On reduction maps and arithmetic dynamics of Mordell–Weil type groups

by

GRZEGORZ BANASZAK and STEFAN BARAŃCZUK (Poznań)

Pamięci Profesora Andrzeja Schinzla

1. Introduction. Let $F$ be an arbitrary number field. Consider the following groups:

- $A(F)$, the Mordell–Weil group of an abelian variety $A/F$;
- $R_{F,S}^\times$, the $S$-unit group, where $S$ is a finite set of ideals in the ring of integers $R_F$;
- $K_{2n+1}(F)$, the algebraic $K$-theory group for some $n \geq 1$.

These groups share numerous properties; we thus handle them together via an appropriate abstract axiomatic setup, and call them Mordell–Weil type groups (cf. [BGK3, Section 2] or [Bar1, Sections 2–4]). In particular, they are equipped with reduction maps modulo prime ideals, enabling investigation of local-global principles (see Remark 1). In this paper we establish two such principles.

For the clarity of exposition, we present our results in terms of Mordell–Weil groups of abelian varieties. For the convenience of those readers whose interests lie in $K$-theory groups and multiplicative groups rather than in abelian varieties, we restate the results appropriately in the Appendix.

The first principle concerns the following problem in arithmetic dynamics. Let $A/F$ be an abelian variety over a number field $F$ such that $\text{End}_\overline{F}(A) = \mathbb{Z}$ (see Remark 2). Let $P \in A(F)$ and let $\phi$ be an endomorphism, i.e., multiplication by a rational integer. Write

2020 Mathematics Subject Classification: Primary 37P15; Secondary 11G10.

Key words and phrases: arithmetic dynamical systems, abelian varieties, reduction maps, Lehmer–Pierce sequences.

Received 1 August 2022; revised 4 May 2023.

Published online 26 June 2023.

DOI: 10.4064/aa220801-17-5
\[ \phi^n = \phi \circ \cdots \circ \phi \]

for the \( n \)th iterate of \( \phi \), and

\[ \mathcal{O}_\phi(P) = \{ \phi^n(P) : n \geq 0 \} \]

for the forward orbit of \( P \). For every prime \( v \) of good reduction we have the orbit \( \mathcal{O}_\phi(P \mod v) \). Denote the set of prime divisors of a nonzero integer \( \alpha \) by \( \text{supp}(\alpha) \). We prove the following theorem in Section 3.

**Theorem 1.1.** Let \( P, Q \in A(F) \) and let \( \phi, \psi \in \text{End}_F(A) = \mathbb{Z} \). The following are equivalent:

- For all but a density zero set of primes \( v \),
  \[ \mathcal{O}_\phi(P \mod v) \cap \mathcal{O}_\psi(Q \mod v) \neq \emptyset. \]

- Either
  \[ \mathcal{O}_\phi(P) \cap \mathcal{O}_\psi(Q) \neq \emptyset, \]
  or we have the singular case: \( \text{supp}(\phi) = \text{supp}(\psi) \) and there is a nonzero torsion point \( T \in A(F) \) of order \( \text{ord} T \) such that \( \text{supp} \left( \text{ord} T \right) \subset \text{supp}(\phi) \) and
  \[ T = \phi^n \psi^m P - \phi^{n'} \psi^{m'} Q \]
  for some nonnegative integers \( n, m, n', m' \) with four possible cases: \( m = n' = 0 \) or \( n = m = 0 \) or \( n' = m' = 0 \) or \( n = m' = 0 \).

Our work was stimulated by Question 22.4 in the recent survey paper on arithmetic dynamics by Benedetto et al. [BI⁺], where the local intersection of two orbits is a part of a local-global formulation of the dynamical Mordell–Lang conjecture.

The second principle we establish in this paper concerns the abelian variety analogue of Lehmer–Pierce sequences with the same prime divisors. Let \( f \in \mathbb{Z}[x] \) be a monic polynomial which factorizes over \( \mathbb{C} \) as \( f(x) = (x - \alpha_1) \cdots (x - \alpha_d) \). The associated Lehmer–Pierce sequence is defined as

\[ \prod_{i=1}^{d} \left| \alpha_i^n - 1 \right| \text{ for } n \geq 1. \]

Its terms are integers; see [EPSW, Example 11.1(4,5)]. Moreover, Lehmer–Pierce sequences are divisibility sequences. Thus the prime divisors of their terms are of interest.

Let \( a_1, \ldots, a_m \) and \( b_1, \ldots, b_l \) be two sequences of pairwise distinct positive integers greater than 1. Define the following two sequences:

\[ x_n = \prod_{i=1}^{m} (1 - a_i^n), \quad y_n = \prod_{j=1}^{l} (1 - b_j^n). \]
In [Ska], M. Skalba proved that if \( \text{supp}(x_n) \subset \text{supp}(y_n) \) for every positive integer \( n \) then for each \( a_i \) which is not a perfect power, there is some \( b_j \) such that \( b_j = a_i^t \) for some positive integer \( t \). He also raised the question whether the assumption that \( a_i \) is not a perfect power can be removed. We answer this question affirmatively (Corollary A.8 in the Appendix).

Sequences (3) have the following direct analogue for elliptic curves \( E/\mathbb{Q} \). If \( P_1, \ldots, P_d \in E(\mathbb{Q}) \) then the associated Lehmer–Pierce sequence can be defined as

\[
\prod_{i=1}^{d} D_{nP_i},
\]

where \( D_P \) denotes the square root of the denominator of the \( x \)-coordinate of \( P \in E(\mathbb{Q}) \).

In general, i.e., for an abelian variety over a number field, we can define the analogue of the set of prime divisors of the terms of Lehmer–Pierce sequences as follows. Let \( A/F \) be an abelian variety over a number field \( F \) such that \( \text{End}_F(A) = \mathbb{Z} \). For \( X \subset A(F) \) define the support of \( X \), to be the set of all prime ideals \( v \) such that \( P \mod v = 0 \) for some \( P \in X \). In Section 4 we prove the following.

**Theorem 1.2.** Let \( P_1, \ldots, P_r, Q_1, \ldots, Q_s \in A(F) \) be points of infinite order. Assume that for each positive integer \( n \),

\[
\text{supp}\{nP_1, \ldots, nP_r\} \subset \text{supp}\{nQ_1, \ldots, nQ_s\}.
\]

Then for every \( i = 1, \ldots, r \) there exists \( j \in \{1, \ldots, s\} \) such that

\[ f_j Q_j = g_i P_i \]

for some nonzero integers \( f_j, g_i \). In particular, suppose that any of the following conditions holds:

(C1) The torsion part of the subgroup of \( A(F) \) generated by \( P_1, \ldots, P_r, Q_1, \ldots, Q_s \) is trivial.

(C2) The points \( Q_1, \ldots, Q_s \) are pairwise linearly independent.

Then we can take \( f_j = 1 \) for every \( i = 1, \ldots, r \).

Let \( X \) be a finite subset of \( A(F) \). A point \( P \in X \) will be called a maximal multiple in \( X \) when \( mP \notin X \) for every \( m \in \mathbb{Z} \) such that \( |m| > 1 \). Denote

\[
\text{M}(X) = \{ \pm P : P \text{ is a maximal multiple in } X \}.
\]

We get the following immediate corollary of Theorem 1.2.

