

Reconstruction from Milnor K -theory modulo the characteristic

OpenAI

October 5, 2026

Abstract

Let K and L be finitely generated extensions of transcendence degree at least two over algebraically closed fields of characteristic p . We prove that every isomorphism of their first Milnor K -groups modulo p preserving the degree-two Steinberg relations is a nonzero scalar multiple of the map induced by a unique field isomorphism. The proof recovers projective lines over the subfields of p th powers by an elementary calculation with derivations.

1 Introduction

Milnor K -theory records multiplication in a field together with relations arising from addition. A reconstruction problem asks whether this information determines the field, and whether isomorphisms of the invariant come from field isomorphisms. We study this question in characteristic p using only the first two Milnor K -groups modulo p .

Fix a prime p and write $\Lambda = \mathbf{F}_p$. For a field F of characteristic p , set

$$V_F = F^\times / (F^\times)^p = K_1^M(F)/p.$$

We write $[f]$ for the class of $f \in F^\times$ and use additive notation in V_F : thus $[f] + [g] = [fg]$, $r[f] = [f^r]$ for $r \in \mathbf{Z}$, and $[1] = 0$. Define the Steinberg relation subspace

$$R_F = \text{Span}_\Lambda\{[f] \otimes [1 - f] : f \in F \setminus \{0, 1\}\} \subset V_F \otimes_\Lambda V_F.$$

The quotient $W_F = (V_F \otimes_\Lambda V_F)/R_F$ is $K_2^M(F)/p$ by the tensor presentation of Milnor K -theory [6, Section 1]. We denote the image of $[f] \otimes [g]$ in W_F by $\{f, g\}_F$.

Remark (notation). F denotes the characteristic- p field to which the local field-theoretic definitions or arguments are applied. In Lemma 2.1, Lemma 2.3, Lemma 2.4, Lemma 5.2: F/κ is finitely generated over an algebraically closed field κ of characteristic p ; no positive lower bound on $\text{trdeg}(F/\kappa)$ is imposed. In Lemma 2.2: F is any field of characteristic p ; finiteness of $[F : F^p]$ is assumed only for the assertions explicitly conditional on finite degree. In Proposition 3.1: $[F : F^p] < \infty$. In Lemma 4.1: $F \neq F^p$; finite power degree and an algebraically closed base are not assumed. $V_F = F^\times / (F^\times)^p$ has additive operations $[f] + [g] = [fg]$ and $r[f] = [f^r]$, with zero $[1]$, while its underlying set is $\mathbf{P}_{F^p}(F)$ via $[f] \mapsto F^p f$, whose projective lines come from two-dimensional F^p -subspaces of F . g is a local nonzero field element; in the class and Milnor-symbol notation it ranges independently over $F^\times$. In Lemma 5.2: For a given integer $m \geq 1$, $g \in F$ is a hypothetical element satisfying $f = g^{p^m}$; it is nonzero because $f \notin \kappa$, and its choice may depend on m . For $f \in F^\times$, $[f]$ is its class modulo $(F^\times)^p$ and, under the identification of the underlying set of V_F with $\mathbf{P}_{F^p}(F)$, represents the one-dimensional F^p -subspace $F^p f$; $[1]$ is the zero of the additive group V_F . f is a local

nonzero element of the field whose multiplicative class is being used. In Lemma 2.3: In the logarithmic-derivative pairing, f ranges over $F^\times$; when checking a Steinberg pair $([f], [1-f])$, it ranges over $F \setminus \{0, 1\}$. In Theorem 1.1: In the induced-map formula and the comparison of semilinear maps $w \mapsto S(fw)$ and $w \mapsto S(f)S(w)$, $f \in K^\times$. In Lemma 5.2: In the proof, $f \in F \setminus \kappa$ is chosen, hence is nonzero and transcendental over κ , and is completed to a transcendence basis. The letter r is local notation; in the convention $r[f] = [f^r]$ it is an integer, whose action on V_F depends only on its residue in $\mathbf{F}_p$. In Lemma 2.2: In the definition of a p -independent list $s_1, \dots, s_r$, r is the finite length of the list and $[C(s_1, \dots, s_r) : C] = p^r$. In Proposition 3.1: In the uniqueness argument, r is a candidate integer exponent with $1 \leq r < p$, satisfying $U^r = h + jX^r$ with $h, j \in C$; the analogous argument applies to V . In Lemma 4.1: $r \in \mathbf{F}_p^\times$ is the scalar multiplying V_F ; its powers in the proof use its unique integer representative $1 \leq r < p$. In Proposition 4.2: In the inverse-map argument, $r \in \mathbf{F}_p^\times$ is chosen so that $r\Psi^{-1}$ maps projective lines into projective lines. In Theorem 1.1: In the injectivity argument, $r \in \mathbf{F}_p^\times$ is the scalar in $\beta_* = r\alpha_*$. $V \in C(Y)^\times$ satisfies $[V] \notin \mathbf{F}_p[Y]$, equivalently $V \notin C^\times Y^i$ for every integer $0 \leq i < p$. In Proposition 4.2: With $H = K^p$ and $C = L^p$, V is a representative in $L^\times$ of $\Theta([y+b])$, where $b \in H^\times$ and $[x], [y]$ is the chosen edge. It is determined only up to multiplication by $C^\times$.

Let $\text{Isom}_M(V_K, V_L)$ be the set of Λ -linear isomorphisms $\Theta : V_K \rightarrow V_L$ satisfying

$$(\Theta \otimes \Theta)(R_K) = R_L.$$

We call these isomorphisms *compatible*. Equivalently, Θ extends to an isomorphism of the degree-one and degree-two groups respecting their product pairing. Scalar multiplication by $\Lambda^\times$ acts on this set. For specified subfields $k \subset K$ and $l \subset L$, write $\text{Isom}(K, k; L, l)$ for the field isomorphisms $\alpha : K \rightarrow L$ with $\alpha(k) = l$. Such an isomorphism induces $\alpha_*([f]) = [\alpha(f)]$ and carries R_K onto R_L .

