FIELD THEORY

December 14, 2025

Contents

1. Definitions

1.1. Algebraic field extensions.

Definition 1.1.1 (Field)**.** A *field* is commutative division ring. In other words, a field is a commutative ring for which all nonzero elements have a multiplicative inverse.

Definition 1.1.2. Let K and L be fields (Definition 1.1.1).

1. A map $\phi : K \to L$ is a *field homomorphism* if it satisfies the following axioms for all $x, y \in K$:
   (a) $\phi(x + y) = \phi(x) + \phi(y)$ (additivity);
   (b) $\phi(xy) = \phi(x)\phi(y)$ (multiplicativity);
   (c) $\phi(1_K) = 1_L$ (unitality).
   Equivalently, a field homomorphism is a ring homomorphism (Definition A.0.7) between fields.
   If such a map exists, we often say that *K embeds into L*; this terminology is justified because field homomorphisms are injective (Definition A.0.8) as set maps (Proposition 1.1.3).
2. A field homomorphism $\phi : K \to L$ is an *isomorphism* if it is bijective (Definition A.0.8).
3. The set of all homomorphisms from a field K to a field L is denoted by $\mathrm{Hom}(K, L)$.
4. Assuming that K and L have a common subfield F, an *F-embedding of K into L* is an embedding $K \to L$ that acts as the identity map (Definition A.0.9) on F. The set of F-embeddings of K into L is denoted by $\mathrm{Hom}_F(K, L)$.

If K and L are fields such that K embeds into L, then that means that there is a subfield (Definition 1.1.5) of L that is isomorphic to K.

Proposition 1.1.3. Let K and L be fields (Definition 1.1.1) and let $\phi : K \to L$ be a field homomorphism (Definition 1.1.2). Then ϕ is injective (Definition A.0.8).

Definition 1.1.4 (Vector space over a field)**.** Let $(k, +, \cdot)$ be a field (Definition 1.1.1). A *vector space over k* or a *k-vector space* is a triple $(V, +, \cdot)$[1] where

1. $(V, +)$ is an abelian group, and
2. $\cdot$ is a map $k \times V \to V$, called *scalar multiplication*

such that the following axioms hold for all $a, b \in k$ and all $u, v \in V$:

1. (Compatibility with field multiplication)
$$(ab) \cdot v = a \cdot (b \cdot v).$$
2. (Identity scalar)
$$1 \cdot v = v.$$
3. (Distributivity over vector addition)
$$a \cdot (u + v) = a \cdot u + a \cdot v.$$
4. (Distributivity over scalar addition)
$$(a + b) \cdot v = a \cdot v + b \cdot v.$$

Definition 1.1.5 (Field Extension)**.** Let K be a field and let L be a field such that $K \subseteq L$ and the operations of K are the restrictions of those of L. Then L is called a *extension field (or just an extension) of K*. The notation L/K is often used synonymously; we say that L/K is a *field extension*. Moreover, K is said to be a *subfield of L*.

Definition 1.1.6. Let R be a ring. There exists a unique ring homomorphism (Definition A.0.7) $\psi : \mathbb{Z} \to R$ defined by mapping $n \mapsto n \cdot 1_K$. The non-negative generator of the kernel of this map, $\ker(\psi) = \langle p \rangle \subseteq \mathbb{Z}$, is called the *characteristic of R*, denoted by $\mathrm{char}(R)$.

Proposition 1.1.7. Let K be a field (Definition 1.1.1). Then $\mathrm{char}(K)$ (Definition 1.1.6) is either 0 or a prime number p.

Definition 1.1.8. (♠ TODO: finite field, rational numbers) Let K be a field. The *prime subfield of K* is the intersection of all subfields (Definition 1.1.5) of K.

- If $\mathrm{char}(K) = p > 0$, the prime subfield is isomorphic to the finite field $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$.
- If $\mathrm{char}(K) = 0$, the prime subfield is isomorphic to the field of rational numbers $\mathbb{Q}$.

Lemma 1.1.9. Let L/K be a field extension (Definition 1.1.5). Then L is a vector space (Definition 1.1.4) over K.

Definition 1.1.10 (Degree of an Extension, Finite Extension)**.** Let L/K be a field extension (Definition 1.1.5). The *degree* of the extension $[L : K] := \dim_K(L)$, i.e. the dimension of L as a K-vector space (Lemma 1.1.9). If $[L : K] < \infty$, the extension L/K is called a *finite field extension* and L is said to be a *finite extension of K*.

[1] Note that $+$ and $\cdot$ are abuse of notation here as these are already used for the addition and multiplication of $\cdot$

Definition 1.1.11 (Algebraic Element, Algebraic Extension)**.** Let L/K be a field extension (Definition 1.1.5) and let $x \in L$.

- If there exists a nonzero polynomial $f(t) \in K[t]$ such that $f(x) = 0$, then x is called an *algebraic element over K*. There exists a unique such monic irreducible polynomial $f(t)$, which is called the *minimal polynomial of x over K*.
- Otherwise, x is called a *transcendental element over K*.

