

Trace Pairing

Julius Zhang

February 4, 2026

Abstract

We show that the packing map of [NOZ26] that converts a vector of finite field elements to a single element of the ring of integers of a cyclotomic extension has an associated inner product formula. The key idea is that the trace pairing on number fields reduces to a perfect pairing on the rings of integers after reduction modulo an unramified prime. This specializes to the 2-power cyclotomic extension setting, which entails the existence of a self-dual basis that allows for efficient computation of the inner product.

Contents

1 Trace form on finite étale algebras	1
1.1 Trace pairing on number fields	2
1.2 2-power cyclotomic specialization	3
Appendix A Non-abelian example: $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$	4

1 Trace form on finite étale algebras

Definition 1 (Trace). *Let K be a field and A be a finite free K -algebra (unital) of rank n . For $a \in A$, the trace is*

$$\mathrm{Tr}_{A/K}(a) := \mathrm{tr}(\mu_a),$$

where $\mu_a : A \rightarrow A$, $x \mapsto ax$ is the K -linear multiplication map and tr denotes the matrix trace. This is independent of the choice of K -basis [Lan02].¹

Definition 2 (Trace form). *The trace form is the K -bilinear pairing*

$$M_{A/K} : A \times A \rightarrow K, \quad M_{A/K}(a, b) := \mathrm{Tr}_{A/K}(ab).$$

Theorem 1 (Nondegeneracy of the trace form). *Let A be a finite K -algebra of rank n . The following are equivalent:*

¹Readers familiar with arithmetic geometry will recognize this as Grothendieck duality applied to the morphism $\mathrm{Spec} A \rightarrow \mathrm{Spec} K$.

1. A is étale over K (i.e. $A \cong \prod_{i=1}^r L_i$ with each L_i/K a finite separable extension),
2. $B_{A/K}$ is a perfect pairing, i.e. the map $A \rightarrow \text{Hom}_K(A, K)$, $a \mapsto B_{A/K}(a, -)$ is an isomorphism,
3. $\text{disc}(A/K) := \det(\text{Tr}_{A/K}(e_i e_j))_{i,j} \neq 0$ for some (equivalently, any) K -basis $\{e_1, \dots, e_n\}$.

Proof. (1) \Leftrightarrow (2) follows from [Aut, Lemma 49.3.1, Tag 0BJF]. (2) \Leftrightarrow (3): standard linear algebra — the bilinear form is nondegenerate iff its Gram matrix is invertible. \square

Corollary 1 (Dual basis). *If A/K is étale and $\{e_1, \dots, e_n\}$ is a K -basis of A , there exists a unique dual basis $\{e_1^*, \dots, e_n^*\}$ satisfying $\text{Tr}_{A/K}(e_i \cdot e_j^*) = \delta_{ij}$.*

Proof. Immediate from the isomorphism $A \xrightarrow{\sim} \text{Hom}_K(A, K)$ of Theorem 1. \square

Proposition 1 (Inner product recovery — general case). *Let A/K be étale of rank n with basis $\{e_i\}$ and dual basis $\{e_i^*\}$. Define the coordinate maps*

$$\psi : K^n \rightarrow A, \quad (a_1, \dots, a_n) \mapsto \sum_{i=1}^n a_i e_i, \quad \psi^* : K^n \rightarrow A, \quad (b_1, \dots, b_n) \mapsto \sum_{i=1}^n b_i e_i^*.$$

Then for any $\mathbf{a}, \mathbf{b} \in K^n$,

$$\text{Tr}_{A/K}(\psi(\mathbf{a}) \cdot \psi^*(\mathbf{b})) = \langle \mathbf{a}, \mathbf{b} \rangle := \sum_{i=1}^n a_i b_i.$$

Proof. Bilinearity of the trace form and $\text{Tr}_{A/K}(e_i \cdot e_j^*) = \delta_{ij}$. \square

Remark 1. *Proposition 1 holds for any finite étale K -algebra without hypotheses on the Galois group. In the cyclotomic setting of Section 1.1, the Gram matrix is scalar and $\psi^* = (k/d) \cdot \sigma_{-1} \circ \psi$; for a non-abelian example where the Gram matrix is not scalar and no such involution σ_{-1} exists, see Appendix A.*

1.1 Trace pairing on number fields

Consider an extension of number fields $L/K/\mathbb{Q}$. The trace form $M(a, b) = \text{Tr}_{L/K}(ab)$ is a perfect pairing, which restricts to a bilinear pairing on rings of integers: $\text{Tr}_{\mathcal{O}_L/\mathcal{O}_K} : \mathcal{O}_L \rightarrow \mathcal{O}_K$. Let H be the Galois group of L/K and suppose a prime p is unramified in L/K , then the pairing $\text{Tr}_{\mathcal{O}_L/\mathcal{O}_K}$ reduces to a perfect pairing after reduction modulo p , which we denote by $\text{Tr}_H : \mathcal{O}_L/p\mathcal{O}_L \rightarrow \mathcal{O}_K/p\mathcal{O}_K$.

