) \cdot (a_2, b_2) = (b_2^{-1}a_1b_2 \cdot a_2, b_1b_2), \quad a_1, a_2 \in A,\ b_1, b_2 \in \langle b\rangle.$$

Lemma 3.1. *Let $E = A \rtimes B$, $A = \langle a\rangle$, $B = \langle b\rangle$, $|a| = e$, $|b| = k$, $(e, k) = 1$, and $b^{-1}ab = a^m$, where $m \in (\mathbb{Z}/e\mathbb{Z})^\times$ and $m^k \equiv 1$ mod e. Then any automorphism θ of E is defined by a triple (r, t, n) via*

$$\theta(a) = a^n, \quad \theta(b) = b^r a^t,$$

where $n \in (\mathbb{Z}/e\mathbb{Z})^\times$, $r \in (\mathbb{Z}/k\mathbb{Z})^\times$, $t \in \mathbb{Z}/e\mathbb{Z}$, $m^r \equiv m$ mod e, and

$$t \cdot (1 + m + m^2 + \cdots + m^{k-1}) \equiv 0 \text{ mod } e. \tag{3.1}$$

Moreover, if $\theta_1 = (r_1, t_1, n_1)$ and $\theta_2 = (r_2, t_2, n_2)$, then $\theta_1 \circ \theta_2 = (r_1r_2, t_1 + t_2n_1, n_1n_2)$. Furthermore, $\theta^{-1} = (r', -n't, n')$ with $n' \equiv n^{-1}$ mod e, $r' \equiv r^{-1}$ mod k, and $\theta^s = (r^s, \alpha_s, n^s)$ with

$$\alpha_s = t \sum_{j=0}^{s-1} n^j. \tag{3.2}$$

Proof. Indeed, note that

$$1 = \theta(b)^k = (b^r a^t)^k = a^{tu},$$

where $u = 1 + m^r + m^{2r} + \cdots + m^{(k-1)r} \equiv 1 + m + m^2 + \cdots + m^{k-1}$ *mod* e, which implies (3.1). Let y denote the order of m in $(\mathbb{Z}/e\mathbb{Z})^\times$. Then y divides both k and $r - 1$, and from (3.1) we get

$$t \cdot (1 + m + m^2 + \cdots + m^{k-1}) \equiv t \cdot (1 + m + m^2 + \cdots + m^{y-1}) \frac{k}{y} \equiv 0 \text{ mod } e. \tag{3.3}$$

Since $(e,k)=1$, we conclude that $t\cdot(1+m+m^2+\cdots+m^{y-1})\equiv 0 \ mod\ e$ and hence $t\cdot(1+m+m^2+\cdots+m^{r-1})\equiv t \ mod\ e$ for any r satisfying $m^r\equiv m \ mod\ e$. To get formulas for $\theta_1\circ\theta_2$ and θ^{-1} note that

$$\theta_1\circ\theta_2(b)=b^{r_1r_2}a^{u+t_2n_1}, \tag{3.4}$$

where $u=t_1(1+m^{r_1}+m^{2r_1}+\cdots+m^{(r_2-1)r_1})\equiv t_1(1+m+m^2+\cdots+m^{r_2-1})\equiv t_1 \ mod\ e$. Using (3.4), formula (3.2) can be easily proved by induction. □

Proposition 3.2. *Let $A=\langle a\rangle$ be a finite cyclic group of order e, let $B=\langle b\rangle$ be a finite cyclic group of order k prime to e, and let $C=\langle c\rangle$ be a finite cyclic group. Let $E=A\rtimes B$ be a semi-direct product with B acting on A via $b^{-1}ab=a^m$ for some $m\in(\mathbb{Z}/e\mathbb{Z})^\times$ and let $G=E\rtimes C$ be a semi-direct product, where C acts on E via $c^{-1}ac=a^n$, $n\in(\mathbb{Z}/e\mathbb{Z})^\times$, $c^{-1}bc=b^ra^t$, $r\in(\mathbb{Z}/k\mathbb{Z})^\times$, $t\in\mathbb{Z}/e\mathbb{Z}$. Let ψ_1 be a (one-dimensional) representation of A, let $\Gamma=A\rtimes\langle b^x\rangle$ denote the stabilizer of ψ_1 in E, and let ψ_2 be a (one-dimensional) representation of $\langle b^x\rangle$. Then both ψ_1 and ψ_2 can be extended to representations of Γ and denote $\phi=\psi_1\otimes\psi_2\in\hat{\Gamma}$. Let $E\rtimes\langle c^s\rangle$ be the stabilizer of $\operatorname{Ind}_\Gamma^E\phi$ in G. Then there exist a unique $i\in\{0,1,\dots,x-1\}$ and a one-dimensional representation μ of $F=\langle A,b^x,c^sb^i\rangle$ such that*

- $c^sb^i\phi=\phi$,
- $\operatorname{Res}_\Gamma^F\mu=\phi$, *and*
- $\sigma=\operatorname{Ind}_F^G\mu$ *is irreducible.*

If, in addition, σ is symplectic, then there exist $g\in\{0,1,\dots,s-1\}$ and $j\in\{0,1,\dots,x-1\}$ such that $\overline{\mu}=\mu_{c^gb^j}$, $(c^gb^j)^2\in F$, and $\mu((c^gb^j)^2)=-1$. Moreover, every irreducible symplectic representation σ of G can be obtained in this way.