If every $x \in L$ is algebraic over K, then L/K is called an *algebraic extension*.

Definition 1.1.12. A field (Definition 1.1.1) F is said to be *algebraically closed* if every nonconstant polynomial $f(x) \in F[x]$ has a root in F, i.e., for every such $f(x)$ there exists $a \in F$ with $f(a) = 0$.

Definition 1.1.13. Let K be a field. A field extension L/K is called an *algebraic closure of K* if the following two conditions hold:

1. Every element $a \in L$ is algebraic over K (Definition 1.1.11).
2. The field L is algebraically closed (Definition 1.1.12).

One often writes an algebraic closure of K by $\overline{K}$.

Definition 1.1.14 (Field Generated by Elements)**.** Let L/K be a field extension (Definition 1.1.5) and let $S \subseteq L$ be a subset. The *field generated by S over K* is the smallest subfield of L that contains K and S. Equivalently, it is the intersection of all subfields of L containing $K \cup S$. This field is denoted by $K(S)$.

In the special case where $S = \{x_1, \dots, x_n\}$ is finite, one writes $K(x_1, \dots, x_n)$. If $n = 1$, then $K(x)$ is called a *simple field extension*.

Definition 1.1.15 (Finitely generated field extension)**.** Let E/F be a field extension (Definition 1.1.5). We say that E/F is *finitely generated* if there exist finitely many elements $\alpha_1, \dots, \alpha_n \in E$ such that $E = F(\alpha_1, \dots, \alpha_n)$ (Definition 1.1.14), where $F(\alpha_1, \dots, \alpha_n)$ denotes the smallest subfield of E containing F and $\{\alpha_1, \dots, \alpha_n\}$.

Definition 1.1.16 (Field Automorphism)**.** Let L be a field. A *field automorphism of L* is a bijective ring homomorphism $L \to L$.

Definition 1.1.17 (Automorphism Group of a Field Extension)**.** Let L/K be a field extension (Definition 1.1.5).

- An automorphism (Definition 1.1.16) $\sigma : L \to L$ is called a *K-automorphism* if σ is a field automorphism of L that fixes every element of K, i.e. $\sigma(a) = a$ for all $a \in K$.
- The set of all such K-automorphisms of L forms a group (Definition A.0.2) under composition, called the *automorphism group of the extension L/K*. It is usually denoted by $\mathrm{Aut}(L/K)$ or $\mathrm{Aut}_K(L)$.

Definition 1.1.18 (Normal Extension)**.** Let K be a field and let $S \subseteq K[t]$ be a set of polynomials.

- A field $L \supseteq K$ is a *splitting field of S over K* if

– every polynomial in S splits completely into linear factors over L, and
– L is generated over K (Definition 1.1.14) by the roots of the polynomials in S, namely

$$L = K(\{\alpha \mid f(\alpha) = 0,\ f \in S\}).$$

- An algebraic extension L/K is called a *normal extension* if L is the splitting field of a family of polynomials in $K[t]$.

Definition 1.1.19 (Separable Element, Separable Extension)**.** Let L/K be a field extension (Definition 1.1.5) and let $x \in L$ be algebraic over K (Definition 1.1.11) with minimal polynomial (Definition 1.1.11) $m_{x,K}(t) \in K[t]$.

- The element x is *separable over K* if $m_{x,K}(t)$ has distinct roots in a splitting field (Definition 1.1.18).
- The element x is *inseparable over K* otherwise.

An algebraic extension (Definition 1.1.11) L/K is called *separable extension* if every element $x \in L$ is separable over K.

See also Definition 1.2.6, which defines separable field extensions in greater generality.

Definition 1.1.20. A field F is said to be *separably closed* if every nonconstant separable polynomial $f(x) \in F[x]$ has a root in F, i.e., for every such $f(x)$ there exists $a \in F$ with $f(a) = 0$ (equivalently, every separable polynomial factors completely into linear factors over F).

Definition 1.1.21. Let K be a field (Definition 1.1.1). A field extension (Definition 1.1.5) L/K is called a *separable closure of K* if the following hold:

1. The extension L/K is separable algebraic (Definition 1.1.19) (i.e., every $a \in L$ is separable over K).
2. The field L is separably closed (Definition 1.1.20).

One often writes a separable closure of K by K^{sep}. Some also write separable closures of K by $\overline{K}$, which may conflict with the common notation for algebraic closures of K.

Definition 1.1.22 (Galois Extension)**.** An extension L/K is called a *Galois extension* if it is both a normal extension (Definition 1.1.18) and a separable algebraic extension (Definition 1.1.19). Its *Galois group*, usually denoted by $\mathrm{Gal}(L/K)$, is defined to be the automorphism group $\mathrm{Aut}(L/K)$ (Definition 1.1.17).