Remark (notation). k denotes the specified source subfield $k \subset K$ in the base-field notation and a basis index in the notation s_k . In Theorem 1.1, Proposition 4.2: k is algebraically closed of characteristic p , and K/k is finitely generated with $\text{trdeg}(K/k) \geq 2$. In Lemma 2.2: k in s_k is an integer basis index with $1 \leq k \leq e$; the intersection assertion is for $j \neq k$. $l \subset L$ is the specified target subfield in $\text{Isom}(K, k; L, l)$. In Theorem 1.1, Proposition 4.2: l is algebraically closed of characteristic p , and L/l is finitely generated with $\text{trdeg}(L/l) \geq 2$. $V_K = K^\times / (K^\times)^p$ has its additive Λ -vector-space structure $[f] + [g] = [fg]$, and its underlying set is $\mathbf{P}_{K^p}(K)$ via $[f] \mapsto K^p f$, so its projective lines are the point sets of two-dimensional K^p -subspaces of K . $V_L = L^\times / (L^\times)^p$ has its additive Λ -vector-space structure $[f] + [g] = [fg]$, and its underlying set is $\mathbf{P}_{L^p}(L)$ via $[f] \mapsto L^p f$, so its projective lines are the point sets of two-dimensional L^p -subspaces of L . $\alpha : K \rightarrow L$ is a field isomorphism. In Theorem 1.1: As an argument of the canonical map, $\alpha \in \text{Isom}(K, k; L, l)$, so $\alpha(k) = l$.

Theorem 1.1. *Let K/k and L/l be finitely generated extensions of algebraically closed fields of characteristic p , with*

$$\text{trdeg}(K/k) \geq 2, \quad \text{trdeg}(L/l) \geq 2.$$

The canonical map

$$\text{Isom}(K, k; L, l) \longrightarrow \text{Isom}_M(V_K, V_L) / \Lambda^\times, \quad \alpha \longmapsto [\alpha_*],$$

is bijective.

The invariant therefore determines the field and its isomorphisms, with exactly the scalar identification in the displayed target. The argument also recovers the named algebraically closed base from the field itself.

1.1 Context and method

Bogomolov and Tschinkel developed a reconstruction method that recovers projective lines from multiplication and algebraic dependence, and applied it to Milnor K -theory in characteristic zero [2]. Cadoret and Pirutka extended reconstruction from the multiplicative group modulo constants and algebraic dependence to finitely generated regular extensions of perfect fields [4, Theorem 4]. For algebraically closed or finite base fields, they also obtained reconstruction from suitable quotients of the Milnor K -ring [4, Corollary 10].

Reconstruction from other reduced forms of K -theory has also been studied. For a prime ℓ different from the characteristic, Topaz recovers perfect closures from mod- ℓ data together with rational subgroups for function fields over algebraically closed bases in transcendence degree at least five [7, Theorem B]. His work on rational Milnor K -theory reconstructs perfect closures for fields of absolute transcendence degree at least five [8, Main Theorem]. Theorem 1.1 concerns reduction modulo the characteristic and starts directly from V_F and R_F ; neither rational subgroups nor algebraic-dependence data are supplied.

The geometric framework of our proof has close predecessors. A differential approach to line recovery appears in an argument of Rovinsky recorded by Bogomolov and Tschinkel [3, Proposition 9]. In positive characteristic, Cadoret and Pirutka recover projective lines over the subfield of p th powers after a common power correction, using a differential intersection calculation [4, Section 1.3, Lemma 23, and Proposition 27]. Here the intersection calculation involves only degree- p extensions of the subfield of p th powers. The resulting intersection statement, Proposition 3.1, and the passage from vanishing symbols to these subextensions are given complete elementary proofs below. These are the two structural ingredients that allow the degree-two mod- p relations to supply the required projective geometry.

1.2 Outline of the proof

Put $C_F = F^p$. Since $(F^\times)^p = C_F^\times$, the underlying set of V_F is the projective point set $\mathbf{P}_{C_F}(F)$. Its point [1] is the zero of the group V_F ; its projective lines are the sets of one-dimensional subspaces in two-dimensional C_F -subspaces of F . The field degree is finite:

$$[F : C_F] = p^{\text{trdeg}(F/\kappa)}$$

for F/κ as in the theorem. This is a projective geometry over C_F , not over the original constant field κ .

Remark (notation). C is the scalar field specified in the local field or vector-space setting. In Lemma 2.1, Lemma 2.2, Lemma 2.3, Lemma 2.4, Proposition 3.1, Lemma 4.1: $C = F^p$. In Theorem 1.1, Proposition 4.2: $C = L^p$, the power subfield of the target field L . In Proposition 5.1: C is an arbitrary field over which E' is a finite-dimensional vector space of dimension at least three; no power-subfield interpretation is imposed.

The first step constrains pairs with vanishing symbol. If $s \notin C_F$ and $\{s, t\}_F = 0$, then $t \in C_F(s)$. To prove this implication, consider a p -independent pair s, t , meaning that $[C_F(s, t) : C_F] = p^2$. Extend it to a monomial basis and take the determinant of two logarithmic derivatives. This pairing kills Steinberg relations and is nonzero on the independent pair. Section 2 supplies the details.

Remark (notation). s denotes a local field element, with its field and restrictions specified by the adjunction, pair, or projective point in which it occurs. In Lemma 2.2: $s \in F \setminus M$, where $C \subseteq M \subseteq F$, is the element in the simple adjunction $M(s)/M$. In Lemma 2.3: $s \in F^\times$, and the implication has antecedent $s \notin C$. In the contrapositive proof, $t \notin C(s)$, so s, t is a p -independent pair used to choose D_s, D_t . In Proposition 4.2: $s \in K^\times$ represents a source projective point; multiplication by s^{-1} takes the line joining $[s], [t]$ to a line through [1]. t denotes an element of the field specified by its local pair, affine expression, or coordinate

chart. In Lemma 2.3: $t \in F^\times$. In the contrapositive proof, $s \notin C$ and $t \notin C(s)$, so the pair s, t is p -independent and is extended to the basis defining D_s, D_t . In Lemma 2.4: $t \in F^\times$ and $c + dt \neq 0$, where $c, d \in C^\times$; no p -independence premise is imposed. In Proposition 4.2: In the line joining $[s], [t]$, $t \in K^\times$ is a representative of a source projective point, and multiplication by s^{-1} translates this line to one through $[1]$. In Proposition 5.1: $t \in H$ is an arbitrary affine coordinate in the lines $(t, t + a)$ and (t, at) ; it may be zero.

