TWISTED ROOT NUMBERS AND RANKS OF ABELIAN VARIETIES*

Maria Sabitova[†]

*Department of Mathematics, CUNY Queens College,
65-30 Kissena Blvd., Flushing, NY 11367, USA*

January 23, 2013

Abstract

We give a formula for the twisted root number $W(A,\tau)$ associated to an abelian variety A over a number field F and a complex representation τ of the absolute Galois group of F in the case when τ has a real-valued character and the conductors of A and τ are relatively prime. As an application we note that the results of E. Kobayashi for elliptic curves can be generalized to abelian varieties, namely, given the maximal abelian extension F^{ab} of F the rank of $A(F^{ab})$ is infinite provided that both the degree of F over $\mathbb{Q}$ and the dimension of A are odd and the parity conjecture holds for A and all its quadratic twists.

2010 Mathematics Subject Classification: 11G10, 11F80, 11R32.

Introduction

Let A be an abelian variety over a number field F and let τ be a complex continuous finite-dimensional representation with real-valued character of the absolute Galois group $\mathrm{Gal}(\overline{F}/F)$ of F, where $\overline{F}$ denotes a fixed algebraic closure of F. Attached to A and τ there is the twisted root number $W(A,\tau)$, which we denote simply by $W(A)$ when τ is trivial. The root number is a sign in the conjectural functional equation for the L-function of A twisted by τ, and under our assumption on the character of τ it is equal to ± 1. Root numbers are often used for studying and

*Supported by NSF grant DMS-0901230 and by grant 64620-00 42 from The City University of New York PSC-CUNY Research Award Program.

†E-mail address: Maria.Sabitova@qc.cuny.edu

predicting facts about ranks of abelian varieties due to the parity conjecture, one form of which asserts that

$$W(A,\chi) = (-1)^{\mathrm{rank}_{\mathbb{Z}} A^{\chi}(F)}, \tag{1}$$

where χ is a one-dimensional representation of $\mathrm{Gal}(\overline{F}/F)$ of order two (a quadratic character) and A^{χ} is an abelian variety over F obtained from A by twisting by χ.

In this note we prove a formula for $W(A,\tau)$ assuming that the conductors of A and τ are relatively prime. It is a generalization of a well-known formula for elliptic curves. We show that

$$W(A,\tau) = (\mathrm{sign}(\det\tau))^{g} \cdot \det\tau(N) \cdot W(A)^{\dim\tau}, \tag{2}$$

where g is the dimension of A and N is the conductor of A (see Proposition 1 below). We also remark that (2) allows one to apply the proofs of E. Kobayashi's results for elliptic curves [K] to abelian varieties. More precisely, this implies that if (1) holds for any χ, the degree of F over $\mathbb{Q}$ is odd, and the dimension of A is odd, then the rank of $A(F^{ab})$ is infinite. (Here F^{ab} denotes the maximal abelian extension of F contained in $\overline{F}$.) The idea of the proof is to use (2) to prove the existence of infinitely many (linearly independent over $\mathbb{F}_2$ with respect to tensor product) quadratic characters χ satisfying $W(A,\chi) = -1$. The parity conjecture applied to those χ then gives points of infinite order on $A(F^{ab})$ and one is to show that they are linearly independent (see Corollary 5 below for more detail). This argument has restrictions imposed by the use of (1) and cannot be applied in general when the degree of F over $\mathbb{Q}$ or the dimension of A is even (see Remark 6 below).

The rank of $A(F^{ab})$ is expected to be infinite for an arbitrary number field F and an abelian variety A over F; it is a consequence of the conjecture that F^{ab} is ample and the theorem stating that for an ample field F of zero characteristic and an abelian variety A over F the rank of $A(F)$ is infinite [FP].

Root numbers

We fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ and for a number field F by F^{ab} we denote the maximal abelian extension of F contained in $\overline{\mathbb{Q}}$.