Remark 2. *Notice that the notation implicitly assumes that we are working with the field extension L/K .*

Remark 3. *In the case that $L = \mathbb{Q}(\zeta_{2^d})$, then every odd prime p is unramified.*

1.2 2-power cyclotomic specialization

We now specialize to the setting of [NOZ26]. Let $d = 2^\alpha$, $\mathcal{O} = \mathbb{Z}[X]/(X^d + 1)$, and let $G \subseteq \text{Aut}(\mathcal{O}/p\mathcal{O})$ be a subgroup of automorphisms. We first state and prove the following lemma:

Lemma 1. $\langle \sigma_{4k+1} \rangle = \{\sigma_{4k\alpha+1} : 0 \leq \alpha \leq d/(2k) - 1\}$ as a set.

Proof. The containment \subseteq follows from the binomial theorem: $(4k+1)^n = \sum_{j=0}^n \binom{n}{j} (4k)^j \equiv 1 \pmod{4k}$ for all $n \geq 0$, so every power of $4k+1$ has the form $4k\alpha+1$. To see equality, by [LS18, Lemma 2.4], the left hand side has cardinality $d/(2k)$, which matches the right hand side. \square

Let $\mathcal{B} = \{e_0, \dots, e_{2n-1}\} = \{X^i\}_{0 \leq i < \frac{d}{2k}} \cup \{X^{\frac{d}{2}+i}\}_{0 \leq i < \frac{d}{2k}}$, with the obvious indices and $n = \frac{d}{2k}$, be a basis of $\mathcal{O}/p\mathcal{O}$ over $\mathcal{O}^H/p\mathcal{O}^H$. The key result in the proof is the following:

Proposition 2. For all $a, b \in \{0, \dots, 2n-1\}$,

$$\text{Tr}_H(e_a \cdot \sigma_{-1}(e_b)) = \frac{d}{k} \cdot \delta_{ab}.$$

Proof. Suppose $e_a = X^i$, $e_b = X^j$, and $i \neq j$, then $e_a \cdot \sigma_{-1}(e_b) = X^i \cdot \sigma_{-1}(X^j) = X^{i-j}$. By inspection, this is equal to X^m for some $m \in \{0, \dots, \frac{d}{2k} - 1\} \cup \{\pm \frac{d}{2} + 0, \dots, \pm \frac{d}{2} + \frac{d}{2k} - 1\}$. By the structure theorem $(\mathbb{Z}/2d\mathbb{Z})^\times \cong \langle -1 \rangle \times \langle g \rangle$ where g has order $d/2$ and $\langle g \rangle$ consists of elements $\equiv 1 \pmod{4}$. Since $4k+1 \equiv 1 \pmod{4}$, we have $\sigma_{4k+1} \in \langle g \rangle$, generating the unique subgroup of order $d/(2k)$. Thus $H = \langle \sigma_{-1} \rangle \times \langle \sigma_{4k+1} \rangle$ and $\text{Tr}_H = \text{Tr}_{\langle \sigma_{-1} \rangle} \circ \text{Tr}_{\langle \sigma_{4k+1} \rangle}$.

By Lemma 1, $\text{Tr}_{\langle \sigma_{4k+1} \rangle}(X^m) = \sum_{\alpha=0}^{d/(2k)-1} X^{(4k\alpha+1)m} = X^m \sum_{\alpha=0}^{d/(2k)-1} \omega^\alpha$ where $\omega = X^{4km}$. The rest of the proof follows from a straightforward calculation:

- *Case $m = 0$:* Then $\text{Tr}(X^m) = \text{Tr}(1) = |H| = d/k$.
- *Case $\frac{d}{2k} \nmid m$:* Then $\omega \neq 1$ and $\omega^{d/(2k)} = X^{2dm} = 1$, so ω is a primitive ℓ -th root of unity for some $\ell \mid \frac{d}{2k}$, $\ell > 1$. The sum of all $\frac{d}{2k}$ -th powers of such a root vanishes.
- *Case $\frac{d}{2k} \mid m$:* Then we must have $m = \pm \frac{d}{2}$ by inspection, and hence $\omega = 1$, so $\text{Tr}_{\langle \sigma_{4k+1} \rangle}(\pm X^{d/2}) = \pm \frac{d}{2k} X^{d/2}$. Then $\text{Tr}_{\langle \sigma_{-1} \rangle}(\pm X^{d/2}) = \pm X^{d/2} + \sigma_{-1}(\pm X^{d/2}) = 0$, since $X^d = -1$.