Theorem 1.1.23 (Fundamental Theorem of Galois Theory)**.** Let L/K be a finite (Definition 1.1.10) Galois extension of fields (Definition 1.1.22) with Galois group $G = \mathrm{Gal}(L/K)$. Then there is an inclusion-reversing bijection between the set of subgroups $H \leq G$ and the set of intermediate fields $K \subseteq F \subseteq L$, given by (♠ TODO: L^H)

$$H \longmapsto L^H := \{\, x \in L \mid \sigma(x) = x \text{ for all } \sigma \in H \,\},$$

$$F \longmapsto \mathrm{Gal}(L/F).$$

This correspondence has the following properties:

(i) L^H is a subfield of L containing K for each subgroup $H \leq G$.

(ii) $\mathrm{Gal}(L/F)$ is a subgroup of G for each intermediate field F.

(iii) $H_1 \subseteq H_2 \iff L^{H_2} \subseteq L^{H_1}$.

(iv) $[L^H : K] = |G : H|, \quad [L : L^H] = |H|$.

(v) F/K is Galois if and only if $\mathrm{Gal}(L/F) \trianglelefteq G$,

in which case $\mathrm{Gal}(F/K) \cong G/\mathrm{Gal}(L/F)$.

Corollary 1.1.24 (Normality of the whole extension)**.** If L/K is a finite (Definition 1.1.10) Galois extension of fields (Definition 1.1.22) with Galois group G, then $K = L^G$. (♠ TODO: L^G)

Theorem 1.1.25 (Primitive element theorem)**.** Let L/K be a finite (Definition 1.1.10) separable extension (Definition 1.1.19). Then there exists an element $\alpha \in L$ such that

$$L = K(\alpha).$$

(Definition 1.1.14) In other words, every finite separable extension is simple (Definition 1.1.14).

Lemma 1.1.26 (Normal extension characterization)**.** (♠ TODO: embedding) Let L/K be a finite extension. Then L/K is normal (Definition 1.1.18) if and only if every K-embedding $\sigma : L \to \overline{K}$ into an algebraic closure (Definition 1.1.11) $\overline{K}$ satisfies $\sigma(L) = L$.

Theorem 1.1.27 (Infinite Galois Theory)**.** Let L/K be a (possibly infinite) Galois extension with Galois group $G = \mathrm{Gal}(L/K)$. Endow G with the Krull topology, i.e. the unique compact, Hausdorff, totally disconnected topology whose neighborhood basis at the identity is given by the open subgroups $\mathrm{Gal}(L/F)$, where F runs through the finite Galois intermediate extensions $K \subseteq F \subseteq L$.

Then there is an inclusion-reversing bijection between: - the closed subgroups $H \leq G$, and - the intermediate fields $K \subseteq F \subseteq L$,

given by

$$H \longmapsto L^H := \{\, x \in L \mid \sigma(x) = x \text{ for all } \sigma \in H \,\},$$
$$F \longmapsto \mathrm{Gal}(L/F).$$

This correspondence satisfies:

(i) $H \leq G$ closed $\iff$ $F = L^H$ for some intermediate field F.

(ii) F/K is finite Galois $\iff$ $\mathrm{Gal}(L/F)$ is open in G.

(iii) F/K is Galois $\iff$ $\mathrm{Gal}(L/F) \trianglelefteq G$,

in which case $\mathrm{Gal}(F/K) \cong G/\mathrm{Gal}(L/F)$.

Proposition 1.1.28 (Krull topology characterization)**.** For a (possibly infinite) Galois extension L/K, the Galois group $G = \mathrm{Gal}(L/K)$ is a profinite group, i.e. a compact, Hausdorff, totally disconnected topological group isomorphic to an inverse limit of finite groups.

1.2. **Transcendence degrees.**

Definition 1.2.1 (Algebraically independent elements)**.** Let E/F be a field extension (Definition 1.1.5), and let $S = \{x_i\}_{i \in I}$ be a subset of E indexed by some set I. We say that S is *algebraically independent over F* if for every finite subset $\{x_{i_1}, \ldots, x_{i_n}\} \subseteq S$ and every non-zero polynomial $P \in F[X_1, \ldots, X_n]$, we have $P(x_{i_1}, \ldots, x_{i_n}) \neq 0$. Equivalently, S is algebraically independent over F if the natural ring homomorphism (Definition A.0.7)

$$F[X_i : i \in I] \to E$$

sending $X_i \mapsto x_i$ is injective, where $F[X_i : i \in I]$ denotes the polynomial ring (Definition A.0.4) over F in the indeterminates $\{X_i\}_{i \in I}$.

Definition 1.2.2 (Transcendence basis)**.** Let E/F be a field extension (Definition 1.1.5). A subset $T \subseteq E$ is called a *transcendence basis* of E over F if:

1. T is algebraically independent over F, i.e., there is no non-trivial polynomial relation with coefficients in F among finitely many elements of T, and
2. E is algebraic (Definition 1.1.11) over $F(T)$, where $F(T)$ denotes the field generated by (Definition 1.1.14) F and T.