Proposition 1. *Let A be an abelian variety of dimension g over a number field F and let N denote the conductor of A. Let τ be a complex continuous finite-dimensional representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ with real-valued character and of conductor f. Assume that f is relatively prime to N. Then*

$$W(A,\tau) = (\mathrm{sign}(\det\tau))^{g} \cdot \det\tau(N) \cdot W(A)^{\dim\tau} \tag{3}$$

(cf. Prop. 10 on p. 337 in [R2]).

Proof. For each place v of F let F_v denote the completion of F with respect to v and let τ_v be the restriction of τ to the decomposition subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ at v. Let $W(A_v, \tau_v)$ be the local root number associated to $A_v = A \times_F F_v$ and τ_v. By definition

$$W(A, \tau) = \prod_v W(A_v, \tau_v),$$

where v runs through all the places of F. If $v = \infty$, then

$$W(A_v, \tau_v) = (-1)^{g \dim \tau} \text{ and hence } W(A_v) = (-1)^g \tag{4}$$

by Lemma 2.1 on p. 4272 in [S]. Suppose $v < \infty$ and let $m_v(A)$ be the exponent of N at v. Then (3) follows from (4) and Proposition 2 below together with

$$\mathrm{sign}(\det \tau) = \prod_{v=\infty} \det \tau_v(-1) = \prod_{v<\infty} \det \tau_v(-1).$$

$\square$

Proposition 2. *Let ϖ_v denote a uniformizer of F_v and suppose that* $\det \tau_v$ *is considered as a multiplicative character of $F_v^\times$ via the local class field theory. Then*

$$W(A_v, \tau_v) = \det \tau_v(-1)^g \cdot \det \tau_v(\varpi_v)^{m_v(A)} \cdot W(A_v)^{\dim \tau}. \tag{5}$$

Proof. Note that $\det \tau_v(\varpi_v)^{m_v(A)}$ does not depend on the choice of ϖ_v, since τ_v is unramified whenever $m_v(A) \neq 0$. To prove (5) we first recall the definition of $W(A_v, \tau_v)$ (see e.g., [S] for more detail). For a rational prime l different from the residual characteristic of F_v let $T_l(A_v)$ be the l-adic Tate module of A_v and let $V_l(A_v)^*$ denote the contragredient of $V_l(A_v) = T_l(A_v) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$. Let $\sigma'_v = \sigma'_{v,A}$ denote a representation of the Weil–Deligne group $\mathcal{W}'(\overline{F}_v/F_v)$ of F_v associated to $V_l(A_v)^*$ via the Deligne–Grothendieck construction (see e.g., [R1]). Then

$$W(A_v, \tau_v) = W(\sigma'_v \otimes \tau_v),$$

where τ_v is viewed as a representation of $\mathcal{W}'(\overline{F}_v/F_v)$. Let ω_v denote the one-dimensional representation of the Weil group $\mathcal{W}(\overline{F}_v/F_v)$ of F_v given by

$$\omega_v|_{I_v} = 1, \quad \omega_v(\Phi_v) = q_v^{-1},$$

where I_v is the inertia subgroup of $\mathrm{Gal}(\overline{F}_v/F_v)$, Φ_v is an inverse Frobenius element of $\mathrm{Gal}(\overline{F}_v/F_v)$, and q_v is the caridnality of the residue field of F_v. By properties of root numbers

$$W(\sigma'_v \otimes \tau_v) = W(\sigma'_v \otimes \omega_v^{1/2} \otimes \tau_v), \tag{6}$$

where $\sigma'_v \otimes \omega_v^{1/2}$ is symplectic.

We now prove (5). Suppose v does not divide N. Then A_v has good reduction over F_v and hence by the criterion of Néron–Ogg–Šhafarevič σ'_v is actually a representation of $\mathcal{W}(\overline{F}_v/F_v)$ trivial on I_v. Since $\sigma'_v \otimes \omega_v^{1/2}$ is symplectic, this implies that

$$\sigma'_v \otimes \omega_v^{1/2} \cong \alpha \oplus \alpha^*$$

for some representation α of $\mathcal{W}(\overline{F}_v/F_v)$. Thus, taking into account that τ_v has finite image and real-valued character, $\det \alpha(-1) = 1$ (α is unramified), and using (6) we have

$$\begin{aligned} W(A_v, \tau_v) = W(\sigma'_v \otimes \omega_v^{1/2} \otimes \tau_v) = W(\alpha \otimes \tau_v) W((\alpha \otimes \tau_v)^*) = \\ = \det(\alpha \otimes \tau_v)(-1) = \det \alpha(-1)^{\dim \tau} \cdot \det \tau_v(-1)^{\dim \alpha} = \det \tau_v(-1)^{\dim \alpha}. \end{aligned} \tag{7}$$