**Corollary 1.3.** Let \( P_1, \ldots, P_r, Q_1, \ldots, Q_s \in A(F) \) be points of infinite order such that the torsion part of the subgroup of \( A(F) \) they generate is trivial. The following are equivalent:
• For each \( n \in \mathbb{N} \),
\[
\text{supp}(\{nP_1, \ldots,nP_r\}) = \text{supp}(\{nQ_1, \ldots,nQ_s\}).
\]
• \( M(\{P_1, \ldots, P_r\}) = M(\{Q_1, \ldots, Q_s\}) \).

**Remark 1.** Research on reduction maps has a long history. The first author was inspired to work with reduction maps by the question of Reinhard Laubenbacher and Bruce Magurn at the Conference on Algebraic \( K \)-theory and Algebraic Topology, Lake Louise 1991, concerning the nontriviality of the reduction map \( K_5(\mathbb{Z}) \to K_5(\mathbb{F}_p) \) in \( K \)-theory. This problem was solved in a much more general form [AB1, Prop. 1, p. 68], and the result was applied to compute orders of Postnikov invariants [AB1, Sections 4 and 5]. This result was further generalized to arithmetic curves in [AB2]. Later on, numerous results on reduction maps of abelian varieties were obtained; see the comments following Theorem 2.3.

Another important application of reduction maps concerns local to global principles in number fields, algebraic \( K \)-theory and abelian and semiabelian varieties. One example is number-theoretical Erdős’ Support Problem, solved in [C-RS]; its numerous generalizations and variations can be found in [C-RS, BGK1, BGK2, L, KP, Bar1, Bar2, Rz]. The second example, closely related to the previous one, is the problem of detecting linear dependence via reduction maps, considered by many authors [Sch2, Ko, We, BGK3, GG, B, Pe2, BK1, JP, BK2, Jo, Rz, Bar3, B1].

**Remark 2.** Frequently in our proofs, it is necessary to control the order of \( \phi P \) for any endomorphism \( \phi \), knowing the order of a point \( P \). This is the reason for our assumption that \( \text{End}_F(A) = \mathbb{Z} \), since then we have \( \text{ord} \phi P = \text{ord} P/\gcd(\phi, \text{ord} P) \). In general, we do not have such control, even for abelian varieties with commutative endomorphism ring.

2. An auxiliary technical result. Let \( A/F \) be an abelian variety over a number field \( F \). For all but finitely many prime ideals \( v \) in the ring of integers \( \mathcal{O}_F \) we have the reduction maps \( r_v : A(F) \to A_v(\kappa_v) \) where \( \kappa_v = \mathcal{O}_F/v \). For a prime number \( l \) let \( A_v(\kappa_v)_l \) denote the \( l \)-torsion part of the group \( A_v(\kappa_v) \). Throughout the paper, we frequently use the following technical result.

**Theorem 2.1.** Let \( P_1, \ldots, P_s \in A(F) \) be linearly independent points over \( \text{End}_F(A) \). Then for any finite set \( \{l_1, \ldots,l_d\} \) of prime numbers and a matrix \( [k_{ij}]_{1 \leq i \leq s, 1 \leq j \leq d} \) of nonnegative integers there is a set of primes \( v \) of positive density such that for all \( 1 \leq i \leq s \) and \( 1 \leq j \leq d \) the order of the image of the point \( P_i \) under the map
\[
A(F) \to A_v(\kappa_v)_{l_j}
\]
is equal to \( l_j^{k_{ij}} \).
Let us look closer at the particular case of Theorem 2.1 where we reduce only one point. Denote the order of \( r_v(P) \) by \( \text{ord}_v P \). We have the following immediate corollary of Theorem 2.1.

**Corollary 2.2.** If \( P \in A(F) \) is nontorsion then for every pair \((n,m)\) of coprime natural numbers there exists a positive density set \( S \) of primes such that for every \( v \in S \), \( n \) divides \( \text{ord}_v P \) and is coprime to \((\text{ord}_v P)/n\), and \( m \) does not divide \( \text{ord}_v P \).

As a by-product of the proof of Theorem 2.1, we obtain the following result on potential independence of Kummer towers. Recall that extensions \( L_1, \ldots, L_n \) of a field \( K \) are called independent if \( L_{i+1} \cap L_1 \cdots L_i = K \) for every \( i = 1, \ldots, n - 1 \). For the description of the Kummer extensions \( F_{l^m}(\frac{1}{l^m} \Gamma) \), see [BGK3, Section 2] and [Bar1, Section 4]; in particular, \( F_{l^m} := F(A[l^m]) \), and for any subgroup \( \Gamma < A(F) \) we define \( \frac{1}{l^m} \Gamma := \{ R \in A(\bar{F}) : l^m R \in \Gamma \} \).

**Theorem 2.3.** Let \( \Gamma \) be a free \( \text{End}_F(A) \) submodule of \( A(F) \) and \( \{l_1, \ldots, l_d\} \) be a finite set of prime numbers. Then the Kummer extensions \( F_{l_i}^{\infty}(\frac{1}{l_i} \Gamma)/F \), where \( F_{l_i}^{\infty}(\frac{1}{l_i} \Gamma) := \bigcup_{m \geq 1} F_{l_i}^m(\frac{1}{l_i} \Gamma) \), are potentially independent, i.e., there exists a finite field extension \( F'/F \) such that the extensions \( F_{l_i}^{\infty}(\frac{1}{l_i} \Gamma)/F' \) are independent.

Theorem 2.1 as stated here for abelian varieties, was proved by geometrical means in [Pe1, Proposition 12]. Using a different, rather algebraic approach, we are able to generalize it to all Mordell–Weil type groups. It is an essential strengthening of [AB1, Prop. 1, p. 68], [BGK1, Section 2], [BGK2, Prop. 2.19, Cor. 2.22], [P, Theorem 4.4], [BGK3, Theorem 3.1], [Bar1, Theorem 5.1] and [BK1, Theorems 2.6, 2.7], inasmuch as they give control over the \( l \)-part of the orders for one prime number \( l \) only.

As to Corollary 2.2 let us recall the following result of Silverman and Cheon and Hahn.

**Theorem** ([Sil, Proposition 10] for \( F = \mathbb{Q} \) and [CH, Theorem] for any number field \( F \)). Let \( E \) be an elliptic curve over a number field \( F \). If \( P \in E(F) \) is nontorsion then there exists a natural number \( N \) such that for every natural number \( n > N \) there exists a prime \( v \) such that \( \text{ord}_v P = n \).

For multiplicative groups of number fields, there is an analogous result due to Schinzel [Sch1, Theorem 1]. No such theorem, however, is known for \( K \)-theory groups of number fields. So our \( K \)-theory analogue of Corollary 2.2 stated in the Appendix (Corollary A.2), is the only known result in this direction.

The tools to prove Theorem 2.1 are Kummer theory for abelian varieties and the version of the Chebotarev theorem stated in Lemma 2.4 and Corollary 2.5 below.
Let $L_1, \ldots, L_n$ be finite Galois extensions of a number field $K$. For every tuple $(\sigma_1, \ldots, \sigma_n) \in \text{Gal}(L_1/K) \times \cdots \times \text{Gal}(L_n/K)$ let

$$P(\sigma_1, \ldots, \sigma_n)$$

denote the set of all prime ideals $v$ of $K$ unramified in every $L_i$ such that for every $i$ there exists a prime ideal $w_i | v$ of $L_i$ satisfying

$$\sigma_i = \left( \frac{L_i/K}{w_i} \right)$$

where the right-hand side is the Frobenius automorphism of $w_i$ over $K$.