\square

Corollary 2. The set \mathcal{B} is an $\mathcal{O}^H/p\mathcal{O}^H$ -module basis of $\mathcal{O}/p\mathcal{O}$

Proof. For a 2-power cyclotomic extension, every odd prime is unramified, so $\mathcal{O}^H/p\mathcal{O}^H = K_1 \times \dots \times K_r$ is a finite product of fields, and hence $\mathcal{O}/p\mathcal{O}$ is a finite product of K_i -vector spaces and therefore a free $\mathcal{O}^H/p\mathcal{O}^H$ -module. From standard algebraic number theory, the rank of $\mathcal{O}/p\mathcal{O}$ as an $\mathcal{O}^H/p\mathcal{O}^H$ -module is $|\mathbb{Q}(\zeta_{2^d}) : \mathbb{Q}(\zeta_{2^d})^H| = \frac{d}{k} = |\mathcal{B}|$. From Proposition 2, the determinant of the Gram matrix associated to the trace pairing and \mathcal{B} is a unit, so \mathcal{B} spans $\mathcal{O}/p\mathcal{O}$ as an $\mathcal{O}^H/p\mathcal{O}^H$ -module. \square

Corollary 3 (Self-dual inner product identity). *With ψ as in Theorem 2 of [NOZ26],*

$$\psi(\mathbf{a}) = \sum_{i=0}^{d/2k-1} a_i X^i + X^{d/2} \sum_{i=0}^{d/2k-1} a_{d/2k+i} X^i, \quad (1)$$

the dual basis is $(k/d) \cdot \{\sigma_{-1}(e_i)\}$, so $\psi^ = (k/d) \cdot \sigma_{-1} \circ \psi$. Substituting into Proposition 1:*

$$\mathrm{Tr}_H(\psi(\mathbf{a}) \cdot \sigma_{-1}(\psi(\mathbf{b}))) = \frac{d}{k} \cdot \langle \mathbf{a}, \mathbf{b} \rangle.$$

Appendix A Non-abelian example: $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$

The minimal polynomial $x^3 - 2$ has roots $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$, where $\omega = e^{2\pi i/3} = (-1 + i\sqrt{3})/2$. The three embeddings $\sigma_j : \mathbb{Q}(\sqrt[3]{2}) \hookrightarrow \mathbb{C}$ send $\sqrt[3]{2} \mapsto \omega^{j-1}\sqrt[3]{2}$, and since $1 + \omega + \omega^2 = 0$, the trace $\mathrm{Tr}(\sqrt[3]{2}^k) = \sqrt[3]{2}^k(1 + \omega^k + \omega^{2k})$ vanishes unless $3 \mid k$. For the power basis $e_1 = 1, e_2 = \sqrt[3]{2}, e_3 = \sqrt[3]{4}$:

$$G = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 6 \\ 0 & 6 & 0 \end{pmatrix}, \quad G^{-1} = \begin{pmatrix} 1/3 & 0 & 0 \\ 0 & 0 & 1/6 \\ 0 & 1/6 & 0 \end{pmatrix}, \quad \det(G) = -108 \neq 0.$$

The dual basis is $e_1^* = \frac{1}{3}, e_2^* = \frac{1}{6}\sqrt[3]{4}, e_3^* = \frac{1}{6}\sqrt[3]{2}$.

References

- [Aut] The Stacks Project Authors, *The Stacks Project*, Tags 00U0 (étale algebras), 030U (trace and separability), 09E4 (discriminant).
- [Lan02] Serge Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer, 2002.
- [LS18] Vadim Lyubashevsky and Gregor Seiler, *Short, invertible elements in partially splitting cyclotomic rings and applications to lattice-based zero-knowledge proofs*, Advances in Cryptology – EUROCRYPT 2018, LNCS, vol. 10820, Springer, 2018, pp. 204–224.
- [NOZ26] Ngoc Khanh Nguyen, George O’Rourke, and Jiapeng Zhang, *Hachi: Commitments from polynomial evaluation codes with smaller communication and faster verification*, 2026, Cryptology ePrint Archive, Report 2026/156.