Definition 1.2.3 (Transcendence degree)**.** Let E/F be a field extension (Definition 1.1.5). The *transcendence degree of E over F*, denoted $\operatorname{tr.deg}_F(E)$ or $\operatorname{trdeg}_F(E)$, is defined as the cardinality (Definition A.0.5) of any transcendence basis (Definition 1.2.2) of E over F. By a classical result, all transcendence bases of E over F have the same cardinality, so the transcendence degree is well-defined.

If E/F is algebraic (Definition 1.1.11), then $\operatorname{tr.deg}_F(E) = 0$. If no transcendence basis is finite, then $\operatorname{tr.deg}_F(E)$ is an infinite cardinal.

Definition 1.2.4 (Function field)**.** Let k be a field (Definition 1.1.1). A field K is called a *function field over k* (or a *function field in n variables over k*) if K is a finitely generated field extension (Definition 1.1.15) of k with transcendence degree (Definition 1.2.3) n over k, where $n \geq 1$. Equivalently, the function field in n variables over k is isomorphic to the fraction field (Definition A.0.6) of the polynomial ring (Definition A.0.4) $k[x_1, \ldots, x_n]$ where $x_1, \ldots, x_n$ are indeterminate variables. Accordingly, the function field in n variables over k is often denoted as $k(x_1, \ldots, x_n)$.

When $n = 1$, we say that K is a *function field of one variable over k* or an *algebraic function field over k* and denote it by $k(x)$.

Definition 1.2.5 (Separating transcendence basis)**.** Let E/F be a field extension (Definition 1.1.5), and let $T \subseteq E$ be a transcendence basis of E over F. We say that T is a *separating transcendence basis* if the algebraic extension $E/F(T)$ (Definition 1.1.14) is separable (Definition 1.1.19), i.e., every element of E is separable over $F(T)$ (meaning that its minimal polynomial (Definition 1.1.11) over $F(T)$ has no repeated roots in an algebraic closure).

Definition 1.2.6 (Separable field extension)**.** Let E/F be a field extension (Definition 1.1.5). In general (allowing transcendental extensions), E/F is called *separable* if there exists a separating transcendence basis (Definition 1.2.5) for E over F. Equivalently, E/F is separable if every finitely generated (Definition 1.1.15) intermediate field $F \subseteq K \subseteq E$ has a separating transcendence basis over F. In particular, a field extension E/F is algebraic and separable in the above sense if and only if it is a separable algebraic extension in the sense of Definition 1.1.19.

Appendix A. Miscellaneous definitions

Definition A.0.1. Let X and Y be sets. A *map* (or *function*) from X to Y is a rule f assigning to each element $x \in X$ exactly one element $f(x) \in Y$. We write $f : X \to Y$.

We say that X is the *domain* and that Y is the *codomain of* f.

Definition A.0.2 (Groups)**.** A *group* is a pair $(G, \cdot)$ where G is a set and $\cdot : G \times G \to G$ is a binary operation, subject to the following conditions:

1. (Associativity) For all $g, h, k \in G$ one has
$$(g \cdot h) \cdot k = g \cdot (h \cdot k).$$
2. (Identity element) There exists an element $e \in G$ such that for all $g \in G$,
$$e \cdot g = g \cdot e = g.$$
3. (Inverse element) For all $g \in G$ there exists an element $g^{-1} \in G$ such that
$$g \cdot g^{-1} = g^{-1} \cdot g = e.$$

The element e is called the *identity element of* G, and g^{-1} is called the *inverse of* g.

Equivalently, a group is a monoid with inverse elements.

A group $(G, \cdot)$ is often simply written as G, when the notation for the binary operation $\cdot$ is clear.

An *abelian group* or synonymously, a *commutative group*, is a group $(G, \cdot)$ whose binary operation $\cdot$ is *abelian* or *commutative*, i.e. satisfies
$$g \cdot h = h \cdot g$$
for all $g, h \in G$.

Definition A.0.3. Let $(R, +, \cdot)$ and $(S, +, \cdot)$ be rings, not assumed to be commutative. A function $f : R \to S$ is called a *ring homomorphism* if for all $r_1, r_2 \in R$ the following properties hold:

1. $f(r_1 + r_2) = f(r_1) + f(r_2)$,
2. $f(r_1 r_2) = f(r_1) f(r_2)$,
3. $f(1_R) = 1_S$ where 1_R and 1_S denote the multiplicative identities in R and S, respectively.

A ring homomorphism is said to be a *ring isomorphism* if it is invertible as a map of sets.

An *R-ring* refers to a ring S equipped with a ring homomorphism $f : R \to S$.

We note that a ring homomorphism $f : R \to S$ yields a natural left R-module structure on S and a natural right R-module structure on S respectively as follows for $r \in R$ and $s \in S$:

$$r \cdot s = f(r) \cdot s$$

$$s \cdot r = s \cdot f(r).$$

However, these left and right module structures need not yield a two-sided R–module structure.