**Lemma 2.4.** Let $L_1, \ldots, L_n$ be independent finite Galois extensions of a number field $K$, i.e., $L_{i+1} \cap L_1 \cdots L_i = K$ for every $i = 1, \ldots, n-1$. For every tuple $(\sigma_1, \ldots, \sigma_n) \in \text{Gal}(L_1/K) \times \cdots \times \text{Gal}(L_n/K)$ the set $P(\sigma_1, \ldots, \sigma_n)$ has density

$$\frac{\prod_{i=1}^{n} \#\langle \sigma_i \rangle}{\#\text{Gal}(L_1 \cdots L_n/K)}$$

where $\langle \sigma_i \rangle$ denotes the conjugacy class of $\sigma_i$ in $\text{Gal}(L_i/K)$.

**Proof.** Since $L_1, \ldots, L_n$ are independent Galois extensions, the composition $L_1 \cdots L_n$ is Galois over $K$ and we have the canonical isomorphism

$$(6) \quad \varphi: \text{Gal}(L_1 \cdots L_n/K) \to \text{Gal}(L_1/K) \times \cdots \times \text{Gal}(L_n/K)$$

defined by restrictions. Let $\sigma$ be the image of $(\sigma_1, \ldots, \sigma_n)$ via $\varphi^{-1}$. By the Chebotarev density theorem the set $P(\sigma)$ has density

$$\frac{\#\langle \sigma \rangle}{\#\text{Gal}(L_1 \cdots L_n/K)}.$$

Our extensions are Galois and independent, so for any prime ideals $w_1, \ldots, w_n$ in $O_{L_1}, \ldots, O_{L_n}$ resp. there is exactly one prime ideal $w$ in $O_{L_1 \cdots L_n}$ such that $w \cap O_{L_i} = w_i$ for every $i = 1, \ldots, n$. For such $w$ we have

$$\varphi \left( \left( \frac{L_1 \cdots L_n/K}{w} \right) \right) = \left( \frac{L_1/K}{w_1}, \ldots, \frac{L_n/K}{w_n} \right)$$

(see e.g. [Jan, Property 2.5, p. 100]). Because $\#\langle \sigma \rangle = \prod_{i=1}^{n} \#\langle \sigma_i \rangle$ and $\#\text{Gal}(L_1 \cdots L_n/K) = \prod_{i=1}^{n} \#\text{Gal}(L_i/K)$, we are done. □

**Corollary 2.5.** Under the assumptions of Lemma 2.4 let $K_0$ be a subfield of $K$ such that $K/K_0$ is finite Galois and all $L_i/K_0$ are finite Galois. Let $\sigma \in \text{Gal}(L_1 \cdots L_n/K_0)$ correspond to $(\sigma_1, \ldots, \sigma_n) \in \text{Gal}(L_1/K) \times \cdots \times \text{Gal}(L_n/K)$ via isomorphism (6). Then the set $P_0$ of prime ideals $v_0$ in $O_{K_0}$ such that there is a prime ideal $w$ in $O_{L_1 \cdots L_n}$ above $v_0$ for which

$$\left( \frac{L_1 \cdots L_n/K_0}{w} \right) = \sigma$$
has positive density

\[ C_0 \prod_{i=1}^{n} \frac{\#(\sigma_i)}{\#\text{Gal}(L_i/K)} \]

where \( C_0 = C_0(\sigma_1, \ldots, \sigma_n) \) is an effectively computable rational number with \( 0 < C_0 \leq 1 \).

**Proof.** Let \( G \) be a finite group and \( H \) its normal subgroup. Denote, for \( h \in H \),

\[ \text{Cl}_H(h) := \{ ghg^{-1} : g \in H \}, \]
\[ N_{\text{Cl}_H(h)} := \{ g \in G : g^{-1} \text{Cl}_H(h)g = \text{Cl}_H(h) \}. \]

Then \( H \) is a normal subgroup of \( N_{\text{Cl}_H(h)} \). Since \( H \) is a normal subgroup of \( G \), we easily see that for every \( g \in G \),

\[ g \text{Cl}_H(h)g^{-1} = \text{Cl}_H(ghg^{-1}) , \]

and for all \( g_1, g_2 \in G \),

\[ \text{Cl}_H(g_1h_{g_1}^{-1}) = \text{Cl}_H(g_2h_{g_2}^{-1}) \iff g_2^{-1}g_1 \in N_{\text{Cl}_H(h)}. \]

It follows that

\[ |\text{Cl}_G(h)| = [G : N_{\text{Cl}_H(h)}]|\text{Cl}_H(h)|, \]

so

\[ (7) \quad \frac{|\text{Cl}_G(h)|}{|G|} = \frac{[G : N_{\text{Cl}_H(h)}]}{[G : H]} \frac{|\text{Cl}_H(h)|}{|H|}. \]

Put \( G := \text{Gal}(L_1 \ldots L_n/K_0) \) and \( H := \text{Gal}(L_1 \ldots L_n/K) \). In view of the Chebotarev density theorem and \( [7] \) the density of \( P_0 \) equals

\[ \frac{|\text{Cl}_G(\sigma)|}{|G|} = \frac{[G : N_{\text{Cl}_H(\sigma)}]}{[G : H]} \frac{|\text{Cl}_H(\sigma)|}{|H|}. \]

Take \( C_0 := [G : N_{\text{Cl}_H(\sigma)}]/[G : H] \). \( \blacksquare \)

**Proof of Theorem 2.1.** For every \( i \in \{1, \ldots, s\} \) denote by \( A_i \) the set of those prime numbers \( l_j \) for which \( k_{ij} > 1 \). Replacing each \( P_i \) by \( \prod_{l \in A_i} l^{k_{ij} - 1} P_i \) we can assume without loss of generality that all positive exponents \( k_{ij} \) are 1. Indeed, if \( P \) is an element in a group, \( l \) is a prime number and \( e > 1 \) is a natural number, then the order of \( P \) equals \( l^e \) if and only if the order of \( l^{e-1}P \) equals \( l \).

For every \( 1 \leq j \leq d \) partition the set \( \{P_1, \ldots, P_s\} \) as \( P_j \cup Q_j \), where \( P_j \) consists of those points for which the exponents \( k_{ij} \) are 1, and \( Q_j \) of those for which they are 0.
We make use of the following diagram of fields:

\[
\begin{align*}
F_{l_j}^{k+1}(\frac{1}{l_j^k} \hat{\Pi}_j, \frac{1}{l_j^k} \hat{\Sigma}_j) & \quad \sigma_j \quad F_{l_j}^{k+1}(\frac{1}{l_j^{k-1}} \hat{\Pi}_j, \frac{1}{l_j^k} \hat{\Sigma}_j) \\
F_{l_j}^{k}(\frac{1}{l_j^k} \hat{\Pi}_j, \frac{1}{l_j^k} \hat{\Sigma}_j) & \quad h_j \quad F_{l_j}^{k} \\
F_{l_j} & \quad F
\end{align*}
\]

where \( \Pi_j \) (resp., \( \Sigma_j \)) is the End\(_F\)(\(A\))-submodule of \(A(F)\) generated by the points in \(P_j\) (resp., in \(Q_j\)), and the fields are Kummer extensions defined as in [Bar1, Section 4].