Since $\dim \alpha = g$, $m_v(A) = 0$, and

$$W(A_v) = W(\sigma'_v) = W(\sigma'_v \otimes \omega_v^{1/2}) = \det \alpha(-1) = 1,$$

formula (7) implies (5).

Suppose v does not divide f. Then τ_v is unramified. Let V be a representation space of τ_v, let $\sigma'_v = (\sigma_v, M)$, where σ_v is a representation of $\mathcal{W}(\overline{F}_v/F_v)$ on a complex vector space W and M is a nilpotent endomorphism on W. Denote $U = W \otimes V$ and $U^{I_v}_{M\otimes 1} = (\ker(M \otimes 1))^{I_v}$. By definition, we have

$$W(\sigma'_v \otimes \tau_v) = W(\sigma_v \otimes \tau_v) \cdot \frac{\delta(\sigma'_v \otimes \tau_v)}{|\delta(\sigma'_v \otimes \tau_v)|}, \tag{8}$$

where $\delta(\sigma'_v \otimes \tau_v) = \det \left(-\Phi_v|_{\left(U^{I_v}/U^{I_v}_{M\otimes 1}\right)} \right)$ (see [R1], §§11,12). Since τ_v is an unramified representation of $\mathcal{W}(\overline{F}_v/F_v)$, we have $U^{I_v} \cong W^{I_v} \otimes V$ and $U^{I_v}_{M\otimes 1} \cong W^{I_v}_M \otimes V$, where $W^{I_v}_M = (\ker M)^{I_v}$. Hence,

$$\begin{aligned} \delta(\sigma'_v \otimes \tau_v) = \det \left(-\Phi_v|_{\left(W^{I_v}/W^{I_v}_M\right)} \right)^{\dim \tau} \cdot \det(\Phi_v|_V)^{\dim W^{I_v} - \dim W^{I_v}_M} = \\ = \delta(\sigma'_v)^{\dim \tau} \cdot \det \tau_v(\varpi_v)^{\dim W^{I_v} - \dim W^{I_v}_M}. \end{aligned} \tag{9}$$

Also, since τ_v is unramified and has finite image, for a nontrivial additive character ψ_v of F_v by (3.4.6) on p. 15 in [T] we have

$$W(\sigma_v \otimes \tau_v) = W(\sigma_v)^{\dim \tau} \cdot \det \tau_v(\varpi_v)^{a(\sigma_v) + 2gn(\psi_v)}, \tag{10}$$

where $a(\sigma_v)$ is the exponent of the conductor of σ_v and $n(\psi_v)$ is an integer. Putting (8), (9), and (10) together and taking into account that the determinant of τ_v is ± 1 (because τ_v has finite image and real-valued character) as well as

$$a(\sigma'_v) = a(\sigma_v) + \dim W^{I_v} - \dim W^{I_v}_M,$$

we get

$$W(\sigma_v' \otimes \tau_v) = W(\sigma_v')^{\dim \tau} \cdot \det \tau_v(\varpi_v)^{a(\sigma_v')}.$$

Since $\det \tau_v(-1) = 1$ and by definition $W(\sigma_v') = W(A_v)$ and $a(\sigma_v') = m_v(A)$, this implies (5). □

Remark 3. In what follows by a quadratic character of $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ we mean a one-dimensional (continuous) complex representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ of order 2.

Corollary 4. *Let χ be a quadratic character of $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ of conductor relatively prime to N. Then*

$$W(A^{\chi}) = W(A, \chi) = (\mathrm{sign}(\chi))^{g} \cdot \chi(N) \cdot W(A) \tag{11}$$

(*cf. Cor. on p.* 338 *in* [*R2*]).