Definition A.0.4 (Polynomial ring over a commutative ring)**.** Let R be a commutative ring. For a set of variables $\{x_i\}_{i\in I}$, the *polynomial ring in variables $\{x_i\}$ over R*, denoted by notations such as $R[x_i \mid i \in I]$ or $R[x_i]_{i\in}$, is defined as the commutative R-algebra whose elements are finite R-linear combinations of monomials in the variables x_i, where the variables commute with each other and with elements of R.

That is, $R[x_i \mid i \in I]$ is the free commutative R-algebra generated by the set $\{x_i\}$.

In the case that I is a finite set, and writing $y_1, \ldots, y_n$ for the variables x_i, it is customary to let $R[y_1, \ldots, y_n]$ denote the polynomial ring.

Definition A.0.5. An ordinal number κ is a *cardinal number* (or simply a *cardinal*) if for every ordinal $\alpha < \kappa$, there is no bijection (Definition A.0.8) between α and κ. Equivalently, a cardinal is an initial ordinal—an ordinal that is not equinumerous with any smaller ordinal.

The *cardinality of an arbitrary set X*, denoted by $|X|$, $\mathrm{card}(X)$, or $\#X$, is the unique cardinal number κ such that there exists a bijection between X and κ. (The existence of such a κ for every set requires the Axiom of Choice).

Definition A.0.6. Let R be an integral domain, and consider the set $R\times(R\setminus\{0\})$ as above. Define a relation $\sim$ on $R \times (R \setminus \{0\})$ by declaring that

$$(a, b) \sim (c, d) \quad \text{if and only if} \quad ad = bc,$$

for $a, c \in R$ and $b, d \in R \setminus \{0\}$. This relation is an equivalence relation. Its equivalence classes are denoted by $\frac{a}{b}$.

The set of equivalence classes

$$\left\{ \tfrac{a}{b} \,\middle|\, a \in R,\, b \in R \setminus \{0\} \right\}$$

under the relation $\sim$ defined above is called the *field of fractions of R*, and is denoted by $\mathrm{Frac}(R)$.

The operations on $\mathrm{Frac}(R)$ are defined by

$$\tfrac{a}{b} + \tfrac{c}{d} = \tfrac{ad+bc}{bd},$$
$$\tfrac{a}{b} \cdot \tfrac{c}{d} = \tfrac{ac}{bd},$$

for $a, c \in R$ and $b, d \in R \setminus \{0\}$. With these operations, $\mathrm{Frac}(R)$ is a field (Definition 1.1.1).

Definition A.0.7. Let $(R, +, \cdot)$ and $(S, +, \cdot)$ be rings, not assumed to be commutative. A function $f : R \to S$ is called a *ring homomorphism* if for all $r_1, r_2 \in R$ the following properties hold:

1. $f(r_1 + r_2) = f(r_1) + f(r_2)$,
2. $f(r_1 r_2) = f(r_1) f(r_2)$,
3. $f(1_R) = 1_S$ where 1_R and 1_S denote the multiplicative identities in R and S, respectively.

A ring homomorphism is said to be a *ring isomorphism* if it is invertible as a map of sets.

An *R-ring* refers to a ring S equipped with a ring homomorphism $f : R \to S$.

We note that a ring homomorphism $f : R \to S$ yields a natural left R-module structure on S and a natural right R-module structure on S respectively as follows for $r \in R$ and $s \in S$:

$$r \cdot s = f(r) \cdot s$$
$$s \cdot r = s \cdot f(r).$$

However, these left and right module structures need not yield a two-sided R–module structure.

Definition A.0.8. Let X and Y be sets and let $f : X \to Y$ be a function.

- The function f is said to be *injective* (or *one-to-one*) if for all $x_1, x_2 \in X$, $f(x_1) = f(x_2)$ implies $x_1 = x_2$.
- The function f is said to be *surjective* (or *onto*) if for every $y \in Y$ there exists $x \in X$ such that $f(x) = y$.
- The map f is *bijective* if it is both injective and surjective. In this case, there exists a unique *inverse map* $f^{-1} : Y \to X$ such that for all $x \in X$ and $y \in Y$,

$$f^{-1}(f(x)) = x \text{ and } f(f^{-1}(y)) = y.$$

Definition A.0.9. Let X be a set. The *identity function on X*, denoted by id_X, is the function (Definition A.0.1) $\mathrm{id}_X : X \to X$ defined by

$$\mathrm{id}_X(x) = x \quad \text{for all } x \in X.$$

It is the unique function on X satisfying $f \circ \mathrm{id}_X = f = \mathrm{id}_X \circ f$ for every function $f : X \to Y$ and every function $f : Y \to X$.

References

[Arm92] Brumer Armand. The average rank of elliptic curves i. *Inventiones mathematicae*, 109(1):445–472, 1992.

[Ayo23] Joseph Ayoub. Counterexamples to F. Morel's conjecture on $\pi_0^{\partial^1}$. *Comptes Rendus. Mathématique*, 361:1087–1090, 2023.