By [Bar1, Steps 1 and 2 of the proof of Theorem 5.1], for \(k\) large enough there exist:

- an automorphism \(\sigma_j \in G(F_{l_j}^{k}(\frac{1}{l_j^k} \hat{\Pi}_j, \frac{1}{l_j^k} \hat{\Sigma}_j)/F_{l_j}^{k}(\frac{1}{l_j^{k-1}} \hat{\Pi}_j, \frac{1}{l_j^k} \hat{\Sigma}_j))\) such that \(\sigma_j\) maps under the Kummer map
  \[G\left(F_{l_j}^{k}(\frac{1}{l_j^k} \hat{\Pi}_j, \frac{1}{l_j^k} \hat{\Sigma}_j)/F_{l_j}^{k}(\frac{1}{l_j^{k-1}} \hat{\Pi}_j, \frac{1}{l_j^k} \hat{\Sigma}_j)\right) \rightarrow (A[l_j])^{#P_j}\]
  to an element whose \(#P_j\) projections on the direct summands \((A[l_j])^{#P_j}\) are all nontrivial,
- a nontrivial homothety \(h_j \in G(F_{l_j}^{k+1}/F_{l_j}^{k})\) whose action on the module \(T_{l_j}\) is multiplication by \(1 + l_j^k u_0\) for some \(u_0 \in (\mathbb{Z}_{l_j})^\times\),
- an automorphism
  \[\gamma_j \in G\left(F_{l_j}^{k+1}(\frac{1}{l_j^k} \hat{\Pi}_j, \frac{1}{l_j^k} \hat{\Sigma}_j)/F\right)\]
  such that
  \[\gamma_j|_{F_{l_j}^{k}(\frac{1}{l_j^k} \hat{\Pi}_j, \frac{1}{l_j^k} \hat{\Sigma}_j)} = \sigma_j \quad \text{and} \quad \gamma_j|_{F_{l_j}^{k+1}} = h_j.\]

Now, for a while, we make the technical assumption that

\[F = F(A[l_1], \ldots, A[l_d]).\]

It follows that for every \(1 \leq j \leq d\) the degree of the field extension
Reduction maps of Mordell–Weil type groups

\[ F_{l,j}^{k+1}(\frac{1}{l_j} \tilde{H}_j, \frac{1}{l_j} \tilde{\Sigma}_j)/F \text{ is a power of } l_j. \] So the extensions \( F_{l,j}^{k+1}(\frac{1}{l_j} \tilde{H}_j, \frac{1}{l_j} \tilde{\Sigma}_j)/F \) are independent, and by Lemma 2.4 the set \( P(\gamma_1, \ldots, \gamma_n) \) has positive density.

Arguing for each \( l_j \) as in [Bar1, Steps 3 and 4 of the proof of Theorem 5.1], we find that for every prime \( v \) in \( P(\gamma_1, \ldots, \gamma_n) \) and every \( 1 \leq j \leq d \) the orders of the \( r_v \)-images of the points in \( \mathcal{P}_j \) equal \( l_j \) and the \( r_v \)-images of the points in \( Q_j \) are trivial.

It remains to show that the assumption (8) can be skipped. Indeed, by Corollary 2.5 the density remains positive. Moreover, if \( F'/F \) is a finite Galois extension and \( v \) a prime in \( F' \) and \( w \) a prime in \( F' \) over \( v \) then the orders of a point \( P \in A(F) \subset A(F') \) modulo \( v \) and modulo \( w \) are equal.

3. Proof of Theorem 1.1. The main ingredients of the proof of Theorem 1.1 are Theorem 2.1, Proposition 3.2, and the following lemma, itself an analogue of Theorem 1.1 for rational integers (cf. [Sch2, Theorem 2]).

**Lemma 3.1.** Let \( a_1, s_1, a_2, s_2 \) be nonzero rational integers. The exponential equation

\[
a_1 s_1^{w_1} + a_2 s_2^{w_2} = 0
\]

has, modulo every natural number, a solution in nonnegative integers \( w_1, w_2 \) if and only if one of the following holds:

- There are nonnegative integers \( u_1, u_2 \) such that \( a_1 s_1^{u_1} + a_2 s_2^{u_2} = 0. \)
- There are integers \( u_1, u_2 \) such that \( a_1 s_1^{u_1} + a_2 s_2^{u_2} = 0 \) and \( \text{supp}(s_1) = \text{supp}(s_2). \)

**Proof.** \((\Rightarrow)\) Suppose that (9) has, modulo every natural number, a solution in nonnegative integers \( w_1, w_2 \). In particular, this means that there is such a solution to (9) rewritten as

\[-\frac{a_1}{a_2} = (s_1^{-1})^{w_1} s_2^{w_2}\]

for all but finitely prime numbers \( p \). Hence by [Sch2, Theorem 2], there are rational integers \( u_1, u_2 \) such that

\[ a_1 s_1^{u_1} + a_2 s_2^{u_2} = 0. \]

If both \( u_1, u_2 \) are nonnegative we are done. If not, there are two cases to consider.

First, suppose that there are nonnegative \( u_1 \) and positive \( u_2 \) such that

\[ a_1 s_1^{u_1} + a_2 s_2^{-u_2} = 0. \]

If \( s_2 = \pm 1 \) then we can replace \( u_2 \) by \(-u_2\) and get a nonnegative solution. So assume \( s_2 \neq \pm 1 \). By (10) we have \( a_2 = -a_1 s_1^{u_1} s_2^{u_2} \). Substituting this to (9) we get

\[ a_1 s_1^{w_1} = a_1 s_1^{u_1} s_2^{u_2+w_2}. \]
This equation, modulo every natural number, has a solution, and so does the equation
\[ s_1^{w_1} = s_1^{u_1} s_2^{u_2+w_2}, \]
obtained by cancelling \( a_1 \). If there exists a prime number \( p \) such that \( p \mid s_2 \) but \( p \nmid s_1 \) then (11) modulo \( p \) cannot have a solution, a contradiction. Thus \( \text{supp}(s_2) \subseteq \text{supp}(s_1) \). Consider the following two sets of prime numbers:
\[ P_1 = \text{supp}(s_1) \setminus \text{supp}(s_2), \quad P_2 = \text{supp}(s_2). \]
Since we have assumed \( s_2 \neq \pm 1 \), the set \( P_2 \) is nonempty. For every prime number \( p \mid s_1 \) let \( p^{e_p} \) be the maximal power of \( p \) dividing \( s_1 \). Define
\[ n_1 = \prod_{p \in P_1} p^{e_p u_1+1} \quad \text{and} \quad n_2 = \prod_{p \in P_2} p^{e_p u_1+1}. \]
These numbers are coprime and greater than 1. The right-hand side of (11) equals 0 modulo \( n_2 \), hence so does the left-hand side. Thus \( w_1 > u_1 \).
Hence the left-hand side of (11) vanishes modulo \( n_1 \), but the right-hand side does not. This contradiction shows that the set \( P_1 \) is empty, so \( \text{supp}(s_2) = \text{supp}(s_1) \).