The fields $C_F(s)$ need not themselves be two-dimensional over C_F , so this implication does not yet recover projective lines. The key calculation in Section 3 uses intersections of two multiplicative translates of such subfields. For a p -independent pair X, Y , suppose $U \in C_F(X)^\times$ and $V \in C_F(Y)^\times$ are not scalar multiples of powers of X, Y , respectively. A nonzero element of

$$X C_F(Y/X) \cap U C_F(V/U)$$

forces, for a unique $1 \leq n < p$,

$$U^n \in C_F + C_F X^n, \quad V^n \in C_F + C_F Y^n.$$

Euler derivations give this common exponent and show that either inclusion determines it. *Remark (notation).* X is a nonzero element of the locally specified ambient field, used through its projective class $[X]$. In Proposition 3.1: $X \in F^\times$ and $[C(X, Y) : C] = p^2$. In Proposition 4.2: $X \in L^\times$ represents $\Theta([x])$ for a nonzero vertex $[x] \in V_K$, with $C = L^p$. For an edge $[x], [y]$, $C(X) \neq C(Y)$ and X, Y are p -independent over C . The representative is determined only up to $C^\times$. Y is a nonzero element of the locally specified ambient field, used through its projective class $[Y]$. In Proposition 3.1: $Y \in F^\times$ and $[C(X, Y) : C] = p^2$. In Proposition 4.2: $Y \in L^\times$ represents $\Theta([y])$ for a nonzero vertex $[y] \in V_K$, with $C = L^p$. For an edge $[x], [y]$, $C(X) \neq C(Y)$ and X, Y are p -independent over C . The representative is determined only up to $C^\times$. $U \in C(X)^\times$ satisfies $[U] \notin \mathbf{F}_p[X]$, equivalently $U \notin C^\times X^i$ for every integer $0 \leq i < p$. In Proposition 4.2: With $H = K^p$ and $C = L^p$, U is a representative in $L^\times$ of $\Theta([x + a])$, where $a \in H^\times$ and $[x], [y]$ is the chosen edge. It is determined only up to multiplication by $C^\times$.

Section 4 produces the required intersections from Steinberg relations. Uniqueness propagates the exponent across a connected graph, giving one scalar n for which $n\Theta$ preserves every projective line. Applying the argument to the inverse, and using the fact that no nontrivial scalar preserves projective lines, yields preservation in both directions. Section 5 then proves the needed projective lifting theorem and uses the multiplicative group law to turn the normalized semilinear lift into a field isomorphism. Finally, the identity $\bigcap_{m \geq 1} F^{p^m} = \kappa$ recovers the original base and completes the theorem.

Remark (notation). n denotes a nonzero power correction modulo p , represented by its unique integer in $\{1, \dots, p-1\}$ when used as an exponent. In Proposition 3.1: n is the unique integer $1 \leq n < p$ such that $U^n \in C + CX^n$ and $V^n \in C + CY^n$; either inclusion determines it uniquely, and both coefficients in each inclusion are nonzero. In Proposition 4.2, Theorem 1.1: $n \in \mathbf{F}_p^\times$ is the unique scalar such that $\Psi = n\Theta$ sends every projective line over K^p onto a projective line over L^p . In the local power calculations its integer representative is used; the scalar is common to all vertices and all affine coefficients.

2 Symbols and projective points over p th powers

Let F/κ be a finitely generated extension of an algebraically closed field of characteristic p , and put

$$C = F^p, \quad d = \text{trdeg}(F/\kappa).$$

Since $(F^\times)^p = C^\times$, the underlying set of V_F is the point set of the projective space $\mathbf{P}_C(F)$: the class $[f]$ represents the one-dimensional C -subspace Cf . These projective points also carry the $\mathbf{F}_p$ -vector-space structure $[f] + [g] = [fg]$, whose zero is $[1]$. We will use both structures, keeping their two scalar fields distinct. Our first task is to extract from a vanishing symbol the field-theoretic constraint that will allow us to recover projective lines.

Remark (notation). The letter d is locally bound, denoting either $\text{trdeg}(F/\kappa)$ or a nonzero affine coefficient in the power subfield. In Lemma 2.1: $d = \text{trdeg}(F/\kappa) \in \mathbb{Z}_{\geq 0}$. In Lemma 2.4: $d \in C^\times$ is the affine coefficient in $c + dt$, where $C = F^p$. In Proposition 4.2: In the affine configuration in the proof, $d \in H^\times$ is the coefficient in $y = c + dx$, where $H = K^p$.

Lemma 2.1. *With the notation above, $[F : C] = p^d$.*

Proof. Choose a transcendence basis $t_1, \dots, t_d$ over κ , and write $F_0 = \kappa(t_1, \dots, t_d)$. Perfectness of κ gives $F_0^p = \kappa(t_1^p, \dots, t_d^p)$. The monomials $t_1^{i_1} \cdots t_d^{i_d}$ with $0 \leq i_j < p$ form a basis of F_0 over F_0^p : group polynomial exponents modulo p , and for rational functions use $a/b = ab^{p-1}/b^p$. Linear independence follows by clearing denominators and separating the exponent classes. Thus $[F_0 : F_0^p] = p^d$.

The extension F/F_0 is finite, and Frobenius induces an isomorphism of extensions $F/F_0 \simeq F^p/F_0^p$. Computing $[F : F_0^p]$ in the two towers through F_0 and F^p gives

$$[F : F_0]p^d = [F : F^p][F^p : F_0^p] = [F : F^p][F : F_0].$$

Cancellation proves the assertion without a separability assumption. $\square$

A list $s_1, \dots, s_r \in F$ is *p-independent over C* if $[C(s_1, \dots, s_r) : C] = p^r$. A *p-independent* list generating F over C is called a *p-basis*. Its monomials supply derivations that record one exponent at a time.

Lemma 2.2. *Let F be any field of characteristic p , and put $C = F^p$. If $C \subseteq M \subseteq F$ and $s \in F \setminus M$, then $[M(s) : M] = p$. If $[F : C]$ is finite, every p -independent list extends to a p -basis $s_1, \dots, s_e$ of F/C , with $[F : C] = p^e$ and monomial basis*

$$\{s_1^{i_1} \cdots s_e^{i_e} : 0 \leq i_j < p\}.$$

For such a basis there are commuting C -linear derivations $D_1, \dots, D_e$ on F satisfying

$$D_j(s_1^{i_1} \cdots s_e^{i_e}) = i_j s_1^{i_1} \cdots s_e^{i_e}.$$

On $C(s_j)$ the kernel of D_j is C , and its nonzero eigenvectors with eigenvalue in C are precisely the elements cs_j^i , where $c \in C^\times$ and $0 \leq i < p$; their eigenvalues are $i \in \mathbf{F}_p$. Moreover, $C(s_j) \cap C(s_k) = C$ when $j \neq k$.