[BBD82] Alexander A. Beilinson, Joseph Berstein, and Pierre Deligne. Analyse et topologie sur les espaces singuliers (i). *Astérisque*, 100, 1982.

[BC19] Tilman Bauer and Magnus Carlson. Tensor products of affine and formal abelian groups. *Documenta Mathematica*, 24:2525–2582, 2019.

[BFK+17] Valentin Blomer, Étienne Fouvry, Emmanuel Kowalski, Philippe Michel, and Djordje Milićević. Some applications of smooth bilinear forms with kloosterman sums. *Proceedings of the Steklov Institute of Mathematics*, 296:18–29, 2017.

[BGI71] Pierre Berthelot, Alexander Grothendieck, and Luc Illusie. *Théorie des Intersections et Théorème de Riemann-Roch (SGA6)*, volume 225 of *Lecture Notes in Mathematics*. Springer-Verlag, 1971.

[BH12] Salman Baig and Chris Hall. Experimental data for goldfeld's conjecture over function fields. *Experimental Mathematics*, 21(4):362–374, 2012.

[BLGHT11] Tom Barnet-Lamb, David Geraghty, Michael Harris, and Richard Taylor. A family of Calabi–Yau varieties and potential automorphy ii. *Publications of the Research Institute for Mathematical Sciences*, 47(1):29–98, 2011.

[Bor12] Armand Borel. *Linear algebraic groups*, volume 126 of *Graduate Texts in Mathematics*. Springer New York, 2012.

[BS15a] Manjul Bhargava and Arul Shankar. Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. *Annals of Mathematics*, pages 191–242, 2015.

[BS15b] Manjul Bhargava and Arul Shankar. Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0. *Annals of Mathematics*, pages 587–621, 2015.

[BS15c] Bhargav Bhatt and Peter Scholze. The pro-étale topology for schemes. *Astérisque*, 360:99–201, 2015.

[BSD65] Bryan John Birch and Peter Francis Swinnerton-Dyer. Notes on elliptic curves. ii. *Journal für die reine und angewandte Mathematik*, 218:79–108, 1965.

[BSS18] Bhargav Bhatt, Christian Schnell, and Peter Scholze. Vanishing theorems for perverse sheaves on abelian varieties, revisited. *Selecta Mathematica*, 24:63–84, 2018.

[Cho08] Utsav Choudhury. Homotopy theory of schemes and a^1-fundamental groups. Master's thesis, Università degli Studi di Padova, 2008.

[CHT08] Laurent Clozel, Michael Harris, and Richard Taylor. Automorphy for some l-adic lifts of automorphic mod l galois representations. *Publications mathématiques*, 108:1–181, 2008.

[DA73] Pierre Deligne and Michael Artin. *Théorie des Topos et Cohomologies Étale des Schémas. Séminaire de Géométrie Algébrique due Bois-Marie 1963-1964 (SGA 4)*. Lecture Notes in Mathematics. Springer Berlin, 1973.

[DBG+77] Pierre Deligne, Jean-François Boutot, Alexander Grothendieck, Luc Illusie, and Jean-Louis Verdier. *Étale Cohomology. Séminaire de Géométrie Algébrique due Bois-Marie 1963-1964 (SGA 4 1/2)*. Lecture Notes in Mathematics. Springer-Verlag, 1977.

[Del80] Pierre Deligne. La conjecture de Weil : II. *Publications Mathématiques de l'IHÉS*, 52:137–252, 1980.

[Del89] Pierre Deligne. Le groupe fondamental de la droite projective moins trois points. In *Galois Groups over Q: Proceedings of a Workshop Held March 23–27, 1987*, pages 79–297. Springer, 1989.

[Dri89] Vladimir Gershonovich Drinfeld. Cohomology of compactified manifolds of modules of f-sheaves. *Journal of Soviet Mathematics*, 46(2):1789–1821, 1989.

[DZ19] Alexander Dunn and Alexandru Zaharescu. Sums of Kloosterman sums over primes in an arithmetic progression. *The Quaterly Journal of Mathematics*, 70(1):319–342, 2019.

[Eke07] Torsten Ekedahl. *On The Adic Formalism*, pages 197–218. Birkhäuser Boston, Boston, MA, 2007.

[FFK24] Arthur Forey, Javier Fresán, and Emmanuel Kowalski. Arithmetic fourier transforms over finite fields: generic vanishing, convolution, and equidistribution, 2024.

[FLR23] Tony Feng, Aaron Landesman, and Eric M. Rains. The geometric distribution of Selmer groups of elliptic curves over function fields. *Mathematische Annalen*, 387:615–687, 2023.

[Fu15] Lei Fu. *Etale Cohomology Theory*, volume 14 of *Nankai Tracts in Mathematics*. World Scientific, 2015.

[GL96] Ofer Gabber and François Loeser. Faisceaux pervers ℓ-adiques sur un tore. *Duke Math J.*, 83(3):501–606, 1996.