Now assume that there are positive \( u_1, u_2 \) such that
\[ a_1 s_1^{-u_1} + a_2 s_2^{-u_2} = 0, \]
so \( a_1 s_2^{u_2} + a_2 s_1^{u_1} = 0 \). Proceeding as above we find that the equation
\[ s_1^{u_1+w_1} = s_2^{u_2+w_2}, \]
modulo every natural number, has a solution. Thus \( \text{supp}(s_1) = \text{supp}(s_2) \).

\((\Rightarrow)\) Only the second case with \( S := \text{supp}(s_1) = \text{supp}(s_2) \) needs to be explained. As above, we consider two cases.

First, suppose that there are nonnegative \( u_1, u_2 \) such that \( a_1 s_1^{u_1} + a_2 s_2^{-u_2} = 0 \). We have to show that the equation \( s_1^{w_1} = s_1^{u_1} s_2^{u_2+w_2} \), modulo every natural number \( n \), has a solution in nonnegative integers \( w_1, w_2 \). Factorize \( n = n_1 n_2 \) where \( \text{supp}(n_1) \subseteq S \), and \( \text{supp}(n_2) \cap S = \emptyset \). Put \( w_1 \) large enough so that \( n_1 \mid s_1^{w_1} \), and the order of \( s_1 \) in \((\mathbb{Z}/n_2\mathbb{Z})^\times\) divides \( w_1 - u_1 \), and put \( w_2 \) large enough so that \( n_1 \mid s_2^{u_2+w_2} \), and the order of \( s_2 \) in \((\mathbb{Z}/n_2\mathbb{Z})^\times\) divides \( u_2 + w_2 \).

Now suppose that there are nonnegative \( u_1, u_2 \) such that \( a_1 s_1^{-u_1} + a_2 s_2^{-u_2} = 0 \). We have to show that the equation \( s_1^{u_1+w_1} = s_2^{u_2+w_2} \), modulo every natural number \( n \), has a solution in nonnegative integers \( w_1, w_2 \). Factorize \( n \) as above and take \( w_1 \) large enough so that \( n_1 \mid s_1^{u_1+w_1} \), and the order of \( s_1 \) in \((\mathbb{Z}/n_2\mathbb{Z})^\times\) divides \( w_1 + u_1 \), and take \( w_2 \) large enough so that \( n_1 \mid s_2^{u_2+w_2} \), and the order of \( s_2 \) in \((\mathbb{Z}/n_2\mathbb{Z})^\times\) divides \( w_2 + u_2 \). \( \blacksquare \)
Fix the following notation:

- $\Lambda_{\text{tors}}$ the torsion part of a subgroup $\Lambda < A(F)$;
- $\text{ord } T$ the order of a torsion point $T \in A(F)$;
- $\text{ord}_v P$ the order of a point $P \mod v$;
- $l^k \| n$ means that $l^k$ exactly divides $n$, i.e. $l^k | n$ and $l^{k+1} \nmid n$, where $l$ is a prime number, $k$ a positive integer, and $n$ a natural number.

**Proposition 3.2.** For almost all $v$ the map $A(F)_{\text{tors}} \to A_v(\kappa_v)$ is injective.

**Proof.** See [K, Lemma in the Appendix]. This follows also from [BGK2, Lemma 2.13].

Before we proceed to the proof of Theorem 1.1, let us recall the following elementary but nonetheless very useful fact. Let $P, Q$ be elements of finite order in an abelian group and $l$ be a prime number. If

$$l^k \| \text{ord } P \quad \text{and} \quad l^k \nmid \text{ord } Q,$$

then

$$l^k \| \text{ord}(P + Q).$$

This fact, together with subtle applications of Theorem 2.1, are constantly used in the remainder of the paper.

**Proof of Theorem 1.1** $(\Rightarrow)$ We can rewrite the assumption (1) as

$$\phi^{n_v} P = \psi^{m_v} Q \mod v,$$

where $n_v, m_v$ are nonnegative integers.

First we suppose that $P, Q$ are points of infinite order and $\phi, \psi \neq 0$.

Let $l$ be a prime number coprime to both $\phi$ and $\psi$. Suppose that $P, Q$ are linearly independent. By Theorem 2.1 there is a set of primes $v$ in $F$ of positive density such that $l | \text{ord}_v P$ and $l \nmid \text{ord}_v Q$. This contradicts (12). So $P, Q$ are linearly dependent, i.e., there are nonzero rational integers $a, b$ such that

$$a P = b Q.$$

Together with (12) this gives

$$(b \phi^{n_v} - a \psi^{m_v}) P = 0 \mod v.$$

Let $k$ be an arbitrary natural number. By Corollary 2.2 there is a positive density set of primes $v$ such that $k | \text{ord}_v P$. For those primes we have $k | (b \phi^{n_v} - a \psi^{m_v})$ by (14). Thus the exponential equation

$$b \phi^n - a \psi^m = 0$$

modulo every natural number has a solution in nonnegative integers $n, m$. We have to consider two cases.
First we analyse the case when \( \text{supp}(\phi) \neq \text{supp}(\psi) \). By Lemma 3.1 there is a solution to (15) in nonnegative integers \( n, m \). Hence by (13) the point (16)

\[
T = \phi^n P - \psi^m Q
\]
is torsion. Suppose \( T \) is not zero, i.e., there is a prime number \( l | \text{ord} \ P \). Assume that \( l \) does not divide one of \( \phi, \psi \), say \( \psi \). By Theorem 2.1 there is a set of primes \( v \) of positive density such that \( l \nmid \text{ord}_v P \). Hence \( l | \text{ord}_v Q \) by (16). This contradicts (12). Thus all prime divisors of \( \text{ord} \ T \) divide both \( \phi \) and \( \psi \). In particular, if either \( \phi \) or \( \psi \) equals \( \pm 1 \), we get \( l | \pm 1 \), a contradiction.

So suppose this is not the case. Since \( \phi \) and \( \psi \) have different sets of prime divisors, there is a prime number \( p \) dividing, say, \( \psi \) and dividing neither \( \phi \) nor \( \text{ord} \ T \). Let \( l^e \) be the maximal power of \( l \) dividing \( \text{ord} \ T \). By Corollary 2.2 there is a set of primes \( v \) of positive density such that

\[
l^{e+1} \| \text{ord}_v \psi^m Q \quad \text{and} \quad p \| \text{ord}_v \psi^m Q.
\]

By (16) this implies

\[
l^{e+1} \| \text{ord}_v \phi^n P \quad \text{and} \quad p \| \text{ord}_v \phi^n P.
\]

Consider (12). By (18) we have

\[p \| \text{ord}_v \phi^n P\]

for any \( n \). By (17) we have

\[p \nmid \text{ord}_v \psi^m Q \quad \text{if} \quad m_v > m,
\]

\[p^2 \| \text{ord}_v \psi^m Q \quad \text{if} \quad m_v < m.
\]

Thus \( m_v = m \). Hence by (16) we get

\[
T = (\phi^n - \phi^{n_v})P \mod v.
\]

If \( n_v \neq n \) then by (18) we have

\[l^{e+1} \| \text{ord}_v (\phi^n - \phi^{n_v})P,
\]

but this contradicts (19) because \( l^e \| \text{ord} \ T \). Thus \( n_v = n \), so \( T = 0 \mod v \). Hence \( T \) is zero by Proposition 3.2.