The next corollary (Corollary 5 below) is a direct generalization to abelian varieties of a result by E. Kobayashi (Thm. 2 in [K]) for elliptic curves. Using (11), the proof of Corollary 5 is the same as in [K]. Since it is short, we reproduce it for the sake of completeness.

Corollary 5. *Let A be an abelian variety of an odd dimension over a number field $F$of an odd degree over $\mathbb{Q}$. Assuming the parity conjecture* (1) *for A and any quadratic character of* $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$*, we have* $\mathrm{rank}_{\mathbb{Z}}\, A(F^{ab}) = \infty$.

Proof. The first step is to show that there exist infinitely many quadratic characters χ of $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ such that $W(A, \chi) = -1$. The claim follows from (11) provided that one can show the existence of infinitely many quadratic characters χ of $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ such that the conductor of χ is coprime with the conductor N of A, $\chi(N) = 1$, and $\mathrm{sign}(\chi) = -W(A)$. We now repeat the proof in [K] (p. 298–299) of the latter claim. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be all the prime ideals of the ring of integers of F dividing the conductor N of A. Denote by $p_1, \ldots, p_r \in \mathbb{Z}$ the primes lying below $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$, respectively, i.e., $p_i\mathbb{Z} = \mathfrak{p}_i \cap \mathbb{Z}$, $i \in \{1, \ldots, r\}$. Let $l \in \mathbb{Z}$ be a prime satisfying

$$l \equiv \begin{cases} 1 \bmod 4p_1p_2\cdots p_r & \text{if } W(A) = -1, \\ -1 \bmod 4p_1p_2\cdots p_r & \text{if } W(A) = 1. \end{cases}$$

In both cases there are infinitely many such l by the Dirichlet's theorem on arithmetic progressions. Also, among those l we take the ones unramified in F (there are still infinitely many choices). Then

$$K = \mathbb{Q}\left(\sqrt{(-1)^{\frac{l-1}{2}} l}\right)$$

is a quadratic extension of $\mathbb{Q}$ and each p_i splits in K. Hence,

$$L = FK = F\left(\sqrt{(-1)^{\frac{l-1}{2}} l}\right)$$

is a quadratic extension of F (note that $K \not\subseteq F$, since l is ramified in K and unramified in F) and each $\mathfrak{p}_i$ splits in L. Let χ be the quadratic character of $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ corresponding to L, i.e., χ is the quadratic character of $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ with kernel $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$. Since the decomposition subgroup of $\mathrm{Gal}(L/F)$ corresponding to each $\mathfrak{p}_i$ is trivial, the conductor of χ is coprime with the conductor N of A and $\chi(N) = 1$. Finally, one can check that

$$\mathrm{sign}(\chi) = (-1)^{r_0},$$

where r_0 is the number of (infinite) real places of F that ramify in L. In the first case (when $l \equiv 1 \bmod 4$) every real place of F is unramified in L and we have $\mathrm{sign}(\chi) = 1$. In the second case (when $l \equiv -1 \bmod 4$) each real place of F ramifies in L and since the degree of F over $\mathbb{Q}$ is odd, F has an odd number of real places, so that r_0 is odd and $\mathrm{sign}(\chi) = -1$.

In [K] the author writes that the set $\mathfrak{S}$ of all quadratic characters χ of $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ satisfying $W(A^\chi) = -1$ together with the trivial representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ form an $\mathbb{F}_2$-vector space (with respect to tensor product). This does not seem to be true if $W(A) = 1$. Indeed, let $\chi_1, \chi_2 \in \mathfrak{S}$ be two distinct quadratic characters with conductors coprime with the conductor N of A. Then $\chi_1 \otimes \chi_2$ is not trivial with the conductor coprime with N. Using (11), it is easy to check that