[Gol06] Dorian Goldfeld. Conjectures on elliptic curves over quadratic fields. In *Number Theory Carbondale 1979: Proceedings of the Southern Illinois Number Theory Conference Carbondale, March 30 and 31, 1979*, pages 108–118. Springer, 2006.

[GR04] Alexander Grothendieck and Michèle Raynaud. Revêtements étales et groupe fondamental (SGA 1). eprint arXiv matyh/0206203, 2004. Updated edition of the book of the same title published by Springer-Verlag in 1971 as volume 224 of the series Lecture Notes in Mathematics.

[Gro77] Alexander Grothendieck. *Cohomologie l-adique et fonctions L Séminaire de Géométrie Algébrique due Bois-Marie 1965-1966 (SGA 5)*, volume 589 of *Springer Lecture Notes*. Springer-Verlag, 1977. Avec la collaboration de I. Bucur, C. Houzel, L. Illusie, J.-P. Jouanolou, et J.-P. Serre.

[GV72] Alexander Grothendieck and Jean-Louis Verdier. *Theorie des Topos et Cohomologie Etale des Schemas. Seminaire de Geometrie Algebrique du Bois-Marie 1963-1964 (SGA 4)*. Lecture Notes in mathematics. Springer-Verlag Berlin Heidelberg, 1 edition, 1972.

[HB04] David Heath-Brown. The average analytic rank of elliptic curves. *Duke Math. J.*, 122:591–623, 2004.

[HK25] Chris Hall and Hyun Jong Kim. Independence of ℓ (title to be determined). In progress, 2025.

[HM73] Dale Husemoller and John Milnor. *Symmetric Bilinear Forms*, volume 73 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 2. Folge*. Springer Berlin Heidelberg, 1973.

[HSBT05] Michael Harris, Nick Shepherd-Barron, and Richard Taylor. Ihara's lemma and potential automorphy, 2005.

[Hub97] Annette Huber. Mixed perverse sheaves for schemes over number fields. *Compositio Mathematica*, 108:107–121, 1997.

[Jor05] Andrei Jorza. The birch and swinnerton-dyer conjecture for abelian varieties over number fields, 2005.

[Kat90] Nicholas M. Katz. *Exponential sums and differential equations*, volume 124 of *Annals of Mathematics Studies*. Princeton University Press, 1990.

[Kat96] Nicholas M. Katz. *Rigid Local Systems*, volume 139 of *annals of Mathematics Studies*. Princeton University Press, 1996.

[Kat98] Nicholas M. Katz. *Gauss Sums, Kloosterman Sums, and Monodromy Groups*, volume 116 of *Annals of Mathematics Studies*. Princeton University Press, 1998.

[Kat12] Nicholas M. Katz. *Convolution and Equidistribution Sato-Tate Theorems for Finite-Field Mellin Transforms*, volume 180 of *Annals of Mathematics Studies*. Princeton University Press, 2012.

[Kim23] Hyun Jong Kim. `trouver`, 2023. GitHub repository: https://github.com/hyunjongkimmath/trouver.

[KL85] Nicholas M. Katz and Gérard Laumon. Transformation de fourier et majoration de sommes exponentielles. *Publications Mathématiques de l'IHÉS*, 62:145–202, 1985.

[KM23] Seoyoung Kim and M. Ram Murty. From the Birch and Swinnerton-Dyer conjecture to Nagao's conjecture. *Mathematics of Computation*, 92(339):385–408, 2023.

[KMS17] Emmanuel Kowalski, Philippe Michel, and Will Sawin. Bilinear forms with Kloosterman sums and applciations. *Annals of Mathematics*, 186:413–500, 2017.

[Krä14] Thomas Krämer. Perverse sheaves on semiabelian varieties. *Rendiconti del Seminario Matematico della Università di Padova*, 132:83–102, 2014.

[KS99] Nicholas M. Katz and Peter Sarnak. *Random matrices, Frobenius eigenvalues, and monodromy*, volume 45. American Mathematical Society, 1999.

[KW13] Reinhardt Kiehl and Rainer Weissauer. *Weil Conjectures, Perverse Sheaves and ℓ'adic Fourier Transform*, volume 42 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics*. Springer Berlin, Heidelberg, 2013.

[KW15] Thomas Krämer and Rainer Weissauer. Vanishing theorems for constructible sheaves on abelian varieties. *J. Algebraic Geometry*, 24:531–568, 2015.

[Laf02] Laurent Lafforgue. Chtoucas de Drinfeld et correspondance de Langlands. *Inventiones mathematicae*, 147:1–241, 2002.

[May99] Jon Peter May. *A Concise Course in Algebraic Topology*. Chicago Lectures in Mathematics. University of Chicago Press, 1999.

[Mil80] James S. Milne. *Etale cohomology*. Number 33 in Princeton Mathematical Series. Princeton university press, 1980.

[Mil07] James S. Milne. Quotients of Tannakian categories. *Theory and Applications of Categories*, 18(21):654–664, 2007.

[Mil13] James S. Milne. Lie algebras, algebraic groups, and lie groups, 2013. Available at www.jmilne.org/math/.

