MUTUAL DIVISIBILITY IN IWASAWA ALGEBRAS AND THE PRINCIPAL-IDEAL PINCH

JONATHAN WASHBURN

Abstract. We prove that mutual divisibility of two nonzero elements in a unique factorization domain (UFD) forces equality of the generated principal ideals. The proof is a short argument from the uniqueness of irreducible factorization. Specializing to the Iwasawa algebra $\Lambda = \mathbb{Z}_p[\![T]\!]$ (a UFD by the p-adic Weierstrass preparation theorem), we obtain: if $A \mid B$ and $B \mid A$ in Λ, then $(A) = (B)$. This *principal-ideal pinch* is the purely algebraic step that upgrades one-sided Iwasawa-theoretic divisibility results (such as Kato's divisibility and a reverse divisibility from Λ-adic height positivity) into the full cyclotomic Iwasawa Main Conjecture equality $\mathrm{char}_\Lambda X_p = (L_p)$ for each fixed good prime p. We also record a finite-to-infinite capacity obstruction used in companion papers for topological veto arguments.

1. Mutual divisibility in UFDs

The core algebraic observation is entirely elementary.

Lemma 1.1 (Mutual divisibility forces association)**.** *Let R be a unique factorization domain and $A, B \in R \setminus \{0\}$. If $A \mid B$ and $B \mid A$, then A and B are associates: there exists a unit $u \in R^\times$ with $A = uB$.*

Proof. Since R is a UFD, write

$$A = \pi \prod_{i \in I} P_i^{a_i}, \qquad B = \pi' \prod_{i \in I} P_i^{b_i},$$

where $\pi, \pi' \in R^\times$ are units, I is a finite index set, the P_i are pairwise non-associate irreducible elements, and $a_i, b_i \geq 0$.

The divisibility $A \mid B$ means $B = A \cdot c$ for some $c \in R$; comparing irreducible factorizations (which are unique up to units and reordering in a UFD) gives $a_i \leq b_i$ for all $i \in I$.

Similarly, $B \mid A$ gives $b_i \leq a_i$ for all $i \in I$.

Hence $a_i = b_i$ for every i. Therefore

$$\frac{A}{B} = \frac{\pi}{\pi'} \in R^\times,$$

so $A = (\pi/\pi')B$ with π/π' a unit. □

Corollary 1.2 (Principal-ideal equality)**.** *Under the hypotheses of Lemma* **??**, *$(A) = (B)$ as ideals of R.*

Proof. $A = uB$ with $u \in R^\times$ gives $(A) \subset (B)$. $B = u^{-1}A$ gives $(B) \subset (A)$. Hence $(A) = (B)$. □

Remark 1.3 (Necessity of UFD). The UFD hypothesis is essential. In the ring $\mathbb{Z}[\sqrt{-5}]$ (which is not a UFD), we have $2 \mid 6$ and $3 \mid 6$, but $(2) \neq (3)$. More to the point, mutual divisibility can fail to imply association in non-UFD domains; see [**?**, Chapter 1] for examples.

Date: February 2026.

2020 *Mathematics Subject Classification.* Primary 13F15; Secondary 11R23, 13F20.

Key words and phrases. Unique factorization domain, mutual divisibility, Iwasawa algebra, Weierstrass preparation, main conjecture.

2. Application to Iwasawa algebras

We now specialize to the ring central to Iwasawa theory.

Definition 2.1 (Iwasawa algebra)**.** For a prime p, the *Iwasawa algebra* is the formal power series ring $\Lambda := \mathbb{Z}_p[\![T]\!]$, where $\mathbb{Z}_p$ denotes the p-adic integers.

Proposition 2.2 (Λ is a UFD)**.** *$\Lambda = \mathbb{Z}_p[\![T]\!]$ is a unique factorization domain.*

Proof. By the p-adic Weierstrass preparation theorem (see Washington [**?**, §7.1] or Neukirch–Schmidt–Wingberg [**?**, §V.1]), every nonzero $f \in \Lambda$ factors uniquely as

$$f = p^a \cdot g(T) \cdot u(T),$$

where $a \geq 0$ is an integer, $g(T) \in \mathbb{Z}_p[T]$ is a distinguished (monic, with non-leading coefficients in $p\mathbb{Z}_p$) polynomial, and $u(T) \in \Lambda^\times$ is a unit power series. The element p is irreducible in Λ. Distinguished polynomials factor into irreducible distinguished polynomials (using the fact that $\mathbb{Z}_p[T]$ is a UFD, by Gauss's lemma applied to the DVR $\mathbb{Z}_p$). Thus Λ has unique factorization into p and irreducible distinguished polynomials, up to units. □