Remark (notation). s_j denotes the j th entry of a finite list $s_1, \dots, s_r \in F$, with $1 \leq j \leq r$; the list is p -independent over C when $[C(s_1, \dots, s_r) : C] = p^r$, and is a p -basis when it is also generating over C . In Lemma 2.2: In the finite-degree clause, $s_1, \dots, s_e$ is an extending p -basis of F/C , $[F : C] = p^e$, and $1 \leq j \leq e$; the monomial exponents satisfy $0 \leq i_j < p$. For a chosen finite p -basis $s_1, \dots, s_e$ of F/C and $1 \leq j \leq e$, D_j is defined by $D_j(s_1^{i_1} \cdots s_e^{i_e}) = i_j s_1^{i_1} \cdots s_e^{i_e}$ for $0 \leq i_k < p$, interpreting i_j in $\mathbf{F}_p \subseteq C$, and extending C -linearly to F . c is a local scalar coefficient whose field and nonvanishing restrictions are specified by the expression in which it occurs. In Lemma 2.2: $c \in C^\times$ is the coefficient of a nonzero eigenvector cs_j^i , where $0 \leq i < p$. In Lemma 2.4: $c \in C^\times$ is the constant coefficient in $c + dt$, with $t, c + dt \in F^\times$. In Proposition 4.2: $c \in H$ is the constant coefficient in the hypothetical dependence $y = c + dx$, with $d \in H^\times$; the proof considers $c = 0$ and $c \neq 0$ separately. In Proposition 5.1: $c \in C^\times$ is the common value of the coefficients c_v in $T(v) = c_v S(v)$ for nonzero $v \in E$, so that $T = cS$.

Proof. Since $s^p \in C$, the minimal polynomial of s over M divides $T^p - s^p = (T - s)^p$. If its degree were $1 \leq e < p$, it would be $(T - s)^e$, and its coefficient $-es$ of T^{e-1} would force $s \in M$. Thus every strict adjunction has degree p . When $[F : C]$ is finite, successive adjunctions must terminate, so they extend any p -independent list to a generating list. If its length is e , the tower formula gives $[F : C] = p^e$, and the usual basis of each simple extension gives the asserted monomial basis.

Remark (notation). e is a nonnegative integer used as a finite p -basis length, except for its explicitly local use as a hypothetical minimal-polynomial degree. In Lemma 2.2: In the statement and the terminating-adjunction argument, e is the length of the extending p -basis and satisfies $[F : C] = p^e$. In the preceding minimal-polynomial contradiction only, e is the hypothetical degree $1 \leq e < p$, so the polynomial would be $(T - s)^e$; this local e is not the basis length.

Define the D_j on these monomials and extend C -linearly. When two monomials are multiplied, reducing an exponent by p only removes a factor in C and leaves its value in $\mathbf{F}_p$ unchanged. This proves the product rule. The operators commute because they are diagonal on the same basis. On $C(s_j)$ their eigenvector assertions follow from the distinct eigenvalues $0, 1, \dots, p-1$ on $1, s_j, \dots, s_j^{p-1}$. Finally, the expansions of an element in both $C(s_j)$ and $C(s_k)$ can have only their constant term in common. $\square$

For a p -independent pair s, t , write D_s, D_t for the corresponding derivations obtained from any extending p -basis. The following proof uses a coordinate form of the logarithmic differential symbol; the much stronger injectivity theorem for that symbol is the Bloch–Gabber–Kato theorem [1, Theorem (2.1)]. Here we check the needed implication directly.

Remark (notation). For a p -independent pair s, t , choose any extending p -basis; D_s is its C -linear Euler derivation with $D_s s = s$ and value zero on every other element of that chosen p -basis. For a p -independent pair s, t , choose any extending p -basis; D_t is its C -linear Euler derivation with $D_t t = t$ and value zero on every other element of that chosen p -basis.

Lemma 2.3. *For $s, t \in F^\times$, one has*

$$s \notin C, \quad \{s, t\}_F = 0 \quad \implies \quad t \in C(s).$$

Remark. D_s, D_t are the coordinate Euler derivations associated with s, t in one fixed, arbitrarily chosen p -basis of F/C extending the pair s, t .

Proof. Suppose instead that $s \notin C$ and $t \notin C(s)$. By Lemma 2.2, the pair s, t is p -independent. Consider

$$\beta([f], [g]) = \frac{D_s f}{f} \frac{D_t g}{g} - \frac{D_t f}{f} \frac{D_s g}{g}, \quad f, g \in F^\times.$$

Each logarithmic derivative is additive on products and vanishes on $C^\times$. Hence β is a well-defined $\mathbf{F}_p$ -bilinear map $V_F \times V_F \rightarrow F$. For $f \neq 0, 1$, the identities $D_s(1 - f) = -D_s f$ and $D_t(1 - f) = -D_t f$ give $\beta([f], [1 - f]) = 0$. Thus β descends through the Steinberg relations to an $\mathbf{F}_p$ -linear map $W_F \rightarrow F$. But $D_s s = s$, $D_t t = t$, and $D_s t = D_t s = 0$, so this map sends $\{s, t\}_F$ to 1. The symbol cannot vanish. $\square$

The symbols arising from an affine line do vanish, by the defining Steinberg relation itself.

Lemma 2.4. *If $c, d \in C^\times$ and $t, c + dt \in F^\times$, then*

$$\{t, c + dt\}_F = 0.$$

Remark. In Lemma 2.4, $d \in C^\times$ is a locally quantified affine coefficient independent of the previously defined integer $\text{trdeg}(F/\kappa)$.

Proof. Put $q = -dt/c$. The hypotheses give $q \neq 0, 1$, while $[q] = [t]$ and $[1 - q] = [c + dt]$, since the omitted factors lie in $C^\times$. Therefore the identity is the Steinberg relation $\{q, 1 - q\}_F = 0$. $\square$

3 An intersection that determines an exponent

For $X \in F \setminus C$, the projective line through $[1]$ and $[X]$ consists of the nonzero elements of $C + CX$, modulo $C^\times$. To recover such lines from degree- p subfields, we need to pass from membership in $C(X)$ to membership in $C + CX$, possibly after taking a power. The following intersection provides such a condition for two p -independent elements at once. Its uniqueness assertion will allow the exponent to be compared between different pairs.