Now we analyse the case when \( \text{supp}(\phi) = \text{supp}(\psi) \). By Lemma 3.1 there are nonnegative integers \( n, m \) such that one of the following holds:

\[
\begin{align*}
b\phi^n - a\psi^m &= 0; \quad &b\phi^{-n} - a\psi^m &= 0 \quad \text{or} \quad b\phi^n - a\psi^{-m} &= 0; \quad &b\phi^{-n} - a\psi^{-m} &= 0.
\end{align*}
\]

Together with (13) this gives the existence of a torsion point \( T \) satisfying one of the equations in (2). Suppose there is a prime number \( l | \text{ord} \ T \) and not dividing \( \phi \) and \( \psi \). By Theorem 2.1 there is a set of primes \( v \) of positive density such that \( l \nmid \text{ord}_v P \). Hence \( l | \text{ord}_v Q \) by (2). This contradicts (12).

Thus every prime divisor of \( \text{ord} \ T \) divides \( \phi \) and \( \psi \).
It remains to analyse the trivial cases, i.e., when the assumption that $P, Q$ are points of infinite order and $\phi, \psi \neq 0$ does not hold.

Suppose first that both orbits $O_\phi(P), O_\psi(Q)$ consist of torsion points only, i.e., $P$ is torsion or $\phi = 0$, and $Q$ is torsion or $\psi = 0$. The assertion is an immediate consequence of Proposition 3.2.

Now suppose that one orbit, say $O_\phi(P)$, consists of nontorsion points, and the other of torsion points, i.e., $P$ is nontorsion, and $\phi \neq 0$ and $Q$ is torsion or $\psi = 0$. Let $l$ be a prime number coprime to both $\phi$ and $\ord Q$.

By Theorem 2.1 there is a set of primes $v$ in $F$ of positive density such that $l | \ord v$. This contradicts (12).

$(\Leftarrow)$ The proof is not straightforward only in the singular case, i.e., when $\supp(\phi) = \supp(\psi)$. Let $k$ be large enough so that $\phi^k$ kills $T$. For any $v$ factorize the order of $Q$ mod $v$ as $o_1o_2$, where all prime numbers dividing $o_1$ divide $\phi$ and $o_2$ is coprime to $\phi$. Choose a natural number $d > n, m$ such that $o_1$ divides both $\phi^{k+d}$ and $\psi^{k+d}$ and such that the order of $\phi/\psi$ in the group $(\mathbb{Z}/o_2\mathbb{Z})^\times$ divides $k + d$. We have

(20) $$(\phi^{k+d} - \psi^{k+d})Q = 0 \mod v.$$

Now we consider each instance of (2) separately.

Let $$\phi^k(\phi^n P - \psi^m Q) = 0.$$ Multiplying this by $\phi^d$ and (20) by $\psi^m$ and summing the results we get

$$\phi^{n+k+d} P - \psi^{m+k+d} Q = 0 \mod v.$$

Let $$\phi^k (P - \phi^n \psi^m Q) = 0.$$ Multiplying this by $\phi^{d-n}$ and (20) by $\psi^m$ and summing the results we get

$$\phi^{d-n+k} P - \psi^{m+k+d} Q = 0 \mod v.$$

Let $$\phi^k (\psi^m P - \phi^n Q) = 0.$$ Multiplying this by $\phi^{d-n}$ and summing the result with (20) we get

(21) $$(\phi^{m+n} - \psi^{m+n} P = 0 \mod v.$$

Factorize the order of $P$ mod $v$ as $s_1s_2$, where all prime numbers dividing $s_1$ divide $\phi$ and $s_2$ is coprime to $\phi$. Choose a natural number $d$ such that $s_1$ divides both $\phi^{m+e}$ and $\psi^{m+e}$, and the order of $\phi/\psi$ in $(\mathbb{Z}/s_2\mathbb{Z})^\times$ divides $m + e$. Then

(22) $$(\phi^{m+e} - \psi^{m+e})P = 0 \mod v.$$

Now multiplying (21) by $\psi^e$ and (22) by $\phi^{k+d-n}$ and summing the results we get

$$\phi^{k+d-n+m+e} P - \psi^{k+d+e} Q = 0 \mod v.$$
4. Proofs of Theorem 1.2 and Corollary 1.3

Proof of Theorem 1.2. From among the points $Q_1, \ldots, Q_s$ choose a maximal independent subset, say for simplicity $Q_1, \ldots, Q_t$. So

$$
c_{t+1}Q_{t+1} = c_{t+1,1}Q_1 + \ldots + c_{t+1,t}Q_t,
$$

$$
\vdots
$$

$$
c_sQ_s = c_{s,1}Q_1 + \ldots + c_{s,t}Q_t,
$$

where all the $c$’s are integers with $c_{t+1}, \ldots, c_s$ being nonzero. Fix a prime number $l$ coprime to all nonzero $c$’s.

Let $P$ be any point from among $P_1, \ldots, P_r$. Suppose that the points $P, Q_1, \ldots, Q_t$ are linearly independent. By Theorem 2.1 there exist infinitely many primes $v$ such that

$$
l \parallel \text{ord}_v P \quad \text{and} \quad i^{i+1} \parallel \text{ord}_v Q_i \quad \text{for} \quad i = 1, \ldots, t.
$$

Choose one such $v$. By (23) we have

$$
l^2 \parallel \text{ord}_v Q_j \quad \text{for} \quad j = t+1, \ldots, s.
$$

This contradicts (4) for $n = \text{ord}_v P$. Thus $P, Q_1, \ldots, Q_t$ are linearly dependent.

Choose from among $Q_1, \ldots, Q_t$ a subset consisting of $t-1$ points, say $Q_1, \ldots, Q_{t-1}$, such that the points $P, Q_1, \ldots, Q_{t-1}$ are linearly independent. We have

$$
d_tQ_t = d_{t,0}P + d_{t,1}Q_1 + \ldots + d_{t,t-1}Q_{t-1},
$$

$$
\vdots
$$

$$
d_sQ_s = d_{s,0}P + d_{s,1}Q_1 + \ldots + d_{s,t-1}Q_{t-1},
$$

where all the $d$’s are integers with $d_t, \ldots, d_s$ being nonzero. Fix a prime number $l$ coprime to all nonzero $d$’s. By Theorem 2.1 there exist infinitely many primes $v$ such that

$$
l \parallel \text{ord}_v P \quad \text{and} \quad i^{i+1} \parallel \text{ord}_v Q_i \quad \text{for} \quad i = 1, \ldots, t-1.
$$

Choose one such $v$. Suppose that for no $i \in \{t, \ldots, s\}$ do we have $d_{i,1} = \cdots = d_{i,t-1} = 0$. By (24) this means that

$$
l^2 \parallel \text{ord}_v Q_i \quad \text{for} \quad i = t, \ldots, s.
$$

This contradicts (4) for $n = \text{ord}_v P$. Hence there is an index $i \in \{t, \ldots, s\}$ such that $d_{i,1} = \cdots = d_{i,t-1} = 0$. Assume without loss of generality that all such indices are $\{i : u \leq i \leq s\}$ for some $u$ such that $t \leq u \leq s$, i.e.,
Reduction maps of Mordell–Weil type groups

\[ d_u Q_u = d_{u,0} P, \]
\[ \vdots \]
\[ d_s Q_s = d_{s,0} P. \]