Theorem 2.3 (Principal-ideal pinch in Λ)**.** *Let $A, B \in \Lambda \setminus \{0\}$ with $A \mid B$ and $B \mid A$. Then $(A) = (B)$ in Λ.*

Proof. Λ is a UFD by Proposition **??**. Apply Lemma **??** and Corollary **??**. □

Corollary 2.4 (IMC equality from two-sided divisibility)**.** *Let $E/\mathbb{Q}$ be an elliptic curve with good reduction at a prime $p \geq 5$, and assume E is modular (by Wiles et al.). Let $\xi_p(T) \in \Lambda$ be a generator of the characteristic ideal $\operatorname{char}_\Lambda X_p(E/\mathbb{Q}_\infty)$ (where X_p is the Pontryagin dual of the p-primary Selmer group over the cyclotomic $\mathbb{Z}_p$-extension), and let $L_p(E,T) \in \Lambda$ be the cyclotomic p-adic L-function (Mazur–Swinnerton-Dyer). If*

(a) *$\xi_p \mid L_p$ in Λ (Kato's one-sided divisibility [**?**]), and*
(b) *$L_p \mid \xi_p$ in Λ (reverse divisibility from Λ-adic height positivity [**?**]),*

then $\operatorname{char}_\Lambda X_p = (L_p)$ as ideals of Λ (equality up to $\Lambda^\times$).

Proof. Apply Theorem **??** with $A = \xi_p$ and $B = L_p$. Hypotheses (a) and (b) give $A \mid B$ and $B \mid A$. Theorem **??** yields $(A) = (B)$, i.e. $\operatorname{char}_\Lambda X_p = (\xi_p) = (L_p)$. □

Remark 2.5 (Sources of the two divisibilities). Condition (a) is the celebrated result of Kato [**?**] for ordinary primes, with supersingular extensions by Kobayashi [**?**] (signed Selmer groups) and Lei–Loeffler–Zerbes [**?**] (Wach modules). Condition (b) is the reverse divisibility established in the companion BSD paper [**?**] via Λ-adic Néron–Tate height positivity. Corollary **??** shows that the algebraic step from two one-sided divisibilities to full Main Conjecture equality is a single application of unique factorization—a one-line argument once the UFD property is in hand.

3. Finite-to-infinite capacity obstruction

We record a combinatorial observation used in companion papers.

Proposition 3.1 (Finite cannot surject onto infinite)**.** *If S is a finite set and T is an infinite set, there is no surjection $f : S \to T$.*

Proof. If $f : S \to T$ is a surjection, then $|T| \leq |f(S)| \leq |S| < \infty$, contradicting $|T| = \infty$. □

Corollary 3.2 (Finite-budget obstruction)**.** *If each operation costs $c > 0$ and the total budget is $B < \infty$, then at most $\lfloor B/c \rfloor$ operations can be performed. In particular, infinitely many operations require infinite budget.*

Proof. n operations cost nc. The constraint $nc \leq B$ gives $n \leq B/c$, hence $n \leq \lfloor B/c \rfloor$. The contrapositive: if infinitely many operations are needed, the cost is $\sum_{n=1}^{\infty} c = \infty > B$. □

Remark 3.3 (Application to topological veto). This elementary budget argument is the algebraic backbone of the topological-capacity veto in [**?**]: when each vortex-line crossing incurs cost $\ln \varphi > 0$ (the link penalty from [**?**]) and the initial data has finite H^1 energy, only finitely many crossings can occur—ruling out blow-up profiles that would require infinitely many.

Acknowledgments

The author thanks the referees for careful reading.

References

[1] J. Washburn, *The Birch and Swinnerton-Dyer conjecture: prime-wise closure via local height diagonalization, Λ-adic reverse divisibility, and a principal-ideal pinch*, preprint, 2026.
[2] J. Washburn, *The canonical reciprocal cost: exact multi-bond minimization, frustration lower bounds, and simultaneous-vs-sequential descent*, preprint, 2026.
[3] J. Washburn, *Alexander-duality linking, link penalties, and the finite-capacity veto in three dimensions*, preprint, 2026.
[4] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Astérisque **295** (2004), ix, 117–290.
[5] S. Kobayashi, *Iwasawa theory for elliptic curves at supersingular primes*, Invent. Math. **152** (2003), 1–36.
[6] A. Lei, D. Loeffler, and S. Zerbes, *Wach modules and Iwasawa theory for modular forms*, Asian J. Math. **14** (2010), 475–528.
[7] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of Number Fields*, 2nd ed., Grundlehren der mathematischen Wissenschaften, vol. 323, Springer, 2008.
[8] P. Samuel, *Unique Factorization Domains*, Tata Institute Lecture Notes, 1964.
[9] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Graduate Texts in Mathematics, vol. 83, Springer, 1997.

Austin, Texas, USA
Email address: washburn.jonathan@gmail.com