The use of differential equations to control such intersections, including the power correction in positive characteristic, appears in Cadoret and Pirutka [4, Sections 3.4–3.5]. Here the degree- p subextensions allow a direct proof using commuting Euler derivations.

Proposition 3.1 (Intersection and exponent). *Let F be a field of characteristic p with $[F : F^p] < \infty$, and put $C = F^p$. Let $X, Y \in F^\times$ be p -independent. Suppose*

$$U \in C(X)^\times, \quad V \in C(Y)^\times, \quad [U] \notin \mathbf{F}_p[X], \quad [V] \notin \mathbf{F}_p[Y].$$

If

$$XC(Y/X)^\times \cap UC(V/U)^\times \neq \emptyset, \tag{3.1}$$

then there is a unique integer n , $1 \leq n < p$, such that

$$U^n \in C + CX^n, \quad V^n \in C + CY^n. \tag{3.2}$$

In fact, either inclusion in (3.2) determines n uniquely. In each inclusion, both coefficients are nonzero.

Remark. $\mathbf{F}_p[X] = \text{Span}_{\mathbf{F}_p}\{[X]\}$ and $\mathbf{F}_p[Y] = \text{Span}_{\mathbf{F}_p}\{[Y]\}$ as subspaces of V_F .

The shape of (3.1) reflects the inclusion $CX + CY \subseteq XC(Y/X)$, and its counterpart for U, V . Thus a common nonzero vector of the two spans yields the required intersection.

Proof. Choose Z in the intersection (3.1). Extend X, Y to a p -basis and let D_X, D_Y be the commuting Euler derivations of Lemma 2.2. We first translate the two descriptions of Z into differential equations. Since U and V are not scalar multiples of monomials in X and Y , respectively, the eigenvector description in that lemma gives

$$D_X U \neq 0, \quad D_Y V \neq 0.$$

Define

$$B_X = \frac{U}{D_X U}, \quad B_Y = \frac{V}{D_Y V}, \quad A_X = B_X - 1, \quad A_Y = B_Y - 1.$$

Here $A_X \in C(X) \setminus C$ and $A_Y \in C(Y) \setminus C$: if, for example, $B_X \in C$, then $D_X U = B_X^{-1} U$, making U an eigenvector and hence a scalar multiple of a monomial in X . In particular, A_X, A_Y, B_X, B_Y are all nonzero.

The derivations

$$\delta = D_X + D_Y, \quad \delta' = B_X D_X + B_Y D_Y$$

satisfy $\delta X = X$, $\delta Y = Y$, $\delta' U = U$, and $\delta' V = V$. Thus δ kills Y/X , whereas δ' kills V/U ; both kill C . The two expressions for Z therefore give

$$\delta Z = Z = \delta' Z.$$

Set

$$q_X = \frac{D_X Z}{Z}, \quad q_Y = \frac{D_Y Z}{Z}.$$

Dividing the preceding equations by Z and subtracting yields

$$q_X + q_Y = 1, \quad A_X q_X + A_Y q_Y = 0. \quad (3.3)$$

Both q_X and q_Y are nonzero: if one vanished, these two equations would force the other A to vanish.

Since δ commutes with D_X and D_Y , the equation $\delta Z = Z$ implies that q_X, q_Y are killed by δ :

$$\delta q_X = \frac{D_X(\delta Z)}{Z} - \frac{D_X Z \delta Z}{Z^2} = 0, \quad \delta q_Y = 0.$$

By (3.3), $A_X/A_Y = -q_Y/q_X$, so $\delta(A_X/A_Y) = 0$. Since $D_Y A_X = D_X A_Y = 0$, we obtain

$$\frac{D_X A_X}{A_X} = \frac{D_Y A_Y}{A_Y}. \quad (3.4)$$

The left side lies in $C(X)$ and the right side in $C(Y)$. Their intersection is C , by the p -monomial basis. Consequently A_X and A_Y are eigenvectors of their respective Euler derivations with the same eigenvalue. The distinct eigenvalues on $1, X, \dots, X^{p-1}$, and on $1, Y, \dots, Y^{p-1}$, now give

$$A_X = c_X X^m, \quad A_Y = c_Y Y^m \quad (3.5)$$

for $c_X, c_Y \in C^\times$ and one integer m , $1 \leq m < p$. The eigenvalue cannot be zero because $A_X, A_Y \notin C$.

It remains to integrate (3.5) inside the one-variable subfields. Put $n = p - m$. The identity $1 + c_X X^m = B_X \neq 0$ ensures that all terms in

$$\frac{D_X(U^n)}{U^n} = \frac{n}{1 + c_X X^m} = \frac{D_X(X^n + c_X X^p)}{X^n + c_X X^p}$$

are defined. Thus D_X kills $U^n/(X^n + c_X X^p) \in C(X)^\times$. Its kernel on $C(X)$ is C , so this quotient belongs to $C^\times$. Since $X^p \in C^\times$, we have $U^n \in C + CX^n$ with both coefficients nonzero. Replacing X, U, c_X, D_X by Y, V, c_Y, D_Y proves the second inclusion.

Finally, suppose $U^r = h + jX^r$ with $h, j \in C$ and $1 \leq r < p$. Both coefficients must be nonzero: otherwise $r[U] \in \mathbf{F}_p[X]$, contrary to $[U] \notin \mathbf{F}_p[X]$. Taking logarithmic derivatives gives

$$\frac{D_X U}{U} = \frac{jX^r}{h + jX^r}, \quad A_X = \frac{h}{jX^r}.$$

The last expression is a nonzero scalar multiple of X^{p-r} , since $X^p \in C^\times$. Comparison with (3.5) and linear independence of the p monomials forces $p - r = m$, hence $r = n$. The argument for the inclusion involving V is identical. $\square$

All hypotheses and conclusions of Proposition 3.1 are unchanged when X, Y, U, V are multiplied by elements of $C^\times$. In particular, its exponent depends on projective points, rather than on the representatives used in the calculation.

4 One scalar recovers all projective lines

The intersection calculation produces a power correction for two points at a time. We now show that a single correction works throughout the projective space. The passage from local power corrections to a global one parallels Cadoret and Pirutka [4, Section 3.5]; here the

degree- p subfields give a particularly simple connected graph on which to propagate the correction.