[Mil17] James S. Milne. *Algebraic Groups*, volume 170 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, 2017.

[Mor06] Fabien Morel. A1-algebraic topology. In *International Congress of Mathematicians*, volume 2, pages 1035–1059, 2006.

[Mor12] Fabien Morel. *A1-Algebraic Topology over a field*. Lecture Notes in Mathematics. Springer Berlin, Heidelberg, 2012.

[MV99] Fabien Morel and Vladimir Voevodsky. A1-homotopy theory of schemes. *Publications Mathématiques de l'IHÉS*, 90:45–143, 1999.

[Nag97] Koh-ichi Nagao. Q(t)-rank of elliptic curves and certain limit coming from the local points. *Manuscripta mathematica*, 92(1):13–32, 1997.

[nLa25a] nLab authors. geometric morphism. `https://ncatlab.org/nlab/show/geometric+morphism`, July 2025. Revision 61.

[nLa25b] nLab authors. homotopy group of a spectrum. `https://ncatlab.org/nlab/show/homotopy+group+of+a+spectrum`, June 2025. Revision 7.

[nLa25c] nLab authors. Introduction to Stable homotopy theory – 1-1. `https://ncatlab.org/nlab/show/Introduction+to+Stable+homotopy+theory+--+1-1`, June 2025. Revision 43.

[nLa25d] nLab authors. model structure on topological sequential spectra. `https://ncatlab.org/nlab/show/model+structure+on+topological+sequential+spectra`, June 2025. Revision 61.

[nLa25e] nLab authors. point of a topos. `https://ncatlab.org/nlab/show/point+of+a+topos`, July 2025. Revision 53.

[nLa25f] nLab authors. sheafification. `https://ncatlab.org/nlab/show/sheafification`, September 2025. Revision 40.

[nLa25g] nLab authors. stable homotopy category. `https://ncatlab.org/nlab/show/stable+homotopy+category`, June 2025. Revision 31.

[Poo18] Bjorn Poonen. Heuristics for the arithmetic of elliptic curves. In *Proceedings of the International Congress of Mathematicians: Rio de Janeiro 2018*, pages 399–414. World Scientific, 2018.

[PR12] BJORN POONEN and ERIC RAINS. Random maximal isotropic subspaces and selmer groups. *Journal of the American Mathematical Society*, 25(1):245–269, 2012.

[Ros02] Michael Rosen. *Number Theory in Function Fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag New York, 2002.

[RS98] Michael Rosen and Joseph H. Silverman. On the rank of an elliptic surface. *Inventiones mathematicae*, 133:43–67, 1998.

[Rud87] Walter Rudin. *Real and Complex Analysis*. Mathematics Series. McGraw-Hill Book Company, 3 edition, 1987.

[Saw24] Will Sawin. General multiple dirichlet series from perverse sheaves. *Journal of Number Theory*, 262:408–453, 2024.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. math*, 15:259–331, 1972.

[SFFK23] Will Sawin, Arthur Forey, Javier Fresán, and Emmanuel Kowalski. Quantitative sheaf theory. *Journal of the American Mathematical Society*, 36(3):653–726, 2023.

[Sil89] Joseph H. Silverman. Elliptic curves of bounded degree and height. *Proceedings of the American Mathematical Society*, 105(3):540–545, 1989.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, 2 edition, 2009.

[ST21] Will Sawin and Jacob Tsimerman. Bounds for the stalks of perverse sheaves in characteristic p and a conjecture of shende and tsimerman. *Inventiones mathematicae*, 224(1):1–32, 2021.

[Sta25] The Stacks project authors. The stacks project. `https://stacks.math.columbia.edu`, 2025.

[Tat65] John T. Tate. Algebraic cycles and poles of zeta functions. In *Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963)*, pages 93–110. Harper & Row, 1965. Also in Collected works of John Tate (2 vols.), Amer. Math. Soc. (2016), vol. 2.

[Tat66] John Tate. On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. In *Séminaire Bourbaki : années 1964/65 1965/66, exposés 277-312*, number 9 in Astérisque, pages 415–440. Société mathématique de France, 1966. talk:306.

[Tay08] Richard Taylor. Automorphy for some l-adic lifts of automorphic mod l galois representations. ii. *Publications mathématiques*, 108:183–239, 2008.

[Voe98] Vladimir Voevodsky. A1-homotopy theory. In *Proceedings of the international congress of mathematicians*, volume 1, pages 579–604. Berlin, 1998.

[Wei94] Charles A. Weibel. *An Introduction to Homological Algebra*, volume 38 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, 1994. First paperback edition 1995 Reprinted 1997.

[Wik25] Wikipedia contributors. Frobenius endomorphisms#frobenius for schemes — Wikipedia, the free encyclopedia, 2025. [Online; accessed 08-July-2025].

[You06] Matthew Young. Low-lying zeros of families of elliptic curves. *Journal of the American Mathematical Society*, 19(1):205–250, 2006.