So rewrite (24) as

\[ (25) \]
\[ d_t Q_t = d_{t,0} P + d_{t,1} Q_1 + \cdots + d_{t,t-1} Q_{t-1}, \]
\[ \vdots \]
\[ d_{u-1} Q_{u-1} = d_{u-1,0} P + d_{u-1,1} Q_1 + \cdots + d_{u-1,t-1} Q_{t-1}, \]
\[ d'_u Q_u = d'_{u,0} P + T_u, \]
\[ \vdots \]
\[ d'_s Q_s = d'_{s,0} P + T_s, \]

where \( d'_u, \ldots, d'_s \) and \( d'_{u,0}, \ldots, d'_{s,0} \) are nonzero integers such that \( \gcd(d'_u, d'_{u,0}) = \cdots = \gcd(d'_s, d'_{s,0}) = 1 \) and \( T_u, \ldots, T_s \in A(F)_{\text{tors}} \). Suppose that none of the coefficients \( d'_u, \ldots, d'_s \) equals \( \pm 1 \), i.e., each has a prime divisor. Let \( L \) be the set of all prime divisors of \( d'_u, \ldots, d'_s \). For every \( l \in L \) let \( e_l \) be a natural number large enough so that \( l^{e_l} \) divides neither any of the nonzero coefficients in (25) nor the order of any of \( T_u, \ldots, T_s \). By Theorem 2.1 there exist infinitely many primes \( v \) such that for every \( l \in L \),

\[ l^{e_l} \mid \text{ord}_v P \quad \text{and} \quad l^{e_l(i+1)} \mid \text{ord}_v Q_i \quad \text{for } i = 1, \ldots, t-1. \]

Choose one such \( v \). By (25) we find that for \( i = t, \ldots, u-1 \) and for every \( l \in L \),

\[ l^{e_l+1} \mid \text{ord}_v Q_i, \]

and for every \( i = u, \ldots, s \) there exists \( l \in L \) such that

\[ l^{e_l+1} \mid \text{ord}_v Q_i. \]

This contradicts (4) for \( n = \text{ord}_v P \). Thus, say, \( d'_s = \pm 1 \).

Now we consider the particular cases.

(C1) We immediately get \( Q_s = \pm d'_{s,0} P \).

(C2) Since the points \( Q_1, \ldots, Q_s \) are pairwise linearly independent, we have \( u = s \). It remains to show that \( T_s \) is trivial. Suppose that there is a prime number \( l \) dividing the order of \( T_s \). Let \( e \) be a natural number large enough so that \( l^e \) does not divide any of the nonzero coefficients in (25). By Theorem 2.1 there exist infinitely many primes \( v \) such that

\[ l \nmid \text{ord}_v P \quad \text{and} \quad l^{e_i} \mid \text{ord}_v Q_i \quad \text{for } i = 1, \ldots, t-1. \]

Choose one such \( v \) that is not exceptional regarding Proposition 3.2. By (25) we have

\[ l \mid \text{ord}_v Q_i \quad \text{for } i = 1, \ldots, s \]
(in particular, \( l \mid \text{ord}_v Q_s \) by Proposition 3.2). This contradicts (4) for \( n = \text{ord}_v P \).

**Proof of Corollary 1.3.** Denote \( P = \{P_1, \ldots, P_r\} \) and \( Q = \{Q_1, \ldots, Q_s\} \).

Suppose that (5) holds for each \( n \in \mathbb{N} \). Let \( P \in P \) be a maximal multiple in \( P \). By Theorem 1.2 there are \( Q \in Q \) and \( a \in \mathbb{Z} \) such that

\[ aP = Q \]

and further there are \( P' \in P \) and \( b \in \mathbb{Z} \) such that

\[ bQ = P' \]

We get

\[ abP = P' \]

so \( |a| = |b| = 1 \) since \( P \) is a maximal multiple in \( P \). Thus \( Q = \pm P \).

Suppose \( Q \) is not a maximal multiple in \( Q \). Let \( mQ \in Q \) with \( m \in \mathbb{Z} \), \( |m| > 1 \), be a maximal multiple in \( Q \). As above we get \( \pm mQ \in P \), so \( \pm mP \in P \); but \( P \) is a maximal multiple in \( P \), a contradiction.

Now suppose that \( M(\{P_1, \ldots, P_r\}) = M(\{Q_1, \ldots, Q_s\}) \).

For every \( P \in A(F) \) and every \( n \in \mathbb{Z} \) we have \( \text{supp}(\{P\}) \subset \text{supp}(\{nP\}) \). Thus \( \text{supp}(X) = \text{supp}(M(X)) \) for every \( X \subset A(F) \).

For every \( n \in \mathbb{Z} \) we have \( M(\{nP_1, \ldots, nP_r\}) = M(\{nQ_1, \ldots, nQ_s\}) \) provided \( M(\{P_1, \ldots, P_r\}) = M(\{Q_1, \ldots, Q_s\}) \).

**Remark 3.** Theorem 1.2 and Corollary 1.3 are generalizations and strengthenings of Skałba’s [Ska] Theorems 1 and 3 resp.

**Appendix.** Analogues for multiplicative groups and higher K-theory groups.** As mentioned in the Introduction, our results stated in terms of abelian varieties have analogues for K-theory groups and multiplicative groups of number fields (more precisely, for \( S \)-unit subgroups).

In the K-theory case, simply replace \( A(F) \) by \( K_{2n+1}(F) \), and \( \text{End}_F(A) \) or \( \text{End}_F(A) \) by \( \mathbb{Z} \). For example, let us formulate the analogues of Theorem 2.1 and Corollary 2.2.

**Theorem A.1.** Let \( F \) be a number field. Fix \( n \geq 1 \). Let \( P_1, \ldots, P_s \in K_{2n+1}(F) \) be linearly independent over \( \mathbb{Z} \). Then for any finite set \( \{l_1, \ldots, l_d\} \) of prime numbers and a matrix \( [k_{ij}]_{1 \leq i \leq s, 1 \leq j \leq d} \) of nonnegative integers there is a set of primes \( v \) of positive density such that for all \( 1 \leq i \leq s \) and \( 1 \leq j \leq d \) the order of the image of the point \( P_i \) under the map

\[ K_{2n+1}(F) \to K_{2n+1}(\kappa_v)l_j \]

is equal to \( l_j^{k_{ij}} \).

**Corollary A.2.** If \( P \in K_{2n+1}(F) \) is nontorsion then for every pair \( (m_1, m_2) \) of coprime natural numbers there exists a positive density set \( S \)
of primes such that for every \( v \in S \), \( m_1 \) divides \( \text{ord}_v P \) and is coprime to \((\text{ord}_v P)/m_1\), and \( m_2 \) does not divide \( \text{ord}_v P \).