We first record why a nontrivial scalar cannot preserve projective lines. This will rule out a new scalar when we apply the line-recovery argument to the inverse map.

Lemma 4.1. *Let F have characteristic p , with $F \neq F^p$. If multiplication by $r \in \mathbf{F}_p^\times$ on V_F maps every projective line over F^p into a projective line, then $r = 1$.*

Proof. Represent r by an integer $1 \leq r < p$ and take $x \in F \setminus F^p$. The points $[1], [x], [x+1]$ lie on one line. Their images under multiplication by r are $[1], [x^r], [(x+1)^r]$. The first two are distinct, so the asserted line containment implies

$$(x+1)^r \in F^p + F^p x^r.$$

If $1 < r < p$, the binomial expansion has nonzero coefficient r at x^{r-1} . This contradicts the linear independence of $1, x, \dots, x^{p-1}$ over F^p from Lemma 2.2. $\square$

Proposition 4.2. *Let K/k and L/l be finitely generated extensions of algebraically closed fields of characteristic p , both of transcendence degree at least two. For every compatible isomorphism $\Theta : V_K \rightarrow V_L$, there is a unique $n \in \mathbf{F}_p^\times$ such that $\Psi = n\Theta$ sends every projective line over K^p onto a projective line over L^p .*

Remark (notation). $\Psi = n\Theta$, where $n \in \mathbf{F}_p^\times$ is the unique scalar for which this map sends every projective line over K^p onto a projective line over L^p .

Proof. Put $H = K^p$ and $C = L^p$. We first find one scalar for which lines map into lines. Only after this construction will we apply it to the inverse.

Remark (notation). H denotes the source scalar field in the projective geometry under consideration. In Theorem 1.1, Proposition 4.2: $H = K^p$. In Proposition 5.1: H is an arbitrary field over which E is a finite-dimensional vector space of dimension at least three. A connected graph of independent image pairs. On the nonzero elements of V_K , join $[x]$ and $[y]$ by an edge when

$$C(X) \neq C(Y), \quad [X] = \Theta([x]), \quad [Y] = \Theta([y]).$$

This condition is independent of the chosen representatives. Since $X, Y \notin C$, the fields $C(X)$ and $C(Y)$ have degree p over C . An edge therefore means that X, Y are p -independent. The graph is complete between distinct parts of the partition by the fields $C(X)$. It has at least two parts: by Lemma 2.1, $[L : C] \geq p^2$, so for any $X \notin C$ there is an element of $L \setminus C(X)$, and Θ is surjective. Thus every vertex has a neighbor, and any two vertices are joined by a path of length at most two.

An affine configuration along an edge. Fix an edge $[x], [y]$. The elements $1, x, y$ are linearly independent over H . Indeed, a dependence would give $y = c + dx$ with $c, d \in H$ and $d \neq 0$, since $x, y \notin H$. If $c = 0$, the two vertices would coincide. Otherwise Lemma 2.4 gives $\{x, y\}_K = 0$, and compatibility followed by Lemma 2.3 gives $Y \in C(X)$, again contradicting the edge condition.

For arbitrary $a, b \in H^\times$, set

$$u = x + a, \quad v = y + b, \quad z = bx - ay = bu - av. \quad (4.1)$$

These are nonzero: u, v are nonzero because $x, y \notin H$, and $z \neq 0$ because x, y are H -linearly independent. Moreover,

$$[u] \notin \mathbf{F}_p[x], \quad [v] \notin \mathbf{F}_p[y]. \quad (4.2)$$

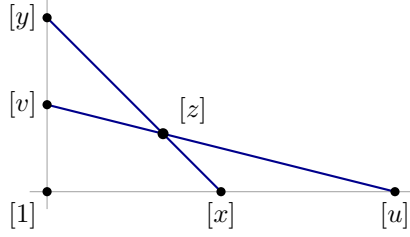


Figure 1: The source configuration in the projective plane $\mathbf{P}_H(H + Hx + Hy)$. The point $[z]$ lies on both the line joining $[x], [y]$ and the line joining $[u], [v]$. The drawing records only incidences; it imposes no order or metric on the characteristic- p field.

For example, $[u] = i[x]$ with $0 \leq i < p$ would give $x + a = hx^i$ for some $h \in H^\times$, contrary to the linear independence of $1, x, \dots, x^{p-1}$ and the condition $a \neq 0$. Figure 1 shows the incidence that explains the two expressions for z .

Lemma 2.4, applied also to $z/x = b - a(y/x)$ and $z/u = b - a(v/u)$, gives

$$\{x, u\}_K = \{y, v\}_K = \{y/x, z/x\}_K = \{v/u, z/u\}_K = 0. \quad (4.3)$$

Write $[U] = \Theta([u])$, $[V] = \Theta([v])$, and $[Z] = \Theta([z])$. Compatibility and Lemma 2.3 applied to the first two symbols show that

$$U \in C(X)^\times, \quad V \in C(Y)^\times.$$

Linearity and injectivity transport (4.2) to $[U] \notin \mathbf{F}_p[X]$ and $[V] \notin \mathbf{F}_p[Y]$. In particular $U, V \notin C$. Also $Y/X \notin C$, since X, Y are p -independent, and $V/U \notin C$: otherwise U would belong to $C(X) \cap C(Y) = C$. We may therefore apply Lemma 2.3 to the last two symbols in (4.3). The result is

$$Z \in XC(Y/X)^\times \cap UC(V/U)^\times.$$

All hypotheses of Proposition 3.1 now hold. It gives a common integer $1 \leq n < p$ such that

$$U^n \in C + CX^n, \quad V^n \in C + CY^n, \quad (4.4)$$

and either inclusion uniquely determines n .

Propagation of the scalar. Fix representatives for all vertices and their images. For a vertex $[x]$, fix one neighbor $[y]$ and one $b \in H^\times$. As $a \in H^\times$ varies, Proposition 3.1 applies to (4.1). The second inclusion in (4.4), whose pair Y, V stays fixed, forces the same n for every a . To compare choices of neighbor and b , specialize to $a = 1$, keeping X and a representative U of $\Theta([x + 1])$ fixed. Uniqueness for the first inclusion shows that these choices cannot change n . Thus each vertex has a well-defined scalar. Adjacent vertices have the same scalar by (4.4). Connectedness consequently supplies a single n for all vertices and all $a \in H^\times$.