$$W(A^{\chi_1 \otimes \chi_2}) = W(A^{\chi_1}) \cdot W(A^{\chi_2}) \cdot W(A),$$

so that $\chi_1 \otimes \chi_2 \notin \mathfrak{S}$ if $W(A) = 1$. However, as follows from the preceding paragraph there are still infinitely many linearly independent (over $\mathbb{F}_2$) quadratic characters χ satisfying $W(A, \chi) = W(A^\chi) = -1$. Let $\chi_1, \chi_2, \ldots \in \mathfrak{S}$ be linearly independent and let $L_i \subset \overline{\mathbb{Q}}$ be the quadratic extension of F corresponding to χ_i, $i \in \{1, 2, \ldots\}$. For any quadratic character χ of $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ we assume the parity conjecture

$$W(A, \chi) = (-1)^{\mathrm{rank}_{\mathbb{Z}} A^\chi(F)},$$

so that for each χ_i there is a point $P_i \in A^{\chi_i}(F)$ of infinite order. Given the non-trivial element σ of $\mathrm{Gal}(L_i/F)$ we identify P_i with an element of the subgroup

$$\{P \in A(L_i) \mid \sigma(P) = -P\}$$

via an isomorphism defining A^{χ_i} as a twist of A by a quadratic character. Then, since P_i has an infinite order, one can easily check that $mP_i \notin A(K)$ for any $m \in \mathbb{Z}$. Finally, one concludes that $P_1, P_2, \ldots$ are linearly independent over $\mathbb{Z}$, for otherwise there exists L_j contained in a compositum $L_{i_1} L_{i_2} \cdots L_{i_k}$, $j \notin \{i_1, i_2, \ldots, i_k\}$. In other words, χ_j is a non-trivial tensor product of some characters in $\{\chi_1, \chi_2, \ldots\}$. This gives a contradiction and thus $A(F^{ab})$ is of infinite rank.

$\square$

Remark 6. If g is even, then there are examples of abelian varieties such that $W(A) = 1$ and $W(A^\chi) = 1$ for any quadratic character χ of $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$, so that the proof of Corollary 5 cannot be applied. For example, we can take $A = E \times E$, a product of two eilliptic curves. Then $\sigma'_{v,A} = \sigma'_{v,E} \oplus \sigma'_{v,E}$ for each place v of F, so that $W(A) = W(E)^2 = 1$ and $W(A^\chi) = W(E,\chi)^2 = 1$. Similarly, if F is of even degree. For example, let F be an imaginary quadratic field such that there exists an elliptic curve E over F with good reduction everywhere. Then $W(E^\chi) = 1$ for every quadratic character χ of $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$. However, under an additional assumption $W(A) = -1$ Corollary 5 remains true for a number field F of an even degree over $\mathbb{Q}$. Indeed, in the notation of the proof of Corollary 5 above one can take primes $l \in \mathbb{Z}$ unramified in F satisfying $l \equiv -1 \bmod 4p_1p_2\cdots p_r$. Then $\mathrm{sign}(\chi) = 1$ and the rest of the proof does not depend on the degree of F and carries over. In particular, each $\mathfrak{p}_i$ still splits in L and $W(A^\chi) = -1$ by (11).

References

[FP] A. Fehm, S. Petersen, *On the rank of abelian varieties over ample fields,* Int. J. Number Theory 6 (2010), no. 3, 579–586.

[K] E. Kobayashi, *A remark on the Mordell–Weil rank of elliptic curves over the maximal abelian extension of the rational number field,* Tokyo J. Math. 29 (2006), no. 2, 295–300.

[R1] D. E. Rohrlich, *Elliptic curves and the Weil-Deligne group*, Elliptic Curves and Related Topics (CRM Proc. Lecture Notes, 4, Amer. Math. Soc., Providence, RI, 1994), 125–157.

[R2] D. E. Rohrlich, *Galois theory, elliptic curves, and root numbers*, Compos. Math. 100 (1996), 311–349.

[S] M. Sabitova, *Root numbers of abelian varieties,* Trans. Amer. Math. Soc., 359 (2007), no. 9, 4259–4284.

[T] J. Tate, *Number theoretic background*, Automorphic forms, Representations, and *L*-Functions, Proc. Symp. Pure Math. **33** – Part 2, Amer. Math. Soc., Providence (1979), 3–26.