For the convenience of readers working in algebraic number theory, we restate all our results for multiplicative groups of number fields. Fix the following notation:

- \( F \) a number field
- \( \mathcal{O}_F \) the ring of integers of \( F \)
- \( \mu \) the group of roots of unity in \( F \)
- \( \text{ord}_\xi \) the order of a number \( \xi \in \mu \)
- \( \text{ord}_v x \) the multiplicative order of a number \( x \) mod \( v \) for a prime ideal \( v \) in \( \mathcal{O}_F \)
- \( l^k \parallel n \) means that \( l^k \) exactly divides \( n \), i.e. \( l^k \mid n \) and \( l^{k+1} \nmid n \) where \( l \) is a prime number, \( k \) a nonnegative integer and \( n \) a natural number
- \( \text{supp}(n) \) the set of prime numbers dividing \( n \in \mathbb{Z} \)
- \( \text{supp}(\alpha) \) the set of prime ideals \( v \) in \( \mathcal{O}_F \) such that \( \alpha \equiv 0 \mod v \), where \( \alpha \in F^\times \)

**Theorem A.3.** Let \( x_1, \ldots, x_s \) be multiplicatively independent numbers in \( F^\times \). For any set \( \{l_1, \ldots, l_d\} \) of prime numbers and a matrix \( [k_{ij}]_{1 \leq i \leq s, 1 \leq j \leq d} \) of nonnegative integers there is a set of prime ideals \( v \) in \( \mathcal{O}_F \) of positive density such that for all \( 1 \leq i \leq s \) and \( 1 \leq j \leq d \),

\[
\begin{align*}
l_j^{k_{ij}} & \mid \text{ord}_v x_i & \text{if} & \ k_{ij} > 0, \\
l_j & \nmid \text{ord}_v x_i & \text{if} & \ k_{ij} = 0.
\end{align*}
\]

**Corollary A.4.** For every number \( x \in F^\times \setminus \mu \) and for every pair \((n,m)\) of coprime natural numbers there exists a set of prime ideals \( v \) in \( \mathcal{O}_F \) of positive density such that \( n \) divides \( \text{ord}_v x \) and \( nm \) is coprime to \( (\text{ord}_v x)/n \).

Compare this with the following generalization of Zsigmondy’s Theorem due to Schinzel.

**Theorem ([Sch1, Theorem 1]).** If \( F \) is a number field and \( x \in F \) is not a root of unity then there exists a natural number \( N \), depending only on the degree of \( x \), such that for every \( n > N \) there is a prime \( v \) of \( F \) satisfying \( \text{ord}_v x = n \).

For any endomorphism \( \phi : F^\times \to F^\times \) write \( \phi^n \) for the \( n \)th iterate of \( \phi \), and \( \mathcal{O}_\phi(x) = \{ \phi^n(x) : n \geq 0 \} \) for the forward orbit of \( x \in F^\times \). For all but finitely many prime ideals \( v \) in \( \mathcal{O}_F \) we have the orbit \( \mathcal{O}_\phi(P \mod v) \).

**Theorem A.5.** Let \( x, y \in F^\times \) and let \( \phi : \alpha \mapsto \alpha^k \) and \( \psi : \alpha \mapsto \alpha^l \) be exponentiation maps with natural exponents. The following are equivalent:

- For all but a density zero set of prime ideals \( v \) in \( \mathcal{O}_F \),
  \[
  \mathcal{O}_\phi(x \mod v) \cap \mathcal{O}_\psi(y \mod v) \neq \emptyset.
  \]
Either
\[ \mathcal{O}_\phi(x) \cap \mathcal{O}_\psi(y) \neq \emptyset, \]
or we have the singular case: \( \text{supp}(k) = \text{supp}(l) \) and there is a \( t \in \mu \setminus \{1\} \) with \( \text{supp}(\text{ord } t) \subseteq \text{supp}(k) \) such that
\[ t = \phi^n \psi^m x/\phi^{n'} \psi^{m'} y \]
for some nonnegative integers \( n, m, n', m' \) with four possible cases: \( m = n' = 0 \) or \( n = m = 0 \) or \( n' = m' = 0 \) or \( n = m' = 0 \).

**Theorem A.6.** Let \( a_1, \ldots, a_r, b_1, \ldots, b_s \in F^\times \setminus \mu \). Assume that for each positive integer \( n \),
\[ \text{supp} \left( \prod_{i=1}^{r} (1 - a_i^n) \right) \subseteq \text{supp} \left( \prod_{j=1}^{l} (1 - b_j^n) \right). \]
Then for every \( i = 1, \ldots, r \) there exists \( j \in \{1, \ldots, s\} \) such that
\[ a_{f_j}^{g_i} = b_j^{g_i} \]
for some nonzero integers \( f_j, g_i \). In particular, suppose that any of the following conditions holds:

(C1) The torsion part of the subgroup of \( F^\times \) generated by \( a_1, \ldots, a_r, b_1, \ldots, b_s \) is trivial.

(C2) The numbers \( b_1, \ldots, b_s \) are pairwise multiplicatively independent.

Then we can take \( f_j = 1 \) for every \( i = 1, \ldots, r \).

Let \( X \) be a finite subset of \( F^\times \). Call \( x \in X \) a maximal power in \( X \) if \( x^m \notin X \) for every \( m \in \mathbb{Z} \) such that \( |m| > 1 \). Denote
\[ M(X) = \{x^{\pm 1} : x \text{ is a maximal power in } X\}. \]

**Corollary A.7.** Let \( a_1, \ldots, a_r, b_1, \ldots, b_s \in F^\times \setminus \mu \) be such that the torsion part of the subgroup of \( F^\times \) they generate is trivial. The following are equivalent:

- For each \( n \in \mathbb{N} \),
\[ \text{supp} \left( \prod_{i=1}^{r} (1 - a_i^n) \right) = \text{supp} \left( \prod_{j=1}^{l} (1 - b_j^n) \right). \]

- \( M(\{a_1, \ldots, a_r\}) = M(\{b_1, \ldots, b_s\}) \).

**Corollary A.8.** Let \( a_1, \ldots, a_r \) and \( b_1, \ldots, b_s \) be two sequences of positive integers greater than 1. The following are equivalent:

- For each \( n \in \mathbb{N} \),
\[ \text{supp} \left( \prod_{i=1}^{r} (1 - a_i^n) \right) = \text{supp} \left( \prod_{j=1}^{l} (1 - b_j^n) \right). \]
• The set of maximal powers in \( \{a_1, \ldots, a_r\} \) equals the set of maximal powers in \( \{b_1, \ldots, b_s\} \).

**Proof.** The assumption that the numbers \( a_1, \ldots, a_r \) and \( b_1, \ldots, b_s \) are positive integers has two consequences.

First, the torsion part of the subgroup of \( \mathbb{Q}^\times \) generated by \( a_1, \ldots, a_r \), \( b_1, \ldots, b_s \) is trivial. Hence the assumption of Corollary [A.7] is fulfilled.

Second, the set of maximal powers in \( \{a_1, \ldots, a_r\} \) equals the set of maximal powers in \( \{b_1, \ldots, b_s\} \) if and only if \( M(\{a_1, \ldots, a_r\}) = M(\{b_1, \ldots, b_s\}) \).

Indeed, in general, if \( I_1, I_2 \) are two sets of positive integers, then \( I_1 = I_2 \) if and only if

\[ \{x^{\pm 1} : x \in I_1\} = \{x^{\pm 1} : x \in I_2\}. \]

**Acknowledgements.** We thank the referee for a thorough reading of the manuscript and providing an exhaustive list of corrections and suggestions.

**References**

D. Blinkiewicz, Local to global principle for semiabelian varieties isogenous to the product of an abelian variety and a torus, Acta Arith. 200 (2021), 221–258.


A. Perucca, Prescribing valuations of the order of a point in the reductions of abelian varieties and tori, J. Number Theory 129 (2009), 469–476.