Set $\Psi = n\Theta$, with n viewed in $\mathbf{F}_p^\times$. The line joining $[1]$ and $[x]$ consists of those two points and $[x + a]$ for $a \in H^\times$. The first inclusion in (4.4) says exactly that its image is contained in the line joining $[1]$ and $[X^n]$. Every projective line is a multiplicative translate of one through $[1]$: multiply the line joining $[s], [t]$ by s^{-1} . Multiplication by a nonzero field element is linear over the field of p -th powers, and Ψ respects the multiplicative group law. Thus Ψ maps every line into a line.

Equality of lines and uniqueness. Scalar multiplication preserves compatibility, since it scales the tensor square by the nonzero scalar n^2 . Hence Ψ^{-1} is compatible. Apply the construction just completed, with the fields reversed, to obtain $r \in \mathbf{F}_p^\times$ for which $r\Psi^{-1}$ maps lines into lines. Its composition with Ψ is multiplication by r on V_K and has the same line-containment

property. Lemma 4.1 forces $r = 1$. Thus both Ψ and its inverse map lines into lines. If $\Psi(\ell) \subseteq \ell'$, choose a line ℓ'' containing $\Psi^{-1}(\ell')$. Then

$$\ell \subseteq \Psi^{-1}(\ell') \subseteq \ell''.$$

Two projective lines cannot properly contain one another, so $\ell = \ell''$ and both inclusions are equalities. Applying Ψ gives $\Psi(\ell) = \ell'$.

Finally, if $m\Theta$ also sends lines onto lines, then $(m\Theta) \circ \Psi^{-1}$ is multiplication by mn^{-1} on V_L and preserves lines. Another application of Lemma 4.1 gives $m = n$. $\square$

5 From projective lines to the field

Proposition 4.2 has recovered a bijection of projective spaces that preserves both lines and the multiplicative group law. The fundamental theorem of projective geometry [5, Section 8.2, Theorem 8.2] recovers addition from the lines; the group law then forces the resulting additive map to be multiplicative. This last passage also appears in Cadoret and Pirutka [4, Section 4, Lemma 29]. We include the coordinate argument to make both the reconstruction and its uniqueness explicit.

Proposition 5.1 (Projective lifting). *Let E and E' be finite-dimensional vector spaces over fields H and C , respectively, with dimensions at least three. Every bijection $\psi : \mathbf{P}_H(E) \rightarrow \mathbf{P}_C(E')$ that maps lines onto lines is induced by an additive bijection $S : E \rightarrow E'$ satisfying*

$$S(av) = \sigma(a)S(v) \quad (a \in H, v \in E)$$

for a field isomorphism $\sigma : H \rightarrow C$. The map σ is unique, and S is unique up to multiplication by an element of $C^\times$.

Remark (notation). E is local notation for a vector space or a field, as specified in its statement or proof. In Proposition 5.1: E is a finite-dimensional vector space over H with $\dim_H E \geq 3$. In Lemma 5.2: For $f \in F \setminus \kappa$, choose a transcendence basis $f, t_2, \dots, t_d$ over κ and put $B = \kappa(t_2, \dots, t_d)$ and $E = B(f)$; the extension F/E is finite. E' is a finite-dimensional vector space over C with $\dim_C E' \geq 3$. $\psi : \mathbf{P}_H(E) \rightarrow \mathbf{P}_C(E')$ is a bijection that maps projective lines onto projective lines. S is an additive bijection between the source and target vector spaces inducing the specified projective bijection and satisfying $S(av) = \sigma(a)S(v)$ for source scalars a and source vectors v . In Proposition 5.1: $S : E \rightarrow E'$ induces ψ and is determined only up to multiplication by an element of $C^\times$. In Theorem 1.1: $S : K \rightarrow L$ lifts $\Psi = n\Theta$ over $H = K^p$ and $C = L^p$; it is scaled to satisfy $S(1) = 1$ and is then a field isomorphism with $S(k) = l$.

Proof. The inverse also maps lines onto lines: a target line is the image of the line joining the preimages of any two distinct points on it. Projective spans are obtained by repeatedly joining pairs of points by lines, so ψ and its inverse preserve spans. Minimal spanning sets therefore correspond, and $\dim_H E = \dim_C E' = N + 1$ for some $N \geq 2$. Choose a basis $e_0, \dots, e_N$ of E and representatives $e'_0, \dots, e'_N$ of their images. They form a basis of E' . Keeping e'_0 fixed, scale each e'_i , $i \geq 1$, so that

$$\psi([e_0 + e_i]) = [e'_0 + e'_i].$$

This is possible because $[e_0 + e_i]$ lies on the line joining $[e_0]$ to $[e_i]$ and differs from both endpoints.

The hyperplanes spanned by $e_1, \dots, e_N$ and by $e'_1, \dots, e'_N$ correspond. On their affine complements use the coordinates

$$(t_1, \dots, t_N) \longleftrightarrow [e_0 + t_1 e_1 + \dots + t_N e_N].$$

The induced affine bijection preserves parallelism: parallel lines have the same point on the corresponding hyperplane at infinity. On the i th coordinate axis it is a bijection $\sigma_i : H \rightarrow C$ fixing 0 and 1. Varying only the j th input coordinate moves along a line with point at infinity $[e_j]$, whose image has point at infinity $[e'_j]$. Hence all other output coordinates are unchanged. It follows that the affine map is

$$(t_1, \dots, t_N) \mapsto (\sigma_1(t_1), \dots, \sigma_N(t_N)).$$

In each plane of two coordinate axes, the diagonal through $(0, 0)$ and $(1, 1)$ maps to the corresponding diagonal. Thus all σ_i equal one bijection $\sigma : H \rightarrow C$. In the first two coordinates, the line $(t, t + a)$ is parallel to this diagonal and passes through $(0, a)$. Its image therefore gives

$$\sigma(t + a) = \sigma(t) + \sigma(a).$$

The line (t, at) passes through $(0, 0)$ and $(1, a)$, so its image gives

$$\sigma(at) = \sigma(a)\sigma(t).$$

Since $\sigma(1) = 1$, it is a field isomorphism.

Define $S(\sum_{i=0}^N t_i e_i) = \sum_{i=0}^N \sigma(t_i) e'_i$. This is an additive, σ -semilinear bijection inducing ψ on the affine chart. Every point at infinity is the direction of an affine line through the origin, so it induces ψ there as well.