Proof. We assume the results of Lemma 2.1 and Lemma 3.1. Note that $m^k\equiv 1 \ mod\ e$ and $m^r\equiv m \ mod\ e$. Then $\psi_1(a)$ is an e-th root of unity of order d in $\mathbb{C}^\times$ and $x=|m|$ in $(\mathbb{Z}/d\mathbb{Z})^\times$. Since d divides e, from $m^r\equiv m \ mod\ e$ we have $r\equiv 1 \ mod\ x$. This implies that the group $F=\langle A,b^x,c^sb^i\rangle$ is normal. Indeed, since A is normal in G, it is enough to show that F/A is normal in G/A. Denoting the images of a, b, and c in G/A again by a, b, and c, respectively, we have

$$\begin{aligned} c^{-1}\cdot b^x\cdot c &= b^{rx},\\ b\cdot c^sb^i\cdot b^{-1} &= c^sb^i\cdot b^{r^s-1},\\ c^{-1}\cdot c^sb^i\cdot c &= c^sb^i\cdot b^{i(r-1)}. \end{aligned}$$

Thus by Lemma 2.1 every irreducible representation of G is induced by a one-dimensional representation from a normal subgroup. Proposition 3.2 then follows from Lemma 3.3 below, which characterizes symplectic irreducible representations of a finite group induced by one-dimensional representations from normal subgroups. □

Lemma 3.3. *Let G be a finite group with a normal subgroup F and let $\sigma=\operatorname{Ind}_F^G\mu$ be an irreducible representation of G induced by a one-dimensional representation μ of F. For*

$g \in G$ let μ_g denote the one-dimensional representation of F given by

$$\mu_g(f) = \mu(g^{-1}fg), \quad f \in F.$$

Let $\overline{\mu}$ denote the contragredient representation of μ. Then σ is symplectic if and only if there exists $t \in G$ such that $\overline{\mu} = \mu_t$, $t^2 \in F$, and $\mu(t^2) = -1$.

Proof. Let χ denote the character of σ. By Proposition 39 on p. 109 in [4], σ is symplectic if and only if

$$\frac{1}{|G|} \cdot \sum_{y \in G} \chi(y^2) = -1. \tag{3.5}$$

Let T denote a system of representatives of F in G. Note that $\mathrm{Res}_F^G \sigma = \bigoplus_{t \in T} \mu_t$ and $\chi(g) = 0$ if $g \notin F$. Thus

$$\sum_{y \in G} \chi(y^2) = \sum_{\substack{t \in T \\ t^2 \in F}} \sum_{f \in F} \chi(t^2 \cdot t^{-1}ft \cdot f) = \sum_{\substack{t \in T \\ t^2 \in F}} \sum_{f \in F} \sum_{t' \in T} \mu_{t'}(t^2)\mu_{t'}(t^{-1}ft)\mu_{t'}(f),$$

where $\sum_{f \in F} \mu_{t'}(t^{-1}ft)\mu_{t'}(f) = |F| \cdot \langle \mu_{(t')^{-1}tt'}, \overline{\mu} \rangle$. Hence

$$\frac{1}{|G|} \cdot \sum_{y \in G} \chi(y^2) = \frac{|F|}{|G|} \cdot \sum_{\substack{t \in T \\ t^2 \in F}} \sum_{t' \in T} \mu_{t'}(t^2) \langle \mu_{(t')^{-1}tt'}, \overline{\mu} \rangle. \tag{3.6}$$

This implies that if σ is symplectic, then there exists $t_0 \in G$ such that ${t_0}^2 \in F$ and $\overline{\mu} = \mu_{t_0}$. Since σ is irreducible, all μ_t's are pairwise distinct and hence from (3.5) and (3.6) we get

$$-1 = \frac{1}{|G|} \cdot \sum_{y \in G} \chi(y^2) = \frac{|F|}{|G|} \cdot \sum_{\substack{t \in T \\ t^2 \in F}} \sum_{t' \in T} \mu_{t'}(t^2) \langle \mu_{(t')^{-1}tt'}, \overline{\mu} \rangle = \mu({t_0}^2),$$

which implies that the conditions in Lemma 3.3 are necessary and it follows from the proof that they are also sufficient. $\square$

Remark 3.4. By Proposition 39 on p. 109 in [4], σ is orthogonal if and only if

$$\frac{1}{|G|} \cdot \sum_{y \in G} \chi(y^2) = 1.$$

Thus it follows from the proof of Lemma 3.3 that σ is orthogonal if and only if there exists $t \in G$ such that $\overline{\mu} = \mu_t$, $t^2 \in F$, and $\mu(t^2) = 1$. In particular, if σ is orthogonal, then either μ is real-valued or the order of G/F is even.

References

[1] Do Ngoc Diep. *Methods of noncommutative geometry for group C*-algebras* (Chapman & Hall/CRC Research Notes in Mathematics, 416. Chapman & Hall/CRC, Boca Raton, FL, 2000).
[2] I. M. Isaacs. *Character theory of finite groups* (Dover Publications, Inc., New York, 1994).
[3] M. Sabitova. Root numbers of abelian varieties. Trans. Amer. Math. Soc., 359 (2007), no. 9, 4259–4284.
[4] J.-P. Serre, *Linear representations of finite groups* (Springer-Verlag, New York-Heidelberg, 1977).

Department of Mathematics, CUNY Queens College, 65-30 Kissena Blvd., Flushing, NY 11367, USA, phone: 646-288-9353, fax: 718-997-5882
E-mail address: Maria.Sabitova@qc.cuny.edu