For uniqueness, suppose that T is another semilinear lift, possibly with a different field isomorphism. For every nonzero $v \in E$ write $T(v) = c_v S(v)$ with $c_v \in C^\times$. If v, w are independent, additivity applied to $v + w$ and independence of $S(v), S(w)$ give $c_v = c_w = c_{v+w}$. Two dependent nonzero vectors can each be compared to a vector outside their common line. Thus c_v is a single scalar c , and $T = cS$. Comparing the images of av then shows that the two field isomorphisms also agree. $\square$

We will also recover the prescribed algebraically closed base directly from the field.

Lemma 5.2. *If F/κ is a finitely generated extension of an algebraically closed field of characteristic p , then*

$$\bigcap_{m \geq 1} F^{p^m} = \kappa.$$

Proof. Perfectness gives the inclusion from right to left. If $f \in F \setminus \kappa$, algebraic closedness makes f transcendental over κ . Complete f to a transcendence basis $f, t_2, \dots, t_d$, and put $B = \kappa(t_2, \dots, t_d)$ and $E = B(f)$. The extension F/E is finite; write $D = [F : E]$. For every $m \geq 1$, the polynomial $T^{p^m} - f$ is Eisenstein at the prime f of $B[f]$, and is therefore irreducible over E . If $f = g^{p^m}$ with $g \in F$, it follows that

$$p^m = [E(g) : E] \leq D.$$

This fails for all sufficiently large m , so f does not belong to the intersection. $\square$

Proof of Theorem 1.1. A field isomorphism $\alpha : K \rightarrow L$ sends K^p to L^p and Steinberg pairs to Steinberg pairs. It therefore induces an element of $\text{Isom}_M(V_K, V_L)$, and the canonical map in the theorem is well defined.

For surjectivity, take $\Theta \in \text{Isom}_M(V_K, V_L)$. Proposition 4.2 gives $n \in \mathbf{F}_p^\times$ such that $\Psi = n\Theta$ maps lines onto lines. Put $H = K^p$ and $C = L^p$. By Lemma 2.1, $\dim_H K$ and $\dim_C L$ are at least $p^2 \geq 4$, so Proposition 5.1 gives a semilinear lift $S : K \rightarrow L$. Since $\Psi([1]) = [1]$, scale S to arrange $S(1) = 1$. For each $f \in K^\times$, the two semilinear bijections

$$w \mapsto S(fw), \quad w \mapsto S(f)S(w)$$

induce the same projective map: the equality is precisely $\Psi([fw]) = \Psi([f]) + \Psi([w])$ in the additive notation for V_L . Their values at 1 agree, so the uniqueness assertion in Proposition 5.1 makes them equal. Thus S is multiplicative, and hence a field isomorphism. It maps every K^{p^m} onto L^{p^m} , so Lemma 5.2 gives $S(k) = l$. Its induced map is $n\Theta$, proving surjectivity onto the scalar quotient.

For injectivity, suppose that field isomorphisms $\alpha, \beta : K \rightarrow L$ induce maps with $\beta_* = r\alpha_*$ for $r \in \mathbf{F}_p^\times$. Both preserve projective lines, so multiplication by r on V_L also preserves lines. Lemma 4.1 gives $r = 1$. The maps α and β are therefore semilinear lifts of the same projective bijection. Proposition 5.1 makes them scalar multiples, and $\alpha(1) = \beta(1) = 1$ makes them equal. $\square$

Remark 5.3 (Frobenius and the target quotient). There is no further Frobenius ambiguity. For a field F/κ as in the theorem, the Frobenius map $F \rightarrow F$, $f \mapsto f^p$, is not surjective and induces the zero map on V_F . By contrast, $F \rightarrow F^p$ is a field isomorphism, whose induced isomorphism has target

$$V_{F^p} = (F^p)^\times / (F^{p^2})^\times.$$

It is already covered by the theorem, with its actual target field F^p .

References

- [1] Spencer Bloch and Kazuya Kato. p -adic étale cohomology. *Publications Mathématiques de l’IHÉS*, 63:107–152, 1986. doi: 10.1007/BF02831624. URL <https://doi.org/10.1007/BF02831624>.
- [2] Fedor Bogomolov and Yuri Tschinkel. Milnor K_2 and field homomorphisms. In Huai-Dong Cao and Shing-Tung Yau, editors, *Geometry, Analysis and Algebraic Geometry: Forty Years of the Journal of Differential Geometry*, volume 13 of *Surveys in Differential Geometry*, pages 223–244. International Press, Somerville, MA, 2009. URL <https://arxiv.org/abs/0902.4875>.
- [3] Fedor Bogomolov and Yuri Tschinkel. Introduction to birational anabelian geometry. In Lucia Caporaso, James McKernan, Mircea Mustață, and Mihnea Popa, editors, *Current Developments in Algebraic Geometry*, volume 59 of *Mathematical Sciences Research Institute Publications*, pages 17–64. Cambridge University Press, Cambridge, 2012. doi: 10.1017/9781139032766.003. URL <https://doi.org/10.1017/9781139032766.003>.
- [4] Anna Cadoret and Alena Pirutka. Reconstructing function fields from Milnor K -theory. *Algebra & Number Theory*, 15(9):2261–2288, 2021. doi: 10.2140/ant.2021.15.2261. URL <https://webusers.imj-prg.fr/~anna.cadoret/K2.pdf>. Numbered locators refer to the author version of August 28, 2019.
- [5] J. I. Hall. Classical groups and geometry. Lecture notes, Michigan State University, 2015. URL https://users.math.msu.edu/users/halljo/classes/MTH913_S15/cgg_2015-05-06.pdf. Version of May 6, 2015.
- [6] John Milnor. Algebraic K -theory and quadratic forms. *Inventiones Mathematicae*, 9(4): 318–344, 1970. doi: 10.1007/BF01425486. URL <https://doi.org/10.1007/BF01425486>.
- [7] Adam Topaz. Reconstructing function fields from rational quotients of mod- ℓ Galois groups. *Mathematische Annalen*, 366(1–2):337–385, 2016. doi: 10.1007/s00208-015-1327-4. URL <https://doi.org/10.1007/s00208-015-1327-4>.

- [8] Adam Topaz. Algebraic dependence and Milnor K -theory, 2023. URL <https://raw.githubusercontent.com/adamtopaz/MilnorAlgDep/main/main.pdf>. Author version of January 18, 2023; originally arXiv:2211.14665 (2022).